Bitdefender

GravityZone

Digitally signed by Celonenco Vitalie
Date: 2021.04.07 15:44:29 EEST
Reason: MoldSign Signature
Location: Moldova

РУКОВОДСТВО АДМИНИСТРАТОРА

Bitdefender GravityZone
Руководство администратора

Дата публикации 2021.02.03

Авторские права© 2021 Bitdefender

Правовое положение

Все права защищены. Никакая часть этой публикации не может быть воспроизведена или передана в любой форме или любыми средствами, электронными или механическими, включая фотокопирование, запись, использование средств хранения и поиска информации, без получения письменного разрешения уполномоченного представителя компании Bitdefender Использование цитат в обзорах разрешается только со ссылкой на цитируемый источник. Запрещено вносить какие-либо изменения в данный материал.

Предупреждение и ограничение ответственности. Данный программный продукт и документация к нему защищены авторским правом. Данный программный продукт и документация к нему защищены авторским правом. Информация в этом документе предоставляется «как есть», без гарантии. Хотя в ходе подготовки этого документа были приняты все меры предосторожности, авторы не несут никакой ответственности перед любым лицом или организацией в отношении каких-либо потерь или ущерба, причиненных или предположительно вызванных прямо или косвенно информацией, содержащейся в документе.

Данная книга содержит ссылки на сторонние веб-сайты, не находящихся под контролем Bitdefender ,поэтому Bitdefender не несет ответственности за их содержание Переходя на сторонние сайты, указанные в документе, вы делаете это на свой страх и риск. Bitdefender приводит эти ссылки только для удобства читателя, но наличие этих ссылок не означает, что Bitdefender берет на себя ответственность за содержание какого-либо стороннего веб-сайта.

Торговые марки. В этом документе могут упоминаться различные торговые марки. В этом документе могут упоминаться различные торговые марки. Все зарегистрированные и незарегистрированные торговые марки, упоминаемые в этом документе, принадлежат только их законным владельцам.

Содержание

Предисловие ... ix
1. Обозначения, используемые в данном руководстве ... ix
1. О GravityZone ... 1
2. Уровни защиты GravityZone ... 2
2.1. Защита от вредоносного ПО ... 2
2.2. Расширенный контроль угроз (Advanced Threat Control) ... 4
2.3. Обнаружение гипервизора ... 4
2.4. Advanced Anti-Exploit ... 5
2.5. Брандмауэр ... 5
2.6. Контроль контента ... 5
2.7. Network Attack Defense ... 5
2.8. Управление исправлениями ... 6
2.9. Контроль устройств ... 6
2.10. Полное шифрование диска ... 6
2.11. Security for Exchange ... 7
2.12. Контроль приложений ... 7
2.13. Sandbox Analyzer ... 7
2.14. События ... 8
2.15. Hypervisor Memory Introspection (HVI) ... 8
2.16. Network Traffic Security Analytics (NTSA) ... 9
2.17. Security for Storage ... 10
2.18. Security for Mobile ... 10
2.19. Доступность уровней защиты GravityZone ... 11
3. Архитектура GravityZone ... 12
3.1. GravityZone VA ... 12
3.1.1. База данных GravityZone ... 13
3.1.2. Сервер обновлений GravityZone ... 13
3.1.3. Коммуникационный Сервер GravityZone ... 13
3.1.4. Сервер обновлений GravityZone ... 13
3.1.5. Веб-консоль (GravityZone Control Center) ... 13
3.2. Security Server ... 14
3.3. Дополнительный пакет HVI ... 14
3.4. Агенты безопасности ... 14
3.4.1. Bitdefender Endpoint Security Tools ... 15
3.4.2. Endpoint Security for Mac ... 17
3.4.3. GravityZone Mobile Client ... 18
3.4.4. Bitdefender Tools (vShield) ... 18
3.5. Sandbox Analyzer Архитектура ... 18
4. Начало работы ... 21
4.1. Подключение к Control Center ... 21
4.2. Интуитивно понятная Control Center ... 22
4.2.1. Обзор Control Center ... 22
4.2.2. Таблица данных ... 24

4.2.3. Панели инструментов . . . 26
4.2.4. Контекстное меню . . . 26
4.2.5. Выбор просмотра . . . 27
4.3. Управление вашей учетной записью . . . 28
4.4. Изменение пароля для входа в систему . . . 31

5. Учетные записи пользователей . . . 32
5.1. Роли пользователей . . . 33
5.2. Права пользователя . . . 35
5.3. Управление учетными записями пользователей . . . 35
5.3.1. Индивидуальное управление учетными записями пользователей . . . 36
5.3.2. Управление несколькими учетными записями пользователей . . . 39
5.4. Сброс паролей входа . . . 44
5.5. Управление двухфакторной аутентификацией . . . 44

6. Управление сетевыми объектами . . . 47
6.1. Виды сетей . . . 49
6.1.1. Компьютеры и виртуальные машины . . . 49
6.1.2. Виртуальные машины . . . 50
6.1.3. Мобильные устройства . . . 51
6.2. Компьютеры . . . 52
6.2.1. Проверка статуса компьютера . . . 53
6.2.2. Получение сведений о компьютере . . . 56
6.2.3. Организация компьютеров в группы . . . 71
6.2.4. Сортировка, фильтрация и поиск компьютеров . . . 73
6.2.5. Запущенные Задачи . . . 76
6.2.6. Формирование быстрых отчетов . . . 113
6.2.7. Назначение политик . . . 113
6.2.8. . . . 115
6.2.9. Синхронизация со службой каталогов Active Directory . . . 116
6.3. Виртуальные машины . . . 116
6.3.1. Проверять статусы виртуальных машин . . . 118
6.3.2. Просмотр подробной информации о виртуальной машине . . . 122
6.3.3. Организация виртуальных машин в группы . . . 131
6.3.4. Сортировка, фильтрация и поиск виртуальных машин . . . 133
6.3.5. Запуск задач на виртуальных машинах . . . 138
6.3.6. Формирование быстрых отчетов . . . 177
6.3.7. Назначение политик . . . 177
6.3.8. Использование Менеджер восстановления (Recovery Manager) для зашифрованных томов . . . 179
6.3.9. Очистка Лицензионных мест . . . 180
6.4. Мобильные устройства . . . 180
6.4.1. Добавление настраиваемых пользователей . . . 182
6.4.2. Добавление мобильных устройств пользователям . . . 183
6.4.3. Организация настраиваемых пользователей в группы . . . 186
6.4.4. Проверка статуса мобильных устройств . . . 188
6.4.5. Совместимые и несовместимые мобильные устройства . . . 189
6.4.6. Проверка подробной информации о пользователях и мобильных устройствах . . . 191

6.4.7. Сортировка, фильтрация и поиск мобильных устройств . . . 194
6.4.8. Запуск задач на мобильных устройствах . . . 199
6.4.9. Формирование быстрых отчетов . . . 204
6.4.10. Назначение политик . . . 205
6.4.11. Синхронизация со службой каталогов Active Directory . . . 206
6.4.12. Удаление пользователей и мобильных устройств . . . 207
6.5. Инвентаризация Приложений . . . 208
6.6. Инвентаризация патча . . . 214
6.6.1. Получение сведений о патчах . . . 215
6.6.2. Поиск и фильтрация патчей . . . 216
6.6.3. Игнорирование исправлений . . . 218
6.6.4. Установка патчей . . . 218
6.6.5. Удаление патчей . . . 220
6.6.6. Создание статистики исправлений . . . 222
6.7. Просмотр и управление задачами . . . 223
6.7.1. Проверить статус задачи . . . 224
6.7.2. Просмотр отчетов задач . . . 226
6.7.3. Перезапуск задач . . . 226
6.7.4. Остановка задач сканирования Exchange . . . 227
6.7.5. Удаление задач . . . 227
6.8. Удаление конечных точек из сетевого содержимого . . . 228
6.9. Настройка параметров сети . . . 229
6.9.1. Настройки инвентаризации сети . . . 229
6.9.2. Автономное удаление машин . . . 230
6.10. Конфигурация настроек Security Server . . . 232
6.11. Диспетчер учетных данных (Credentials Manager) . . . 233
6.11.1. Операционная система . . . 234
6.11.2. Виртуальная среда . . . 235
6.11.3. Удаление учетных данных из диспетчера учетных данных . . . 236

7. Политики безопасности (Security Policies) . . . 237
7.1. Управление политиками . . . 238
7.1.1. Создание политик . . . 239
7.1.2. Назначение политик . . . 241
7.1.3. Изменение настроек политики . . . 252
7.1.4. Изменение имен политик . . . 253
7.1.5. Удаление политик . . . 253
7.2. Политики компьютеров и виртуальных машин . . . 254
7.2.1. Основные . . . 255
7.2.2. HVI . . . 271
7.2.3. Защита от вредоносного ПО . . . 280
7.2.4. Sandbox Analyzer . . . 323
7.2.5. Брандмауэр . . . 331
7.2.6. Защита сети . . . 347
7.2.7. Управление исправлениями . . . 363
7.2.8. Контроль приложений . . . 367
7.2.9. Контроль устройств . . . 373
7.2.10. Ретранслятор . . . 379
7.2.11. Защита Exchange . . . 381

7.2.12. Шифрование . . . 415
7.2.13. NSX . . . 420
7.2.14. Защита хранилища . . . 420
7.2.15. Инциденты Sensor . . . 424
7.3. Политики мобильных устройств . . . 425
7.3.1. Основные . . . 426
7.3.2. Управление устройствами . . . 426

8. Информационная панель мониторинга . . . 449
8.1. Панель управления . . . 449
8.1.1. Обновление данных портлета . . . 450
8.1.2. Редактирование настроек портлета . . . 451
8.1.3. Добавление нового портлета . . . 451
8.1.4. Удаление портлета . . . 451
8.1.5. Расположение портлетов . . . 451

9. Расследование происшествий . . . 453
9.1. Страница инцидентов . . . 453
9.1.1. Сетка фильтров . . . 455
9.1.2. Просмотр списка событий безопасности . . . 458
9.1.3. Обзор обнаруженных угроз . . . 462
9.2. Занесение в черный список . . . 508

10. Использование отчетов . . . 512
10.1. Типы отчетов . . . 512
10.1.1. Отчеты по компьютерам и виртуальным машинам . . . 513
10.1.2. Отчеты сервера Exchange . . . 528
10.1.3. Отчеты по мобильным устройствам . . . 532
10.2. Создание отчетов . . . 534
10.3. Просмотр и управление отчетами по расписанию . . . 537
10.3.1. Просмотр отчетов . . . 538
10.3.2. Редактирование отчетов по расписанию . . . 538
10.3.3. Удаление отчета по расписанию . . . 540
10.4. Выполнение действий, основанные на данных отчета . . . 540
10.5. Сохранение отчетов . . . 541
10.5.1. Экспорт отчетов . . . 541
10.5.2. Загрузка отчетов . . . 542
10.6. Отправка отчетов . . . 542
10.7. Печать отчетов . . . 543

11. Карантин . . . 544
11.1. Просмотр карантина . . . 544
11.2. Карантин компьютеров и виртуальных машин . . . 545
11.2.1. Просмотр подробной информации карантина . . . 545
11.2.2. Управление файлами в карантине . . . 546
11.3. Карантин серверов Exchange . . . 551
11.3.1. Просмотр подробной информации карантина . . . 551
11.3.2. Объекты на карантине . . . 553

12. Использование Sandbox Analyzer . . . 557

12.1. Фильтрация карточек отправки . . . 557
12.2. Просмотр подробностей анализа . . . 560
12.3. Повторное представление образца . . . 561
12.4. Удаление карточек подачи . . . 563
12.5. Manual Submission . . . 563
12.6. Инфраструктура управления Sandbox Analyzer . . . 566
12.6.1. Проверка статуса Sandbox Analyzer . . . 566
12.6.2. Настройка одновременных детонаций . . . 568
12.6.3. Проверка состояния VM. . . . 569
12.6.4. Настройка и управление VM . . . 570

13. Журнал активности пользователя . . . 572

14. Использование инструментов . . . 574
14.1. Ввод инструментов пользователя с HVI . . . 574

15. Уведомления . . . 576
15.1. Типы уведомлений . . . 576
15.2. Просмотр уведомлений . . . 586
15.3. Удаление уведомлений . . . 587
15.4. Настройка параметров уведомлений . . . 588

16. Статус системы . . . 591
16.1. Состояние OK . . . 592
16.2. Статус учетной записи . . . 592
16.3. Параметры . . . 593

17. Получение справки . . . 596
17.1. Центр поддержки Bitdefender . . . 596
17.2. Обращение за помощью . . . 598
17.3. Использование инструментов поддержки . . . 598
17.3.1. Использование инструмента поддержки на операционных системах Windows . . . 598
17.3.2. Использование инструмента поддержки на операционных системах Linux . . . 600
17.3.3. Использование инструментов поддержки на операционных системах Mac . . . 601
17.4. Контактная информация . . . 602
17.4.1. Адреса веб-сайтов . . . 603
17.4.2. Местные дистрибьюторы . . . 603
17.4.3. Офисы Bitdefender . . . 603

A. Приложения . . . 607
A.1. Поддерживаемые типы файлов . . . 607
A.2. Типы сетевых объектов и статусы . . . 608
A.2.1. Типы сетевых объектов . . . 608
A.2.2. Состояние сетевых объектов . . . 609
A.3. Типы файлов приложений . . . 610
A.4. Фильтрация вложений по типу файлов . . . 611
A.5. Системные переменные . . . 611
A.6. Инструменты модуля Управления приложениями . . . 613
A.7. Объекты Sandbox Analyzer . . . 614

A.7.1. Поддерживаемые Типы и Расширения Фалов для Отправки Вручную 614
A.7.2. Типы Файлов Поддерживаемые Предварительной Фильтрацией Контента при Автоматической Отправке 615
A.7.3. Исключения По Умолчанию в Автоматической Отправке 615
A.7.4. Рекомендуемые приложения для детонации виртуальных машин 615
A.8. Процессоры данных 616

Глоссарий 619

Предисловие

Это руководство предназначено для сетевых администраторов, отвечающий за управление защитой GravityZone в своих организациях.

Цель данного документа объяснить, как применять и просматривать параметры безопасности конечных точек сети, под своей учетной записью, используя GravityZone Control Center. Вы узнаете, как просматривать инвентаризацию сети в Control Center, как создавать и применять политику на управляемых конечных точках, как создавать отчеты, как управлять карантином и как использовать панель управления.

1. Обозначения, используемые в данном руководстве

Типографские обозначения

Это руководство использует несколько текстовых стилей для улучшения читаемости. Узнайте об их аспекте и значении из таблицы ниже.

Виды шрифтов и стилей	Описание
`образец`	Встроенные имена команд и синтаксис, пути и имена файлов, файлы конфигурации, вводимый текст печатается стандартными `моноширинными` шрифтами.
http://www.bitdefender.com	Ссылки URL на внешние источники (http или ftp серверы).
gravityzone-docs@bitdefender.com	Адреса электронной почты в тексте приводятся в качестве контактной информации.
«Предисловие» (p. ix)	В кавычках приводятся внутренние ссылки на другие материалы в пределах этого документа.
опция	Все параметры продукта выделены **жирным** шрифтом.

Виды шрифтов и стилей	Описание
ключевое слово	Опции интерфейса, ключевые слова или сочетания клавиш выделены с помощью **bold** шрифта.

Примечания

Примечания — это текстовая информация, выделенная в основном тексте различными средствами, целью которой является привлечение вашего внимания к дополнительной информации, имеющей отношение к содержанию текущего раздела руководства.

Примечание
Примечание – это краткое замечание. Вы можете пропустить его, но в нем может содержаться ценная информация, например определенная особенность или ссылка на источник, имеющий отношение к данному материалу.

Важно
Эта информация требует вашего внимания, и ее не рекомендуется пропускать. Обычно, здесь приводится важная информация о факторах, которые не имеют угрожающего характера для безопасности вашей системы.

Предупреждение
Это критическая информация, к которой следует отнестись с максимальным вниманием. Ничего плохого не случится, если вы будете следовать указаниям. Внимательно прочтите и попытайтесь понять суть предупреждения, поскольку в нем описываются весьма опасные угрозы для безопасности вашей системы.

1. О GRAVITYZONE

Решение GravityZone было разработано специально для виртуализированных сред и облаков, с помощью которых можно предоставлять услуги по защите бизнеса для физических конечных устройств (в том числе мобильных), виртуальных машин в частных и общедоступных облаках, а также почтовых серверов Exchange.

GravityZone это продукт с единой консолью управления доступной в облаке, предоставляемый Bitdefender, или организованный в качестве виртуального устройства установленного локально в компании, что обеспечивает единую точку для развертывания, соблюдения и управления политиками безопасности для любого количества конечных точек, любого типа, в любом месте.

GravityZone обеспечивает несколько уровней безопасности для конечных точек, почтовых серверов Microsoft Exchange: защита от вредоносного ПО с мониторингом поведения, защита от угроз нулевого дня, контроль приложений и "песочница", межсетевой экран, управление устройствами, управление контентом, антифишинг и антиспам.

2. УРОВНИ ЗАЩИТЫ GRAVITYZONE

GravityZone обеспечивает следующие уровни защиты:

- Защита от вредоносного ПО
- Расширенный контроль угроз (Advanced Threat Control)
- Обнаружение гипервизора
- Advanced Anti-Exploit
- Брандмауэр
- Контроль контента
- Управление исправлениями
- Контроль устройств
- Полное шифрование диска
- Security for Exchange
- Контроль приложений
- Sandbox Analyzer
- Обнаружение и отклик конечной точки (EDR)
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Защита от вредоносного ПО

Уровень защиты от вредоносного ПО основан на сканировании сигнатур и эвристическом анализе (B-HAVE, ATC) против: вирусов, червей, троянов, программ-шпионов, рекламного ПО, кейлоггеров, руткитов и других типов вредоносных программ.

Технология сканирования Bitdefender на наличие вредоносного ПО основана на следующих технологиях:

- Во-первых, используется традиционный метод сканирования, когда отсканированное содержимое сравнивается с базой данных сигнатур. В базе данных сигнатур содержатся записи байт-кодов, характерные для известных угроз, которые регулярно обновляются Bitdefender. Этот метод сканирования является эффективным против известных угроз, которые были исследованы и задокументированы. Тем не менее, независимо от того, насколько оперативно база данных обновляет записи, всегда есть

окно уязвимости между временем, когда новая угроза обнаружена и когда исправление выпущено.

- Против новых, незарегистрированных угроз, защиту осуществляет второй слой Bitdefender, используя эвристический двигатель **B-HAVE**. Эвристические алгоритмы обнаруживают вредоносные программы на основе поведенческих характеристик. B-HAVE запускает подозрительные вредоносные программы в виртуальной среде, чтобы проверить их воздействие на систему и удостовериться, что они не представляют никакой угрозы. Если угроза обнаружена, предотвращается запуск программы.

Сканирующие движки

Bitdefender GravityZone может автоматически выбирать антивирусные движки при создании пакетов агентов безопасности в соответствии с конфигурацией конечной точки.

Также администратор может подстроить сканирующий движок, выбирая между несколькими технологиями сканирования:

1. **Локальное сканирование**, когда сканирование выполняется на конечном устройстве. Режим локального сканирования подходит для мощных машин, где все механизмы защиты хранятся локально.
2. **Гибридное сканирование со световыми двигателями (общее облако)**, для средних групп, использует сканирование в облаке и, частично, локальные механизмы защиты. Данный режим сканирования предоставляет лучшее задействование ресурсов, по сравнению с использованием удаленного сканирования.
3. **Централизованное сканирование в общем или частном облаке** с небольшим объемом памяти, требующим Security Server для сканирования. В этом случае механизмы защиты не хранятся локально и сканирование выгружается на Security Server.

Примечание
Существует минимальный набор движков, хранящийся локально, необходимый для распаковки сжатых файлы.

4. **Централизованное сканирование (сканирование в частном или публичном облаке с помощью Security Server) с локальным резервом* (Local Scan - при наличии полных движков).**
5. **Централизованное сканирование (сканирование в частном или публичном облаке с помощью Security Server) с резервом* гибридного сканирования (Local Scan - публичное облако с облегченным движками).**

* Когда используются двойные движки сканирования - если первый движок не доступен, резервный движок может быть задействован. Потребление ресурсов и утилизация сети будет зависеть от используемых движков.

2.2. Расширенный контроль угроз (Advanced Threat Control)

Для угроз, которые ускользают даже от эвристического движка, присутствует еще один слой защиты в виде Advanced Threat Control (ATC).

ATC постоянно отслеживает запущенные процессы и оценивает подозрительное поведение, такое как: попытки замаскировать тип процесса, выполнение кода в пространстве памяти процесса (захват памяти для привилегированной эскалации), репликация, перемещение файлов, скрытность в списке технологических процессов и т.д. Каждое подозрительное поведение повышает рейтинг процесса. Когда достигается порог, включается сигнал тревоги.

2.3. Обнаружение гипервизора

Bitdefender HyperDetect - дополнительный уровень безопасности, разработанный специально для обнаружения продвинутых атак и подозрительной активности ещё до выполнения процессов. HyperDetect содержит модели машинного обучения и технологии обнаружения скрытых атак против угроз, таких как: атаки нулевого дня, продвинутые устойчивые угрозы (APT), скрытое вредоносное ПО, безфайловые атаки (злоупотребление PowerShell, инструментарием управления Windows и т. д.), кража учетных данных, целевые кибератаки, специализированное вредоносное ПО, атаки на основе сценариев, эксплойты, инструменты взлома, подозрительный сетевой трафик, потенциально нежелательные приложения (PUA), вымогатели.

2.4. Advanced Anti-Exploit

Основанная на машинном обучении, технология Advanced Anti-Exploit блокирует атаки нулевого дня, использующие трудно-обнаруживаемые эксплойты. Advanced anti-exploit в режиме реального времени отслеживает последние эксплойты и устраняет уязвимости повреждения памяти, которые могут использоваться для обхода существующих решений безопасности. Технология защищает большинство стандартных приложений, таких как браузеры, редакторы Microsoft Office и Adobe Reader и другие. Модуль следит за системными процессами и защищает от брешей в безопасности и перехватов существующих процессов.

2.5. Брандмауэр

Брандмауэр контролирует доступ приложений к сети и к Интернету. Доступ разрешается автоматически, основываясь на базе данных известных, легитимных приложений. Кроме того, брандмауэр может защитить систему от сканирования портов, ограничивать использование общего доступа к Интернет (ICS) и предупредить, когда новые узлы подключаются по Wi-Fi.

2.6. Контроль контента

Модуль Контентного Контроля помогает обеспечить соблюдение политики компании в отношении разрешенного трафика, веб-доступа, защиты данных и контроля приложений. Администраторы могут задавать параметры сканирования трафика и исключения, составлять график доступа к веб, блокировать или разрешать определенные веб-адреса или категории, настраивать правила защиты данных и устанавливать разрешения для использования конкретных приложений.

2.7. Network Attack Defense

Модуль Network Attack Defense опирается на технологии Bitdefender, нацеленные на распознание сетевых атак, целью которых является получение доступа к конечным точкам при помощи таких средств как: атаки методом перебора, сетевые "эксплоиты", программы для кражи паролей, векторы заражения посредством скрытой загрузки, боты и трояны.

2.8. Управление исправлениями

Полностью интегрированный в GravityZone, модуль управления исправлениями поддерживает последнюю версию операционной системы и приложений, а также обеспечивает полное представление о состоянии исправления в управляемых точках Windows.

Модуль управление исправлениями GravityZone включает несколько особенностей, таких как сканирование патчей по требованию / запланированное, автоматическое / ручное сканирование исправлений или создание отчетов об отсутствующих патчах.

Вы можете узнать больше о продавцах и продуктах управления исправлениями GravityZone из этой статьи базы знаний.

Примечание
Модуль управления исправлениями - это дополнение, доступное при наличии отдельного лицензионного ключа для всех доступных пакетов GravityZone.

2.9. Контроль устройств

Модуль Контроля устройств позволяет предотвратить утечки конфиденциальных данных и проникновение вредоносного ПО через внешние устройства, подключаемые к конечным точкам, применяя блокирующие правила и исключения с помощью политик для широкого спектра устройств (таких, как USB флэш-накопители, устройства Bluetooth, CD/DVD-плееры, устройства хранения, и т.д.).

2.10. Полное шифрование диска

Данный уровень защиты позволяет Вам осуществлять шифрование всего диска на машине, управляя BitLocker для Windows, и FileVault и diskutil для macOS. Вы можете зашифровать и дешифровать загрузочные и обычные тома одним щелчком мыши, т.к. GravityZone обрабатывает весь процесс с минимальным вмешательством со стороны пользователей. Кроме того, GravityZone хранит ключи восстановления, необходимые для разблокировки томов, на тот случай, если пользователь забыл свой пароль.

Примечание
Полное шифрование диска - это дополнение, доступное при наличии отдельного лицензионного ключа для всех доступных пакетов GravityZone.

2.11. Security for Exchange

Bitdefender обеспечивает защиту Security for Exchange от вредоносных программ, антиспам, антифишинг, фильтрацию контента и содержимого писем, полностью интегрирована с серверами Microsoft Exchange, для обеспечения безопасной среды обмена сообщениями и повышения производительности. Используя признанные технологии защиты от вредоносных программ и спама, программа защищает пользователей Exchange от новейших, самых сложных вредоносных программ и от попыток украсть конфиденциальные и ценные данные пользователей.

Важно

Security for Exchange разработан для защиты всей Exchange-организации, к которой принадлежит защищаемый Exchange-сервер. Это означает, что происходит защита всех активных почтовых ящиков, включая user/room/equipment/shared mailboxes.

В дополнение к защите Microsoft Exchange, эта лицензия также покрывает установленные на сервере модули защиты конечных точек.

2.12. Контроль приложений

Модуль Управления приложениями предотвращает активность вредоносных программ, атаки "нулевого дня" и повышает безопасность, не влияя на производительность. Управление приложениями обеспечивает гибкое соблюдение политик для приложений из "белого" списка, который идентифицирует, предотвращает установку и выполнение каких-либо нежелательных, ненадежных или вредоносных приложений.

2.13. Sandbox Analyzer

Bitdefender Sandbox Analyzer обеспечивает мощный уровень защиты от продвинутых угроз путем автоматического и глубокого анализа подозрительных файлов, не подписанных антивирусным движком Bitdefender. В «песочнице» используется обширный набор технологий Bitdefender для выполнения полезных нагрузок в изолированной виртуальной среде, размещенной в Bitdefender или развернутой локально, анализа их поведения и сообщения о любых тонких системных изменениях, которые свидетельствуют о противоправных действиях.

Sandbox Analyzer использует серию датчиков для детонации контента с управляемых конечных точек, потоков сетевого трафика, централизованного карантина и серверов ICAP.

Кроме того, Sandbox Analyzer позволяет передать образцы вручную и через API.

Примечание
Функциональность этого модуля может быть предоставлена Sandbox Analyzer Cloud и Sandbox Analyzer On-Premises. Sandbox Analyzer On-Premises доступен с отдельным лицензионным ключом.

2.14. События

Характеристика инцидента - это компонент корреляции событий, способный выявлять сложные угрозы или активные атаки. В рамках корпоративной интегрированной платформы характеристика инцидентов объединяет возможности всех устройств, работающих в корпоративной сети. Это решение приходит на помощь в случаях, когда группы немедленного реагирования распознают и отвечают на серьезные угрозы.

Посредством Bitdefender Endpoint Security Tools Вы можете активировать защитный модуль, который называется датчиком инцидентов, в управлении конечной точки, чтобы объединять данные компьютера и операционной системы. Сбор и обработка метаданных с обеих сторон идет на платформе клиент-сервер.

Этот компонент несет детальную информацию по обнаруженным происшествиям, интерактивной карте происшествий, действиям по исправлению и интеграции с Sandbox Analyzer и HyperDetect.

2.15. Hypervisor Memory Introspection (HVI)

Широко известно, что высоко организованные, ориентированные на извлечение прибыли, злоумышленники, ищут неизвестные уязвимости (уязвимости нулевого дня) или используют разовые, специально встроенные эксплойты (эксплойты нулевого дня) и другие инструменты. Злоумышленники также используют передовые методы, чтобы задерживать и последовательно атаковать полезную нагрузку, для маскировки вредоносной активности. Более новые, управляемые атаки, в целях извлечения прибыли, построены

таким образом, чтобы быть незаметными и обходить традиционные средства безопасности.

Для виртуальных сред проблема теперь решена, HVI защищает дата-центры с высокой плотностью виртуальных машин против передовых и сложных угроз, что не могут сделать движки на основе сигнатурного анализа. Это достигается соблюдением строгой изоляции, что обеспечивает обнаружение атак в реальном масштабе времени, их блокировку, как только они происходят, и немедленное удаление угроз.

Будет ли защищенная машина на Windows или Linux, сервер или рабочая станция, HVI даст представление на уровне, который невозможно достичь на уровне гостевой операционной системы. Подобно тому, как гипервизор контролирует доступ к оборудованию от имени каждой гостевой виртуальной машины, HVI имеет глубокое "понимание" как оба режима - пользователя и ядра, ведут себя в "гостевой" памяти. В результате HVI имеет полное представление о гостевой памяти, и, следовательно, ее полный контекст. В то же время, HVI изолирован от защищенных гостей, так же, как изолирован и сам гипервизор. Действуя на уровне гипервизора и используя функциональные возможности гипервизора, HVI превосходит технические возможности традиционных систем безопасности для выявления вредоносной активности в дата-центрах.

HVI идентифицирует методы атаки, а не шаблоны атаки. Таким образом, технология может идентифицировать, информировать и предотвращать общие методы взломов. Ядро защищено от методов взлома, типа руткит, которые используются во время атаки цели, чтобы обеспечить незаметность. Пользовательские процессы также защищены от внедрения кода, функции обхода и выполнения кода из стека.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

2.16. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) - сетевое решение безопасности, которое анализирует потоки трафика IPFIX на наличие подозрительного поведения и вредоносного ПО.

Bitdefender NTSA предназначен для того, чтобы действовать наряду с вашими существующими мерами безопасности как дополнительная гарантия, которая

способна покрыть слепые зоны, не отслеживаемые традиционными инструментами.

Традиционные инструменты безопасности сетей обычно пытаются предотвратить вредоносные заражения анализируя входящий трафик (с помощью песочницы, брандмауэра, антивируса и т.д.) Bitdefender NTSA фокусируется исключительно на анализе исходящего сетевого трафика на наличие подозрительного поведения.

2.17. Security for Storage

GravityZone Security for Storage предоставляет защиту в реальном времени для ведущих систем обмена файлами и сетей хранения. Система и алгоритмы обнаружения угроз обновляются автоматически - без каких-либо усилий с вашей стороны или создания помех для конечных пользователей.

Два или более GravityZone Security Servers Multi-Platform выполняет роль сервера ICAP выполнять роль сервера ICAP, предоставляющего службы защиты от вредоносных программ для устройств сетевого хранилища (NAS) и систем совместного использования файлов, соответствующих протоколу Internet Content Adaptation Protocol (ICAP, как определено в RFC 3507).

Когда пользователь делает запрос на открытие, чтение, запись или закрытие файла с ноутбука, рабочей станции, мобильного или другого устройства, клиент ICAP (NAS или система обмена файлами) отправляет запрос на сканирование к Security Server и получает результат относительно данного файла. В зависимости от результата, Security Server разрешает доступ, запрещает доступ или удаляет файл.

Примечание
Этот модуль - это дополнение, доступное при наличии отдельного лицензионного ключа

2.18. Security for Mobile

Унифицирует управление безопасностью всего предприятия и контроль iPhone, iPad и Android устройств, обеспечивая надежность программного обеспечения и предоставление обновлений через онлайн-магазины Apple или Android. Решение было разработано для возможности управления личными устройствами (BYOD), последовательно продвигая политику использования любых портативных устройств. Функции безопасности включают блокировку

экрана, контроль подлинности, местоположение устройства, удаленную очистку, обнаружение root или jailbrake устройств и профили безопасности. На устройствах Android уровень безопасности расширен сканированием в режиме реального времени и шифрованием съемных носителей. В результате, мобильные устройства находятся под контролем и важная для бизнеса информация, находящаяся на них, защищена.

2.19. Доступность уровней защиты GravityZone

Уровни защиты GravityZone отличаются в зависимости от операционной системы на конечной точке. Чтобы узнать больше, обратитесь к статье Доступность слоев защиты GravityZone в Базе Знаний.

3. АРХИТЕКТУРА GRAVITYZONE

Уникальная архитектура GravityZone позволяет с легкостью масштабировать решение и защитить любое количество систем. GravityZone может быть настроена на использование нескольких виртуальных устройств и множество экземпляров конкретных ролей (база данных, коммуникационный сервер, сервер обновлений и веб-консоль), чтобы обеспечить надежность и масштабируемость.

Каждый экземпляр роли может быть установлен на разных устройствах. Встроенные балансировщики ролей позволяют доказать, что развертывание GravityZone защитит даже самые крупные корпоративные сети, не вызывая замедления или узкие места. Уже существующие программные или аппаратные балансировщики также могут быть использованы вместо встроенной балансировки, если они присутствуют в сети.

Поставляясь в качестве виртуального контейнера, GravityZone может быть импортирована на любую платформу виртуализации, включая VMware, Citrix, Microsoft Hyper-V, Nutanix Prism, Microsoft Azure.

Интеграция с VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element и Microsoft Azure упрощает развертывание защиты как для физических, так и для виртуальных машин.

Решение GravityZone включает в себя следующие компоненты:

- Виртуальные устройства GravityZone
- Security Server
- Дополнительный пакет HVI
- Агенты безопасности

3.1. GravityZone VA

Локальное решение GravityZone поставляется как настроенное виртуальное устройство на базе Linux Ubuntu, встроенное в образ виртуальной машины, которое можно легко установить и настроить через CLI (Интерфейс командной строки). Виртуальное устройство доступно в нескольких вариантах, совместимых с основными платформами виртуализации (OVA, XVA, VHD, OVF, RAW).

3.1.1. База данных GravityZone

Центральная логика архитектуры GravityZone. Bitdefender использует не-реляционную базу данных MongoDB, которую легко масштабировать и реплицировать.

3.1.2. Сервер обновлений GravityZone

Сервер обновлений играет важную роль в обновлении решения GravityZone и конечных агентов путем репликации и публикации необходимых пакетов или установочных файлов.

3.1.3. Коммуникационный Сервер GravityZone

Коммуникационный Сервер является связующим звеном между агентами безопасности и базами данных, передавая политики и задачи для защиты конечных точек, а также генерируя отчеты от агентов безопасности.

3.1.4. Сервер обновлений GravityZone

Сервер инцидентов - это связующее звено между агентами безопасности и базой данных, собирающее данные конечных точек и генерирующее инциденты на основе угроз, которые обнаружены с помощью технологий предотвращения и алгоритмов машинного обучения.

3.1.5. Веб-консоль (GravityZone Control Center)

Решения безопасности Bitdefender управляются из единой точки управления, веб-консоли Control Center. Это упрощает управление и доступ к общей системе безопасности, обеспечивает контроль над всеми модулями безопасности, защищающими виртуальные и физические компьютеры, серверы и мобильные устройства от глобальных угроз. Работая на архитектуре Gravity, Control Center способна удовлетворить потребности даже самых крупных организаций.

Control Center интегрируется в существующие системы управления и системы мониторинга, чтобы упростить и автоматически применять защиту для неуправляемых рабочих станций, серверов и мобильных устройств, которые появляются в Microsoft Active Directory, VMware vCenter, Nutanix Prism Element или Citrix XenServer, или которые просто обнаружены в сети.

3.2. Security Server

Security Server является специализированной виртуальной машиной, которая дедуплицирует и централизует большую часть функциональностей защиты от вредоносных программ, агентов защиты от вредоносных программ, действуя в качестве сервера сканирования.

Существуют три версии Security Server, для каждого типа сред виртуализации:

- **Security Server for VMware NSX.** Эта версия автоматически устанавливается на каждом хосте в кластере, где был развернут Bitdefender.
- **Security Server for VMware vShield Endpoint.** Эта версия должна быть установлена на каждом хосте, которые должны быть защищены.
- **Security Server Multi-Platform.** Эта версия предназначена для других виртуальных сред и она должна быть установлена на одном или нескольких хостах, чтобы соответствовать количеству защищаемых виртуальных машин. При использовании HVI, Security Server должен быть установлен на каждом хосте, содержащем виртуальные машины, которые должны быть защищены.

3.3. Дополнительный пакет HVI

Пакет HVI обеспечивает связь между гипервизором и Security Server, расположенным на одном хосте. Таким образом, Security Server может контролировать используемую память на хосте, где он установлен, на основе политик безопасности GravityZone.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

3.4. Агенты безопасности

Чтобы Bitdefender защитил вашу сеть, необходимо установить соответствующих агентов безопасности GravityZone на сетевых конечных точках.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac
- GravityZone Mobile Client

- Bitdefender Tools (vShield)

3.4.1. Bitdefender Endpoint Security Tools

GravityZone обеспечивает защиту физических и виртуальных Windows и Linux машин с помощью Bitdefender Endpoint Security Tools - интеллектуального агента, который адаптируется к типу конечной точки. Bitdefender Endpoint Security Tools может быть развернут на любой машине, как физической так и виртуальной, обеспечивая гибкую систему сканирования и являясь идеальным выбором для смешанных сред (физических, виртуальных и облачных).

В дополнение к защите файлов системы,Bitdefender Endpoint Security Tools также включает защиту почтовых серверов Microsoft Exchange.

Bitdefender Endpoint Security Tools использует единый шаблон политики для физических и виртуальных устройств, а также один установочный комплект для любой среды (физической или виртуальной), работающей на Windows.

Слои защиты

Следующие уровни защиты доступны в Bitdefender Endpoint Security Tools:

- Защита от вредоносного ПО
- Расширенный контроль угроз (Advanced Threat Control)
- Обнаружение гипервизора
- Брандмауэр
- Контроль контента
- Network Attack Defense
- Управление исправлениями
- Контроль устройств
- Полное шифрование диска
- Security for Exchange
- Sandbox Analyzer
- События
- Контроль приложений

Роли конечных точек

- Привилегированный пользователь
- Ретранслятор
- Сервер кэширования патчей

- Защита Exchange

Привилегированный пользователь

Администраторы Центра управления (Control Center) могут предоставлять права привилегированных пользователей обычным пользователям конечных устройств с помощью параметров политики безопасности. Модуль привилегированных пользователей разрешает предоставление администраторских прав уровню пользователей, которые разрешат конечным пользователям получать доступ и изменять настройки безопасности, используя локальную консоль. Control Center будет уведомлена, когда конечная точка находится в режиме привилегированного пользователя и администратор Control Center всегда может переназначить локальные настройки безопасности.

Важно
Этот модуль доступен только для поддерживаемых настольных и серверных операционных систем Windows. Для получения более подробной информации, обратитесь к руководству по установке GravityZone.

Ретранслятор

Агенты конечных точек с ролью Bitdefender Endpoint Security Tools Relay выступают как прокси-сервер и сервер обновлений для других конечных точек в сети. Агенты конечных устройств с ролью ретранслятора особенно необходимы в организациях с изолированными сетями, где весь трафик проходит через единую точку доступа.

В компаниях с большими распределенными сетями, агент-ретранслятор помогает снизить использование полосы пропускания, предотвращая защищаемые конечные устройства и серверы безопасности от прямого взаимодействия с машинами GravityZone.

После того, как агент Bitdefender Endpoint Security Tools Relay установлен в сети, другие конечные точки могут быть сконфигурированы с помощью политик, чтобы общаться с Control Center через агента ретрансляции.

Агенты Bitdefender Endpoint Security Tools Relay служат для следующих целей:

- Обнаружение всех незащищенных конечных точек в сети.
- Развертывание агентов конечных точек внутри локальной сети.
- Обновление защищаемых конечных точек в сети.

- Обеспечение связи между Control Center и подключенными конечными точками.
- Выступать в качестве прокси-сервера для защищаемых конечных точек.
- Оптимизации сетевого трафика во время обновления, развертывания, сканирования и других ресурсоемких задач.

Сервер кэширования патчей

Конечные точки с ролью ретранслятора также могут выступать в качестве сервера кэширования исправлений. При включении этой роли ретрансляторы служат для хранения исправлений программного обеспечения, загружаемых с веб-сайтов поставщиков, и их распространения на конечные точки сети. Всякий раз, когда подключенная конечная точка имеет программное обеспечение с отсутствующими исправлениями, она берет их с сервера, а не с веб-сайта поставщика, таким образом оптимизируя генерируемый трафик и нагрузку на пропускную способность сети.

Важно
Эта дополнительная роль доступна с зарегистрированной надстройкой Patch Management.

Защита Exchange

Bitdefender Endpoint Security Tools с ролью защитника Exchange может быть установлен на сервере Microsoft Exchange с целью защиты пользователей Exchange от угроз передаваемых по электронной почте.

Bitdefender Endpoint Security Tools с ролью защитника Exchange защищает как сам сервер, так и сервисы Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac - это агент безопасности, созданный для защиты устройств на базе Macintosh. В качестве технологии сканирования доступно **Локальное сканирование**, с локально расположенными механизмами защиты.

Слои защиты

Следующие уровни защиты доступны в Endpoint Security for Mac:

- Защита от вредоносного ПО
- Расширенный контроль угроз (Advanced Threat Control)

- Контроль контента
- Контроль устройств
- Полное шифрование диска

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client распространяет политики безопасности на любое количество Android и iOS устройств, защищая их от несанкционированного использования, от потенциально опасных программ и потери конфиденциальных данных. Функции безопасности включают блокировку экрана, контроль подлинности, местоположение устройства, удаленную очистку, обнаружение root или jailbrake устройств и профили безопасности. На устройствах Android уровень безопасности расширен сканированием в режиме реального времени и шифрованием съемных носителей.

GravityZone Mobile Client распространяется через Apple App Store и Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools является облегченным агентом для виртуальных сред VMware, который интегрирован с конечными точками vShield. Агент безопасности устанавливается на виртуальные машины, защищенные Security Server, что позволяет вам получить дополнительные функциональные возможности, которые он обеспечивает:

- Позволяет запускать задачи сканирования памяти и процессов на компьютере.
- Информирует пользователя об обнаруженных инфекциях и принятых в их отношении мерах.
- Добавляет больше возможностей для создания исключений при сканировании от вредоносных программ.

3.5. Sandbox Analyzer Архитектура

Bitdefender Sandbox Analyzer обеспечивает мощный уровень защиты от новейших угроз путем автоматического и глубокого анализа подозрительных файлов, не подписанных антивирусными ядрами Bitdefender.

Sandbox Analyzer доступен в двух вариантах:

- Sandbox Analyzer Cloud , размещенный в Bitdefender.

- Sandbox Analyzer On-Premises , доступный как виртуальное устройство, которое можно развернуть локально.

Sandbox Analyzer Облако

Sandbox Analyzer Cloud содержит следующие компоненты:

- **Sandbox Analyzer Portal** - размещенный коммуникационный сервер связи, используемый для передачи запросов между конечными точками и кластером безопасной среды Bitdefender.
- **Sandbox Analyzer Cluster** - размещенная инфраструктура безопасной среды, в которой происходит выборочный анализ поведения объектов. На этом уровне отправленные файлы проверяются на виртуальных машинах под управлением Windows 7.

GravityZone Control Center – функционирует как консоль управления и отчетов, где вы настраиваете политики безопасности, просматриваете отчеты анализа и уведомления.

Bitdefender Endpoint Security Tools (BEST) - агент безопасности, установленный на конечных точках, действует как датчик подачи данных в Sandbox Analyzer.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises представляет собой виртуальное устройство Linux Ubuntu, встроенное в образ виртуальной машины, его можно легко установить и сформировать при помощи интерфейса командной строки (CLI). Sandbox Analyzer On-Premises доступен в формате OVA, также может быть развернут в VMWare ESXi.

ЭкземплярSandbox Analyzer On-Premises содержит в себе следующие компоненты:

- **Менеджер песочницы**. Это компонент является оркестром песочницы. Sandbox Manager связывается с гипервизором ESXi посредством API и использует их технические оснащение для постройки и эксплуатации среды анализа вредоносных программ.
- **Виртуальная машины детонации**. Данный компонент состоит из машин, используемых Sandbox Analyzer, для создания файлов и анализа их режима работы. Виртуальные машины детонации могут управлять Windows 7, а также 64-разрядной версией системы Windows 10.

GravityZone Control Center работает как консоль управления и отчетности, где вы настраиваете политики безопасности и просматриваете аналитические отчеты и уведомления.

Sandbox Analyzer On-Premises управляет следующими датчики подачи:

- **Датчик конечной точки** . Bitdefender Endpoint Security Tools для Windows действует как датчик подачи, установленный на конечных точках. Агент Bitdefender использует передовые алгоритмы машинного обучения и нейронной сети для определения подозрительного контента и отправки его в Sandbox Analyzer, включая объекты из централизованного карантина.
- **Сетевой датчик**. Виртуальное устройство сетевой безопасности (NSVA) - это виртуальное устройство, которое можно развернуть в той же виртуализированной среде ESXi, что и экземпляр Sandbox Analyzer. Датчик сети извлекает контент из сетевых потоков и передает его в Sandbox Analyzer.
- **Датчик ICAP**. Развернутая на устройствах с сетевым хранилищем (NAS) по протоколу ICAP, Bitdefender Security Server поддерживает отправку содержимого в Sandbox Analyzer.

В дополнение к этим датчикам Sandbox Analyzer On-Premises поддерживает ручную отправку и через API. Подробнее см. Главу **Использование Sandbox Analyzer** в Руководстве администратора GravityZone.

4. НАЧАЛО РАБОТЫ

Решения GravityZone могут быть сконфигурированы и управляться с помощью централизованной платформы управления под названием Control Center. Control Center имеет веб-интерфейс, к которому вы можете получить доступ с помощью имени пользователя и пароля.

4.1. Подключение к Control Center

Доступ к Control Center осуществляется с помощью учетных записей пользователей. Вы получите регистрационную информацию по электронной почте, как только ваш аккаунт будет создан.

Требования к системе:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Рекомендуемое разрешение экрана 1280 x 800 или выше

Предупреждение
Control Center не будет работать должным образом / отображаться в Internet Explorer 9 и выше с включенным режимом совместимости, что эквивалентно использованию неподдерживаемой версии браузера.

Подключение к Control Center:

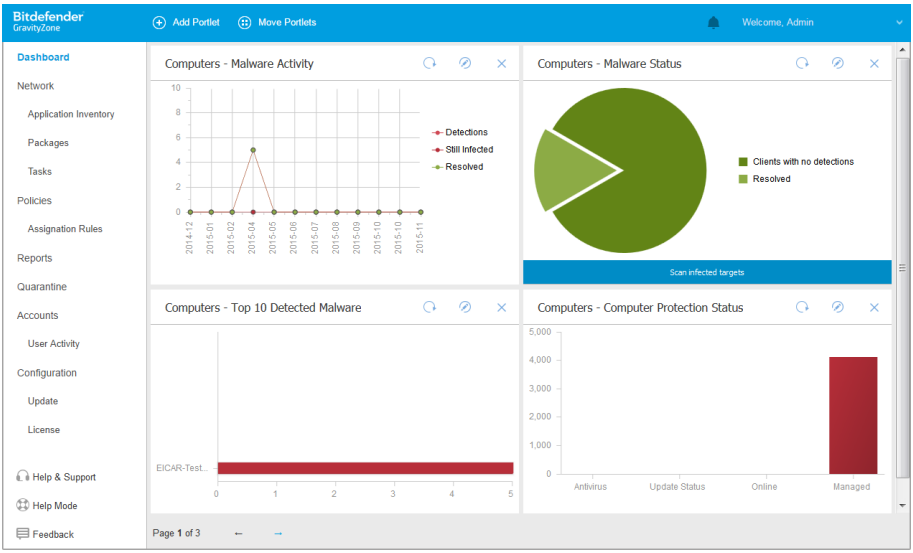
1. В адресной строке веб-браузера введите IP-адрес или DNS-имя хоста Control Center (используя префикс `https://`).
2. Введите имя пользователя и пароль.
3. Введите шестизначный код из Google Authenticator, Microsoft Authenticator или любого двухфакторного TOTP (Time-Based One-Time Password Algorithm) аутентификатора, совместимого со стандартом RFC6238. Дополнительные сведения см. в разделе «Управление вашей учетной записью» (p. 28).
4. Нажмите **Войти**.

При первом входе в систему вы должны согласиться с Условиями обслуживания Bitdefender. Нажмите **Продолжить**, чтобы начать использовать GravityZone.

Примечание
Если вы забыли свой пароль, воспользуйтесь ссылкой восстановления пароля, чтобы получить новый пароль. Вы должны предоставить адрес электронной почты вашей учетной записи.

4.2. Интуитивно понятная Control Center

Control Center организована таким образом, чтобы обеспечить легкий доступ ко всем функциям. Используйте панель меню справа, чтобы перемещаться по консоли. Доступные функции зависят от уровня доступа пользователя к консоли.



Информационная панель

4.2.1. Обзор Control Center

Пользователи с ролью администратора компании имеют полные права на конфигурацию Control Center и сетевых настроек безопасности, в то время как пользователи, с ролью администратора имеют доступ к функциям сетевой безопасности, включая управление пользователями.

Используйте кнопки **Просмотр меню** в левом верхнем углу чтобы свернуть, скрыть или развернуть меню. Нажмите на клавишу чтобы поочередно изменять вид меню, или нажмите два раза, чтобы пропустить.

В зависимости от Вашей роли, вы можете получить доступ к следующим разделам меню:

Панель управления
Просмотр простых графиков, позволяющих прочитать ключевую информацию о безопасности вашей сети.

События
Просмотр и управление инцидентами безопасности в сети компании.

Сеть
Установка защиты, применение политик для управления настройками безопасности, выполнение удаленных задач и быстрое создание отчетов.

Политики
Создание и управление политиками безопасности.

Отчеты
Получение отчетов о безопасности по управляемым клиентам.

Карантин
Удаленное управление файлами в карантине.

Учетные записи
Управление доступом к Control Center для других сотрудников компании.

В этом меню вы также можете найти страницу **Активность пользователя** , которая позволяет получить доступ к журналам активности пользователей.

Примечание
Это меню доступно только пользователям с **Управление пользователями** .

Конфигурация
Настройте параметры Control Center, такие как почтовый сервер, интеграция с Active Directory или средами виртуализации, сертификаты безопасности и параметры инвентаризации сети, включая запланированные правила для автоматической очистки неиспользуемых виртуальных машин.

Примечание
Это меню доступно только пользователям с правами **Управление решениями**.

При нажатии на имя пользователя в правом верхнем углу консоли, доступны следующие опции:

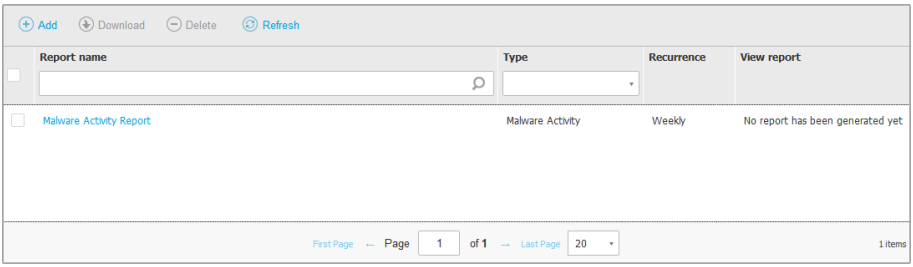
- **Моя учетная запись**. Выберите этот параметр, чтобы управлять своими реквизитами пользователя и настройками.
- **Диспетчер учетных данных**. Выберите этот параметр для добавления и управления учетными данными, необходимыми для задач удаленной установки.
- **Помощь & Поддержка**. Выберите данную опцию, чтобы получить информацию о помощи и поддержке.
- **Обратная связь**. Нажмите эту опцию, чтобы отобразить форму, позволяющую редактировать и отправлять сообщения обратной связи относительно вашей работы с GravityZone.
- **Выход**. Выход из учетной записи.

Кроме того, в верхнем правом углу консоли вы можете найти:

- Значок **Режим справки** , который активизирует расширяемые всплывающие подсказки, помещенные на элементы Control Center. Здесь вы легко сможете найти полезную информацию, касающуюся функций Control Center.
- Значок **Уведомления** обеспечивает легкий доступ к сообщениям уведомлений, а также к странице **Уведомления**.

4.2.2. Таблица данных

Таблицы часто используются на консоли для организации данных в легко понятном формате.



Страница отчетов

Навигация по Страницам

Таблицы с более чем 20 записями размещаются на нескольких страницах. По умолчанию, только 20 записей отображаются на одной странице. Для перемещения по страницам используйте кнопки навигации в нижней части таблицы. Вы можете изменить количество записей, отображаемые на странице, выбрав другую опцию в меню рядом с кнопками навигации.

Поиск конкретных записей

Чтобы легко найти конкретные записи, используйте окна поиска доступные под заголовками столбцов.

Введите слово для поиска в соответствующем поле. Соответствующие элементы отобразятся в таблице, по мере ввода запроса. Чтобы сбросить содержимое таблицы, очистите поля поиска.

Сортировка данных

Для сортировки данных по определенному столбцу, щелкните заголовок столбца. Нажмите на заголовок столбца еще раз, чтобы вернуть порядок сортировки.

Обновление данных таблицы

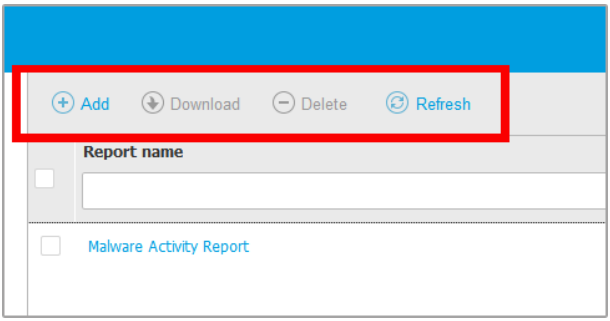
Чтобы убедиться, что консоль отображает последнюю информацию, нажмите кнопку **Обновить** в верхней части таблицы.

Данная функция может быть полезной, если вы длительное время находитесь на странице.

4.2.3. Панели инструментов

Панели инструментов в Control Center позволяют выполнять определенные операции, относящиеся к разделу, в котором вы находитесь. Каждая панель инструментов содержит набор иконок, которые обычно расположены вверху таблицы. Например, панель инструментов в разделе **Отчеты** позволяет вам выполнить следующие действия:

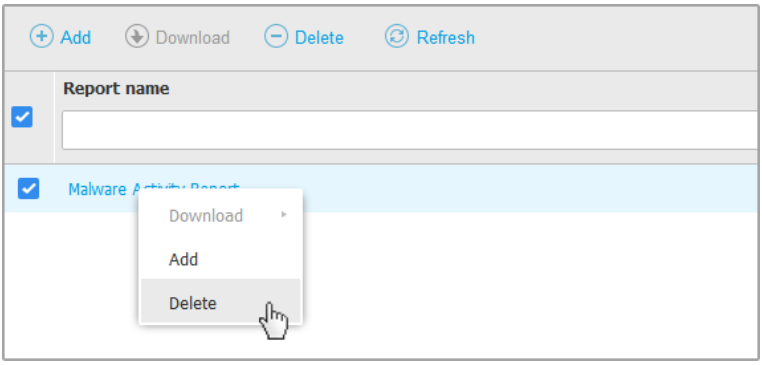
- Создать новый отчет.
- Загрузить отчет по расписанию.
- Удалить отчет по расписанию.



Страница отчетов - Панель Инструментов.

4.2.4. Контекстное меню

Также команды панели инструментов доступны из контекстного меню. При нажатии правой кнопки мыши в разделе Control Center, в котором вы находитесь, вы можете выбрать необходимую команду из предложенного списка.



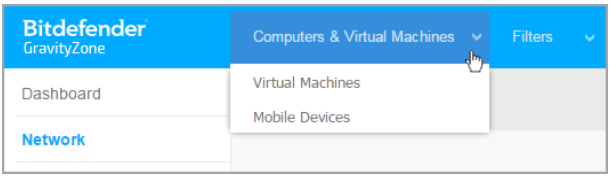
Страница отчетов - Контекстное меню

4.2.5. Выбор просмотра

Если вы работаете с различными типами конечных устройств, вы можете получить доступ к ним на странице **Сеть**, где они сгруппированы по типу устройств, в виде нескольких сетей.

- **Компьютеры & и виртуальные машины**: отображает группы и компьютеры в службе каталогов Active Directory, а также физические и виртуальные рабочие станции вне Active Directory, обнаруженные в сети.
- **Виртуальные машины**: отображает инфраструктуру виртуального окружения интегрированного с Control Center и содержит все виртуальные машины.
- **Мобильные устройства**: отображает пользователей и мобильные устройства закрепленные за ними.

Чтобы выбрать отображение нужной сети, нажмите меню просмотра в правом верхнем углу страницы.



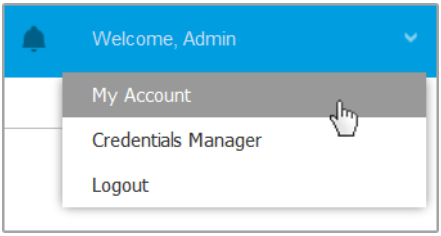
Выбор просмотра

Примечание
Вы сможете видеть только те конечные устройства, которые предусмотрены разрешениями, назначенные администратором, который добавил вашу учетную запись в Control Center.

4.3. Управление вашей учетной записью

Чтобы проверить или изменить данные и настройки вашей учетной записи:

1. Нажмите на ваше имя пользователя в правом верхнем углу консоли и выберите **Мой аккаунт**.



Меню учетных записей

2. **Подробности аккаунта**, позволяет исправить или обновить данные учетной записи. Если вы используете учетную запись в службе каталогов Active Directory, вы не можете изменить данные о ней.
   - **Имя пользователя.** Имя пользователя является уникальным идентификатором учетной записи и не может быть изменено.
   - **Полное имя.** Введите свое полное имя.
   - **Эл. почта.** Это ваш логин и контактный адрес электронной почты. Отчеты и важные уведомления безопасности будут отправляться на этот адрес. Уведомления по электронной почте рассылаются автоматически всякий раз при обнаружении значимых угроз в сети.
   - Ссылка **Изменить пароль** позволяет изменить пароль для входа.
3. **Настройки** позволяет настроить параметры учетной записи в соответствии с вашими предпочтениями.
   - **Часовой пояс.** Выберите в меню часовой пояс для вашего аккаунта. Консоль будет отображать информацию о времени в соответствии с выбранным часовым поясом.
   - **Язык.** Выберите из меню язык отображения консоли.

- **Временной интервал сеанса.** Выберите временной интервал до завершения вашего сеанса в результате бездействия.

4. В разделе **Login Security** настройте двухфакторную аутентификацию и проверьте состояние политик, доступных для защиты Вашей учетной записи GravityZone. Общекорпоративные политики доступны только для чтения

   Чтобы включить двухфакторную аутентификацию:

   a. **Двухфакторная аутентификация.** Двухфакторная идентификация добавляет дополнительный слой защиты доя Вашего аккаунта GravityZone, требуя код аутентификации помимо Вашего статуса / полномочий Control Center.

      При первом входе в свою учетную запись GravityZone Вам будет предложено загрузить и установить Аутентификатор Google Authenticator, Microsoft Authenticator или любой двухфакторный TOTP (Time-Based One-Time Password Algorithm), совместимый со стандартным RFC6238 на мобильном устройстве, связать его с Впшей учетной записью GravityZone, а затем использовать его с каждым входом в систему Control Center. Google Authenticator генерирует 6-значный код каждые 30 секунд. Чтобы войти в систему Control Center под своим логином, после ввода пароля вам понадобится предоставить 6-значный код из Google Authenticator.

      Примечание
      Вы можете пропустить этот этап 3 раза, затем вам будет недоступен вход без двухфакторной аутентификации.

      Чтобы включить двухфакторную аутентификацию:

      i. Нажмите на **Включено** кнопку, расположенную под **Двухфакторная аутентификация** сообщением.

      ii. В этом диалоговом окне нажмите нужную ссылку, чтобы загрузить и установить Аутентификатор Гугл на Ваше мобильное устройство.

      iii. На вашем мобильном устройстве откройте Аутентификатор Гугл.

      iv. На экране **Доавить аккаунт** отсканируйте QR-код, чтобы связать приложение с вашим аккаунтом GravityZone.

      Вы также можете ввести секретный ключ вручную.

Произвести это действие требуется единожды, чтобы включить активировать функцию в GravityZone.

Важно
Убедитесь, что скопировали и сохранили в надежном месте ваш секретный ключ. Нажмите **Напечатать резервную копию**, чтобы создать PDF файл с QR-кодом и секретным ключом. Если вы потеряли или заменили мобильное устройство, с которого проходили двухфакторную аутентификацию, то вам необходимо установить Аутентификатор Гугл на новом устройстве и ввести секретный ключ для связи с аккаунтом GravityZone.

v. Введите 6-значный код в поле **Код аутентификации Гугл**.

vi. Нажмите **Включить**, чтобы завершить активацию данной функции.

Примечание
Имейте ввиду, что если для вашей учетной записи отключен 2FA, то секретный ключ не будет действительным.

b. **Политика истечения срока действия пароля.** Регулярные изменения Вашего пароля обеспечивают дополнительный уровень защиты от несанкционированного использования паролей или ограничивают продолжительность несанкционированного использования. При включении функции GravityZone требуется изменить пароль не позднее чем через 90 дней.

c. **Политика блокировки учетной записи.** Эта политика запрещает доступ к Впшей учетной записи после пяти последовательных неудачных попыток входа в систему. Эта мера используется с целью защиты от зловредных действий.

   Чтобы разблокировать свою учетную запись, Вам нужно сбросить пароль со страницы входа в систему или обратиться к другому администратору GravityZone.

5. Нажмите **Сохранить**, чтобы сохранить изменения.

Примечание
Вы не можете удалить собственную учетную запись.

4.4. Изменение пароля для входа в систему

После того, как ваша учетная запись будет создана, вы получите письмо с учетными данными для входа.

Если вы не используете учетные данные Active Directory, чтобы получить доступ к Control Center, рекомендуется сделать следующее:

- Изменить пароль по умолчанию, который вы в первый раз использовали при доступе к Control Center.
- Периодически менять пароль для входа.

Чтобы изменить пароль для входа:

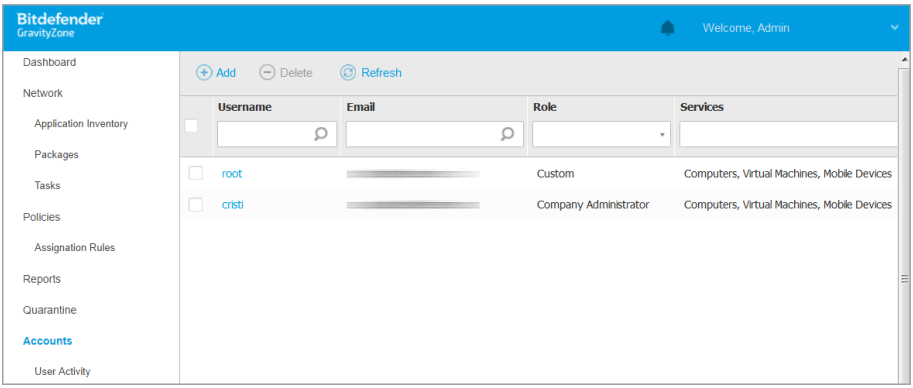
1. Нажмите на ваше имя пользователя в правом верхнем углу консоли и выберите **Мой аккаунт**.
2. В **Account Details** нажмите **Change password**.
3. Введите текущий пароль и новый пароль в соответствующие поля.
4. Нажмите **Сохранить**, чтобы сохранить изменения.

5. УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ

Вы можете создать первую учетную запись пользователя GravityZone во время начальной настройки Control Center, после развертывания устройства GravityZone. Начальная учетная запись пользователя Control Center имеет роль администратора компании, с полными правами на конфигурацию Control Center и управление сетью. Из этого аккаунта вы можете создать все другие учетные записи, необходимые для управления сетью вашей компании.

Вот, что вам нужно знать об учетных записях GravityZone:

- Чтобы разрешить другим сотрудникам компании доступ к Control Center, вы можете создать учетные записи пользователей по отдельности или включить динамический доступ для нескольких учетных записей посредством интеграции Active Directory или правил доступа. Вы можете назначить учетные записи с разными ролями, в соответствии с их уровнем доступа в компании.
- Для каждой учетной записи пользователя, вы можете настроить доступ к функциям GravityZone или к определенным частям сети, к которой он принадлежит.
- Вы можете управлять только учетными записями с равными или меньшими правами.



Страница учетных записей

Существующие учетные записи будут отображаться в таблице. Для каждой учетной записи пользователя, вы можете просмотреть следующее:

- Имя пользователя учетной записи (используется для входа в Control Center).
- Адрес электронной почты учетной записи (используется в качестве контактного адреса). Отчеты и важные уведомления безопасности будут отправляться на этот адрес. Уведомления по электронной почте рассылаются автоматически всякий раз при обнаружении значимых угроз в сети.
- Роль пользователя (администратор компании / сетевой администратор / специалист по безопасности / пользовательская).
- Служба безопасности GravityZone, которой пользователь может управлять (компьютерами, виртуальными машинами, мобильными устройствами).
- Статус двухфакторной аутентификации, который позволяет быстро проверить, включена ли у пользователя двухфакторная аутентификация.
- Статус Правила Доступа показывает учетную запись пользователя, созданную с помощью правила разрешения доступа. Учетные записи, созданные вручную, будут отображаться как **N/A**.

5.1. Роли пользователей

Роль пользователя состоит из определенных комбинаций прав пользователей. При создании учетной записи пользователя, вы можете выбрать одну из предопределенных ролей или вы можете создать собственную роль, выбрав только определенные права пользователя.

Примечание
Вы можете управлять только аккаунтами с равными правами, как у вашего аккаунта, или ниже.

Доступны следующие роли пользователей:

1. **Администратор компании** - Обычно, уникальная учетная запись пользователя, с ролью Администратора компании, создается для каждой компании отдельно, с полным доступом ко всем функциям управления решением GravityZone. Администратор компании конфигурирует настройки Control Center, управляет лицензионными ключами служб безопасности,

управляет учетными записями пользователей, также имея административные привилегии по настройке сетевой безопасности всей компании. Администраторы компании могут частично или полностью делегировать свои оперативные обязанности подчиненным администраторам и специалисту по безопасности учетных записей пользователей.

2. **Администратор сети** - Несколько аккаунтов могут быть созданы в компании с ролями Сетевого администратора, с административными привилегиями по развертыванию агентов безопасности во всей компании или по определенным группам конечных точек, включая управление пользователями. Сетевые администраторы отвечают за активное управление настройками безопасности сети.
3. **Специалист по безопасности** - учетные записи специалиста по безопасности доступны только для чтения. Они разрешают доступ только к данным, отчетам и журналам,связанным с безопасностью. Такие учетные записи могут быть созданы для персонала, отвечающего за мониторинг безопасности или для других сотрудников, которые должны отслеживать статус безопасности.
4. **Пользователь** - Предопределенные роли пользователей, включающие определенную комбинацию прав пользователей. Если предопределенная роль пользователя не соответствует вашим требованиям, вы можете создать собственный аккаунт, назначив ему те права, в которых вы заинтересованы.

В следующей таблице приведена взаимосвязь различных ролей аккаунта и их прав. Для получения дополнительной информации перейдите к «Права пользователя» (p. 35).

Роль аккаунта	Разрешения дочерних учетных записей	Права пользователя
Администратор компании	Администратор компании, Сетевой администратор, Специалист по безопасности	Управление решением Управление компанией Управление пользователями Управление сетями Просмотреть и проанализировать данные

Роль аккаунта	Разрешения дочерних учетных записей	Права пользователя
Сетевой администратор	Сетевой администратор, аналитик по безопасности	Управление пользователями Управление сетями Просмотреть и проанализировать данные
Аналитик по безопасности	-	Просмотреть и проанализировать данные

5.2. Права пользователя

Вы можете назначить следующие права доступа учетным записям GravityZone:

- **Управление решением**. Позволяет сконфигурировать настройки Control Center (сервер электронной почты и настройки прокси-сервера, интеграции с Active Directory и платформами виртуализации, сертификаты безопасности и обновления GravityZone). Эти права только для учетных записей администраторов компании.
- **Управление пользователями**. Создание, редактирование или удаление учетных записей пользователей.
- **Управление компанией**. Пользователи могут управлять своим собственным лицензионным ключом GravityZone и редактировать параметры профиля компании. Эти права только для учетных записей администраторов компании.
- **Управление сетями**. Обеспечивает административные права по настройкам сетевой безопасности (инвентаризация сети, политики, задачи, инсталляционные пакеты, карантин). Эти права только для учетных записей сетевых администраторов.
- **Просмотреть и проанализировать данные**. Просмотр события и журналы безопасности, управление отчетами и приборная панель.

5.3. Управление учетными записями пользователей

Для создания, редактирования, удаления и настройки учетных записей пользователей используйте следующие методы:

- Индивидуальное управление учетными записями пользователей. Используйте этот метод для добавления учетных записей локальных пользователей или учетных записей Active Directory. Чтобы настроить интеграцию с Active Directory, обратитесь к Руководству по установке GravityZone.

  Перед тем как создать учетную запись пользователя, убедитесь, что у вас под рукой есть требуемый адрес электронной почты. Пользователь получит регистрационные данные GravityZone на предоставленный адрес электронной почты.

- Управление несколькими учетными записями пользователей. Используйте этот метод для включения динамического доступа посредством правила доступа. Данный метод требует интеграции домена Active Directory. Для получения дополнительной информации об интеграции Active Directory см. Руководство по установке GravityZone.

5.3.1. Индивидуальное управление учетными записями пользователей

В Control Center вы можете персонально создавать, редактировать и удалять учетные записи пользователей.

Зависимости

- Локально созданные учетные записи могут поспособствовать удалению аккаунтов, созданных путем интеграции Active Directory независимо от их роли.
- Локально созданные учетные записи не могут способствовать удалению таких же аккаунтов независимо от их роли.

Индивидуальное создание учетных записей пользователей

Чтобы добавить учетную запись пользователя в Control Center:

1. Перейдите на страницу **Аккаунты**.
2. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.
3. В разделе **Подробная информация** укажите следующее:

- Для учетных записей пользователей Active Directory настройте следующие данные:

  Имя пользователя для учетных записей пользователей Active Directory (AD). Выберите учетную запись пользователя из выпадающего списка и перейдите к шагу 4.

  Вы можете добавлять учетные записи пользователей AD только при настроенной интеграции. При добавлении учетной записи пользователя AD данные пользователя импортируются из соответствующего домена. Пользователь входит в Control Center, используя имя пользователя и пароль AD.

  Примечание

  – Чтобы убедиться, что последние изменения Active Directory импортированы в Control Center, нажмите кнопку **Синхронизировать**.

  – Пользователи с правом **Управление решением** могут настроить интервал синхронизации Active Directory с помощью параметров, доступных на вкладке **Конфигурация > Active Directory** . Для получения дополнительной информации см. главы **Установка защиты > Установка GravityZone** и **Настройка > Настройка параметров центра Control Center** из Руководства по установке GravityZone.

- Для локальных учетных записей настройте следующие данные:

  – **Имя пользователя** для локальной учетной записи. Отключите **Импорт из Active Directory** и введите имя пользователя.

  – **Email**. Введите адрес электронной почты пользователя.

    Адрес электронной почты должен быть уникальным. Вы не можете создать другую учетную запись пользователя с одним и тем же адресом электронной почты.

    GravityZone использует данный адрес электронной почты для отправки уведомлений.

  – **Полное имя**. Введите полное имя пользователя.

  – **Пароль**. Введите пароль, который пользователь может использовать для входа.

Пароль должен содержать, по крайней мере, один символ верхнего регистра, по крайней мере, одну строчную букву и, по крайней мере, одну цифру или специальный символ.

– **Подтвердите пароль**. Подтвердите пароль для проверки.

4. В разделе **Настройки и привилегии**, настройте следующие параметры:

- **Часовой пояс**. Выберите в меню часовой пояс для учетной записи. Консоль будет отображать информацию о времени в соответствии с выбранным часовым поясом.
- **Язык**. Выберите в меню консоли язык отображения.
- **Роль**. Выберите роль пользователя. Для получения подробной информации относительно ролей пользователей, обратитесь к «Роли пользователей» (p. 33).
- **Права**. Каждая предопределенная роль пользователя имеет определенную конфигурацию прав. Тем не менее, вы можете выбрать те права, которые вам нужны. В этом случае, роль пользователя изменится на **Пользователь**. Для получения подробной информации относительно прав пользователей, обратитесь к «Права пользователя» (p. 35).
- **Выбрать цель**. Выберите сетевые группы, в которых пользователь будет иметь доступ к каждой доступной службе безопасности. Вы можете ограничить доступ пользователей к определенным службам безопасности GravityZone или к конкретным областям сети.

Примечание
Опция выбора объекта не будет отображаться для пользователей с правами Управления решением, которые, по умолчанию, имеют полномочия на всю сеть и службы безопасности.

Важно
Всякий раз, когда вы вносите изменения в структуру своей сети или настраиваете новую интеграцию с другим vCenter Server или системой XenServer, не забывайте проверять и обновлять права доступа для существующих пользователей.

5. Нажмите **Save**, чтобы добавить пользователя. Новая учетная запись появится в списке учетных записей пользователей.

Control Center автоматически отправляет пользователю электронное письмо с данными регистрации, если настройки почтового сервера были правильно введены. Более подробную информацию о конфигурации почтового сервера см. в разделе **Установка защиты > GravityZone Установка и настройка > Настройка Control Center Настройки центра** из раздела GravityZone Руководство по установке.

Индивидуальное редактирование учетных записей пользователей

Чтобы добавить учетную запись пользователя в Control Center:

1. Войдите в Control Center.
2. Перейдите на страницу **Аккаунты**.
3. Нажмите на имя пользователя.
4. Измените данные учетной записи и настройки при необходимости.
5. Нажмите **Сохранить**, чтобы сохранить изменения.

Примечание
Все аккаунты с правами **Управление пользователями** могут создавать, редактировать и удалять учетные записи других пользователей. Вы можете управлять только аккаунтами с равными правами, как у вашего аккаунта, или ниже.

Индивидуальное удаление учетных записей пользователей

Чтобы удалить учетную запись пользователя в Control Center:

1. Войдите в Control Center.
2. Перейдите на страницу **Аккаунты**.
3. Выберите учетную запись пользователя из списка.
4. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

   Нажмите **Да** для подтверждения.

5.3.2. Управление несколькими учетными записями пользователей

Создайте правила доступа, чтобы предоставить GravityZone Control Center доступ к пользователям Active Directory на основе групп безопасности.

Требования к системе

Чтобы управлять несколькими учетными записями пользователей, вам нужна интеграция домена Active Directory с GravityZone. Чтобы интегрировать и синхронизировать домен Active Directory, см. главу **Active Directory** в Руководстве по установке GravityZone.

Зависимости

Правила разрешения доступа связаны с группами безопасности Active Directory (AD) и соответствующими учетными записями пользователей. Любые изменения, внесенные в домены Active Directory, могут повлиять на соответствующие правила доступа. Вот что необходимо знать об отношении между правилами, пользователями и доменами Active Directory:

- Правило разрешения доступа добавляет учетную запись пользователя, только если электронная почта еще не связана с существующей учетной записью.
- Для одинаковых адресов электронной почты в группе безопасности правило разрешения доступа создает учетную запись пользователя GravityZone только для первой учетной записи пользователя Active Directory, которая входит в систему Control Center.

  Например, группа безопасности содержит повторяющийся адрес электронной почты для разных пользователей, и все они пытаются войти в Control Center, используя свои учетные данные Active Directory. Если правило разрешения доступа связано с этим конкретным доменом Active Directory, оно создаст учетную запись пользователя только для первого пользователя, который вошел в систему Control Center с использованием повторяющегося адреса электронной почты.
- Учетные записи пользователей, созданные с помощью правил доступа, становятся неактивными, если они удаляются из связанной с ними группы безопасности AD. Те же пользователи могут стать активными, если они связаны с новым правилом доступа.
- Правила доступа становятся доступными только для чтения, когда связанный домен Active Directory больше не интегрируется с GravityZone. Пользователи, связанные с этими правилами, становятся неактивными.
- Аккаунты пользователей, созданные посредством правил доступа, не могут поспособствовать удалению локально созданных пользователей

- Аккаунты, созданные посредством правила доступа, не могут способствовать удалению аккаунтов Администраторов компании.

Создание нескольких учетных записей пользователей

Чтобы добавить несколько учетных записей пользователей, создайте правила доступа. Правила разрешения доступа связаны с группами безопасности Active Directory.

Чтобы добавить правило разрешения доступа:

1. Перейдите на страницу **Конфигурация > Active Directory > Разрешения на доступ**.
2. Если у вас несколько интеграций, выберите домен в верхней левой части таблицы.
3. Нажмите ⊕ **Добавить** в левой части таблицы.
4. Настройте следующие параметры разрешений на доступ:
   - **Приоритет**. Правила обрабатываются в приоритетном порядке. Чем меньше число, тем выше приоритет.
   - **Имя**. Название правила доступа.
   - **Домен**. Домен, с которого необходимо добавить группы безопасности.
   - **Группы Безопасности**. Группы безопасности, которые содержат ваших будущих пользователей GravityZone. Вы можете использовать поле автозаполнения. Группы безопасности, добавленные в этот список, не подлежат изменению, добавлению или удалению после сохранения правила доступа.
   - **Часовой пояс**. Часовой пояс пользователя.
   - **Язык**. Язык отображения консоли.
   - **Роль**. Предопределенные роли пользователей. Для получения дополнительной информации см. главу **Учетные записи пользователей** в Руководстве администратора GravityZone.

   Примечание
   Вы можете предоставлять и отзывать привилегии другим пользователям с такими же или меньшими привилегиями, чем ваша учетная запись.

- **Права**. Каждая предопределенная роль пользователя имеет определенную конфигурацию прав. Для получения дополнительной информации см. главу **Учетные записи пользователей** в Руководстве администратора GravityZone.
- **Выберите цели** Выберите сетевые группы, в которых пользователь будет иметь доступ к каждой доступной службе безопасности. Вы можете ограничить доступ пользователей к определенным службам безопасности GravityZone или к конкретным областям сети.

  Примечание
  Опция выбора объекта не будет отображаться для пользователей с правами Управления решением, которые, по умолчанию, имеют полномочия на всю сеть и службы безопасности.

5. Нажмите **Сохранить**.

   Правило доступа сохраняется при отсутствии влияния пользователя. В противном случае вам будет предложено указать пользовательские исключения. Например, когда вы добавляете правило с более высоким приоритетом, затронутые пользователи, связанные с другими правилами, привязываются к прежнему правилу.
6. При необходимости выберите пользователей, которых вы хотите исключить. Для получения дополнительной информации см. Исключения учетной записи пользователя.
7. Нажмите **Подтвердить**. Правило отображается на странице **Разрешения на доступ**.

Пользователи в группах безопасности, указанных в правилах доступа, теперь могут получить доступ к GravityZone Control Center со своими учетными данными домена. Control Center автоматически создает новые учетные записи пользователей при первом входе в систему, используя пользовательские адрес электронной почты Active Directory и пароль.

Учетные записи пользователей, созданные с помощью правила доступа, имеют имя правила доступа, отображаемое на странице **Учетные записи** в столбце **Правило доступа**.

Редактирование нескольких учетных записей пользователей

Чтобы изменить правило разрешения доступа:

1. Перейдите на страницу **Конфигурация > Active Directory > Разрешения на доступ**.
2. Выберите имя правила доступа, чтобы открыть окно конфигурации.
3. Изменить настройки разрешения на доступ. Для получения дополнительной информации см. Добавление разрешений на доступ.
4. Нажмите **Сохранить**. Правило сохраняется при отсутствии влияния пользователя. В противном случае вам будет предложено указать исключения учетной записи пользователя. Например, если вы обновите приоритет правила, затронутые пользователи могут переключиться на другое правило.
5. При необходимости выберите пользователей, которых вы хотите исключить. Для получения дополнительной информации см. Исключения учетной записи пользователя.
6. Нажмите **Подтвердить**.

Примечание
Вы можете открепить учетные записи пользователей, созданные с помощью правил доступа, изменив их права в системе Control Center. Учетную запись пользователя невозможно снова привязать к правилам доступа.

Удаление нескольких учетных записей пользователей

Чтобы удалить правило доступа:

1. Перейдите на страницу **Конфигурация > Active Directory > Разрешения на доступ**.
2. Выберите правило доступа, которое вы хотите удалить, и нажмите ⊖ **Удалить**. , Появившееся окно предложит вам подтвердить ваши действия. Если есть влияние на пользователя, вам будет предложено указать исключения учетной записи пользователя. Например, вы можете указать исключения для пользователей, на которых повлияло удаление правила.
3. При необходимости выберите пользователей, которых вы хотите исключить. Для получения дополнительной информации см. Пользовательские исключения.
4. Нажмите **Подтвердить**.

Удаление правила аннулирует доступ к соответствующим учетным записям пользователей. Все пользователи, созданные через него, будут удалены, если другие правила не предоставляют им доступ.

Исключения учетной записи пользователя

Когда вы добавляете, редактируете или удаляете правила доступа, которые влияют на пользователя, вы можете указать исключения учетной записи пользователя. Вы также можете просмотреть причины и последствия влияния пользователей.

Укажите пользовательские исключения следующим образом:

1. Выберите пользователей, которых вы хотите исключить. Или установите флажок в верхней части таблицы, чтобы добавить всех пользователей в список.
2. Нажмите **X** в поле имени пользователя, чтобы удалить его из списка.

5.4. Сброс паролей входа

Акаунты владельцев, которые забыли свой пароль, можно сбросить с помощью восстановления пароля, использовав ссылку на странице входа. Вы также можете сбросить забытый пароль, отредактировав соответствующий аккаунт из консоли.

Чтобы сбросить пароль пользователя для входа:

1. Войдите в Control Center.
2. Перейдите на страницу **Аккаунты**.
3. Нажмите на имя пользователя.
4. Введите новый пароль в соответствующих полях (в **Подробности**).
5. Нажмите **Сохранить**, чтобы сохранить изменения. Владелец аккаунта получит письмо с новым паролем.

5.5. Управление двухфакторной аутентификацией

Выбрав учетную запись пользователя, вы сможете просматривать статус его двухфакторной аутентификации (вкл или выкл) в разделе **Двухфакторная аутентификация**. Вы можете предпринять следующие действия:

- **Сбросить или отключить двухфакторную аутентификацию пользователя**. Если пользователь с двухфакторной аутентификацией изменил или стер мобильное устройство и потерял секретный ключ:

  1. Введите пароль GravityZone в поле доступа.
  2. Нажмите **Сбросить** (когда двухфакторная аутентификация включена) or **Отключить** (когда двухфакторная аутентификация выключена).
  3. Сообщение с подтверждением информирует вас о том, что двухфакторная аутентификация была сброшена / отключена для текущего пользователя.

     После отключения двухфакторной аутентификации, когда эта функция включена, при входе в учетную запись окно конфигурации предложит пользователю заново настроить двухфакторную аутентификацию с новым секретным ключом.

- Если у пользователя отключена двухфакторная аутентификация, и вы хотите ее активировать, вам будет необходимо попросить пользователя включить эту функцию в настройках его учетной записи.

Примечание
Если у вас есть учетная запись администратора компании, вы можете включить двухфакторную аутентификацию для всех учетных записей GravityZone. Дополнительную информацию можно найти в Руководстве по установке в разделе **Установка защиты > Установка и настройка GravityZone > Настройка параметров Центра управления**.

Важно
Приложение аутентификации по выбору (Google Authenticator, Microsoft Authenticator или любой двухфакторный TOTP (Time-Based One-Time Password Algorithm) аутентификатор, совместимый сстандартом RFC6238), объединяет секретный ключ с текущей отметкой времени мобильного устройства для генерации шестизначного кода. Имейте ввиду, что текущая метка времени на мобильном устройстве и устройстве GravityZone должны совпадать, чтобы 6-значный ключ оказался рабочим. Чтобы избежать проблем при синхронизации временных меток, мы рекомендуем включать автоматические настройки времени и даты на мобильном устройстве.

Другой метод проверки изменений двухфакторной аутентификации, связанных с учетными записями пользователей, заключается в том, чтобы получить

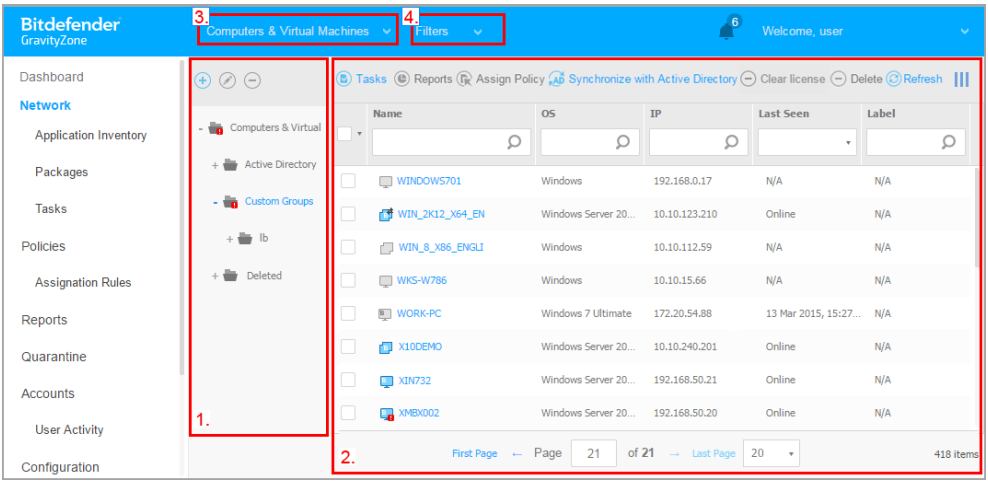
доступ к странице **Учетные записи > Активность пользователя** и просмотреть журналы активности с помощью следующего фильтра:

- Область > Учетные записи / Компания
- Действие > Изменено

Чтобы получить больше информации о включении двухфакторной аутентификации, оращайтесь к«Управление вашей учетной записью» (p. 28)

6. УПРАВЛЕНИЕ СЕТЕВЫМИ ОБЪЕКТАМИ

Раздел **Сеть** предоставляет несколько возможностей для исследования и управления каждым типом сетевых объектов, имеющихся в Control Center (компьютеры, виртуальные машины и мобильные устройства). Интерфейс раздела **Сеть** состоит из двух панелей, которые отображают состояние сетевых объектов в реальном времени:



Раздел - Сеть

1. Левая панель отображает дерево имеющейся сети. В зависимости от выбранного вида сети, эта панель отображает сетевую инфраструктуру, интегрированную с Control Center, такую как Active Directory, vCenter Server или Xen Server.

   В то же время, все компьютеры и виртуальные машины, обнаруженные в сети, которые не принадлежат к какой-либо интегрированной инфраструктуре, отображаются в **Custom Groups**.

   Все удаленные конечные точки хранятся в папке **Deleted**. Чтобы узнать больше, обратитесь к «Удаление конечных точек из сетевого содержимого» (p. 228).

Примечание
Вы можете просматривать и управлять только группами, на которые у вас есть права администратора.

2. Правая панель отображает содержимое группы, выбранной в левой панели. Эта панель представляет собой сетку, где строки содержат сетевые объекты, а столбцы определенную информацию для каждого типа объекта.

   В этой панели, вы можете сделать следующее:
   - Просмотреть под своей учетной записью подробную информацию о каждом объекте сети. Вы можете просмотреть состояние каждого объекта, проверяя значок рядом с его именем. Наведите курсор мыши на значок, чтобы просмотреть всплывающую информацию. Нажмите на название объекта, чтобы отобразить окно, содержащее более конкретные детали.

     Каждый тип объекта, например компьютер, виртуальная машина или папка, представлены соответствующей иконкой. Каждый объект сети может иметь определенный статус, характеризующий состояние управления, проблемы безопасности, связи и так далее. Для получения подробной информации относительно описания каждого значка сетевого объекта и имеющихся статусов, обратитесь к «Типы сетевых объектов и статусы» (p. 608).
   - Используйте Панель инструментов в верхней части таблицы, чтобы выполнить определенные операции над каждым сетевым объектом (например, запуск задачи, создание отчетов, назначение политики и удаление) и обновление данных таблицы.
3. меню видов в верхней части сетевой панели, позволяет переключаться между различным содержимым сетевых элементов, в зависимости от типов конечных точек, с которами вы хотите работать.
4. Меню **Фильтры**, доступное в верхней части сетевой панели, легко позволяет отображать только определенные сетевые объекты, предоставляя несколько способов фильтрации. Опции меню **Фильтры** связаны с вариантами отображения выбранной сети.

Из раздела **Сеть** вы также можете управлять инсталляционными пакетами и задачами для каждого типа сетевых объектов.

Примечание
Чтобы узнать больше об инсталляционных пакетах, обратитесь к руководству по установке GravityZone.

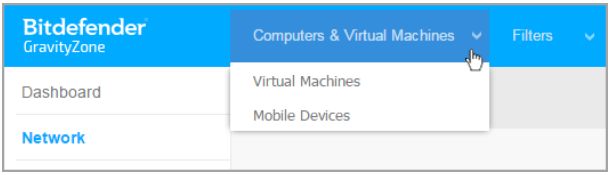
Для получения подробной информации о сетевых объектах, обратитесь к:

- «Виды сетей» (p. 49)
- «Компьютеры» (p. 52)
- «Виртуальные машины» (p. 116)
- «Мобильные устройства» (p. 180)
- «Инвентаризация патча» (p. 214)
- «Просмотр и управление задачами» (p. 223)
- «Удаление конечных точек из сетевого содержимого» (p. 228)
- «Настройка параметров сети» (p. 229)
- «Конфигурация настроек Security Server» (p. 232)
- «Диспетчер учетных данных (Credentials Manager)» (p. 233)

6.1. Виды сетей

Различные типы конечных точек, доступных в Control Center, сгруппированы в разделе **Сеть**, как различные виды сетей. Каждый вид сети отображает определенный тип сетевой инфраструктуры, содержащей типы конечных точек, которыми можно управлять.

Чтобы выбрать вид сети, перейдите в левую верхнюю часть раздела **Сеть** и нажмите меню видов:



Выбор просмотра

Доступны следующие виды сетей:

- Компьютеры и виртуальные машины
- Виртуальные машины
- Мобильные устройства

6.1.1. Компьютеры и виртуальные машины

Этот вид предназначен для компьютеров и виртуальных машин, интегрированных в Active Directory и предоставляет определенные действия

и параметры фильтрации для управления сетевыми компьютерами. Если интеграция с Active Directory выполнена, дерево Active Directory загружается вместе с соответствующими конечными точками.

При работе с видом **Компьютеры и виртуальные машины**, вы можете в любое время синхронизировать содержимое Control Center с Active Directory, используя кнопку **Синхронизировать с Active Directory** панели инструментов.

В то же время, все компьютеры и виртуальные машины, которые не интегрированы в Active Directory сгруппированы в пользовательские группы (Custom Groups). Эта группа может содержать следующие типы конечных точек:

- Компьютеры и виртуальные машины, доступные в вашей сети вне Active Directory.
- Виртуальные машины из виртуализированной инфраструктуры доступной в вашей сети.
- Серверы безопасности, которые уже установлены и настроены в вашей сети.

Примечание
Когда виртуальная инфраструктура доступна, вы можете разворачивать и управлять серверами безопасности из раздела меню **Виртуальные машины**. В противном случае, серверы безопасности могут быть установлены и настроены только локально на хостах.

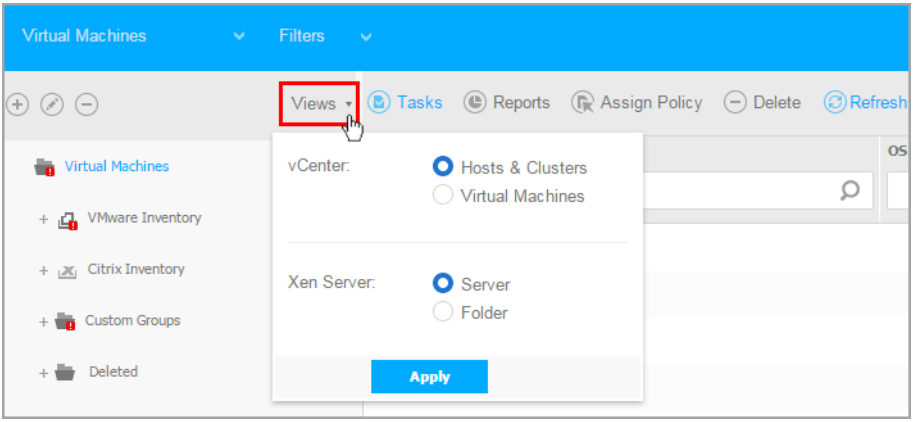
Важно
Назначение политик виртуальным машинам из меню **Компьютеры и виртуальные машины** может быть запрещена менеджером решения GravityZone при конфигурировании vCenter Server или Xen Server на странице **Конфигурация > Поставщики средств виртуализации**. Чтобы узнать больше, обратитесь к главе **Установка защиты > GravityZone Установка и настройка** из руководства по установке GravityZone.

6.1.2. Виртуальные машины

Данный вид специально разработан для отображения интеграции вашей виртуальной инфраструктуры. параметры фильтрации доступные в этом окне, позволяют задать специальные критерии для отображения объектов виртуальной среды.

Вы можете просмотреть виртуальные ресурсы Nutanix, VMware или Citrix на левой панели.

В верхней части левой панели вы также можете найти меню **Views**, позволяющее вам выбрать режим отображения виртуального содержимого.



Раздел Сеть - Меню виртуальных машин

Все виртуальные машины в вашей сети, которые не интегрированы в виртуальную инфраструктуру, отображаются как пользовательские группы (**Пользовательские группы**).

Для доступа к виртуальной инфраструктуре, интегрированной с Control Center, вы должны указать пользовательские данные для каждого доступного vCenter Server. Control Center использует ваши учетные данные для подключения к виртуальной инфраструктуре, отображая только те ресурсы, к которым у вас есть доступ (задается в vCenter Server). Если вы не указали ваши авторизационные учетные данные, вы должны будете ввести их, когда будете пытаться просматривать ресурсы любого vCenter Server. Единожды введя ваши учетные данные, они будут сохранены в вашем менеджере учетных данных и вам не придется вводить их повторно в дельнейшем.

6.1.3. Мобильные устройства

Данный вид специально разработан для просмотра и управления мобильными устройствами в вашей сети, предоставляя специальные действия и опции фильтрации.

В этом специфическом меню вы можете отображать сетевые элементы по пользователям или устройствам.

В случае доступности, сетевая панель отображает структуру дерева вашего Active Directory. В этом случае все пользователи Active Directory появятся среди элементов сети, а также мобильные устройства закрепленные за ними.

Примечание
Данные пользователей Active Directory будут автоматически загружены и не могут быть изменены.

Пользовательские группы (Custom Groups) содержат все мобильные устройства пользователей, которые могут быть добавлены вручную в Control Center.

6.2. Компьютеры

Чтобы увидеть под вашей учетной записью компьютеры, перейдите в раздел **Сеть** и выберите **Компьютеры и виртуальные машины** из меню видов.

Вы можете увидеть доступную структуру сети в левой панели и детальную информацию о каждом конечном устройстве на панели справа.

Все компьютеры и виртуальные машины, обнаруженные в вашей сети, отображаются как неуправляемые (Неуправляемый) и вы можете удаленно произвести установку защиты на них.

Для настройки отображения детальной информации о компьютерах в таблице:

1. Нажмите кнопку **Колонки** справа от Панель действий
2. Выберите столбцы, которые вы хотите отобразить.
3. Нажмите кнопку **Восстановить**, чтобы вернуться к виду столбцов по умолчанию.

На странице **Сеть**, вы можете выполнить следующие действия с компьютерами:

- Проверить статус компьютера
- Получить сведения о компьютере
- Организовать компьютеры в группы
- Выполнить сортировку, фильтрацию и поиск
- Управление патчами
- Запустить задачи
- Сформировать быстрые отчеты

- Назначить политики
- Синхронизироваться с Active Directory

Для просмотра самой актуальной информации, нажмите кнопку **Обновить** в нижнем левом углу таблицы. Данная функция может быть полезной, если вы длительное время находитесь на странице.

6.2.1. Проверка статуса компьютера

Каждый компьютер представлен на странице сети, иконкой определенного типа и состояния.

Обратитесь к «Типы сетевых объектов и статусы» (p. 608), чтобы просмотреть список со всеми доступными типами значков и статусов.

Для получения подробной информации о статусе, обратитесь к:

- Состояние управления
- Состояние подключения
- Статус безопасности

Состояние управления

Компьютеры могут иметь следующие статусы управления:

- **Управляемые** - компьютеры, на которых установлен агент безопасности.
- **Ожидают перезагрузки** - конечные точки, которые требуют перезагрузки системы после установки или обновления системы защиты Bitdefender.
- **Неуправляемые** - обнаруженные компьютеры, на которых агенты безопасности еще не были установлены.
- **Удаленные** - компьютеры, которые вы удалили из Control Center. Для получения более подробной информации, обратитесь к «Удаление конечных точек из сетевого содержимого» (p. 228).

Состояние подключения

Состояние подключения может отображаться только для управляемых машин. Исходя из этого управляемые компьютеры могут быть:

- **Онлайн**. Синий значок означает, что компьютер находится в сети.
- **Офлайн**. Серый значок означает, что компьютер находится в автономном режиме.

Компьютер переходит в автономный режим, если агент безопасности неактивен более 5 минут. Возможные причины, по которым компьютеры находятся в автономном режиме:

- Компьютер выключен, в режиме сна или гибернации.

  Примечание
  Компьютер остается в режиме online, даже когда он заблокирован или пользователь отключен.

- У агента безопасности нет подключения к коммуникационному серверуGravityZone:
  – Компьютер может быть отключен от сети.
  – Сетевой брандмауэр или маршрутизатор может блокировать связь между агентом безопасности и коммуникационным сервером GravityZone.
  – Компьютер находится за прокси-сервером и настройки прокси-сервера не были правильно настроены в примененной политике.

  Предупреждение
  Для компьютеров за прокси-серверером, настройки прокси-сервера должны быть правильно сконфигурированы в установочном пакете агента безопасности, в противном случае компьютер не сможет соединиться с консолью GravityZone и всегда будет появляться в автономном режиме, независимо от того, что политика с правильными настройками прокси-сервера была применена после установки.

- Агент безопасности работает ненадлежащим образом.

Чтобы узнать, как долго компьютеры были неактивны:

1. Отобразите только управляемые компьютеры. Нажмите меню **Фильтры** в верхней части таблицы, выберите все "Управляемые" варианты, которые вам нужны из вкладки **Безопасность**, выберите **Все предметы рекурсивно** из вкладки **Глубина** и нажмите **Сохранить**.
2. Нажмите на заголовок столбца **Последний просмотр**, чтобы отсортировать компьютеры по периоду бездействия.

Вы можете игнорировать короткие периоды бездействия (минуты, часы), так как они, вероятно, являются результатом временного состояния. Например, компьютер в настоящее время выключен.

Более длительные периоды бездействия (дни, недели), как правило, указывает на проблему с компьютером.

Примечание
Рекомендуется обновлять данные таблицы сети, время от времени, чтобы обновлять информацию о состоянии конечных точек.

Статус безопасности

Состояние безопасности может отображаться только для управляемых машин. Вы можете определить компьютеры с проблемами безопасности, проверяя значки состояния, отображающие символ предупреждения:

- Компьютер управляется, с проблемами, онлайн.
- Компьютер управляется, с проблемами, офлайн.

Компьютер может иметь проблемы с безопасностью, по крайней мере, в одной из следующих ситуаций:

- Защита от вредоносных программ отключена.
- Срок действия лицензии истек.
- Агент безопасности устарел.
- Механизмы защиты устарели.
- Обнаружены вредоносные программы.
- Связь с Bitdefender Cloud Services не может быть установлена из-за следующих возможных причин:
  - Компьютер имеет проблемы с подключением к Интернету.
  - Сетевой брандмауэр блокирует соединение с Bitdefender Cloud Services.
  - Порт 443, требующийся для связи с Bitdefender Cloud Services, закрыт.

  В этом случае защита от вредоносных программ полагается исключительно на локальный движок, в то время как сканирование в облаке выключено, это означает, что агент безопасности не может обеспечить полную защиту в режиме реального времени.

Если вы заметили компьютер с проблемами безопасности, нажмите на его имя, чтобы отобразить окно **Информация**. Вы можете определить проблемы безопасности по значку !. Убедитесь, что вы проверили информацию о безопасности на всех вкладках информационных страниц. Наведите курсор мыши на значок, чтобы отобразить подсказку, содержащую подробности. Могут потребоваться дальнейшие локальные расслдеования.

Примечание
Рекомендуется обновлять данные таблицы сети, время от времени, чтобы обновлять информацию о состоянии конечных точек.

6.2.2. Получение сведений о компьютере

На странице **Сеть** можно узнать подробные сведения о каждом компьютере следующим образом:

- Проверка **Сеть** страница
- Проверка **Информация** окно

Проверка страницы сети

Чтобы узнать подробную информацию о компьютере, проверьте данные в таблице правой панели на странице **Сеть**

Чтобы добавить или удалить столбцы с информацией о конечной точке, нажмите кнопку **Столбцы** в правой верхней части панели.

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемую группу в левой панели.

   Все доступных конечные точки выбранной группы выводятся в таблице правой панели.
4. Вы можете легко определить состояние компьютера, проверив соответствующий значок. Для получения дополнительной информации перейдите к «Проверка статуса компьютера» (p. 53).
5. Проверьте информацию, отображаемую в столбцах для каждого компьютера.

   Используйте строку заголовка для поиска определенных конечных точек в соответствии с доступными критериями:

   - **Имя**: имя конечной точки.
   - **FQDN**: полное доменное имя, которое включает в себя имя хоста и имя домена.
   - **OS**: операционная система установленая на конечной точке.
   - **IP**: IP-адрес конечной точки.

- **Последняя активность**: дата и время, когда виртуальная машина была в последний раз онлайн.

  Примечание
  Важно следить за полем **Последняя активность**, так как длительные периоды бездействия могут указывать на проблему связи или отключении компьютера.

- **Ярлык** : настраиваемая строка с дополнительной информацией о рабочей станции. Можете добавить метку в **Окно** Информации конечной точки, а затем использовать ее в поиске.
- **Политика**: политика, применяемая к конечной точке, содержит ссылку для просмотра или изменения параметров политики.

Проверка информационного окна

В правой боковой панели страницы **Сеть** щелкните имя интересующей вас конечной точки, чтобы отобразить окно **Сведения**. В этом окне отображаются сгруппированные по нескольким вкладкам данные, доступные только для выбранной конечной точки.

В окне **Информация** приведен полный список сведений в соответствии с типом конечной точки и сведениями о ее безопасности.

Вкладка "Общие"

- Общие сведения о компьютере, например, имя, полное доменное имя, IP-адрес, операционная система, инфраструктура, родительская группа и текущее состояние соединения.

  В этом разделе можно назначить конечную точку с меткой. Вы сможете быстро находить конечные точки с одной и той же меткой и принимать меры по отношению к ним, независимо от их расположения в сети. Для получения дополнительных сведений о фильтрации конечных точек перейдите к «Сортировка, фильтрация и поиск компьютеров» (p. 73).

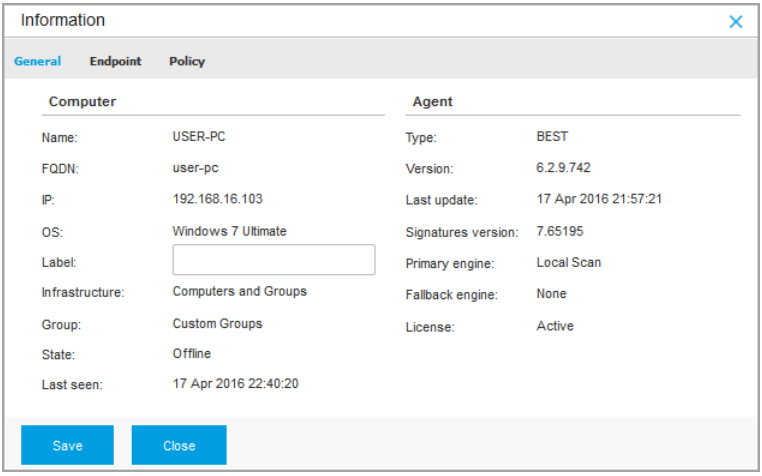
- Сведения об уровнях защиты, в том числе список технологий безопасности, приобретенных при помощи решения GravityZone, и статус их лицензии, которые могут быть:
  - **Доступен/Активный** - лицензионный ключ для данного уровня защиты активен на конечной точке.

– **Истек срок действия** — истек срок действия лицензионного ключа для данного уровня защиты.

– **Ожидание подтверждения** — лицензионный ключ еще не подтвержден.

Примечание
Дополнительная информация об уровнях защиты доступна на вкладке **Защита** .

- **Подключение ретрансляции**: имя, IP-адрес и метка ретранслятора, к которому подключена конечная точка.



Информационное окно - вкладка «Общие»

Вкладка "Защита"

Эта вкладка содержит сведения о каждом уровне защиты, применимом на конечной точке.

- Сведения об агенте безопасности, такие как название продукта, версия, статус обновления и расположение обновлений, а также конфигурация механизмов сканирования и версии содержимого безопасности. Для изменения защиты, версия антиспама также применима.
- Состояние безопасности для каждого уровня защиты. Этот статус отображается в правой части имени уровня защиты:

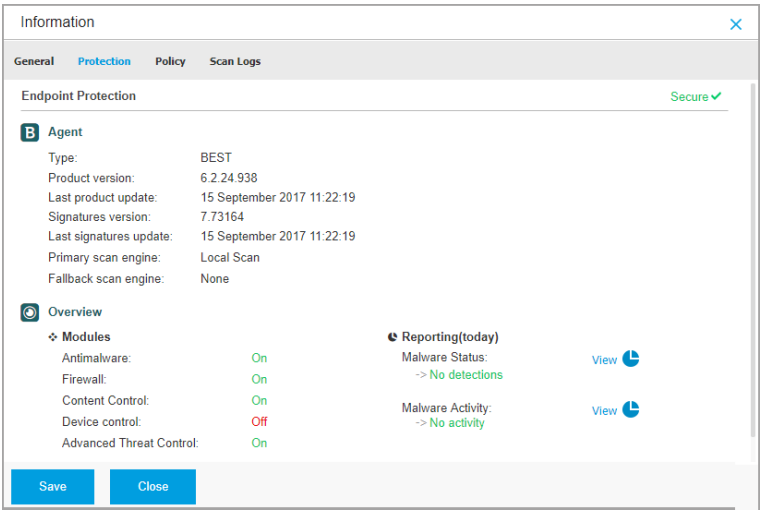
  - **Безопасный**, если на конечных точках, применяемых с уровнем защиты, не обнаружены проблемы безопасности.
  - **Уязвимый**, если на конечных точках, применяемых с уровнем защиты, обнаружены проблемы безопасности. Дополнительные сведения см. в разделе «Статус безопасности» (p. 55).

- Связанный Security Server. Каждый назначенный Security Server отображается в случае развертывания без агентов или при сканировании антивирусных механизмов безопасности, настроенных для использования удаленного сканирования. Информация Security Server помогает идентифицировать виртуальное устройство и получить статус его обновления.
- Статусы модулей защиты. Вы можете легко просмотреть, какие модули защиты были установлены на конечной точке, а также статус доступных модулей (**Вкл. / Выкл.**), установленных с помощью применяемой политики.
- Краткий обзор активности модулей и отчетов о вредоносном ПО за текущий день.

  Нажмите ссылку **Просмотр**, чтобы получить доступ к параметрам отчета, а затем Создать отчет. Для получения более подробной информации, обратитесь к «Создание отчетов» (p. 534)
- Информация, касающаяся слоя защиты Sandbox Analyzer:
  - Статус использования Sandbox Analyzer в конечных точках отображается с правой стороны окна:
    - **Активный**: Sandbox Analyzer лицензирован (доступен) и включается, исходя из политики в конечной точке.
    - **Неактивный**:Sandbox Analyzer лицензирован (доступен), но не включен, исходя из политики в конечной точке.
  - Название агента, который действует как датчик подачи.
  - Состояние модуля на конечной точке:
    - **Вкл** - Sandbox Analyzer включен в конечной точке, согласно политике.
    - **Выкл** -Sandbox Analyzer не включен в конечной точке, согласно политике.
  - Чтобы просмотреть угрозы обнаруженные на прошлой неделе, просмотрите отчет перейдя по ссылке **Просмотреть** .

- Дополнительная информация о модуле шифрования, например:
  - Обнаруженные тома (с указанием загрузочного диска).
  - Состояние шифрования для каждого тома (**Зашифрован**, **Выполняется шифрование**, **Выполняется дешифрование**, **Незашифрован**, **Заблокирован** или **Приостановлен**).

    Нажмите ссылку **Восстановление** , чтобы получить ключ восстановления для соответствующего зашифрованного тома. Подробнее о получении ключей восстановления см. «» (p. 115).
- Состояние телеметрии безопасности, которое информирует Вас о том, установлено ли и работает ли соединение между конечной точкой и SIEM-сервером, отключено или имеет проблемы.



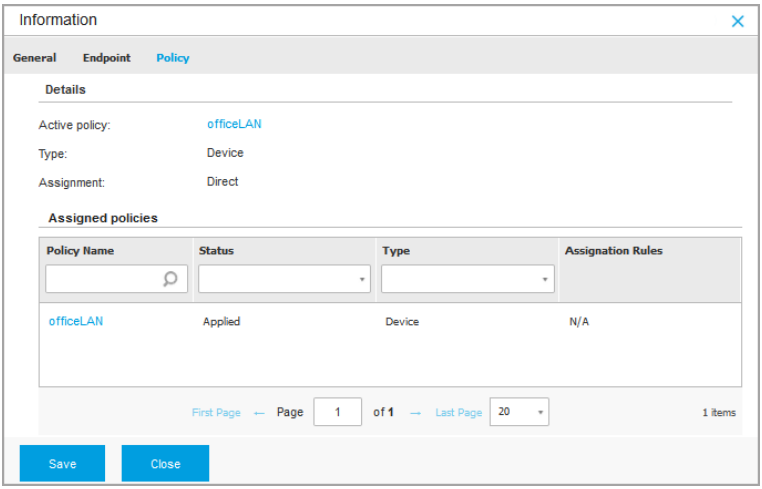
Информационное окно - вкладка "Защита"

Вкладка "Политика"

Конечная точка может применяться с одной или несколькими политиками, но одна политика может быть активна только с одной конечной точкой. На вкладке **Политика** отображаются сведения о всех политиках, применяемых к конечной точке.

- Имя активной политики. Нажмите на название политики, чтобы открыть шаблон политики и просмотреть ее настройки.
- Тип активной политики, который может быть:
  - **Устройство**: если сетевым администратором вручную назначена политика для конечной точки.
  - **Местоположение**: политика, основываясь на правилах, автоматически назначается конечной точке в том случае, если сетевые настройки конечной точки соответствуют заданным условиям правил назначения .

    Например, ноутбуку назначены две политики по месторасположению: одна называется `Office`, которая становится активной при подключении к сети компании, и `Roaming`, которая становится активной, когда пользователь работает удаленно и подключается к другим сетям.
  - **Пользователь**: политика, основываясь на правилах, автоматически назначается конечной точке в том случае, если она соответствует цели Active Directory, указанной в правиле назначения.
  - **Внешний (NSX)**: если политика определена в среде VMware NSX.
- Тип назначения активной политики, который может быть:
  - **Прямой**: если политика применяется непосредственно к конечной точке.
  - **Наследственный**: если конечная точка наследует политику родительской группы.
- **Применимые политики**: отображает список политик, связанных с существующими правилами назначения. Эти политики могут применяться к конечной точке, если она соответствует заданным условиям правил назначения.

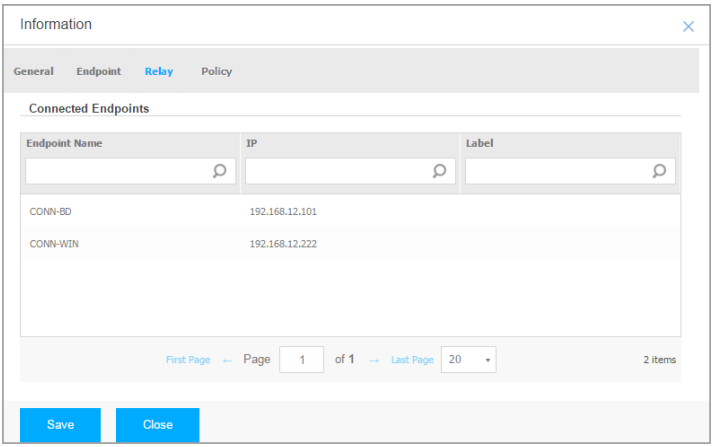


Информационное окно - вкладка «Политика»

Для получения дополнительной информации, касающейся политики, см.«Изменение настроек политики» (p. 252)

Вкладка подключенных конечных точек

Вкладка **Подключенные конечные точки** доступна только для конечных точек с ролью реле. Эта вкладка отображает информацию о конечных точках, подключенных к текущему ретранслятору, такую как имя, IP-адрес и метка.

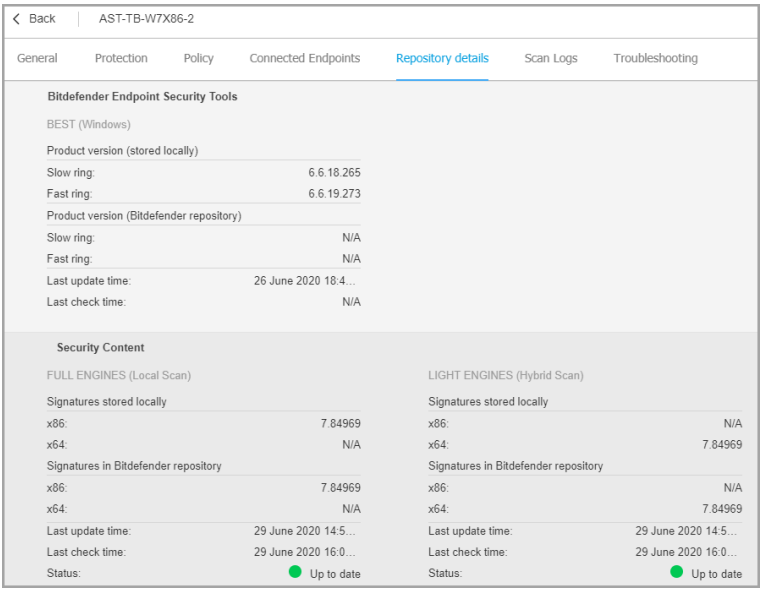


Информационное окно - вкладка подключенных конечных точек

вкладка содержимого репозитория

Вкладка **Сведения о репозитории** доступна только для конечных точек с ролью реле и отображает информацию об обновлениях агента безопасности и содержимом безопасности.

Вкладка содержит сведения о версиях продукта и сигнатур, хранящихся на реле, а также о доступных в официальном репозитории, кольцах обновлений, дате и времени обновления, и о последней проверке на наличие новых версий.



Информационное окно - вкладка содержимого репозитория

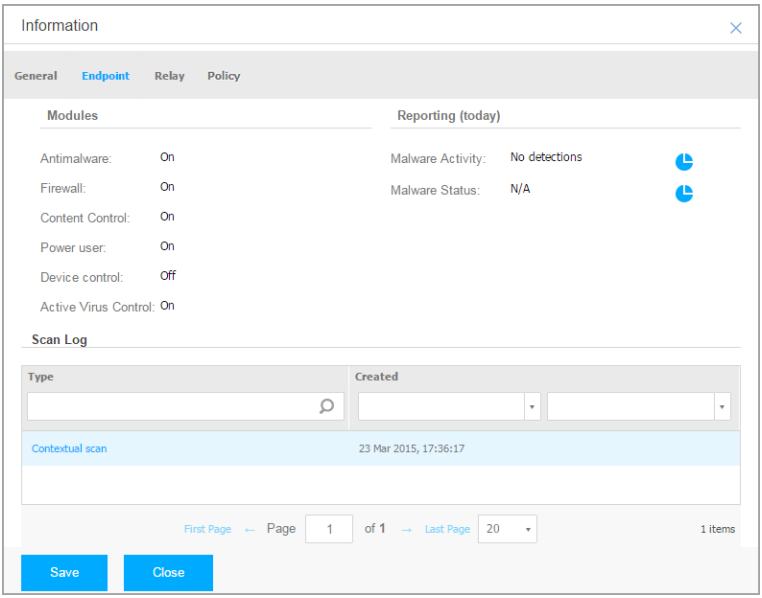
Вкладка "Журналы сканирования"

На вкладке **Сканирование журналов** отображается подробная информация обо всех задачах сканирования, выполняемых на конечной точке.

Журналы сгруппированы по уровню защиты, и вы можете выбрать в выпадающем списке, для какого уровня отображать журналы.

Выберите нужную задачу сканирования, и журнал откроется на новой странице браузера.

Если доступно много журналов сканирования, они могут занимать несколько страниц. Для перемещения по страницам используйте кнопки навигации в нижней части таблицы. Если доступно слишком много записей, вы можете использовать опции фильтрации, доступные в верхней части таблицы.

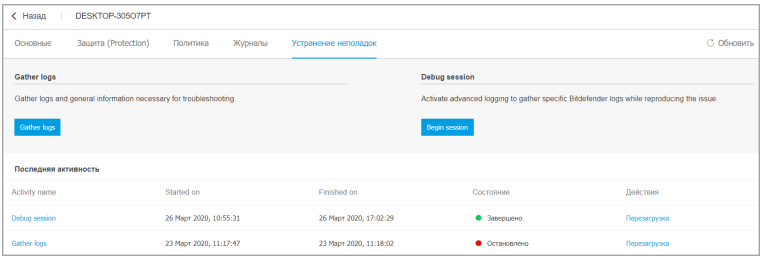


Информационное окно - вкладка «Журналы сканирования»

Вкладка "Устранение неполадок"

Этот раздел посвящен агенту устранения неполадок. Вы можете собирать общие или специальные журналы безопасности с конечных точек, проверять или участвовать в текущих событиях устранения неполадок и просматривать предыдущую активность.

Важно
Устранение неисправностей доступно лишь для Windows,Linux, macOS и всех типов серверов безопасности.



Информационное окно - вкладка "Устранение неполадок"

- **Сбор журналов**

  Эта опция помогает собирать журналы безопасности и общую информацию, необходимую для устранения неполадок таких как настройки, активные модули или политика безопасности, конкретная для целевой машины. Все сгенерированные данные сохраняются в архив.

  Рекомендуется использовать это опцию когда источник проблемы неясен.

  Для начала процесса устранения неполадок:

  1. Нажмите кнопку **Сбор журналов**. Появится окно конфигурации.
  2. В разделе **Хранилище журналов** выберите место хранения:
     - **Целевой компьютер**: архив журналов сохраняется по указанному локальному пути. Путь не настраивается для серверов безопасности.
     - **Общий сетевой ресурс**: архив журналов сохраняется по указанному пути из общего местоположения.

     Вы можете использовать опцию **Сохраняйте журналы также на целевой машине** , чтобы сохранять копию архивов журналов безопасности затронутых машин в качестве резервной копии.
  3. Внесите необходимую информацию (локальные пути, параметры доступа к ресурсам сети, путь к общему доступу) в зависимости выбранного местоположения.
  4. Нажмите кнопку **Сбор журналов**.

- **Сеанс отладки**

С помощью сеанса отладки вы можете активировать продвинутую регистрацию на целевой машине, чтобы собирать определенные журналы при воспроизведении проблемы.

Вам следует использовать эту опцию, когда вы обнаружили, какой модуль вызывает проблемы, или по рекомендации службы поддержки Bitdefender. Все сгенерированные данные сохраняются в архив.

Для начала процесса устранения неполадок:

1. Нажмите кнопку **Начать сеанс**. Появится окно конфигурации.
2. В разделе **Тип проблемы** выберите проблему, которая, по вашему мнению, касается компьютера.

   Типы проблем для компьютеров Windows и macOS:

Тип проблемы	Сценарий использования
Защита от вредоносного ПО (при доступе или при запросе)	– Общее снижение производительности конечной точки – Программа или системный ресурс слишком долго отвечает – Процесс сканирования занимает больше времени чем обычно – Нет соединения с ошибкой сервиса безопасности хоста
Ошибки обновления	– Сообщения об ошибке во время обновления продукта или механизмов защиты
Контроль содержимого (сканирование трафика и контроль пользователя)	– Сайт не загружается – Элементы на странице отображаются не полностью
Подключение к Облачным сервисам	– У конечной точки отсутствует соединение с Облачными сервисами Bitdefender
Общие проблемы продукта (чрезмерно	– Воспроизведите общую сообщенную проблему с подробным ведением журнала

Тип проблемы	Сценарий использования
детализированное ведение протокола)	

Issue types for Linux machines:

Тип проблемы	Сценарий использования
Защита от вредоносных программ и обновление	– Процесс сканирования занимает больше времени, чем обычно, и потребляет больше ресурсов – Сообщения об ошибке во время обновления продукта или механизмов защиты – Не удалось установить соединение конечных точек с GravityZone консолью.
Общие проблемы продукта (чрезмерно детализированное ведение протокола)	– Воспроизведите общую сообщенную проблему с подробным ведением журнала

Типы проблем для серверов безопасности:

Тип проблемы	Сценарий использования
Защита от вредоносного ПО (при доступе или при запросе)	Любое непредвиденное поведение Сервера безопасности, в том числе: – Виртуальные машины не защищены должным образом – Задачи сканирования на наличие вредоносных программ не выполняются или занимают больше времени, чем ожидалось – Обновления продукта установлены неправильно – Неисправность общего сервера безопасности (демоны bd не работают)

Тип проблемы	Сценарий использования
Связь с Центром управления GravityZone	Любое неожиданное поведение, наблюдаемое из консоли GravityZone: – Виртуальные машины не отображаются должным образом в консоли GravityZone – Вопросы политики (политика не применяется) – Сервер безопасности не может установить соединение с консолью GravityZone **Примечание** Используйте этот метод по рекомендации службы поддержки Bitdefender Enterprise.

3. Для **Продолжительность сеанса отладки** выберите временной интервал после которого сеанс отладки будет автоматически завершен.

   Примечание
   Рекомендуется вручную останавливать сеанс, используя опцию **Завершить сеанс**, сразу после воспроизведения проблемы.

4. В разделе **Хранилище журналов** выберите место хранения:
   - **Целевой компьютер**: архив журналов сохраняется по указанному локальному пути. Путь не настраивается для серверов безопасности.
   - **Общий сетевой ресурс**: архив журналов сохраняется по указанному пути из общего местоположения.

   Вы можете использовать опцию **Сохраняйте журналы также на целевой машине** , чтобы сохранять копию архивов журналов безопасности затронутых машин в качестве резервной копии.
5. Внесите необходимую информацию (локальные пути, параметры доступа к ресурсам сети, путь к общему доступу) в зависимости выбранного местоположения.
6. Нажмите кнопку **Начать сеанс**.

Важно
Вы можете запустить только один процесс устранения неполадок за раз (**Сбор журналов**/**Отладка**) на уязвимом компьютере.

- **История устранения неполадок**

  Раздел **Последняя активность** показывает активность устранения неполадок на затронутом компьютере. Сетка отображает только последние 10 событий устранения неполадок в хронологическом обратном порядке и автоматически удаляет активность старше 30 дней.

  Сетка отображает детали каждого процесса устранения неполадок.

  Процесс имеет основной и промежуточный статусы. В зависимости от пользовательских настроек вы можете иметь следующий статус, где вам необходимо принять меры:

  – **Выполняется (готов к воспроизведению вопроса)** - перейдите на затронутую машину вручную или дистанционно и воспроизведите проблему.

  У вас есть несколько опций для остановки процесса устранения неполадок:

  – **Завершить сеанс**: завершает сеанс отладки и процесс сбора на машине, сохраняя все собранные данные в специальное место хранения.

    Рекомендуется использовать эту опцию сразу после воспроизведения проблемы.

  – **Отменить**: эта опция отменяет процесс и журналы безопасности не собираются.

    Используйте эту опцию, если вы не хотите собирать какие-либо журналы с целевой машины.

  – **Принудительно завершить**: принудительно завершает процесс устранения неполадок.

    Используйте эту опцию, если отмена сессии занимает слишком много времени или целевая машина не отвечает. Вы сможете начать новую сессию за несколько минут.

  Для повторного запуска процесса устранения неполадок:

  – **Перезапуск**: эта кнопка, связанная с каждым событием и расположенная в разделе **Действия**, перезапускает выбранное действие по устранению неполадок, сохраняя прежние настройки.

Важно

– Чтобы убедиться, что консоль отображает последнюю информацию используйте кнопку **Обновить** на верхней правой стороне страницы **Устранение неполадок**.

– Для получения подробностей о конкретном событии нажмите на имя события из сетки.

6.2.3. Организация компьютеров в группы

Вы можете управлять группами компьютеров в левой панели раздела **Сеть**.

Основным преимуществом этой функции является то, что вы можете использовать групповые политики для удовлетворения различных требований к безопасности.

Компьютеры, импортированные из Active Directory, сгруппированы в папку **Active Directory**. Вы не можете редактировать группы Active Directory. Вы можете только просматривать и управлять соответствующими компьютерами.

Все обнаруженные в сети компьютеры не-Active Directory, находятся в **Пользовательские группы**, где можно организовать их в группы по вашему усмотрению. В **Пользовательские группы** вы можете создавать, удалять , переименовывать и перемещать группы компьютеров в произвольной древовидной структуре.

Примечание

- Группа может содержать как компьютеры, так и другие группы.
- При выборе группы в левой панели, вы можете просмотреть все компьютеры кроме тех, которые находятся в своих подгруппах. Для просмотра всех компьютеров, входящих в группу и в свои подгруппы, нажмите меню **Фильтры**, расположенное в верхней части таблицы и выберите **Все предметы рекурсивно** в разделе **Глубина**.

Создание групп

Прежде чем начать создавать группы, подумайте о причине создания, зачем они вам нужны и продумайте схему группировки. Например, вы можете сгруппировать конечные точки на основе одного или нескольких следующих критериев:

- Организационная структура (продажи, маркетинг, контроль качества, разработка программного обеспечения, управление и т.д.).
- Требования безопасности (настольные компьютеры, ноутбуки, сервера и т.д.).
- Местонахождение (штаб, местные офисы, удаленные сотрудники, домашние офисы и т.д.).

Для организации вашей сети в группы:

1. Выберите **Пользовательские группы** в левой панели.
2. Нажмите кнопку **Добавить группу** в верхней части левой панели.
3. Введите подходящее имя группы и нажмите **OK**. Новая группа появится в разделе **Пользовательские группы**.

Переименование групп

Чтобы переименовать группу:

1. Выберите группу в левой панели.
2. Нажмите кнопку **Редактировать группу** в верхней части левой панели.
3. Введите новое имя в соответствующем поле.
4. Нажмите **OK** для подтверждения.

Перемещение групп и компьютеров

Вы можете перемещать объекты **Пользовательские группы** в любое место внутри иерархии групп. Для перемещения объекта, перетащите его из правой панели в желаемую группу левой панели.

Примечание

Объект, который перемещается, унаследует параметры политик новой родительской группы, если другая политика не была непосредственно применена к нему. Для получения более подробной информации о наследовании политик, обратитесь к «Политики безопасности (Security Policies)» (p. 237).

Удаление групп

Удаление группы - это окончательное действие. В результате агент безопасности, установленный на целевой конечной точке, будет удален.

Чтобы удалить группу:

1. Нажмите на пустую группу в левой панели раздела **Сеть**.

2. Нажмите кнопку ⊖ **Удалить группу** в верхней части левой панели. Вы должны будете подтвердить ваши действия, нажав **Да**.

6.2.4. Сортировка, фильтрация и поиск компьютеров

В зависимости от количества конечных точек, правая панель может занимать несколько страниц (всего 20 записей на каждой странице отображается по умолчанию). Для перемещения по страницам используйте кнопки навигации в нижней части таблицы. Чтобы изменить количество записей отображаемых на странице, введите другое значение в поле рядом с кнопками навигации.

Если записей слишком много, вы можете использовать поля поиска под заголовками столбцов или меню **Фильтры** в верхней части страницы, чтобы отобразить только те объекты, которые вам необходимы. Например, вы можете искать конкретный компьютер или выбрать для просмотра только управляемые компьютеры.

Сортировка компьютеров

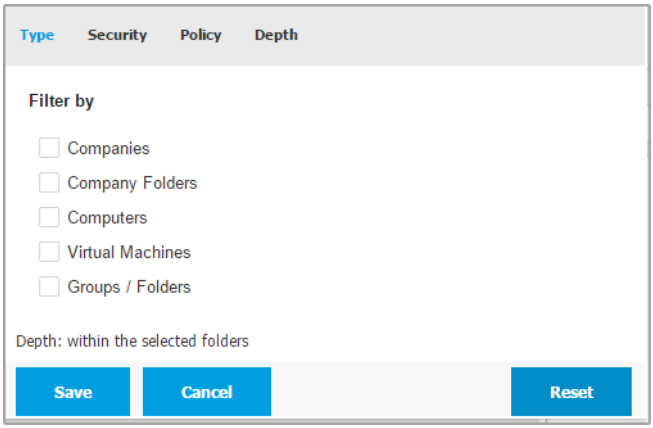
Для сортировки данных по определенному столбцу, щелкните заголовок столбца. Например, если вы хотите отсортировать компьютеры по имени, щелкните на заголовок **Имя**. При повторном нажатии на заголовок компьютеры будут отображаться в обратной последовательности.

Сортировка компьютеров

Фильтрация компьютеров

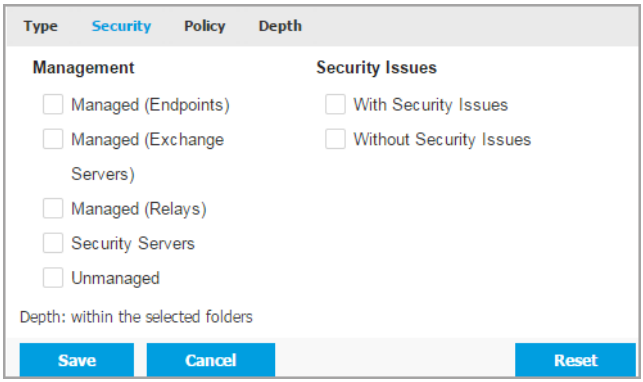
Чтобы отфильтровать ваши сетевые объекты, используйте меню **Фильтры** в правой верхней части сетевой панели.

1. Выберите желаемую группу из левой панели.
2. Нажмите меню **фильтры** в правой верхней части сетевой панели.
3. Вы можете использовать следующие критерии фильтрации:
   - **Тип**. Выберите тип объектов, которые будут отображаться (компьютеры, виртуальные машины, папки).



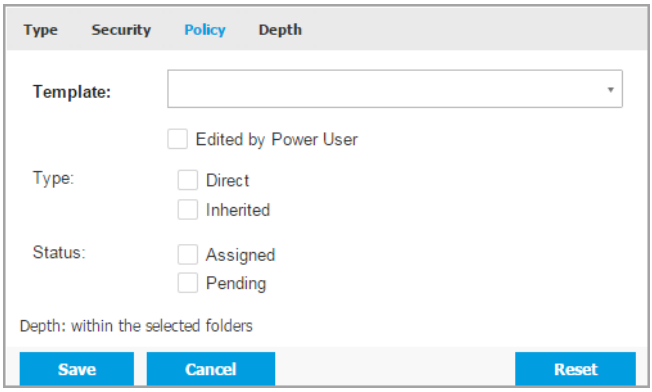
Компьютеры - Фильтрация по типу

- **Безопасность**. Выберите отображение компьютеров по управлению защитой, состоянием безопасности или ожидающими действиями.



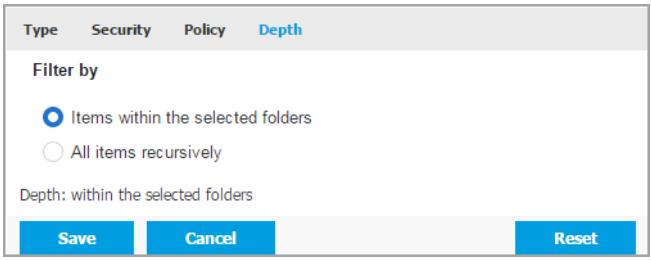
Компьютеры - Фильтрация по безопасности

- **Политика**. Выберите шаблон политики, для которого нужно фильтровать компьютеры, тип назначения политики (прямой или наследуемый), а также статус назначения политики (активный, применяемый или в ожидании). Вы также можете выбрать для отображения объекты только с политиками, отредактированными привилегированными пользователями.



Компьютеры - Фильтрация по политикам

- **Глубина**. При управлении структурированной сетью, компьютеры в подгруппах не будут отображаться при выборе корневой группы. Чтобы просмотреть все компьютеры, входящие в текущую группу и все подгруппы, выберите **Все элементы рекурсивно**.



Компьютеры - Фильтрация по глубине

При выборе рекурсивного просмотра всех элементов Control Center отображает их в виде простого списка. Чтобы найти местоположение элемента, выберите интересующий вас элемент и нажмите **Перейдите в контейнер** в верхней части таблицы. Вы будете перенаправлены в вышестоящий контейнер выбранного элемента.

Примечание
Вы можете просмотреть все выбранные критерии фильтрации в нижней части окна **Filters**.

Если вы хотите очистить все фильтры, нажмите кнопку **сбросить**.

4. Нажмите **Сохранить**, чтобы отфильтровать компьютеры по выбранным критериям. Фильтр в разделе **Сеть** остается активным, пока вы не выйдите из раздела или не сбросите фильтр.

Поиск компьютеров

1. Выберите нужную группу в левой панели.
2. Введите слово для поиска в соответствующем поле под заголовками столбцов в правой панели. Например, введите IP-адрес компьютера, который вы ищете в поле **IP**. В таблице отобразится только соответствующий компьютер.

   Очистите окно поиска, чтобы отобразить полный список компьютеров.

Поиск компьютеров

6.2.5. Запущенные Задачи

В разделе **Сеть** вы можете удаленно запускать на компьютерах ряд администраторских задач.

Вы можете выполнить следующие задачи:

- «СКАНИРОВАТЬ» (p. 77)
- «Задачи патчей» (p. 89)
- «Сканирование Exchange» (p. 92)
- «Установить» (p. 96)
- «Удаление клиента» (p. 103)
- «Обновление клиента» (p. 104)
- «Перенастройка клиента» (p. 105)
- «Обслуживание клиента» (p. 107)
- «Перезагрузка машины» (p. 108)
- «Сетевое Обнаружение» (p. 109)

- «Обнаружение Приложений» (p. 109)
- «Обновление Security Server» (p. 110)
- «Ввести Пользовательский инструмент» (p. 111)

Вы можете создавать задачи отдельно для каждого компьютера или для групп компьютеров. Например, вы можете удаленно установить агент безопасности группе неуправляемых компьютеров. Позже, вы можете создать задачу сканирования определенного компьютера в этой группе.

Для каждого компьютера вы можете запускать только совместимые задачи. Например, если вы выберите неуправляемый компьютер, то вы можете выбрать только установку агента безопасности, все другие задачи будут недоступны.

Задача, выбранная для группы, будет выполнена только на совместимых компьютерах. Если ни один из компьютеров в группе не совместим с выбранной задачей, вы будете уведомлены, что задача не может быть выполнена.

После создания, задача запустится сразу же, когда компьютеры будут онлайн. Если компьютер находится в автономном режиме, задание начнет выполняться, как только он подключится к сети.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

СКАНИРОВАТЬ

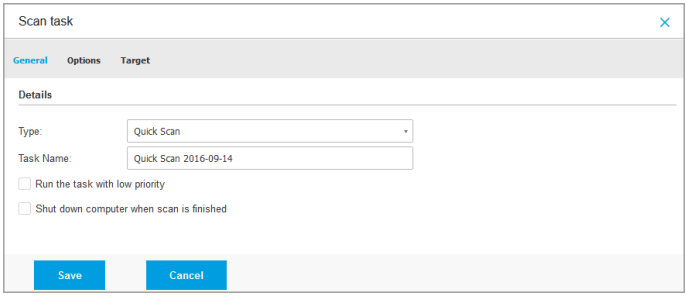
Для удаленного запуска задачи сканирования на одном или нескольких компьютерах:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Отметьте флажками компьютеры или группы, которые вы хотите просканировать.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Сканировать**.

   Появится окно настроек.

6. Настройте параметры сканирования:

- На вкладке **Общее** вы можете выбрать тип сканирования и ввести имя для задачи проверки. Название задачи сканирования предназначено для более простой идентификации соответствующей задачи на странице **Задачи**.



Задача сканирования компьютеров - Настройка общих параметров

Выберите тип сканирования из меню **Тип**:

– **Быстрое сканирование** использует облачное сканирование для обнаружения вредоносных программ, запущенных в системе. Данный тип сканирования предварительно настроен, чтобы сканировать только критические системные области Windows и Linux. Быстрое сканирование занимает, как правило, менее минуты. Быстрое сканирование использует лишь незначительную часть системных ресурсов, в отличие от процесса стандартного антивирусного сканирования.

  Bitdefender автоматически переходит к обезвреживанию, если обнаружены вредоносные программы или руткиты. Если по какой-либо причине файл нельзя вылечить, он перемещается в карантин. Этот тип сканирования игнорирует подозрительные файлы.

– **Полное сканирование** проверяет всю систему на все типы вредоносных программ, угрожающих безопасности, таких как вирусы, программы-шпионы, рекламное ПО, руткиты и другие.

  Bitdefender автоматически пытается обезвреживать файлы, обнаруженные вредоносными программами. Если вредоносная

программа не может быть удалена, она перемещвется в карантин, где она не может навредить. Подозрительные файлы игнорируются. Если вы хотите принять меры и в отношении подозрительных файлов, или если вы хотите выполнить другие действия по умолчанию для зараженных файлов, выберите вариант «Запуск пользовательского сканирования».

– **Сканирование памяти** проверяет программы, запущенные в памяти компьютера.

– **Сканирование сети** тип пользовательского сканирования, позволяющий сканировать сетевые диски, используя агента безопасности Bitdefender, установленного на выбранной конечной точке.

  Для выполнения задачи сетевого сканирования:

  - Вам необходимо назначить задачу для одной конечной точки в сети.
  - Для агента безопасности вам необходимо ввести учетные данные пользователя с правами чтения/записи для выбранных сетевых дисков, чтобы иметь возможность получить доступ и выполнить требуемые действия на этих сетевых дисках. Необходимые учетные данные могут быть сконфигурированы на вкладке **Цель** окна задач.

– **Выборочное сканирование** позволяет выбирать места сканирования и настраивать параметры сканирования.

Для выборочного сканирования, сканирования памяти и сети, вы можете выбрать следующие опции:

– **Выполнить задачу с низким приоритетом**. Установите этот флажок для снижения приоритета процесса сканирования, чтобы другие программы смогли работать быстрее. При это может увеличится время, необходимое для завершения процесса сканирования.

Примечание
Эта опция применима только к Bitdefender Endpoint Security Tools и Endpoint Security (устаревший агент)

– **Выключить компьютер после завершения сканирования** Установите этот флажок, чтобы выключить машину, если вы не собираетесь использовать ее некоторое время.

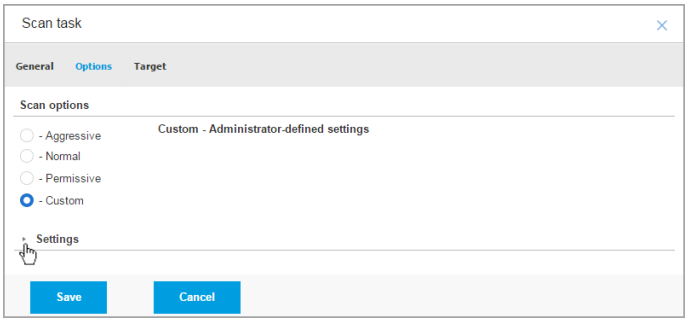
Примечание
Эта опция применима к Bitdefender Endpoint Security Tools, Endpoint Security (устаревший агент) и Endpoint Security for Mac.

Примечание
Только два варианта применимы к Bitdefender Endpoint Security Tools и Endpoint Security (устаревший агент).

Для пользовательского сканирования (Custom Scan) настройте следующие параметры:

– Перейдите на вкладку **Опции**, чтобы установить параметры сканирования. Выберите уровень безопасности, который лучше всего соответствует вашим потребностям (Интенсивный, Нормальный или Рекомендуемый). Используйте описания справа от шкалы, которые помогут сделать выбор.

  В зависимости от выбранного профиля, параметры сканирования в разделе **Настройки** будут сконфигурированы автоматически. Тем не менее, при желании, вы можете настроить их более детально. Чтобы сделать это, отметьте чек-бокс **Пользователь** и затем раскройте раздел **Настройки**.



Задачи сканирования компьютеров - Настройка пользовательского режима

Доступны следующие опции:

- **Типы файлов.** Используйте данную настройку, чтобы задать типы файлов, которые вы хотите просканировать. Вы можете указать агенту безопасности просканировать все файлы (независимо от их расширений), только файлы приложений или специфические типы файлов, которые вы считаете потенциально опасными. При сканировании всех файлов обеспечивается оптимальная защита. Сканируя только приложения, можно повысить скорость сканирования.

  Примечание

  Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 610).

  Если вы хотите просканировать только специфические типы файлов, выберите в меню **Пользовательские расширения** и затем введите желаемые расширения в редактируемом поле, нажимая `войти` после каждого расширения.

  Важно

  Агенты безопасности Bitdefender устанавливаются в операционных системах Windows и Linux, сканируют большинство .ISO форматов, но не предпринимают никаких действий над ними.

Настройка задач по сканированию компьютеров - Добавление пользовательских расширений

- **Архивы.** Архивы, содержащие инфицированные файлы, не представляют непосредственной угрозы безопасности системы. Вредоносные программы могут повлиять на систему только

если зараженный файл извлечен из архива и будет исполнен при выключенной защите в реальном времени. Тем не менее, рекомендуется сканировать архивы для обнаружения и удаления любой потенциальной угрозы, даже не представляющей собой непосредственной угрозы системе.

Важно
Сканирование файлов, сжатых в архив, увеличивает общее время сканирования и занимает больший объем системных ресурсов.

– **Сканирование внутри архивов.** Выберите эту опцию, если вы хотите проверить заархивированные файлы на наличие вредоносных программ. Если вы решили использовать данную опцию, вам необходимо настроить следующие параметры оптимизации:

  - **Ограничение размера архива (Мб).** Вы можете установить максимально допустимый размер архивов для сканирования. Поставьте флажок в соответствующем поле и введите максимальный размер архива (в МБ).
  - **Максимальная глубина архива (уровни).** Отметьте соответствующий флажок и выберите в меню максимальную глубину архива. Для лучшей производительности выберите наименьшее значение, для максимальной защиты выберите наибольшее значение.

– **Сканировать архивы электронной почты.** Выберите данную опцию если хотите разрешить проверку почтовых сообщений и почтовых баз, включая такие форматы файлов как .eml, .msg, .pst, .dbx, .mbx, .tbb и другие.

Важно
Процесс сканирования почтовых архивов является достаточно ресурсоемким и может повлиять на производительность системы.

- **Разное.** Выберите соответствующие флажки, чтобы включить нужные параметры сканирования.

- **Сканирование загрузочных секторов.** Проверка загрузочных секторов системы. Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки. Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.
- **Сканирование реестра.** Выберите этот параметр для сканирования ключей реестра. Реестр Windows — это база данных, в которой хранятся настройки и параметры конфигурации для компонентов операционной системы Windows и установленных приложений.
- **Сканирование на наличие руткитов.** Выберите этот параметр для сканирования на наличие руткитов и объектов, скрытых с помощью такого программного обеспечения.
- **Сканирование на наличие клавиатурных шпионов.** Выберите данную опцию для сканирования системы на наличие клавиатурных шпионов.
- **Сканировать общие сетевые ресурсы.** Эта опция сканирует подключенные сетевые диски.

  Для быстрого сканирования эта опция отключена по умолчанию. Для полного сканирования опция активирована по умолчанию. Для сканирования по выбору пользователя, если вы установите уровень безопасности **Интенсивный/Нормальный**, параметр **Сканирование общих сетевых ресурсов** включается автоматически. Если вы установите уровень безопасности **Рекомендуемый**, параметр **Сканирование общих сетевых ресурсов** автоматически отключается.
- **Сканирование памяти.** Выберите этот параметр для сканирования программ, запущенных в системной памяти.
- **Сканирование файлов cookie.** Выберите эту опцию для сканирования cookies-файлов, сохраненных браузерами на компьютере.
- **Сканирование только новых/измененных файлов.** Сканируя только новые и измененные файлы, можно значительно

повысить общее быстродействие системы с минимальными потерями в безопасности.

– **Сканирование на наличие потенциально нежелательных приложений (PUA).** Потенциально нежелательные приложения (PUA) это программы, которые могут быть нежелательными для ПК, а иногда и поставляться в комплекте с программным обеспечением бесплатного. Такие программы могут быть установлены без согласия (также называются рекламными) или включены по умолчанию в комплект экспресс-установки (как дополнение). Потенциальное воздействие этих программ заключается в показе всплывающих окон, установке нежелательных панелей инструментов в браузере по умолчанию или работе нескольких процессов в фоновом режиме, что замедляет производительность компьютера.

– **Сканирование съемных носителей.** Выберите этот параметр для сканирования любых съемных накопителей, подключаемых к компьютеру.

- **Действия.** В зависимости от типа обнаруженного файла автоматически выполняются следующие действия:

  – **Действие при обнаружении зараженного файла.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ). Агент безопасности Bitdefender может удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция известна как лечение.

    По умолчанию, если зараженный файл обнаружен, агент безопасности Bitdefender автоматически попытается вылечить его. Если файл не удается вылечить, он перемещается в карантин в целях предотвращения распространения вируса.

    Важно
    В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является

полностью вредоносным. В таких случаях выполняется удаление зараженного файла с диска.

– **Действие при обнаружении подозрительного файла.** Для обнаружения подозрительных файлов Bitdefender использует Эвристический анализ и другие технологии . Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные). Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.

  По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин. Помещенные в карантин файлы отправляются на анализ в лабораторию Bitdefender на регулярной основе. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить.

– **Когда найден руткит.** Руткиты представляют собой специализированное программное обеспечение, используемое для того, чтобы скрыть файлы операционной системы. Однако, руткиты часто используются, чтобы скрыть вредоносные программы, либо для сокрытия присутствия злоумышленника в системе.

  Обнаруженные руткиты и скрытые файлы по умолчанию игнорируются.

Хотя это и не рекомендуется, вы можете изменить действие по умолчанию. Можно задать дополнительное действие, которое будет выполнено в случае, если не удалось выполнить первое, а также различные действия для каждой из категорий. Выберите в соответствующих меню первое и второе действие, которые будут выполняться в отношении всех типов обнаруженных файлов. Доступны следующие действия:

Лечить

Удаляет вредоносный код из зараженных файлов. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов.

Перемещение файлов в карантин

Перемещает зараженные файлы из исходного расположения в папку карантина. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице консоли Quarantine.

Удалить

Удаляет обнаруженные файлы с диска без предупреждения. Желательно избегать использование этого действия.

Пропустить

Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования.

– Перейдите на вкладку **Цель**, чтобы настроить местоположения, которые вы хотите просканировать на компьютерах.

  В разделе **Сканирование цели** вы можете добавить новый файл или папку, которые необходимо проверить:

  a. Выберите предопределенное месторасположение из выпадающего меню или введите конкретные пути в **конкретные пути**, которые вы хотите просканировать.

  b. Укажите путь к объекту для сканирования в поле редактирования.

  - Если вы выбрали предопределенное место, необходимо корректно завершить путь. Например, для сканирования всей папки `Програмные файлы`, достаточно выбрать соответствующее предопределенное место из выпадающего меню. Для сканирования конкретной папки из `Програмные файлы`, необходимо завершить путь, добавив обратную косую черту (\) и имя папки.

  - Если вы выбрали **Конкретные пути**, введите полный путь к объекту проверки. Желательно использовать системные переменные (в соответствующих случаях), чтобы быть уверенным, что путь действителен для всех нужных компьютеров. Для получения более подробной информации

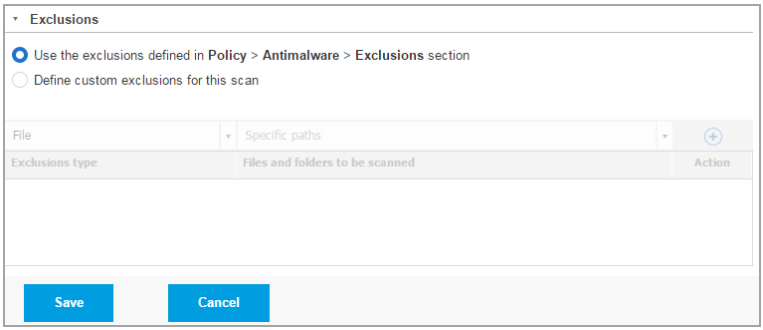
о системных переменных, обратитесь к «Системные переменные» (p. 611).

c. Нажмите соответствующую кнопку ⊕ **Добавить**.

Чтобы изменить существующий путь, нажмите на него. Чтобы удалить папку из списка, нажмите соответствующую кнопку ⊗ **Удалить**.

Для агента безопасности вам необходимо ввести учетные данные пользователя с правами чтения/записи для выбранных сетевых дисков, чтобы иметь возможность получить доступ и выполнить требуемые действия на этих сетевых дисках.

Нажмите на раздел **Исключения**, если вы хотите добавить исключения.



Задача сканирования компьютеров - Добавление исключений

Вы можете либо использовать исключения определенные политикой, либо определить явные исключения для текущей задачи сканирования. За более подробной информацией об исключениях, обратитесь к «Исключения» (p. 312).

7. Нажмите **Сохранить**, чтобы создать задачу сканирования. Появится окно подтверждения.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Примечание
Чтобы запланировать задачу сканирования, перейдите на страницу **Политики**, выберите политику, которая будет назначена требуемым компьютерам и добавьте задачу проверки в разделе **Защита от вредоносных программ > По требовнию**. Для получения более подробной информации, обратитесь к «Сканирование по запросу (On-Demand)» (p. 290).

Сканирование рисков

Вы можете в любое время запустить задачи сканирования рисков по требованию на выбранных конечных точках, выполнив следующие действия:

1. Перейдите в раздел **Сеть**.
2. Просмотрите контейнеры в левой части экрана и выберите конченые точки, которые вы хотите сканировать.
3. Нажмите кнопку **Задачи** и выберите **Сканирование на наличие рисков**.

   Будет появляться сообщение с требованием подтверждения запуска сканирования на наличие рисков.

   Примечание
   Сканирование на наличие рисков будет запущено при всех показателях, которые активируются по умолчанию.

4. После успешного завершения операции Вы можете перейти на вкладкуНеправильная настройка страницы **Рисков безопасности**, проанализировав их, и выбрать показатели, которые следует проигнорировать.

   Оценка всех рисков компании будет пересмотрена в связи с оставленными без внимания индикаторами риска.

   Примечание
   Чтобы просмотреть полный список индикаторов и их описание, см. эту статью Базы Знаний.

Важно
Задачи **Сканирование рисков** не запустятся/не будут выполняться на конечных точках в следующих ситуациях:

- На конечной точке нет операционной системы Windows.

- Лицензия агента конечной точки Bitdefender недействительна.
- Политика, примененная к конечной точке, отключила Модуль управления рисками.

Задачи патчей

Рекомендуется регулярно проверять обновления ПО и применять их как можно скорее. GravityZone автоматизирует этот процесс с помощью политик безопасности, но если вам нужно обновить программное обеспечение сразу на определенных конечных точках, выполните следующие задачи в следующем порядке:

1. Сканирование патча
2. Установка патча

Требования к системе

- Агент безопасности с модулем управления исправлениями устанавливается на конечных точках.
- Для успешного выполнения задач сканирования и установки конечные точки Windows должны соответствовать следующим условиям:
  - **Доверенные корневые центры сертификации** хранит **Сертификат корневого ЦС DigiCert Assured ID**.
  - **Промежуточные центры сертификации** включает в себя **центр сертификации подписанного кода DigiCert SHA2**.
  - На конечных точках установлены исправления для Windows 7 и Windows Server 2008 R2, упомянутые в этой статье Microsoft: Рекомендации по безопасности Microsoft 3033929

Сканирование патча

Конечные точки с устаревшим программным обеспечением уязвимы для атак. Рекомендуется регулярно проверять и устанавливать обновление ПО на конечных точках. Чтобы сканировать конечные точки на наличие пропущенных исправлений:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.

3. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
4. Выберите целевые конечные точки
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Сканировать исправления**. Появится окно подтверждения.
6. Нажмите **Да** чтобы подтвердить задачу сканирования

   Когда задача заканчивается, GravityZone добавляет в Инвентарь исправлений все исправления, необходимые для вашего программного обеспечения. Дополнительные сведения см. в разделе «Инвентаризация патча» (p. 214).

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Примечание
Чтобы запланировать сканирование исправлений, измените политики, назначенные целевым конечным точкам, и настройте параметры в разделе **Управление исправлениями**. Для получения более подробной информации, обратитесь к «Управление исправлениями» (p. 363).

Установка патча

Чтобы установить 1 или несколько исправлений на целевой конечной точке:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Установить исправления**.

   Появится окно настроек. Здесь вы можете просмотреть все патчи, отсутствующие на целевых конечных точках.
5. При необходимости используйте параметры сортировки и фильтрации в верхней части таблицы, чтобы найти конкретные исправления.
6. Нажмите кнопку **Столбцы** в верхней правой части панели, чтобы просмотреть только соответствующую информацию.

7. Выберите исправления, которое вы хотите установить.

   Некоторые исправления зависят от других В таком случае они автоматически выбираются один раз вместе с исправлением.

   При нажатии на номера **CVE** или **Продукты** отобразится панель с левой стороны. Панель содержит дополнительную информацию, такую как CVE, которые исправляет исправление, или продукты, к которым применяется исправление. Как только прочитаете, нажмите **Закрыть**, чтобы скрыть панель.

8. Выберите **Перезагрузить конечные точки после установки исправления, если необходимо**, чтобы перезапустить конечные точки сразу после установки исправления, если требуется перезагрузка системы. Учтите, что это действие может прервать сеанс пользователя.

9. Щелкните **Установить**.

   Задача установки создается вместе с подзадачами для каждой целевой конечной точки.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Примечание

- Чтобы запланировать развертывание исправлений, измените политики, назначенные целевым конечным точкам, и настройте параметры в разделе **Управление исправлениями**. Для получения более подробной информации, обратитесь к «Управление исправлениями» (p. 363).
- Вы также можете установить исправление со страницы **Инвентарь исправлений**, начиная с определенного интересующего вас исправления. В этом случае выберите исправление из списка, нажмите кнопку **Установить** в верхней части таблицы и настройте параметры установки исправления. Дополнительные сведения см. в разделе «Установка патчей» (p. 218).
- После установки исправления мы рекомендуем отправить задачу Сканировать исправления конечным точкам. Это действие обновит информацию об исправлении, сохраненную в GravityZone для ваших управляемых сетей.

Вы можете удалить исправления:

- Удаленно, отправив из GravityZone Задача удаления исправлений.

- Локально на конечной точке В этом случае вам необходимо войти в систему как администратор конечной точки и запустить деинсталлятор вручную.

Сканирование Exchange

Вы можете удаленно сканировать базу данных сервера Exchange, запустив задачу **Exchange Scan**.

Для того, чтобы сканировать базу данных Exchange, необходимо включить сканирование по запросу, указав учетные данные администратора Exchange. Для получения более подробной информации, обратитесь к «Сканирование хранилища Exchange» (p. 391).

Для сканирования базы данных сервера Exchange:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. В левой панели, выберите группу, содержащую нужный сервер Exchange. Желаемый сервер вы можете выбрать в правой панели.

   Примечание
   При желании, вы можете использовать фильтры, чтобы быстро найти нужный сервер:
   - Нажмите меню **Фильтры** и выберите следующие параметры: **Управляемый (Exchange Servers)** на вкладке **Безопасность** и **Все пункты рекурсивно** на вкладке **Глубина**.
   - Введите имя сервера или IP-адрес в нужном поле под заголовком соответствующего столбца.

4. Отметьте флажком сервер Exchange, базу данных которого вы хотите проверить.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Exchange Scan**. Появится окно настроек.
6. Настройте параметры сканирования:
   - **Общее** Введите подходящее имя задачи.

     Для больших баз данных задача сканирования может занимать много времени и может повлиять на производительность сервера. В таких случаях, установите флажок **Остановите сканирование, если это займет больше времени, чем** и выбрать подходящий интервал времени в соответствующем меню.

- **Цель** Выберите контейнеры и объекты, которые будут проверяться. Вы можете выбрать для сканирования: почтовые ящики, общие папки или и то, и другое. Кроме электронной почты, вы можете выбрать для сканирования другие объекты, такие, как **Контакты**, **Задачи**, **Фурнитура** и **Опубликовать элементы**. Кроме того, вы можете установить следующие ограничения на содержимое, которое будет проверяться:
  - Только непрочитанные сообщения
  - Только элементы с вложениями
  - Только новое, полученное в указанный промежуток времени

  Например, вы можете выбрать для сканирования только письма почтовых пользователей, принятые за последние семь дней.

  Выберите флажок **Исключения**, если вы хотите определить исключения при сканировании. Чтобы создать исключение, используйте поля из заголовков таблицы следующим образом:

  a. Выберите тип репозитория из меню.
  b. В зависимости от типа хранилища укажите объекты, которые должны быть исключены:

Тип хранилища	Формат объекта
Почтовый ящик	Адрес электронной почты
Общая папка	Путь к папке, начиная с корня каталога
База данных	Идентификатор базы данных

  Примечание
  Для получения идентификатора базы данных, используйте команду оболочки Exchange:
  `Get-MailboxDatabase | fl name,identity`

  Вы можете ввести только одну команду за один раз. Если у вас есть несколько объектов одного типа, вы должны задать столько правил, сколько элементов.

  c. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы сохранить исключение и добавить его в список.

  Чтобы удалить правило исключения из списка, нажмите соответствующую кнопку ⊖ **Удалить**.

- **Параметры** Настройте параметры сканирования для сообщений электронной почты, соответствующих правилу:
  - **Типы отсканированных файлов** Используйте эту опцию, чтобы указать, какие типы файлов вы хотите просканировать. Вы можете сканировать все файлы (независимо от их расширения), только файлы приложений или определенные типы файлов, которые вы считаете опасными. Сканирование всех файлов обеспечивает наилучшую защиту, в то время как сканирование только приложений рекомендуется для быстрого сканирования.

    Примечание
    Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 610).

    Если вы хотите сканировать файлы с определенными расширениями, у вас есть два варианта:
    - **Пользовательские расширения**, где вы должны указать только те расширения, которые будут проверяться.
    - **Все файлы, кроме определенных расширений**, где вы должны ввести только те расширения, которые будут пропущены при сканировании.
  - **Максимальный размер вложения / тела письма (MB).** Установите этот флажок и введите значение в соответствующем поле, чтобы установить максимально допустимый размер прикрепленного файла или тела сообщения электронной почты, которые будут проверяться.
  - **Максимальная глубина архива (уровней).** Установите флажок и выберите максимальную глубину архива из соответствующего поля. Чем ниже уровень глубины, тем выше производительность и ниже степень защиты.
  - **Сканирование на наличие потенциально нежелательных приложений(PUA).** Установите этот флажок, чтобы просканировать возможность проникновения вредоносных или нежелательных приложений, таких как программы показа рекламы, которые могут установиться на системах без согласия пользователя, изменить поведение различных программных продуктов и снизить производительность системы.
- **Действия** Вы можете указать различные автоматические действия агента безопасности для файлов, в зависимости от типа обнаружения.

Тип обнаружения делит файлы на три категории:

– **Зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ).
– **Подозрительные файлы.** Эти файлы опредеояются, как подозрительные с помощью эвристического анализа и других технологий Bitdefender. Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные).
– **Не сканируемые файлы** Эти файлы не могут быть просканированы. Это могут быть файлы защищенные паролем, зашифрованные, перепакованные и другие.

Для каждого типа обнаружения, вы можете выбрать действия по умолчанию или основные и альтернативные действия, если основные не выполняются. Хотя это и не рекомендуется, можно изменить эти действия в соответствующих меню. Выберите действие, которое будет принято:

– **Дезинфицировать** Удаляет вредоносный код из инфицированных файлов и восстанавливает исходный файл. В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.
– **Отклонить / удалить письмо.** На серверах с ролью пограничного транспорта (Edge Transport), обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.
– **Удалить файл** Удаляет проблемные вложения без предупреждения. Желательно избегать использование этого действия.
– **Заменить файл.** удаляет проблемные файлы и вставляет текстовый файл, который уведомляет пользователя о принятых мерах.
– **Переместить файл в карантин.** Перемещает обнаруженные файлы в карантин и вставляет текстовый файл, который уведомляет пользователя о принятых мерах. Файлы, помещенные в карантин,

не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице **Карантин**.

Примечание
Пожалуйста, обратите внимание, что карантин для серверов Exchange требует дополнительное дисковое пространство на разделе, где установлен агент безопасности. Размер карантина зависит от количества хранящихся элементов и их размера.

– **Не предпринимать никаких действий** Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования. По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин.
– По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других оставшихся правил. Если вы хотите продолжить проверку другими правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

7. Нажмите **Сохранить**, чтобы создать задачу сканирования. Появится окно подтверждения.
8. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Установить

Для защиты компьютеров с агентом безопасности Bitdefender, необходимо установить его на каждом из них.

Важно
В изолированных сетях, которые не имеют прямой связи с устройствами GravityZone, вы можете установить агента безопасности с ролью Роь ретранслятора В этом случае, связь между устройством GravityZone и другими агентами безопасности будет осуществляться через агента ретрансляции, который также будет выступать в качестве локального сервера обновлений для агентов безопасности, защищающих изолированную сеть.

После того, как вы установили агента ретрансляции, он будет автоматически обнаруживать незащищенные компьютеры в этой же сети.

Примечание

- Рекомендуется чтобы компьютер, на котором вы установите агента ретрансляции, был всегда включен.
- Если агент ретрансляции не установлен в сети, обнаружение незащищенных компьютеров может быть сделано вручную путем запуска задачи **Обнаружение сети**.

Защита Bitdefender может быть установлена на компьютерах удаленно из Control Center.

Удаленная установка выполняется в фоновом режиме, без ведома пользователя.

Предупреждение

Перед установкой, убедитесь, что на компьютере удалено существующее программное обеспечение для защиты от вредоносного ПО и брандмауэр. Установка защиты Bitdefender вместе с другим программным обеспечением безопасности может повлиять на работу и вызвать серьезные проблемы с системой. Защитник Windows и брандмауэр Windows будут отключены автоматически, когда начнется установка.

Если вы хотите развернуть агент безопасности на компьютере с Антивирусом Bitdefender для Mac 5. X, сначала необходимо удалить его вручную. Для инструкции для выполнения смотрите эту статью базы знаний.
При развертывании агента через Linux Relay должны выполняться следующие условия:

- На конечной точке с Relay ролью должен быть установлен пакет Samba (`smbclient`) версии 4.1.0 или выше и `net` binary/command для развертывания агентов на Windows.

  Примечание

  `net` binary/command обычно используется с samba-клиентом и/или стандартными пакетами samba. В некоторых дистрибутивах Linux (например CentOS 7.4) `net` command устанавливается только, когда установлен Samba Samba suite (Common + Client + Server). Убедитесь, что на конечной точке с Relay ролью доступна `net` command.

- Целевые конечные точки Windows должны иметь доступ к ресурсам администрирования и сети.
- В целевых конечных точках Linux и Mac должен быть включен SSH и отключен брандмауэр.

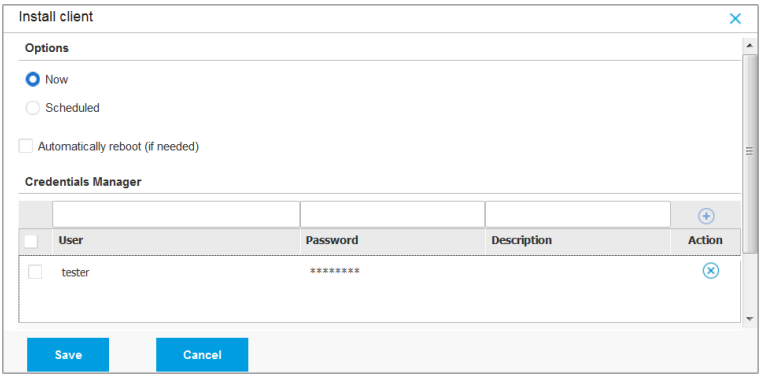
Чтобы запустить задачу удаленной установки:

1. Подключитесь и войдите в Control Center.
2. Перейдите в раздел **Сеть**.
3. Выберите **компьютеры и виртуальные машины** из меню видов сетей.
4. Выберите нужную группу в левой панели. Объекты, содержащиеся в выбранной группе, будут отображены в таблице правой панели.

   Примечание
   При желании, вы можете применять фильтры для отображения только неуправляемых конечных точек. Нажмите меню **Фильтры** и выберите следующие параметры: **Неуправляемые** на вкладке **Безопасность** и **Все предметы рекурсивно** на вкладке **Глубина**.

5. Выберите объекты (конечные точки или группы конечных точек), на которых вы хотите установить защиту.
6. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Установить**.

   Отобразится мастер установки **Install Client**.



Установка Bitdefender Endpoint Security Tools из меню задач

7. В разделе **Опции**, настройте время установки:
   - **Сейчас**, чтобы немедленно начать развертывание.
   - **Запланировано**, настроить интервал повторения развертывания. В этом случае, выберите желаемый интервал времени (ежечасно, ежедневно или еженедельно) и настройте его в соответствии с вашими потребностями.

   Примечание
   Например, когда некоторые операции требуется выполнить на нужной машине перед установкой клиента (например, удаление другого программного обеспечения и перезагрузки ОС), вы можете запланировать запуск задачи развертывания каждые 2 часа. Задача будет запускаться на каждом компьютере каждые 2 часа до тех пор, пока развертывание не будет завершено.

8. Если вы хотите, чтобы заданные конечные точки перезапустились после завершения установки, выберите **Автоматическая перезагрузка (при необходимости)** .
9. В разделе **Диспетчер учетных задач**, укажите учетные данные администратора, необходимые для удаленной аутентификации на заданных конечных точках. Вы можете добавить учетные данные, набрав имя пользователя и пароль, для каждой выбранной операционной системы.

Важно
Для станций под Windows 8.1, необходимо предоставить учетные данные встроенной учетной записи администратора или учетной записи администратора домена. Для получения подробной информации смотрите эту статью базы знаний.

Чтобы добавить необходимые учетные данные ОС:

a. Введите имя пользователя и пароль учетной записи администратора в соответствующих полях заголовка таблицы.

   Если компьютеры находятся в домене, достаточно ввести учетные данные администратора домена.

   Используйте правила именования Windows при вводе имени учетной записи:

   - Для машин из службы каталогов Active Directory используйте следующий синтаксис: `username@domain.com` и `domain\username`. Чтобы быть уверенным, что введенные учетные данные будут работать, добавьте их в обоих видах (`username@domain.com` и `domain\username`).
   - Для машин из рабочей группы достаточно ввести только имя пользователя без имени рабочей группы.

   При желании, вы можете добавить описание, которое поможет вам проще определить каждый аккаунт.

b. Нажмите кнопку ⊕ **Добавить**. Учетная запись будет добавлена в список учетных данных.

Примечание
Указанные учетные данные автоматически сохраняются в Менеджере учетных данных, так что вам не придется вводить их в следующий раз. Для доступа к диспетчеру учетных данных, просто укажите ваше имя пользователя в правом верхнем углу консоли.

Важно
Если предоставленные учетные данные являются недействительными, развертывание клиента на соответствующих конечных точках не произойдет. Не забудьте обновить учетные данные введенной ОС в диспетчере учетных данных, если они изменились на конечных точках.

10. Установите флажки на соответствующие аккаунты, которые вы хотите использовать.

Примечание
Предупреждающее сообщение будет отображаться до тех пор, пока вы не выберите какие-нибудь учетные данные. Этот шаг является обязательным для удаленной установки агента безопасности на конечных точках.

11. В разделе **Установщик**, выберите объект, к которому выбранные конечные точки будут подключаться для установки и обновления клиента:

- **GravityZone Appliance**, если конечные точки будут подключаться непосредственно к устройству GravityZone.

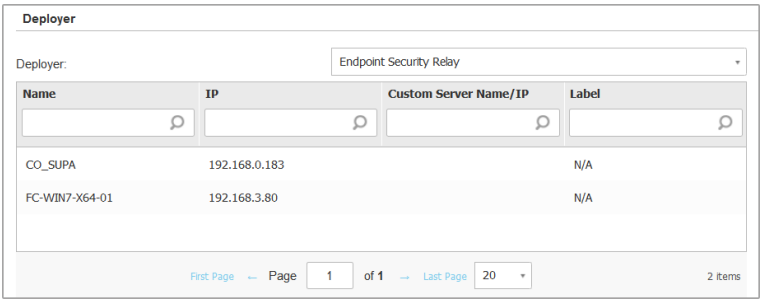
  В этом случае, вы также можете указать:

  – Пользовательский коммуникационный сервер, набрав его IP-адрес или имя хоста, в случае необходимости.

  – Настройки прокси-сервера, если требуемые конечные точки будут общаются с устройством GravityZone через прокси-сервер. В этом случае выберите **Использовать прокси для общения** и введите необходимые параметры прокси-сервера в полях ниже.

- **Ретранслятор безопасности конечной точки**, если вы хотите подключить конечные точки к клиенту Relay, установленному в вашей сети. Все машины с ролью ретранслятора, обнаруженные в вашей сети, будут отображены в таблице ниже. Выберите компьютер с ролью ретранслятора, который Вам нужен. Подключенные конечные точки будут сообщаться при помощи Control Center только через выбранный компьютер с ролью ретранслятора.

Важно
При развертывании через агента ретранслятора, должен быть открыт 7074 порт.



12. Используйте раздел **Дополнительные цели**, если вы хотите развернуть клиента на определенных машинах в вашей сети, которые не отображаются в сетевом содержимом. Раскройте раздел и введите через запятую IP-адреса или имена хостов этих машин в специальном поле. Вы можете добавить столько IP-адресов, сколько вам нужно.

13. Вы должны выбрать один установочный пакет для текущего развертывания. Нажмите на список **Использовать пакет** и выберите установочный пакет, который вам нужен. Вы можете найти здесь все инсталляционные пакеты, созданные ранее под вашей учетной записью, а также пакеты установки по умолчанию, доступные в Control Center.

14. При необходимости, вы можете изменить некоторые настройки выбранного пакета установки с помощью кнопки **Настроить**, рядом с полем **Использовать пакет**.

    Настройки инсталляционного пакета появятся ниже и вы сможете сделать необходимые изменения. Чтобы узнать больше о редактировании инсталляционных пакетов, обратитесь к руководству по установке GravityZone.

    Если вы хотите сохранить изменения как новый пакет, выберите опцию **Сохранить как пакет**, расположенную в нижней части списка параметров пакета, и введите имя для нового пакета установки.

15. Нажмите **Сохранить**. Появится окно подтверждения.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**.

Важно

При использовании VMware Horizon View Persona Management рекомендуется настроить групповую политику Active Directory, чтобы исключить следующие процессы Bitdefender (без полного пути):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Эти исключения должны применяться до тех пор, пока агент безопасности работает в конечной точке. Подробнее см. на этой странице документации VMware Horizon .

Клиент обновления

Эта задача доступна только тогда, когда агент Endpoint Security установлен и обнаружен в сети. Bitdefender рекомендует выполнить обновление с Endpoint Security до нового Bitdefender Endpoint Security Tools для защиты конечной точки последнего поколения.

Чтобы легко найти клиентов, которые не были обновлены, вы можете создать отчет о состоянии обновления. Для получения информации о том, как создать отчеты см. «Создание отчетов» (p. 534).

Удаление клиента

Для удаленного удаления защиты Bitdefender:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Выберите флажки на компьютерах, с которых вы хотите удалить агент безопасности Bitdefender.

5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Удалить клиента**.
6. Появится окно конфигурации, которое позволит вам сделать следующие настройки:
   - Вы можете выбрать хранение объектов карантина на клиентской машине.
   - Для интегрированной среды vShield, вы должны выбрать необходимые учетные данные для каждой машины, в противном случае удаление не произойдет. Выберите **Используйте учетные данные для интеграции vShield**, затем ниже проверьте все соответствующие учетные данные в таблице диспетчера учетных данных.
7. Нажмите **Сохранить**, чтобы создать задачу. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Примечание
Если вы хотите переустановить защиту, в первую очередь обязательно перезагрузите компьютер.

Обновление клиента

Периодически проверяйте статус управляемых компьютеров. Если вы заметили компьютер с проблемами безопасности, нажмите на его имя, чтобы отобразить страницу **Информация**. Для получения более подробной информации, обратитесь к «Статус безопасности» (p. 55).

Устаревшие клиенты или устаревшие механизмы защиты представляют проблемы безопасности. В этих случаях, вы должны запустить обновление на соответствующем компьютере. Эта задача может быть запущена локально с компьютера, или дистанционно с Control Center.

Для удаленного обновления клиента и механизмов защиты на управляемых компьютерах:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.

3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Установите флажки на компьютерах, на которых вы хотите запустить обновление клиента.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обновить**. Появится окно настроек.
6. Вы можете обновить только продукт, только механизмы защиты или всё сразу.
7. Для ОС Linux и машин, интегрированных с vShield, также является обязательным выбрать необходимые учетные данные. Проверьте опцию **Используйте учетные данные для интеграции Linux и vShieldn**, затем выберите соответствующие учетные данные из таблицы диспетчера учетных данных, которые отображаются ниже.
8. Нажмите **Обновить** для запуска задачи. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Перенастройка клиента

Модули защиты агента безопасности, роли и режимы сканирования изначально заданы в установочном пакете. После того как вы установили агента безопасности в вашей сети, вы можете в любое время изменить исходные настройки, отправив задачу перенастройки **Reconfigure Client** к требуемым управляемым конечным точкам.

Предупреждение
Пожалуйста, обратите внимание, что задача **Reconfigure Client** перезаписывает все параметры установки и ни одна из начальных настроек не сохраняется. Во время использования этой задачи, убедитесь, что перенастроили все настройки установки для требуемых конечных точек.

Примечание
Задача **Перенастроить клиента** удалит все неподдерживаемые модули из существующих установок в устаревшей Windows.

Параметры установки можно изменить в области **Сеть** или в отчете **Статус модулей конечных точек**.

Чтобы изменить настройки установки для одного или нескольких компьютеров:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемую группу в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Установите флажки компьютеров, для которых вы хотите изменить параметры установки.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Перенастроить клиента**.
6. Выберите одно из следующих действий:
   - **Добавить**. Добавьте новые модули к существующим.
   - **Удалить**. Удалить определенные модули из существующих.
   - **Список путей**. Подберите модули, установленные по вашему выбору.
7. Выберите модули и роли, которые вы собираетесь установить или удалить на целевых конечных точках.

   Предупреждение
   Будут установлены только поддерживаемые модули. Например, брандмауэр устанавливается только на поддерживаемые рабочие станции Windows. Дополнительную информацию смотрите в разделе Наличие уровней защиты GravityZone.

8. Выберите **Удалить конкурентов, если это необходимо**, чтобы убедиться, что выбранные модули не будут конфликтовать с другими решениями безопасности, установленными на целевых конечных точках.
9. Выберите один из доступных режимов сканирования:
   - **Автоматически**. Агент безопасности обнаруживает, какие механизмы сканирования подходят для ресурсов конечной точки.
   - **Custom**. Вы напрямую выбираете, какие механизмы сканирования использовать.

Для получения информации о доступных вариантах обратитесь к разделу Создание инсталляционных пакетов из Руководства по установке.

Примечание
Этот раздел доступен только для **Списка совпадений**.

10. В разделе **Планировщик** выберите время запуска задачи:
    - **Сейчас**, чтобы немедленно начать задачу.
    - **Запланировано**, чтобы настроить интервал повторяемости задачи.

      В этом случае выберите временной интервал (ежечасно, ежедневно или еженедельно) и настройте его в соответствии с вашими потребностями.
11. Нажмите **Сохранить**. Появится окно подтверждения.

    Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Обслуживание клиента

Используйте Repair Client task в качестве начальной задачи устранения неполадок для любого количества проблем, связанных с конечными точками. Задача загружает последний установочный пакет на целевую конечную точку, а затем выполняет переустановку агента.

Примечание
- The modules currently configured on the agent will not be changed.
- Задача восстановления сбросит агент безопасности до версии, опубликованной на странице **Configuration > Update > Components**.

Чтобы Repair Client task клиенту на ремонт:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.

4. Установите флажки на компьютерах, на которых Вы хотите запустить исправление клиента.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Исправление клиента**. Появится окно подтверждения.
6. Установите флажок **Японимаю и согласен** и нажмите кнопку **Сохранить**, чтобы запустить задачу.

Примечание
Для завершения задачи по восстановлению может потребоваться перезапуск клиента

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Перезагрузка машины

Вы можете удаленно перезагрузить управляемые компьютеры.

Примечание
Проверьте страницу **Сеть > Задачи** перед перезапуском определенных компьютеров. Ранее созданные задачи еще могут быть в процессе выполнения на выбранных компьютерах.

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Отметьте флажками компьютеры, которые вы хотите перезагрузить.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Перезагрузить машину**.
6. Выберите опции перезагрузки по расписанию:
   - Выберите **Перезапустить сейчас**, чтобы немедленно перезагрузить компьютеры.
   - Выберите **Включить перезагрузку** и используйте поля ниже, чтобы запланировать перезагрузку в определенную дату и время.

7. Нажмите **Сохранить**. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Сетевое Обнаружение

Обнаружение сети выполняется автоматически агентами безопасности с ролью ТРАНСЛЯТОР . Если у вас в сети нет агента ретрансляции, вам придется вручную запускать задачу сетевого обнаружения из защищенной конечной точки.

Чтобы запустить задачу сетевого обнаружения в вашей сети:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Отметьте флажком компьютер, на котором вы хотите выполнить сетевое обнаружение.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обнаружение сети**.
6. Появится окно подтверждения. Нажмите **Да**.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Обнаружение Приложений

Чтобы обнаружить приложения в вашей сети:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемую группу в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Выберите компьютеры, на которых необходимо выполнить обнаружение приложений.

5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обнаружение приложений**.

> **Примечание**
> Bitdefender Endpoint Security Tools с модулем Управления приложениями должен быть установлен и активирован на выбранных компьютерах. В противном случае, задача будет неактивна. Когда выбранная группа содержит и действительные, и недействительные объекты, задача будет отправлена только действительным конечным точкам.

6. Нажмите **Да** в окне подтверждения для продолжения.

Обнаруженные приложения и процессы отображаются на странице **Сеть > Инвентаризация приложений**. Для получения более подробной информации, обратитесь к «Инвентаризация Приложений» (p. 208).

> **Примечание**
> Задача **Обнаружение приложений** занимает некоторое время, в зависимости от количества установленных приложений. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Обновление Security Server

Установленные Security Server также можно просматривать и управлять в разделе **Компьютеры и виртуальные машины** из папки **Пользовательские группы**.

Если Security Server устарел, вы можете отправить ему задачу обновления:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите группу, где установлен Security Server.

   Чтобы легче найти Security Server, вы можете использовать меню **Фильтры** следующим образом:

   - Перейдите на вкладку **Безопасность** и выберите только **Серверы безопасности**.
   - Перейдите на вкладку **Глубина** и выберите **Все предметы рекурсивно**.

4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обновить Security Server**.
5. Вам нужно будет подтвердить ваши действия. Нажмите **Да**, чтобы создать задачу.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Важно
Рекомендуется использовать этот метод, чтобы обновить Security Server для NSX, в противном случае вы потеряете файлы карантина, сохраненные на устройстве.

Ввести Пользовательский инструмент

Примечание
Эта задача связана с модулем HVI, который может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Для ввода программных средств в гостевые операционные системы:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемую группу в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
4. Установите флажки для целевых конечных точек.
5. Нажмите в верхней части таблицы кнопку **Задачи** и выберите **Ввести инструмент пользователя** Появится окно конфигурации.
6. В раскрывающемся меню выберите все инструменты, которые хотите ввести. Для каждого выбранного инструмента будет отображаться раздел с настройками.

   Эти инструменты были ранее загружены в GravityZone. Если вы не можете найти нужный инструмент в списке, перейдите в раздел **Центр управления инструментами** и добавьте его оттуда. Для получения более подробной информации, обратитесь к «Ввод инструментов пользователя с HVI» (p. 574).

7. Для каждого инструмента, отображаемого в окне:
   a. Для того, чтобы просмотреть или скрыть раздел инструмента, нажмите на его название.
   b. Введите командную строку инструмента, вместе со всеми необходимыми входными параметрами, таким же образом, как это делается в командной строке. Например:

      ```
      bash script.sh <param1> <param2>
      ```

      Из двух раскрывающихся меню можно выбрать действие для восстановления и исправления резервной копии для средств восстановления Bitdefender.
   c. Укажите место, из которого Security Server должен собирать журналы:
      - **стандартный вывод** . Установите этот флажок, чтобы записывать журналы из стандартного выходного канала связи.
      - **Выходной файл**. Установите этот флажок, чтобы получать сохраненный на конечной точке файл журнала. В этом случае необходимо указать путь к месту, где Security Server может найти файл. Вы можете использовать абсолютный путь или системные переменные.

        Здесь находится дополнительная опция: **Удалить гостевые файлы журнала после их передачи**. Выберите его, если вам больше не потребуются файлы на конечной точке.
8. Если вы хотите перенести файл журналов из Security Server в другое место, необходимо указать путь к месту назначения и учетные данные аутентификации.
9. Для завершения работы инструмента может потребоваться больше предполагаемого времени или он может перестать отвечать на запросы. Во избежание сбоев в таких ситуациях, в разделе **Конфигурация безопасности** выберите, через сколько часов Security Server должен автоматически завершить процесс инструмента.
10. Нажмите **Сохранить**.

Статус задачи можно узнать на странице **Задачи**. Также для получения дополнительных сведений можно проверить отчет о **Статусе введения HVI Третьей стороны**.

6.2.6. Формирование быстрых отчетов

Вы можете создавать быстрые отчеты на управляемых компьютерах, используя страницу **Сеть**:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите требуемую группу в левой панели. Все компьютеры из выбранной группы отобразятся в таблице правой панели.

   При желании, вы можете отфильтровать содержимое выбранной группы только для управляемых компьютеров.
4. Отметьте флажками компьютеры, которые вы хотите включить в отчет.
5. Нажмите кнопку **Отчет** в верхней части таблицы и выберите из меню тип отчета.

   Для получения более подробной информации, обратитесь к «Отчеты по компьютерам и виртуальным машинам» (p. 513).
6. Настройте параметры отчета. Для получения более подробной информации, обратитесь к «Создание отчетов» (p. 534).
7. Нажмите **Создать**. Отчет отобразится немедленно.

   Время, необходимое для формирования отчетов, может изменяться в зависимости от количества выбранных компьютеров.

6.2.7. Назначение политик

Вы можете управлять настройками безопасности на компьютерах с помощью политики.

В разделе **Сеть** вы можете просматривать, изменять и назначать политики для каждого компьютера или группы компьютеров.

Примечание
Настройки безопасности доступны только для управляемых компьютеров. Для облегчения просмотра и управления настройками безопасности, вы можете отфильтровать сетевое содержимое только для управляемых компьютеров.

Для просмотра политики, назначенной определенному компьютеру:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемую группу в левой панели. Все компьютеры из выбранной группы отображаются в таблице правой панели.
4. Нажмите на имя управляемого компьютера, который вам необходим. Появится информационное окно.
5. На вкладке **Общее**, в разделе **Политика**, нажмите на название текущей политики, чтобы просмотреть ее настройки.
6. Вы можете изменить настройки безопасности в случае необходимости, при условии, что владелец политики позволил другим пользователям вносить в нее изменения. Пожалуйста, обратите внимание, что любое изменение, которое вы делаете, влияет на все компьютеры с такой же политикой.

   Для получения более подробной информации о настройках политик компьютера, обратитесь к «Политики компьютеров и виртуальных машин» (p. 254).

Чтобы назначить политику компьютеру или группе:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемую группу в левой панели. Все компьютеры из выбранной группы отображаются в таблице правой панели.
4. Отметьте флажком компьютер или группу, которую вы хотите выбрать. Вы можете выбрать один или несколько объектов одного типа, только одного уровня.
5. Нажмите кнопку **Назначить политику** в верхней части таблицы.

6. Сделайте необходимые настройки в окне **Назначение политики**. Для получения более подробной информации, обратитесь к «Назначение политик» (p. 241).

Использование Менеджер восстановления (Recovery Manager) для зашифрованных томов

Когда пользователи конечных точек забывают свои пароли шифрования и не могут больше получать доступ к зашифрованным томам на своих компьютерах, вы можете помочь им, получив ключи восстановления со страницы **Сеть**.

Чтобы получить ключ восстановления:

1. Перейдите в раздел **Сеть**.
2. Нажмите кнопку **Менеджер восстановления** на панели инструментов действий на панели слева. Появится новое окно.
3. В разделе окна **Идентификатор** введите следующие данные:
   a. Идентификатор ключа восстановления зашифрованного тома. Идентификатор ключа восстановления представляет собой строку цифр и букв, доступных в конечной точке на экране восстановления BitLocker.

      В Windows идентификатор ключа восстановления представляет собой строку цифр и букв, доступных на конечной точке на экране восстановления BitLocker.

      Кроме того, вы можете использовать параметр **Восстановление** на вкладке **Защита** в Сведениях о компьютере для автоматического ввода идентификатора ключа восстановления, для конечных точек как Windows так и macOS.

   b. Пароль вашей учетной записи GravityZone.
4. Нажмите **Открыть** . Окно расширяется.

   В разделе **Информация о томе** представлены следующие данные:

   a. Имя тома
   b. Тип тома (загрузочный или не загрузочный).
   c. Имя конечной точки (как указано в Инвентаризации сети)

d. Ключ восстановления. В Windows ключ восстановления - это пароль, автоматически генерируемый при шифровании тома. На Mac ключ восстановления - это пароль учетной записи пользователя.

5. Отправьте ключ восстановления пользователю конечной точки.

Подробнее о шифровании и дешифровке томов с помощью GravityZone см. «Шифрование» (p. 415).

6.2.9. Синхронизация со службой каталогов Active Directory

Сетевое содержимое автоматически синхронизируется с Active Directory через интервал времени, заданный в разделе конфигурации Control Center. Более подробную информацию см. в главе GravityZone по установке и настройке в руководстве по установке GravityZone

Чтобы вручную синхронизировать отображаемое в данный момент содержимое сети с Active Directory:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Нажмите кнопку **Синхронизировать с Active Directory** в верхней части таблицы.
4. Вы должны будете подтвердить ваши действия, нажав **Да**.

Примечание

Для больших сетей со службой каталогов Active Directory завершение синхронизации может занять больше времени.

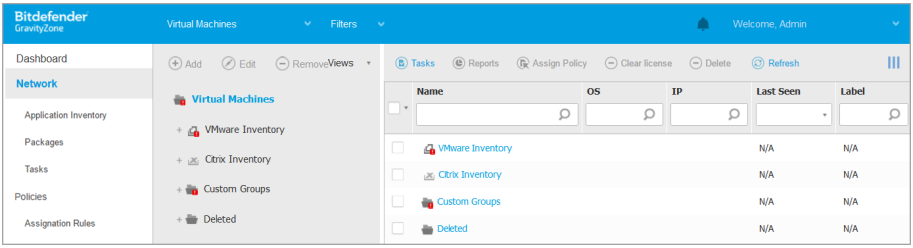
6.3. Виртуальные машины

Для просмотра виртуальной инфраструктуры под своей учетной записью, перейдите в раздел **Сеть** и выберите **Виртуальные машины** из меню видов сетей.

Примечание

Вы можете управлять виртуальными машинами также из **Компьютеры и виртуальные машины**, но просматривать виртуализированную инфраструктуру и фильтровать ее содержимое, используя специальные критерии, вы можете только используя вид **Виртуальные машины**.

За более подробной информацией о работе с видами сетей, обратитесь к «Виды сетей» (p. 49).



Сеть - Просмотр виртуальных машин

Вы можете увидеть доступные виртуальные машины в левой панели и детальную информацию о каждой виртуальной машине на панели справа.

Для настройки отображения детальной информации о виртуальных машинах в таблице:

1. Нажмите на кнопку **Колонки** в правой верхней части правой панели.
2. Выберите столбцы, которые вы хотите отобразить.
3. Нажмите кнопку **Восстановить**, чтобы вернуться к виду столбцов по умолчанию.

Левая панель отображает дерево каталогов виртуальной инфраструктуры. Корень дерева называется **Виртуальные машины** и виртуальные машины сгруппированы под корнем, в следующих категориях, основанных на технологии виртуализации поставщика:

- **Инвентаризация Nutanix .** Содержит список систем Nutanix Prism Element, к которым у вас есть доступ.
- **Содержимое VMware.** Содержит список серверов vCenter, к которым у вас есть доступ.
- **Содержимое Citrix.** Содержит список систем XenServer, к которым у вас есть доступ.
- **Пользовательские группы.** Содержит серверы безопасности и виртуальные машины, обнаруженные в вашей сети за пределами любого сервера vCenter или системы XenServer.

Левая панель также содержит вверху меню под названием **Виды**, из которого пользователь может выбрать тип представления для каждого поставщика технологии виртуализации.

Для доступа к виртуальной инфраструктуре, интегрированной с Control Center, вы должны указать пользовательские данные для каждого доступного vCenter Server. Единожды введя ваши учетные данные, они будут сохранены в вашем менеджере учетных данных и вам не придется вводить их повторно в дельнейшем. Для получения более подробной информации, обратитесь к «Диспетчер учетных данных (Credentials Manager)» (p. 233).

В разделе **Сеть**, вы можете управлять виртуальными машинами следующим образом:

- Проверять состояние виртуальных машин
- Просмотр сведений о виртуальной машине
- Организовывать виртуальные машины в группы
- Выполнить сортировку, фильтрацию и поиск
- Запустить задачи
- Сформировать быстрые отчеты
- Назначить политики
- Очистить лицензионные места

В разделе **Настройки > Настройки сети** вы можете настроить Запланированные правила для автоматической очистки неиспользованных виртуальных машин из инвентаризации сети.

6.3.1. Проверять статусы виртуальных машин

Каждая виртуальная машина представленая на странице сети, иконкой определенного типа и состояния.

Обратитесь к «Типы сетевых объектов и статусы» (p. 608), чтобы просмотреть список со всеми доступными типами значков и статусов.

Для получения подробной информации о статусе, обратитесь к:

- Состояние управления
- Состояние подключения
- Статус безопасности

Состояние управления

Виртуальные машины могут иметь следующие статусы управления:

- **Управляемые** - виртуальные машины, на которых установлена защита Bitdefender.
- **Ожидание перезапуска** - виртуальные машины, которые требуют перезагрузки системы после установки или обновления системы защиты Bitdefender.
- **Неуправляемые** - обнаруженные виртуальные машины, на которых защита Bitdefender еще не была установлена.
- **Удаленные** - виртуальные машины, которые вы удалили из Control Center. Для получения более подробной информации, обратитесь к «Удаление конечных точек из сетевого содержимого» (p. 228).

Состояние подключения

Состояние подключения относится к управляемым виртуальным машинам и Security Serveram. Следовательно, управляемые виртуальные машины могут быть:

- **Онлайн**. Синий значок означает, что компьютер находится в сети.
- **Оффлайн**. Серый значок означает, что компьютер находится в автономном режиме.

Виртуальная машина переходит в автономный режим, если агент безопасности неактивен более 5 минут. Причины, по которым виртуальные машины могут находится в автономном режиме:

- Виртуальная машина выключена, в режиме сна или гибернации.

  Примечание
  Виртуальные машины продолжают оставаться в статусе online, даже если они заблокированы или пользователь отключен.

- У агента безопасности нет подключения к коммуникационному серверуGravityZone:
  – Виртуальные машины могут быть отключены от сети.
  – Сетевой брандмауэр или маршрутизатор может блокировать связь между агентом безопасности и Bitdefender Control Center или назначенным Endpoint Security Relay.
  – Виртуальная машина находится за прокси-сервером и настройки прокси-сервера не были правильно настроены в примененной политике.

Предупреждение
Для виртуальных машин за прокси-серверером, настройки прокси-сервера должны быть правильно сконфигурированы в установочном пакете агента безопасности, в противном случае виртуальная машина не будет общаться с кансолью GravityZone и всегда будет появляться в автономном режиме, независимо от того, что политика с правильными настройками прокси была применена после установки.

- Агент безопасности удален вручную из виртуальной машины, в то время когда виртуальная машина не имела связи с Bitdefender Control Center или с назначенным Endpoint Security Relay. Обычно, когда агент безопасности вручную удален из виртуальной машины, Control Center уведомляет об этом событии, и виртуальная машина помечается как неуправляемая.
- Агент безопасности работает ненадлежащим образом.

Чтобы узнать, как долго виртуальные машины были неактивны:

1. Показывать только управляемые виртуальные машины. Нажмите меню **Фильтры** в верхней части таблицы, выберите все "Управляемые" варианты, которые вам нужны из вкладки **Безопасность**, выберите **Все предметы рекурсивно** из вкладки **Глубина** и нажмите **Сохранить**.
2. Щелкните на столбец **Последняя активность**, чтобы отсортировать виртуальные машины по периоду бездействия.

Вы можете игнорировать короткие периоды бездействия (минуты, часы), так как они, вероятно, являются результатом временного состояния. Например, виртуальные машины в настоящее время выключены.

Более длительные периоды бездействия (дни, недели), как правило, указывает на проблему с виртуальной машиной.

Примечание
Рекомендуется обновлять данные таблицы сети, время от времени, чтобы обновлять информацию о состоянии конечных точек.

Статус безопасности

Состояние безопасности относится к управляемым виртуальным машинам и Security Server. Вы можете определить виртуальные машины или Security

Serverы с проблемами безопасности, проверяя значки состояния, отображающие символ предупреждения:

- Имеются проблемы.
- Проблем не обнаружено.

Виртуальная машина или Security Server имеет проблемы с безопасностью, предусмотренные по крайней мере в одной из следующих ситуациях:

- Защита от вредоносных программ отключена (только для виртуальных машин).
- Срок действия лицензии истек.
- Продукт Bitdefender устарел.
- Механизмы защиты устарели.
- Дополнительный пакет HVI устарел.
- Обнаружено вредоносное ПО (только для виртуальных машин).
- Связь с Bitdefender Cloud Services не может быть установлена из-за следующих возможных причин:
  - Виртуальная машина имеет проблемы с подключением к Интернету.
  - Сетевой брандмауэр блокирует соединение с Bitdefender Cloud Services.
  - Порт 443, требующийся для связи с Bitdefender Cloud Services, закрыт.

  В этом случае защита от вредоносных программ полагается исключительно на локальный движок, в то время как сканирование в облаке выключено, это означает, что агент безопасности не может обеспечить полную защиту в режиме реального времени.

Если вы заметили виртуальную машину с проблемами безопасности, нажмите на ее имя, чтобы отобразить окно **Информация**. Вы можете определить проблемы безопасности по значку !. Убедитесь, что вы проверили информацию о безопасности на всех вкладках информационных страниц. Наведите курсор мыши на значок, чтобы отобразить подсказку, содержащую подробности. Могут потребоваться дальнейшие локальные расслдеования.

Примечание

Рекомендуется обновлять данные таблицы сети, время от времени, чтобы обновлять информацию о состоянии конечных точек.

Конечные точки, которые не получают обновлений в течение последних 24 часов, автоматически помечаются как **Содержит угрозы**, независимо от версии содержимого безопасности, присутствующей на ретрансляторе или в GravityZone Update Server.

6.3.2. Просмотр подробной информации о виртуальной машине

Подробные сведения о каждой виртуальной машине можно узнать на странице **Сеть** следующим образом:

- Проверка **Сеть** страница
- Проверка **Информация** окно

Проверка страницы сети

Для того, чтобы узнать подробную информацию о виртуальной машине, проверьте информацию в таблице правой панели на странице **Сеть**.

Чтобы добавить или удалить столбцы с информацией о виртуальной машине, нажмите кнопку **Столбцы** в правой верхней части панели.

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемую группу в левой панели.

   Все виртуальные машины, доступные в выбранной группе, отображаются в правой панели таблицы.
4. Вы можете легко определить состояние виртуальной машины, проверив соответствующий значок. Для получения дополнительной информации перейдите к «Проверять статусы виртуальных машин» (p. 118).
5. Проверьте информацию, отображаемую в столбцах для каждой виртуальной машины.

   Используйте строку заголовка для поиска определенных виртуальных машин в соответствии с доступными критериями:

   - **Имя**: имя виртуальной машины.
   - **FQDN**: полное доменное имя, которое включает в себя имя хоста и имя домена.
   - **OS**: операционная система установленая на виртуальной машине.
   - **IP**: IP-адрес виртуальной машины.
   - **Последняя активность**: дата и время, когда виртуальная машина была в последний раз онлайн.

Примечание
Важно следить за полем **последняя активность**, длительные периоды бездействия могут указывать на проблему связи или отключенную виртуальную машину.

- **Ярлык** : настраиваемая строка с дополнительной информацией о рабочей станции. Можете добавить метку в **Окно** Информации виртуальной машины и затем использовать ее в поиске.
- **Политика**: политика, применяемая к виртуальной машине, содержит ссылку для просмотра или изменения параметров политики.

Проверка информационного окна

Для того, чтобы отобразить окно **Сведения**, щелкните имя интересующей вас виртуальной машины в правой боковой панели страницы **Сеть**. В этом окне отображаются сгруппированные по нескольким вкладкам данные, которые доступны только для выбранной виртуальной машины.

В окне **Информация** приведен полный список сведений в соответствии с типом виртуальной машины (виртуальная машина, экземпляр Security Server) и информация о ее безопасности.

Вкладка "Общие"

- Основная информация о виртуальной машине, например, имя, информация FQDN, IP-адрес, операционная система, инфраструктура, родительская группа и текущее состояние.

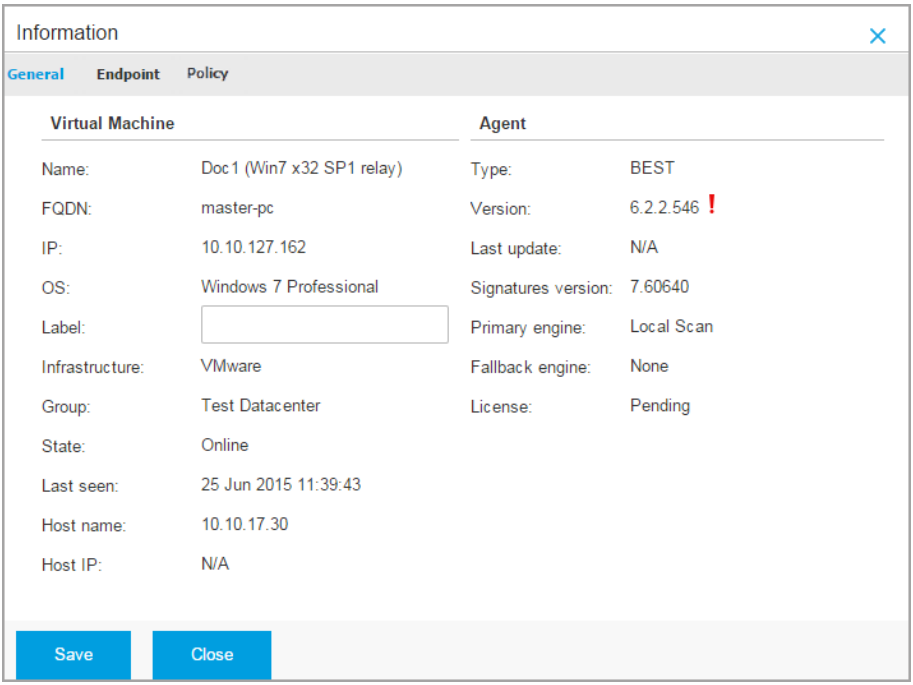
  В этом разделе вы можете поставить метку к виртуальной машине. Вы сможете быстро находить виртуальные машины с одной и той же меткой и принимать меры по отношению к ним, независимо от их расположения в сети. Для получения дополнительных сведений о фильтрации виртуальной машины перейдите к «Сортировка, фильтрация и поиск виртуальных машин» (p. 133).
- **Предварительные требования HVI**, содержащие информацию о том, можно ли использовать Security Server для развертывания защиты HVI или нет. Таким образом, если хост Security Server работает на поддерживаемой версии XenServer и дополнительный пакет установлен, вы можете включить HVI на виртуальных машинах на этом хосте.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

- Сведения об уровнях защиты, в том числе список технологий безопасности, приобретенных при помощи решения GravityZone, и статус их лицензии, которые могут быть:
  - **Доступен/Активный** - на виртуальной машине активен лицензионный ключ для данного уровня защиты.
  - **Истек срок действия** — истек срок действия лицензионного ключа для данного уровня защиты.
  - **Ожидание подтверждения** — лицензионный ключ еще не подтвержден.

    Примечание
    Дополнительная информация об уровнях защиты доступна на вкладке **Защита** .

- **Подключение ретрансляции**: имя, IP-адрес и метка ретранслятора, к которому подключена виртуальная машина.



Информационное окно - вкладка «Общие»

Вкладка "Защита"

Эта вкладка содержит сведения о каждом уровне защиты, лицензированном на конечной точке. Подробности содержат информацию о:

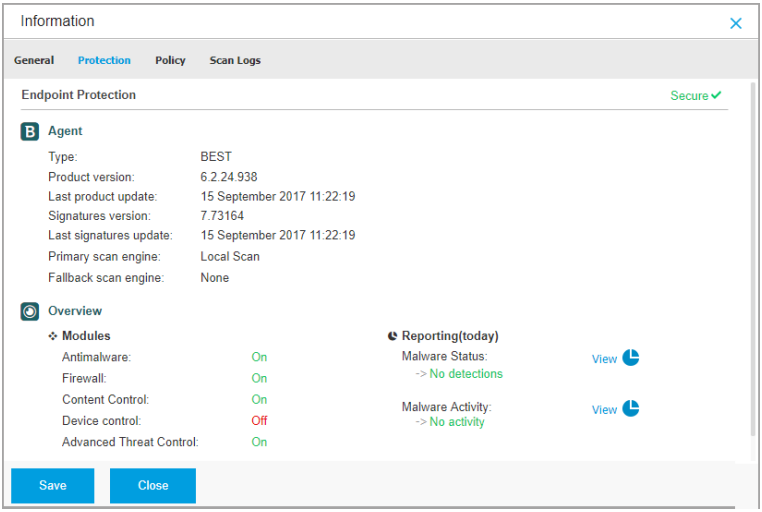
- Сведения о агентах безопасности, такие как название и версия продукта, конфигурация и состояние сканирования механизмов сканирования. Для Exchange Protection также доступны версии антиспама и версии сигнатур.
- Состояние безопасности для каждого уровня защиты. Этот статус отображается в правой части имени уровня защиты:
  - **Безопасный**, если на конечных точках, применяемых с уровнем защиты, не обнаружены проблемы безопасности.
  - **Уязвимый**, если на конечных точках, применяемых с уровнем защиты, обнаружены проблемы безопасности. Дополнительные сведения см. в разделе «Статус безопасности» (p. 120).

- Связанный Security Server. Каждый назначенный Security Server отображается в случае развертывания без агентов или при сканировании антивирусных механизмов безопасности, настроенных для использования удаленного сканирования. Информация Security Server помогает идентифицировать виртуальное устройство и получить статус его обновления.
- Информация, связанная с NSX, такая как статус тега вируса и группа безопасности, к которой принадлежит виртуальная машина. Если тег безопасности был применен, это сообщает о том, что машина заражена. В противном случае, машина чиста или же не использует тег безопасности.
- Статусы модулей защиты. Вы можете легко просмотреть, какие модули защиты были установлены на конечной точке, а также статус доступных модулей (**Вкл. / Выкл.**), установленных с помощью применяемой политики.
- Краткий обзор активности модулей и отчетов о вредоносном ПО за текущий день.

  Нажмите ссылку **Просмотр**, чтобы получить доступ к параметрам отчета, а затем Создать отчет. Для получения более подробной информации, обратитесь к «Создание отчетов» (p. 534)
- Информация, касающаяся слоя защиты Sandbox Analyzer:
  - Статус использования Sandbox Analyzer на виртуальной машине отображается с правой стороны окна:
    - **Активный**: Sandbox Analyzer лицензирован (доступен) и включен через политику на виртуальной машине.
    - **Неактивный**: Sandbox Analyzer лицензирован (доступен), но не включен через политику на виртуальной машине.
  - Название агента, который действует как датчик подачи.
  - Состояние модуля на виртуальной машине:
    - **Включен** - Sandbox Analyzer включен на виртуальной машине с помощью политики.
    - **Выключен** - Sandbox Analyzer не включен с помощью политики на виртуальной машине.
  - Чтобы просмотреть угрозы обнаруженные на прошлой неделе, просмотрите отчет перейдя по ссылке **Просмотреть** .

- Дополнительная информация о модуле шифрования, например:
  - Обнаруженные тома (с указанием загрузочного диска).
  - Состояние шифрования для каждого тома (**Зашифрован**, **Выполняется шифрование**, **Выполняется дешифрование**, **Незашифрован**, **Заблокирован** или **Приостановлен**).

    Нажмите ссылку **Восстановление** , чтобы получить ключ восстановления для соответствующего зашифрованного тома. Подробнее о получении ключей восстановления см. «Использование Менеджер восстановления (Recovery Manager) для зашифрованных томов» (p. 179).



Информационное окно - вкладка "Защита"

Для Security Servers данная вкладка содержит информацию о модуле "Защита Хранилища". Подробности содержат информацию о:

- Статус сервиса:
  - **N/A** - Защита Хранилища лицензирована, но служба еще не настроена.
  - **Включено** - служба включена в политику и работает.
  - **Отключено** - служба не работает либо потому, что она отключена из политики, либо срок действия лицензионного ключа истек.

- Список подключенных ICAP-совместимых устройств хранения со следующими данными:
  - Имя устройства хранения
  - IP-адрес устройства хранения
  - Тип устройства хранения
  - The date and time of the last communication between the storage device and Security Server.

Вкладка "Политика"

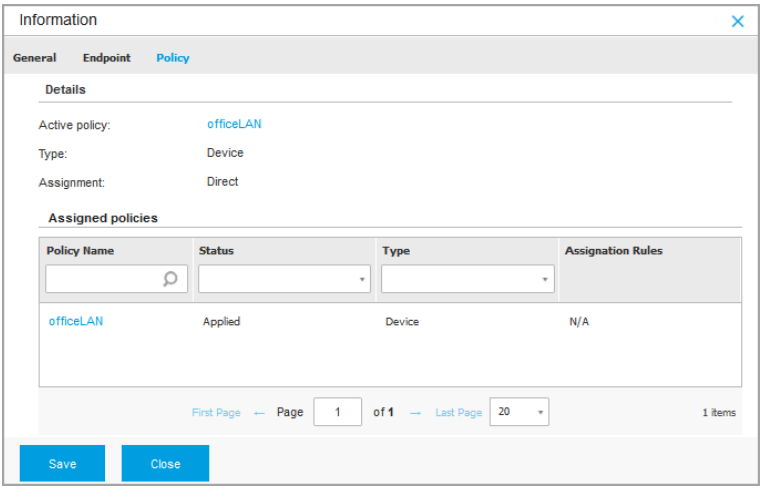
Виртуальная машина может применяться с одной или несколькими политиками, но одна политика может быть активна только с одной виртуальной машиной. Сведения о всех политиках, применяемых к виртуальной машине, отображены на вкладке **Политика**.

- Имя активной политики. Нажмите на название политики, чтобы открыть шаблон политики и просмотреть ее настройки.
- Тип активной политики, который может быть:
  - **Устройство**: если сетевым администратором вручную назначена политика для виртуальной машины.
  - **Местоположение**: политика, основываясь на правилах, автоматически назначается виртуальной машине в том случае, если сетевые настройки конечной точки соответствуют заданным условиям правил назначения .
  - **Пользователь**: политика, основываясь на правилах, автоматически назначается конечной точке в том случае, если она соответствует цели Active Directory, указанной в правиле назначения.

    Например, машине может быть назначено две политики, зависящие от пользователя, одна для администраторов и одна для других сотрудников. Одна из политик становится активной, в зависимости от прав пользователя зашедшего на машину.
  - **Внешний (NSX)**: если политика определена в среде VMware NSX.
- Тип назначения активной политики, который может быть:
  - **Прямой**: если политика применяется непосредственно к виртуальной машине.

– **Наследственный**: если виртуальная машина наследует политику родительской группы.

- **Применимые политики**: отображает список политик, связанных с существующими правилами назначения. Эти политики могут применяться к виртуальной машине, если она соответствует заданным условиям правил назначения.

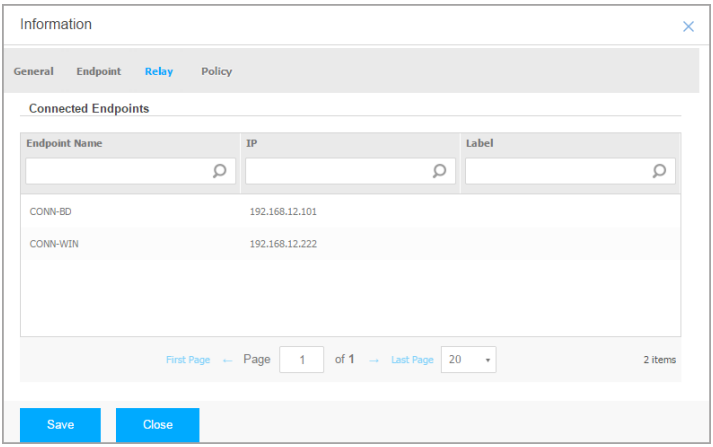


Информационное окно - вкладка «Политика»

Для получения дополнительной информации, касающейся политики, см.«Управление политиками» (p. 238)

Вкладка «Ретранслятор»

Вкладка **Ретранслятор** доступна только для виртуальных машин с ролями ретранслятора. Эта вкладка отображает информацию о конечных точках, подключенных к текущему ретранслятору, такую как имя, IP-адрес и метка.



Информационное окно - вкладка «Ретранслятор»

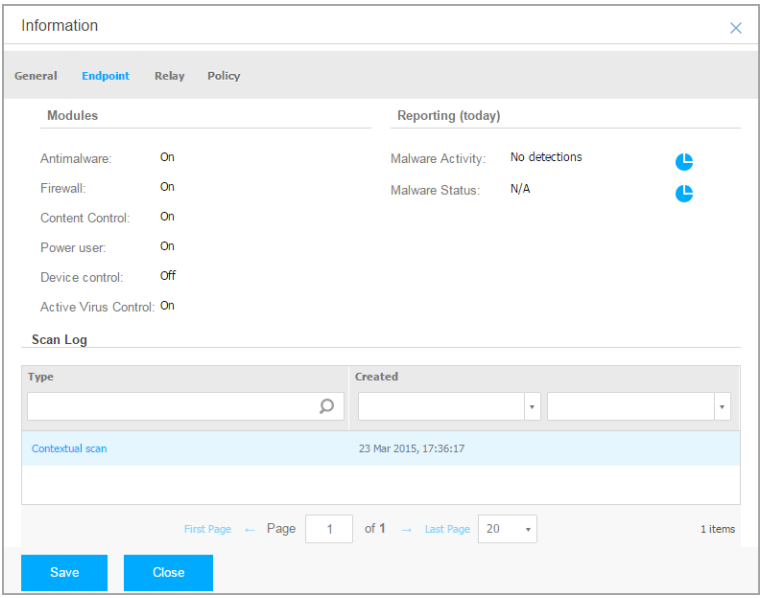
Вкладка "Журналы сканирования"

Таблица **Сканирование журнаов** выводит подробные сведения обо всех задачах сканирования, выполненных на виртуальной машине.

Журналы сгруппированы по уровню защиты, и вы можете выбрать в выпадающем списке, для какого уровня отображать журналы.

Выберите нужную задачу сканирования, и журнал откроется на новой странице браузера.

Если доступно много журналов сканирования, они могут занимать несколько страниц. Для перемещения по страницам используйте кнопки навигации в нижней части таблицы. Если доступно слишком много записей, вы можете использовать опции фильтрации, доступные в верхней части таблицы.



Информационное окно - вкладка «Журналы сканирования»

Каждое свойство , которое создает проблемы безопасности в этом окне помечено значком **!** . Наведите мышь на значок для появления подсказки, чтобы выяснить подробности. Могут потребоваться дальнейшие локальные расслдеования.

6.3.3. Организация виртуальных машин в группы

Вы можете управлять группами виртуальных машин в левой панели раздела **Сеть** из папки **Пользовательские группы**.

Виртуальные машины, импортированные из Nutanix Prism Element, сгруппированы в папке **Инвентаризация Nutanix**. Виртуальные машины, импортированные из VMware vCenter сгруппированы в папке **VMware Inventory**. Виртуальные машины, импортированные из XenServer сгруппированы в папке **Citrix Inventory**. Вы не можете редактировать Инвентаризацию Nutanix, Инвентаризацию VMware или Инвентаризацию Citrix. Вы можете только просматривать и управлять соответствующими виртуальными машинами.

Все виртуальные машины, которые не управляются системами Nutanix Prism, vCenter или XenServer, определяются Network Discovery и помещаются в **Пользовательские группы**, где вы можете организовать их в группы по своему усмотрению. Основным преимуществом этой возможности является то, что вы можете использовать групповые политики для решения различных требований безопасности.

В **Пользовательские группы** вы можете создавать, удалять, переименовывать и перемещать группы виртуальных машин, создавая требуемую древовидную структуру.

Примечание

- Группа может содержать как виртуальные машины, так и другие группы.
- При выборе группы в левой панели, вы можете просмотреть все виртуальные машины кроме тех, которые находятся в своих подгруппах. Для просмотра всех виртуальных машин, входящих в группу и в дочерние подгруппы, нажмите меню **Фильтры**, расположенное в верхней части таблицы и выберите **Все элементы рекурсивно** в разделе **Глубина**.

Создание групп

Прежде чем начать создавать группы, подумайте о причине создания, зачем они вам нужны и продумайте схему группировки. Например, вы можете сгруппировать виртуальные машины на основе одного или нескольких следующих критериев:

- Организационная структура (продажи, маркетинг, контроль качества, разработка программного обеспечения, управление и т.д.).
- Требования безопасности (настольные компьютеры, ноутбуки, сервера и т.д.).
- Местонахождение (штаб, местные офисы, удаленные сотрудники, домашние офисы и т.д.).

Для организации вашей сети в группы:

1. Выберите **Пользовательские группы** в левой панели.
2. Нажмите кнопку ⊕ **Добавить группу** в верхней части левой панели.
3. Введите подходящее имя группы и нажмите **OK**. Появится новая группа в **Пользовательские группы**.

Переименование групп

Чтобы переименовать группу:

1. Выберите группу в левой панели.
2. Нажмите кнопку **Редактировать группу** в верхней части левой панели.
3. Введите новое имя в соответствующем поле.
4. Нажмите **OK** для подтверждения.

Перемещение групп и виртуальных машин

Вы можете перемещать объекты в любое расположение внутри иерархии **Пользовательские группы**. Для перемещения объекта, перетащите его из правой панели в желаемую группу левой панели.

Примечание

Объект, который перемещается, наследует параметры политик новой родительской группы, если наследование не было запрещено или другая политика не была непосредственно применена к нему. Для получения более подробной информации о наследовании политик, обратитесь к «Политики безопасности (Security Policies)» (p. 237).

Удаление групп

Группа не может быть удалена, если она содержит по меньшей мере одну виртуальную машину. Переместите все виртуальные машины из группы, которую вы хотите удалить, в другую группу. Если группа включает в себя подгруппы, вы можете выбрать для перемещения все подгруппы, а не отдельные виртуальные машины.

Чтобы удалить группу:

1. Выберите пустую группу.
2. Нажмите кнопку **Удалить группу** в верхней части левой панели. Вы должны будете подтвердить ваши действия, нажав **Да**.

6.3.4. Сортировка, фильтрация и поиск виртуальных машин

В зависимости от количества виртуальных машин, правая панель может занимать несколько страниц (всего по умолчанию отображается 20 записей на каждой странице). Для перемещения по страницам используйте кнопки

навигации в нижней части таблицы. Чтобы изменить количество записей отображаемых на странице, введите другое значение в поле рядом с кнопками навигации.

Если записей слишком много, вы можете использовать поля поиска под заголовками столбцов или меню **Фильтры** в верхней части страницы, чтобы отобразить только те объекты, которые вам необходимы. Например, вы можете искать определенную виртуальную машину или выбрать для просмотра только управляемые виртуальные машины.

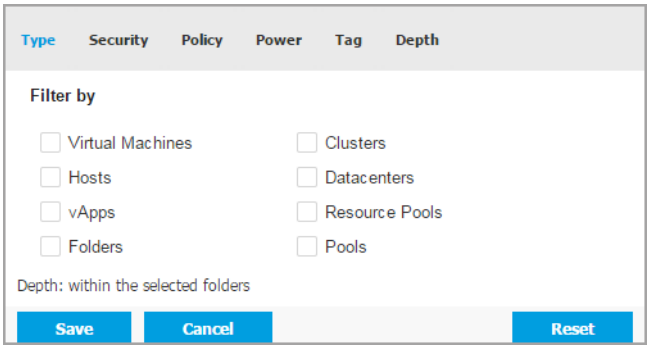
Сортировка виртуальных машин

Для сортировки данных по определенному столбцу, щелкните заголовок столбца. Например, если вы хотите отсортировать виртуальные машины по имени, щелкните на заголовок **Имя**. При повторном нажатии на заголовок виртуальные машины будут отображаться в обратной последовательности.

Сортировка компьютеров

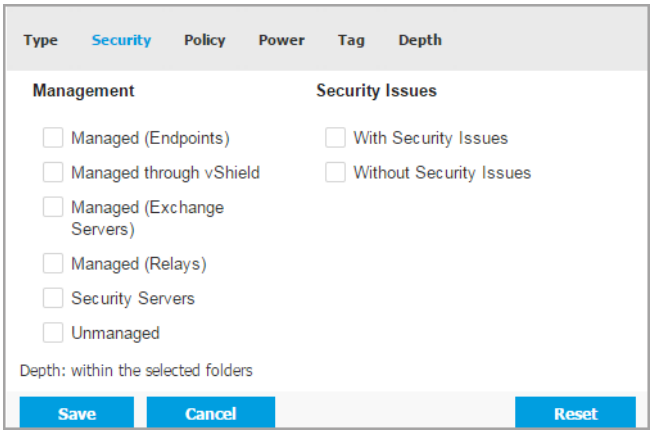
Фильтрация виртуальных машин

1. Выберите желаемую группу из левой панели.
2. Нажмите меню **фильтры** в правой верхней части сетевой панели.
3. Вы можете использовать следующие критерии фильтрации:
   - **Тип**. Выберите тип виртуальных объектов, которые будут отображаться.



Виртуальные машины - Фильтрация по типу

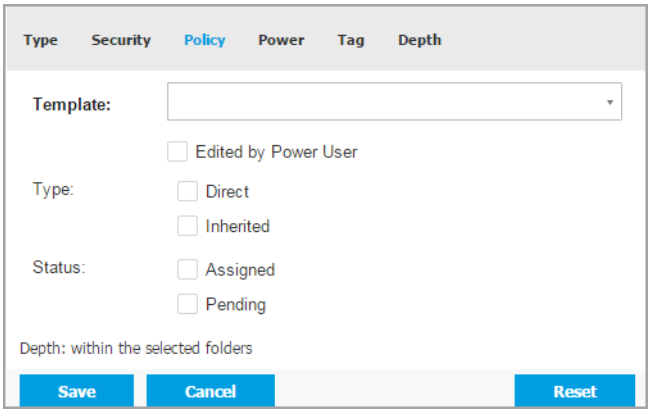
- **Безопасность**. Выберите управление защитой и/или статус безопасности, чтобы по ним отфильтровать сетевые объекты. Например, вы можете выбрать для просмотра только машины Security Server, или вы можете просматривать только конечные точки с проблемами безопасности.



Виртуальные машины - Фильтрация по безопасности

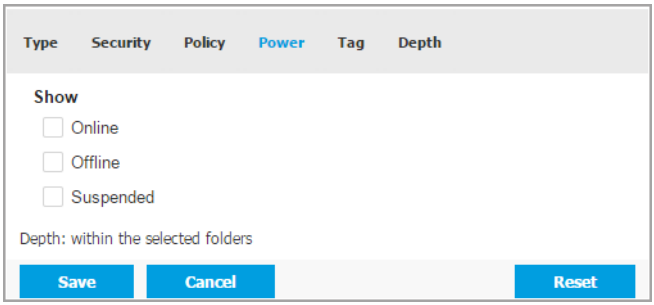
- **Политика**. Выберите шаблон политики, для которого нужно фильтровать виртуальные машины, тип назначения политики (прямой или

наследуемый), а также статус назначения политики (активный, применяемый или в ожидании).



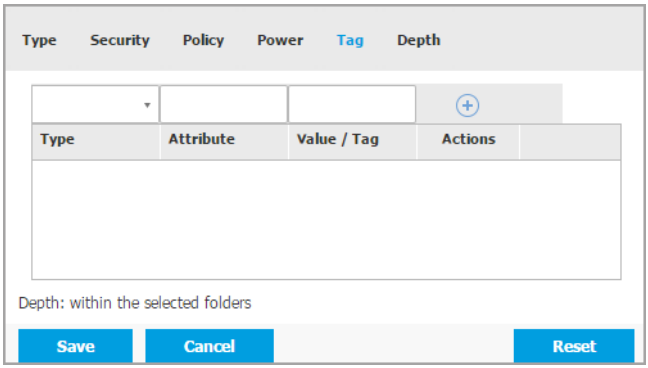
Виртуальные машины - Фильтрация по политикам

- **Питание**. Вы можете выбрать отображение виртуальных машин в режимах онлайн, офлайн и ожидания.



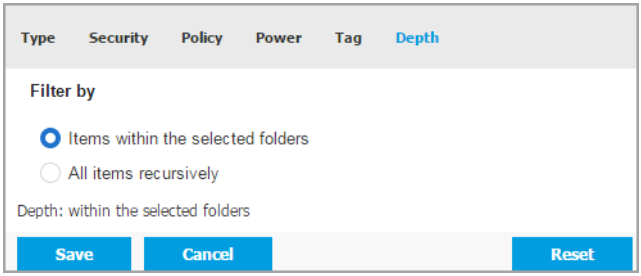
Виртуальные машины - Фильтрация по питанию

- **Метки**. Вы можете выбрать фильтрацию виртуальных машин с помощью тегов и атрибутов, которые вы определили в вашей среде виртуализации.



Виртуальные машины - Фильтрация по тэгам

- **Глубина**. При управлении деревом сетевой структуры виртуальных машин, виртуальные машины, размещенные в подгруппах, не отображаются по умолчанию. Выберите **Все предметы рекурсивно**, чтобы просмотреть все виртуальные машины, входящие в текущую группу и все подгруппы.



Виртуальные машины - Фильтрация по глубине

Примечание
Нажмите **Сбросить**, чтобы очистить фильтры и отобразить все виртуальные машины.

4. Нажмите **Сохранить**, чтобы отфильтровать виртуальные машины по выбранным критериям.

Поиск виртуальных машин

1. Выберите нужный контейнер в левой панели.
2. Введите слово для поиска в соответствующем поле под заголовками столбцов (Имя, ОС или IP) в правой панели. Например, введите IP-адрес виртуальной машины, которую вы ищете, в поле **IP**. Только соответствующая виртуальная машина появится в таблице.

   Очистите окно поиска, чтобы отобразить полный список виртуальных машин.

6.3.5. Запуск задач на виртуальных машинах

В разделе **Сеть**, вы можете удаленно запускать ряд администраторских задач на виртуальных машинах.

Вы можете выполнить следующие задачи:

- «СКАНИРОВАТЬ» (p. 139)
- «Задачи патчей» (p. 150)
- «Сканирование Exchange» (p. 153)
- «Установить» (p. 157)
- «Удаление клиента» (p. 163)
- «Обновления» (p. 163)
- «Перенастройка клиента» (p. 164)
- «Сетевое Обнаружение» (p. 166)
- «Обнаружение Приложений» (p. 167)
- «Перезагрузка машины» (p. 167)
- «Установка Security Server» (p. 168)
- «Удаление Security Server» (p. 171)
- «Обновление Security Server» (p. 171)
- «Установка дополнительного пакета HVI» (p. 172)
- «Удалите дополнительный пакет HVI» (p. 173)
- «Обновление дополнительного пакета HVI» (p. 174)

Вы можете создавать задачи отдельно для каждой виртуальной машины или для групп виртуальных машин. Например, вы можете удаленно установить Bitdefender Endpoint Security Tools на группу неуправляемых виртуальных машин. Позже, вы можете создать задачу сканирования определенной виртуальной машины в той же группе.

Для каждой виртуальной машины, вы можете запускать только совместимые задачи. Например, если вы выберите неуправляемую виртуальную машину, вы можете выбрать только установку агента безопасности, все другие задачи будут недоступы.

Для группы выбранная задача будет создана только для совместимых виртуальных машин. Если ни одна из виртуальных машин в группе не совместима с выбранной задачей, вы будете уведомлены, что задача не может быть создана.

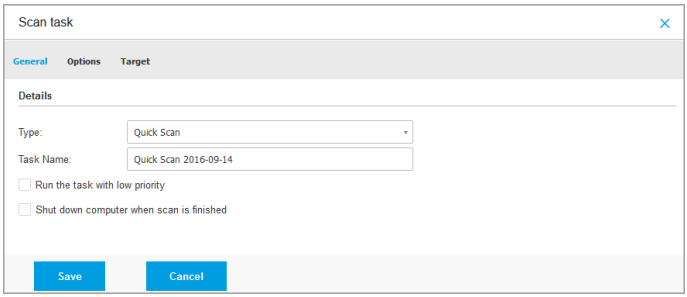
После создания, задача запустится сразу же, когда виртуальные машины будут онлайн. Если компьютер находится в автономном режиме, задание начнет выполняться, как только он подключится к Интернету.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

СКАНИРОВАТЬ

Для удаленного запуска задачи сканирования на одной или нескольких виртуальных машинах:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты, содержащиеся в выбранной группе, выводятся в таблице правой панели.
4. Отметьте флажками соответствующие объекты, которые вы хотите просканировать.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Сканировать**. Появится окно настроек.
6. Настройте параметры сканирования:
   - На вкладке **Общее** вы можете выбрать тип сканирования и ввести имя для задачи проверки. Имя задачи сканирования предназначено, чтобы помочь вам легче определить текущее сканирование на странице **Задачи**.



Задача сканирования виртуальных машин - Настройка общих параметров

Выберите тип сканирования из меню **Тип**:

– **Быстрое сканирование** предварительно сконфигурировано для сканирования только важных системных местоположений и новых файлов. Быстрое сканирование занимает, как правило, менее минуты. Быстрое сканирование использует лишь незначительную часть системных ресурсов, в отличие от процесса стандартного антивирусного сканирования.

  Bitdefender автоматически переходит к обезвреживанию, если обнаружены вредоносные программы или руткиты. Если по какой-либо причине файл нельзя вылечить, он перемещается в карантин. Этот тип сканирования игнорирует подозрительные файлы.

– **Полное сканирование** проверяет всю систему на все типы вредоносных программ, угрожающих безопасности, таких как вирусы, программы-шпионы, рекламное ПО, руткиты и другие.

  Bitdefender автоматически пытается обезвреживать файлы, обнаруженные вредоносными программами. Если вредоносная программа не может быть удалена, она перемещвется в карантин, где она не может навредить. Подозрительные файлы игнорируются. Если вы хотите принять меры и в отношении подозрительных файлов, или если вы хотите выполнить другие действия по умолчанию для зараженных файлов, выберите вариант «Запуск пользовательского сканирования».

– **Сканирование памяти** проверяет программы, запущенные в памяти виртуальной машины.

– **Сканирование сети** тип пользовательского сканирования, позволяющий сканировать сетевые диски, используя агента безопасности Bitdefender, установленного на выбранной виртуальной машине.

  Для выполнения задачи сетевого сканирования:

  - Вам необходимо назначить задачу для одной конечной точки в сети.
  - Для агента безопасности вам необходимо ввести учетные данные пользователя с правами чтения/записи для выбранных сетевых дисков, чтобы иметь возможность получить доступ и выполнить требуемые действия на этих сетевых дисках. Необходимые учетные данные могут быть сконфигурированы на вкладке **Цель** окна задач.

– **Выборочное сканирование** позволяет выбирать места сканирования и настраивать параметры сканирования.

Для выборочного сканирования, сканирования памяти и сети, вы можете выбрать следующие опции:

– **Выполнить задачу с низким приоритетом**. Установите этот флажок для снижения приоритета процесса сканирования, чтобы другие программы смогли работать быстрее. При это может увеличится время, необходимое для завершения процесса сканирования.

  Примечание
  Эта опция применима только к Bitdefender Endpoint Security Tools и Endpoint Security (устаревший агент)

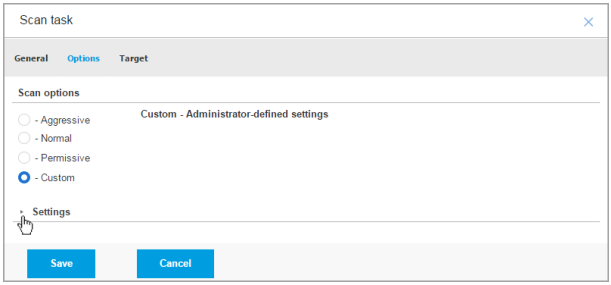
– **Выключить компьютер после завершения сканирования** Установите этот флажок, чтобы выключить машину, если вы не собираетесь использовать ее некоторое время.

  Примечание
  Эта опция применима к Bitdefender Endpoint Security Tools, Endpoint Security (устаревший агент) и Endpoint Security for Mac.

Для пользовательского сканирования (Custom Scan) настройте следующие параметры:

– Перейдите на вкладку **Опции**, чтобы установить параметры сканирования. Выберите уровень безопасности, который лучше всего соответствует вашим потребностям (Интенсивный, Нормальный или Рекомендуемый). Используйте описания справа от шкалы, которые помогут сделать выбор.

  В зависимости от выбранного профиля, параметры сканирования в разделе **Настройки** будут сконфигурированы автоматически. Тем не менее, при желании, вы можете настроить их более детально. Чтобы сделать это, выберите опцию **Пользователь** и затем раскройте раздел **Настройки**.



Задания по сканированию виртуальных машин - Настройка пользовательского режима сканирования

Доступны следующие опции:

- **Типы файлов.** Используйте данную настройку, чтобы задать типы файлов, которые вы хотите просканировать. Вы можете указать агенту безопасности просканировать все файлы (независимо от их расширений), только файлы приложений или специфические типы файлов, которые вы считаете потенциально опасными. При сканировании всех файлов обеспечивается оптимальная защита. Сканируя только приложения, можно повысить скорость сканирования.

  Примечание

  Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 610).

Если вы хотите просканировать только специфические типы файлов, выберите в меню **Пользовательские расширения** и затем введите желаемые расширения в редактируемом поле, нажимая `войти` после каждого расширения.

Важно
Агенты безопасности Bitdefender устанавливаются в операционных системах Windows и Linux, сканируют большинство .ISO форматов, но не предпринимают никаких действий над ними.

Настройка заданий по сканированию виртуальных машин - Добавление пользовательских расширений

- **Архивы.** Архивы, содержащие инфицированные файлы, не представляют непосредственной угрозы безопасности системы. Вредоносные программы могут повлиять на систему только если зараженный файл извлечен из архива и будет исполнен при выключенной защите в реальном времени. Тем не менее, рекомендуется сканировать архивы для обнаружения и удаления любой потенциальной угрозы, даже не представляющей собой непосредственной угрозы системе.

  Важно
  Сканирование файлов, сжатых в архив, увеличивает общее время сканирования и занимает больший объем системных ресурсов.

  – **Сканирование внутри архивов.** Выберите эту опцию, если вы хотите проверить заархивированные файлы на наличие вредоносных программ. Если вы решили использовать данную опцию, вам необходимо настроить следующие параметры оптимизации:

- **Ограничение размера архива (Мб).** Вы можете установить максимально допустимый размер архивов для сканирования. Поставьте флажок в соответствующем поле и введите максимальный размер архива (в МБ).
- **Максимальная глубина архива (уровни).** Отметьте соответствующий флажок и выберите в меню максимальную глубину архива. Для лучшей производительности выберите наименьшее значение, для максимальной защиты выберите наибольшее значение.

– **Сканировать архивы электронной почты.** Выберите данную опцию если хотите разрешить проверку почтовых сообщений и почтовых баз, включая такие форматы файлов как .eml, .msg, .pst, .dbx, .mbx, .tbb и другие.

Важно
Процесс сканирования почтовых архивов является достаточно ресурсоемким и может повлиять на производительность системы.

- **Разное.** Выберите соответствующие флажки, чтобы включить нужные параметры сканирования.

– **Сканирование загрузочных секторов.** Проверка загрузочных секторов системы. Этот сектор жесткого диска содержит код виртуальной машины необходимый для запуска процесса загрузки. Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.

– **Сканирование реестра.** Выберите этот параметр для сканирования ключей реестра. Реестр Windows — это база данных, в которой хранятся настройки и параметры конфигурации для компонентов операционной системы Windows и установленных приложений.

– **Сканирование на наличие руткитов.** Выберите этот параметр для сканирования на наличие руткитов и объектов, скрытых с помощью такого программного обеспечения.

- **Сканирование на наличие клавиатурных шпионов.** Выберите данную опцию для сканирования системы на наличие клавиатурных шпионов. По своей природе кейлогеры не являются вредоносным ПО, но они могут быть использованы злоумышленниками. В украденных данных хакер может найти личную информацию, такую как номера банковских счетов и пароли, и использовать ее в личных целях.
- **Сканирование памяти.** Выберите этот параметр для сканирования программ, запущенных в системной памяти.
- **Сканирование файлов cookie.** Выберите эту опцию для сканирования cookies-файлов, сохраненных браузерами на компьютере.
- **Сканирование только новых/измененных файлов.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие системы с минимальными потерями в безопасности.
- **Сканирование на наличие потенциально нежелательных приложений (PUA).** Потенциально нежелательные приложения (PUA) это программы, которые могут быть нежелательными для ПК, а иногда и поставляться в комплекте с программным обеспечением бесплатного. Такие программы могут быть установлены без согласия (также называются рекламными) или включены по умолчанию в комплект экспресс-установки (как дополнение). Потенциальное воздействие этих программ заключается в показе всплывающих окон, установке нежелательных панелей инструментов в браузере по умолчанию или работе нескольких процессов в фоновом режиме, что замедляет производительность компьютера.
- **Сканирование съемных носителей.** Выберите этот параметр для сканирования любых съемных накопителей, подключаемых к компьютеру.

• **Действия.** В зависимости от типа обнаруженного файла автоматически выполняются следующие действия:

- **Действие при обнаружении зараженного файла.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры

вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ). Агент безопасности Bitdefender может удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция известна как лечение.

Если зараженный файл обнаружен, агент безопасности Bitdefender автоматически попытается его вылечить. Если файл не удается вылечить, он перемещается в карантин в целях предотвращения распространения вируса.

Важно
В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. В таких случаях выполняется удаление зараженного файла с диска.

– **Действие при обнаружении подозрительного файла.** Для обнаружения подозрительных файлов Bitdefender использует Эвристический анализ и другие технологии . Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные). Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.

  По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин. Помещенные в карантин файлы отправляются на анализ в лабораторию Bitdefender на регулярной основе. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить.

– **Когда найден руткит.** Руткиты представляют собой специализированное программное обеспечение, используемое для того, чтобы скрыть файлы операционной системы. Однако, руткиты часто используются, чтобы скрыть вредоносные программы, либо для сокрытия присутствия злоумышленника в системе.

Обнаруженные руткиты и скрытые файлы по умолчанию игнорируются.

При обнаружении вируса на виртуальной машине NSX, Security Server автоматически помечает виртуальную машину меткой (тегом) безопасности, при условии, что эта опция была выбрана при интеграции сервера vCenter.

Для этих целей NSX может содержать три метки безопасности, в зависимости от серьезности угрозы:

- `ANTI_VIRUS.VirusFound.threat=low`, применяется к машине, когда Bitdefender находит вредоносное ПО с низким уровнем риска, которое он может удалить.
- `ANTI_VIRUS.VirusFound.threat=medium`, применяется к машине, если Bitdefender не может удалить инфицированный файл, но вместо этого пытается вылечить его.
- `ANTI_VIRUS.VirusFound.threat=high`, применяется к машине, если Bitdefender не может ни удалить, ни вылечить зараженные файлы, но блокирует доступ к ним.

Вы можете изолировать зараженные машины путем создания групп безопасности с динамическим членством на основе тегов безопасности.

Важно

- Если Bitdefender найдет на машине угрозы с различными уровнями сложности, то применит соответствующие метки.
- Тег безопасности удаляется на машине только после выполнения полного сканирования и дезинфекции машины.

Хотя это и не рекомендуется, вы можете изменить действие по умолчанию. Можно задать дополнительное действие, которое будет выполнено в случае, если не удалось выполнить первое, а также различные действия для каждой из категорий. Выберите в соответствующих меню первое и второе действие, которые будут выполняться в отношении всех типов обнаруженных файлов. Доступны следующие действия:

Лечить

Удаляет вредоносный код из зараженных файлов. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов.

Перемещение файлов в карантин

Перемещает зараженные файлы из исходного расположения в папку карантина. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице консоли Quarantine.

Удалить

Удаляет обнаруженные файлы с диска без предупреждения. Желательно избегать использование этого действия.

Пропустить

Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования.

– Перейдите на вкладку **Цель**, чтобы настроить расположения, которые вы хотите просканировать на требуемых виртуальных машинах.

  В разделе **Сканирование цели** вы можете добавить новый файл или папку, которые необходимо проверить:

  a. Выберите предопределенное месторасположение из выпадающего меню или введите конкретные пути в **конкретные пути**, которые вы хотите просканировать.

  b. Укажите путь к объекту для сканирования в поле редактирования.

  - Если вы выбрали предопределенное место, необходимо корректно завершить путь. Например, для сканирования всей папки `Програмные файлы`, достаточно выбрать соответствующее предопределенное место из выпадающего меню. Для сканирования конкретной папки из `Програмные файлы`, необходимо завершить путь, добавив обратную косую черту (\) и имя папки.

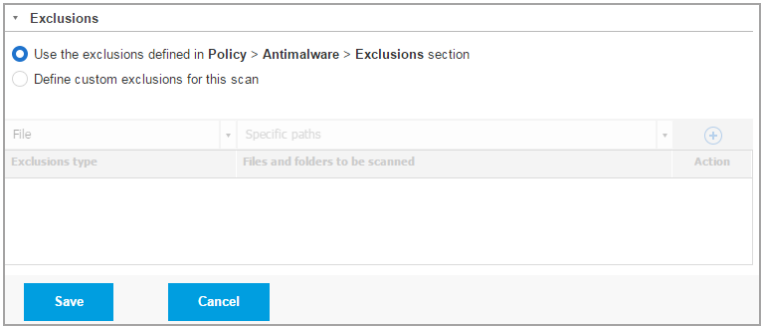
- Если вы выбрали **Конкретные пути**, введите полный путь к объекту проверки. Желательно использовать системные переменные (в определенных случаях), чтобы убедиться, что путь действителен для всех выбранных виртуальных машин. Для получения более подробной информации о системных переменных, обратитесь к «Системные переменные» (p. 611).

c. Нажмите соответствующую кнопку ⊕ **Добавить**.

Чтобы изменить существующий путь, нажмите на него. Чтобы удалить папку из списка, нажмите соответствующую кнопку ⊗ **Удалить**.

Для агента безопасности вам необходимо ввести учетные данные пользователя с правами чтения/записи для выбранных сетевых дисков, чтобы иметь возможность получить доступ и выполнить требуемые действия на этих сетевых дисках.

Нажмите на раздел **Исключения**, если вы хотите добавить исключения.



Задание по сканированию виртуальных машин - Определение исключений

Вы можете либо использовать исключения определенные политикой, либо определить явные исключения для текущей задачи сканирования. За более подробной информацией об исключениях, обратитесь к «Исключения» (p. 312).

7. Нажмите **Сохранить**, чтобы создать задачу сканирования. Появится окно подтверждения.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Примечание
Чтобы запланировать задание сканирования, перейдите на страницу **Политики**, выберите политику, назначенную виртуальным машинам, и добавьте задачу проверки в раздел **Защита от вредоносных программ > По требованию**. Для получения более подробной информации, обратитесь к «Сканирование по запросу (On-Demand)» (p. 290).

Задачи патчей

Рекомендуется регулярно проверять обновления ПО и применять их как можно скорее. GravityZone автоматизирует этот процесс с помощью политик безопасности, но если вам нужно сразу обновить программное обеспечение на определенных виртуальных машинах, выполните следующие задачи в следующем порядке:

1. Сканирование патча
2. Установка патча

Требования к системе

- Агент безопасности с модулем управления исправлениями устанавливается на конечных точках.
- Для успешного выполнения задач сканирования и установки конечные точки Windows должны соответствовать следующим условиям:
  - **Доверенные корневые центры сертификации** хранит **Сертификат корневого ЦС DigiCert Assured ID**.
  - **Промежуточные центры сертификации** включает в себя **центр сертификации подписанного кода DigiCert SHA2**.
  - На конечных точках установлены исправления для Windows 7 и Windows Server 2008 R2, упомянутые в этой статье Microsoft: Рекомендации по безопасности Microsoft 3033929

Сканирование патча

Виртуальные машины с устаревшим программным обеспечением уязвимы для атак. Рекомендуется регулярно проверять и устанавливать обновление ПО на конечных точках. Чтобы проверить виртуальные машины на наличие неустановленных исправлений:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
4. Выберите целевые конечные точки
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Сканировать исправления**. Появится окно подтверждения.
6. Нажмите **Да** чтобы подтвердить задачу сканирования

   Когда задача заканчивается, GravityZone добавляет в Инвентарь исправлений все исправления, необходимые для вашего программного обеспечения. Дополнительные сведения см. в разделе «Инвентаризация патча» (p. 214).

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Примечание
Чтобы запланировать сканирование исправлений, измените политики, назначенные целевым конечным точкам, и настройте параметры в разделе **Управление исправлениями**. Для получения более подробной информации, обратитесь к «Управление исправлениями» (p. 363).

Установка патча

Чтобы установить одно или несколько исправлений на целевые виртуальные машины:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.

4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Установить исправления**.

   Появится окно настроек. Здесь вы можете просмотреть все исправления, отсутствующие на целевых виртуальных машинах.

5. При необходимости используйте параметры сортировки и фильтрации в верхней части таблицы, чтобы найти конкретные исправления.

6. Нажмите кнопку **Столбцы** в верхней правой части панели, чтобы просмотреть только соответствующую информацию.

7. Выберите исправления, которое вы хотите установить.

   Некоторые исправления зависят от других В таком случае они автоматически выбираются один раз вместе с исправлением.

   При нажатии на номера **CVE** или **Продукты** отобразится панель с левой стороны. Панель содержит дополнительную информацию, такую как CVE, которые исправляет исправление, или продукты, к которым применяется исправление. Как только прочитаете, нажмите **Закрыть**, чтобы скрыть панель.

8. Выберите **Перезагрузить конечные точки после установки исправления, если необходимо**, чтобы перезапустить конечные точки сразу после установки исправления, если требуется перезагрузка системы. Учтите, что это действие может прервать сеанс пользователя.

9. Щелкните **Установить**.

   Задача установки создается вместе с подзадачами для каждой целевой виртуальной машины.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Примечание

- Чтобы запланировать установку исправлений, измените политики, назначенные целевым машинам, и настройте параметры в разделе **Управление исправлениями**. Для получения более подробной информации, обратитесь к «Управление исправлениями» (p. 363).
- Вы также можете установить исправление со страницы **Инвентарь исправлений**, начиная с определенного интересующего вас исправления. В этом случае выберите исправление из списка, нажмите кнопку **Установить**

в верхней части таблицы и настройте параметры установки исправления. Дополнительные сведения см. в разделе «Установка патчей» (p. 218).

- После установки исправления мы рекомендуем отправить задачу Сканировать исправления конечным точкам. Это действие обновит информацию об исправлении, сохраненную в GravityZone для ваших управляемых сетей.

Вы можете удалить исправления:

- Удаленно, отправив из GravityZone Задача удаления исправлений.
- Локально на машине. В этом случае вам необходимо войти в систему как администратор конечной точки и запустить деинсталлятор вручную.

Сканирование Exchange

Вы можете удаленно сканировать базу данных сервера Exchange, запустив задачу **Exchange Scan**.

Для того, чтобы сканировать базу данных Exchange, необходимо включить сканирование по запросу, указав учетные данные администратора Exchange. Для получения более подробной информации, обратитесь к «Сканирование хранилища Exchange» (p. 391).

Для сканирования базы данных сервера Exchange:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. В левой панели, выберите группу, содержащую нужный сервер Exchange. Желаемый сервер вы можете выбрать в правой панели.

   Примечание
   При желании, вы можете использовать фильтры, чтобы быстро найти нужный сервер:
   - Нажмите меню **Фильтры** и выберите следующие параметры: **Управляемый (Exchange Servers)** на вкладке **Безопасность** и **Все пункты рекурсивно** на вкладке **Глубина**.
   - Введите имя сервера или IP-адрес в нужном поле под заголовком соответствующего столбца.

4. Отметьте флажком сервер Exchange, базу данных которого вы хотите проверить.

5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Exchange Scan**. Появится окно настроек.
6. Настройте параметры сканирования:
   - **Общее** Введите подходящее имя задачи.

     Для больших баз данных задача сканирования может занимать много времени и может повлиять на производительность сервера. В таких случаях, установите флажок **Остановите сканирование, если это займет больше времени, чем** и выбрать подходящий интервал времени в соответствующем меню.
   - **Цель** Выберите контейнеры и объекты, которые будут проверяться. Вы можете выбрать для сканирования: почтовые ящики, общие папки или и то, и другое. Кроме электронной почты, вы можете выбрать для сканирования другие объекты, такие, как **Контакты**, **Задачи**, **Фурнитура** и **Опубликовать элементы**. Кроме того, вы можете установить следующие ограничения на содержимое, которое будет проверяться:
     – Только непрочитанные сообщения
     – Только элементы с вложениями
     – Только новое, полученное в указанный промежуток времени

     Например, вы можете выбрать для сканирования только письма почтовых пользователей, принятые за последние семь дней.

     Выберите флажок **Исключения**, если вы хотите определить исключения при сканировании. Чтобы создать исключение, используйте поля из заголовков таблицы следующим образом:
     a. Выберите тип репозитория из меню.
     b. В зависимости от типа хранилища укажите объекты, которые должны быть исключены:

Тип хранилища	Формат объекта
Почтовый ящик	Адрес электронной почты
Общая папка	Путь к папке, начиная с корня каталога
База данных	Идентификатор базы данных

Примечание
Для получения идентификатора базы данных, используйте команду оболочки Exchange:
`Get-MailboxDatabase | fl name,identity`

Вы можете ввести только одну команду за один раз. Если у вас есть несколько объектов одного типа, вы должны задать столько правил, сколько элементов.

c. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы сохранить исключение и добавить его в список.

Чтобы удалить правило исключения из списка, нажмите соответствующую кнопку ⊖ **Удалить**.

- **Параметры** Настройте параметры сканирования для сообщений электронной почты, соответствующих правилу:
  - **Типы отсканированных файлов** Используйте эту опцию, чтобы указать, какие типы файлов вы хотите просканировать. Вы можете сканировать все файлы (независимо от их расширения), только файлы приложений или определенные типы файлов, которые вы считаете опасными. Сканирование всех файлов обеспечивает наилучшую защиту, в то время как сканирование только приложений рекомендуется для быстрого сканирования.

    Примечание
    Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 610).

    Если вы хотите сканировать файлы с определенными расширениями, у вас есть два варианта:
    - **Пользовательские расширения**, где вы должны указать только те расширения, которые будут проверяться.
    - **Все файлы, кроме определенных расширений**, где вы должны ввести только те расширения, которые будут пропущены при сканировании.
  - **Максимальный размер вложения / тела письма (MB).** Установите этот флажок и введите значение в соответствующем поле, чтобы установить максимально допустимый размер прикрепленного файла или тела сообщения электронной почты, которые будут проверяться.
  - **Максимальная глубина архива (уровней).** Установите флажок и выберите максимальную глубину архива из соответствующего поля. Чем ниже уровень глубины, тем выше производительность и ниже степень защиты.
  - **Сканирование на наличие потенциально нежелательных приложений(PUA).** Установите этот флажок, чтобы просканировать

возможность проникновения вредоносных или нежелательных приложений, таких как программы показа рекламы, которые могут установиться на системах без согласия пользователя, изменить поведение различных программных продуктов и снизить производительность системы.

- **Действия** Вы можете указать различные автоматические действия агента безопасности для файлов, в зависимости от типа обнаружения.

  Тип обнаружения делит файлы на три категории:
  - **Зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ).
  - **Подозрительные файлы.** Эти файлы опредеояются, как подозрительные с помощью эвристического анализа и других технологий Bitdefender. Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные).
  - **Не сканируемые файлы** Эти файлы не могут быть просканированы. Это могут быть файлы защищенные паролем, зашифрованные, перепакованные и другие.

  Для каждого типа обнаружения, вы можете выбрать действия по умолчанию или основные и альтернативные действия, если основные не выполняются. Хотя это и не рекомендуется, можно изменить эти действия в соответствующих меню. Выберите действие, которое будет принято:
  - **Дезинфицировать** Удаляет вредоносный код из инфицированных файлов и восстанавливает исходный файл. В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.
  - **Отклонить / удалить письмо.** На серверах с ролью пограничного транспорта (Edge Transport), обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.

- **Удалить файл** Удаляет проблемные вложения без предупреждения. Желательно избегать использование этого действия.
- **Заменить файл.** удаляет проблемные файлы и вставляет текстовый файл, который уведомляет пользователя о принятых мерах.
- **Переместить файл в карантин.** Перемещает обнаруженные файлы в карантин и вставляет текстовый файл, который уведомляет пользователя о принятых мерах. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице **Карантин**.

  Примечание
  Пожалуйста, обратите внимание, что карантин для серверов Exchange требует дополнительное дисковое пространство на разделе, где установлен агент безопасности. Размер карантина зависит от количества хранящихся элементов и их размера.

- **Не предпринимать никаких действий** Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования. По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин.
- По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других оставшихся правил. Если вы хотите продолжить проверку другими правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

7. Нажмите **Сохранить**, чтобы создать задачу сканирования. Появится окно подтверждения.
8. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Установить

Чтобы защитить ваши виртуальные машины с помощью Security for Virtualized Environments, необходимо установить агентов безопасности Bitdefender на каждой из них. Агент безопасности Bitdefender управляет защитой на виртуальных машинах. Он также общается с Control Center, чтобы принимать

команды администратора и отправлять результаты своих действий. После того, как вы подключите агента безопасности Bitdefender к сети, он будет автоматически обнаруживать незащищенные виртуальные машины в этой сети. Затем защита Security for Virtualized Environments может быть установлена на этих виртуальных машинах удаленно из Control Center. Удаленная установка выполняется в фоновом режиме, без ведома пользователя.

В изолированных сетях, которые не имеют прямой связи с устройствами GravityZone, вы можете установить агента безопасности с ролью Роь ретранслятора В этом случае, связь между устройством GravityZone и другими агентами безопасности будет осуществляться через агента ретрансляции, который также будет выступать в качестве локального сервера обновлений для агентов безопасности, защищающих изолированную сеть.

Примечание
Рекомендуется, чтобы виртуальная машина, на которой вы установите агента ретрансляции, была всегда включена.

Предупреждение
Перед установкой убедитесь, что удалили существующее программное обеспечение для защиты от вредоносного ПО и брандмауэр на виртуальной машине. Установка защиты Bitdefender вместе с другим программным обеспечением безопасности может повлиять на работу и вызвать серьезные проблемы с системой. Защитник Windows и брандмауэр Windows будут отключены автоматически, когда начнется установка.

Для удаленной установки защиты Security for Virtualized Environments на одной или нескольких виртуальных машинах:

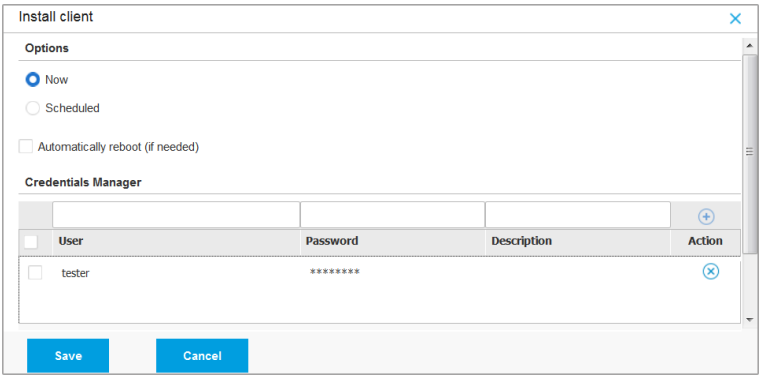
1. Подключитесь и войдите в Control Center.
2. Перейдите в раздел **Сеть**.
3. Выберите **Виртуальные машины** из меню видов сетей.
4. Выберите желаемый контейнер в левой панели. Объекты, содержащиеся в выбранной группе, будут отображены в таблице правой панели.

   Примечание
   При желании, вы можете применять фильтры для отображения только неуправляемых виртуальных машин. Нажмите меню **Фильтры** и выберите

следующие параметры: **Неуправляемые** на вкладке **Безопасность** и **Все предметы рекурсивно** на вкладке **Глубина**.

5. Выберите объекты (виртуальные машины, хосты, кластеры или группы), на которых вы хотите установить защиту.
6. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Установить > BEST**.

   Отобразится мастер установки **Install Client**.



Установка Bitdefender Endpoint Security Tools из меню задач

7. В разделе **Опции**, настройте время установки:
   - **Сейчас**, чтобы немедленно начать развертывание.
   - **Запланировано**, настроить интервал повторения развертывания. В этом случае, выберите желаемый интервал времени (ежечасно, ежедневно или еженедельно) и настройте его в соответствии с вашими потребностями.

   Примечание
   Например, когда некоторые операции требуется выполнить на нужной машине перед установкой клиента (например, удаление другого программного обеспечения и перезагрузки ОС), вы можете запланировать запуск задачи развертывания каждые 2 часа. Задача будет запускаться на каждом компьютере каждые 2 часа до тех пор, пока развертывание не будет завершено.

8. Если вы хотите, чтобы заданные конечные точки перезапустились после завершения установки, выберите **Автоматическая перезагрузка (при необходимости)** .
9. В разделе **Диспетчер учетных задач**, укажите учетные данные администратора, необходимые для удаленной аутентификации на заданных конечных точках. Вы можете добавить учетные данные, набрав имя пользователя и пароль, для каждой выбранной операционной системы.

Важно
Для станций под Windows 8.1, необходимо предоставить учетные данные встроенной учетной записи администратора или учетной записи администратора домена. Для получения подробной информации смотрите эту статью базы знаний.

Примечание
Предупреждающее сообщение будет отображаться до тех пор, пока вы не выберите какие-нибудь учетные данные. Этот шаг является обязательным для удаленной установки Bitdefender Endpoint Security Tools на конечных точках.

Чтобы добавить необходимые учетные данные ОС:

a. Введите имя пользователя и пароль учетной записи администратора для каждой выбранной операционной системы в соответствующих полях заголовков таблицы. При желании, вы можете добавить описание, которое поможет вам проще определить каждый аккаунт.

   Если виртуальные машины находятся в домене, достаточно ввести учетные данные администратора домена.

   Используйте правила именования Windows при вводе имени учетной записи:

   - Для машин из службы каталогов Active Directory используйте следующий синтаксис: `username@domain.com` и `domain\username`. Чтобы быть уверенным, что введенные учетные данные будут работать, добавьте их в обоих видах (`username@domain.com` и `domain\username`).
   - Для машин из рабочей группы достаточно ввести только имя пользователя без имени рабочей группы.

b. Нажмите кнопку ⊕ **Добавить**. Учетная запись будет добавлена в список учетных данных.

Примечание
Указанные учетные данные автоматически сохраняются в Менеджере учетных данных, так что вам не придется вводить их в следующий раз. Для доступа к диспетчеру учетных данных, просто укажите ваше имя пользователя в правом верхнем углу консоли.

Важно
Если предоставленные учетные данные являются недействительными, развертывание клиента на соответствующих конечных точках не произойдет. Не забудьте обновить учетные данные введенной ОС в диспетчере учетных данных, если они изменились на конечных точках.

c. Установите флажки на соответствующие аккаунты, которые вы хотите использовать.

10. В разделе **Установщик**, выберите объект, к которому выбранные машины будут подключаться для установки и обновления клиента:

- **GravityZone Appliance**, когда машины подключаются непосредственно к устройству GravityZone.

  В этом случае вы можете также определить пользовательский коммуникационный сервер, введя, в случае необходимости, его IP-адрес или имя хоста.

- **Endpoint Security Relay**, если вы хотите подключить машины к клиенту-ретранслятору, установленному в вашей сети. Все машины с ролью ретранслятора, обнаруженные в вашей сети, будут отображены в таблице ниже. Выберите компьютер с ролью ретранслятора, который Вам нужен. Подключенные конечные точки будут сообщаться при помощи Control Center только через выбранный компьютер с ролью ретранслятора.

Важно

– При развертывании через агента ретранслятора, должен быть открыт 7074 порт.

– При развертывании агента через Linux Relay должны выполняться следующие условия:

- На конечной точке с Relay ролью должен быть установлен пакет Samba (`smbclient`) версии 4.1.0 или выше и `net` binary/command для развертывания агентов на Windows.

  Примечание
  `net` binary/command обычно используется с samba-клиентом и/или стандартными пакетами samba. В некоторых дистрибутивах Linux (например CentOS 7.4) `net` command устанавливается только, когда установлен Samba Samba suite (Common + Client + Server). Убедитесь, что на конечной точке с Relay ролью доступна `net` command.

- Целевые конечные точки Windows должны иметь доступ к ресурсам администрирования и сети.
- В целевых конечных точках Linux и Mac должен быть включен SSH и отключен брандмауэр.

11. Вы должны выбрать один установочный пакет для текущего развертывания. Нажмите на список **Использовать пакет** и выберите установочный пакет, который вам нужен. Вы можете найти здесь все инсталляционные пакеты, созданные ранее для вашей компании.
12. При необходимости, вы можете изменить некоторые настройки выбранного пакета установки с помощью кнопки **Настроить**, рядом с полем **Использовать пакет**.

    Настройки инсталляционного пакета появятся ниже и вы сможете сделать необходимые изменения. Чтобы узнать больше о редактировании инсталляционных пакетов, обратитесь к руководству по установке GravityZone.

    Предупреждение
    Пожалуйста, обратите внимание, что модуль брандмауэр доступен только для поддерживаемых рабочих станций Windows.

    Если вы хотите сохранить изменения как новый пакет, выберите опцию **Сохранить как пакет**, расположенную в нижней части списка параметров пакета, и введите имя для нового пакета установки.
13. Нажмите **Сохранить**. Появится окно подтверждения.

Удаление клиента

Для удаленного удаления защиты Bitdefender:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты из выбранного контейнера отображаются в таблице правой панели.
4. Отметьте флажками виртуальные машины, на которых вы хотите удалить агента безопасности Bitdefender.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Удалить клиента**.
6. Появится окно конфигурации, которое позволит вам сделать следующие настройки:
   - Вы можете выбрать хранение объектов карантина на клиентской машине.
   - Для интегрированной среды vShield, вы должны выбрать необходимые учетные данные для каждой машины, в противном случае удаление не произойдет. Выберите **Используйте учетные данные для интеграции vShield**, затем ниже проверьте все соответствующие учетные данные в таблице диспетчера учетных данных.
7. Нажмите **Сохранить**, чтобы создать задачу. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Примечание
Если вы хотите переустановить защиту, в первую очередь обязательно перезагрузите компьютер.

Обновления

Периодически проверяйте статус управляемых виртуальных машин. Если вы заметили виртуальную машину с проблемами безопасности, нажмите на ее имя, чтобы отобразить окно **Информация**. Для получения более подробной информации, обратитесь к «Статус безопасности» (p. 120).

Устаревшие клиенты или устаревшие механизмы защиты представляют проблемы безопасности. В этих случаях, вы должны запустить обновление на соответствующей виртуальной машине. Эта задача может быть запущена локально на виртуальной машине, или дистанционно с Control Center.

Для удаленного обновления клиента и механизмов защиты на управляемых виртуальных машинах:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты из выбранного контейнера отображаются в таблице правой панели.
4. Отметьте флажками виртуальные машины, где вы хотите запустить обновление клиента.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обновить**. Появится окно настроек.
6. Вы можете обновить только продукт, только механизмы защиты или всё сразу.
7. Для ОС Linux и машин, интегрированных с vShield, также является обязательным выбрать необходимые учетные данные. Проверьте опцию **Используйте учетные данные для интеграции Linux и vShieldn**, затем выберите соответствующие учетные данные из таблицы диспетчера учетных данных, которые отображаются ниже.
8. Нажмите **Обновить** для запуска задачи. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Перенастройка клиента

Модули защиты агента безопасности, роли и режимы сканирования изначально заданы в установочном пакете. После того как вы установили агента безопасности в вашей сети, вы можете в любое время изменить исходные настройки, отправив задачу перенастройки **Reconfigure Client** к требуемым управляемым конечным точкам.

Предупреждение
Пожалуйста, обратите внимание, что задача **Reconfigure Client** перезаписывает все параметры установки и ни одна из начальных настроек не сохраняется. Во время использования этой задачи, убедитесь, что перенастроили все настройки установки для требуемых конечных точек.

Чтобы изменить параметры установки для одной или нескольких виртуальных машин:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты из выбранного контейнера отображаются в таблице правой панели.
4. Отметьте флажками виртуальные машины, для которых вы хотите изменить параметры установки.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Перенастроить клиента**.
6. В разделе **Общие**, настройте время выполнения задачи:
   - **Сейчас**, чтобы немедленно начать задачу.
   - **Запланировано**, чтобы настроить интервал повторяемости задачи. В этом случае, выберите желаемый интервал времени (ежечасно, ежедневно или еженедельно) и настройте его в соответствии с вашими потребностями.

     Примечание
     Например, когда другие важные процессы также должны работать на выбранной машине, вы можете запланировать запуск задачи через каждые 2 часа. Задача будет запускаться на каждой выбранной машине через каждые 2 часа, пока не будет завершена.

7. Настройте необходимые модули, роли и режимы сканирования для выбранной конечной точки. Для получения более подробной информации, обратитесь к руководству по установке GravityZone.

   Предупреждение
   - Будут установлены только поддерживаемые модули для каждой операционной системы.

Пожалуйста, обратите внимание, что модуль брандмауэр доступен только для поддерживаемых рабочих станций Windows.

- Bitdefender Tools (стандартный клиент) поддерживает только централизованное сканирование.

8. Нажмите **Сохранить**. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Сетевое Обнаружение

Сетевое обнаружение происходит автоматически только агентами безопасности с Роль ретранслятора. Если у вас в сети нет агента ретрансляции, вам придется вручную запускать задачу сетевого обнаружения из защищенной конечной точки.

Чтобы запустить задачу сетевого обнаружения в вашей сети:

Важно
Если вы используете ретранслятор Linux для обнаружения других конечных точек Linux или Mac, вы должны либо установить Samba на целевые конечные точки, либо присоединиться к ним в Active Directory и использовать DHCP. Таким образом, NetBIOS будет автоматически настроен на них.

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты из выбранного контейнера отображаются в таблице правой панели.
4. Отметьте флажком машину, на которой вы хотите выполнить задачу сетевого обнаружения.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обнаружение сети**.
6. Появится окно подтверждения. Нажмите **Да**.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Обнаружение Приложений

Чтобы обнаружить приложения в вашей сети:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все виртуальные машины, из выбранного контейнера, отобразятся в таблице правой панели.
4. Выберите виртуальные машины, на которых вы хотите выполнить обнаружение приложений.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обнаружение приложений**.

Примечание
Bitdefender Endpoint Security Tools с модулем Управления приложениями должен быть установлен и активирован на выбранных виртуальных машинах. В противном случае, задача будет неактивна. Когда выбранная группа содержит и действительные, и недействительные объекты, задача будет отправлена только действительным конечным точкам.

6. Нажмите **Да** в окне подтверждения для продолжения.

Обнаруженные приложения и процессы отображаются на странице **Сеть > Инвентаризация приложений**. Для получения более подробной информации, обратитесь к «Инвентаризация Приложений» (p. 208).

Примечание
Задача **Обнаружение приложений** занимает некоторое время, в зависимости от количества установленных приложений. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Перезагрузка машины

Вы можете удаленно перезагрузить управляемые виртуальные машины.

Примечание
Проверьте страницу **Сеть > Задачи** перед перезапуском определенных виртуальных машин. Ранее созданные задачи еще могут быть в процессе выполнения на выбранных виртуальных машинах.

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты из выбранного контейнера отображаются в таблице правой панели.
4. Установите флажки на виртуальных машинах, которые вы хотите перезагрузить.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Перезагрузить машину**.
6. Выберите опции перезагрузки по расписанию:
   - Выберите **Перезапустить сейчас**, чтобы немедленно перезагрузить виртуальные машины.
   - Выберите **Включить перезагрузку** и используйте поля ниже, чтобы запланировать перезагрузку в определенную дату и время.
7. Нажмите **Сохранить**. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

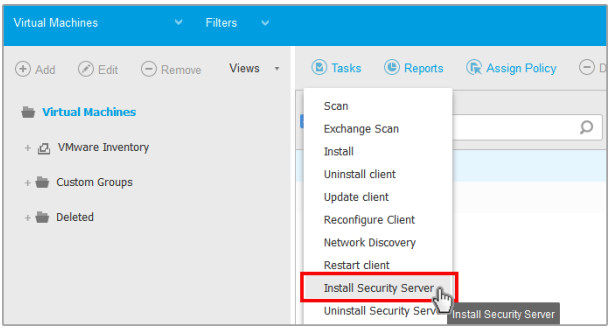
Установка Security Server

Чтобы установить Security Server в вашей виртуальной среде:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Просмотрите инвентаризацию Nutanix, VMware или Citrix и установите флажки на соответствующих хостах или контейнерах (Nutanix Prism, vCenter Server, XenServer или ЦОД). Для быстрого выбора, вы можете сразу выбрать корневой контейнер (Nutanix, VMware или Citrix). Вы сможете выбрать хосты самостоятельно в мастере установки.

   Примечание
   Вы не можете выбрать хосты из разных папок.

4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **УстановитьSecurity Server** в меню. Отобразится окно установки **Security Server Установка**.



Установка Security Server из меню задач

5. Все хосты, обнаруженные в выбранном контейнере, появятся в списке. Выберите хосты, на которых вы хотите установить экземпляр Security Server.
6. Выберите параметры конфигурации, которые вы хотите использовать.

Важно
Использование общих настроек, при развертывании нескольких экземпляров Security Server одновременно, требует: одно общее хранилище для хостов; наличие собственных IP-адресов, назначенных с помощью DHCP-сервера; находится в одной сети.

7. Нажмите **Далее**.
8. Укажите соответствующие учетные данные VMware vShield для каждой машины vCenter.
9. Введите подходящее имя для Security Server.
10. Для среды VMware, выберите контейнер, в который вы хотите включить Security Server из меню **Установить контейнер**.
11. Выберите расположение хранилища.

12. Выберите тип диска (provisioning type). Рекомендуется развернуть устройство на "толстых" дисках (thick provisioning).

Важно
Если вы используете "тонкие" диски (thin provisioning) и дисковое пространство в хранилище данных закончится, Security Server заморозится и, следовательно, хосты останутся незащищенными.

13. Настройте распределение памяти и ресурсов процессора, основанное на коэффициенте консолидации виртуальной машины на хосте. Выберите **Низкий**, **Средний** или **Высокий**, чтобы загрузить рекомендуемые параметры распределения ресурсов или **настройка вручную**, чтобы настроить распределение ресурсов вручную.
14. Задайте пароль администратора для консоли Security Server. Установка пароля администратора перезаписывает пароль по умолчанию ("sve").
15. Установите часовой пояс устройства.
16. Выберите тип конфигурации сети для сети Bitdefender. IP-адрес Security Server не должен изменяться со временем, так как он используется агентами Linux для общения.

    Если вы выберите DHCP, убедитесь, что настроили DHCP-сервер на резервирование IP-адреса для устройства.

    Если вы выберите статический, вы должны ввести информацию о IP-адресе, маске подсети, шлюзе и DNS.
17. Выберите сеть vShield и введите учетные данные vShield. По умолчанию метка для vShield сети `vmservice-vshield-pg`.
18. Нажмите **Сохранить**, чтобы создать задачу. Появится окно подтверждения.

Важно

- Пакеты Security Server не включены по умолчанию в устройства GravityZone. В зависимости от настроек, сделанных главным администратором, необходимый для вашей среды пакет Security Server либо загрузится при запуске установки Security Server, либо администратор будет уведомлен об ошибке пакета и установка не будет завершена. Если пакет отсутствует, главному администратору придется вручную загрузить его до установки.

- Установка Security Server на Nutanix через удаленную задачу может окончиться неудачей, когда кластер Prism Element зарегистрирован на Prism Central или по другой причине. В данной ситуации, рекомендуется произвести ручную установку Security Server. За подробной информацией, обратитесь к этой статье Базы знаний.

19. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Удаление Security Server

Чтобы удалить Security Server:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите датацентр или папку, содержащую хост, на котором Security Server установлен.
4. Установите флажок в поле соответствующего хоста, на котором Security Server установлен.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Удалить Security Server**.
6. Введите учетные данные vShield и нажмите **Да**, чтобы создать задачу.
7. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Обновление Security Server

Чтобы обновить Security Server:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите хост, на котором Security Server установлен.

   Чтобы легче найти Security Server, вы можете использовать меню **Фильтры** следующим образом:

- Перейдите на вкладку **Безопасность** и выберите только **Серверы безопасности**.
- Перейдите на вкладку **Глубина** и выберите **Все предметы рекурсивно**.

Примечание
Если вы используете инструмент управления виртуализацией, которая в настоящее время не интегрирована с Control Center, то Security Server будет находиться в **Custom Groups**.
Для получения более подробной информации о поддерживаемых платформах виртуализации, обратитесь к руководству по установке GravityZone.

4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обновить Security Server**.
5. Вы должны будете подтвердить ваши действия, нажав **Да**.
6. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Важно
Рекомендуется использовать этот метод, чтобы обновить Security Server для NSX, в противном случае вы потеряете файлы карантина, сохраненные на устройстве.

Установка дополнительного пакета HVI

Для защиты виртуальных машин HVI, вам необходимо установить дополнительный пакет на хосте. Роль этого пакета заключается в обеспечении связи между гипервизором и Security Server, установленным на хосте. После установки, HVI будет защищать виртуальные машины, на которых HVI-защита включена в политике.

Важно

- HVI защищает виртуальные машины исключительно на гипервизорах Citrix Xen.
- Вам не нужно удалять существующего агента безопасности с виртуальной машины.

Чтобы установить дополнительный пакет на хост:

1. Перейдите на страницу **Настройки > Обновить**.
2. Выберите Дополнительный пакет HVI в списке **Компоненты** и нажмите кнопку **Загрузить** в верхней части таблицы.
3. Перейдите на страницу **Сеть** и выберите **Виртуальные машины** в переключателе обзора.
4. Выберите **Сервер** из меню **Виды** в левой панели.
5. Выберите один или несколько Xen-хостов в сетевом содержимом. Вы можете легко просмотреть доступные хосты, выбрав опцию **Тип > Хосты** в меню **Фильтры** .
6. Нажмите кнопку **Задачи** в правой панели и выберите **Установить HVI Дополнительный пакет**. Откроется окно установки.
7. Вы можете запланировать задачу установки. Вы можете сразу же запустить задачу после сохранения задания или в определенное время. В случае если установка не может быть завершена в указанное время, задача автоматически повторится в соответствии с настройками повторения. Например, если вы выбрали несколько хостов и один хост недоступен в запланированное время, задание будет запущено снова в заданное время.
8. Хост должен перезагрузиться, чтобы применить изменения и завершить установку. Если вы хотите, чтобы хост перезагрузился без запроса, выберите **Автоматическая перезагрузка хоста(если необходимо)**.
9. Нажмите **Сохранить**. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**.

Удалите дополнительный пакет HVI

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Чтобы удалить дополнительный пакет с хостов:

1. Перейдите на страницу **Сеть** и выберите **Виртуальные машины** в переключателе обзора.

2. Выберите **Сервер** из меню **Виды** в левой панели.
3. Выберите один или несколько Xen-хостов в сетевом содержимом. Вы можете легко просмотреть доступные хосты, выбрав опцию **Тип > Хосты** в меню **Фильтры** .
4. Нажмите кнопку **Задачи** в правой панели и выберите **Удалить пакет HVI Supplemental Pack** . Откроется окно конфигурации.
5. Запланировать, когда удалить пакет. Вы можете сразу же запустить задачу после сохранения задания или в определенное время. В случае если удаление не может быть завершено в указанное время, задача автоматически повторится в соответствии с настройками повторения. Например, если вы выбрали несколько хостов и один хост недоступен в запланированное время, задание будет запущено снова в заданное время.
6. Хост должен перезапуститьсяб чтобы завершить удаление. Если вы хотите, чтобы хост перезагрузился без запроса, выберите **Автоматическая перезагрузка хоста(если необходимо)**.
7. Нажмите **Сохранить**. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**.

Обновление дополнительного пакета HVI

Чтобы обновить дополнительный пакет на хостах:

1. Установка последнего HVIдополнительного пакета доступна.

   Для получения более подробной информации, обратитесь к «Установка дополнительного пакета HVI» (p. 172).
2. Перейдите в раздел **Сеть**.
3. Выберите **Виртуальные машины** из меню видов сетей.
4. Выберите **Сервер** из меню **Виды** в левой панели.
5. Выберите один или несколько Xen-хостов в сетевом содержимом.

   Вы можете легко просмотреть доступные хосты, выбрав опцию **Тип > Хосты** в меню **Фильтры** .
6. Нажмите кнопку **Задачи** в правой панели и выберите **Обновить Дополнительный пакет HVI**. Откроется окно конфигурации.

7. Запланировать, когда обновить пакет. Вы можете сразу же запустить задачу после сохранения задания или в определенное время.

   В случае если обновление не может быть завершено в указанное время, задача автоматически повторится в соответствии с настройками повторения. Например, если вы выбрали несколько хостов и один хост недоступен в запланированное время, обновление будет запущено снова в заданное время.

8. Выберете **Автоматическую перезагрузку (при необходимости)**, если Вы хотите перезапустить необслуживаемый хост. Вы должны перезапустить хост вручную для запуска обновлений

9. Нажмите **Сохранить**. Появится окно подтверждения.

Вы так же можете проверять статус выполнения задания на странице **Сеть > Задачи**.

Ввести Пользовательский инструмент

Примечание
Эта задача связана с модулем HVI, который может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Для ввода программных средств в гостевые операционные системы:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемую группу в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
4. Установите флажки для целевых конечных точек.
5. Нажмите в верхней части таблицы кнопку **Задачи** и выберите **Ввести инструмент пользователя** Появится окно конфигурации.
6. В раскрывающемся меню выберите все инструменты, которые хотите ввести. Для каждого выбранного инструмента будет отображаться раздел с настройками.

   Эти инструменты были ранее загружены в GravityZone. Если вы не можете найти нужный инструмент в списке, перейдите в раздел **Центр управления инструментами** и добавьте его оттуда. Для получения более подробной

информации, обратитесь к «Ввод инструментов пользователя с HVI» (p. 574).

7. Для каждого инструмента, отображаемого в окне:
   a. Для того, чтобы просмотреть или скрыть раздел инструмента, нажмите на его название.
   b. Введите командную строку инструмента, вместе со всеми необходимыми входными параметрами, таким же образом, как это делается в командной строке. Например:

      ```
      bash script.sh <param1> <param2>
      ```

      Из двух раскрывающихся меню можно выбрать действие для восстановления и исправления резервной копии для средств восстановления Bitdefender.
   c. Укажите место, из которого Security Server должен собирать журналы:
      - **стандартный вывод** . Установите этот флажок, чтобы записывать журналы из стандартного выходного канала связи.
      - **Выходной файл**. Установите этот флажок, чтобы получать сохраненный на конечной точке файл журнала. В этом случае необходимо указать путь к месту, где Security Server может найти файл. Вы можете использовать абсолютный путь или системные переменные.

        Здесь находится дополнительная опция: **Удалить гостевые файлы журнала после их передачи**. Выберите его, если вам больше не потребуются файлы на конечной точке.
8. Если вы хотите перенести файл журналов из Security Server в другое место, необходимо указать путь к месту назначения и учетные данные аутентификации.
9. Для завершения работы инструмента может потребоваться больше предполагаемого времени или он может перестать отвечать на запросы. Во избежание сбоев в таких ситуациях, в разделе **Конфигурация безопасности** выберите, через сколько часов Security Server должен автоматически завершить процесс инструмента.
10. Нажмите **Сохранить**.

Статус задачи можно узнать на странице **Задачи**. Также для получения дополнительных сведений можно проверить отчет о **Статусе введения HVI Третьей стороны**.

6.3.6. Формирование быстрых отчетов

Вы можете выбрать создание быстрых отчетов на управляемых виртуальных машинах, используя страницу **Сеть**:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все виртуальные машины, из выбранного контейнера, отобразятся в таблице правой панели.
4. Фильтр содержимого выбранной группы доступен только для управляемых виртуальных машин.
5. Установите флажки на соответствующих виртуальных машинах, которые будут включены в отчет.
6. Нажмите кнопку **Отчет** в верхней части таблицы и выберите из меню тип отчета. Для получения более подробной информации, обратитесь к «Отчеты по компьютерам и виртуальным машинам» (p. 513).
7. Настройте параметры отчета. Для получения более подробной информации, обратитесь к«Создание отчетов» (p. 534)
8. Нажмите **Создать**. Отчет отобразится немедленно. Время, необходимое для создания отчетов, может изменяться в зависимости от количества выбранных виртуальных машин.

6.3.7. Назначение политик

Вы можете управлять настройками безопасности на виртуальных машинах с помощью политик.

В разделе **Сеть** вы можете просматривать, изменять и назначать политики для каждой виртуальной машины или группы виртуальных машин.

Примечание
Настройки безопасности доступны только для управляемых виртуальных машин. Для облегчения просмотра и управления настройками безопасности,

вы можете отфильтровать сетевое содержимое только для управляемых виртуальных машин.

Для просмотра параметров безопасности, назначенных виртуальной машине:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все виртуальные машины, из выбранного контейнера, отобразятся в таблице правой панели.
4. Нажмите на имя виртуальной машины, которая вас интересует. Появится информационное окно.
5. На вкладке **Общее**, в разделе **Политика**, нажмите на название текущей политики, чтобы просмотреть ее настройки.
6. Вы можете изменить настройки безопасности в случае необходимости, при условии, что владелец политики позволил другим пользователям вносить в нее изменения. Пожалуйста, обратите внимание, что любые изменения, которые вы вносите, влияет на все виртуальные машины, которым назначена данная политика.

   Для получения более подробной информации о настройках политик виртуальных машин, обратитесь к«Политики безопасности (Security Policies)» (p. 237)

Чтобы назначить политику виртуальной машине или группе виртуальных машин:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все виртуальные машины, из выбранного контейнера, отобразятся в таблице правой панели.
4. Отметьте флажок на желаемом объекте. Вы можете выбрать один или несколько объектов одного типа, только одного уровня.
5. Нажмите кнопку **Назначить политику** в верхней части таблицы.
6. Сделайте необходимые настройки в окне **Назначение политики**.

   Для получения более подробной информации, обратитесь к «Назначение политик» (p. 241).

Предупреждение
Для применения политик с включенным Hypervisor Memory Introspection целевым машинам может потребоваться перезагрузка сразу после назначения политики. Машины в этом состоянии отмечены на странице **Сеть** с помощью **Ожидание перезапуска** .

6.3.8. Использование Менеджер восстановления (Recovery Manager) для зашифрованных томов

Когда пользователи конечных точек забывают свои пароли шифрования и не могут больше получать доступ к зашифрованным томам на своих компьютерах, вы можете помочь им, получив ключи восстановления со страницы **Сеть**.

Чтобы получить ключ восстановления:

1. Перейдите в раздел **Сеть**.
2. Нажмите кнопку **Менеджер восстановления** на панели инструментов действий на панели слева. Появится новое окно.
3. В разделе окна **Идентификатор** введите следующие данные:
   a. Идентификатор ключа восстановления зашифрованного тома. Идентификатор ключа восстановления представляет собой строку цифр и букв, доступных в конечной точке на экране восстановления BitLocker.

      В Windows идентификатор ключа восстановления представляет собой строку цифр и букв, доступных на конечной точке на экране восстановления BitLocker.

      Кроме того, вы можете использовать параметр **Восстановление** на вкладке **Защита** в Сведениях о виртуальных машинах для автоматического ввода идентификатора ключа восстановления, для конечных точек как Windows так и macOS.

   b. Пароль вашей учетной записи GravityZone.
4. Нажмите **Открыть** . Окно расширяется.

   В разделе **Информация о томе** представлены следующие данные:

   a. Имя тома
   b. Тип тома (загрузочный или не загрузочный).

c. Имя конечной точки (как указано в Инвентаризации сети)

d. Ключ восстановления. В Windows ключ восстановления - это пароль, автоматически генерируемый при шифровании тома. На Mac ключ восстановления - это пароль учетной записи пользователя.

5. Отправьте ключ восстановления пользователю конечной точки.

Подробнее о шифровании и дешифровке томов с помощью GravityZone см. «Шифрование» (p. 415).

6.3.9. Очистка Лицензионных мест

В Active Directory, сервере vCenter (без vShield, NSX или HVI) и содержимом Xen-сервера, вы можете легко освободить лицензируемые места, используемые виртуальными машинами, с которых агент безопасности был удален без запуска программы деинсталляции.

После того, как вы сделаете это, выбранные машины станут неуправляемыми в сетевом содержимом.

Для очистки лицензируемого места:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** или **Виртуальные машины** из меню выбора отображения.
3. Выберите требуемую группу в левой панели. Все виртуальные машины будут отображаться в правой части таблицы.
4. Выберите виртуальную машину, с которой вы хотите удалить лицензию.
5. Нажмите кнопку ⊖ **Очистить лицензию** в верхней части таблицы.
6. Нажмите **Да** в окне подтверждения для продолжения.

6.4. Мобильные устройства

Для управления безопасностью мобильных устройств, используемых в вашей компании, сначала вы должны связать их с конкретными пользователями в Control Center, а затем установить и активировать программу GravityZone Mobile Client на каждом из них.

Мобильные устройства могут быть собственностью предприятия или личными. Вы можете установить и активировать GravityZone Mobile Client на

каждом мобильном устройстве, а затем передать его соответствующему пользователю. Пользователи также могут установить и активировать GravityZone Mobile Client сами, следуя инструкциям, полученным по электронной почте. Для получения более подробной информации, обратитесь к руководству по установке GravityZone.

Для просмотра мобильных устройств пользователей под своей учетной записью, перейдите в раздел **Сеть** и выберите **Мобильные устройства** из меню видов сетей. Раздел **Сеть** отображает доступные группы пользователей в левой панели и соответствующих пользователей и устройства в правой панели.

Если интеграция с Active Directory настроена, вы можете добавить мобильные устройства к существующим пользователям Active Directory. Вы также можете создавать пользователей в **Пользовательские группы** и добавлять им мобильные устройства.

Вы можете переключить вид правой панели по **пользователи** или **Устройства** с помощью вкладки **Вид** из меню **Фильтры**, расположенного в верхней части таблицы. Вид **Пользователи** позволяет управлять пользователями в Control Center, добавлять пользователей и мобильные устройства, и проверять количество устройств по каждому пользователю. Используйте вид **Устройства**, чтобы было проще управлять и проверять информацию о каждом мобильном устройстве в Control Center.

Вы можете управлять пользователями и мобильными устройствами в Control Center следующим образом:

- Добавление настраиваемых пользователей
- Добавление мобильных устройств пользователям
- Организация настраиваемых пользователей в группы
- Фильтрация и поиск пользователей и устройств
- Проверка статуса и подробностей о пользователях или устройствах
- Запуск задач на мобильных устройствах
- Создание быстрых отчетов о мобильных устройствах
- Проверка и изменение параметров безопасности устройств
- Синхронизация содержимого Control Center с Active Directory
- Удаление пользователей и мобильных устройств

6.4.1. Добавление настраиваемых пользователей

Если интеграция с Active Directory настроена, вы можете добавить мобильные устройства к существующим пользователям Active Directory.

В ситуациях без Active Directory, вы должны сначала создать настраиваемых пользователей для того, чтобы иметь возможность идентифицировать владельцев мобильных устройств.

Есть два способа создания настраиваемых пользователей. Вы можете либо добавить их по одному, либо импортировать файл CSV.

Чтобы добавить настраиваемого пользователя:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Нажмите на меню **Фильтры** в верхней части таблицы и перейдите на вкладку **Вид**. Убедитесь, что параметр **Пользователи** выбран.
4. В левой панели выберите **Пользовательские группы**.
5. Нажмите кнопку **Добавить пользователя** в верхней части таблицы. Появится окно настроек.
6. Укажите необходимые сведения о пользователе:
   - Подходящее имя пользователя (например, полное имя пользователя)
   - Адрес электронной почты пользователя

   Важно

   - Убедитесь, что это действительный адрес электронной почты. Пользователю по электронной почте будет выслана инструкция по установке, когда вы добавите устройство.
   - Каждый адрес электронной почты может быть связан только с одним пользователем.

7. Нажмите **OK**.

Чтобы импортировать пользователей мобильных устройств:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.

3. Нажмите на меню **Фильтры** в верхней части таблицы и перейдите на вкладку **Вид**. Убедитесь, что параметр **Пользователи** выбран.
4. В левой панели выберите **Пользовательские группы**.
5. Нажмите **Импортировать пользователей**. Появится новое окно.
6. Выберите файл CSV и нажмите **Импортировать**. Окно закроется и таблица заполнится импортированными пользователями.

> **Примечание**
> Если возникнут какие-либо ошибки, появится сообщение и таблица заполнится только корректными пользователями. Не корректные пользователи будут пропущены.

После этого вы можете создать группы пользователей в **Пользовательские группы**.

Политика и задачи назначенные пользователю будет применяться для всех устройств, принадлежащих соответствующему пользователю.

6.4.2. Добавление мобильных устройств пользователям

Пользователь может иметь неограниченное число мобильных устройств. Можно добавить устройства одному или нескольким пользователям, но одновременно только одно устройство каждому пользователю.

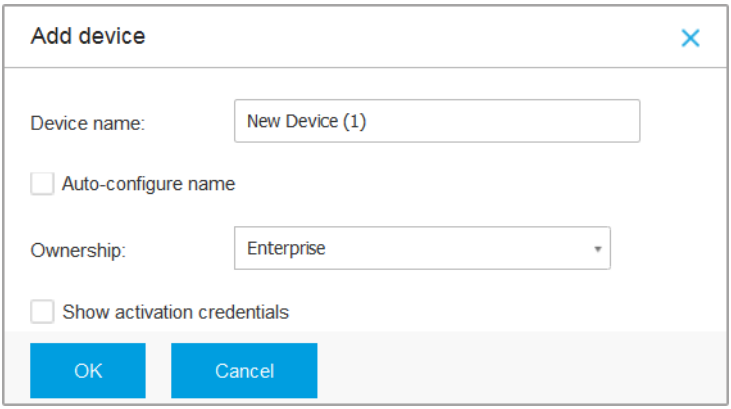
Добавление устройства одному пользователю

Чтобы добавить устройство определенному пользователю:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Найдите пользователя в группе **Активный катаог** или в **Пользовательские группы** и поставьте соответствующий флажок в правой панели.

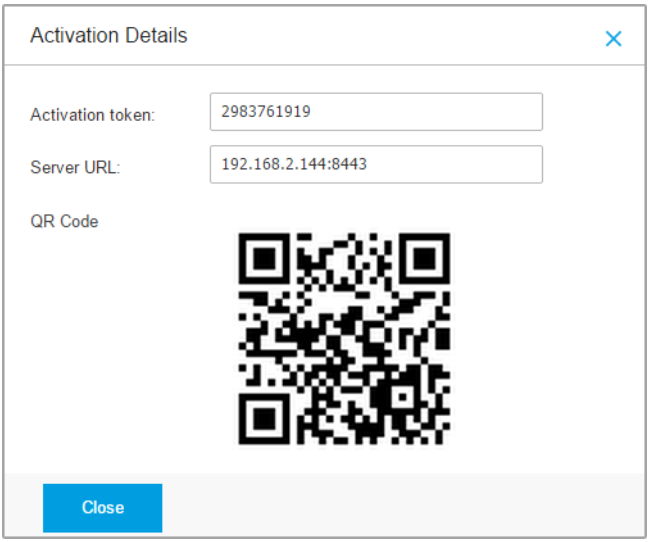
> **Примечание**
> На вкладке **Вид** на **Пользователи** должен быть установлен соответствующий **Фильтры**.

4. Нажмите кнопку **Добавить устройство** в верхней части таблицы. Появится окно настроек.



Добавление мобильного устройства пользователю

5. Настройка подробной информации о мобильных устройствах:
   a. Введите подходящее имя для устройства.
   b. Используйте опцию **Автоматическая настройка имени**, если вы хотите, чтобы имя устройства назначалось автоматически. При добавлении устройство имеет обобщенное имя. После активации устройству автоматически будет присвоено имя, основанное на информации о производителе и модели устройства.
   c. Выберите тип владельца устройства (предприятие или личное). Вы можете в любое время отфильтровать мобильные устройства по владельцам и управлять ими в соответствии с вашими потребностями.
   d. Выберите опцию **Показать учетные данные активации**, если вы собираетесь установить GravityZone Mobile Client на устройстве пользователя.
6. Нажмите **OK**, чтобы добавить устройство. Пользователю будет незамедлительно отправлено письмо с инструкциями по установке, подробностями по активации и настройке устройства. Подробности активации включают маркер активации и адрес коммуникационного сервера (и соответствующий QR Code).
7. Если вы выбрали опцию **Показать учетные данные активации**, появится окно **Подробности активации**, в котором отображается уникальный ключ активации, адрес коммуникационного сервера и соответствующий QR код для нового устройства.



Подробности активации мобильных устройств

После установки GravityZone Mobile Client, когда будет предложено активировать устройство, введите маркер активации и адрес коммуникационного сервера или просканируйте предоставленный QR код.

Добавление устройств нескольким пользователям

Чтобы добавить мобильные устройства выбранным пользователям и группам:

1. Перейдите в раздел **Сеть**.
2. Определите пользователей или группы в папках **Активный каталог** или в **Пользовательские группы** и отметьте их соответствующими флажками в правой панели.

   Примечание
   На вкладке **Вид** на **Пользователи** должен быть установлен соответствующий **Фильтры**.

3. Нажмите кнопку **Добавить устройство** в верхней части таблицы. В этом случае, в окне конфигурации вы должны определить только владельца устройства.

Если есть пользователи без адресов электронной почты, вы будете немедленно уведомлены сообщением об этом. Список соответствующих пользователей будет доступен в **Уведомление** из Control Center.

Мобильные устройства, созданные вручную, имеют по умолчанию обобщенное имя в Control Center. После активации устройству автоматически будет присвоено имя, основанное на информации о производителе и модели устройства.

4. Нажмите **OK**, чтобы добавить устройство. Пользователю незамедлительно будет отправлено письмо с инструкциями по установке, подробностями по активации и настройке устройства. Подробности активации включают маркер активации и адрес коммуникационного сервера (и соответствующий QR Code).

Вы можете проверить количество устройств, назначенных каждому пользователю, в правой панели в колонке **Устройства**.

6.4.3. Организация настраиваемых пользователей в группы

Вы можете просмотреть доступные группы пользователей в левой панели в разделе **Network**.

Пользователи Активного каталога сгруппированы в контейнере **Активный каталог**. Вы не можете редактировать группы Active Directory. Вы можете просмотреть и добавить устройства соответствующим пользователям.

Вы можете разместить всех пользователей не из Активного каталога в **Пользовательские группы**, где вы можете создать и организовать группы по вашему усмотрению. Основным преимуществом этой возможности является то, что вы можете использовать групповые политики для решения различных требований безопасности.

В **Пользовательские группы** вы можете создавать, удалять, переименовывать и перемещать группы в произвольной древовидной структуре.

Важно

Пожалуйста, обратите внимание на следующее:

- Группа может содержать как пользователей, так и другие группы.
- При выборе группы в левой панели, вы можете просмотреть всех пользователей кроме тех, которые находятся в своих подгруппах. Для просмотра всех пользователей, входящих в группу, и в дочерние подгруппы,

нажмите меню **Фильтры**, расположенное в верхней части таблицы и выберите **Все элементы рекурсивно** в разделе **Глубина**.

Создание групп

Чтобы создать пользовательскую группу:

1. Выберите **Пользовательские группы** в левой панели.
2. Нажмите кнопку ⊕ **Добавить группу** в верхней части левой панели.
3. Введите подходящее имя группы и нажмите **OK**. Появится новая группа в **Пользовательские группы**.

Переименование групп

Чтобы переименовать пользовательскую группу:

1. Выберите группу в левой панели.
2. Нажмите кнопку ✎ **Редактировать группу** в верхней части левой панели.
3. Введите новое имя в соответствующем поле.
4. Нажмите **OK** для подтверждения.

Перемещение групп и пользователей

Вы можете перемещать группы и пользователей в любое расположение внутри иерархии **пользовательские группы**. Чтобы переместить группу или пользователей, перетащите их из текущего местоположения в новое.

Примечание

Объект, который перемещается, наследует параметры политик новой родительской группы, если наследование не было запрещено или другая политика не была непосредственно применена к нему.

Удаление групп

Группа не может быть удалена, если она содержит по меньшей мере одного пользователя. Переместите всех пользователей из группы, которую вы хотите удалить, в другую группу. Если группа включает в себя подгруппы, вы можете выбрать для перемещения все подгруппы, а не отдельных пользователей.

Чтобы удалить группу:

1. Выберите пустую группу.
2. Нажмите кнопку ⊗ **Удалить группу** в верхней части левой панели. Вы должны будете подтвердить ваши действия, нажав **Да**.

6.4.4. Проверка статуса мобильных устройств

Каждое мобильное устройство представлено на странице сети, иконкой определенного типа и состояния.

Обратитесь к «Типы сетевых объектов и статусы» (p. 608), чтобы просмотреть список со всеми доступными типами значков и статусов.

Мобильные устройства могут иметь следующие статусы управления:

- **Управляемый (Активный)**, когда удовлетворяются все следующие условия:
  - GravityZone Mobile Client активирован на устройстве.
  - GravityZone Mobile Client синхронизирован с Control Center в последние 48 часов.
- **Управляемый (не активный)**, когда удовлетворяются все следующие условия:
  - GravityZone Mobile Client активирован на устройстве.
  - GravityZone Mobile Client не синхронизирован с Control Center в последние 48 часов.
- **Неуправляемый**, в следующих ситуациях:
  - GravityZone Mobile Client до сих пор не установлен и не активирован на мобильном устройстве.
  - GravityZone Mobile Client был удален с мобильного устройства (только для устройств Android).
  - MDM профиль Bitdefender был удален из устройства (только для IOS устройств).

Чтобы проверить статус управления устройства:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. В левой панели выберите необходимую группу.

4. Нажмите меню **Фильтры** расположенное в верхней части таблицы и сделайте следующие настройки:
   a. Перейдите на вкладку **Вид** и выберите **Устройства**.
   b. Перейдите на вкладку **Безопастность** и выберите интересующий вас статус в разделе **Управление**. Одновременно вы можете выбрать один или несколько критериев фильтра.
   c. Вы также можете выбрать для просмотра все вложенные устройства, выбрав соответствующую опцию на вкладке **Глубина**.
   d. Нажмите **Сохранить**.

      Все мобильные устройства, соответствующие выбранным критериям, отобразятся в таблице.

Вы также можете сформировать отчет о состоянии синхронизации одного или нескольких мобильных устройств. Данный отчет содержит подробную информацию о состоянии синхронизации каждого выбранного устройства, в том числе дату и время последней синхронизации. Для получения более подробной информации, обратитесь к«Формирование быстрых отчетов» (p. 204)

6.4.5. Совместимые и несовместимые мобильные устройства

После того, как приложение GravityZone Mobile Client активируется на мобильном устройстве, Control Center начнет проверять соответствие устройства всем необходимым требованиям. Мобильные устройства могут иметь следующие статусы безопасности:

- **Без проблем с безопасностью**, когда все технические требования соблюдаются.
- **С проблемами с безопасностью**, когда по крайней мере одно из необходимых требований не удовлетворено. Когда устройство несовместимо, пользователю будет предложено исправить проблемы соответствия. Пользователь должен сделать требуемые изменения в течение определенного периода времени, в противном случае будет применено действие для несовместимых устройств, определенное в политике безопасности.

  Для получения дополнительной информации о несовместимости и критериях соответствия, обратитесь к «Совместимость» (p. 431).

Чтобы проверить статус совместимости устройства:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. В левой панели выберите необходимую группу.
4. Нажмите меню **Фильтры** расположенное в верхней части таблицы и сделайте следующие настройки:
   a. Перейдите на вкладку **Вид** и выберите **Устройства**.
   b. Перейдите на вкладку **Безопасность** и выберите интересующий вас статус в разделе **Вопросы безопасности**. Одновременно вы можете выбрать один или несколько критериев фильтра.
   c. Вы также можете выбрать для просмотра все вложенные устройства, выбрав соответствующую опцию на вкладке **Глубина**.
   d. Нажмите **Сохранить**.

      Все мобильные устройства, соответствующие выбранным критериям, отобразятся в таблице.
5. Вы можете просмотреть совместимость устройств по каждому пользователю:
   a. Нажмите меню **Фильтры**, расположенное в верхней части таблицы, и выберите **Пользователи** из меню **Вид**. Все пользователи выбранной группы отобразятся в таблице.
   b. Проверьте столбец **Устойчивость**, чтобы увидеть сколько устройств от общего количества устройств, принадлежащих пользователю, отвечает требованиям.

Вы также можете сформировать отчет о соответствии для одного или нескольких мобильных устройств. Данный отчет содержит подробную информацию о соблюдении соответствия каждым выбранным устройством, в том числе и причины несоответствия. Для получения более подробной информации, обратитесь к«Формирование быстрых отчетов» (p. 204)

6.4.6. Проверка подробной информации о пользователях и мобильных устройствах

Вы можете получить подробную информацию о каждом пользователе и мобильном устройстве в разделе **Сеть**.

Проверка подробной информации о пользователе

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Выберите нужную группу в левой панели.
4. Нажмите меню **Фильтры** в верхней части таблицы, перейдите на вкладку **Вид** и выберите **Пользователи**. Для отображения вложенных пользователей, перейдите на вкладку **Глубина** и выберите **Все компоненты рекурсивно**. Нажмите **Сохранить**. Все пользователи выбранной группы отобразятся в таблице.
5. Проверьте информацию, отображаемую в столбцах таблицы для каждого пользователя:
   - **Имя**. Имя пользователя.
   - **Устройства**. Количество устройств, закрепленных за пользователем. Нажмите на номер, чтобы перейти к просмотру **Devices** и отобразить только соответствующие устройства.
   - **Устойчивость**. Отношение совместимых устройств к общему количеству устройств, закрепленных за пользователем. Нажмите первое значение, чтобы перейти к просмотру **Устройства** и отобразить только совместимые устройства.
6. Нажмите на имя интересующего вас пользователя. Появится окно конфигурации, где вы можете просматривать и редактировать имена пользователей и адреса электронной почты.

Проверка подробной информации об устройстве

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Выберите нужную группу в левой панели.

4. Нажмите меню **Фильтры** в верхней части таблицы, перейдите на вкладку **Вид** и выберите **Устройства**. Нажмите **Сохранить**. Все устройства, принадлежащие пользователям в выбранной группе, отобразятся в таблице.
5. Проверьте информацию, отображаемую в столбцах таблицы для каждого устройства:
   - **Имя**. Имя устройства.
   - **Пользователь**. Имя пользователя, владеющего соответствующим устройством.
   - **OS**. Операционная система соответствующего устройства.
6. Нажмите на название устройства для получения более подробной информации. В появившемся окне **Подробная информация о мобильном устройстве**, вы можете проверить следующую информацию, сгруппированную во вкладках **Просмотреть** и **Детали**:
   - **Общее**.
     - **Имя**. Имя устройства, указанное при добавлении в Control Center.
     - **Пользователь**. Имя владельца устройства.
     - **Группа**. Родительская группа мобильного устройства в сетевом содержимом.
     - **OS**. Операционная система мобильного устройства.
     - **Право собственности**. Тип владельца мобильного устройства (предприятие или личный).
   - **Безопасность**.
     - **Версия клиента**. Версия приложения GravityZone Mobile Client, установленного на устройстве, определенная после регистрации.
     - **Политика**. Политика, назначенная мобильному устройству в настоящий момент. Нажмите на название политики, чтобы перейти к соответствующей странице **Политика** и проверить настройки безопасности.

Важно

По умолчанию, только пользователь, создавший политику, может изменить ее. Чтобы внести изменения, владелец политики должен

выбрать опцию **Разрешить другим пользователям изменять эту политику** на странице политик в разделе **Подробности**. Изменения, внесенные в политику, будут влиять на все устройства, которым данная политика назначена. Для получения более подробной информации, обратитесь к «Назначение политик» (p. 205).

– **Статус лицензии**. Просмотр информации о лицензии для соответствующего устройства.

– **Статус соответствия**. Статус соответствия доступен для управляемых мобильных устройств. Мобильное устройство может иметь статус Совместимый или Не совместимый.

Примечание
Для не совместимых мобильных устройств, отображается значок уведомления ❗. Используйте значок подсказки, чтобы посмотреть причину несоответствия.
Для получения более подробной информации о соответствии мобильных устройств обратитесь к «Совместимость» (p. 431).

– **Вредоносная активность (за последние 24 часа)**. Краткий обзор о количестве обнаруженных вредоносных программ для соответствующего устройства за текущий день.

– **Замок-пароль**. Уникальный пароль, генерируемый автоматически при подключении устройства, которое используется для удаленной блокировки устройства (только для устройств Android).

– **Статус шифрования**. Некоторые устройства с версией Android 3.0 и выше поддерживают функцию шифрования устройств. Чтобы узнать поддерживает ли соответствующее устройство функцию шифрования, проверьте состояние шифрования на странице подробной информации об устройстве. Если шифрование было назначено политикой безопасности на устройстве, вы также можете просмотреть состояние активации шифрования.

- **Подробная информация об активации**

  – **Код активации**. Уникальный маркер активации, назначенный устройству.

  – Адрес коммуникационного сервера.

  - **QR-код**. Уникальный QR-код, содержащий маркер активации и адрес коммуникационного сервера.

- **Аппаратура**. В этом разделе вы можете просмотреть информацию об аппаратных характеристиках устройства, доступную только для управляемых (активированных) устройств. Информация об оборудовании проверяется каждые 12 часов и обновляется при возникновении изменений.

  Важно
  Запуск с Android 10, GravityZone Mobile Client не имеет доступа к ряду номеров, IMEI, IMSI и MAC адресам устройства. Данные ограничения приводят к следующей ситуации:
  - Если мобильное устройство, уже установленное GravityZone Mobile Client, меняет устаревшую версию Android на Android 10, Control Center будет отображать корректные сведения об устройстве. Прежде чем приступить к обновлению убедитесь, что Ваше устройство запускает версию GravityZone Mobile Client.
  - Если GravityZone Mobile Client устанавливает на устройство Android 10, Control Center будет отображать неточные сведения об устройстве в связи с ограничением со стороны операционной системы.

- **Сеть**. В данном разделе вы можете просмотреть информацию о подключениях к сети, доступную только для управляемых (активированных) устройств.

6.4.7. Сортировка, фильтрация и поиск мобильных устройств

Содержимое таблиц мобильных устройств может занимать несколько страниц, в зависимости от количества пользователей или устройств (всего по умолчанию отображается 10 записей на странице). Для перемещения по страницам используйте кнопки навигации в нижней части таблицы. Чтобы изменить количество записей отображаемых на странице, введите другое значение в поле рядом с кнопками навигации.

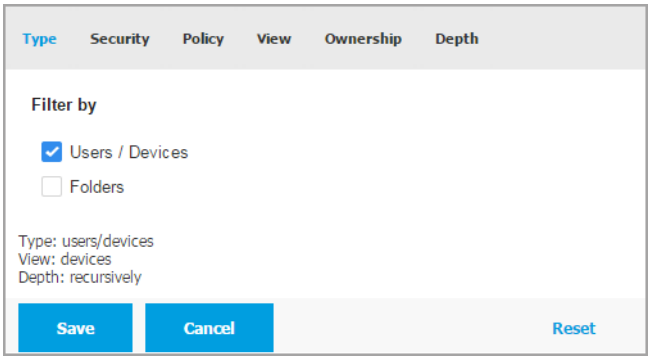
Если записей слишком много, вы можете использовать опции фильтрации для отображения только интересующих вас объектов. Например, вы можете найти конкретное мобильное устройство или выбрать для просмотра только управляемые устройства.

Сортировка перечня мобильных устройств

Для сортировки данных по определенному столбцу, щелкните заголовок столбца. Например, если вы хотите отсортировать устройства по имени, нажмите на заголовок **Имя**. При повторном нажатии на заголовок, устройства будут отображаться в обратной последовательности.

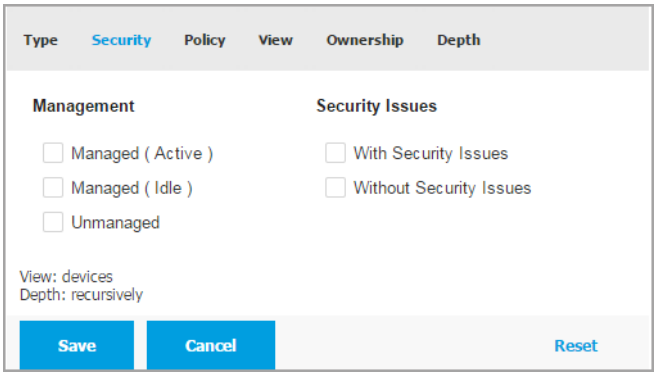
Фильтрация перечня мобильных устройств

1. Выберите желаемую группу из левой панели.
2. Нажмите меню **фильтры** в правой верхней части сетевой панели.
3. Вы можете использовать следующие критерии фильтрации:
   - **Тип**. Выберите тип объектов, которые будут отображаться (пользователи/устройства и папки).



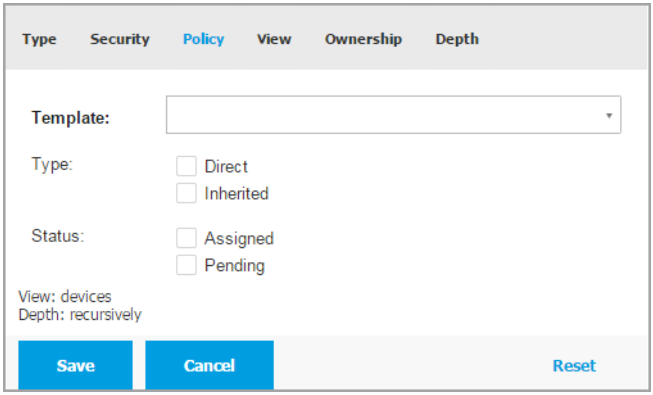
Мобильные устройства - Фильтрация по типу

   - **Безопасность**. Выберите для отображения компьютеры по состоянию управления и безопасности.



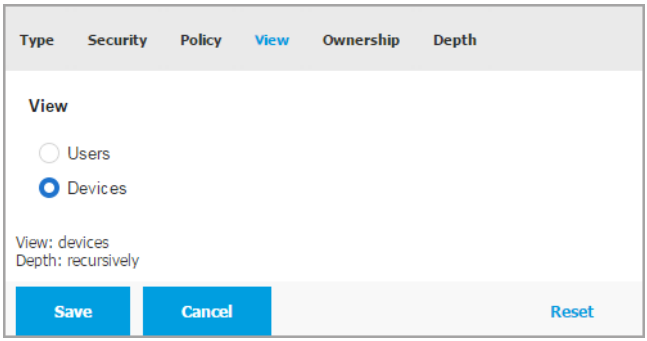
Мобильные устройства - Фильтрация по безопасности

- **Политика**. Выберите шаблон политики, который нужно фильтровать для мобильных устройств, тип назначения политики (прямой или наследуемый), а также статус назначения политики (активный, прикладной или ожидающий).



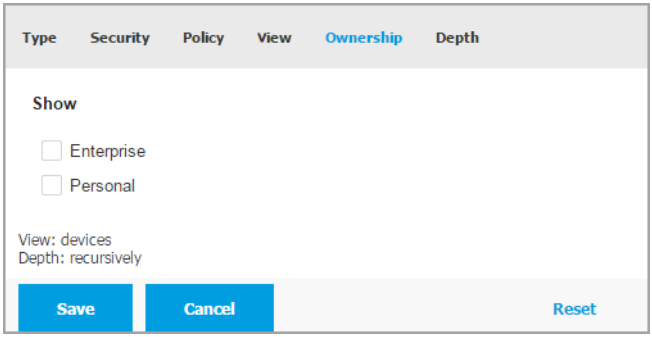
Мобильные устройства - Фильтрация по политикам

- **Вид**. Выберите **Пользователи** для отображения пользователей в выбранной группе. Выберите **Устройства** для отображения устройств в выбранной группе.



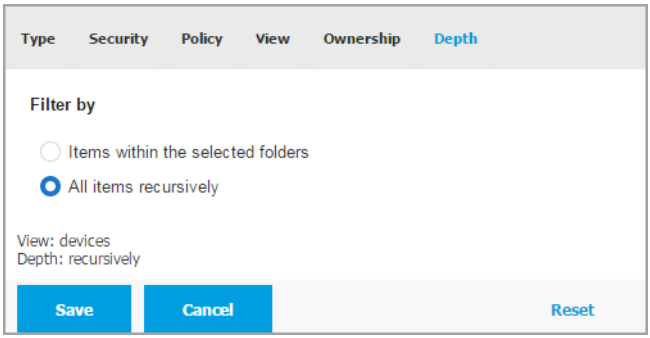
Мобильные устройства - Фильтрация по виду

- **Право собственности**. Вы можете отфильтровать мобильные устройства по владельцам, выбирая отображение устройств предприятия **Предприятие** либо личных устройств **Личные**. Атрибут владельца определен в подробной информации о мобильных устройствах.



Мобильные устройства - Фильтрация по владельцам

- **Глубина**. При управлении древовидной структурой сети, мобильные устройства и пользователи, размещенные в подгруппах, не отображаются при выборе корневой группы. Выберите **Все элементы рекурсивно**, чтобы просмотреть все объекты, входящие в текущую группу, и все ее подгруппы.



Мобильные устройства - Фильтрация по глубине

4. Выберите **Сохранить**, чтобы отфильтровать мобильные устройства по выбранным критериям.

   Фильтр в разделе **Сеть** остается активным, пока вы не выйдите из раздела или не сбросите фильтр.

Поиск мобильных устройств

Правая панель предоставляет информацию о пользователях и мобильных устройствах. Вы можете использовать категории, имеющиеся в каждом столбце, чтобы отфильтровать содержимое таблицы.

1. Выберите нужную группу в левой панели.
2. Выберите требуемый вид (пользователи или мобильные устройства), используя меню **Фильтры** в правой верхней области панели сети.
3. Поиск необходимых объектов осуществляется с помощью поисковых полей под заголовками каждого столбца в правой панели:
   - Введите искомое слово в соответствующем поле поиска.

     Например, выберите вид **Устройства** и введите имя пользователя, которого вы ищете в поле **Пользователь**. В таблице отобразится только соответствующее мобильное устройство.
   - Выберите искомый атрибут в соответствующем раскрывающемся списке.

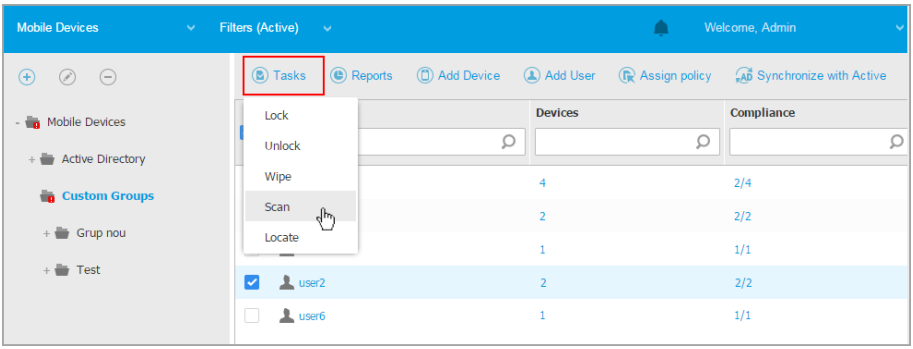
     Например, выберите вид **Устройства**, нажмите на список **OS** и выберите **Android** для отображения только мобильных устройств Android.

Примечание
Чтобы очистить условия поиска и отобразить все объекты, поместите курсор мыши в соответствующее поле и нажмите на значок ×.

6.4.8. Запуск задач на мобильных устройствах

В разделе **Сеть** вы можете удаленно запускать ряд администраторских задач на мобильных устройствах. Вы можете выполнить следующие задачи:

- «Заблокировать» (p. 200)
- «Стереть данные» (p. 201)
- «СКАНИРОВАТЬ» (p. 202)
- «Местоположение» (p. 203)



Запуск задач на мобильных устройств

Для удаленного запуска задач на мобильных устройствах должны быть выполнены некоторые условия. Для получения более подробной информации, обратитесь к главе требований по установке руководства по установке GravityZone.

Вы можете создавать задачи отдельно для каждого мобильного устройства, для каждого пользователя или для групп пользователей. Например, вы можете удаленно сканировать мобильные устройства группы пользователей на наличие вредоносного ПО. Вы также можете запустить задачу определения местоположения для определенного мобильного устройства.

Сетевое содержимое может включать активные, неработающие или неуправляемые мобильные устройства. После создания, задача запустится

сразу же на активных мобильных устройствах. Для неработающих устройств, задача запустится, как только они станут онлайн. Задачи не может быть создана для неуправляемых мобильных устройств. В этом случае будет отображаться уведомление о том, что задача не может быть создана.

Вы можете просматривать и управлять задачами на странице **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Заблокировать

Задача блокировки сразу блокирует экран выбранных мобильных устройств. Поведение задачи блокировки зависит от операционной системы:

- Задача блокировки для устройств Android (7.0 или новее) будет применять пароль, установленный в консоли GravityZone только в том случае, если на устройстве не настроена защита блокировки. В ином случае для защиты устройства будут использоваться существующие параметры блокировки экрана, такие как PIN-код, пароль, отпечаток пальца или смарт-блокировка.

  Примечание

  – Пароль разблокировки экрана, сгенерированный Control Center, можно увидеть в окне подробной информации о мобильном устройстве.

  – Задача разблокировки больше недоступна для устройств Android (7.0 или новее). Вместо этого пользователи могу разблокировать свои устройства вручную. Однако Вы должны заранее убедиться в том, что эти устройства поддерживают ожидаемые требования к сложности пароля разблокировки.

  – Из-за технических ограничений задачи блокировки недоступны на Android 11.

- На iOS, если устройство имеет блокировку экрана с паролем, устройство попросит его разблокировать.

Чтобы удаленно заблокировать мобильные устройства:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Выберите желаемую группу в левой панели.

4. Нажмите меню **Фильтры**, расположенное в верхней части сетевой панели и выберите **Пользователи** из категории **Вид**. Нажмите **Сохранить**. Все пользователи выбранной группы отобразятся в таблице.
5. Отметьте флажками требуемых пользователей. Вы можете выбрать одного или нескольких пользователей одновременно.
6. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Заблокировать**.
7. Вы должны будете подтвердить ваши действия, нажав **Да**. Сообщение проинформирует вас, была ли создана задача или нет.
8. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Стереть данные

Задача **Стереть** восстанавливает выбранные мобильные устройства к заводским установкам. Запустите эту задачу дистанционно, чтобы стереть всю конфиденциальную информацию и приложения, хранящиеся на выбранных мобильных устройствах.

Предупреждение

Используйте задачу **Стереть** осторожно. Проверьте владельца на выбранных устройствах (если вы хотите исключить стирание личных мобильных устройств) и убедитесь, что вы действительно хотите стереть выбранные устройства. После отправки, задача **Стереть** не может быть отменена.

Примечание

Из-за технических ограничений задачи блокировки недоступны на Android 11.

Чтобы удаленно стереть мобильное устройство:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Выберите желаемую группу в левой панели.
4. Нажмите меню **Фильтры** расположенное в верхней части сетевой панели и выберите **Устройства** из категории **Вид**. Нажмите **Сохранить**. Все устройства в выбранной группе отобразятся в таблице.

Примечание
Вы также можете выбрать **Все элементы рекурсивно** в разделе **Глубина**, чтобы также отобразить все устройства в подгруппах.

5. Установите флажок на соответствующем устройстве, которое вы хотите стереть.
6. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Стереть**.
7. Вы должны будете подтвердить ваши действия, нажав **Да**. Сообщение проинформирует вас, была ли создана задача или нет.
8. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

СКАНИРОВАТЬ

Задача **Сканировать** позволяет проверить выбранные мобильные устройства на наличие вредоносных программ. Пользователь устройства будет уведомлен о любых обнаруженных вредоносных программах и ему будет предложено удалить их. Сканирование выполняется в облаке, поэтому устройство должно иметь доступ в Интернет.

Примечание
Дистанционное сканирование не работает на устройствах iOS (ограничение платформы).

Чтобы удаленно просканировать мобильные устройства:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Выберите желаемую группу в левой панели.
4. Нажмите меню **Фильтры** расположенное в верхней части сетевой панели и выберите **Устройства** из категории **Вид**. Нажмите **Сохранить**. Все устройства в выбранной группе отобразятся в таблице.

Примечание
Вы также можете выбрать **Все элементы рекурсивно** в разделе **Глубина**, чтобы также отобразить все устройства в подгруппах.

Чтобы отобразить только Android-устройства в выбранной группе, перейдите к заголовоку столбца **OS** в правой панели и выберите **Android** из соответствующего списка.

5. Установите флажки на соответствующих устройствах, которые вы хотите просканировать.
6. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Сканировать**.
7. Вы должны будете подтвердить ваши действия, нажав **Да**. Сообщение проинформирует вас, была ли создана задача или нет.
8. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Отчет о сканировании будет доступен после завершения задачи. Нажмите соответствующий значок в столбце **Отчёты**, чтобы сгенерировать быстрый отчет.

   Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

Местоположение

Задача местоположения открывает карту, показывающую расположение выбранных устройств. Можно найти одно или несколько устройств одновременно.

Чтобы запустить задачу определения местоположения, соответствующая служба должна быть включена на мобильных устройствах.

Чтобы найти мобильные устройства:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Выберите желаемую группу в левой панели.
4. Нажмите меню **Фильтры** расположенное в верхней части сетевой панели и выберите **Устройства** из категории **Вид**. Нажмите **Сохранить**. Все устройства в выбранной группе отобразятся в таблице.

   Примечание
   Вы также можете выбрать **Все элементы рекурсивно** в разделе **Глубина**, чтобы также отобразить все устройства в подгруппах.

5. Установите флажок на соответствующем устройстве, которое вы хотите найти.
6. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Расположить**.
7. Откроется окно **Расположение**, в котором будет отображена следующая информация:
   - Карта, показывающая местоположение выбранных мобильных устройств. Если устройство не синхронизировано, карта будет отображать его последнее известное местоположение.
   - Таблица, отображающая подробную информацию о выбранных устройствах (имя, пользователь, дата и время последней синхронизации). Для просмотра местоположения определенного устройства из таблицы на карте, просто отметьте его флажком. Карта немедленно сфокусируется на местоположении соответствующего устройства.
   - Опция **Автообновление** автоматически обновляет местоположения выбранных мобильных устройств каждые 10 секунд.
8. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 223).

6.4.9. Формирование быстрых отчетов

Вы можете создавать мгновенные отчеты по мобильным устройствам, используя раздел **Сеть**:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Выберите требуемую группу в левой панели.
4. Нажмите меню **Фильтры** расположенное в верхней части сетевой панели и выберите **Устройства** из категории **Вид**. Вы также можете выбрать опцию управляемости из вкладки **Безопасность**, чтобы отфильтровать выбранную группу только по управляемым устройствам. Нажмите **Сохранить**. Все устройства, соответствующие критериям фильтров в выбранной группе, отобразятся в таблице.

5. Установите флажки на интересующих вас мобильных устройствах. Вы можете выбрать одно или несколько устройств одновременно.
6. Нажмите кнопку **Отчет** в верхней части таблицы и выберите из меню тип отчета. Для получения более подробной информации, обратитесь к«Отчеты по мобильным устройствам» (p. 532)
7. Настройте параметры отчета. Для получения более подробной информации, обратитесь к«Создание отчетов» (p. 534)
8. Нажмите **Создать**. Отчет отобразится немедленно. Время, необходимое для подготовки отчетов, варьируется в зависимости от количества выбранных мобильных устройств.

6.4.10. Назначение политик

Вы можете управлять настройками безопасности на мобильных устройствах, используя политики.

В разделе **Сеть** вы можете просматривать, изменять и назначать политики для мобильных устройств под своей учетной записью.

Вы можете назначить политику для группы, пользователей или конкретных мобильных устройств.

Примечание

Политика, назначенная пользователю, повлияет на все устройства, принадлежащие этому пользователю. Для получения более подробной информации, обратитесь к «Назначение локальных политик» (p. 241).

Для просмотра параметров безопасности, назначенных мобильному устройству:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Нажмите меню **Фильтры** расположенное в верхней части сетевой панели и выберите **Устройства** из категории **Вид**. Нажмите **Сохранить**. Все устройства, принадлежащие пользователям в выбранной группе, отобразятся в таблице.
4. Нажмите на название интересующего вас мобильного устройства. Появится окно с подробной информацией.

5. В разделе **Безопасность** на странице **Просмотр** нажмите на имя назначенной политики, чтобы посмотреть ее параметры.
6. Вы можете изменять настройки безопасности по мере необходимости. Пожалуйста, обратите внимание, что любое изменение, которое вы делаете, будет применяться также на всех других устройствах, на которых данная политика активна.

   Для получения более подробной информации, обратитесь к«Политики мобильных устройств» (p. 425)

Чтобы назначить политику мобильному устройству:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. В левой панели выберите необходимую группу.
4. Нажмите меню **Фильтры** расположенное в верхней части сетевой панели и выберите **Устройства** из категории **Вид**. Нажмите **Сохранить**. Все устройства, принадлежащие пользователям в выбранной группе, отобразятся в таблице.
5. Установите в правой панели флажок на интересующем вас мобильном устройстве.
6. Нажмите кнопку **Определить политику** в верхней части таблицы.
7. Сделайте необходимые настройки в окне **Назначение политики**. Для получения более подробной информации, обратитесь к «Назначение локальных политик» (p. 241).

6.4.11. Синхронизация со службой каталогов Active Directory

Сетевое содержимое автоматически синхронизируется с Active Directory через интервал времени, заданный в разделе конфигурации Control Center. Более подробную информацию см. в главе GravityZone по установке и настройке в руководстве по установке GravityZone

Чтобы вручную синхронизировать отображаемых пользователей с Active Directory:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.

3. Нажмите кнопку **Синхронизировать с Active Directory** в верхней части таблицы.
4. Вы должны будете подтвердить ваши действия, нажав **Да**.

Примечание

Для больших сетей со службой каталогов Active Directory завершение синхронизации может занять больше времени.

6.4.12. Удаление пользователей и мобильных устройств

Когда сетевое содержимое отображает выбывших пользователей или мобильные устройства, рекомендуется их удалить.

Удаление мобильных устройств из сетевого содержимого

При удалении устройства из Control Center:

- GravityZone Mobile Client отключается, но не удаляется из устройства.
- Для iOS-устройств MDM-профиль будет удален. Если устройство не подключено к сети Интернет, MDM-профиль останется в устройстве, пока не станет доступно новое соединение.
- Все журналы, связанные с удаленным устройством, будут по-прежнему доступны.
- Ваша личная информация и приложения не будут затронуты.

Предупреждение

- Вы не сможете восстановить удаленные мобильные устройства.
- Если вы случайно удалили заблокированное устройство, вам придется сбросить устройство к заводским установкам, чтобы его разблокировать.

Чтобы удалить мобильное устройство:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. В левой панели выберите необходимую группу.

4. Нажмите меню **Фильтры** расположенное в верхней части сетевой панели и выберите **Устройства** из категории **Вид**.
5. Нажмите **Сохранить**.
6. Установите флажок на соответствующих мобильных устройствах, которые вы хотите удалить.
7. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

Удаление пользователей из сетевого содержимого

Пользователи, связанные с мобильными устройствами, не могут быть удалены. В первую очередь, вам необходимо удалить соответствующие мобильные устройства.

Примечание
Вы можете удалять пользователей только из Custom Groups.

Чтобы удалить пользователя:

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. В левой панели выберите необходимую группу.
4. Нажмите меню **Фильтры**, расположенное в верхней части сетевой панели и выберите **Пользователи** из категории **Вид**.
5. Нажмите **Сохранить**.
6. Установите флажок на соответствующем пользователе, которого требуется удалить.
7. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

6.5. Инвентаризация Приложений

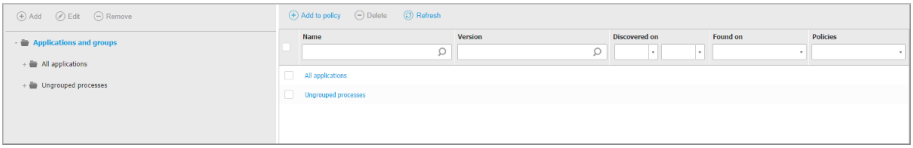
Вы можете просмотреть все приложения, обнаруженные в вашей сети, с помощью задачи **Обнаружение приложений** в разделе **Приложения и группы**. Для получения более подробной информации, обратитесь к «Обнаружение Приложений» (p. 109).

Приложения и процессы автоматически добавляются в папку **Приложения и группы** в левой боковой панели.

Вы можете организовать приложения и процессы в пользовательские группы.

Все приложения/процессы выбранной папки отображаются в правой панели таблицы. Вы можете выполнить поиск по имени, версии, издателю/автору, обновившему, расположению и политике.

Для просмотра самой актуальной информации, нажмите кнопку **Обновить** в верхней части таблицы. Данная функция может быть полезной, если вы длительное время находитесь на странице.



Инвентаризация Приложений

Важно

Новые приложения, обнаруживаемые каждый раз при запуске задачи **Обнаружение приложений**, автоматически помещаются в папку **Разгруппированные приложения**. Процессы, которые не связаны с конкретными приложениями, помещаются в папку **Разгруппированные процессы**.

Дерево Приложений и Групп

Чтобы добавить пользовательскую группу в дерево **Приложения и группы**:

1. Выберите папку **Все приложения**.
2. Нажмите кнопку **Добавить** в верхней части дерева.
3. Введите имя в новом окне.
4. Нажмите **OK** для создания новой группы.
5. Выберите папку **Разгруппированные приложения**. Все приложения, сгруппированные в выбранной папке, отобразятся в правой панели таблицы.
6. Выберите нужные приложения в правой панели таблицы. Перетащите выбранные элементы из правой панели в желаемую пользовательскую группу в левой панели.

Чтобы добавить пользовательское приложение:

1. Выберите папку в **Все приложения**.
2. Нажмите кнопку ⊕ **Добавить** в верхней части дерева.
3. Введите имя в новом окне.
4. Нажмите **OK** чтобы создать пользовательское приложение.
5. Вы можете добавлять процессы, связанные с новым пользовательскими приложениями из папки **Разгруппированные процессы** или из других папок, отображаемых в дереве **Приложения и группы**. После выбора папки все процессы отображаются в правой панели таблицы.
6. Выберите нужные процессы в правой панели таблицы. Перетащите выбранные элементы из левой панели, чтобы переместить их в список пользовательских приложений.

Примечание
Приложение может быть включено только в одну группу.

Чтобы изменить имя папки или приложения:

1. Выберите объект в дереве **Приложения и группы**.
2. Нажмите кнопку **Редактировать** в верхней части дерева.
3. Измените имя на желаемое.
4. Нажмите **OK**.

Вы можете перемещать группы и приложения в любое место внутри иерархии **Приложения и группы**. Чтобы переместить группу или приложение, перетащите его из текущего местоположения в новое.

Чтобы удалить пользовательскую папку или приложение, выберите его в дереве **Приложения и группы**, а затем нажмите кнопку ⊖ **Убрать** в верхней части дерева.

Добавление приложений к политикам

Для добавления приложения или процесса к правилу непосредственно из содержимого Application:

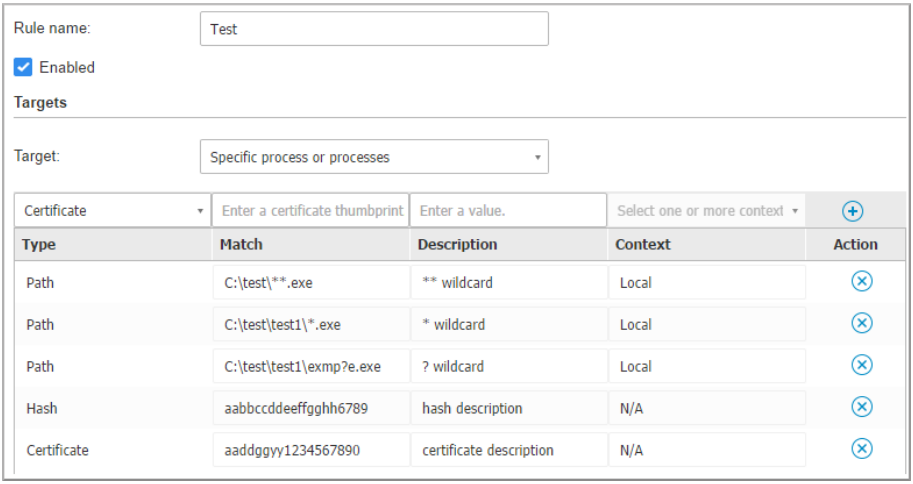
1. Выберите нужную папку из дерева **Приложения и группы**. Содержимое папки перечислено в правой панели.

2. Выберите требуемые процессы или приложения в правой панели.
3. Нажмите кнопку ⊕ **Добавить в политику**, чтобы открыть окно настроек.
4. В разделе **Применить правило к этим политикам** введите имя существующей политики. Используйте форму поиска, чтобы найти политику по названию или владельцу.
5. В разделе **Детали правила** введите **Имя правила**.
6. Отметьте флажок **Включить**, чтобы активировать правило.
7. Выбранный тип распознается автоматически. При необходимости, измените существующие критерии:
   - **Конкретный процесс или процессы**, чтобы определить процесс, запуск которого разрешен или запрещен. Вы можете авторизовать его по пути, хэшу или сертификату. Условия внутри правила складываются логическим AND.
     - Для авторизации приложения по конкретному пути:
       a. Выберите **Путь** в столбце **Тип**. Укажите путь к объекту. Вы можете указать абсолютный или относительный путь к файлу и использовать знаки подстановки. Символ звездочки (*) соответствует любому файлу в директории. Двойная звездочка (**) соответствует всем файлам и каталогам в определенной директории. Вопросительный знак (?) соответствует только одному символу. Кроме того, вы можете добавить описание, чтобы помочь идентифицировать процесс.
       b. Из выпадающего меню **Выберите один или несколько контекстов** вы можете выбрать локальный, CD-ROM, съемный или сетевой диск. Вы можете заблокировать выполнение приложения со съемного носителя или разрешить, если приложение выполняется локально.
     - Для авторизации приложение на основе хэша, выберите **Хэш** в столбце **Тип** и введите значение хеш-функции. Кроме того, вы можете добавить описание, чтобы помочь идентифицировать процесс.

Важно
Для генерации значения хэша, скачайте инструмент Отпечаток пальца. Для получения более подробной информации, обратитесь к «Инструменты модуля Управления приложениями» (p. 613)

– Для авторизации на основе сертификата, выберите **Сертификат** в столбце **Тип** и введите отпечаток сертификата. Кроме того, вы можете добавить описание, чтобы помочь идентифицировать процесс.

Важно
Чтобы получить отпечаток сертификата, скачайте инструмент Thumbprint. Для получения более подробной информации, обратитесь к «Инструменты модуля Управления приложениями» (p. 613)



Правила приложений (Application Rules)

Нажмите ⊕ **Добавить**, чтобы добавить правило. Вновь созданное правило будет иметь самый высокий приоритет в этой политике.

- **Инвентаризация приложений или групп**, чтобы добавить группу или приложение, обнаруженное в вашей сети. Вы можете просматривать приложения, запущенные в вашей сети, на странице **Сеть >Инвентаризация приложений**.

  Вставьте имена приложений или названия групп в поле, разделенные запятой. Функция автоматического заполнения отображает подсказки при вводе.

8. Отметьте флажок **Включить подпроцессы**, чтобы применить правило к порожденным дочерним процессам.

Предупреждение
При настройке правил для приложений браузера, рекомендуется отключить эту опцию, чтобы предотвратить угрозы безопасности.

9. Дополнительно, вы также можете задать исключения для правила запуска процесса. Сложение операций аналогично описанию в предыдущих шагах.
10. В разделе **Разрешения** выберите, следует разрешить или запретить правила для запуска.
11. Нажмите **Сохранить**, чтобы сохранить изменения.

Для удаления приложения или процесса:

1. Выберите нужную папку из дерева **Приложения и группы**.
2. Выберите требуемые процессы или приложения в правой панели.
3. Нажмите кнопку **Удалить**.

Кто обновляет

Вы должны определить, кто будет выполнять обновления приложений, которые обнаружены в вашей сети.

Предупреждение
Если вы не назначите ответственных за обновление приложений, то обновлять приложения из "белого" списока будет запрещено.

Чтобы назначить обновляющих:

1. Выберите нужную папку в дереве **Приложения и группы**. Содержимое папки будет перечислено в правой панели.
2. В правой панели выберите файл, который вы хотите использовать в качестве обновляющего.
3. Нажмите кнопку **Назначить обновляющих**
4. Нажмите **Да**, чтобы подтвердить выбор. Обновляющий будет обозначен специфической иконкой:

Обновляющий

Чтобы отменить обновляющего:

1. Выберите нужную папку в дереве **Приложения и группы**. Содержимое папки будет перечислено в правой панели.
2. В правой панели выберите обновляющего, которого вы хотите удалить.
3. Нажмите кнопку **Отклонить обновление**.
4. Нажмите **Да** для подтверждения.

6.6. Инвентаризация патча

GravityZone выясняет, какие патчи требуются вашему ПО посредством задачи **Сканирование патчей** и затем добавляет их в инвентарь.

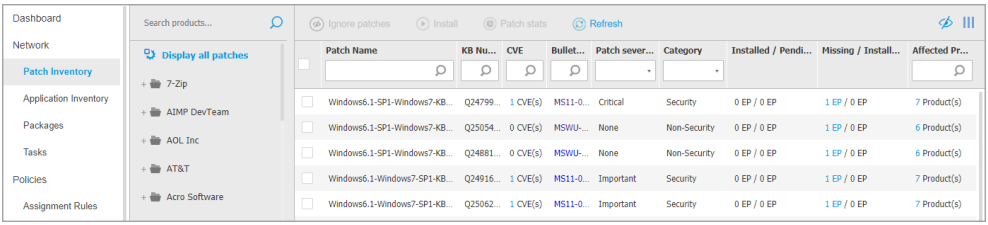
Страница **Patch Inventory** отображает все обнаруженные патчи для ПО, установленные в конечных точках и предлагает несколько действий, которые вы можете предпринять с этими патчами.

Используйте Patch Inventory когда вам это необходимо, чтобы сразу же развернуть определенные патчи. Эта альтернатива позволяет вам легко решать некоторые проблемы, о которые вам известно Например, вы прочитали статью об уязвимости ПО и вы знаете CVE ID. Вы можете найти инвентарь для патчей, подходящий CVE и затем посмотреть, какая конечная точка нуждается в обновлении.

Чтобы перейти в Patch Inventory, выберите опцию **Сеть > Patch Inventory** в основном меню Control Center.

Страница организована в двух панелях:

- Панель слева отображает продукты ПО, установленные в вашей сети, сгруппированные продавцом.
- Панель справа отображает таблицу доступных патчей и информацию о них.



Инвентаризация патча

Далее вы узнаете, как использовать инвентарь. Вы можете выполнить следующие задачи:

- См. детали патчей
- Искать и фильтровать патчи
- Игнорировать патчи
- Устанавливать патчи
- Удалять патчи
- Создавать статистику о патчах

6.6.1. Получение сведений о патчах

Таблица патчей дает информацию, которая помогает вам идентифицировать патчи, оценить их важность, просмотреть статус их установки и объем. Детали описаны здесь:

- **Имя патча.** Это имя запускаемого файла, содержащего патч.
- **KB номер.** Этот номер идентифицирует статью KB, в которой есть информация об освобождении патча.
- **CVE.** Это номер CVE, на которые ссылается патч. Нажимая на номер, вы увидите список CVE IDs.
- **ID бюллетени** Это ID бюллетеня по безопасности, выпускаемый продавцом. Этот ID связан с актуальной статьей, которая описывает патч и дает детали установки.
- **Важность патча.** Этот рейтинг информирует вас о важности патча в отношении ущерба, который он предотвращает.

- **Категория.** В зависимости от типа проблем, которые они решают, патчи группируются на: патчи безопасности и иные. Это поле информирует вас о том, в какой категории находится патч.
- **Установлено / Ожидает установки.** Эти числа показывают, сколько конечных точек установили исправление и сколько ожидают его установки. Числа ссылаются на список данных конечных точек.
- **Пропущено / Установка не удалась.** Эти числа показывают, на скольких конечных точках не установлено исправление, а на скольких - установка не удалась. Числа ссылаются на список данных конечных точек.
- **Затронутые продукты.** Это количество продуктов, для которых выпущен патч. Количество связано со списком этих продуктов ПО.
- **Удаляемые.** Если вам нужно откатить какой-либо патч, вы должны сначала убедиться в том, что его можно удалить. Используйте этот фильтр, чтобы узнать, какие патчи можно удалить (откатить). Для большей информации обратитесь к Uninstall patches.

Чтобы настроить детали, отображенные в таблице:

1. Нажмите кнопку **Колонки** справа от Панель действий
2. Выберите столбцы, которые вы хотите отобразить.
3. Нажмите кнопку **Восстановить**, чтобы вернуться к виду столбцов по умолчанию.

Пока вы находитесь на странице, процессы GravityZone, протекающие фоном, могут повлиять на базы данных. Убедитесь, что вы просматриваете последнюю информацию в таблице, нажимая кнопку **Обновить** в верхней части таблицы.

GravityZone просматривает список доступных исправлений и удаляет те, которые больше не применяются в связи с тем, что связанных приложений или конечных точек больше не существует.

GravityZone также ежедневно просматривает и удаляет патчи, недоступные в списке, хотя они могут присутствовать на некоторых конечных точках.

6.6.2. Поиск и фильтрация патчей

По умолчанию Control Center отображает все доступные исправления для вашего программного обеспечения. GravityZone предоставляет вам несколько вариантов быстрого поиска нужных вам исправлений.

Фильтрация патчей по продукту

1. Расположите продукт в левой панели.

   Это можно сделать, прокрутив список, чтобы найти его поставщика, или введя его имя в поле поиска в верхней части панели.

2. Нажмите на имя поставщика, чтобы развернуть список и просмотреть его продукты.

3. Выберите продукт, чтобы просмотреть доступные исправления, или отмените выбор, чтобы скрыть его исправления.

4. Повторите предыдущие шаги с другими интересующими вас продуктами.

Если вы хотите снова просмотреть исправления для всех продуктов, нажмите кнопку **Показать все исправления** в верхней части левой панели.

Фильтрация патчей по утилите

Исправление становится ненужным, если, например, оно само или более новая версия уже развернуты в конечной точке. Поскольку инвентарь может в какой-то момент содержать такие патчи, GravityZone позволяет вам их игнорировать. Выберите эти исправления, а затем нажмите кнопку **Игнорировать исправления** в верхней части таблицы.

Control Center отображает пропущенные патчи в другом виде. Нажмите кнопку **Управляемый / Пропущенный** справа от Панели инструментов действий, чтобы переключаться между представлениями:

- - чтобы увидеть пропущенные исправления.
- - чтобы увидеть управляемые исправления.

Фильтрация исправлений по деталям

Используйте возможности поиска для фильтрации исправлений по определенным критериям или после известных деталей. Введите условия поиска в поля поиска в верхней части таблицы исправлений. Совпадающие исправления отображаются в таблице по мере ввода или после выбора.

Очистка поля поиска сбрасывает поиск.

6.6.3. Игнорирование исправлений

Возможно, вам придется исключить некоторые исправления из инвентаря исправлений, если вы не планируете устанавливать их на свои конечные точки, с помощью команды **Игнорировать исправления**.

Игнорируемое исправление будет исключено из задач автоматического исправления и отчетов о исправлении и не будет считаться отсутствующим исправлением.

Чтобы игнорировать исправление:

1. НА странице **Инвентарь исправлений** выберите одно или несколько исправлений, которые вы хотите игнорировать.
2. Нажмите кнопку **Игнорировать патчи** в верхней части таблицы.

   Появится окно конфигурации, где вы можете просмотреть сведения о выбранных исправлениях, а также любые подчиненные исправления.
3. Нажмите **Игнорировать**. Исправление будет удалено из списка инвентаря исправлений.

Вы можете найти пропущенные исправления в отдельном формате и выполнить действия над ними:

- Нажмите кнопку **Показать пропущенные исправления** в правой верхней части таблицы. Вы увидите список всех пропущенных исправлений.
- Вы можете получить больше информации об отдельном пропущенном исправлении, сгенерировав статистический отчет исправлений. Выберите нужное вам исправление и нажмите кнопку **Статистика исправлений** в верхней части таблицы. Дополнительные сведения см. в разделе «Создание статистики исправлений» (p. 222)
- Чтобы восстановить пропущенные исправления, выберите их и нажмите кнопку **Восстановить исправления** в верхней части таблицы.

  Появится окно конфигурации, где вы можете просмотреть подробную информацию о выбранных исправлениях.

  Нажмите кнопку **Восстановить** чтобы отправить исправление в инвентарь.

6.6.4. Установка патчей

Чтобы установить исправления из инвентаря:

1. Перейдите в раздел **Сеть> Инвентарь исправлений**.
2. Найдите исправления, которые вы хотите установить. Если необходимо, отфильтруйте их для быстрого поиска
3. Выберите исправления и нажмите кнопку **Установить** в верхней части таблицы. Появится окно конфигурации, где вы можете редактировать детали установки исправления.

   Вы увидите выбранные исправления вместе с любыми подчиненными исправлениями.

   - Выберите целевую группу конечных точек.
   - **При необходимости перезагрузите конечные точки после установки патча**. Эта опция перезапустит конечные точки сразу после установки исправлений, если потребуется перезагрузка системы. Учтите, что это действие может прервать сеанс пользователя.

     Если этот параметр отключен, это означает, что, если требуется перезагрузка системы на целевых конечных точках, они будут отображать значок состояния ожидающего перезапуска в сетевой инвентаризации GravityZone. В этом случае вам доступны следующие варианты:

     – Отправить задачу **Перезагрузить компьютер** ожидающим конечным точкам перезапуска в любое время по вашему выбору. Дополнительные сведения см. в разделе «Перезагрузка машины» (p. 108).

     – Настроить активную политику, чтобы уведомить пользователя конечной точки о необходимости перезагрузки. Для этого перейдите к активной политике на целевой конечной точке, перейдите в раздел **Общие > Уведомления** и включите параметр **Уведомление о перезапуске конечной точки**. В этом случае пользователь будет получать всплывающее окно каждый раз, когда требуется перезапуск из-за изменений, внесенных указанными компонентами GravityZone (в данном случае, Управление исправлениями). Всплывающее окно предоставляет возможность отложить перезагрузку. Если пользователь выбирает отложить, то уведомления перезагрузки будут периодически появляться на экране до тех пор пока пользователь не перезагрузит систему, или пока не истечет назначенное администратором компании время.

Дополнительные сведения см. в разделе «Уведомление о перезапуске конечной точки» (p. 261).

4. Щелкните **Установить**.

   Задача установки создается вместе с подзадачами для каждой целевой конечной точки.

Примечание

- Вы также можете установить исправление со страницы **Сеть**, начиная с определенных конечных точек, которыми вы хотите управлять. В этом случае выберите конечные точки из инвентаризации сети, нажмите **Задачи** нажмите в верхней части таблицы и выберите **Установка исправлений**. Для получения более подробной информации, обратитесь к «Установка патча» (p. 90).
- После установки исправления мы рекомендуем отправить задачу Сканировать исправления конечным точкам. Это действие обновит информацию об исправлении, сохраненную в GravityZone для ваших управляемых сетей.

6.6.5. Удаление патчей

Возможно, вам придется удалить исправления, которые вызвали сбои в работе конечных точек. GravityZone предоставляет функцию отката для исправлений, установленных в вашей сети, которая восстанавливает программное обеспечение до его предыдущего состояния перед применением исправления.

Функция удаления доступна только для сменных исправлений. Инвентаризация исправлений GravityZone включает в себя столбец **Удаляемые**, где вы можете фильтровать исправления по степени их удаляемости.

Примечание

Атрибут съемности зависит от того, каким образом исправление было выпущено производителем или от изменений, внесенных исправлением в программное обеспечение. Для исправлений, которые невозможно удалить, вам может понадобиться переустановить ПО.

Чтобы удалить исправление:

1. Перейдите в раздел **Сеть> Инвентарь исправлений**.

2. Выберите исправление, которое вы хотите удалить. Для поиска определенного исправления используйте фильтры, доступные в столбцах, например номер КБ или CVE. Используйте колонку **Удаляемые** чтобы отобразить только те исправления, которые можно удалить.

   Примечание
   Вы можете удалить одновременно только одно исправление для одной конечной точки или нескольких сразу.

3. Нажмите кнопку **Удалить** в верхней части таблицы. Появится окно конфигурации, в котором вы можете редактировать детали задачи удаления.

   - **Название задачи:**. Вы можете изменить имя по умолчанию для задачи удаления исправления, если хотите. Таким образом, вы легче определите задачу на странице **Задачи** .
   - **Добавить патч в список пропущенных патчей**. Обычно вам больше не понадобится исправление, которое вы хотите удалить. Этот параметр автоматически добавляет исправление в список игнорируемых после удаления исправления.
   - **При необходимости перезагрузите конечные точки после удаления патча**. Эта опция перезапустит конечные точки сразу после удаления исправления, если потребуется перезагрузка системы. Учтите, что это действие может прервать сеанс пользователя.

     Если этот параметр отключен, это означает, что, если требуется перезагрузка системы на целевых конечных точках, они будут отображать значок состояния ожидающего перезапуска в сетевой инвентаризации GravityZone. В этом случае вам доступны следующие варианты:

     – Отправить задачу **Перезагрузить компьютер** ожидающим конечным точкам перезапуска в любое время по вашему выбору. Дополнительные сведения см. в разделе «Перезагрузка машины» (p. 108).

     – Настроить активную политику, чтобы уведомить пользователя конечной точки о необходимости перезагрузки. Для этого перейдите к активной политике на целевой конечной точке, перейдите в раздел **Общие > Уведомления** и включите параметр **Уведомление о**

перезапуске конечной точки. В этом случае пользователь будет получать всплывающее окно каждый раз, когда требуется перезапуск из-за изменений, внесенных указанными компонентами GravityZone (в данном случае, Управление исправлениями). Всплывающее окно предоставляет возможность отложить перезагрузку. Если пользователь выбирает отложить, то уведомления перезагрузки будут периодически появляться на экране до тех пор пока пользователь не перезагрузит систему, или пока не истечет назначенное администратором компании время.

Дополнительные сведения см. в разделе «Уведомление о перезапуске конечной точки» (p. 261).

- В таблице **Цели отката** выберите конечные точки, на которых вы хотите удалить исправление.

  Вы можете выбрать одну или несколько конечных точек в вашей сети. Используйте доступные фильтры, чтобы найти конечную точку, которую вы хотите.

  Примечание
  В таблице отображаются только те конечные точки, где установлено выбранное исправление.

4. Нажмите **Подтвердить**. Задача **Удаление исправлений** будет создана и отправлена на целевые конечные точки.

   Отчет **Удаление исправления** автоматически создается для каждой завершенной задачи удаления исправления, предоставляя сведения об исправлении, конечных точках назначения и состоянии задачи удаления исправления.

Примечание
После удаления исправления мы рекомендуем отправлять на целевые конечные точки задачу Сканировать исправления. Это действие обновит информацию об исправлении, сохраненную в GravityZone для ваших управляемых сетей.

6.6.6. Создание статистики исправлений

Если вам нужны подробности о состоянии определенного исправления для всех конечных точек, используйте функцию **Статистика исправлений**, которая генерирует мгновенный отчет для выбранного исправления:

1. На странице **Инвентарь исправления** выберите нужное вам исправление из правой панели.
2. Нажмите кнопку **Статистика исправлений** в верхней части таблицы.

   Отображается отчет о статистике исправлений, предоставляющий различные сведения о состоянии исправлений, в том числе:

   - Круговая диаграмма, показывающая процентное соотношение установленного, неудачного, отсутствующего и ожидающего состояния исправления для конечных точек, сообщивших о исправлении.
   - Таблица, отражающая следующую информацию:
     - **Имя**, **полное доменное имя**, **IP** и **ОС** каждой конечной точки, которая сообщила об исправлении.
     - **Последняя проверка**: время, когда исправление проверялось последний раз на конечной точке.
     - **Статус исправления**: установлен, не выполнен, отсутствует или игнорируется.

Примечание
Функциональность статистики исправлений доступна как для управляемых, так и для игнорируемых исправлений.

6.7. Просмотр и управление задачами

Страница **Сеть > Задачи** позволяет просматривать и управлять всеми задачами, которые вы создали.

После того как вы создали задачу хотя бы для одного сетевого объекта, вы можете просмотреть ее в таблице задач.

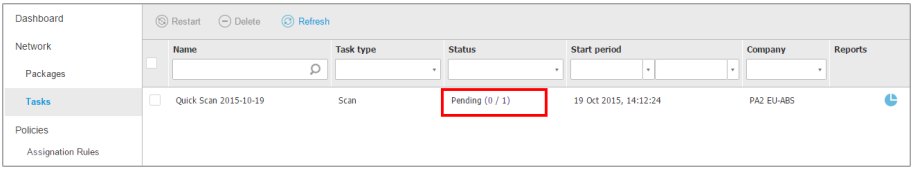
Вы можете выполнить следующие задачи в разделе **Сеть > Задачи**:

- Проверить статус задачи
- Просмотреть отчеты задач
- Перезапустить задачи
- Остановить задачи сканирования Exchange
- Удалить задачи

6.7.1. Проверить статус задачи

Каждый раз, когда вы создаете задачу для одного или нескольких сетевых объектов, вы можете проверить ход выполнения задачи и получить уведомления, когда происходят ошибки.

Перейдите в раздел **Сеть > Задачи** и проверьте колонку **Статус** для каждой интересующей вас задачи. Вы можете проверить статус основной задачи, а также получить подробную информацию о каждой подзадаче.



Страница задач

- **Проверка статуса основной задачи**.

  Основная задача относится к действиям, запущенным на сетевых объектах (например, установка клиента или сканирование) и содержит определенное количество подзадач, по одной для каждого выбранного сетевого объекта. Например, основная задача установки клиента, созданная для восьми компьютеров, содержит восемь подзадач. Цифры в скобках показывают соотношение завершенных задач к общему количеству. Например, (2/8) означает, что две из восьми подзадач закончены.

  Статус основной задачи может быть следующим:
  - **В стадии ожидания**, когда ни одна из подзадач еще не началась или когда лимит количества одновременных развертываний превышен. Максимальное количество одновременных развертываний можно установить в меню **Настройки**. Для получения более подробной информации, обратитесь к руководству по установке GravityZone.
  - **Выполняется**, когда все подзадачи выполняются. Основная задача будет находится со статусом "Выполняется" пока последняя подзадача не будет выполнена.
  - **Завершена**, когда все подзадачи (удачно или неудачно) завершены. В случае неудачного выполнения подзадач, отобразится предупреждающий символ.

- **Проверка статуса подзадач**.

Перейдите к интересующей вас задаче и нажмите на ссылку в колонке **Статус**, чтобы открыть окно **Статус**. Вы можете просмотреть список сетевых объектов с запущенной главной задачей и статус соответствующих подзадач. Статус подзадачи может быть следующим:

– **Выполняется,** если подзадача еще выполняется.

  Для Exchange, вы также можете просмотреть статус завершения задач сканирования по запросу.

– **Завершена**, если подзадача успешно завершена.

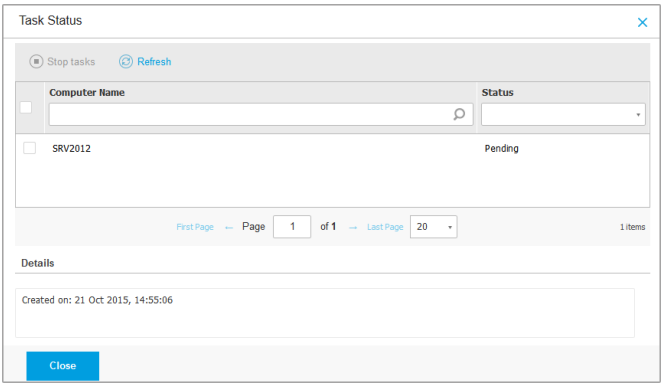
– **Ожидание**, если выполнение подзадачи еще не начато. Это может случится в следующих ситуациях:

  - Подзадача ожидает очереди.
  - Существует проблема подключения между Control Center и выбранным сетевым объектом.
  - Выбранное устройство не работает (офлайн, в случае с мобильными устройствами). Задача запустится на выбранном устройстве, как только оно станет онлайн.

– **Провалена**, если подзадача не может быть запущена или она остановлена из-за ошибок, таких как неверные учетные данные для аутентификации и нехватка памяти.

– **Остановка**, когда сканирование по запросу занимает слишком много времени и вы решили его остановить.

Для просмотра сведений о каждой подзадаче, выберите ее и проверьте раздел **Подробности** в нижней части таблицы.



Подробная информация о статусах задач

Вы сможете получить следующую информацию:

– Дата и время, когда задача была запущена.
– Дата и время, когда задача была завершена.
– Описание встречающихся ошибок.

6.7.2. Просмотр отчетов задач

На странице **Сеть > Задачи** у вас есть возможность просмотреть отчеты задач быстрого сканирования.

1. Перейдите на страницу **Сеть > Задачи**.
2. Выберите нужный сетевой объект из меню видов сетей.
3. Установите флажок на интересующей вас задаче сканирования.
4. Нажмите соответствующую кнопку в колонке **Отчеты**. Дождитесь отображения отчета. Для получения более подробной информации, обратитесь к «Использование отчетов» (p. 512).

6.7.3. Перезапуск задач

По различным причинам задачи установки клиента, удаления или обновления могут быть не завершены. В таких случаях, вы можете перезапустить эти задачи вместо создания новых, выполнив следующие шаги:

1. Перейдите на страницу **Сеть > Задачи**.

2. Выберите нужный сетевой объект из меню видов сетей.
3. Установите флажки на требуемых незавершенных задачах.
4. Нажмите кнопку **Перезапуск** в верхней части таблицы. Выбранные задачи будут перезапущены и их статус изменится на **Повторение**.

Примечание
Для задач с несколькими подзадачами, задача **Перезапуск** станет доступна только тогда, когда все подзадачи будут завершены, а перезапущены будут только незавершенные подзадачи.

6.7.4. Остановка задач сканирования Exchange

Сканирование хранилища Exchange может занимать длительное время. Если по каким-либо причинам вы хотите остановить задачу сканирования Exchange по запросу, выполните следующие шаги:

1. Перейдите на страницу **Сеть > Задачи**.
2. Выберите нужный вид сети из меню видов сетей.
3. Нажмите на ссылку в колонке **Статус**, чтобы открыть окно **Статус задачи**.
4. Установите флажок на соответствующих отложенных или запущенных подзадачах, которые вы хотите остановить.
5. Нажмите кнопку **Остановить задачи** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

Примечание
Вы также можете остановить сканирование хранилища Exchange по запросу из области событий Bitdefender Endpoint Security Tools.

6.7.5. Удаление задач

GravityZone автоматически удаляет ожидающие задачи через два дня и завершает задачи через 30 дней. Если у вас по-прежнему много задач, рекомендуется удалить задачи, которые вам больше не нужны, чтобы предотвратить засорение списка.

1. Перейдите на страницу **Сеть > Задачи**.
2. Выберите нужный сетевой объект из меню видов сетей.

3. Установите флажок на соответствующей задаче, которую вы хотите удалить.
4. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

Предупреждение
Удаление отложенного задания, также отменит и само задание.
Если задача в процессе выполнения, ее удаление отменит и все подзадачи, находящиеся в режиме ожидания. Все завершенные подзадачи отменены быть не могут.

6.8. Удаление конечных точек из сетевого содержимого

Инвентаризация сети включает, по умолчанию, папку **Удаленные**, предназначенную для хранения конечных точек, которыми вы больше не хотите управлять.

Действие **Удалить** имеет следующие последствия:

- Когда неуправляемые конечные точки удаляются, они перемещаются непосредственно в папку **Удаленные**.
- Когда управляемые конечные точки удалены:
  - Задача удаления клиента создана
  - Лицензионное место освобождено
  - Конечные точки перемещены в папку **Удаленные**

Чтобы удалить конечные точки из инвентаризации сети:

1. Перейдите в раздел **Сеть**.
2. Выберите требуемый вид сети из меню видов сетей.
3. Выберите **Пользовательские группы** в левой панели. Все доступных конечные точки в этой группе отобразятся в таблице правой панели.

Примечание
Вы можете удалять только конечные точки, отображаемые в **Custom Groups**, которые были обнаружены за пределами любой интегрированной сетевой инфраструктуры.

4. Установите в правой панели флажок напротив конечной точки, которую хотите удалить.
5. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

   Если удаленная конечная точка управляется, задача **Удалить клиент** будет создана на странице **Задачи**, а агент безопасности будет удален из конечной точки, освобождая одно лицензионное место.
6. Конечная точка перемещена в папку **Удаленные**.

Вы можете в любое время переместить конечные точки из папки **Удаленные** в **Пользовательские группы** , используя перетаскивание.

Примечание

- Если вы хотите навсегда исключить определенные конечные точки из управления, вы должны сохранить их в папке **Удаленные**.
- Если вы удалите конечные точки из папки **Удаленные**, они будут полностью удалены из базы данных GravityZone. Тем не менее исключенные конечные точки, которые находятся в сети, будут обнаружены при следующей задаче обнаружения сети, и они будут отображаться в инвентаризации сети как новые конечные точки.

6.9. Настройка параметров сети

На странице **Настройки > Настройки сети** вы можете настроить параметры инвентаризации сети, такие как: сохранение фильтров, сохранение последнего просмотренного местоположения, создание и управление запланированными правилами удаления неиспользуемых виртуальных машин.

Настройки объединены в следующие разделы:

- Настройки инвентаризации сети
- Автономное удаление машин

6.9.1. Настройки инвентаризации сети

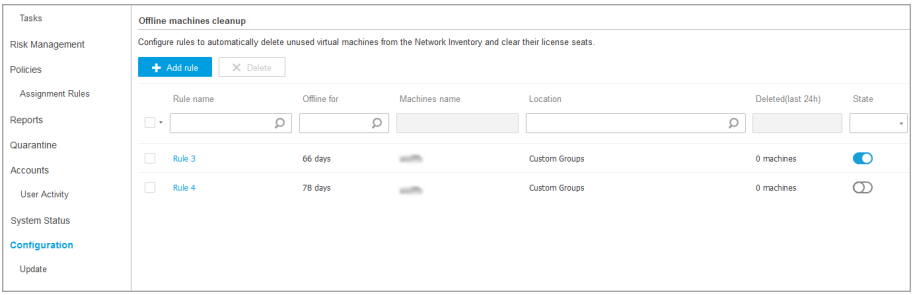
В разделе **Настройки инвентаризации сети** доступны следующие параметры:

- **Сохранить фильтры инвентаризации сети**. Установите этот флажок, чтобы сохранить ваши фильтры на странице **Сеть** между сеансами Control Center.

- **Запомнить последнее просмотренное местоположение в инвентаризации сети (Network Inventory), пока я не выйду из системы**. Установите этот флажок, чтобы сохранить последнее местоположение, к которому вы обращались при выходе со страницы **Сеть**. Местоположение между сессиями не сохраняется.
- **Избегайте дублирования клонированных конечных точек**. Выберите эту опцию, чтобы включить новый тип сетевых объектов в GravityZone, называемых золотыми образом. Таким образом, вы можете различать исходные конечные точки от их клонов. Далее необходимо пометить каждую конечную точку, которую вы клонируете, следующим образом:
  1. Перейдите в раздел **Сеть**.
  2. Выберите конечную точку, которую вы хотите клонировать.
  3. В контекстном меню выберите **Пометить как Золотое изображение**.

6.9.2. Автономное удаление машин

В разделе **Очистка автономных компьютеров** вы можете запланировать правила автоматического удаления неиспользуемых виртуальных машин из инвентаризации сети.



Настройки - Настройки сети - Автономное удаление машин

Создание правил

Для создания правила удаления:

1. В разделе **Автономная уборка машин** нажмите кнопку **Добавить правило**.
2. На странице конфигурации:

a. Введите имя правила.

b. Выберите час для ежедневного удаления.

c. Определите критерии удаления:

- Количество дней, в течение которых машины были отключены (от 1 до 90).
- Шаблон имени, который может применяться к одной виртуальной машине или к нескольким виртуальным машинам.

  Например, используйте `machine_1`, чтобы удалить машину с этим именем. Либо добавьте `machine_*`, чтобы удалить все машины, имя которых начинается с `machine_`.

  Это поле чувствительно к регистру и принимает только буквы, цифры и специальные символы звездочка (*), подчеркивание (_) и дефис (-). Имя не может начинаться со звездочки (*).

d. Выберите целевые группы конечных точек в Инвентаризации сети, где применить правило.

3. Нажмите **Сохранить**.

Просмотр и управление правилами

В разделе **Настройки сети > Очистка автономных компьютеров** отображаются все созданные вами правила. Выделенная таблица содержит следующую информацию:

- Имя правила.
- Количество дней, прошедших с тех пор, как машины отключились.
- Шаблоны имен машин.
- Расположение в инвентаризации сети.
- Количество удаленных машин за последние 24 часа.
- Состояние: включено, отключено или недействительно.

Примечание
Правило является недействительным, если цели больше не действительны по определенным причинам. Например, виртуальные машины были удалены или у вас больше нет к ним доступа.

Вновь созданное правило включено по умолчанию. Вы можете в любое время включать и отключать правила, используя переключатель «Вкл/Выкл» в столбце **Состояние**.

При необходимости используйте параметры сортировки и фильтрации в верхней части таблицы, чтобы найти конкретные правила.

Чтобы изменить правило:

1. Нажмите на название правила.
2. На странице конфигурации редактируйте детали правила.
3. Нажмите **Сохранить**.

Чтобы удалить одно или несколько правил:

1. Используйте флажки, чтобы выбрать одно или несколько правил.
2. Нажмите кнопку **Удалить** в верхней части таблицы.

6.10. Конфигурация настроек Security Server

Security Server использует свой механизм кэширования для дедупликации сканирования против зловредных действий, оптимизируя данный процесс. Оптимизация сканирования предназначена для разделения кэша с другим Security Server

Совместное использование кэша работает только между однотипными Security Servers. Например,Security Server Мультиплатформа будет разделять кэш лишь с Security Server Мультиплатформой и не с Security Server для NSX.

Осуществление разделения кэша:

1. Перейдите к **Конфигурации > Security Server настройки страницы**
2. Select the **Security Server Cache Sharing** check box.
3. Выберете диапазон разделения:
   - Доступно для Security Server

     Рекомендуется использовать данную функцию, если всеSecurity Server находятся в одной сети.
   - Security Server доступен в списке задач.

Используйте данную функцию, когда Security Server распространяется на ряд работ в сети, и разделение кэша может способствовать большому объему трафика.

4. При ограничении диапазона создайте группу Security Server Выберете Security Server из раскрывающегося списка и нажмите **Add**.

   ЛишьSecurity Serverиз таблицы будет заниматься разделением своего кэша.

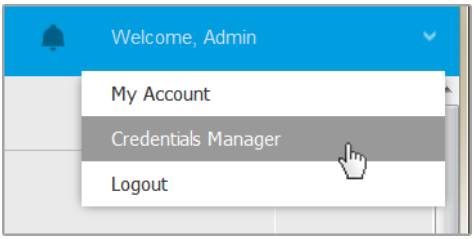
   Примечание
   Security Server для NSX-T и NSX-V обмена данных кэша только в одном сервере vCenter.

5. Нажмите **Сохранить**.

6.11. Диспетчер учетных данных (Credentials Manager)

Диспетчер учетных данных поможет вам определить учетные данные, необходимые для доступа к имеющимся ресурсам vCenter Server, а также для удаленной аутентификации в различных операционных системах вашей сети.

Чтобы открыть диспетчер учетных данных, нажмите на имя пользователя в правом верхнем углу страницы и выберите **Диспетчер учетных данных**.



Меню диспетчера учетных данных

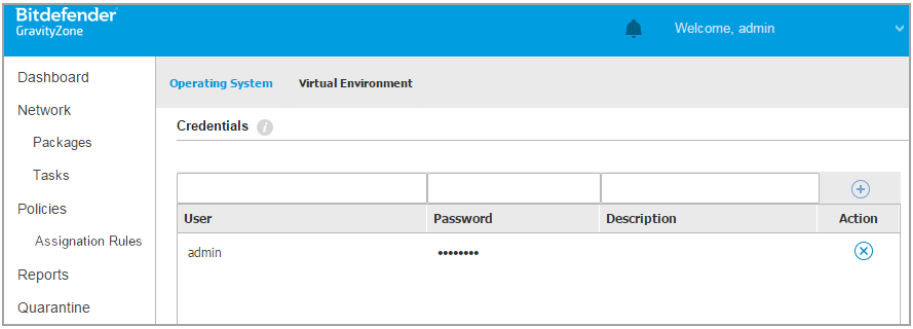
Окно **Диспетчер учетных данных** содержит две вкладки:

- Операционная система
- Виртуальная среда

6.11.1. Операционная система

На вкладке **Operating System**, вы можете управлять учетными данными администратора, необходимыми для удаленной аутентификации во время установки, отправки задач для компьютеров и виртуальных машин в вашей сети.

Чтобы добавить набор учетных данных:



Диспетчер учетных данных (Credentials Manager)

1. Введите имя пользователя и пароль учетной записи администратора для каждой требуемой операционной системы в соответствующих полях в верхней части над заголовком таблицы. При желании, вы можете добавить описание, которое поможет вам проще определить каждый аккаунт. Если компьютеры находятся в домене, достаточно ввести учетные данные администратора домена.

   Используйте правила именования Windows при вводе имени учетной записи:

   - Для машин из службы каталогов Active Directory используйте следующий синтаксис: `username@domain.com` и `domain\username`. Чтобы быть уверенным, что введенные учетные данные будут работать, добавьте их в обоих видах (`username@domain.com` и `domain\username`).
   - Для машин из рабочей группы достаточно ввести только имя пользователя без имени рабочей группы.

2. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Новый набор учетных данных будет добавлен в таблицу.

> **Примечание**
> Если вы не указали учетные данные, вам будет необходимо ввести их при запуске задачи установки. Указанные учетные данные автоматически сохраняются в диспетчере учетных данных, так что вам не придется вводить их в следующий раз.

6.11.2. Виртуальная среда

На вкладке Virtual Environment вы можете управлять учетными данными для доступных виртуальных серверных систем.

Для доступа к виртуальной инфраструктуре, интегрированной с Control Center, вы должны указать свои учетные данные для каждой доступной серверной системы. Control Center использует ваши учетные данные для подключения к виртуальной инфраструктуре, отображая только те ресурсы, к которым у вас есть доступ (задается на виртуальном сервере).

Чтобы задать учетные данные, необходимые для подключения к виртуальному серверу:

1. Выберите сервер из соответствующего меню.

> **Примечание**
> Если меню недоступно, значит интеграция еще не была выполнена или все необходимые учетные данные уже настроены.

2. Введите имя пользователя, пароль и подходящее описание.
3. Нажмите кнопку ⊕ **Добавить**. Новый набор учетных данных будет добавлен в таблицу.

> **Примечание**
> Если вы не настроили учетные данные в диспетчере учетных данных, вам будет необходимо ввести их, когда вы будете пытаться просмотреть ресурсы любой виртуализованной серверной системы. Единожды введя ваши учетные данные, они будут сохранены в вашем менеджере учетных данных и вам не придется вводить их повторно в дельнейшем.

Важно
Всякий раз, когда вы изменяете свой пароль пользователя виртуального сервера, не забудьте также обновить его в диспетчере учетных данных.

6.11.3. Удаление учетных данных из диспетчера учетных данных

Чтобы удалить устаревшие учетные данные из диспетчера учетных данных:

1. Нажмите на строку таблицы, содержащую учетные данные, которые вы хотите удалить.
2. Нажмите кнопку ⊗ **Удалить** с правой стороны соответствующей строки таблицы. Выбранный аккаунт будет удален.

7. ПОЛИТИКИ БЕЗОПАСНОСТИ (SECURITY POLICIES)

После установки, защита Bitdefender может быть настроена и управляться из Control Center с помощью политик безопасности. Политика определяет параметры безопасности, которые должны применяться к определенным объектам сетевого содержимого (компьютеры, виртуальные машины или мобильные устройства).

Сразу же после установки, объектам инвентаризации сети присваиваются политики по умолчанию, которые предварительно сконфигурированы с рекомендованными настройками защиты. При условии, что интеграция с NSX включена, по умолчанию доступно еще три политики безопасности для NSX, по одной для каждого уровня безопасности: рекомендуемый, нормальный и интенсивный. Эти правила предварительно сконфигурированы с рекомендуемыми параметрами защиты. Вы не можете изменить или удалить политики по умолчанию.

Вы можете создать столько политик, сколько вам нужно, на основе требований безопасности для каждого типа управляемого объекта сети.

Вот то, что вам нужно знать о политиках:

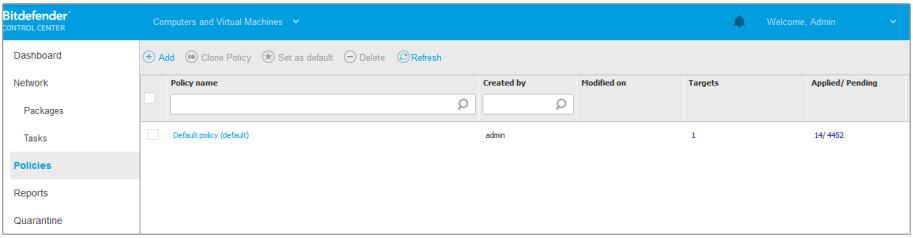
- Политики создаются на странице **Политики** и назначаются сетевым объектам в разделе **Сеть**.
- Политики могут наследовать некоторые настройки модулей из других политик.
- Вы можете настроить назначение политик для конечных точек таким образом, что политика сможет применяться только при определенных условиях - на основании местоположения или зашедшего пользователя. Таким образом, конечная точка может иметь больше назначаемых политик.
- Конечные точки могут иметь одну активную политику одновременно.
- Вы можете назначить политику отдельным конечным точкам или группам конечных точек. При назначении политики также должны быть определены параметры наследования политики. По умолчанию каждая конечная точка наследует политику родительской группы.
- Политики отправляются объектам сети сразу после их создания или модификации. Настройки будут применены к объектам сети менее, чем за минуту (при условии, что они онлайн). Если объект сети не онлайн, настройки будут применены как только он станет онлайн.
- Политика применяется только к установленным модулям защиты.
- Страница **Политики** отображает только следующие виды политик:

  - Политики, созданные вами.
  - Другие политики (например, политики по умолчанию или шаблоны, созданные другими пользователями), которые назначаются конечным точкам под вашей учетной записью.
- Вы не можете редактировать политики, созданные другими пользователями (если владельцы политик не позволяют этого в настройках политики), но вы можете отменить их, назначив требуемым объектам иную политику.

Предупреждение
Только поддерживаемые модули политик будут применяться к требуемым конечным точкам.
Пожалуйста, обратите внимание, что только модуль защиты от вредоносных программ поддерживается серверными операционными системами.

7.1. Управление политиками

Вы можете просматривать и управлять политиками на странице **Политики**.



Страница политик

Каждый тип конечной точки имеет определенные параметры политик. Для управления политиками, вы должны сначала выбрать тип конечной точки (**Компьютеры и виртуальные машины** или **Мобильные устройства**) из меню видов сетей.

Существующие политики отобразятся в таблице. По каждой политике вы можете посмотреть:

- Имя политики.
- Пользователя, который создал политику.
- Дату и время последнего изменения политики.

- Количество объектов, которым назначена политика.*
- Количество устройств, на которых политика была применена / в процессе выполнения.*

Для политик с включенным модулем NSX, доступна дополнительная информация:

- Имя политики NSX используется для идентификации политики Bitdefender в VMware VSphere.
- Видимость политики в консоли управления позволяет вам фильтровать политики для NSX. Таким образом, если политики **Локальные** видны только вBitdefender Control Center, то политики **Глобальные** также видны и в VMware NSX.

Эти детали скрыты по умолчанию.

Для детальной настройки политики, отображаемой в таблице:

1. Нажмите кнопку **Колонки** справа от Панель действий
2. Выберите столбцы, которые вы хотите отобразить.
3. Нажмите кнопку **Восстановить**, чтобы вернуться к виду столбцов по умолчанию.

* При нажатии на цифру произойдет перенаправление на страницу **Network**, где вы можете просмотреть соответствующие конечные точки. Вам будет предложено выбрать вид сети. Это действие создаст фильтр с помощью критериев политики.

Вы можете сортировать доступные политики, а также осуществлять поиск определенной политики, используя доступные критерии.

7.1.1. Создание политик

Вы можете создавать политики либо путем добавления новой или дублирования (клонирования) существующей политики.

Для создания политики безопасности:

1. Перейдите на страницу **Политики**.
2. Выберите требуемый тип конечной точки из меню видов сетей.
3. Выберите способ создания политики:
   - **Добавить новую политику**.

  – Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Эта команда создает новую политику, начиная с шаблона политики по умолчанию.

- **Копировать существующие политики**.
  a. Установите флажок на политике, которую вы хотите продублировать.
  b. Нажмите кнопку **Копировать** в верхней части таблицы.

4. Настройте параметры политики. Для получения более подробной информации, обратитесь к:
   - «Политики компьютеров и виртуальных машин» (p. 254)
   - «Политики мобильных устройств» (p. 425)
5. Нажмите **Сохранить**, чтобы создать политику и вернуться к списку политик.

При определении политики для использования в VMware NSX, помимо настройки параметров защиты от вредоносных программ в GravityZone Control Center, также необходимо создать политику в NSX, тем самым дав ей понять использовать политики GravityZone в качестве профиля службы. Для создания политики безопасности NSX:

1. Войдите в веб-клиент vSphere.
2. Перейдите на вкладку **Сеть & Безопасность > Сервисный Композитор > Политики безопасности**.
3. Нажмите на кнопку **Создать политику безопасности** в верхней части панели инструментов таблицы политик. Появится окно конфигурации.
4. Введите имя политики и нажмите кнопку **Далее**.

   При желании вы можете также добавить краткое описание.
5. Нажмите кнопку **Добавить гостевую службу самоанализа** в верхней части таблицы. Откроется окно конфигурации службы Guest Introspection.
6. Введите имя и описание службы.
7. Оставьте выбранное действие по умолчанию, чтобы позволить Bitdefender применить профиль службы к группе безопасности.
8. Из меню **Название сервиса** выберите **Bitdefender**.
9. Из меню **Сервисный профиль** выберите существующую политику GravityZone.
10. Оставьте значения по умолчанию в опциях **Состояние** и **Принудительно**.

Примечание
Для получения дополнительной информации о параметрах политики безопасности, обратитесь к документации по VMware NSX.

11. Нажмите **OK**, чтобы добавить службу.
12. Нажимайте **Далее** до последнего шага, а затем нажмите кнопку **Завершить**.

7.1.2. Назначение политик

Конечным точкам первоначально назначена политика по умолчанию. После того, как вы создали необходимую политику на странице **Policies**, вы можете назначить ее конечным точкам.

Процесс назначения политики зависит от различных сред с которыми интегрирован GravityZone. Для некоторых интегрированных сред, таких как VMware NSX, политики доступны за пределами GravityZone Control Center. Они также относятся к внешним политикам.

Назначение локальных политик

Вы можете назначить локальную политику двумя способами:

- Назначение на основе устройства, означает ручной выбор конечных точек, которым вы назначите политику. Эти политики также известны, как политики устройств.
- Назначение на основе правил, означает, что политика назначается управляемой конечной точке, сетевые настройки которой соответствуют заданным условиям существующего правила присвоения.

Примечание

- Вы можете назначить только те политики, которые были созданы вами. Чтобы назначить политику, созданную другим пользователем, вы должны ее сначала клонировать в разделе **Политики**.
- На виртуальных машинах, защищенных только HVI, вы можете назначать только политики устройств. Если на них также установлен Bitdefender Endpoint Security Tools, вы также можете назначать политики на основе правил, в таком случае агент безопасности управляет активацией политики.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Назначение политик устройств

В GravityZone можно назначать политики несколькими способами:

- Назначить политику непосредственно на цель.
- Назначить политику родительской группы через наследование.
- Принудительное наследование политики.

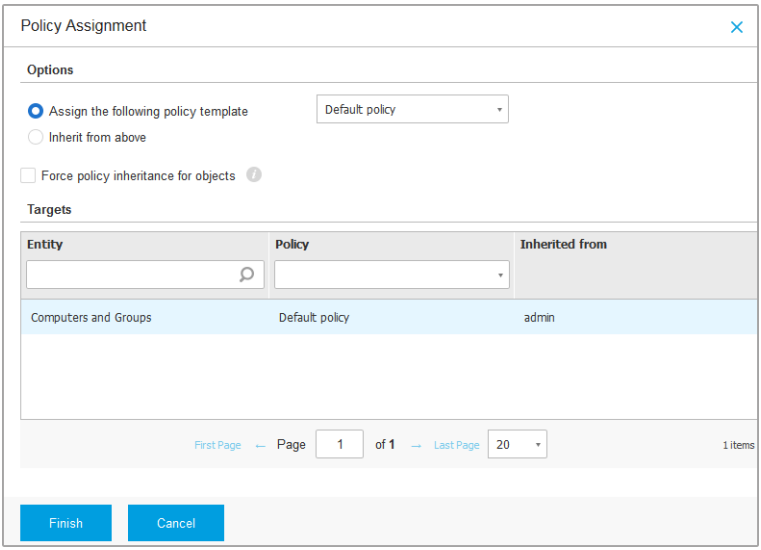
По умолчанию каждая конечная точка или группа конечных точек наследует политику родительской группы. Если вы измените политику родительской группы, будут затронуты все потомки этой группы, кроме тех, у которых есть принудительная политика.

Чтобы назначить политику устройства:

1. Перейдите в раздел **Сеть**.
2. Выберите нужный вид сети из меню видов сетей.
3. Выберите целевые конечные точки Вы можете выбрать одну или несколько конечных точек или групп конечных точек.

   Для целей наследования вы не можете изменить политику корневой группы по умолчанию. Например, **Компьютеры и виртуальные машины** всегда будут иметь назначенную **Политику по умолчанию**.
4. Нажмите кнопку **Назначить политику** в верхней части рабочей области или выберите параметр **Назначить политику** в контекстном меню.

   Страница **Назначение политики** отображается:



Назначение политик

5. Проверьте таблицу с целевыми конечными точками. Для каждой конечной точки вы можете просмотреть:
   - Назначенная политика.
   - Родительская группа, от которой целевой объект наследует политику.

     Если группа применяет политику, вы можете щелкнуть на её имя, чтобы просмотреть страницу **Назначение политики** с этой группой в качестве цели.
   - Статус исполнения.

     Данный статус показывает, принуждает ли данная группа наследование политик дочерним группам, либо сама является принуждаемой.

     Обратите внимание на цели с принудительной политикой (статус **Принудительно**). Данные политики заменить нельзя. В таком случае отображается предупреждение.
6. В случае предупреждения нажмите на ссылку **Исключить эти цели** , чтобы продолжить.

7. Выберите один из доступных вариантов назначения политики:
   - **Назначьте следующий шаблон политики**- назначить конкретную политику непосредственно конечным точкам.
   - **Наследовать по убыванию** - использовать политику родительской группы.
8. Если вы решили назначить шаблон политики:
   a. Выберите политику из выпадающего списка.
   b. Выберите **Принудительное наследование политик дочерним группам** , чтобы добиться следующего:
      - Назначьте политику всем потомкам целевых групп, без исключения.
      - Запретите изменять его из других мест в иерархии.

      В новой таблице представлено рекурсивное отображение всех затронутых конечных точек и их групп, а также политики, которые будут заменены.
9. Нажмите **Завершить**, чтобы сохранить и применить изменения. В противном случае нажмите **Назад** или **Отмена** , чтобы вернуться на предыдущую страницу.

При завершении, политики сразу же направляются к конечным точкам. Настройки на конечных точках вступают в силу менее чем за минуту (при условии, что они онлайн). Если конечная точка не в сети, настройки будут применены, как только она появится в сети.

Для проверки успешного применения политики:

1. На странице **Сеть** щелкните имя интересующей вас конечной точки. Control Center отобразит окно **Информация**.
2. Проверьте раздел **Политика**, чтобы просмотреть статус текущей политики. Должно отображаться как **Применено**.

Другой способ проверить статус назначения - из деталей политики:

1. Перейдите на страницу **Политики**.
2. Найдите политику, которую вы назначили.

   В столбце **Активна/Применена/Ожидает** вы можете просмотреть количество конечных точек для каждого из трех статусов.

3. Нажмите на любую цифру, чтобы просмотреть список конечных точек с соответствующим статусом на странице **Сеть**.

Назначение политик на основе правил

Страница **Политики > правила назначения** позволяет вам задать политику по пользователю и местоположению. Например, вы можете применять более строгие правила файрволла, когда пользователи подключаются к сети Интернет из-за пределов компании или вы можете включить Управление веб-доступом для пользователей, которые не входят в группу администраторов.

Что вам нужно знать о правилах назначения политик:

- Конечные точки могут иметь только одну активную политику одновременно.
- Применяемая политика перезапишет установленную на конечной точке политику устройства.
- Если ни одно из правил назначения не применимо, тогда будет назначена политика устройства.
- Правила упорядочены и обрабатываются по приоритетам, 1 имеет самый высокий приоритет. Вы можете иметь несколько правил для одного объекта. В этом случае будет применяться первое правило, которое соответствует активным настройкам соединения на определенной конечной точке.

  Например, если конечная точка соответствует пользовательскому правилу с приоритетом 4, а правило местонахождения имеет приоритет 3, будет применено правило местонахождения.

Предупреждение
Убедитесь, какие параметры вы считаете чувствительными - исключения, соединения или детальные настройки прокси - при создании правил.
Лучшие практики рекомендуют использовать наследование политик, чтобы сохранять критические параметры политик устройств также в политиках, назначаемых правилами.

Для создания нового правила:

1. Перейдите на страницу **Правила назначения** .
2. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

3. Выберите тип правила:
   - Правило местонахождения
   - Правило для пользователя
   - Правило тегов
4. Настройте нужные параметры правила.
5. Нажмите **Сохранить**, чтобы сохранить изменения и применить правило политики для выбранных конечных точек.

Чтобы изменить параметры существующего правила:

1. На странице **Правила назначения** найдите правило, которое вас интересует и нажмите на него для редактирования.
2. Настройте нужные параметры правила.
3. Нажмите **Сохранить**, чтобы применить изменения и закрыть окно. Чтобы выйти из окна без сохранения изменений, нажмите кнопку **Отменить**.

Если вы больше не хотите использовать правило, выберите правило и нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вам будет предложено подтвердить свои действия, нажатием кнопки **Да**.

Чтобы быть уверенным, что отображается актуальная информация, нажмите кнопку ⟲ **Обновить** в верхней части таблицы.

Настройка правил местоположения

Местонахождение сетевого сегмента определяется одним или несколькими сетевыми параметрами, такими как используемый шлюз, DNS-сервер для разрешения URL-адресов или подсеть IP-адресов. Например, вы можете определить местоположение по сети компании, набору серверов отдела.

В конфигурационном окне правила, выполните следующие действия:

1. Введите подходящее имя и описание правила, которое хотите создать.
2. Установите приоритет правила. Правила отсортированы по приоритетам, правило с приоритетом 1 имеет наивысший приоритет. Одинаковый приоритет не может быть установлен дважды.
3. Выберите политику, для которой вы создаете правило назначения.
4. Задайте местоположения, по которым применяется правило.

a. Выберите тип сетевых настроек из меню в верхней части таблицы месторасположений. Доступны следующие типы:

Тип	Значение
Диапазон IP / IP-адресов	Укажите IP-адреса сети или подсетей. Для подсетей используйте формат CIDR. Например: `10.10.0.12` или `10.10.0.0/16`
Адрес шлюза	IP-адрес шлюза
Адрес сервера WINS	IP-адрес сервера WINS **Важно** Этот параметр не применяется в системах Linux и Mac.
Адрес сервера DNS	IP-адрес сервера DNS
DHCP-суффикс подключения DNS	DNS-имя без имени хоста для конкретного соединения DHCP Например: `hq.company.biz`
Конечная точка может разрешать имена хостов	Имя хоста. Например: `fileserv.company.biz`
Конечная точка может подключиться к GravityZone	Да/Нет
Тип сети	Беспроводное/Ethernet-соединение При выборе беспроводного соединения, вы также можете добавить сетевой идентификатор SSID. **Важно** Этот параметр не применяется в системах Linux и Mac.
Имя хоста	Имя хоста For example: `cmp.bitdefender.com`

Тип	Значение

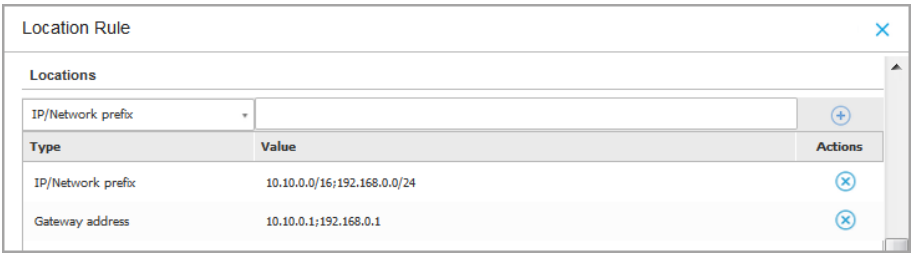
	Важно
	Вы также можете использовать подстановочные символы. Звездочка (*) заменяет ноль или более символов, а знак вопроса (?) заменяет ровно один символ. Примеры:
	`*.bitdefender.com`
	`cmp.bitdefend??.com`

b. Введите значение для выбранного типа. Там, где это применимо, вы можете ввести несколько значений в выделенном поле, разделенных точкой с запятой (;) и без дополнительных пробелов. Например, когда вы вводите `10.10.0.0/16;192.168.0.0/24`, правило будет относится к конечным точкам с IP-адресами, соответствующими любой из этих подсетей.

Предупреждение
Вы можете использовать только один тип сетевых настроек для каждого из правил месторасположения. Например, если вы добавили местоположение с помощью **IP/network prefix**, вы не можете использовать эту же настройку еще раз в этом же правиле.

c. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

Сетевые настройки конечных точек должны полностью соответствовать всем условиям, заданным при определении местоположения, чтобы правило применилось к ним. Например, для идентификации офисной локальной сети можно задать шлюз, тип сети и сервер DNS; кроме того, при добавлении подсети, вы сможете определить отдел в локальной сети компании.



Правило местоположения

Нажмите поле **Значение** для редактирования существующих критериев, а затем нажмите кнопку `Войти`, чтобы сохранить изменения.

Чтобы удалить местоположение, выберите его и нажмите кнопку ⊗ **Удалить**.

5. Вы можете исключить определенные местоположения из правил. Чтобы создать исключение для определенного местоположения, которое будет исключено из правила:

   a. Отметьте чек-бокс **Исключения** в таблице местоположений.

   b. Выберите тип сетевых настроек в меню в верхней части таблицы исключений. Для получения более подробной информации о параметрах, пожалуйста, обратитесь к«Настройка правил местоположения» (p. 246).

   c. Введите значение для выбранного типа. Вы можете ввести несколько значений в выделенном поле, разделенных точкой с запятой (;) без дополнительных пробелов.

   d. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

   Сетевые настройки конечных точек должны полностью соответствовать всем условиям, предусмотренным в таблице исключений, чтобы исключить применение.

   Нажмите поле **Значение** для редактирования существующих критериев, а затем нажмите кнопку `Войти`, чтобы сохранить изменения.

   Чтобы удалить исключение, нажмите кнопку ⊗ **Удалить** в правой части таблицы.

6. Нажмите **Сохранить**, чтобы сохранить правило назначения и применить его.

После создания правила расположения оно автоматически применится ко всем управляемым конечным точкам.

Настройка правила для пользователя

Важно

- Вы можете создать правила для пользователей, только если выполнена интеграция с Active Directory.
- Вы можете создать правила для пользователей только для групп и пользователей из Active Directory. Правила, основанные на группах Active Directory, не поддерживаются в системах Linux.

В конфигурационном окне правила, выполните следующие действия:

1. Введите подходящее имя и описание правила, которое хотите создать.
2. Установка приоритета. Правила отсортированы по приоритетам, правило с приоритетом 1 имеет наивысший приоритет. Одинаковый приоритет не может быть установлен дважды.
3. Выберите политику, для которой вы создаете правило назначения.
4. В разделе **Targets**, выберите требуемых пользователей и группы безопасности, к которым вы хотите применить правило политики. Вы можете увидеть то, что выбрали, в таблице справа.
5. Нажмите **Сохранить**.

   После создания, правило для пользователей применяется к управляемым конечным точкам при входе пользователя в систему.

Настройка правил тегов

Важно

Вы можете создавать правила тегов, только если доступна интеграция с Amazon EC2 или Microsoft Azure.

Вы можете использовать теги, определенные в облачных инфраструктурах, чтобы назначить конкретную политику GravityZone для ваших виртуальных машин, размещенных в облаке. Все виртуальные машины, имеющие теги, указанные в правиле тега, будут применяться с политикой, установленной правилом.

Примечание
В соответствии с облачной инфраструктурой вы можете определить теги виртуальной машины следующим образом:

- Для Amazon EC2: на вкладке **Теги** экземпляра EC2.
- Для Microsoft Azure: в разделе **Обзор** виртуальной машины.

Правило тега может содержать один или несколько тегов. Чтобы создать правило тега:

1. Введите подходящее имя и описание правила, которое хотите создать.
2. Установите приоритет правила. Правила отсортированы по приоритетам, правило с приоритетом 1 имеет наивысший приоритет. Одинаковый приоритет не может быть установлен дважды.
3. Выберите политику, для которой вы создаете правило тега.
4. В таблицу **Тег** добавьте один или несколько тегов.

   Тег состоит из чувствительной к регистру пары ключ-значение. Убедитесь, что вводите теги, которые определены в вашей облачной инфраструктуре. Будут задействованы только действительные пары ключ-значение.

   Чтобы добавить тег:

   a. В поле **Ключ тега** введите имя ключа.
   b. В поле **Значение тега** введите имя значения.
   c. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

Назначение политик NSX

В NSX политики безопасности назначаются группам безопасности. Группа безопасности может содержать различные объекты vCenter, такие как дата-центры, кластеры и виртуальные машины.

Чтобы назначить политику безопасности для группы безопасности:

1. Войдите в веб-клиент vSphere.
2. Перейдите в **Сеть & Безопасность > Сервисный композитор** и нажмите на вкладку **Группы безопасности**.
3. Создайте столько групп безопасности сколько требуется. Для получения дополнительной информации обратитесь к документации VMware.

Вы можете создавать динамические группы безопасности, основанные на тегах безопасности. Таким образом, вы сможете сгруппировать все обнаруженные зараженные виртуальные машины.

4. Щелкните правой кнопкой мыши по требуемой группе безопасности и нажмите **Применить политику**.
5. Выберите применяемую политику и нажмите **OK**.

7.1.3. Изменение настроек политики

Параметры политики можно настроить изначально при ее создании. Позже вы можете изменить их по мере необходимости в любое удобное время.

Примечание
По умолчанию, только пользователь, создавший политику, может изменить ее. Чтобы внести изменения, владелец политики должен выбрать опцию **Разрешить другим пользователям изменять эту политику** на странице политик в разделе **Подробности**.

Чтобы изменить настройки существующей политики:

1. Перейдите на страницу **Политики**.
2. Выберите требуемый тип конечной точки из меню видов сетей.
3. Найдите в списке необходимую политику и нажмите для редактирования на ее имя.
4. Настройте необходимые параметры политики. Для получения более подробной информации, обратитесь к:
   - «Политики компьютеров и виртуальных машин» (p. 254)
   - «Политики мобильных устройств» (p. 425)
5. Нажмите **Сохранить**.

   Политики отправятся объектам сети сразу же после изменения объектов, которым они назначены, или после изменения параметров политик. Настройки будут применены к объектам сети менее чем за минуту (при условии, что они онлайн). Если объект сети не онлайн, настройки будут применены как только он станет онлайн.

7.1.4. Изменение имен политик

Политики должны иметь подходящие имена, чтобы вы или другой администратор могли их быстро и просто идентифицировать.

Чтобы переименовать политику:

1. Перейдите на страницу **Политики**.
2. Выберите требуемый тип конечной точки из меню видов сетей.
3. Нажмите на имя политики. Откроется страница политики.
4. Введите новое имя политики.
5. Нажмите **Сохранить**.

Примечание
Имя политики должно быть уникальным. Вы должны присваивать разные имена для каждой новой политики.

7.1.5. Удаление политик

Если политика вам больше не нужна, удалите ее. После удаления политики, объектам сети, к которым она применялась, будет назначена политика родительской группы. Если никакая другая политика не будет применена, объекту будет назначена политика по умолчанию. При удалении политики с разделами, унаследованными от других политик, настройки унаследованных разделов вернутся к дочерним.

Примечание
По умолчанию, только пользователь, создавший политику, может ее удалить. Чтобы внести изменения, владелец политики должен выбрать опцию **Разрешить другим пользователям изменять эту политику** на странице политик в разделе **Подробности**.

Для того, чтобы иметь возможность удалить политику NSX из GravityZone Control Center, вы должны убедиться, что политика не используется. Поэтому, назначьте выбранной группе другой профиль безопасности. Для получения более подробной информации, обратитесь к «Назначение политик NSX» (p. 251).

Чтобы удалить политику:

1. Перейдите на страницу **Политики**.

2. Выберите требуемый тип конечной точки из меню видов сетей.
3. Установите флажок на политике, которую необходимо удалить.
4. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

7.2. Политики компьютеров и виртуальных машин

Параметры политики можно настроить изначально при ее создании. Позже вы можете изменить их по мере необходимости в любое удобное время.

Чтобы настроить параметры политики:

1. Перейдите на страницу **Политики**.
2. Выберите **компьютеры и виртуальные машины** из меню видов сетей.
3. Нажмите на имя политики. Откроется страница настройки политики.
4. Настройте необходимые параметры политики. Настройки расположены в следующих разделах:
   - Основные
   - HVI
   - Защита от вредоносного ПО
   - Sandbox Analyzer
   - Брандмауэр
   - Защита сети
   - Управление исправлениями
   - Контроль приложений
   - Контроль устройств
   - Ретранслятор
   - Защита Exchange
   - Шифрование
   - NSX
   - Защита хранилища
   - Инциденты Sensor

   Для перемещения по разделам используйте меню в левой части страницы.
5. Нажмите **Сохранить**, чтобы сохранить изменения и применить их на выбранных компьютерах. Чтобы покинуть страницу политик без сохранения изменений, нажмите **Отменить**.

Примечание
Чтобы узнать о работате с политиками, обратитесь к «Управление политиками» (p. 238).

7.2.1. Основные

Общие настройки помогут вам управлять настройками пользовательского интерфейса, парольной защитой, настройками прокси-сервера, настройками привилегированных пользователей, параметрами связи и обновлений для определенных конечных точек.

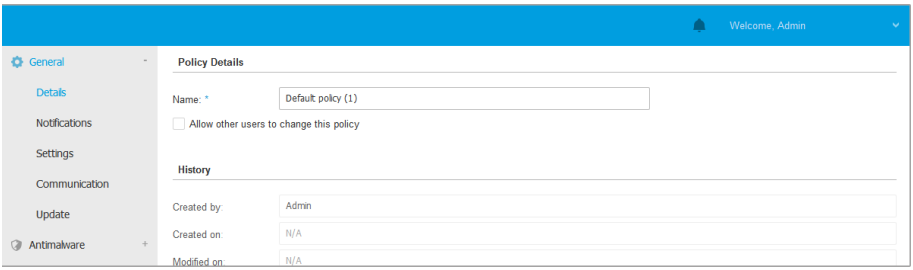
Настройки объединены в следующие разделы:

- Подробная информация
- Уведомления
- Настройки
- Коммуникации
- Обновления

Подробная информация

Страница **Подробности** содержит общие сведения о политике:

- Название политики
- Пользователь, который создал политику
- Дата и время, когда политика была создана
- Дата и время последнего изменения политики



Политики компьютеров и виртуальных машин

Вы можете переименовать политику, введя новое имя в соответствующем поле и нажав кнопку **Сохранить** в нижней части страницы. Политики должны

иметь подходящие имена, чтобы вы или другой администратор могли их быстро и просто идентифицировать.

Примечание
По умолчанию, только пользователь, создавший политику, может изменить ее. Чтобы внести изменения, владелец политики должен выбрать опцию **Разрешить другим пользователям изменять эту политику** на странице политик в разделе **Подробности**.

Правила наследования

Вы можете задать разделы, которые будут наследовать параметры других политик. Чтобы это сделать:

1. Выберите модуль и раздел, для которого требуется включить наследование. Все разделы будут наследовать параметры, за исключением **Общее > Подробности**.
2. Выберите интересующий вас раздел политики, для которого вы хотите включить наследование.
3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

Если исходная политика удаляется, унаследственные точки и настройки разделов вернутся к дочерним настройкам.

Унаследованные разделы не могут дополнительно наследоваться другими политиками. Рассмотрим следующий пример:

Политика А наследует настройки раздела **Защита от вредоносных программ > По требованию** от политики Б. Политика В уже не сможет наследовать настройки раздела **Защита от вредоносных программ > По требованию** от политики А.

Информировать о технической поддержке

Вы можете настроить контактную информацию и информацию о технической поддержке, которая будет доступна в агенте безопасности в разделе **О программе**, заполнив соответствующие поля.

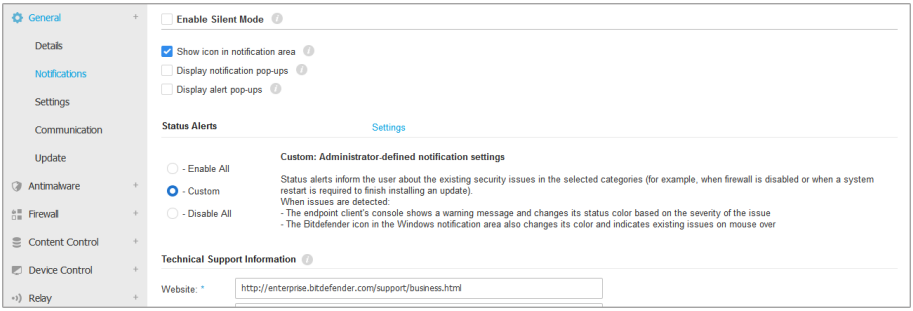
Чтобы настроить адрес электронной почты в окне **О программе**, чтобы он открывал приложение электронной почты по умолчанию на конечной точке, необходимо добавить его в поле с пометкой "mailto:"**Электронная почта**. Пример: `mailto: name@domain.com`.

Пользователь сможет получить данную информацию из агента безопасности, нажав правую кнопку мыши на значке Bitdefender в системном трее и выбрав раздел **О программе**.

Уведомления

В этом разделе вы можете настроить параметры отображения интерфейса пользователя агента безопасности Bitdefender в доступном и интуитивно понятном виде.

Всего лишь одним щелчком мыши вы можете включить или выключить типы уведомлений, оставив только те, которые действительно имеют значение для вас. Кроме того, на той же странице, вы получаете полный контроль над видимостью проблем конечных точек.



Политики - Настройки отображения

- **"Без оповещений".** Установите флажок, чтобы включить или выключить режим "Без оповещений" (Silent Mode). Режим "Без оповещений" разработан чтобы запретить вмешательство пользователей в действия агента безопасности. При включении режима "Без оповещений" вносятся следующие изменения в конфигурацию политики:
  - Опции **Показать значок в области уведомлений**, **Отображать всплывающие уведомления** и **Отображать всплывающие окна с предупреждениями** в этом разделе будут отключены.
  - Если уровень защиты файрвола установлен в **Правила и вопросы** или **Правила, известные файлы и вопросы** режим, то он будет изменен на **Набор правил, известные файлы и разрешения**. В противном случае, настройки уровня защиты останутся неизменными.

- **Отображать значок в области уведомлений.** Выберите эту опцию, чтобы показать значок Bitdefender в области уведомлений (также известной как системный трей). Значок информирует пользователей о состоянии их защиты, изменяя свой внешний вид и отображая соответствующие всплывающие уведомления. Кроме того, пользователи могут щелкнуть правой кнопкой мыши для быстрого открытия главного окна агента безопасности или окна **О программе**.
- **Отображать всплывающие предупреждения.** Пользователи информируются через всплывающие уведомления о событиях безопасности, которые требуют ответных действий. Если вы установили - не отображать всплывающие уведомления, то агент безопасности автоматически предпримет рекомендованные действия. Всплывающие предупреждения генерируются в следующих ситуациях:
  - Если настройки файрвола требуют запросить действия пользователя для неизвестных программ, требующих доступ к сети или в Интернет.
  - Если Расширенное управление угрозами/Система обнаружения вторжений (Advanced Threat Control / Intrusion Detection System) включены, каждый раз, когда обнаружено потенциально опасное приложения.
  - Если сканирование устройств включено, каждый раз, когда внешнее устройство хранения подключается к компьютеру. Вы можете настроить данные параметры в разделе **Защита от вредоносных программ > По требованию**.
- **Отображать всплывающие уведомления.** В отличие от всплывающих предупреждений, всплывающие уведомления информируют пользователей о различных событиях безопасности. Всплывающие уведомления будут автоматически исчезать в течение нескольких секунд без вмешательства пользователя.

  Выберите **Отображать всплывающие уведомления**, затем нажмите ссылку **Показать модульные настройки**, чтобы выбрать события, которые будут отображаться пользователям. Есть три типа всплывающих уведомлений, в зависимости от серьезности событий:
  - **Info**. Пользователи информируются о существенных событиях безвредных для безопасности. Например, о приложении, которое подключилось к сети Интернет.

– **Низкий**. Пользователи информируются о важных событиях безопасности, которые могут потребовать вмешательства. Например, сканирование On-Access обнаружило угрозу и файл был удален или помещен в карантин.

– **Критичный**. Эти всплывающие уведомления информируют пользователей об опасных ситуациях, например, сканирование On-Access обнаружило угрозу, но действие политики по умолчанию - **Не предпринимать действий** (не предпринимать действий), в результате вредоносная программа по-прежнему присутствует на конечной точке, или процесс обновления не может быть завершен.

Установите соответствующий флажок, связанный с набранным именем, для такого рода всплывающих уведомлений во всех модулях одновременно. Установите флажки, связанные с отдельными модулями, для включения или отключения конкретных уведомлений.

Например, после выбора флажков, связанных с Sandbox Analyzer, Bitdefender Endpoint Security Tools информирует пользователя о том, что файл отправляется на поведенческий анализ.

Список модулей может варьироваться в зависимости от вашей лицензии.

- **Видимость проблем конечных точек.** В этом случае пользователи решают самостоятельно, когда их конечное устройство имеет проблемы с конфигурацией безопасности или при других угрозах безопасности, на основе предупреждений о состоянии. Например, пользователи могут видеть, когда возникают проблемы, связанные с их защитой от вредоносного ПО, например: отключение модуля сканирования или когда полное сканирование системы запущено. Пользователи информируются о состоянии их защиты в двух случаях:

  – Проверьте область уведомлений главного окна, которая отображает соответствующие сообщения о состоянии, и меняет свой цвет в зависимости от серьезности проблем безопасности. Пользователи имеют возможность просматривать возникающие проблемы более подробно, нажав соответствующую кнопку.

  – Проверьте иконку Bitdefender в системном трее, которая меняет свой внешний вид при обнаружении проблем.

  Агенты безопасности Bitdefender используют следующие цветовые схемы в области уведомлений:

– Зеленая: Проблем не обнаружено.

– Желтая: Конечное устройство имеет незначительные проблемы, влияющие на безопасность. Пользователи могут не прерывать свою текущую работу для решения таких проблем.

– Красная: Конечное устройство имеет критическую проблему, требующую немедленной реакции пользователя.

Выберите **Видимость проблем конечной точки**, затем нажмите ссылку **Показать модульные настройки**, чтобы настроить оповещения о состоянии, отображаемые в интерфейсе агентов Bitdefender.

Для каждого модуля вы можете выбрать отображение уведомлений как предупреждений, как критических проблем, или не показывать вообще. Ниже приведены возможные варианты:

– **Общее**. Предупреждение о состоянии генерируется каждый раз при необходимости перезапуска системы во время или после установки продукта, а также, когда агент безопасности не может подключиться к облачному сервису Bitdefender.

– **Защита от вредоносных программ**. Предупреждении о состояние генерируется в следующих случаях:

  - Сканирование по запросу включено, но слишком много локальных файлов пропущено.

  - Прошло определенное количество дней с момента последнего полного сканирования системы, выполненного на компьютере.

    Вы можете задать, как отображать оповещения и задать количество дней для предупреждения после последнего полного сканирования системы.

  - Для завершения процесса лечения требуется перезагрузка системы.

– **Завершение**. Предупреждения о состоянии генерируется, когда модуль файрвола отключен.

– **Контроль приложений**. Этот статус предупреждения генерируется, когда модуль Управления приложениями модифицируется.

– **Управление контентом**. Предупреждения о состоянии генерируется, когда модуль контентной фильтрации отключен.

– **Обновить**. Предупреждения о состоянии генерируется каждый раз, когда требуется перезагрузка системы для завершения обновлений.

- **Уведомление о перезапуске конечной точки.** Эта опция отображает предупреждение о перезапуске на конечной точке каждый раз, когда требуется перезагрузка системы из-за изменений, внесенных в конечную точку модулями GravityZone, выбранными в модульных настройках.

Примечание
Конечные точки, требующие перезагрузки системы, имеют определенный значок состояния ( ) в инвентаре GravityZone.

Вы можете дополнительно настроить оповещения о перезапуске, нажав **Показать модульные настройки**. Доступны следующие опции:

– **Перезапуск** - Выберите этот параметр, чтобы активировать уведомления о перезапуске обновления агента.

– **Управление патчами** - Выберите этот параметр, чтобы активировать уведомления о перезапуске установки патчей.

Примечание
Вы также можете установить ограничение на сколько часов пользователь может отложить перезапуск. Для этого выберите **Автоматический перезапуск машины после** и введите значение от 1 до 46.

Предупреждение о перезапуске требует от пользователя выбора одного из следующих действий:

– **Перезагрузить сейчас**. В этом случае система перезапустится автоматически.

– **Отложить перезагрузку**. В этом случае уведомление о перезапуске будет периодически появляться до тех пор, пока пользователь не перезапустит систему или пока не пройдет время, установленное администратором компании.

Настройки

В данном разделе вы можете изменить следующие настройки:

- **Настройка пароля.** Чтобы предотвратить деинсталляцию защиты с компьютеров пользователями с правами администратора, вы должны установить пароль.

  Пароль деинсталляции должен быть задан до процесса установки, путем настройки инсталляционного пакета. Если вы это сделали, то нажмите **Сохранить настройки установки**, чтобы сохранить текущий пароль.

  Чтобы установить пароль или изменить текущий пароль, выберите **Включить пароль** и введите желаемый пароль. Чтобы снять парольную защиту, выберите **Отключить пароль**.

- **Настройка прокси**

  Если ваша сеть находится за прокси-сервером, вам необходимо задать настройки прокси, которые позволят вашим конечным устройствам соединяться с компонентами решения GravityZone. В этом случае вам необходимо разрешить опцию **Конфигурация прокси** и заполнить требуемые параметры.
  - **Сервер** - введите IP-адрес прокси-сервера
  - **Порт** - введите порт, используемый для подключения к прокси-серверу.
  - **Имя пользователя** - введите имя пользователя, распознаваемое прокси-сервером.
  - **Пароль** - введите корректный пароль указанного пользователя.

- **Привилегированный пользователь**

  Модуль привилегированных пользователей разрешает предоставление администраторских прав для уровня конечных устройств, что позволяет пользователям конечных устройств иметь доступ и модифицировать настройки политик через локальную консоль посредством интерфейса Bitdefender Endpoint Security Tools.

  Если вы хотите разрешить конечным устройствам работать с правами привилегированных пользователей, для начала вам необходимо включить данный модуль в состав агента безопасности, устанавливаемого на выбранном конечном устройстве. После этого вам необходимо настроить параметры привилегированных пользователей в политике, применяемой к этим конечным точкам:

  Важно
  Модуль привилегированных пользователей доступен только для серверов и рабочих станций, работающих под управлением Windows.

1. Разрешить опцию **Power User**.
2. Задать пароль привилегированного пользователя в поле ниже.

   Пользователи, пытающиеся получить доступ к режиму привилегированных пользователей на локальном конечном устройстве, должны будут ввести заданный пароль.

Для доступа к режиму привилегированных пользователей, пользователи должны нажать правой кнопкой мыши на значок Bitdefender в системном трее и выбрать **Пользователь** из контекстного меню. После ввода пароля в окне входа, консоль будет отображать применяемые в настоящее время параметры политики, которые пользователь конечного устройства сможет просмотреть или модифицировать.

Примечание
Только некоторые функции безопасности могут быть доступны локально с помощью консоли привилегированных пользователей, касающиеся модулей защиты от вредоносных программ (Antimalware), файрвола (Firewall), контроля содержимого (Content Control) и управления устройством (Device Control).

Чтобы вернуть изменения, сделанные в режиме привилегированного пользователя:

– Откройте в Control Center шаблон политики, назначенной конечной точке, с правами привилегированного пользователя и нажмите **Сохранить**. В этом случае оригинальные настройки будут переприменены к целевой конечной точке.
– Примените новую политику конечной точке с правами привилегированного пользователя.
– Зайдите локально на конечное устройство, откройте консоль привилегированного пользователя и нажмите **Синхронизировать**.

Чтобы быстро найти конечные точки с модифицированной политикой в режиме привилегированного пользователя:

– В разделе **Сеть** нажмите меню **Фильтры** и выберите опцию **Отредактировано пользователем** на вкладке **Полиика**.
– В разделе **Сеть** нажмите на интересующее вас конечное устройство для отображения окна **Информация**. Если политика была изменена в

режиме привилегированного пользователя, уведомление будет отображаться в разделе **Общее** > **Политика**.

Важно
Модуль привилегированного пользователя специально разработан для устранения неполадок, что позволяет администратору сети легко просматривать и изменять параметры политик на локальном компьютере. Назначение прав доступа привилегированного пользователя другим пользователям в компании должно быть ограничено уполномоченным персоналом, чтобы гарантировать, что политики безопасности всегда применялись на всех конечных точках сети компании.

- **Параметры**

  В этом разделе вы можете задать следующие параметры:

  – **Удалять старые события (дни).** Агент безопасности Bitdefender ведет подробный журнал событий, касающихся его деятельности на компьютере (в том числе компьютерной активности, контролируемой модулем управления контентом). По умолчанию, из журнала удаляются события старше 30 дней. Если вы хотите изменить этот интервал, выберите другой вариант из меню.

  – **Отправлять отчеты о сбоях в Bitdefender.** Выберите этот параметр, чтобы отчеты о сбоях агента безопасности отправлялись в лабораторию Bitdefender для анализа. Отчеты помогут нашим инженерам выяснить, что вызвало проблему и предотвратить ее повторное возникновение. Никакая персональная информация не будет отправлена.

  – **Отправьте подозрительные исполняемые файлы для анализа.** Выберите этот параметр, чтобы отправить файлы, которые кажутся ненадежными или имеют подозрительное поведение, в Bitdefender Labs для анализа.

  – **Отправьте отчет о нарушении памяти HVI в Bitdefender.** По умолчанию HVI отправляет анонимную информацию об обнаруженных нарушениях на облачные серверы Bitdefender для дальнейшего использования в статистике и повышения скорости обнаружения продукта. Этот флажок можно снять, если не требуется отправлять подобную информацию из вашей сети.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Коммуникации

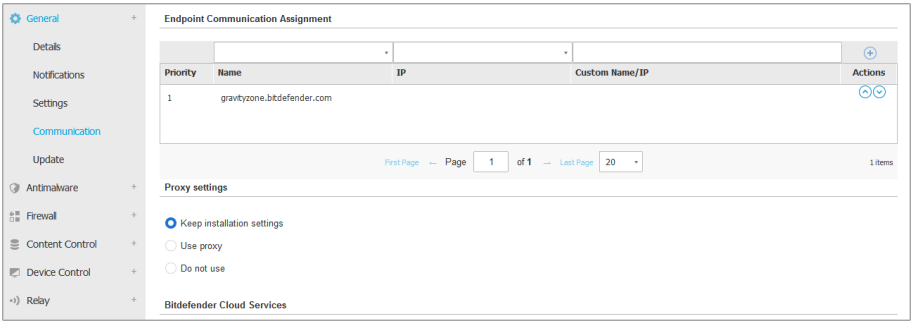
В этом разделе вы можете назначить одну или несколько машин-ретрансляторов для требуемых конечных точек, а затем настроить прокси-сервер для связи между этими конечными точками и GravityZone.

Назначение коммуникационных параметров конечной точке

Когда несколько коммуникационных серверов устанавливается на устройство GravityZone, вы можете назначить выбранным компьютерам один или несколько коммуникационных серверов с помощью политики. Доступные конечные точки-ретрансляторы, которые выступают в качестве коммуникационных серверов, также будут учтены.

Чтобы назначить коммуникационные серверы выбранным компьютерам:

1. В окне **Назначение связи конечной точки**, нажмите на поле **Имя**. Появится список обнаруженных коммуникационных серверов.
2. Выберите объект.



Политики компьютеров и виртуальных машин - Настройки коммуникационных параметров

3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

Коммуникационный сервер добавится к списку. Все выбранные компьютеры будут общаться с Control Center через указанный коммуникационный сервер.

4. Выполните те же действия, чтобы добавить несколько коммуникационных серверов, при их наличии.
5. Вы можете настроить приоритет использования коммуникационных серверов, с помощью стрелок вверх и вниз, доступных справа от каждого объекта. Связь выбранных компьютеров будет осуществляться через объект, размещенный вверху списку. Когда связь с этим объектом будет потеряна, использоваться будет следующий объект списка.
6. Для удаления одного объекта из списка нажмите на соответствующую кнопку ⊗ **Удалить** в правой части таблицы.

Связь между конечной точкой и ретранслятором / GravityZone

В этом разделе вы можете настроить прокси-сервер для связи между желаемыми конечными точками и назначенными машинами-ретрансляторами или между требуемыми конечными точками и устройством GravityZone (если ретранслятор не был назначен):

- **Сохранить настройки установки**, чтобы использовать параметры прокси-сервера, определенные в установочном пакете.
- **Использовать прокси, определенный в общем разделе**, чтобы использовать параметры прокси-сервера, определенные в текущей политике в разделе **Общее > Настройки**.
- **Не использовать**, когда целевые конечные точки не взаимодействуют с определенными компонентами GravityZone через прокси-сервер.

Связь между конечными точками и облачными сервисами

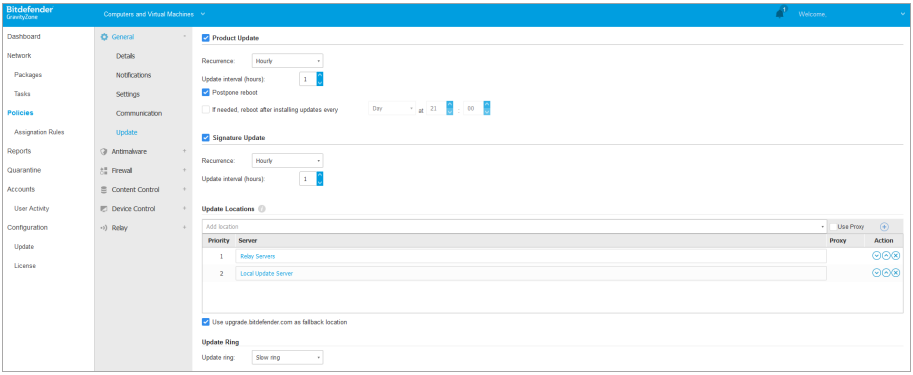
В этом разделе вы можете настроить прокси-сервер для связи между нужными конечными точками и Bitdefender Cloud Services (требуется подключение к Интернету):

- **Сохранить настройки установки**, чтобы использовать параметры прокси-сервера, определенные в установочном пакете.
- **Использовать прокси, определенный в общем разделе**, чтобы использовать параметры прокси-сервера, определенные в текущей политике в разделе **Общее > Настройки**.

- **Не использовать**, когда целевые конечные точки не взаимодействуют с определенными компонентами GravityZone через прокси-сервер.

Обновления

Обновления являются очень важной деталью, которая позволяет противодействовать новейшим угрозам. Bitdefender публикует все обновления продукта и механизмов защиты через серверы Bitdefender в Интернете. Все обновления зашифрованы и имеют цифровую подпись, чтобы их нельзя было подделать. Когда доступно новое обновление, агент безопасности Bitdefender проверяет цифровую подпись обновления для аутентификации и содержимое пакета для обеспечения целостности. Затем каждый файл обновления анализируется, и его версия проверяется на соответствие установленной. Более новые файлы загружаются локально и проверяются на соответствие хэшу MD5, чтобы убедиться, что они не изменены. В этом разделе вы можете настроить агент безопасности Bitdefender и параметры обновления механизмов защиты.



Политики компьютеров и виртуальных машин - Параметры обновлений

- **Обновление продукта.** Агент безопасности Bitdefender автоматически проверяет, загружает и устанавливает обновления каждый час (настройки по умолчанию). Автоматическое обновление выполняется в фоновом режиме.
  - **Возобновление**. Чтобы изменить периодичность автоматических обновлений, выберите другую опцию из меню и настройте ее в соответствии с вашими потребностями в последующих полях.

– **Отложить перезагрузку**. Некоторые обновления для установки и корректной работы требуют перезагрузки системы. По умолчанию продукт будет продолжать работать со старыми файлами до перезапуска компьютера, после чего будут применены самые последние обновления. Уведомление в пользовательском интерфейсе будет предлагать пользователю перезагрузить систему всякий раз, когда этого потребует обновление. Рекомендуется оставить этот параметр включенным. В противном случае система автоматически перезагрузится после установки необходимого обновления. Пользователи будут уведомлены о необходимости сохранить свою работу, но перезагрузка не может быть отменена.

– Если вы выберете отложенную перезагрузку, вы можете установить удобное время, когда компьютеры, в случае необходимости, будут перезагружаться автоматически. Такой вариант больше подходит для серверов. Выберите **При необходимости перезагрузите компьютер после установки обновлений.** и укажите удобное время перезагрузки (ежедневно или еженедельно в определенный день, в определенное время суток).

– Для большего контроля над изменением конфигурации и обновлением промежуточного процесса Вы можете настроить лучший агент на Ваших устройствах Linux для выполнения обновлений модуля ядра EDR через **Обновление продукта**.

  Если включен флажок **Обновление продукта** :

  - Если Вы включите флажок **Обновить модули Linux EDR с помощью обновления продукта**, то GravityZone обновит версии ядра с помощью **Обновления продукта**.
  - Если Вы оставите эту опцию отключенной, версии ядра будут обновлены с помощью **Security Content Update**.

  Примечание
  Если Вы включите флажок **Обновить модули Linux EDR с помощью обновления продукта**, но отключите параметр **Обновление продукта**, модули Linux EDR обновляться не будут.

- **Обновление механизмов защиты.** К механизмам защиты относятся статические и динамические меры предотвращения угроз, такие как движки сканирования, модели машинного обучения, эвристические

методы, правила, сигнатуры и черные списки. Агент безопасности Bitdefender автоматически проверяет, загружает и устанавливает обновления механизмов защиты каждый час (настройки по умолчанию). Автоматическое обновление выполняется в фоновом режиме. Чтобы изменить периодичность автоматических обновлений, выберите другую опцию из меню и настройте ее в соответствии с вашими потребностями в последующих полях.

- **Расположение обновлений**. По умолчанию, агенты безопасности Bitdefender обновляются с локального сервера обновлений GravityZone. Добавить источник обновлений можно путем выбора предварительно заданных ресурсов в выпадающем меню или путем ввода IP-адреса или имени хоста одного или нескольких серверов обновлений в вашей сети. Настройте их приоритет, используя кнопки вверх и вниз, отображаемые при наведении мыши. Если первый источник обновлений недоступен, будет использован следующий в списке и так далее.

  Чтобы настроить локальный адрес для обновлений:

  1. Введите адрес сервера обновлений в поле **Добавить локацию**. Доступны следующие возможности:
     - Выбор предопределенного источника:
       - **серверы-ретрансляторы** Конечная точка будет автоматически подключаться к назначенным серверам-ретрансляторам.

         Предупреждение
         Серверы ретрансляции не поддерживаются в устаревших операционных системах. Для подробной информации обратитесь в Гид по установке.

         Примечание
         Вы можете проверить назначенные серверы-ретрансляторы в окне **Information**. За более подробной информацией обратитесь к Просмотр сведений о компьютере

       - **Локальный сервер обновлений**
     - Введите IP-адрес или имя хоста одного или нескольких серверов обновлений в вашей сети. Используйте один из следующих вариантов синтаксиса:

- `update_server_ip:port`
- `update_server_name:port`

По умолчанию используется порт 7074.

Флажок **Применять серверы Bitdefender в качестве резервного местоположения** установлен по умолчанию. Если источники обновлений недоступны, будет использоваться резервный вариант.

Предупреждение
Отключение резервного источника остановит автоматическое обновление, что приведет к образованию уязвимостей в вашей сети, если указанные источники обновлений окажутся недоступны.

2. Если клиентские компьютеры подключаются к локальному серверу обновлений через прокси-сервер, выберите **Использовать прокси**.
3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.
4. Используйте стрелки ⌃ вверх / ⌄ вниз в колонке **Действие**, чтобы установить приоритет использования источников обновлений. Если первый источник обновлений недоступен, будет использован следующий в списке и так далее.

Чтобы удалить папку из списка, нажмите соответствующую кнопку ⊗ **Удалить**. Вы можете удалить источник обновлений по умолчанию (не рекомендуется).

- **Последовательность Обновлений .** Вы можете задать последовательность обновлений продуктов по очереди, с помощью порядка обновления:
  - **Медленное обновление** Машины с политикой медленного обновления будут получать обновления в более поздний срок, в зависимости от готовности конечных точек с быстрым обновлением. Это дополнительная мера предосторожности в процессе обновления. Данные настройки приняты по умолчанию.
  - **Быстрое обновление** Машины с политикой быстрого обновления получат новейшие доступные обновления в первую очередь. Данные параметры рекомендуются для некритичных машин, используемых в деятельности компании.

Важно

- Маловероятно, но в случае возникновения проблем с быстрым обновлением у машин с определенными конфигурациями, то они будут исправлены еще до выхода медленных обновлений.
- BEST for Windows Legacy не поддерживает постановку. Устаревшие конечные точки в промежуточном местоположении должны быть перемещены в производственное местоположение.

7.2.2. HVI

Примечание

HVI обеспечивает защиту виртуальных машин только на гипервизорах Citrix Xen.
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Hypervisor Memory Introspection защищает виртуальные машины от передовых угроз, от которых сигнатурные движки не способны защитить. Она обеспечивает в реальном масштабе времени обнаружение атак, с помощью мониторинга процессов за пределами гостевой операционной системы. Механизм защиты включает в себя несколько вариантов блокировки атак по мере их появления и немедленного устранения угрозы.

Следуя принципу разделения памяти операционных систем, HVI также включает в себя два модуля защиты, организованные в соответствующие категории:

- Пространство пользователя, адресация нормальных процессов пользовательских приложений.
- Пространство ядра, адресация, зарезервированная под процессы ядра операционной системы.

Кроме того, политика HVI предусматривает две функции, которые помогут вам управлять безопасностью и поддерживать защищенные виртуальные машины:

- Исключения для просмотра и управления процессами, исключенными из сканирования.

- Инструменты пользователя для ввода инструментов, необходимых для оперативной и судебной экспертизы в гостевых операционных системах.

Пространство пользователя

В этом разделе можно настроить параметры защиты процессов, запущенных в пространстве памяти пользователя.

Используйте флажок **Самоанализ памяти пользовательского пространства**, чтобы включить или отключить защиту.

Функциональность этого модуля основывается на правилах, что позволяет настроить защиту отдельно для разных групп процессов. Кроме того, вы можете выбрать сбор дополнительных данных для экспертного анализа.

- Правила пользовательского пространства
- данные для экспертного анализа

Правила пользовательского пространства

Модуль поставляется с набором предопределенных правил, которые касаются наиболее уязвимых приложений. Таблица в этом разделе содержит существующие правила, предоставляя важную информацию о каждом из них:

- Имя правила
- Процессы, к которым применяется правило
- Режим мониторинга
- Действие, которое блокирует обнаруженную атаку
- Действия по удалению угрозы

Вы также можете создать список пользовательских правил для процессов, которые вы хотите контролировать. Для создания нового правила:

1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Это действие открывает окно настройки правил.
2. Настройте модуль, используя следующие параметры правила:
   - **Имя правила.** Введите имя, под которым правило будет отображаться в таблице правил. Например, для таких процессов, как `firefox.exe` или `chrome.exe`, вы можете назвать правило `Браузеры`.

- **Процессы.** Введите имена процессов, которые вы собираетесь мониторить, разделяя их точкой с запятой (;).
- **Режим мониторинга.** Для быстрой настройки, выберите уровень безопасности, который наилучшим образом соответствует вашим потребностям (**Интенсивный**, **Нормальный** или **Рекомендуемый**). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

  Вы можете настроить параметры модуля более детально, выбрав уровень защиты **Пользователь** и задав один или несколько следующих вариантов:

  – **Хуки будут устновлены на критические библиотеки DLLs.** Обнаружение DLL "инъекций", которые загружают вредоносный код в вызывающий их процесс.

  – **Попытки распаковки / дешифрования в основном исполняемом файле** Обнаруживать попытки дешифровки кода в основных исполняемых процессах и защищать процессы от изменения вредоносными инструкциями.

  – **Иностранные записи внутри целевого процесса** Защита от внедрения кода в защищенный процесс.

  – **Эксплойты.** Обнаружение подозрительного поведения процесса, вызванного попыткой использования ошибки, обнаруженной в предыдущих уязвимостях. Используйте эту опцию, если вы хотите контролировать выполнение кода из динамической памяти или стека защищенных приложений.

  – **Подключение WinSock..** Блок перехвата сетевых библиотек (DLL), используемых операционной системой, обеспечивающих коммуникации звука по TCP/IP.
- **Действия.** Есть несколько действий, которые вы можете применить при обнаружении угроз. Каждое действие, в свою очередь, имеет несколько возможных вариантов или вторичных действий. Их описание приведено ниже:

  – **Основное действие.** Это немедленное действие, которое вы можете предпринять при обнаружении атаки на гостевой машине, что позволяет заблокировать ее. Доступны следующие опции:

- **:Журнал.** Только записать событие в базу данных. В этом случае вы получите только уведомление (если оно настроено) и будете иметь возможность просмотреть этот инцидент в отчете **HVI Деятельность**.
- **Отклонить.** Отклонение любых попыток угроз, изменяющих какой-либо процесс.
- **Выключить машину.** Выключение виртуальной машины, на которой запущен целевой процесс.

Важно
Рекомендуется сначала установить основное действие в **Журнал**. Используйте политику в течение определенного периода времени чтобы убедиться, что все работает в соответствии с ожиданиями После этого вы можете выбрать любое действие, которое вы хотите предпринять в случае, если зафиксировано нарушение памяти.

– **Действие по исправлению.** В зависимости от выбранных настроек, Security Server встраивает инструмент исправления на гостевой операционной системе. Инструмент автоматически начинает сканирование на наличие вредоносных программ и при обнаружении угрозы, он осуществляет выбранное действие. Доступны следующие опции:

- **Дезинфицировать.** Удаляет вредоносный код из зараженных файлов. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов.
- **Удалить.** Удаляет обнаруженные файлы с диска без предупреждения. Желательно избегать использование этого действия.
- **Игнорировать.** Инструмент исправления обнаруживает и только сообщает об обнаруженных файлах.
- **Нет.** Инструмент исправления не будет внедрятся в гостевую операционную систему.

Примечание
Закрытие инструмента приведет к его удалению из системы и не оставит никаких следов пребывания в гостевой операционной системе.

– **Действие по исправлению резервной копии.** Когда действие исправления выходит из строя, вы можете выбрать другой механизм исправления из доступных вариантов.

3. Нажмите **Сохранить**.

После создания вы можете изменить правило в любое время. При нажатии на имя правила откроется окно его настройки.

GravityZone также позволяет быстро настроить параметры поведения модуля самоанализа памяти при обнаружениях, изменив одновременно несколько правил. Чтобы выбрать несколько правил с одинаковыми действиями:

1. Выберите правила, которые вы хотите изменить.
2. Нажмите кнопку **Действие и исправление** в верхней части таблицы.
3. Выберите нужный параметр для каждого действия.
4. Нажмите **Сохранить**. Новые действия вступят в силу после сохранения политики, при условии, что целевые машины находятся в сети.

Чтобы удалить одно или несколько правил из списка, выберите их, а затем нажмите кнопку ⊗ **Удалить** в верхней части таблицы.

данные для экспертного анализа

Установите флажок **События сбоя приложения** под таблицей правил территории пользователя, чтобы включить сбор подробной информации, когда приложения завершаются.

Вы можете просмотреть эту информацию в отчете об активности HVI и найти причину, по которой приложение завершило свою работу. Вы можете просмотреть эту информацию в отчете об активности HVI и найти причину, по которой приложение завершило свою работу.

Адресное пространство ядра

HVI защищает ключевые элементы операционной системы, такие как:

- Критические драйверы ядра и связанные с ними объекты, включая операции быстрого ввода/вывода, связанные с основными драйверами ядра.

- Сетевые драйверы, изменение которых позволило бы вредоносному ПО перехватывать трафик и внедрять вредоносные компоненты в поток трафика.
- Образ ядра операционной системы, включая следующее: раздел кода, раздел данных и раздел только для чтения, в том числе Import Address Table (IAT), Export Address Table (EAT) и ресурсы.

В этом разделе можно настроить параметры защиты для процессов, запускаемых в пространстве памяти ядра.

Используйте флажок **Самоанализ памяти пространства ядра**, чтобы включить или выключить защиту.

Для быстрой настройки, выберите уровень безопасности, который лучше всего соответствует вашим потребностям (**Интенсивный**, **Нормальный** или **Рекомендуемый**). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

Вы можете настроить параметры модуля более детально, выбрав уровень защиты **Пользователь** и задав один или несколько следующих вариантов:

- **Контроль регистров** . Контроль регистров (CR) (регистров процессора), контролируют общее поведение процессора или других цифровых устройств. Выберите эту опцию для обнаружения попыток загрузки недопустимых значений в определенные регистры.
- **Типовые регистры**. Это любые регистры, относящиеся к контролируемым регистрам в наборе команд x86, используемые для отладки, трассировки выполнения программы, мониторинга производительности компьютера и включения определенных функций центрального процессора. Выберите эту опцию для обнаружения попыток изменения этих регистров.
- **IDT/GDT Целостность**. Глобальная таблица дескрипторов или таблица дескрипторов прерываний (IDT/GDT) используются процессором для определения правильного ответа на прерывания и исключения. Выберите этот параметр, чтобы обнаружить любые попытки изменения этих таблиц.
- **Защита драйверов от вредоносных программ.** Выберите этот параметр, чтобы обнаружить попытки изменения драйвера, используемого программой-антивирусом.
- **Защита драйверов Xen.** Выберите этот параметр, чтобы обнаружить попытки изменения драйверов гипервизора Citrix XenServer.

Есть несколько действий, которые вы можете предпринять при обнаружении угроз. Каждое действие, в свою очередь, имеет несколько возможных вариантов или вторичных действий. Их описание приведено ниже:

- **Первичное действие.**
  - **:Журнал.** Только записать событие в базу данных. В этом случае вы получите только уведомление (если оно настроено) и будете иметь возможность просмотреть этот инцидент в отчете **Интроспекция памяти**.
  - **Отклонить.** Отклонение любых попыток угроз, изменяющих какой-либо процесс.
  - **Выключить машину.** Выключение виртуальной машины, на которой запущен целевой процесс.

Важно
Рекомендуется сначала установить основное действие в **Журнал**. Используйте политику в течение определенного периода времени чтобы убедиться, что все работает в соответствии с ожиданиями После этого вы можете выбрать любое действие, которое вы хотите предпринять в случае, если зафиксировано нарушение памяти.

- **Действие исправления.**
  - **Дезинфицировать.** Удаляет вредоносный код из зараженных файлов. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов.
  - **Удалить.** Удаляет обнаруженные файлы с диска без предупреждения. Желательно избегать использование этого действия.
  - **Игнорировать.** Инструмент исправления обнаруживает и только сообщает об обнаруженных файлах.
  - **Нет.** Инструмент исправления не будет внедрятся в гостевую операционную систему.
- **Действие по исправлению резервной копии.** Когда действие исправления выходит из строя, вы можете выбрать другой механизм исправления из доступных вариантов.

Кроме того, вы можете собирать информацию, которая обогатит данные, для экспертной оценки. Установите флажки **События сбоя ОС** и **События**

драйверов, чтобы включить сбор информации о сбоях гостевой операционной системы или событиях, генерируемых дополнительными модулями загруженными Операционной системой. Эти события, предшествовавшие инциденту, помогут сэкспертной оценке ускорить обнуление коренной причины нападения.

Эти события агрегируются в отчете о деятельности HVI по инциденту, который привел к ним.

Исключения

GravityZone допускает исключение процессов из сканирования HVI, путем использования отчетов **Заблокированных приложений** и **Действия HVI**. Раздел **Исключения** собирает все эти процессы из указанных отчетов и отображает их в виде таблицы.

О причине исключения процесса можно узнать в комментарии.

Если вы измените решение в отношении исключенного процесса, нажмите в верхней части таблицы кнопку **Удалить**, в дальнейшем этот процесс будет включен в сканирование.

пользовательские инструменты

В этом разделе можно настроить средства ввода на целевые гостевые операционные системы. Перед применением этих инструментов необходимо загрузить их на GravityZone. Для получения более подробной информации, обратитесь к «Ввод инструментов пользователя с HVI» (p. 574).

Для настройки ввода:

1. Установите флажок **Активировать ввод**, чтобы включить или отключить эту функцию.
2. Для добавления нового инструмента нажмите в верхней части таблицы кнопку ⊕ **Добавить** Появится окно конфигурации.
3. Из раскрывающегося списка выберите необходимый инструмент **Выберите инструмент**.

   Эти инструменты были ранее загружены в GravityZone. Если вы не можете найти нужный инструмент в списке, перейдите в раздел **Центр управления инструментами** и добавьте его оттуда. Для получения более подробной информации, обратитесь к «Ввод инструментов пользователя с HVI» (p. 574).

4. В разделе **Описание инструмента** введите предполагаемое использование инструмента или другие сведения, которые могут оказаться полезными.
5. Введите командную строку инструмента, вместе со всеми необходимыми входными параметрами, таким же образом, как это делается в командной строке. Например:

```
bash script.sh <param1> <param2>
```

.

Из двух раскрывающихся меню можно выбрать действие для восстановления и исправления резервной копии для средств восстановления Bitdefender.

6. Укажите место, из которого Security Server должен собирать журналы:
   - **стандартный вывод** . Установите этот флажок, чтобы записывать журналы из стандартного выходного канала связи.
   - **Выходной файл**. Установите этот флажок, чтобы получать сохраненный на конечной точке файл журнала. В этом случае необходимо указать путь к месту, где Security Server может найти файл. Вы можете использовать абсолютный путь или системные переменные.

     Здесь есть два дополнительных варианта:

     a. **Удалять файлы журнала с гостевого компьютера после их передачи**. Выберите этот параметр, если файлы на конечной точке больше не нужны.

     b. **передать журналы в**. Чтобы переместить файл журналов из Security Server в другое место, выберите этот параметр. В этом случае необходимо указать путь к месту назначения и учетным данным аутентификации.
7. Выберите способ запуска инструмента. Для выбора доступны следующие параметры:
   - **После обнаружения нарушения на гостевой виртуальной машине.** Инструмент вводится сразу, когда на виртуальной машине обнаружена угроза.
   - **По специальному расписанию.** Используйте параметры планирования для настройки расписания ввода инструмента. Вы можете запускать

инструмент каждые несколько часов, дней или недель, начиная с указанной даты и времени.

Обратите внимание, что виртуальная машина должна быть включена в то время, которое указано в расписании. Запланированное введение инструмента не будет выполнено, если устройство выключено или приостановлено. В таких ситуациях рекомендуется установить флажок **Если запланированное время ввода пропущено, выполнить задачу как можно скорее**.

- Для завершения работы инструмента может потребоваться больше предполагаемого времени или он может перестать отвечать на запросы. Во избежание сбоев в таких ситуациях, в разделе **Конфигурация безопасности** выберите, через сколько часов Security Server должен автоматически завершить процесс инструмента.
- Нажмите **Сохранить**. Инструмент будет добавлен в таблицу.

Вы можете добавить столько инструментов, сколько вам необходимо, следуя упомянутым выше шагам.

7.2.3. Защита от вредоносного ПО

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- Linux
- ОС MAK

Модуль защиты от вредоносного ПО обеспечивает защиту системы от всех типов вредоносных угроз (вирусов, вирусов-троянов, шпионских и рекламных программ, руткитов и пр.). Защита делится на три категории:

- Сканирование при доступе: предотвращает проникновение новых угроз в систему.
- Проверка при выполнении: проактивно защищает от угроз, автоматически обнаруживает и блокирует безфайловые атаки при предварительном выполнении.

- Сканирование по требованию: позволяет распознавать и удалять вредоносные программы, уже присутствующие в системе.

В случае обнаружения вируса или других вредоносных программ агент безопасности Bitdefender попытается автоматически удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция называется "лечение". Файлы, которые не удается вылечить, перемещаются в папку карантина для исключения распространения вируса. Вирус, изолированный в карантине, не может причинить никакого вреда, так как его нельзя запустить или открыть для чтения.

Если сканирование определенных файлов или типов файлов выполнять не требуется, опытные пользователи могут настроить исключения при сканировании.

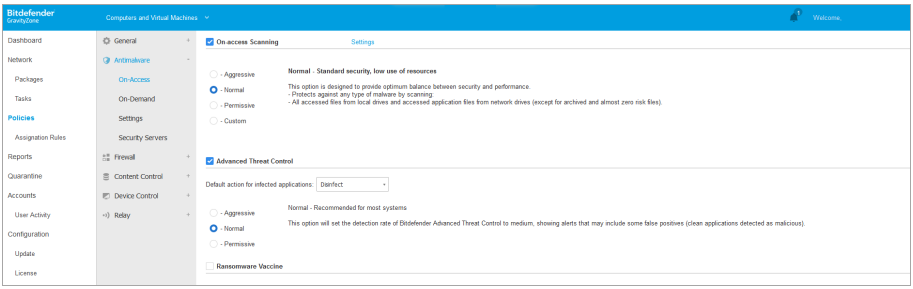
Настройки объединены в следующие разделы:

- Сканирование при доступе (On-Access)
- При выполнении
- Сканирование по запросу (On-Demand)
- Обнаружение гипервизора
- Advanced Anti-Exploit
- Настройки
- Серверы безопасности (Security Servers)

Сканирование при доступе (On-Access)

В этом разделе вы можете настроить компоненты, которые обеспечивают защиту при доступе к файлу или приложению:

- Сканирование при доступе
- Средство от вымогателей



Политики - Настройки при доступе

Сканирование при доступе

Сканирование при доступе предотвращает проникновение в систему новых угроз вредоносных программ путем сканирования локальных и сетевых файлов, если они доступны (открыты, перемещены, скопированы или выполняются), загрузочных секторов и потенциально нежелательных приложений (PUA).

Примечание
Эта функция имеет определенные ограничения в системах на основе Linux. Подробнее см. Главу требований в Руководстве по установке GravityZone.

Чтобы настроить сканирование при доступе к файлам:

1. Установите флажок, чтобы включить или отключить сканирование.

   Предупреждение
   Если вы отключите сканирование при доступе, конечные точки будут уязвимы для вредоносных программ.

2. Выберите для быстрой настройки уровень безопасности, который лучше всего соответствует вашим потребностям (интенсивный, нормальный или рекомендуемый). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.
3. Вы можете более детально настроить параметры сканирования, выбрав уровень защиты **Пользователь** и нажав на ссылку **Настройки**. Появится окно **Настройки сканирования при доступе**, содержащее несколько вариантов, организованных в двух вкладках - **Общее** и **Расширенные**.

   Опции вкладки **Общее** описаны ниже:

- **Расположение файлов**. Используйте данную настройку, чтобы задать типы файлов, которые вы хотите просканировать. Параметры сканирования можно настроить отдельно для локальных файлов (сохраненных на локальной конечной точке) или сетевых файлов (хранящихся на сетевых ресурсах). Если защита от вредоносных программ установлена на всех компьютерах в сети, вы можете отключить сканирование сетевых файлов, чтобы разгрузить сеть.

  Вы можете указать агенту безопасности просканировать все доступные файлы (независимо от их расширений), только файлы приложений или специфические расширения файлов, которые вы считаете потенциально опасными. Наиболее качественная защита обеспечивается посредством сканирования всех открываемых файлов, однако сканирование только приложений обеспечивает оптимальную производительность системы.

  Примечание
  Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 610).

  Если вы хотите просканировать только файлы со специфическими расширениями, выберите в меню **Пользовательские расширения** и затем введите желаемые расширения в редактируемом поле, нажимая `Войти` после каждого расширения.

  Примечание
  В системах на основе Linux расширения файлов чувствительны к регистру, а файлы с одинаковым именем, но с другим расширением считаются различными объектами. Например, `file.txt` и `file.TXT` - разные файлы.

  Для повышения производительности системы вы можете также исключить из сканирования большие файлы. Выберите флажок **Maximum size (MB)** и укажите ограничение по размеру файлов, которые будут проверяться. Используйте эту опцию аккуратно, так как вредоносные программы могут также затронуть и большие файлы.
- **СКАНИРОВАТЬ.** Выберите соответствующие флажки, чтобы включить нужные параметры сканирования.

- **Только новые или измененные файлы.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие системы с минимальными потерями в безопасности.
- **Загрузочные секторы.** Проверка загрузочных секторов системы. Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки. Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.
- **Сканирование на наличие клавиатурных шпионов.** Кейлоггеры (клавиатурные перехватчики) записывают то, что вы набираете на клавиатуре и отправляют отчеты хакерам через интернет. В украденных данных хакер может найти личную информацию, такую как номера банковских счетов и пароли, и использовать ее в личных целях.
- **Сканирование на наличие потенциально нежелательных приложений (PUA).** Потенциально нежелательные приложения (PUA) это программы, которые могут быть нежелательными для ПК, а иногда и поставляться в комплекте с программным обеспечением бесплатного. Такие программы могут быть установлены без согласия (также называются рекламными) или включены по умолчанию в комплект экспресс-установки (как дополнение). Потенциальное воздействие этих программ заключается в показе всплывающих окон, установке нежелательных панелей инструментов в браузере по умолчанию или работе нескольких процессов в фоновом режиме, что замедляет производительность компьютера.
- **Архивы**. Выберите эту опцию, если вы хотите включить сканирование при доступе к файлам архивов. Сканирование архивов — медленный процесс, занимающий большой объем системных ресурсов. Именно поэтому не рекомендуется выполнять такое сканирование в режиме реального времени. Архивы, содержащие инфицированные файлы, не представляют непосредственной угрозы безопасности системы. Вредоносные программы могут повлиять на систему только если зараженный файл извлечен из архива и будет исполнен при выключенной защите в реальном времени.

Если вы решили использовать данную опцию, вам необходимо настроить следующие параметры оптимизации:

- **Максимальный размер архива (МБ).** Вы можете установить максимально допустимый размер архивов, которые необходимо сканированировать. Поставьте флажок в соответствующем поле и введите максимальный размер архива (в МБ).
- **Максимальная глубина архива (уровни).** Отметьте соответствующий флажок и выберите в меню максимальную глубину архива. Для лучшей производительности выберите наименьшее значение, для максимальной защиты выберите наибольшее значение.

– **Отложенное Сканирование.** Отложенное сканирование повышает производительность системы при выполнении операций доступа к файлам. Например, системные ресурсы не задействуются, когда копируются большие файлы. Эта опция включена по умолчанию.

- **Сканирование**. В зависимости от типа обнаруженного файла автоматически выполняются следующие действия:

– **Действие по умолчанию для зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ). Агент безопасности Bitdefender может удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция известна как лечение.

По умолчанию, если зараженный файл обнаружен, агент безопасности Bitdefender автоматически попытается вылечить его. Если файл не удается вылечить, он перемещается в карантин в целях предотвращения распространения вируса. Вы можете изменить этот рекомендуемый поток в соответствии с вашими потребностями.

Важно
В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. В таких случаях выполняется удаление зараженного файла с диска.

– **Действие по умолчанию для подозрительных файлов.** Для обнаружения подозрительных файлов Bitdefender использует

Эвристический анализ и другие технологии . Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные). Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.

Если обнаружен подозрительный файл, доступ пользователей к этому файлу блокируется, во избежание потенциальной инфекции.

Хотя это и не рекомендуется, вы можете изменить действие по умолчанию. Можно определить два вида действий для каждого типа файлов. Доступны следующие действия:

Запретить доступ

Запретить доступ к обнаруженным файлам.

Важно

Для конечных точек MAC применяется опция перемещения в карантин (**Перейти на карантин**), а не запрета доступа (**Запретить доступ**).

Лечить

Удаляет вредоносный код из зараженных файлов. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов.

Удалить

Удаляет обнаруженные файлы с диска без предупреждения. Желательно избегать использование этого действия.

Перемещение файлов в карантин

Перемещает зараженные файлы из исходного расположения в папку карантина. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице консоли Quarantine.

Не предпринимать никаких действий

Система только сообщает, когда зараженные файлы обнаружены Bitdefender.

Вкладка **Дополнительные настройки** предназначена для сканирования при доступе на Linux-машинах. Используйте флажок, чтобы включить или отключить его.

В приведенной ниже таблице вы можете настроить каталоги Linux, которые вы хотите сканировать. По умолчанию есть пять записей, каждая из которых соответствует определенному местоположению в конечных точках: `/home`, `/ bin`, `/sbin`, `/usr`, `/etc`.

Добавить больше записей:

- Запишите любое имя пользовательского местоположения в поле поиска в верхней части таблицы.
- Выберите предопределенные каталоги из списка, отображаемого при нажатии стрелки в правом конце поля поиска.

Нажмите кнопку ⊕ **Добавить**, чтобы сохранить местоположение в таблице и кнопку ⊗ **Удалить**, чтобы удалить его.

Средство от вымогателей

Средство от вымогателей иммунизирует ваши машины против **известных** вымогателей, блокируя процесс шифрования, даже если компьютер заражен. Используйте флажок, чтобы включить или выключить средство от вымогателей.

Функция борьбы с вымогателями по умолчанию отключена. Лаборатория Bitdefender анализирует поведение широко распространенных программ-вымогателей, а для устранения новейших угроз с каждым обновлением механизмов защиты поставляются новые сигнатуры.

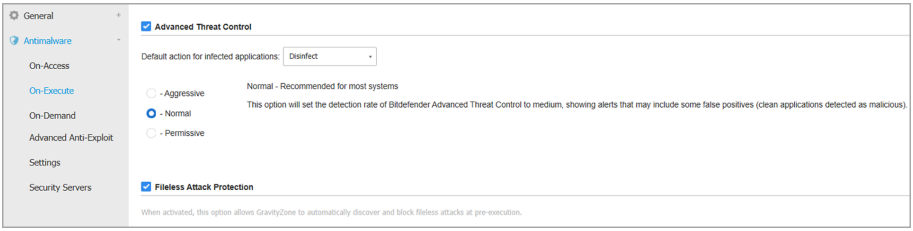
Предупреждение
Для большего повышения защиты от вымогателей, проявляйте осторожность в отношении нежелательных или подозрительных вложений и убедитесь, что все механизмы защиты обновлены.

Примечание
Вакцина от вымогателей доступна лишь при Bitdefender Endpoint Security Tools для Windows.

При выполнении

В этом разделе вы можете настроить защиту от вредоносных процессов, когда они выполняются. Он охватывает следующие защитные слои:

- Облачное обнаружение угроз
- Расширенный контроль угроз (Advanced Threat Control)
- Защита от безфайловых атак
- Смягчение последствий вымогателей



Политики - Настройки при выполнении

Расширенный контроль угроз (Advanced Threat Control)

Примечание

Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- ОС MAK

Bitdefender Advanced Threat Control - это технология проактивного обнаружения, которая использует расширенные эвристические методы для обнаружения новых потенциальных угроз в режиме реального времени.

Advanced Threat Control беспрерывно отслеживает приложения, запущенные на компьютере, на предмет признаков вредоносных действий. Для всех вышеперечисленных действий присваивается определенный балл и для каждого процесса подсчитывается общий рейтинг. При достижении общим рейтингом процесса заданного порогового значения, процесс считается вредоносным.

Advanced Threat Control будет автоматически пытаться вылечить обнаруженный файл. Если лечение не удалось, Advanced Threat Control удалит данный файл.

Примечание
Перед выполнением действий по лечению, копия файла отправляется в карантин, так что вы сможете позже восстановить данный файл в случае ложного срабатывания. Это действие может быть настроено с помощью опции **Скопируйте файлы на карантин перед применением дезинфицирующего действия.**, которая доступна на вкладке **Защита от вредоносных программ > Настройки** параметров политики. Эта опция включена по умолчанию в шаблонах политик.

Для настройки Advanced Threat Control:

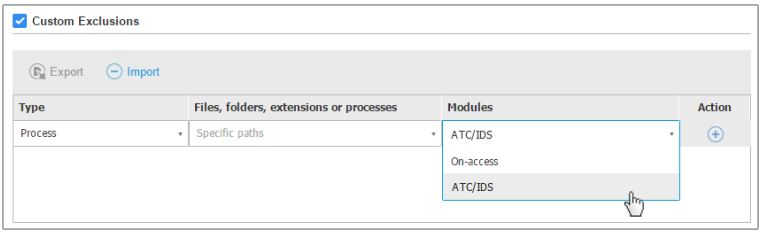
1. Установите этот флажок, чтобы включить или отключить Advanced Threat Control .

   Предупреждение
   Если вы выключите Advanced Threat Control, компьютеры станут уязвимы для неизвестного вредоносного ПО.

2. По умолчанию, используется действие лечения для инфицированных приложений, обнаруженных Advanced Threat Control . Вы можете задать другие действия по умолчанию, используя доступное меню:
   - **Блокировать** чтобы отказать в доступе к зараженному приложению.
   - **Не предпринимать действий**, только сообщать о зараженных приложениях, обнаруженных Bitdefender.
3. Выберите уровень безопасности, который наилучшим образом соответствует вашим потребностям (**Агрессивный, Обычный или Разрешительный**). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

   Примечание
   При установке более высокого уровня защиты Advanced Threat Control будет требовать меньше признаков вредоносного поведения для отметки процесса как вредоносного. В результате этого увеличится количество приложений, признанных вредоносными, при этом, также повысится вероятность ложных срабатываний (безопасные приложения отмечаются как вредоносные).

Настоятельно рекомендуется создать правила исключений для часто используемых или известных приложений, с целью предотвращения ложных срабатываний (ошибочное распознавание допустимых приложений). Перейдите на вкладку Защита от вредоносных программ > Настройки и настройте правила исключения процессов для доверенных приложений (ATC/IDS).



Политики компьютеров и виртуальных машин - Исключение процессов ATC/IDS

Защита от безфайловых атак

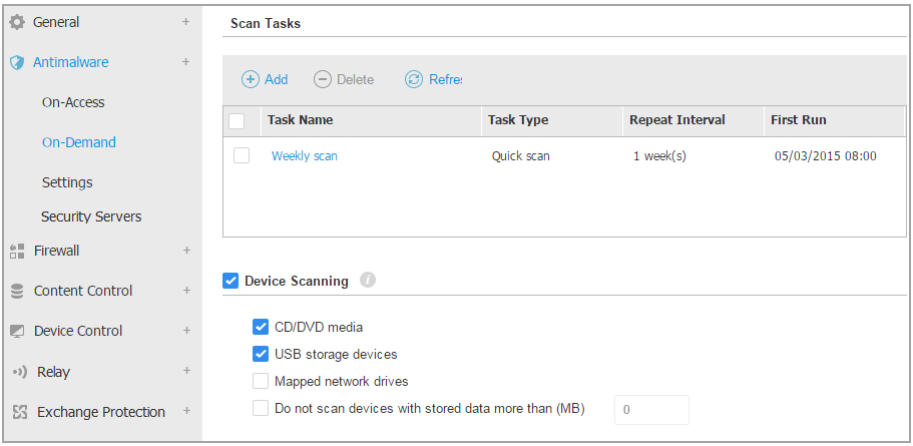
Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов

Защита от безфайловых атак обнаруживает и блокирует вредоносные безфайловые программы при предварительном выполнении, в том числе завершает работу PowerShell, запускающего вредоносную командную строку, блокирует вредоносный трафик, анализирует буфер памяти до внедрения кода и блокирует процесс внедрения кода.

Сканирование по запросу (On-Demand)

В этом разделе вы можете добавить и настроить задачи проверки защиты от вредоносного ПО, которые будут регулярно работать на определенных компьютерах, в соответствии с установленным графиком.



Политики компьютеров и виртуальных машин - Задачи сканирования по запросу

Сканирование производится в фоновом режиме, независимо от того вошел пользователь в систему или нет.

Хотя это и не обязательно, рекомендуется запланировать полное сканирование системы еженедельно на всех конечных точках. Регулярное сканирование конечных точек является активной мерой безопасности, которая может помочь обнаружить и блокировать вредоносные программы, которые могли обойти функции защиты в реальном времени.

Кроме того, вы также можете настроить регулярное сканирование внешних съемных носителей.

Управление задачами сканирования

Панель задач сканирования информирует вас о существующих задачах, предоставляя важную информацию о каждой из них:

- Имя и тип задачи.
- Расписание регулярно выполняемых задач (повторяющихся).
- Время первого запуска задачи.

Вы можете добавить и настроить следующие типы задач сканирования:

- **Быстрое сканирование** использует облачное сканирование для обнаружения вредоносных программ, запущенных в системе. Быстрое

сканирование занимает, как правило, менее минуты. Быстрое сканирование использует лишь незначительную часть системных ресурсов, в отличие от процесса стандартного антивирусного сканирования.

Bitdefender автоматически переходит к обезвреживанию, если обнаружены вредоносные программы или руткиты. Если по какой-либо причине файл нельзя вылечить, он перемещается в карантин. Этот тип сканирования игнорирует подозрительные файлы.

Быстрое сканирование (Quick Scan) - задача проверки по умолчанию с предустановленными опциями, которые не могут быть изменены. Вы можете добавить только одну задачу быстрого сканирования для одной политики.

- **Полное сканирование** (Full Scan) - проверяет все конечные точки по всем типам вредоносных программ, угрожающих безопасности, таких как вирусы, программы-шпионы, рекламное ПО, руткиты и другие.

  Bitdefender автоматически пытается обезвреживать файлы, обнаруженные вредоносными программами. Если вредоносная программа не может быть удалена, она перемещвется в карантин, где она не может навредить. Подозрительные файлы игнорируются. Если вы хотите принять меры и в отношении подозрительных файлов, или если вы хотите выполнить другие действия по умолчанию для зараженных файлов, выберите вариант «Запуск пользовательского сканирования».

  Полное сканирование - задача проверки по умолчанию с предустановленными опциями, которые не могут быть изменены. Вы можете добавить только одну задачу полного сканирования для одной политики.

- **Пользовательское сканирование** (Custom Scan) - позволяет выбирать расположение объектов для сканирования и настроить параметры сканирования.

- **Сетевое сканирование** (Network Scan) - это тип пользовательского сканирования, который может быть назначен одной управляемой конечной точке для сканирования сетевых дисков, задав определенные настройки параметров сканирования и указав определенные области, которые будут проверяться. Для агента безопасности вам необходимо ввести учетные данные пользователя с правами чтения/записи для выбранных сетевых дисков, чтобы иметь возможность получить доступ и выполнить требуемые действия на этих сетевых дисках.

Задача повторяющегося сетевого сканирования будет отправлена только выбранной сканирующей конечной точке. Если выбранная конечная точка недоступна, будут применены параметры локального сканирования.

Примечание
Создавать задачи сканирования сети можно только в политике, которая уже применяется к конечной точке, используемой в качестве сканера.

Кроме задач сканирования по умолчанию (которые вы не можете удалить или дублировать), вы можете создать столько пользовательских задач сканирования и задач сканирования сети, сколько вы хотите.

Чтобы создать и настроить новые пользовательские задачи или задачи сканирования сети, нажмите кнопку ⊕ **Добавить** в правой части таблицы. Чтобы изменить параметры существующей задачи сканирования, щелкните на имя этой задачи. Обратитесь к следующей теме, чтобы узнать, как настроить параметры задач.

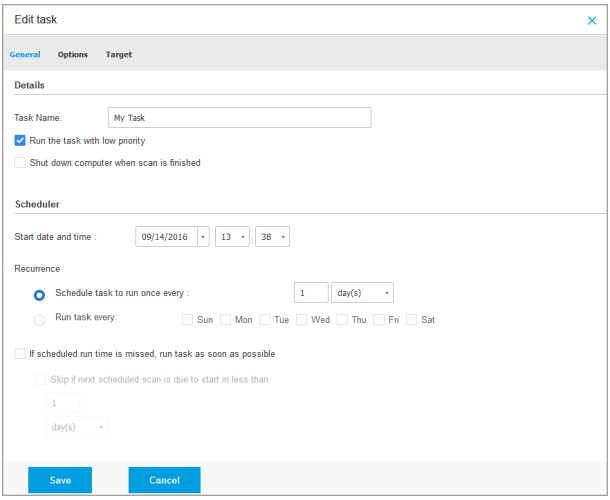
Чтобы удалить задачу из списка, выберите задачу и нажмите кнопку ⊖ **Удалить** в правой части таблицы.

Настройка задач сканирования

Настройки задач сканирования расположены в трех вкладках:

- **Общее**: имя задачи и график выполнения.
- **Опции**: выбор профиля сканирования для быстрой конфигурации параметров и настройка параметров проверки пользовательского сканирования.
- **Цель**: выбор файлов и папок, которые будут проверяться и настройка исключений сканирования.

Опции, от первой до последней вкладки, описаны далее:



Политики компьютеров и виртуальных машин - Общие настройки задач сканирования по запросу

- **Подробности.** Выберите подходящее имя задаче, которое поможет вам легче определить ее назначение. При выборе имени задачи, учитывайте ее назначение и возможные параметры сканирования.

  По умолчанию, задачи проверки запускаются с наименьшим приоритетом. Таким образом, Bitdefender позволяет другим программ работать быстрее, но увеличивает время, необходимое для завершения процесса проверки. Используйте флажок **Запустите задачу с низким приоритетом**, чтобы запретить или разрешить данную функцию.

  Примечание
  Эта опция применима только к Bitdefender Endpoint Security Tools и Endpoint Security (устаревший агент)

  Отметьте флажок **Выключите компьютер после завершения сканирования**, чтобы выключить машину, если вы не собираетесь использовать ее некоторое время.

  Примечание
  Эта опция применима к Bitdefender Endpoint Security Tools, Endpoint Security (устаревший агент) и Endpoint Security for Mac.

- **Проверка по расписанию.** Используйте параметры планирования для настройки расписаний сканирований. Вы можете установить время запуска задачи сканирования каждые несколько часов, дней или недель, начиная с указанной даты и времени.

  Конечные точки должны быть включены по графику. Запланированная задача сканирования не будет выполнятся если машина выключена, находится в режиме гибернации или в спящем режиме. В таких ситуациях, проверка будет отложена до следующего раза.

  Примечание
  Проверка по расписанию будет работать на выбранных конечных точках с учетом местного времени. Например, если запланирована задача сканирования, которая должна начаться в 6:00, и конечная точка находится в другом часовом поясе с Control Center, задача сканирования начнется в 6:00 (по времени конечной точки).

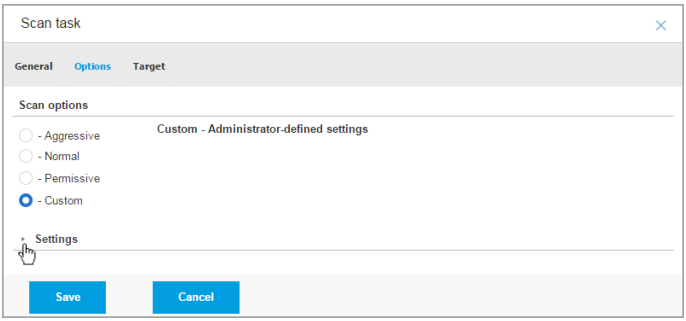
  При желании вы можете указать, что происходит, когда задача проверки не может быть запущена в запланированное время (конечная точка была отключена или отключена). Используйте параметр **Если запланированное время выполнения пропущено, запустите задачу как можно скорее** в соответствии с вашими потребностями:

  – Если вы оставите этот флажок выключенным, задача проверки будет выполняться снова в следующий запланированный момент времени.

  – Когда вы выбираете опцию, вы запускаете сканирование как можно скорее. Чтобы настроить оптимальное время выполнения сканирования и не беспокоить пользователя в рабочее время, выберите **Пропустить, если следующее запланированное сканирование должно начаться менее чем через**, затем укажите интервал, который вы хотите.

- **Параметры сканирования.** Выберите уровень безопасности, который лучше всего соответствует вашим потребностям (Интенсивный, Нормальный или Рекомендуемый). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

  В зависимости от выбранного профиля, параметры сканирования в разделе **Настройки** будут сконфигурированы автоматически. Тем не менее, при желании, вы можете настроить их более детально. Чтобы сделать это, отметьте флажком опцию **Пользователь** и затем перейдите в раздел **Настройки**.



Задачи сканирования компьютеров - Настройка пользовательского режима

- **Типы файлов.** Используйте данную настройку, чтобы задать типы файлов, которые вы хотите просканировать. Вы можете указать агенту безопасности просканировать все файлы (независимо от их расширений), только файлы приложений или специфические типы файлов, которые вы считаете потенциально опасными. При сканировании всех файлов обеспечивается оптимальная защита. Сканируя только приложения, можно повысить скорость сканирования.

  Примечание

  Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 610).

  Если вы хотите просканировать только файлы со специфическими расширениями, выберите в меню **Пользовательские расширения** и затем введите желаемые расширения в редактируемом поле, нажимая `Войти` после каждого расширения.

- **Архивы.** Архивы, содержащие инфицированные файлы, не представляют непосредственной угрозы безопасности системы. Вредоносные программы могут повлиять на систему только если зараженный файл извлечен из архива и будет исполнен при выключенной защите в реальном времени. Тем не менее, рекомендуется использовать этот параметр для обнаружения и удаления всех угроз, даже тех, которые не представляют собой непосредственной опасности для системы.

Примечание
Сканирование файлов, сжатых в архив, увеличивает общее время сканирования и занимает больший объем системных ресурсов.

– **Сканирование внутри архивов.** Выберите эту опцию, если вы хотите проверить заархивированные файлы на наличие вредоносных программ. Если вы решили использовать данную опцию, вам необходимо настроить следующие параметры оптимизации:

  - **Ограничение размера архива (Мб).** Вы можете установить максимально допустимый размер архивов для сканирования. Поставьте флажок в соответствующем поле и введите максимальный размер архива (в МБ).
  - **Максимальная глубина архива (уровни).** Отметьте соответствующий флажок и выберите в меню максимальную глубину архива. Для лучшей производительности выберите наименьшее значение, для максимальной защиты выберите наибольшее значение.

– **Сканировать архивы электронной почты.** Выберите данную опцию если хотите разрешить проверку почтовых сообщений и почтовых баз, включая такие форматы файлов как .eml, .msg, .pst, .dbx, .mbx, .tbb и другие.

Примечание
Процесс сканирования почтовых архивов является достаточно ресурсоемким и может повлиять на производительность системы.

- **Разное.** Выберите соответствующие флажки, чтобы включить нужные параметры сканирования.

  – **Сканирование загрузочных секторов.** Проверка загрузочных секторов системы. Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки. Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.

  – **Сканирование реестра.** Выберите этот параметр для сканирования ключей реестра. Реестр Windows — это база данных, в которой хранятся настройки и параметры конфигурации для компонентов операционной системы Windows и установленных приложений.

- **Сканирование на наличие руткитов.** Выберите этот параметр для сканирования на наличие руткитов и объектов, скрытых с помощью такого программного обеспечения.
- **Сканирование на наличие клавиатурных шпионов.** Выберите данную опцию для сканирования системы на наличие клавиатурных шпионов.
- **Сканировать общие сетевые ресурсы.** Эта опция сканирует подключенные сетевые диски.

  Для быстрого сканирования эта опция отключена по умолчанию. Для полного сканирования опция активирована по умолчанию. Для сканирования по выбору пользователя, если вы установите уровень безопасности **Интенсивный/Нормальный**, параметр **Сканирование общих сетевых ресурсов** включается автоматически. Если вы установите уровень безопасности **Рекомендуемый**, параметр **Сканирование общих сетевых ресурсов** автоматически отключается.
- **Сканирование памяти.** Выберите этот параметр для сканирования программ, запущенных в системной памяти.
- **Сканирование файлов cookie.** Выберите эту опцию для сканирования файлов cookie, сохраненных браузерами на конечных точках.
- **Сканирование только новых/измененных файлов.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие системы с минимальными потерями в безопасности.
- **Сканирование на наличие потенциально нежелательных приложений (PUA).** Потенциально нежелательные приложения (PUA) это программы, которые могут быть нежелательными для ПК, а иногда и поставляться в комплекте с программным обеспечением бесплатного. Такие программы могут быть установлены без согласия (также называются рекламными) или включены по умолчанию в комплект экспресс-установки (как дополнение). Потенциальное воздействие этих программ заключается в показе всплывающих окон, установке нежелательных панелей инструментов в браузере по умолчанию или работе нескольких процессов в фоновом режиме, что замедляет производительность компьютера.

- **Действия.** В зависимости от типа обнаруженного файла автоматически выполняются следующие действия:

– **Действие по умолчанию для зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ). Агент безопасности может удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция известна как лечение.

  Если зараженный файл обнаружен, агент безопасности будет пытаться вылечить его автоматически. Если файл не удается вылечить, он перемещается в карантин в целях предотвращения распространения вируса.

  Важно
  В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. В таких случаях выполняется удаление зараженного файла с диска.

– **Действие по умолчанию для подозрительных файлов.** Для обнаружения подозрительных файлов Bitdefender использует Эвристический анализ и другие технологии . Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные). Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.

  По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин. Помещенные в карантин файлы отправляются на анализ в лабораторию Bitdefender на регулярной основе. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить.

– **Действие по умолчанию для руткитов.** Руткиты представляют собой специализированное программное обеспечение, используемое для того, чтобы скрыть файлы операционной системы. Однако, руткиты часто используются, чтобы скрыть вредоносные программы, либо для сокрытия присутствия злоумышленника в системе.

  Обнаруженные руткиты и скрытые файлы по умолчанию игнорируются.

Хотя это и не рекомендуется, вы можете изменить действие по умолчанию. Можно задать дополнительное действие, которое будет выполнено в случае, если не удалось выполнить первое, а также различные действия для каждой из категорий. Выберите в соответствующих меню первое и второе действие, которые будут выполняться в отношении всех типов обнаруженных файлов. Доступны следующие действия:

Не предпринимать никаких действий
Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования.

Лечить
Удаляет вредоносный код из зараженных файлов. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов.

Удалить
Удаляет обнаруженные файлы с диска без предупреждения. Желательно избегать использование этого действия.

Перемещение файлов в карантин
Перемещает зараженные файлы из исходного расположения в папку карантина. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице консоли Quarantine.

- **Сканирование объектов.** Добавьте в список все области, которые вы хотите просканировать, на выбранных компьютерах.

  Чтобы добавить новый файл или папку для сканирования:

  1. Выберите предопределенное месторасположение из выпадающего меню или введите конкретные пути в **конкретные пути**, которые вы хотите просканировать.
  2. Укажите путь к объекту для сканирования в поле редактирования.
     – Если вы выбрали предопределенное место, необходимо корректно завершить путь. Например, для сканирования всей папки `Програмные файлы`, достаточно выбрать соответствующее предопределенное место из выпадающего меню. Для сканирования конкретной папки из `Програмные файлы`, необходимо завершить путь, добавив обратную косую черту (\) и имя папки.

– Если вы выбрали **Конкретные пути**, введите полный путь к объекту проверки. Желательно использовать системные переменные (в соответствующих случаях), чтобы быть уверенным, что путь действителен для всех нужных компьютеров.

3. Нажмите соответствующую кнопку ⊕ **Добавить**.

Чтобы изменить существующий путь, нажмите на него. Чтобы удалить папку из списка, наведите курсор на эту папку и нажмите соответствующую кнопку ⊖ **Удалить**.

- Для агента безопасности вам необходимо ввести учетные данные пользователя с правами чтения/записи для выбранных сетевых дисков, чтобы иметь возможность получить доступ и выполнить требуемые действия на этих сетевых дисках.
- **Исключения.** Вы можете использовать либо исключения, определенные в разделе **Защита от вредоносных программ > Исключения** нынешней политики, либо вы можете задать пользовательские исключения для текущего задания сканирования. За более подробной информацией об исключениях, обратитесь к «Исключения» (p. 312).

Сканирование устройств

Вы можете настроить агент безопасности на автоматическое обнаружение и сканирование внешних устройств хранения данных при их подключении к конечной точке. Обнаруженные устройства относятся к одной из следующих категорий:

- CD/DVD
- Запоминающие устройства USB, такие как флэш-носители и внешние жесткие диски
- Устройства с более определенным количеством хранимых данных.

Сканирование устройств автоматически попытается вылечить файлы, обнаруженные как зараженные или переместит их в карантин, если лечение невозможно. Обратите внимание, что некоторые устройства, такие как CD/DVD, предназначены только для чтения. Никакие действия не могут быть предприняты для зараженных файлов, содержащихся в такой поддержке хранилища.

Примечание
Во время сканирования устройства пользователь может получать доступ к любым данным этого устройства.

Если всплывающие предупреждения включены в разделе **Основные> Уведомления**, то вместо автоматического запуска, у пользователя будет запрошено действие на сканирование или отмену сканирования обнаруженного устройства.

При запуске сканирования устройства:

- Всплывающее уведомление информирует пользователя о сканировании устройства, при условии, что всплывающие уведомления включены в разделе **Основные > Уведомления**.

После завершения задачи сканирования, пользователь должен проверить обнаруженные угрозы, если таковые имеются.

Выберите опцию **Сканирование устройства** для того, чтобы включить автоматическое обнаружение и сканирование устройств хранения. Чтобы настроить проверку устройств индивидуально для каждого типа устройства, используйте следующие параметры:

- **Носители CD/DVD**
- **Запоминающие устройства USB**
- **Не сканируйте устройства с сохраненными данными более(MB)**. Используйте эту опцию, чтобы автоматически пропускать сканирование обнаруженного устройства, если количество хранимых данных превысит указанный объем. Введите в соответствующем поле ограничение по размеру (в мегабайтах). Ноль означает, что ограничения по размеру не предусмотрены.

Обнаружение гипервизора

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- Linux

HyperDetect добавляет дополнительный уровень безопасности к существующим технологиям сканирования (сканирование при доступе, по требованию и сканирование трафика) для борьбы с новым поколением киберугроз, включая вирусы для атак на объекты критической инфраструктуры (APT). Hyper Detect расширяет модули защиты от вредоносных программ и контента с помощью мощных эвристических программ на основе искусственного интеллекта и машинного обучения.

Благодаря своей способности прогнозировать целенаправленные атаки и обнаруживать самые сложные вредоносные программы на этапе предварительного исполнения, HyperDetect обнаруживает угрозы намного быстрее, чем технологии, основанные на сигнатуре или поведенческом режиме.

Чтобы настроить HyperDetect:

1. Установите флажок **HyperDetect** , чтобы включить или выключить модуль.
2. Выберите, от какого типа угроз вы хотите защитить свою сеть. По умолчанию защита включена для всех типов угроз: целенаправленных атак, подозрительных файлов и сетевого трафика, эксплойтов, вирусов-вымогателей или условно вредоносного ПО .

   Примечание
   Для эвристики сетевого трафика требуется включить **Контроль контента > Сканирование трафика** .

3. Настройте уровень защиты от угроз выбранных типов.

   Используйте главный переключатель в верхней части списка угроз, чтобы выбрать уникальный уровень защиты для всех типов объектов, или выберите индивидуальные уровни для точной настройки защиты.

   Установка модуля на определенном уровне приведет к тому, что действия будут приняты на этом уровне. Например, если установлено значение **Нормальный уровень** , модуль обнаруживает и сдерживает угрозы, подходящие под параметр **Рекомендуемый уровень** и **Нормальный уровень** , но не **Интенсивный уровень**.

   Защита увеличивается от уровня **Рекомендуемый** до **Интенсивный**.

   Имейте в виду, что Интенсивный уровень защиты может привести к ложным срабатываниям, в то время как Рекомендуемый уровень может подвергнуть вашу сеть некоторым угрозам. Рекомендуется сначала

установить уровень защиты на максимум, а затем постепенно снижать его в случае множества ложных срабатываний, пока вы не достигнете оптимального баланса.

Примечание
Всякий раз, когда вы включаете защиту для типа угроз, для их обнаружения автоматически устанавливается значение по умолчанию (уровень **Нормальный**).

4. В разделе **Действия** настройте реакцию HyperDetect на обнаруженное ПО. Используйте параметры раскрывающегося меню, чтобы установить действие, которое необходимо предпринять в случае обнаружения угроз:
   - Для файлов: запретить доступ, обезвреживание, удаление, карантин или просто отчет о файле.
   - Для сетевого трафика: блокировать или просто сообщать о подозрительном трафике.
5. Установите флажок **Расширить отчетность на более высоких уровнях** рядом с раскрывающимся меню, если вы хотите просматривать угрозы, обнаруженные на более высоких уровнях защиты, чем установленные.

Если вы не уверены в текущей конфигурации, вы можете легко восстановить первоначальные настройки, нажав кнопку **Сбросить по умолчанию** в нижней части страницы.

Advanced Anti-Exploit

Примечание
Данный модуль доступен для:
- Windows для рабочих станций

Advanced Anti-Exploit - активная технология для обнаружения эксплойтов в реальном времени. Основанная на машинном, она защищает от известных и неизвестных эксплойтов, включая безфайловые атаки.

Чтобы активировать защиту от эксплойтов, отметьте галочку напротив **Advanced Anti-Exploit**.

Advanced Anti-Exploit изначально настроен на запуск с рекомендуемыми параметрами. Вы можете настроить защиту по-другому, если это необходимо.

Для восстановления изначальных настроек, нажмите на ссылку **Настройки по умолчанию** в правой части заголовка раздела.

Настройки анти-эксплойта в GravityZone распределены по трем разделам:

- **Общесистемные обнаружения**

  Методы защиты от эксплойтов в этом разделе отслеживают системные процессы, которые являются объектами эксплойтов.

  Для получения дополнительной информации о доступных методах и о том, как настроить их параметры, см. «Настройка общесистемного смягчения» (p. 305).

- **Предопределенные приложения**

  Модуль Advanced Anti-Exploit предварительно настроен со списком распространенных приложений, таких как Microsoft Office, Adobe Reader или Flash Player, которые наиболее подвержены эксплойтам.

  Для получения дополнительной информации о доступных методах и о том, как настроить их параметры, см. «Настройка Application-Specific Techniques» (p. 306).

- **Дополнительные приложения**

  В этом разделе вы можете добавить и настроить защиту для других приложений на ваш выбор.

  Для получения дополнительной информации о доступных методах и о том, как настроить их параметры, см. «Настройка Application-Specific Techniques» (p. 306).

Вы можете развернуть или свернуть любой раздел, нажав его заголовок. Таким образом, вы быстро перейдете к параметрам, которые хотите настроить.

Настройка общесистемного смягчения

В данном разделе присутствуют следующие опции:

Метод	Описание
Повышение прав	Предотвращает процессы, направленные на получение несанкционированных привилегий и доступа к ресурсам.

Метод	Описание
	Действие по умолчанию: Завершает процесс
Защита процесса LSASS	Защищает процесс LSASS от утечки секретной информации, такой как хеши паролей и настройки безопасности. Действие по умолчанию: Блокирует процесс

Эти методы защиты от эксплойтов включены по умолчанию. Чтобы отключить любой из методов, снимите флажок.

При желании вы можете изменить действие, предпринимаемое автоматически при обнаружении. Выберите действие, доступное в соответствующем меню:

- **Завершить процесс**: немедленно завершает эксплуатируемый процесс.
- **Блокировать процесс**: предотвращает доступ вредоносного процесса к недоверенным ресурсам.
- **Только отчет**: GravityZone сообщает о событии без каких-либо действий по смягчению последствий. Вы можете просмотреть подробности события в уведомлении **Advanced Anti-Exploit**, а также в отчетах "Заблокированные приложения" и "Аудит безопасности".

Настройка Application-Specific Techniques

Будь то предопределенные или дополнительные приложения, все они используют один и тот же набор методов защиты от эксплойтов. Вы можете найти описание здесь:

Метод	Описание
ROP Emulation	Обнаруживает попытки сделать страницы памяти данных исполняемыми, использующие метод возвратно-ориентированного программирования (ROP). Действие по умолчанию: Завершить процесс
ROP Stack Pivot	Обнаруживает попытки перехвата потока кода, использующих метод ROP, путем проверки местоположения стека. Действие по умолчанию: Завершить процесс

Метод	Описание
ROP Illegal Call	Обнаруживает попытки перехвата потока кода, использующих метод ROP,путем проверки инициаторов вызова чувствительных системных функций. Действие по умолчанию: Завершить процесс
ROP Stack Misaligned	Обнаруживает попытки повреждения стека, использующих метод ROP, путем проверки выравнивания адресов стека. Действие по умолчанию: Завершить процесс
ROP Return To Stack	Обнаруживает попытки выполнения кода непосредственно в стеке, использующих метод ROP, путем проверки диапазона адресов возврата. Действие по умолчанию: Завершить процесс
ROP сделать стек исполняемым	Обнаруживает попытки повреждения стека, использующих метод ROP, путем проверки защиты страницы стека. Действие по умолчанию: Завершить процесс
Flash Generic	Обнаруживает попытки эксплуатации Flash Player. Действие по умолчанию: Завершить процесс
Flash Payload	Обнаруживает попытки выполнения вредоносного кода во Flash Player путем сканирования объектов Flash в памяти. Действие по умолчанию: Завершить процесс
VBScript Generic	Обнаруживает попытки использования VBScript. Действие по умолчанию: Завершить процесс
Выполнение Shellcode	Обнаруживает попытки создания новых процессов или загрузки файлов, использующих шелл-код. Действие по умолчанию: Завершить процесс
Библиотека загрузки шелл-кода	Обнаруживает попытки выполнения кода по сетевым путям, использующих шелл-код. Действие по умолчанию: Завершить процесс

Метод	Описание
Anti-Detour	Обнаруживает попытки обхода проверки безопасности для создания новых процессов. Действие по умолчанию: Завершить процесс
Shellcode EAF (Export Address Filtering)	Обнаруживает попытки получения вредоносным кодом доступа к чувствительным системным функциям из экспорта DLL. Действие по умолчанию: Завершить процесс
Shellcode Thread	Обнаруживает попытки внедрения вредоносного кода путем проверки вновь созданных потоков. Действие по умолчанию: Завершить процесс
Anti-Meterpreter	Обнаруживает попытки создания обратной оболочки путем сканирования страниц исполняемой памяти. Действие по умолчанию: Завершить процесс
Создание процесса устарело	Обнаруживает попытки создания новых процессов с использованием устаревших методов. Действие по умолчанию: Завершить процесс
Создание дочернего процесса	Блокирует создание любого дочернего процесса. Действие по умолчанию: Завершить процесс
Enforce Windows DEP	Обеспечивает предотвращение выполнения данных (DEP) для блокировки выполнения кода на страницах данных. По умолчанию: Отключено
Принудительное перемещение модулей (ASLR)	Предотвращает загрузку кода в предсказуемые места путем перемещения модулей памяти. По умолчанию: Включено
Новые эксплойты	Защищает от любых новых возникающих угроз или эксплойтов. Быстрые обновления используются для этой категории, прежде чем могут быть сделаны более всеобъемлющие изменения. По умолчанию: Включено

Чтобы отслеживать другие приложения, кроме предопределенных, нажмите кнопку **Добавить приложение**, расположенную вверху и внизу страницы.

Чтобы настроить параметры защиты от эксплойтов для приложения:

1. Для существующих приложений, нажмите на название приложения. Для новых приложений нажмите кнопку **Добавить**.

   На новой странице отображаются все методы и их настройки для выбранного приложения.

   Важно
   Будьте осторожны при добавлении новых приложений для мониторинга. Bitdefender не может гарантировать совместимость с любым приложением. Таким образом, рекомендуется сначала протестировать функцию на нескольких некритичных конечных точках, а затем развернуть ее в сети.

2. При добавлении нового приложения введите его имя и имена его процессов в соответствующие поля. Используйте точку с запятой (;) для разделения процессов.
3. Если необходимо быстро проверить описание метода, нажмите на стрелку рядом с его названием.
4. При необходимости установите или снимите флажки используемых методов.

   Используйте опцию **Все**, если хотите выделить все методы разом.
5. Если необходимо, измените автоматическое действие при обнаружении. Выберите действие, доступное в соответствующем меню:
   - **Завершить процесс**: немедленно завершает эксплуатируемый процесс.
   - **Только отчет**: GravityZone сообщает о событии без каких-либо действий по смягчению последствий. Подробные сведения о событии можно просмотреть в уведомлении **Advanced Anti-Exploit** и в отчетах.

   По умолчанию все методы для предопределенных приложений настроены для смягчения проблемы, а для дополнительных приложений - просто сообщать о событии.

   Для быстрой смены действия, применяемого ко всем методам зашиты сразу, выберите действие из меню, соответствующее варианту **Все**.

Нажмите кнопку **Назад** в верхней части страницы для того, чтобы вернуться к общим настройкам модуля Anti-Exploit.

Настройки

В этом разделе вы можете настроить параметры карантина и правила исключений для сканирования.

- Изменение настроек карантина
- Настройка исключений сканирования

Карантин

Вы можете настроить следующие параметры для файлов в карантине на конечных точках:

- **Удалить файлы, чей срок более (дней)..** По умолчанию, файлы в карантине старше 30 дней автоматически удаляются. Если вы хотите изменить этот интервал, выберите другой вариант из меню.
- **Отправить помещенные в карантин файлы Bitdefender Лаборатории каждые (часы).** По умолчанию файлы из карантина автоматически отправляются в лаборатории Bitdefender каждый час. Вы можете отредактировать интервал времени отправки файлов из карантина (один час по умолчанию). Специалисты по вирусам Bitdefender проанализируют образцы файлов. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить.
- **Повторно сканировать файлы из карантина после обновления механизмов защиты.** Выберите данную опцию для автоматического сканирования файлов карантина после каждого обновления механизмов защиты. Очищенные файлы автоматически возвращаются на свое место.
- **Скопируйте файлы на карантин перед применением дезинфицирующего действия.** Выберите эту опцию, чтобы предотвратить потерю данных в случае ложных срабатываний и копировать каждый инфицированный файл в карантине перед лечением. После этого вы сможете восстановить здоровые файлы из карантина на странице **Карантин**.
- **Разрешить пользователям выполнять действия в локальном карантине.** Этот параметр управляет действиями, которые пользователи конечной точки могут предпринять в локальных файлах, помещенных на карантин, с помощью интерфейса Bitdefender Endpoint Security Tools. По умолчанию

локальные пользователи могут восстанавливать или удалять файлы, помещенные на карантин, с помощью параметров, доступных в Bitdefender Endpoint Security Tools. Отключив эту опцию, пользователи больше не будут иметь доступа из интерфейса Bitdefender Endpoint Security Tools к кнопкам действий с файлами на карантине.

Централизованный карантин

Если файлы, помещенные на карантин из конечных точек, необходимо сохранить для дальнейшего анализа, используйте параметр **Централизованный карантин**, который отправляет архивированную копию каждого локального файла, помещенного на карантин, в общий сетевой ресурс.

После включения этого параметра каждый файл, помещенный на карантин из управляемых конечных точек, копируется и упаковывается в защищенный паролем ZIP-архив на указанное расположение в сети. Именем архива является хэш файла, помещенного в карантин.

Важно
Максимальный размер архива составляет 100 МБ. Если архив превышает 100 МБ, он не будет сохранен в общей сетевой папке.

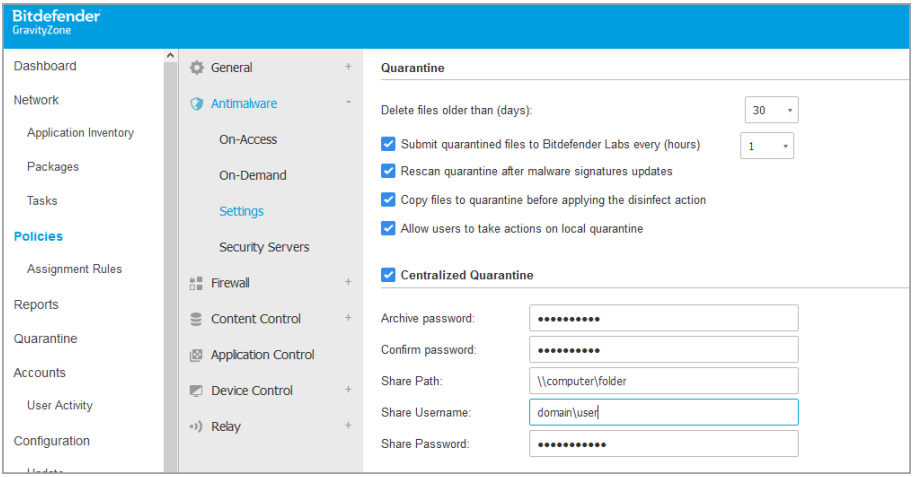
Чтобы настроить параметры централизованного карантина, заполните следующие поля:

- **Пароль архива**: введите пароль для архива файлов, помещенных в карантин. Пароль должен содержать, по крайней мере, один символ верхнего регистра, по крайней мере, одну строчную букву и, по крайней мере, одну цифру или специальный символ. Подтвердите пароль в следующем поле.
- **Общий путь**: введите сетевой путь, в котором будут храниться архивы (например, `\\computer\folder`).
- Имя пользователя и пароль, необходимые для подключения к сетевой папке. Поддерживаемые форматы для имени пользователя:
  - `username@domain`
  - `domain\username`
  - `Имя пользователя`.

Для корректной работы централизованного карантина убедитесь, что выполнены следующие условия:

- Общее расположение доступно в сети.
- Конечные точки имеют подключение к сетевому ресурсу.
- Учетные данные для выполнения входа являются действительными и предоставляют доступ к записи на сетевом ресурсе.
- На сетевом ресурсе достаточно места на диске.

Примечание
Централизованный карантин не применяется к карантину почтовых серверов.



Централизованный карантин

Если у вас есть локальный экземпляр Sandbox Analyzer, настроенный в разделе **Sandbox Analyzer> Датчик конечной точки** , вы можете установить флажок **Автоматически отправлять элементы из карантина в Sandbox Analyzer** . Обратите внимание, что представленные элементы должны иметь максимальный размер 50 МБ.

Исключения

Агент безопасности Bitdefender может исключить из сканирования определенные типы объектов. Исключения при сканировании должны использоваться в особых случаях или при рекомендациях Microsoft или

Bitdefender. Чтобы просмотреть обновленный список исключений, рекомендованный Microsoft, пожалуйста, обратитесь к этой статье article.

В этом разделе вы можете настроить использование различных типов исключений агентом безопасности Bitdefender.

- **Встроенные исключения**, которые по умолчанию доступны и включены в агенте безопасности Bitdefender.

  Вы можете отключить встроенные исключения, если хотите просканировать все типы объектов, но этот вариант будет значительно влиять на производительность машины и увеличит время сканирования.

- Вы также можете задать **Пользовательские исключения** для собственных приложений или специально настроенных утилит, в соответствии с вашими требованиями.

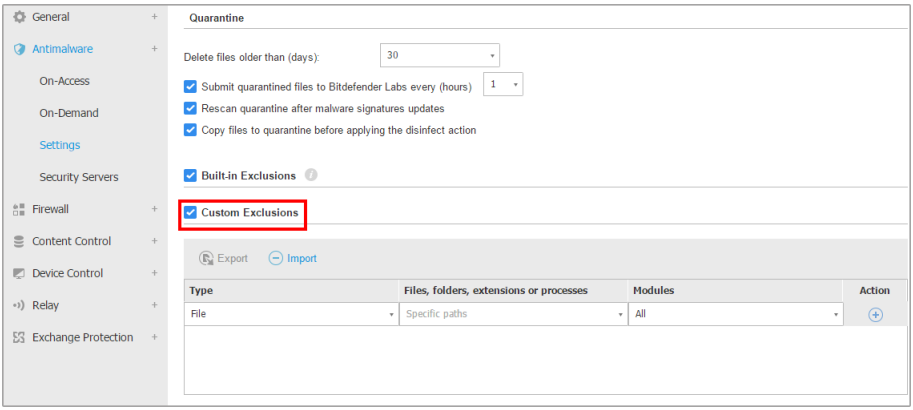
  Пользовательские исключения сканирования применяются к одному или нескольким следующим методам:

  – Сканирование при доступе
  – Сканирование по требованию
  – Расширенный контроль угроз (Advanced Threat Control)
  – Защита от безфайловых атак

  Важно

  – При наличии тестового файла EICAR, который периодически используется для тестирования защиты от вредоносных программ, необходимо исключить его из сканирования при доступе.
  – Если вы используете VMware Horizon View 7 и AppStacks AppStacks, пожалуйста, ознакомьтесь с Документ VMware .

  Для исключения определенных элементов из сканирования, отметьте галочку **Пользовательские исключения** и добавьте правила в таблицу снизу.



Политики компьютеров и виртуальных машин - Пользовательские исключения

Чтобы добавить пользовательское правило исключений:

1. Выберите тип исключения из меню:
   - **Файл**: только указанный файл
   - **Папка**: все файлы и процессы внутри указанной папки и всех подпапок.
   - **Расширение**: все элементы с указанным расширением
   - **Процесс**: любой объект доступный данному исключенному процессу.
   - **Хэш файла**: файл с указанным хэшем
   - **Хэш Сертификата**: все приложения с указанным хэшем сертификата (отпечатком)
   - **Название угрозы**: любой элемент с именем обнаружения (недоступно для операционных систем Linux)
   - **Командная строка**: указанная командная строка (доступно только для операционных систем Windows)

Предупреждение
В безагентной среде VMware , интегрированной с VSHIELD, вы можете исключать только папки и расширения. Установив Bitdefender Tools на виртуальных машинах, вы также сможете исключать файлы и процессы.

Во время процесса установки, при настройке пакета, вам необходимо отметить соответствующий флажок **Развертывание конечной точки с помощью vShield при обнаружении среды VMware, интегрированной с vShield** Для получения дополнительной информации обратитесь к разделу **Создание инсталляционных пакетов** Руководства по установке.

2. Заполните информацию для указанного типа исключения:

   Файл, Папка или Процесс

   Введите путь к элементу, исключаемому из сканирования. Для написания пути вы можете воспользоваться несколькими способами:

   – Указать путь явно.

     Например: `C: emp`

     Чтобы добавить исключение в формате UNC, используйте следующий синтаксис:

     `\\hostName\shareName\filePath`

     `\\IPaddress\shareName\filePath`

   – Используйте системные переменные, доступные из выпадающего меню.

     Для исключения процесса необходимо также добавить имя исполняемого файла приложения.

     Например:

     `%ProgramFiles%` - исключает папку Program Files

     `%WINDIR%\system32` – исключает папку system32 в папке Windows

     Примечание
     Желательно использовать системные переменные (где это возможно), чтобы путь был действительным для всех выбранных компьютеров.

   – Используйте подстановочные символы.

     Звездочка (*) заменяет неопределенное количество символов. Вопросительный знак (?) заменяет только один символ. Вы можете использовать несколько вопросительных знаков, чтобы задать любую возможную комбинацию из определенного количества

символов. Например, ??? заменяет любую комбинацию, состоящую из трех символов.

Например:

Исключения файлов:

`C:\Test\*` - исключает все файлы из папки Test

`C:\Test\*.png` - Исключает все PNG файлы из папки Test

Исключение папок:

`C:\Test\*` - исключает все папки из папки Test

Исключения процесса:

`C:\Program Files\WindowsApps\Microsoft.Not??.exe` – Исключает все процессы Microsoft Notes

Примечание
Исключения процессов не поддерживают подстановочные символы в операционных системах Linux.

Расширение

Укажите одно или несколько расширений файлов для исключения из сканирования, разделив их точкой с запятой ";". Можно вводить расширения с или без точки. Например, введите txt, чтобы исключить текстовые файлы.

Примечание
В системах на основе Linux расширения файлов чувствительны к регистру, а файлы с одинаковым именем, но с другим расширением считаются различными объектами. Например, `file.txt` и `file.TXT` - разные файлы.

Хэш файла, Хэш сертификата, Имя угрозы или Командная строка

Введите хэш файла, отпечаток сертификата (хэш), точное название угрозы и командную строку в зависимости от правила исключения. Вы можете использовать один элемент для исключения.

3. Выберите методы сканирования, к которым правило будет применяться. Некоторые исключения могут быть актуальны только для сканирования при доступе, некоторые только для сканирования

по запросу, некоторые только для ATC/IDS,а другие могут быть рекомендованы для всех трех модулей.

4. При необходимости нажмите кнопку **Показать замечания**, чтобы добавить заметку о правиле в столбец **Замечания**.
5. Нажмите кнопку ⊕ **Добавить**.

   Новое правило будет добавлено в список.

Чтобы удалить правило из списка, нажмите соответствующую кнопку ⊗ **Удалить**.

Важно
Пожалуйста, обратите внимание, что исключения сканирования по запросу НЕ будут применяться к контекстному сканированию. Контекстное сканирование запускается при нажатии правой кнопки мыши на файле или папке и выборе **Сканировать с Bitdefender Endpoint Security Tools**.

Импорт и экспорт исключений

Если вы намерены использовать правила исключений в других политиках, вы можете их экспортировать и импортировать.

Чтобы экспортировать пользовательские исключения:

1. Нажмите **Экспорт** в верхней части таблицы исключений.
2. Сохраните файл CSV на вашем компьютере. В зависимости от настроек вашего браузера, файл может автоматически загрузится или вам будет предложено сохранить его в определенное место.

Каждая строка в файле CSV соответствует одному правилу с полями в следующем порядке:

```
<exclusion type>, <object to be excluded>, <modules>
```

Доступные значения для полей в файле CSV:

Тип исключения:

1, для исключений файлов

2, для исключений папок

3, для исключений расширений

4, для исключений процессов

5, для исключений хеша файла

6, для исключений хеша сертификата

7, для исключений по имени угрозы

8, для исключений командной строки

Исключаемый объект:

Путь или расширение файла

Модули:

1, для сканирования по запросу

2, для сканирования при доступе

3, для всех модулей

4, для ATC/IDS

Например, файл CSV, содержащий исключения, может выглядеть следующим образом:

```
1,"d:\\temp",1
1,%WinDir%,3
4,"%WINDIR%\\system32",4
```

Примечание

Пути Windows должны иметь двойной обратный слеш (\). Например, `%WinDir%\\System32\\LogFiles`.

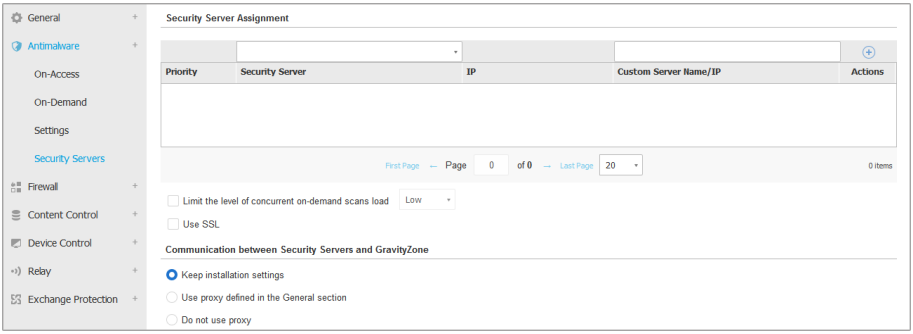
Чтобы ипортировать пользовательские исключения:

1. Нажмите **Импорт**. Откроется окно **Import Policy Exclusions**.
2. Нажмите **Добавить** и затем выберите файл CSV.
3. Нажмите **Сохранить**. Таблица заполняется корректными правилами. Если файл CSV содержит некорректные правила, предупреждение проинформирует вас о соответствующих номерах строк.

Серверы безопасности (Security Server)

В данном разделе вы можете настроить:

- Назначение Security Server
- Специальные настройки Security Server



Политики - Компьютеры и виртуальные машины - Защита от вредоносного ПО - Серверы безопасности

Назначение Security Server

Вы можете назначить один или несколько Security Server целевым конечным точкам и установить приоритет, с которым конечные точки будут выбирать Security Server для отправки запросов сканирования.

Примечание
Рекомендуется использовать Security Servers для сканирования виртуальных машин или компьютеров с ограниченными ресурсами.

Чтобы назначить Security Server целевым конечным точкам, добавьте Security Servers, которые вы хотите использовать, в таблицу **Назначение Security Server**, выполнив следующие действия:

1. Нажмите на выпадающий список **Security Server** и выберите Security Server.
2. Если Security Server находится в DMZ или за сервером NAT, введите FQDN или IP-адрес сервера NAT в поле **Пользовательское имя сервера/ IP-адрес**.

Важно
Убедитесь, что переадресация портов правильно настроена на сервере NAT, чтобы трафик от конечных точек мог доходить до Security Server. Подробнее о портах см. Коммуникационные порты GravityZoneБаза знаний.

3. Нажмите кнопку ⊕ **Добавить** в столбце **Действия**.

   Security Server добавится в список.

4. Повторите предыдущие шаги, чтобы добавить другие Security Servers, если они доступны или необходимы.

Чтобы установить приоритет Security Servers:

1. Используйте стрелки вверх и вниз, доступные в столбце **Действия**, чтобы увеличить или уменьшить приоритет каждого Security Server.

   При назначении большего количества Security Servers, находящийся сверху будет иметь наибольший приоритет и будет выбран первым. Если этот Security Server недоступен или перегружен, выбирается следующий Security Server. Трафик сканирования перенаправляется на первый доступный и имеющий подходящую загрузку Security Server.

2. Выберите **Сначала подключиться к Security Server, установленному на том же физическом хосте, если он доступен, независимо от назначенного приоритета** для равномерного распределения конечных точек и оптимизации задержки. Если данный Security Server недоступен, то Security Server из списка будет выбран в порядке приоритета.

Важно
Этот параметр работает только с Security Server Multi-Platform и только если GravityZone интегрирована с виртуализированной средой.

Чтобы удалить Security Server из списка, нажмите соответствующую кнопку ⊗ **Удалить** в столбце **Действия**.

Настройки Security Server

При назначении политики для Security Servers вы можете настроить следующие параметры:

- **Ограничить количество одновременных проверок по требованию**.

Запуск нескольких задач сканирования по запросу на виртуальных машинах, использующих одно хранилище данных, может создать Сканирование вредоносных программ. Чтобы предотвратить это и разрешить одновременное выполнение только определенного количества задач сканирования:

1. Выберите параметр **Ограничить количество одновременных проверок по требованию**.
2. Выберите уровень разрешенных одновременных задач сканирования в выпадающем меню. Вы можете выбрать предопределенный уровень или ввести пользовательское значение.

   Формула для нахождения максимального количества задач сканирования для каждого предопределенного уровня:`N = a x MAX(b ; vCPUs - 1)`, где:

   – `N` = максимальное количество задач сканирования
   – `a` = коэффициент умножения, имеющий следующие значения: `1` - для Низкого; `2` - для Среднего; `4` - для Высокого
   – `MAX(b;vCPU-1)` = функция, которая возвращает максимальное количество слотов сканирования, доступных на Security Server.
   – `b` = количество слотов для сканирования по требованию, которое по умолчанию равно 4.
   – `vCPUs` = количество виртуальных процессоров, выделенныхSecurity Server

   Например:

   Для Security Server с 12 процессорами и Высоким уровнем одновременных сканирований, мы имеем:

   `N = 4 x MAX(4 ; 12-1) = 4 x 11 = 44` одновременных задач сканирования по запросу.

- **Включить правила привязки для Security Server Multi-Platform**

  Выберите поведение Security Server при переходе в режим обслуживания:

  – Если включено, Security Server остается привязанным к хосту и GravityZone отключает его. По окончанию обслуживания, GravityZone автоматически перезапускает Security Server.

Данное поведение установлено по умолчанию.

– Если отключено, Security Server переходит к другому хосту и продолжает работу. В данном случае, имя Security Server изменяется в Control Center для указания старого хоста. Измененное имя сохраняется до тех пор, пока Security Server не возвратится к первоначальному хосту.

  При достаточном количестве ресурсов, Security Server можете перейти на хост с другим установленным Security Server.

  Важно
  Эта опция не действует, если Security Server также используется HVI.

- **Использовать SSL**

  Активируйте эту функцию для шифрования подключения между целевыми конечными точками и указанными устройствами Security Server.

  По умолчанию, GravityZone использует самоподписанные сертификаты безопасности. Вы можете изменить их своими собственными сертификатами в **Настройка > Сертификаты** на странице Control Center. Для получения дополнительной информации см. главу «Настройка параметров Control Center» в Руководстве по установке.

- **Связь между Security Servers и GravityZone**

  Выберите один из доступных вариантов, чтобы задать параметры прокси-сервера для связи между выбранными машинами Security Server и GravityZone:

  – **Сохранить настройки установки**, чтобы использовать параметры прокси-сервера, определенные в установочном пакете.

  – **Использовать прокси, определенный в общем разделе**, чтобы использовать параметры прокси-сервера, определенные в текущей политике в разделе **Общее > Настройки**.

  – **Не использовать прокси-сервер**, когда целевые конечные точки не взаимодействуют с определенными компонентами Bitdefender через прокси-сервер.

7.2.4. Sandbox Analyzer

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов

Sandbox Analyzer обеспечивает мощный уровень защиты от расширенных угроз, выполняя автоматический всесторонний анализ подозрительных файлов, которые еще не подписаны механизмами защиты от вредоносных программ Bitdefender.

В этом разделе вы можете настроить следующее:

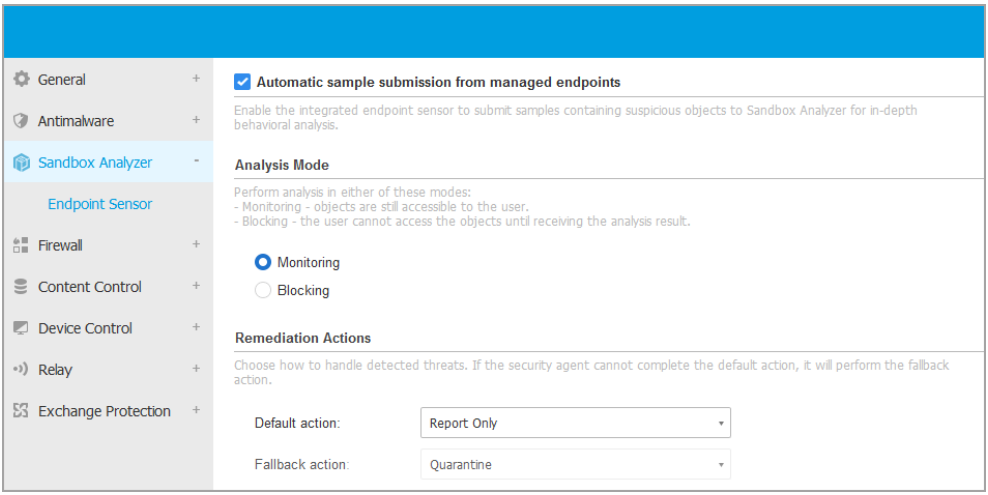
- Подача через датчик конечной точки
- Подача через датчик сети
- Подача через датчик ICAP
- Настройки Sandbox Manager

В настройках политики вы также можете настроить автоматическую отправку из централизованного карантина. Дополнительные сведения см. в разделе «Централизованный карантин» (p. 311).

Подробнее о ручной подаче см. «Manual Submission» (p. 563). Подробнее о передаче через API см. В главах **Sandbox** и **Sandbox Portal** в GravityZone API Guide (On-Premises) .

Датчик конечной точки

Bitdefender Endpoint Security Tools может выступать в качестве датчика подачи для Sandbox Analyzer с конечных точек Windows.



Политики > Sandbox Analyzer > Датчик конечной точки

Чтобы настроить автоматическую отправку через датчик конечной точки:

1. В разделе **Настройки подключения** выберите один из вариантов:
   - **Использовать облако Sandbox Analyzer** - датчик конечной точки отправит образцы в экземпляр Sandbox Analyzer, размещенный Bitdefender, в зависимости от вашего региона.
   - **Использовать локальный экземпляр Sandbox Analyzer**- датчик конечной точки отправит образцы в экземпляр Sandbox Analyzer On-Premises. Выберите предпочтительный экземпляр Sandbox Analyzer из выпадающего меню.

   Если у вас есть сеть за прокси-сервером или брандмауэром, вы можете настроить прокси для подключения к Sandbox Analyzer, установив флажок **Используйте настройки прокси**.

   Вы должны заполнить следующие поля:
   - **Сервер** - IP-адрес прокси-сервера.
   - **Порт** - порт, используемый для подключения к прокси-серверу.
   - **Имя польхователя** имя пользователя, опознаваемое прокси-сервером.
   - **Пароль** - корректный пароль указанного пользователя.

2. Выберите **Автоматическая отправка файлов с управляемых конечных точек**, чтобы включить автоматическую передачу подозрительных файлов в Sandbox Analyzer.

Важно

- Sandbox Analyzer требует сканирование при доступе. Убедитесь, что включен модуль **Антивирусная защита > Сканирование по доступу**.
- Sandbox Analyzer использует те же цели и исключения, которые определены в **Антивирусная защита > Сканирование при доступе**. При настройке Sandbox Analyzer внимательно просмотрите параметры сканирования при доступе.
- Чтобы предотвратить ложные срабатывания (неправильное обнаружение законных приложений), вы можете настроить исключения по имени файла, расширения, размеру файла и пути к файлу. Для получения дополнительной информации о сканировании по доступу см.«Защита от вредоносного ПО» (p. 280).
- Предел загрузки для любого файла или архива составляет 50 МБ.

3. Выберите **Режим анализа** . Доступны две опции:
   - **Мониторинг**. Пользователь может получить доступ к файлу во время анализа безопасной среды, но ему не рекомендуется выполнять его до получения результата анализа.
   - **Блокировка**. Пользователь не может выполнить файл, пока результат анализа не будет возвращен в конечную точку из кластера Sandbox Analyzer через портал Sandbox Analyzer.
4. Укажите **Действия по восстановлению** . Они берутся во внимание когда Sandbox Analyzer обнаруживает угрозу. Для каждого режима анализа вам предоставляется двойная настройка, состоящая из одного действия по умолчанию и одного резервного действия. Sandbox Analyzer сначала выполняет действие по умолчанию, а затем возвращается, если первое не может быть выполнено.

   При первом доступе к этому разделу доступны следующие настройки:

Примечание
Наилучшим решением будет предпринять действия по исправлению в этой конфигурации.

- В режиме **Мониторинг** действием по умолчанию является **Только отчет** , при этом аварийное действие отключено.
- В режиме **Блокировка** действием по умолчанию является **Карантин** , при этом аварийным действием является действие **Удалить**.

Sandbox Analyzer предоставляет вам следующие действия по исправлению:

- **Обезвредить**. Данное действие удаляет вредоносный код из зараженных файлов.
- **Удалить**. Данное действие полностью удаляет обнаруженный файл с диска.
- **Карантин**. Данное действие перемещает зараженные файлы из исходного расположения в папку карантина. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице **Карантин** на Control Center.
- **только отчет**. Sandbox Analyzer анализирует только обнаруженные угрозы без каких-либо других действий.

Примечание
В зависимости от действия по умолчанию резервное действие может быть недоступно.

5. Как стандартные, так и резервные действия по исправлению устанавливаются в режим **Только отчет**.
6. В разделе **Предварительная фильтрация контента** настройте уровень защиты от потенциальных угроз. Датчик конечной точки имеет встроенный механизм фильтрации содержимого, который определяет необходимость проверки подозрительного файла в Sandbox Analyzer.

   Поддерживаемые типы объектов: приложения, документы, сценарии, архивы, электронные письма. Для получения дополнительной информации о поддерживаемых типах объектов см. «Типы Файлов Поддерживаемые Предварительной Фильтрацией Контента при Автоматической Отправке» (p. 615).

   Используйте главный переключатель в верхней части списка угроз, чтобы выбрать уникальный уровень защиты для всех типов объектов, или выберите индивидуальные уровни для точной настройки защиты.

Установка модуля на определенном уровне приведет к определенному количеству отправленных образцов:

- **Разрешимый**. Датчик конечной точки автоматически отправляет Sandbox Analyzer только объекты с наибольшей вероятностью вредоносности и игнорирует остальные объекты.
- **Обычный**. Датчик конечной точки находит баланс между отправленными и игнорируемыми объектами и отправляет в Sandbox Analyzer оба объекта с большей и с меньшей вероятностью быть вредоносными.
- **Агрессивный**. Датчик конечной точки передает Sandbox Analyzer практически все объекты, независимо от их потенциального риска.

В отдельном поле вы можете определить исключения для типов объектов, которые вы не хотите отправлять в Sandbox Analyzer.

Вы также можете определить ограничения по размеру отправленных объектов, установив соответствующий флажок и введя требуемые значения от 1 КБ до 50 МБ.

7. В разделе **Профиль детонации** настройте уровень сложности поведенческого анализа, влияя на пропускную способность Sandbox Analyzer. Например, если установлено значение **Высокое**, Sandbox Analyzer будет выполнять более точный анализ на меньшем количестве образцов за тот же интервал, чем на **Среднее** или **Низкое**.

Sandbox Analyzer поддерживает локальную отправку файлов через конечные точки с ролью ретрансляции, которые могут подключаться к различным адресам портала Sandbox Analyzer в зависимости от вашего региона. Подробнее о настройках конфигурации ретранслятора см. «Ретранслятор» (p. 379).

Примечание
Прокси-сервер, настроенный в настройках соединения Sandbox Analyzer, переопределит любые конечные точки с ролью ретрансляции.

Сетевой датчик

В этом разделе вы можете настроить автоматическую отправку образцов сетевого трафика в Sandbox Analyzer через датчик сети. Этот модуль требует развертывания и настройки виртуального устройства сетевой безопасности с помощью Sandbox Analyzer On-Premises

Для настройки автоматической отправки через датчик сети:

1. Установите флажок **Automatic samples submission from network sensor** , чтобы включить автоматическую отправку подозрительных файлов в Sandbox Analyzer.

2. В разделе **Предварительная фильтрация контента** настройте уровень защиты от потенциальных угроз. В датчик сети встроен механизм фильтрации содержимого, который определяет необходимость детонирования подозрительного файла в Sandbox Analyzer.

   Поддерживаемые типы объектов: приложения, документы, сценарии, архивы, электронные письма. Для получения дополнительной информации о поддерживаемых типах объектов см. «Типы Файлов Поддерживаемые Предварительной Фильтрацией Контента при Автоматической Отправке» (p. 615).

   Используйте главный переключатель в верхней части списка угроз, чтобы выбрать уникальный уровень защиты для всех типов объектов, или выберите индивидуальные уровни для точной настройки защиты.

   Установка модуля на определенном уровне приведет к определенному количеству отправленных образцов:

   - **Разрешимый**. Датчик сети автоматически отправляет Sandbox Analyzer только объекты, которые с наибольшей вероятностью могут быть вредоносными и игнорирует остальные объекты.
   - **Обычный**. Датчик сети находит баланс между отправленными и проигнорированными объектами и отправляет в Sandbox Analyzer те, которые могу быть вредоносными в большей или в меньшей степени.
   - **Агрессивный**. Датчик сети передает Sandbox Analyzer практически все объекты, независимо от их потенциального риска.

   В отдельном поле вы можете определить исключения для типов объектов, которые вы не хотите отправлять в Sandbox Analyzer.

   Вы также можете определить ограничения по размеру отправленных объектов, установив соответствующий флажок и введя требуемые значения от 1 КБ до 50 МБ.

3. В разделе **Настройки подключения** выберите предпочтительный экземпляр Sandbox Analyzer для отправки сетевого содержимого.

Если у вас есть сеть за прокси-сервером или брандмауэром, вы можете настроить прокси для подключения к Sandbox Analyzer, установив флажок **Используйте настройки прокси**.

Вы должны заполнить следующие поля:

- **Сервер** - IP-адрес прокси-сервера.
- **Порт** - порт, используемый для подключения к прокси-серверу.
- **Имя польховательля** имя пользователя, опознаваемое прокси-сервером.
- **Пароль** - корректный пароль указанного пользователя.

4. В разделе **Профиль детонации** настройте уровень сложности поведенческого анализа, влияя на пропускную способность Sandbox Analyzer. Например, если установлено значение **Высокое**, Sandbox Analyzer будет выполнять более точный анализ на меньшем количестве образцов за тот же интервал, чем на **Среднее** или **Низкое**.

Датчик ICAP

В этом разделе вы можете настроить автоматическую отправку в Sandbox Analyzer через датчик ICAP.

Примечание
Для Sandbox Analyzer требуется Security Server, настроенный для сканирования устройств сетевого хранилища (NAS), использующих протокол ICAP. Подробности см. в«Защита хранилища» (p. 420)

1. Установите флажок **Automatic samples submissions from ICAP sensor**, чтобы включить автоматическую отправку подозрительных файлов в Sandbox Analyzer.
2. В разделе **Предварительная фильтрация контента** настройте уровень защиты от потенциальных угроз. В датчик сети встроен механизм фильтрации содержимого, который определяет необходимость детонирования подозрительного файла в Sandbox Analyzer.

   Поддерживаемые типы объектов: приложения, документы, сценарии, архивы, электронные письма. Для получения дополнительной информации о поддерживаемых типах объектов см. «Типы Файлов Поддерживаемые Предварительной Фильтрацией Контента при Автоматической Отправке» (p. 615).

Используйте главный переключатель в верхней части списка угроз, чтобы выбрать уникальный уровень защиты для всех типов объектов, или выберите индивидуальные уровни для точной настройки защиты.

Установка модуля на определенном уровне приведет к определенному количеству отправленных образцов:

- **Разрешимый**. Датчик ICAP автоматически отправляет Sandbox Analyzer только объекты, которые с наибольшей вероятностью могут быть злонамеренными и игнорирует остальные объекты.
- **Обычный**. Датчик ICAP находит баланс между отправленными и проигнорированными объектами и отправляет в Sandbox Analyzer оба объекта, которые с большей и с меньшей вероятностью могут быть вредоносным.
- **Агрессивный**. Датчик ICAP передает Sandbox Analyzer практически все объекты, независимо от их потенциального риска.

В отдельном поле вы можете определить исключения для типов объектов, которые вы не хотите отправлять в Sandbox Analyzer.

Вы также можете определить ограничения по размеру отправленных объектов, установив соответствующий флажок и введя требуемые значения от 1 КБ до 50 МБ.

3. В разделе **Настройки подключения** выберите предпочтительный экземпляр Sandbox Analyzer для отправки сетевого содержимого.

   Если у вас есть сеть за прокси-сервером или брандмауэром, вы можете настроить прокси для подключения к Sandbox Analyzer, установив флажок **Используйте настройки прокси**.

   Вы должны заполнить следующие поля:

   - **Сервер** - IP-адрес прокси-сервера.
   - **Порт** - порт, используемый для подключения к прокси-серверу.
   - **Имя польхователя** имя пользователя, опознаваемое прокси-сервером.
   - **Пароль** - корректный пароль указанного пользователя.

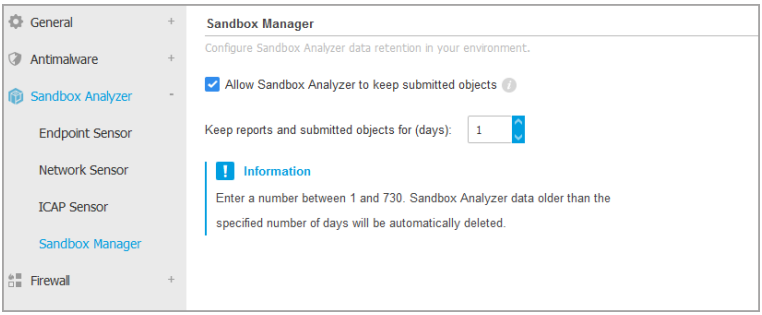
4. В разделе **Профиль детонации** настройте уровень сложности поведенческого анализа, влияя на пропускную способность Sandbox Analyzer. Например, если установлено значение **Высокое**, Sandbox Analyzer

будет выполнять более точный анализ на меньшем количестве образцов за тот же интервал, чем на **Среднее** или **Низкое**.

Sandbox Manager

В этом разделе вы настраиваете хранение данных для ваших экземпляров Sandbox Analyzer:

- Установите флажок **Разрешить Sandbox Analyzer, чтобы сохранить отправленные объекты** . Этот параметр позволяет использовать параметр **Повторно отправить на анализ** в области карточек отправки интерфейса отчетности Sandbox Analyzer.
- Укажите, какое количество дней вы хотите, чтобы Sandbox Analyzer сохранял отчеты и отправленные объекты в хранилище данных. Максимальное количество данных, которое вы можете ввести, составляет 730. По истечении заданного периода все данные будут удалены.



Политики > Sandbox Analyzer > Sandbox Manager

7.2.5. Брандмауэр

Примечание
Этот модуль доступен для Windows для рабочих станций.

Брандмауэр служит для защиты конечных точек от попыток установления несанкционированных входящих и исходящих соединений.

Функциональность брандмауэра основана на сетевых профилях. Профили основаны на уровнях доверия, которые должны быть определены для каждой сети.

Брандмауэр обнаруживает каждое новое подключение, сравнивает информацию адаптера с информацией существующих профилей и применяет подходящий профиль. Для получения более подробной информации о применении профилей, обратитесь к «Настройки сети» (p. 335).

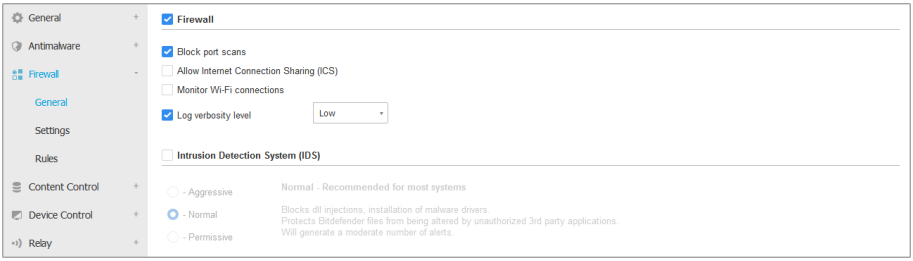
Важно
Модуль файрвола доступен только для поддерживаемых рабочих станций Windows.

Настройки объединены в следующие разделы:

- Основные
- Настройки
- Правила

Основные

В этом разделе можно включить или отключить файрвол Bitdefender и настроить общие параметры.



Политики компьютеров и виртуальных машин - Основные настройки файрвола

- **Брандмауэр.** Используйте флажок, чтобы включить или выключить брандмауэр.

  Предупреждение
  Если вы отключите брандмауэр, компьютеры будут уязвимы к сетевым и Интернет-атакам.

- **Блокировать сканирование портов.** Сканирование портов часто используется хакерами для обнаружения открытых портов на вашем

компьютере. Они могут проникнуть в ваш компьютер, если найдут уязвимый или менее защищенный порт.

- **Разрешить использование общего доступа к Интернет (ICS).** Выберите эту опцию, чтобы разрешить файрволу пропускать трафик общего доступа к сети интернета.

  Примечание
  Эта опция автоматически не разрешает совместный доступ к Интернет на системах пользователей.

- **Отслеживать Wi-Fi подключения.** Агент безопасности Bitdefender может сообщать пользователям, подключенным к сети Wi-Fi, о подключении к сети нового компьютера. Для отображения таких уведомлений на экране пользователя, выберите эту опцию.
- **Уровень детализации сообщений.** Агент безопасности Bitdefender ведет журнал событий, касающихся использования модуля файрвола (включение/выключение, блокировка трафика, изменение параметров) или генерируется обнаруженными данным модулем действиями (сканирование портов, блокировка попыток соединения или трафика согласно правилам). Выберите опцию из **Уровень детализации журнала**, чтобы указать, какую информацию должен накапливать журнал.
- **Система обнаружения вторжений.** Система обнаружения вторжений проверяет вашу систему на подозрительные действия (к примеру, неавторизированная попытка изменить файлы Bitdefender, DLL-инъекции, попытки кейлоггера и др.)

  Примечание
  Параметры политики системы обнаружения вторжений (IDS) применяются только к Endpoint Security (устаревшему агенту безопасности). Агент Bitdefender Endpoint Security Tools интегрирует возможности системы обнаружения вторжений на основе хоста в свой модуль Advanced Threat Control (ATC).

  Настройка системы обнаружения вторжений:

  1. Используйте кнопку-флажок, чтобы включить или выключить систему обнаружения вторжений.

2. Выберите уровень безопасности, который лучше всего соответствует вашим потребностям (Интенсивный, Нормальный или Рекомендуемый). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

Чтобы предотвратить срабатывание системы обнаружения вторжений на действия доверенных приложений, добавьте **ATC/IDS правило исключения процесса** для этого приложения в разделе **Защита от вредоносных программ > Настройки > Пользовательские исключения** .

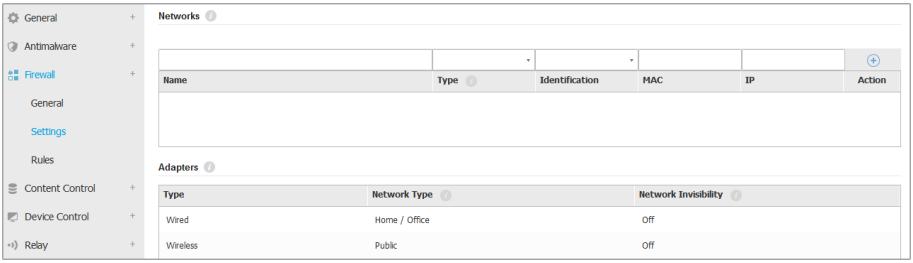
Важно
Система обнаружения вторжений доступна только для клиентов Endpoint Security.

Настройки

Файрвол автоматически применит подходящий профиль, основанный на уровне доверия. Вы можете установить различные уровни доверия для сетевых соединений в зависимости от архитектуры сети или типа адаптера, использующегося для установления сетевого соединения. Например, если внутри сети вашей компании существуют подсети, вы можете установить уровень доверия к каждой подсети.

Настройки расположены в следующих разделах:

- Сети
- Адаптеры



Политики - Настройки файрвола

Настройки сети

Если вы хотите, чтобы файрвол применял различные профили для разных сегментов сети вашей компании, вы должны указать управляемые сети в разделе **Networks**. Заполните поля в таблице **Сети**, как описано ниже:

- **Имя.** Введите имя, по которому вы сможете распознавать сеть в списке.
- **Тип.** Выберите из меню тип профиля, назначаемый сети.

  Агент безопасности Bitdefender автоматически применяет один из четырех сетевых профилей для каждого обнаруженного сетевого соединения на конечной точке, чтобы установить основные параметры фильтрации трафика. Типы профилей:

  – **Безопасная**. сеть Надежная сеть, в которой файрвол отключается на определенных адаптерах.

  – **Домашяя/Офисная** сеть Домашняя или офисная сеть, в которой разрешается весь трафик "в" и "из" компьютеров в локальной сети, а остальной трафик фильтруется.

  – **Общественная** Сеть Весь трафик фильтруется.

  – **Небезопасная**. Ненадежная сеть, в которой блокируется весь сетевой трафик и доступ в Интернет через соответствующий адаптер.
- **Идентификация.** Выберите из меню способ, через который сеть будет идентифицирована агентом безопасности Bitdefender. Сети могут быть определены тремя способами: **DNS**, **Шлюх** и **Сеть**.

  – **DNS**: идентифицирует все конечные точки, используя указанный DNS.

  – **Gateway**: идентифицирует все конечные точки связанные через указанный шлюз.

  – **Network**: идентифицирует все конечные точки из указанного сегмента сети, определенных по их сетевому адресу.
- **MAC**. Используйте это поле, чтобы указать MAC-адрес DNS-сервера или шлюза, разделяющего сети, в зависимости от выбранного метода идентификации.

  Вы должны ввести MAC-адрес в шестнадцатеричном формате, разделенный дефисом (-) или двоеточием (:). Например, оба данных адреса будут действительны `00-50-56-84-32-2b` и `00:50:56:84:32:2b`.

- **IP.** Используйте это поле, чтобы указать конкретные IP-адреса в сети. Формат IP-адреса зависит от способа идентификации:
  - **Сеть.** Введите номер сети в формате CIDR. Например, `192.168.1.0/24`, где `192.168.1.0` это адрес сети и `/24` это маска сети.
  - **Шлюз.** Введите IP-адрес шлюза.
  - **DNS.** Введите IP-адрес DNS-сервера.

После того как вы задали характеристики сети, нажмите кнопку **Добавить** в правой части таблицы, чтобы добавить ее в список.

Настройки адаптеров

Если будет обнаружена сеть, которая отсутствует в списке **Сети**, агент безопасности Bitdefender определит тип сетевого адаптера и применит к нему соответствующий профиль подключения.

Поля в таблице **Адаптеры** обозначают следующее:

- **Тип.** Отображает тип сетевых адаптеров. Агент безопасности Bitdefender может обнаруживать три предопределенных типа адаптеров: проводной (**Wired**), беспроводной (**Wireless**) и виртуальный (**Virtual** - виртуальная частная сеть).
- **Тип сети.** Описывает профиль сети, назначенный определенному типу адаптера. Сетевые профили описаны в разделе настроек сети. Нажав на тип сети, вы сможете изменить настройки.

  Если вы выберите **Let Windows decide**, то для любого нового подключения к сети, обнаруженного после применения политики, агент безопасности Bitdefender применит профиль файрвола, основанный на сетевой классификации Windows, не обращая внимания на настройки из раздела **Адаптеры**.

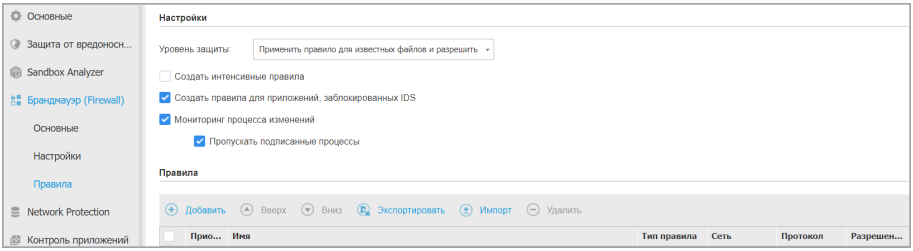
  Если обнаружение, основанное на управлении сетями Windows, даст сбой, будет применена попытка основного обнаружения. Общий профиль используется, когда назначен сетевой профиль **Общественный** и настройки видимости установлены в состояние **Включен**.

  Когда конечная точка, подключенная в Active Directory, подключается к домену, для профиля брандмауэра автоматически устанавливается значение **Дом/офис**, а для параметров скрытности - **Удаленный**. Если компьютер не в домене, то это условие не применимо.

- **Сетевое Обнаружение.** Скрывает компьютер от вредоносного программного обеспечения и хакеров в сети или в Интернете. При необходимости настройте видимость компьютера в сети для каждого типа адаптера, выбрав один из следующих параметров:
  - **Да.** любой человек из локальной сети или Интернета может проверять и обнаруживать компьютер.
  - **Нет.** компьютер невидим как из локальной сети, так и из Интернета.
  - **Удаленный.** Компьютер не может быть обнаружен из сети Интернет. Любой желающий в локальной сети сможет пропинговать и обнаружить компьютер.

Правила

В этом разделе вы можете настроить правила доступа приложений к сети и для трафика данных, назначаемых файрволом. Обратите внимание, что имеющиеся параметры применяются только к **Домашний/Офисный** и **Общественный** профилям.



Политики компьютеров и виртуальных машин - Настройка правил файрвола

Настройки

Вы можете настроить следующие параметры:

- **Уровень защиты.** Выбранный уровень защиты определяет логику принятия решений файрволом, используемую, когда приложения выдают запросы на доступ к сети и Интернет-услугам. Доступны следующие опции:

Применить правило и разрешить

Применяет существующие правила файрвола и автоматически разрешает все другие попытки соединений. Для каждой новой попытки соединения создается правило и добавляется к набору.

Применить правило и спросить

Применяет существующие правила файрвола и запрашивает у пользователя действия для всех других попыток подключения. Предупреждающее окно с подробной информацией о неизвестной попытке подключения будет отображено на экране пользователя. Для каждой новой попытки соединения создается правило и добавляется к набору.

Применить правило и запретить

Применяет существующие правила файрвола и автоматически запрещает все другие попытки соединения. Для каждой новой попытки соединения создается правило и добавляется к набору.

Применить правило для известных файлов и разрешить

Применяет существующие правила файрвола, автоматически разрешает попытки подключения, сделанные известными приложениями, и автоматически разрешает все другие неизвестные попытки подключений. Для каждой новой попытки соединения создается правило и добавляется к набору.

Применить правило для известных файлов и спросить

Применяет существующие правила файрвола, автоматически разрешает попытки подключения, сделанные известными приложениями, и запрашивает у пользователя действия для всех других неизвестных попыток подключения. Предупреждающее окно с подробной информацией о неизвестной попытке подключения будет отображено на экране пользователя. Для каждой новой попытки соединения создается правило и добавляется к набору.

Применить правило для известных файлов и запретить

Применяет существующие правила файрвола, автоматически разрешает попытки подключения, сделанные известными приложениями, и автоматически запрещает все другие неизвестные попытки подключения. Для каждой новой попытки соединения создается правило и добавляется к набору.

Примечание
Известные файлы представляют собой большую базу безопасных, надежных приложений, которая составляется и постоянно поддерживается Bitdefender.

- **Создать интенсивные правила.** При выборе данного параметра файрвол создаст правила для каждого процесса, который открывает приложения, запрашивающие доступ к сети или в Интернет.
- **Создать правила для приложений, заблокированных IDS.** При выборе данной опции файрвол автоматически создает правило **Отказать** каждый раз, когда система обнаружения вторжений блокирует приложение.
- **Мониторинг процесса изменений.** Выберите эту опцию если хотите проверять каждое изменившееся приложение, которое пытается подключиться к Интернет, дополнительным правилом, контролирующим его доступ в Интернет. Если приложение было изменено, новое правило будет создано в соответствии с существующим уровнем защиты.

Примечание
Как правило, изменения в приложения вносятся посредством обновлений. Однако существует риск того, что приложения могут быть изменены вредоносными программами с целью заражения локального компьютера и остальных компьютеров в сети.

Приложения с цифровой подписью считаются надежными и имеют более высокую степень безопасности. Вы можете выбрать **Игнорировать подписанные процессы**, автоматически позволяя измененным подписанным приложениям подключения к сети Интернет.

Правила

В таблице правил перечислены существующие правила файрвола, содержащие важную информацию о каждом из них:

- Имя правила или приложения, к которому оно относится.
- Протокол, к которому применяется правило.
- Действие правила (разрешить или запретить пакеты).
- Действия, которые вы можете выполнять над правилом.
- Приоритет правил.

Примечание

Существуют правила файрвола однозначно назначаемые политикой. Дополнительные правила могут быть сконфигурированы для компьютеров в результате применения параметров файрвола.

Существует ряд правил файрвола по умолчанию, позволяющий достаточно просто разрешить или запретить популярные типы трафика. Выберите нужную опцию из меню **Разрешение**.

Входящие ICMP/ICMPv6
Разрешите или запретите сообщения ICMP/ICMPv6. Сообщения ICMP часто используются хакерами для проведения атак на компьютерные сети. По умолчанию этот тип трафика разрешен.

Входящие подключения к удаленному рабочему столу
Разрешите или запретите другим компьютерам подключения к удаленному рабочему столу. По умолчанию этот тип трафика разрешен.

Отправка сообщений электронной почты
Разрешите или запретите отправку электронных сообщений по SMTP. По умолчанию этот тип трафика разрешен.

Веб-просмотр HTTP
Разрешите или запретите веб-просмотр по протоколу HTTP. По умолчанию этот тип трафика разрешен.

Сетевая печать
Разрешите или запретите доступ к принтерам в другой локальной сети. По умолчанию этот тип трафика запрещен.

Трафик проводника Windows по протоколу HTTP/FTP
Разрешите или запретите трафик HTTP и FTP из Windows Explorer. По умолчанию этот тип трафика запрещен.

Кроме правил по умолчанию, вы можете создать дополнительные правила файрвола для других приложений, установленных на конечных точках. Эти настройки предназначены для администраторов с хорошим уровнем знания сетей.

Чтобы создать и настроить новое правило, нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Обратитесь к этой теме для получения дополнительной информации.

Чтобы удалить правило из списка, выберите его и нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Примечание
Вы не можете удалить или изменить правила файрвола по умолчанию.

Настройка пользовательских правил

Вы можете настроить два типа правил файрвола:

- **Правила, основанные на приложениях.** Такие правила применяются к конкретному программному обеспечению, найденному на клиентских компьютерах.
- **Правила, основанные на подключениях.** Такие правила распространяются на любые приложения или службы, которые используют сетевые подключения.

Чтобы создать и настроить новое правило, нажмите кнопку ⊕ **Добавить** в верхней части таблицы и выберите нужный тип правила из меню. Чтобы отредактировать существующее правило, щелкните на имя правила.

Доступна настройка следующих параметров:

- **Имя правила.** Введите имя, под которым правило будет отображаться в таблице правил (например, имя приложения, к которому применяется данное правило).
- **Путь приложения** (только для правил, основанных на приложениях). Вы должны указать путь к исполняемому файлу приложения на требуемых компьютерах.
  - Выберите из меню предопределенное месторасположение и завершите путь по мере необходимости. Например, приложение установлено в папке `Программные файлы`, выберите `%ProgramFiles%` и завершите путь, добавив обратную косую черту (\) и имя папки приложения.
  - Введите полный путь в поле редактирования. Желательно использовать системные переменные (в соответствующих случаях), чтобы быть уверенным, что путь действителен для всех нужных компьютеров.
- **Командная строка** (только для правил, основанных на приложениях). Если вы хотите, чтобы правило применялось только когда указанное приложение запущено определенной командой в интерфейсе командной

строки Windows, введите соответствующую команду в поле ввода. В противном случае оставьте это поле пустым.

- **Приложение MD5** (только для правил, основанных на приложениях). Если вы хотите, чтобы правило проверяло целостность данных файлов приложений, основанную на их MD5 хэш-коде, введите его в поле редактирования. В противном случае оставьте это поле пустым.
- **Локальный адрес.** Укажите локальный IP-адрес и порт, к которому будет применяться правило. Если у вас несколько сетевых адаптеров, вы можете снять флажок **Любой** и ввести определенный IP-адрес. Аналогично для фильтрации соединений по конкретному порту или диапазону портов, снимите флажок **Любой** и введите нужные порт или диапазон портов в соответствующем поле.
- **Удаленный адрес.** Укажите удаленный IP-адрес и порт, к которому будет применяться правило. Чтобы отфильтровать трафик к и от конкретного компьютера, снимите флажок **Любой** и введите его IP-адрес.
- **Применить это правило только для непосредственно подключенных компьютеров.** Вы можете фильтровать доступ на основе MAC-адресов.
- **Протокол.** Выберите IP-протокол, к которому будет применяться правило.
  - Если вы хотите, чтобы правило применялось ко всем протоколам, выберите **Любой**.
  - Если вы хотите применить правило к TCP, выберите **TCP**.
  - Если вы хотите применить правило к UDP, выберите **UDP**.
  - Если вы хотите, чтобы правило применялось к определенному протоколу, выберите этот протокол из меню **Другое**.

  Примечание

  Диапазоны IP-адресов выделяются Администрацией адресного пространства Интернет (IANA). Полный список выделенных IP-адресов можно найти на странице http://www.iana.org/assignments/protocol-numbers.

- **Направление.** Выберите направление трафика, к которому будет применяться правило.

Направление	Описание
Исх.	Правило будет применяться только к исходящему трафику.
Входящий	Правило применяется только ко входящему трафику.
Оба	Правило будет применяется и к входящему, и к исходящему трафику.

- **Версия IP.** Выберите версию IP (напр., IPv4, IPv6 или any), к которой будет применяться правило.
- **Сеть.** Выберите тип сети, для которого будет назначено правило.
- **Разрешение.** Выберите одно из доступных разрешений:

Разрешение	Описание
Разрешить	Указанному приложению будет разрешен доступ в сеть/Интернет при определенных обстоятельствах.
Запретить	Указанному приложению будет запрещен доступ в сеть/Интернет при определенных обстоятельствах.

Нажмите **Сохранить**, чтобы добавить правило.

Для правил, которые вы создали, используйте стрелки в правой части таблицы, чтобы установить каждому приоритет. Правило с более высоким приоритетом будет находиться в списке выше.

Правила импорта и экспорта

Вы можете экспортировать и импортировать правила брандмауэра, чтобы использовать их в других политиках или компаниях. Чтобы экспортировать правила:

1. Нажмите **Экспорт** в верхней части таблицы правил.
2. Сохраните файл CSV на вашем компьютере. В зависимости от настроек вашего браузера, файл может автоматически загрузится или вам будет предложено сохранить его в определенное место.

Важно

- Каждая строка в CSV-файле соответствует одному правилу и имеет несколько полей.
- Место правил брандмауэра в файле CSV определяет их приоритет. Вы можете изменить приоритет правила, перемещая всю строку.

Для набора правил по умолчанию вы можете изменить только следующие элементы:

- **Приоритет**. Установите приоритет правила в любом желаемом порядке, перемещая строку CSV.
- **Разрешение**. Измените поле `set.Permission`, используя доступные разрешения:
  - 1 для **Разрешить**
  - 2 за **Запретить**

Любые другие корректировки игнорируются при импорте.

Для пользовательских правил брандмауэра все значения полей настраиваются следующим образом:

Поле	Имя и значение
`ruleType`	**Тип правила**: 1 для **Правила приложений** 2 для **Правила подключений**
`тип`	Значение для этого поля не является обязательным.
`details.name`	**Имя правила**
`details.applictionPath`	**Путь приложения** (только для правил, основанных на приложениях)
`details.commandLine`	**Командная строка** (только для правил, основанных на приложениях)

Поле	Имя и значение
`details.applicationMd5`	**Приложение MD5** (только для правил, основанных на приложениях)
`settings.protocol`	**Протокол** 1 для **Любого** 2 для **TCP** 3 для **UDP** 4 для **Другого**
`settings.customProtocol`	Требуется только в том случае, если для **Протокола** установлено значение **Другой**. Для конкретных значений, рассмотрите эту страницу. Значения 0, 4, 6, 41, 61, 63, 68, 99, 114, 124, 34–37, 141–143 не поддерживаются.
`settings.direction`	**Направление**: 1 для **Оба** 2 для **Входящие** 3 для **Исходящие**
`settings.ipVersion`	**IP-версия**: 1 для **Любого** 2 для **IPv4** 3 для **IPv6**
`settings.localAddress.any`	**Локальный адрес** установлен на **Любой**. 1 для Правильного 0 или пустой для Неправильного

Поле	Имя и значение
`settings.localAddress.ipMask`	**Локальный адрес** установлен на **IP или IP/Mask**
`settings.remoteAddress.portRange`	**Удаленный адрес** имеет значение **Порт или диапазон портов**
`settings.directlyConnected.enable`	**Применять правило только к компьютерам с прямым подключением**. 1 для включен 0 для пуст или отключен
`settings.directlyConnected.remoteMac`	**Применять правило только к компьютерам с прямым подключением** с фильтром **MAC-адрес**.
`permission.home`	**Сеть**, к которой применяется правило: **Дом/Офис**: 1 для Правильного 0 для пустой или неправильной
`permission.public`	**Сеть**, к которой применяется правило, является **Общедоступной**: 1 для Правильного 0 для пустой или неправильной
`permission.setPermission`	Доступные разрешения: 1 для **Разрешить** 2 за **Запретить**

Чтобы импортировать правила:

1. Нажмите **Импорт** в верхней части таблицы правил.

2. В новом окне нажмите **Добавить** и выберите файл CSV.
3. Нажмите **Сохранить**. Таблица заполняется корректными правилами.

7.2.6. Защита сети

Используйте раздел «Защита сети», чтобы настроить параметры фильтрации содержимого, защиты данных для действий пользователей, включая просмотр веб-страниц, почтовых и программных приложений, а также обнаружение методов сетевых атак, которые пытаются получить доступ к определенным конечным точкам. Вы можете ограничить или разрешить веб-доступ и использование приложений, настроить параметры сканирования трафика, антифишинг и правила защиты данных.

Пожалуйста, обратите внимание, что настроенные параметры управления контентом будут применяться ко всем пользователям, которые вошли на рабочие станции.

Настройки объединены в следующие разделы:

- Основные
- Контроль контента
- Веб-защита
- сетевые атаки

Примечание

- Модуль Контент Контроля доступен для:
  - Windows для рабочих станций
  - ОС MAK
- Модуль Network Attack Defense доступен для:
  - Windows для рабочих станций

Важно

Для macOS Content Control использует расширение ядра. Установка расширения ядра требует вашего подтверждения на macOS High Sierra (10.13.x). Система уведомляет пользователя о том, что расширение системы от Bitdefender было заблокировано. Пользователь может разрешить это в настройках **Безопасность и конфиденциальность** . Пока пользователь не утвердит расширение системы Bitdefender, этот модуль не будет работать, а пользовательский интерфейс Endpoint Security for Mac покажет критическую проблему, запрашивающую утверждение.

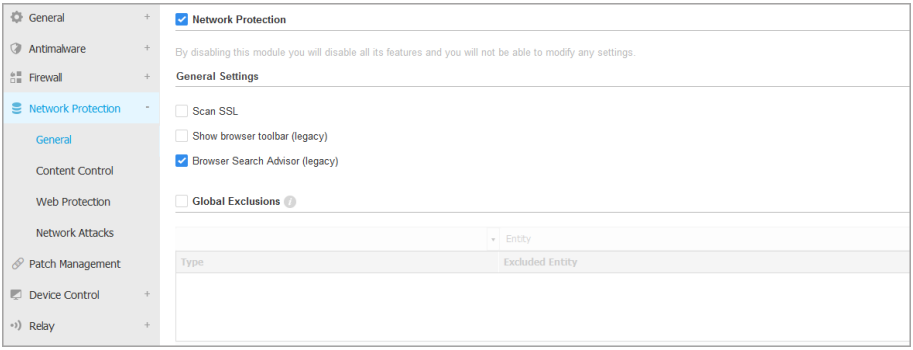
Чтобы исключить вмешательство пользователя, вы можете предварительно утвердить расширение ядра Bitdefender, занеся его в белый список с помощью инструмента управления мобильными устройствами. Подробнее о расширениях ядра Bitdefender см. эту статью базы знаний .

Основные

На этой странице вы можете настроить такие параметры, как включение или отключение функций и настроить исключения.

Настройки объединены в следующие разделы:

- Общие настройки
- Глобальные исключения



Политики компьютеров и виртуальных машин - Защита сети - Общее

Общие настройки

- **Сканировать SSL**. Выберите эту опцию, если вы хотите, чтобы веб-трафик SSL (Secure Sockets Layer) проверялся защитными модулями агента безопасности Bitdefender.
- **Показать панель инструментов браузера (старая версия)**. Панель Bitdefender информирует пользователей о рейтинге безопасности веб-страниц, которые они просмотрают. Панель инструментов Bitdefender отличается от стандартной панели инструментов браузера. В браузере появляется только небольшой значок в верхней части каждой веб-страницы. Нажатие на значок открывает панель инструментов.

В зависимости от того, как Bitdefender классифицирует веб-страницу, одна из следующих оценок отображается в левой части панели:

– Сообщение "This page is not safe"(страница небезопасна) появляется на красном фоне.
– Сообщение "Caution is advised" (требуется осторжность) появляется на оранжевом фоне.
– Сообщение "This page is safe" (страница безопасна) появляется на зеленом фоне.

Примечание

– Эта опция недоступна для macOS.
– Эта опция удалена из Windows, начиная с новых установок Bitdefender Endpoint Security Tools версии 6. 6. 5. 82.

- **Поисковой советник браузера (устаревший).** Поисковой Советник оценивает результаты поисковых систем Google, Bing и Yahoo!, а также ссылки из Facebook и Twitter, поместив значок перед каждым результатом. Используемые значки и их значение:

  Эту веб-страницу посещать не следует.
  Данная веб-страница может содержать опасную информацию. Соблюдайте осторожность, если вы решите ее посетить.
  Эта страница безопасна для посещения.

Примечание

– Эта опция недоступна для macOS.
– Эта опция удалена из Windows, начиная с новых установок Bitdefender Endpoint Security Tools версии 6. 6. 5. 82.

Глобальные исключения

Вы можете пропустить определенный трафик при проверке на наличие вредоносных программ, пока включены параметры **Защита сети**.

Примечание

Эти исключения применяются к **Сканированию трафика** и **Антифишингу** в разделе **Веб-защита**, и **Network Attack Defense** в разделе **Сетевые атаки**.

Исключения **Защиты данных** настраиваются отдельно, в разделе **Контроль контента**.

Чтобы определить исключение:

1. Выберите тип исключения из меню.
2. В зависимости от типа исключения, задайте содержимое трафика, которое будет исключено из сканирования, следующим образом:
   - **IP/mask**. Введите IP-адрес или IP-маску, для которой вы не хотите сканировать входящий и исходящий трафик, включая методы сетевой атаки.
   - **URL**. Исключает из сканирования указанные веб-адреса. Обратите внимание, что исключения на основе URL применяются по-разному для соединений HTTP и HTTPS, как описано ниже.

     Вы можете определить исключение на основе URL следующим образом:

     – Введите определенный URL, такой как `www.example.com/example.html`
       - В случае с HTTP-соединениями, только конкретный URL будет исключен из процесса сканирования.
       - Для HTTPS-соединений, добавление конкретного URL исключит целый домен и любые его субдомены. Следовательно, в этом случае вы можете указать домен, который следует исключить из сканирования.

     – Используйте подстановочные знаки для определения шаблонов веб-адресов (только для HTTP-соединений).

     Важно
     Исключения с подстановочными знаками не работают для соединений HTTPS.

     Можно использовать следующие подстановочные символы:
       - Звездочка (*) заменяет ноль или более символов.
       - Знак вопроса (?) заменяет ровно один символ. Вы можете использовать несколько вопросительных знаков, чтобы задать любую возможную комбинацию из определенного количества

символов. Например, ??? заменит любую комбинацию ровно из трех символов.

В следующей таблице вы можете найти несколько примеров синтаксиса для указания веб-адресов (URLs).

Синтаксис	Применимость исключений
www.example*	Любой URL начинающийся с www.example вне зависимости от доменного расширения. Исключение не будет применяться к поддоменам указанного веб-сайта, например, subdomain.example.com.
*example.com	Любой URL заканчивающийся на example.com, включая их субдомены.
example.com	Любой URL, который содержит указанную строку.
*.com	Любой веб-сайт, имеющий доменное расширение .com, включая их субдомены. Используйте этот синтаксис, чтобы исключить из сканирования целые домены верхнего уровня.
www.example?.com	Любой веб-адрес, начинающийся с www.example?.com, где ? заменяет один любой символ. Это могут быть сайты: www.example1.com или www.exampleA.com и др.

Примечание
Вы можете использовать относящиеся к протоколу URL.

- **Application**. Исключает из сканирования указанный процесс или приложение. Чтобы определить исключения при сканировании приложений:

- Введите полный путь к приложению. Например, `C:\Program Files\Internet Explorer\iexplore.exe`
- Используйте переменные среды, чтобы определить точный путь к приложению. Например: `%programfiles%\Internet Explorer\iexplore.exe`
- Используйте маски, чтобы указать любые приложения, соответствующие определенному шаблону имени. Например:
  - `c*.exe` соответствует всем приложениям, начинающимся с "c" (chrome.exe).
  - `??????.exe` соответствует всем приложениям с именем, которое состоит из шести символов (chrome.exe, safari.exe и т.д.).
  - `[^c]*.exe` соответствует всем приложениям, кроме тех, которые начинаются с "c".
  - `[^ci]*.exe` соответствует всем приложениям, кроме тех, которые начинаются с "c" или "i".

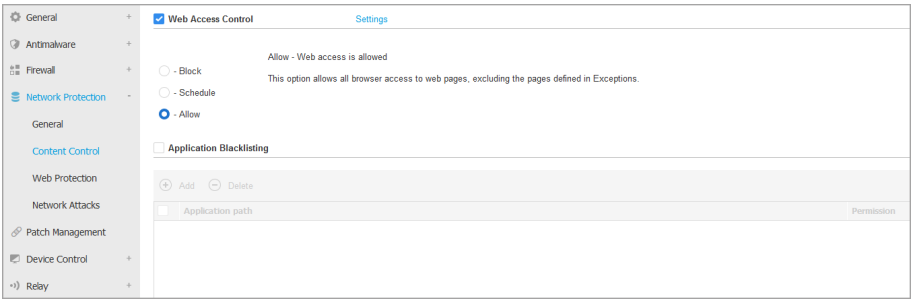
3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

Чтобы удалить объект из списка, нажмите соответствующую кнопку ⊗ **Удалить**.

Контроль контента

Настройки Контент Контроля организованы в следующие разделы:

- Управление веб-доступом
- Application Blacklisting
- Защита данных



Управление веб-доступом

Управление веб-доступом позволяет разрешить или запретить веб-доступ пользователям или приложениям в определенные интервалы времени.

Веб-страницы, заблокированные модулем управления веб-доступом, не будут отображаться в браузере. Вместо этого будет отображаться веб-страница по умолчанию, сообщающая пользователю о том, что запрашиваемая веб-страница была заблокирована модулем управления веб-доступом.

Используйте переключатель, чтобы включить или выключить **Web Access Control**.

У вас есть три возможных варианта:

- Выберите **Разрешить**, чтобы всегда предоставлять доступ в интернет.
- Выберите **Блокировать**, чтобы всегда запрещать доступ в интернет.
- Выберить **Запланировать**, чтобы ввести временные ограничения на веб-доступ по подробному расписанию.

Если вы выберете разрешить или запретить веб-доступ, можно настроить исключения в этих действиях для целых веб-категорий или только для определенных веб-адресов. Нажмите **Настройки**, чтобы настроить расписание веб-доступа и исключения, следующим образом:

Проверка по расписанию

Чтобы ограничить доступ к сети Интернет в определенное время дня еженедельно:

1. Выберите из сетки временные интервалы, в течение которых вы хотите запретить доступ в Интернет.

Можно щелчком мыши отметить отдельные клетки или нажать и расширить ее, чтобы задать более длительный период. Нажмите еще раз на клетку, чтобы изменить выбор.

Чтобы создать новый интервал, нажмите **Разрешить всем** или **Блокировать все**, в зависимости от типа ограничения, которое вы хотите реализовать.

2. Нажмите **Сохранить**.

Примечание
Агент безопасности Bitdefender будет обновляться каждый час независимо от блокировки веб-доступа.

Категории

Веб-фильтр по категориям это динамическая фильтрация доступа к сайтам на основе их содержимого. Вы можете использовать веб-Фильтр по категориям для создания исключений в выбранных действиях управления веб-доступом (Allow или Block) для целых веб-категорий (таких как игры, контент для взрослых или онлайн сети).

Чтобы настроить веб-фильтр по категориям:

1. Включите **Фильтр веб-категорий**.
2. Для быстрой настройки, выберите один из предустановленных профилей (**Интенсивный**, **Нормальный** или **Рекомендуемый**). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень. Вы можете просмотреть предопределенные действия для доступных веб-категорий, раскрыв раздел **Правила сети**, размещенный ниже.
3. Если параметры по умолчанию вам не подходят, вы можете создать пользовательский фильтр:
   a. Выберите **Пользователь**.
   b. Нажмите **Правила сети**, чтобы раскрыть соответствующий раздел.
   c. Найдите категорию, которая вам нужна, в списке и выберите нужное действие из меню. Дополнительную информацию о доступных категориях веб-сайтов см. В этой статье базы знаний .

4. Выберите вариант **Обработать веб-категории как исключения для веб-доступа** , если вы хотите игнорировать существующие настройки веб-доступа и применять только фильтр веб-категорий.
5. Сообщение по умолчанию, отображаемое для пользователя,дает доступ к ограниченным веб-сайтам, также содержит категорию, которой соответствует содержимое веб-сайта. Снимите флажок **Показывать подробные оповещения на клиенте** , если вы хотите скрыть эту информацию от пользователя.

   Примечание
   Эта опция недоступна для macOS.

6. Нажмите **Сохранить**.

Примечание

- Разрешение **Разрешить** для указанных веб-категорий также будет учтено во время блокировки веб-доступа модулем управления.
- Разрешение **Разрешить** работает только тогда, когда веб-доступ запрещен модулем управления, в то время как разрешение **Блокировать** работает только тогда, когда веб-доступ разрешен.
- Вы можете переопределить разрешения категорий для отдельных веб-адресов, добавив их с противоположными разрешениями в **Контроль веб-доступа > Настройки > Исключения**. Например, если веб-адрес заблокирован веб-фильтром категории, можно добавить веб-правило для этого адреса с разрешением **Разрешить**.

Исключения

Вы также можете задать веб-правила по блокировке или разрешению определенных веб-адресов, переопределив существующие настройки модуля управления веб-доступом. Например, пользователи смогут получить доступ к определенной веб-странице, даже если веб-браузинг заблокирован модулем управления веб-доступом.

Чтобы создать веб-правило:

1. Включите опцию **Использовать исключения**.
2. Введите адрес, который вы хотите разрешить или запретить в поле **Веб-адрес**.

3. Выберите **Разрешить** или **Блокировать** из меню **Разрешение**.
4. Нажмите на кнопку ⊕ **Добавить** в правой части таблицы, чтобы добавить адрес в список исключений.
5. Нажмите **Сохранить**.

Чтобы изменить веб-правило:

1. Нажмите веб-адрес, который вы хотите отредактировать.
2. Измените существующий URL.
3. Нажмите **Сохранить**.

Чтобы удалить веб-правило, нажмите соответствующую кнопку ⊗ **Удалить**.

Application Blacklisting

В этом разделе вы можете настроить "черный" список приложений, который поможет вам полностью заблокировать или ограничить доступ пользователей к приложениям на своих компьютерах. Таким образом можно заблокировать игры, мультимедиа и программы обмена мгновенными сообщениями, а также другие категории программного обеспечения и вредоносных программ.

Чтбоы настроить "черный" список приложений:

1. Включите опцию **Черный список приложений**.
2. Укажите приложения, к которым вы хотите ограничить доступ. Чтобы ограничить доступ к приложению:
   a. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.
   b. Вы должны указать путь к исполняемому файлу приложения на требуемых компьютерах. Существует два способа сделать это:
      - Выберите из меню предопределенное местоположение и завершите путь по мере необходимости. Например, для приложения, установленного в папке `Программные файлы`, выберите `%ProgramFiles` и завершите путь, добавив обратную косую черту (\) и имя папки приложения.
      - Введите полный путь в поле редактирования. Желательно использовать системные переменные (где это возможно), чтобы путь был действительным для всех выбранных компьютеров.

c. **Планировщик доступа**. Еженедельное расписание доступа к приложениям в определенное время дня:
   - Выберите из сетки временные интервалы, в течение которых вы хотите, чтобы доступ к приложению был заблокирован. Можно щелчком мыши отметить отдельные клетки или нажать и расширить ее, чтобы задать более длительный период. Нажмите еще раз на клетку, чтобы изменить выбор.
   - Чтобы создать новый отбор, нажмите **Разрешить все** или **Блокировать все**, в зависимости от типа ограничения, которое вы хотите реализовать.
   - Нажмите **Сохранить**. Новое правило будет добавлено в список.

Чтобы удалить правило из списка, выберите его и нажмите кнопку ⊗ **Удалить** в верхней части таблицы. Чтобы отредактировать существующее правило, щелкните на него, чтобы открыть окно настроек.

Защита данных

Защита данных предотвращает несанкционированное разглашение конфиденциальных данных, основываясь на определенных правилах, заданных администратором.

Примечание
Данный компонент недоступен для macOS.

Вы можете создать правила для защиты любой части личной или конфиденциальной информации, такой как:

- Персональная информация заказчика
- Названия и ключевые детали, разрабатываемых продуктов и технологий
- Контактная информация руководителей компании

Защищаемая информация может включать имена, номера телефонов, кредитные карты и информацию о банковских счетах, адреса электронной почты и так далее.

На основании правил защиты данных, которые вы создаете, Bitdefender Endpoint Security Tools сканирует веб и исходящий трафик электронной почты для конкретных символьных строк (например, номер кредитной карты). Если будет найдено совпадение, соответствующая веб-страница или сообщение электронной почты заблокируется, чтобы предотвратить отправку

защищаемых данных. Пользователь будет немедленно оповещен о действиях, предпринятых Bitdefender Endpoint Security Tools, через веб-страницу с предупреждением или сообщением электронной почты.

Чтобы настроить защиту данных:

1. Отметьте соответствующий флажок, чтобы включить защиту данных.
2. Создайте правила защиты для всех конфиденциальных данных, которые необходимо защитить. Чтобы создать правило:
   a. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.
   b. Введите имя, под которым правило будет отображаться в таблице правил. Выберите подходящее имя, чтобы вы или другой администратор мог легко определить назначение этого правила.
   c. Выберите тип данных, которые вы хотите защитить.
   d. Введите данные, которые вы хотите защитить (например, номер телефона представителя компании, или внутреннее имя нового продукта, над которым работает компания). Это может быть любая комбинация слов, цифр или строк, состоящих из буквенно-цифровых и специальных символов (например, @, # или $) принимается.

      Введите по меньшей мере пять символов для того, чтобы избежать ошибочной блокировки сообщений электронной почты и веб-страниц.

      Важно

      Данные будут храниться в зашифрованном виде на защищаемых конечных точках, но эту информацию можно будет увидеть под вашим аккаунтом в Control Center. Для дополнительной безопасности не вводите полные данные, которые вы хотите защитить. В этом случае, вы должны очистить опцию **Совпадение целых слов**.

   e. Настройте требуемые параметры сканирования трафика.
      - **Веб сканирование (HTTP traffic)** - сканирует HTTP (веб) трафик и блокирует исходящие данные, которые соответствуют данным правилам.

- **Email сканирование (SMTP traffic)** - сканирует SMTP (почта) трафик и блокирует исходящие сообщения электронной почты, содержащие данные правил.

Вы можете выбрать: применять правило только в случае если совпадение произойдет по всему слову целиком или же если совпадение произойдет по нахождению искомой строки.

f. Нажмите **Сохранить**. Новое правило будет добавлено в список.

3. Настройте исключения в правилах защиты данных так, чтобы пользователи могли отправлять защищаемые данные разрешенным веб-сайтам и получателям. Исключения могут быть применены в глобальном масштабе (для всех правил) или только для определенных правил. Чтобы добавить исключение:
   a. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.
   b. Введите веб-адрес или адрес электронной почты пользователей, которым разрешено раскрывать защищаемые данные.
   c. Выберите тип исключения (веб-адрес или адрес электронной почты).
   d. Из таблицы **Правила**, выберите правило(а) защиты данных, для которого это исключение следует применять.
   e. Нажмите **Сохранить**. Новое правило исключений будет добавлено в список.

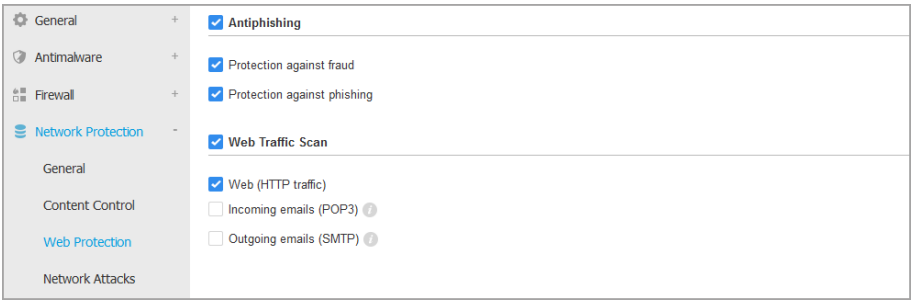
Примечание
Если письмо, содержащее блокируемые данные, адресовано нескольким получателям, для которых были определены исключения, они его получат.

Чтобы удалить правило или исключения из списка, нажмите соответствующую кнопку ⊗ **Удалить** в правой части таблицы.

Веб-защита

На этой странице настройки организованы в следующие разделы:

- Антифишинг
- Сканирование веб-трафика



Политики компьютеров и виртуальных машин - Защита сети - Веб-защита

Антифишинг

Защита от фишинга автоматически блокирует известные фишинговые веб-страницы, чтобы пользователи случайно не раскрыли частную или конфиденциальную информацию интернет-мошенникам. При этом вместо фишинговых веб-страниц отображается особая страница предупреждения в браузере, чтобы сообщить пользователю, что запрошенная веб-страница опасна.

Выберите **Анти-Фишинг**, чтобы активировать антифишинговую защиту. Вы можете дополнительно настроить антифишинг, с помощью следующих параметров:

- **Защита от мошенничества**. Выберите эту опцию если вы хотите расширить защиту от других видов мошенничества, помимо фишинга. Например, от веб-сайтов, представляющих поддельные компании, которые непосредственно не запрашивают конфиденциальную информацию, но вместо этого пытаются представиться в качестве законных предприятий и получить прибыль, обманывая людей в деловых отношениях с ними.
- **Защита от фишинга**. Используйте эту опцию, чтобы защитить пользователей от попыток фишинга.

Если легитимная веб-страница некорректно определяется как фишинговая и блокируется, вы можете добавить ее в белый список, чтобы позволить пользователям доступ к ней. Список должен содержать только веб-сайты, которым вы полностью доверяете.

Для управления исключениями модуля антифишинга:

1. Перейдите в раздел **Общие настройки** и нажмите кнопку **Глобальные исключения**.
2. Введите веб-адрес и нажмите кнопку ⊕ **Добавить**.

   Если вы хотите исключить весь сайт, напишите имя домена, например, `http://www.website.com`, а если вы хотите исключить только веб-страницу, напишите точный веб-адрес этой страницы.

   Примечание
   Символы шаблонов не применяются при указании URL.

3. Чтобы удалить исключение из списка, нажмите соответствующую кнопку ⊗ **Удалить**.
4. Нажмите **Сохранить**.

Сканирование веб-трафика

Входящие сообщения электронной почты (POP3) и веб-трафик проверяются в режиме реального времени, чтобы предотвратить проникновение вредоносного ПО в конечную точку. Исходящие письма (SMTP) проверяются для предотвращения заражения вредоносными программами других конечных точек. Сканирование веб-трафика может несколько замедлить работу в Интернет, однако такое сканирование позволяет блокировать вредоносные программы, которые проникают в ваш компьютер из Интернет, включая скрытые загрузки.

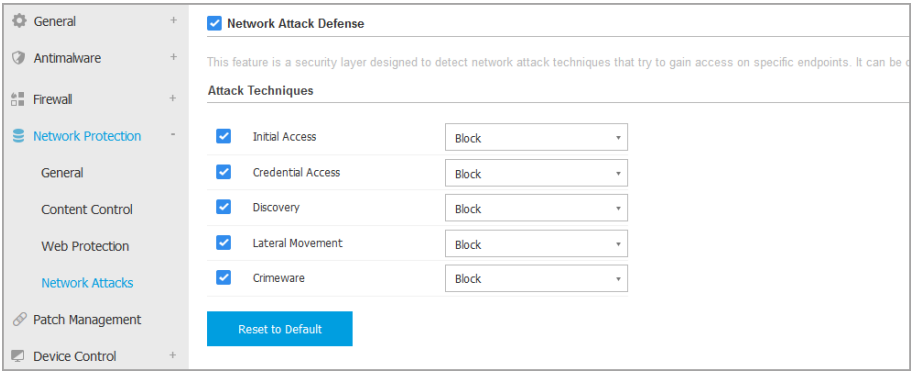
При обнаружении зараженной электронной почты, она автоматически заменяется стандартным письмом, информирующим получателя оригинального зараженного письма. Если веб-страница содержит или распространяет вредоносные программы, она автоматически блокируется. При этом будет отображена специальная страница предупреждения, информирующая пользователя о том, что запрашиваемая веб-страница опасна.

Можно отключить сканирование электронной почты и веб-трафика, чтобы увеличить производительность системы (не рекомендуется). Данное действие не будет представлять существенной угрозы до тех пор, пока сканирование при доступе локальных файлов остается включенным.

Примечание
Параметры **Входящие сообщения** и **Исходящие сообщения** недоступны для macOS.

сетевые атаки

Network Attack Defense предоставляет уровень безопасности, основанный на технологии Bitdefender, которая обнаруживает и предпринимает действия против сетевых атак, предназначенных для получения доступа к конечным точкам, с помощью специальных методов, таких как: атаки методом перебора, сетевые "эксплоиты" и программы для кражи паролей.



Политики компьютеров и виртуальных машин - Защита сети - Сетевые атаки

Чтобы настроить Network Attack Defense:

1. Установите флажок **Network Attack Defense** , чтобы включить модуль.
2. Установите соответствующие флажки, чтобы включить защиту от каждой категории сетевых атак. Методы сетевых атак сгруппированы в соответствии с данными MITRE ATT&CK, основанными на следующем:
   - **Начальный доступ** - злоумышленник получает доступ в сеть различными способами, в том числе уязвимости общедоступных веб-серверов. Например: эксплойты для раскрытия информации, эксплойты SQL-инъекций, векторы заражения посредством скрытой загрузки.
   - **Доступ к учетным данным** - злоумышленник крадет такие учетные данные, как имена пользователей и пароли, чтобы получить доступ к

системам. Например: атаки методом перебора, эксплойты несанкционированной аутентификации, программы для кражи паролей.

- **Обнаружение** - после проникновения злоумышленник пытается получить информацию о системах и внутренней сети, прежде чем решить, что делать дальше. Например: эксплойты выхода в файловую систему сервера, эксплойты выхода в файловую систему HTTP.
- **Боковое движение** - злоумышленник исследует сеть, часто перемещаясь по нескольким системам, чтобы найти основную цель. Злоумышленник может использовать специальные инструменты для достижения цели. Например: эксплойты с использованием командных инъекций, эксплойты Shellshock, эксплойты с двойным расширением.
- **Мошенническое ПО** - эта категория включает в себя методы, предназначенные для автоматизации киберпреступности. Например, методы мошенничества: ядерные эксплойты, различные вредоносные программы, такие как трояны и боты.

3. Выберите действия, которые вы хотите предпринять против каждой категории методов сетевой атаки, из следующих вариантов:
   a. **Блокировка** - Network Attack Defense останавливает попытку атаки после обнаружения.
   b. **Только отчет**- Network Attack Defense информирует вас о обнаруженной попытке атаки, но не пытается остановить ее.

Вы можете легко восстановить первоначальные настройки, нажав кнопку **Восстановление настроек по умолчанию** в нижней части страницы.

Подробная информация о попытках сетевых атак доступна в отчете о сетевых инцидентах и в уведомлении о сетевых инцидентах.

7.2.7. Управление исправлениями

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов

Модуль управления исправлениями освобождает вас от необходимости обновлять конечные точки с помощью последних обновлений программного

обеспечения, автоматически распределяя и устанавливая исправления для широкого спектра продуктов.

Примечание
Вы можете проверить список поддерживаемых поставщиков и продуктов в этой статье базы знаний .

Этот раздел политики содержит параметры для автоматического развертывания исправлений. Сначала вы будете настраивать, как патчи загружаются в конечные точки, а затем какие патчи устанавливать и когда.

Настройка параметров загрузки исправления

В процессе распространения исправлений используются серверы кэширования исправлений для оптимизации сетевого трафика. Конечные точки подключаются к этим серверам и загружают исправления через локальную сеть. Для высокой доступности исправлений рекомендуется использовать более одного сервера.

Чтобы назначить серверы кэширования исправлений целевым конечным точкам:

1. В разделе **Параметры загрузки исправлений** щелкните поле в верхней части таблицы. Появится список обнаруженных серверов кеширования патчей.

   Если список пуст, вам нужно установить роль сервер кеширования исправлений на реле в вашей сети. Для подробной информации обратитесь в Гид по установке.

2. Выберите сервер из списка.
3. Нажмите кнопку ⊕ **Добавить**.
4. Если необходимо, повторите предыдущие шаги чтобы добавить другие серверы.
5. Используйте стрелки вверх и вниз с правой стороны таблицы, чтобы установить приоритет сервера. Приоритет уменьшается сверху вниз по списку.

   Конечная точка запрашивает исправление у назначенных серверов в порядке приоритета. Конечная точка загружает исправление с сервера, где оно находит его первым. Сервер, на котором отсутствует запрошенное

исправление, автоматически загрузит его от поставщика, чтобы сделать его доступным для будущих запросов.

Чтобы удалить ненужные серверы, нажмите соответствующую кнопку ⊖Удалить в правой части таблицы.

Выберите параметр **Использовать веб-сайты поставщиков в качестве запасного места для загрузки исправлений** , чтобы убедиться, что ваши конечные точки получают исправления программного обеспечения в случае недоступности серверов кэширования исправлений.

Настройка и установка сканирования исправлений

GravityZone выполняет развертывание исправление в два независимых этапа:

1. Оценка По запросу через консоль управления конечные точки сканируют отсутствующие исправления и сообщают о них.
2. Установка Консоль отправит агентам список исправлений, которые вы хотите установить. Конечная точка загружает исправления с сервера кэширования исправлений, а затем устанавливает их.

Политика предоставляет параметры для автоматизации этих процессов, частично или полностью, чтобы они периодически запускались в соответствии с предпочтительным расписанием.

Чтобы настроить автоматическое сканирование исправлений:

1. Выберите флажок **Автоматическое сканирование исправлений**.
2. Используйте параметры планирования для настройки повторения сканирования. Вы можете настроить сканирование ежедневно или в определенные дни недели, в определенное время.
3. Выберите **Интеллектуальное сканирование при установке нового приложения/программы**, чтобы определить, когда новое приложение было установлено на конечной точке и какие патчи доступны для него.

Чтобы настроить автоматическую установку исправлений:

1. Установите флажок **Установить исправления автоматически после сканирования** .
2. Выберите, какие исправления следует установить: безопасности, иные или все сразу.

3. Используйте параметры планирования для настройки времени запуска задач установки. Вы можете настроить сканирование сразу после завершения сканирования исправлений, ежедневно или в определенные дни недели, в определенное время. Мы рекомендуем устанавливать исправления безопасности сразу после их обнаружения.

4. По умолчанию все продукты имеют право на исправления. Если вы хотите автоматически обновить только набор продуктов, которые вы считаете важными для вашего бизнеса, выполните следующие действия:

   a. Выберите флажок **Особый поставщик и продукт**.

   b. Нажмите поле **Поставщик** в верхней части таблицы. Отобразится список всех поддерживаемых поставщиков.

   c. Прокрутите список и выберите поставщика для продуктов, которые вы хотите исправить.

   d. Нажмите поле **Продукт** в верхней части таблицы. Отобразится список всех продуктов выбранного поставщика.

   e. Выберите все продукты, которые вы хотите исправить.

   f. Нажмите кнопку ⊕ **Добавить**.

   g. Повторите предыдущие шаги для оставшихся поставщиков и продуктов.

   Если вы забыли добавить продукт или хотите удалить его, найдите поставщика в таблице, дважды щелкните поле **Продукты** и выберите или отмените выбор продукта в списке.

   Чтобы удалить поставщика и все его продукты, найдите его в таблице и нажмите соответственно кнопку ⊖ **Удалить** в правой части таблицы.

5. По различным причинам конечная точка может быть отключена, когда назначена установка исправления. Выберите параметр **Если пропущено, запустите как можно скорее** , чтобы установить исправления сразу после того, как конечная точка вернется в оперативный режим.

6. Некоторые исправления требуют перезагрузки системы после установки. Если вы хотите сделать это вручную, выберите параметр **Отложить перезапуск**.

Важно

Для успешной оценки и установки на конечных точках Windows необходимо убедиться, что выполнены следующие требования:

- **Доверенные корневые центры сертификации** хранит **Сертификат корневого ЦС DigiCert Assured ID**.
- **Промежуточные центры сертификации** включает в себя **центр сертификации подписанного кода DigiCert SHA2**.
- На конечных точках установлены исправления для Windows 7 и Windows Server 2008 R2, упомянутые в этой статье Microsoft: Рекомендации по безопасности Microsoft 3033929

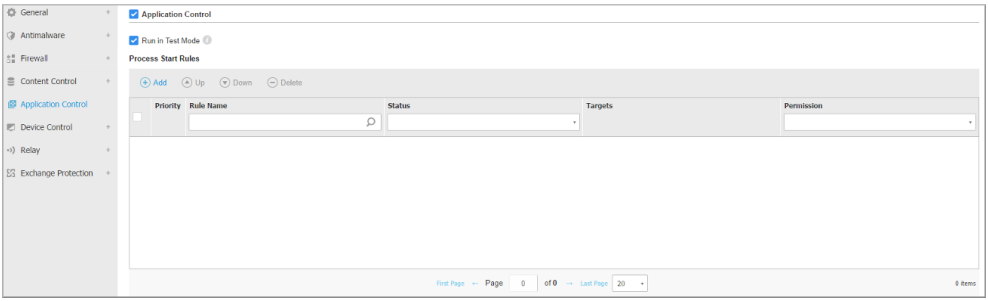
7.2.8. Контроль приложений

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов

Модуль Контроль приложений добавляет еще один уровень защиты от всех видов вредоносных угроз (вымогателей, атак нулевого дня, эксплойтов на сторонние приложения, троянов, шпионских программ, руткитов, рекламного ПО и т. Д.) блокирование запуска неавторизованных приложений и процессов. Управление приложениями уменьшает поверхность атаки, которую вредоносные программы могут усиленно использовать для воздействия на конечную точку, предотвращает установку и выполнение каких-либо нежелательных, ненадежных или вредоносных приложений.

Управление приложениями обеспечивает гибкое соблюдение политик, которые позволяют формировать "белый" список приложений и управлять разрешениями на их обновления.



Контроль приложений

Важно

- Чтобы включить **Контроль приложений** для ваших текущих установленных клиентов, запустите задачу **Переконфигурировать клиента**. После установки модуля вы можете просмотреть его статус в окне **Информация**.
- Управление приложениями сильно влияет на режим привилегированного пользователя после обновления приложения. Например, когда "белый" список приложений обновится, конечная точка будет представлять новую информацию. GravityZone обновляет правила с новыми значениями и повторно отправляет политику.

Вы должны запустить задачу **Обнаружение приложений** для просмотра запущенных приложений и процессов в вашей сети. Для получения более подробной информации, обратитесь к «Обнаружение Приложений» (p. 109). Затем, вы можете определить правила Управления приложениями.

Управление приложениями работает в двух режимах:

- **Тестовый режим**. Управление приложениями только обнаруживает и сообщает информацию приложениям в Control Center, в результате чего они продолжают работать как обычно. Вы можете настроить и проверить свои правила и политики для "белого" списка, но приложения не будут заблокированы.
- **Режим производства**. Управление приложениями блокирует все неизвестные приложения. Процессы операционной системы Microsoft и процессы Bitdefender включены в "белый" список по умолчанию. Приложениям, указанным в "белом" списке, будет разрешен запуск. Для обновления "белого" списка приложений, необходимо определить, кто

имеет право обновлять список приложений. Это специфические процессы, которым разрешено изменять существующие приложения. Для получения более подробной информации, обратитесь к «Инвентаризация Приложений» (p. 208).

Предупреждение

- Чтобы убедиться в том, что легитимные приложения не ограничивается модулем Управления приложениями, вы должны запустить модуль, в первую очередь, в тестовом режиме. Таким образом, вы сможете убедиться, что правила и политики для "белого" списка заданы правильно.
- Процессы, которые работали при переключении модуля Управления приложениями в режим **Режим производства**, будут заблокированы после следующего перезапуска.

Для управления разрешениями на запуск приложений:

1. Отметьте флажком **Контроль приложений**, чтобы включить этот модуль.
2. Используйте флажок **Запустить в тестовом режиме** для включения или выключения тестового режима.

Примечание

- В тестовом режиме вы будете уведомлены, когда модуль Управления приложениями заблокирует определенное приложение. Для получения более подробной информации, обратитесь к «Типы уведомлений» (p. 576).
- **Заблокированное приложение** уведомления будут отображаться в области уведомлений при обнаружении новых приложений и при блокировке приложений из "черного" списка.

3. Определение правил запуска процесса.

Правило Запуска процесса

Модуль Управления приложениями позволяет вам вручную разрешать определенные приложения и процессы, основываясь на хэше исполняемых файлов, отпечатке сертификата и пути приложения. Вы также можете задать исключения для правил:

Примечание
Чтобы получить собственные значения хэш исполняемого файла и отпечаток сертификата используйте«Инструменты модуля Управления приложениями» (p. 613)

Таблица **Правила запуска процесса** информирует вас о существующих правилах, предоставляя важную информацию:

- Приоритет правил. Правило с более высоким приоритетом будет находиться в списке выше.
- Имя правила и статус.
- Приложения и разрешение на их запуск. Выбор представляет собой определенное количество условий, которые должны выполняться для применения правила.

Чтобы создать правило запуска процесса:

1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы открыть окно конфигурации.
2. В разделе **Общее** введите **Имя правила**.
3. Отметьте флажок **Включить**, чтобы активировать правило.
4. В разделе **Задачи** укажите назначение правила:
   - **Конкретный процесс или процессы**, чтобы определить процесс, запуск которого разрешен или запрещен. Вы можете авторизовать его по пути, хэшу или сертификату. Условия внутри правила складываются логическим AND.
     – Для авторизации приложения по конкретному пути:
       a. Выберите **Путь** в столбце **Тип**. Укажите путь к объекту. Вы можете указать абсолютный или относительный путь к файлу и использовать знаки подстановки. Символ звездочки (*) соответствует любому файлу в директории. Двойная звездочка (**) соответствует всем файлам и каталогам в определенной директории. Вопросительный знак (?) соответствует только одному символу. Кроме того, вы можете добавить описание, чтобы помочь идентифицировать процесс.
       b. Из выпадающего меню **Выберите один или несколько контекстов** вы можете выбрать локальный, CD-ROM, съемный или сетевой

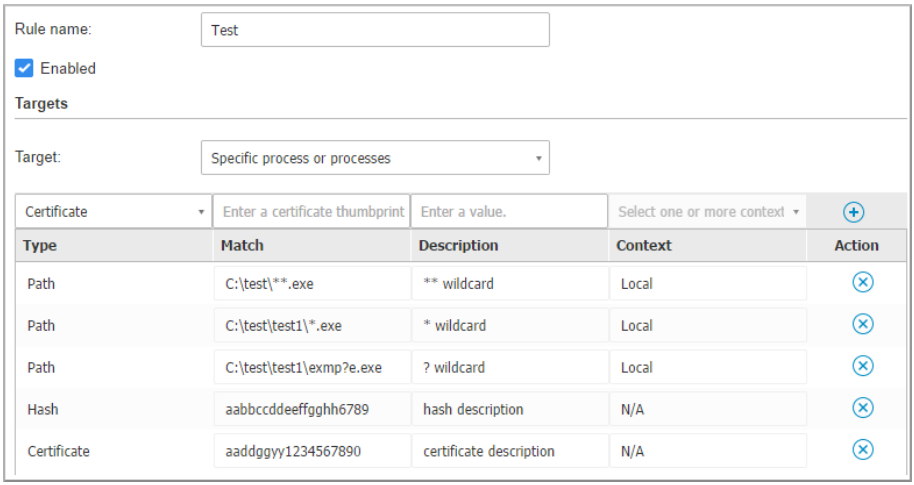
диск. Вы можете заблокировать выполнение приложения со съемного носителя или разрешить, если приложение выполняется локально.

– Для авторизации приложение на основе хэша, выберите **Хэш** в столбце **Тип** и введите значение хеш-функции. Кроме того, вы можете добавить описание, чтобы помочь идентифицировать процесс.

Важно
Для генерации значения хэша, скачайте инструмент Отпечаток пальца. Для получения более подробной информации, обратитесь к «Инструменты модуля Управления приложениями» (p. 613)

– Для авторизации на основе сертификата, выберите **Сертификат** в столбце **Тип** и введите отпечаток сертификата. Кроме того, вы можете добавить описание, чтобы помочь идентифицировать процесс.

Важно
Чтобы получить отпечаток сертификата, скачайте инструмент Thumbprint. Для получения более подробной информации, обратитесь к «Инструменты модуля Управления приложениями» (p. 613)



Правила приложений (Application Rules)

Нажмите ⊕ **Добавить**, чтобы добавить правило.

- **Инвентаризация приложений или групп**, чтобы добавить группу или приложение, обнаруженное в вашей сети. Вы можете просматривать приложения, запущенные в вашей сети, на странице **Сеть >Инвентаризация приложений**. Для получения более подробной информации, обратитесь к «Инвентаризация Приложений» (p. 208).

  Вставьте имена приложений или названия групп в поле, разделенные запятой. Функция автоматического заполнения отображает подсказки при вводе.

5. Отметьте флажок **Включить подпроцессы**, чтобы применить правило к порожденным дочерним процессам.

   Предупреждение
   При настройке правил для приложений браузера, рекомендуется отключить эту опцию, чтобы предотвратить угрозы безопасности.

6. Дополнительно, вы также можете задать исключения для правила запуска процесса. Сложение операций аналогично описанию в предыдущих шагах.

7. В разделе **Разрешения** выберите, следует разрешить или запретить правила для запуска.
8. Нажмите **Сохранить**, чтобы сохранить изменения.

Для редактирования существующего правила:

1. Нажмите на название правила, чтобы открыть окно конфигурации.
2. Задайте новые значения для опций, которые вы хотите изменить.
3. Нажмите **Сохранить**, чтобы сохранить изменения.

Для того, чтобы установить приоритет правила:

1. Отметьте флажком нужное правило.
2. Используйте кнопки для задания приоритетов в правой части таблицы:
   - Нажмите кнопку **Вверх**, чтобы поднять приоритет выбранного правила.
   - Нажмите кнопку **Вниз**, чтобы понизить ее приоритет.

Вы можете удалить одно или несколько правил одновременно. Все, что вам нужно сделать, это:

1. Выберите правила, которые вы хотите удалить.
2. Нажмите кнопку **Удалить** в верхней части таблицы. После удаления правило нельзя восстановить.

7.2.9. Контроль устройств

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- ОС MAK

Модуль управления устройствами позволяет предотвратить утечки данных и проникновение вредоносного ПО через внешние устройства, подключаемые к конечным точкам, применяя с помощью политик правила блокировок и исключений, для широкого спектра типов устройств.

Важно

Для macOS Контроль устройств использует расширение ядра. Установка расширения ядра требует подтверждения пользователя на macOS High Sierra (10.13.x). Система уведомляет пользователя о том, что расширение системы от Bitdefender было заблокировано. Пользователь может разрешить это в настройках **Безопасность и конфиденциальность** . Пока пользователь не утвердит расширение системы Bitdefender, этот модуль не будет работать, а пользовательский интерфейс Endpoint Security for Mac покажет критическую проблему, запрашивающую утверждение.

Чтобы исключить вмешательство пользователя, вы можете предварительно утвердить расширение ядра Bitdefender, занеся его в белый список с помощью инструмента управления мобильными устройствами. Подробнее о расширениях ядра Bitdefender см. эту статью базы знаний .

Для использования модуля управления устройствами, необходимо сначала включить его в агент безопасности, устанавливаемый на выбранных конечных точках, затем включить опцию **Контроль устройства** в политике, применяемой к этим конечным точкам. После этого, каждый раз при подключении внешнего устройства к управляемой конечной точке, агент безопасности будет отправлять информацию об этом событии в Control Center, в том числе об имени устройства, классе, ID, дате и времени подключения.

В следующей таблице вы можете найти типы устройств, которые поддерживаются Контролем устройств в системах Windows и macOS:

Тип устройств	Windows	ОС MAK
Адаптеры Bluetooth	x	x
Устройства CD-ROM	x	x
Дисковые накопители на гибких дисках	x	Данные отсутствуют
IEEE 1284.4	x	
IEEE 1394	x	
Устройства обработки изображений	x	x
Модемы	x	Сетевые адаптеры, управляемые из-под системы
Ленточные накопители	x	Данные отсутствуют

Тип устройств	Windows	ОС MAK
Портативные Windows-устройства	x	x
Порты COM/LPT	x	LPT к последовательным портам поддерживается
SCSI Raid	x	
Принтеры	x	Поддерживает только локально подключенные принтеры
Сетевой адаптер	x	x (включая ключи Wi-Fi)
Беспроводные сетевые адаптеры	x	x
Внутренние устройства хранения информации	x	
Внешнее устройство хранения информации	x	x

Примечание

- В macOS, если для определенного класса устройств выбрано **Пользователь** разрешение, будут применяться только разрешения, настроенные для подкатегории **Другое**. ,
- Device Control разрешает или запрещает доступ к адаптеру Bluetooth на системном уровне в Windows и macOS в соответствии с политикой. Возможность установки конкретного исключения для каждого сопряженного устройства отсутствует.

Модуль управления устройствами позволяет управлять разрешениями следующим образом:

- Создание правил разрешений
- Создание правил исключений

Правила

Раздел **Правила** позволяет создавать разрешения для устройств, подключаемых к конечным точкам.

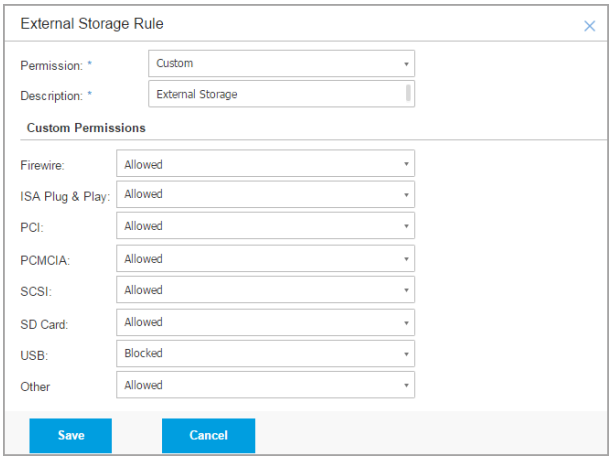
Чтобы задать разрешения определенным типам устройств:

1. Перейдите в **Управление устройством > Правила**.
2. Нажмите на название устройства в представленной таблице.
3. Выберите один тип разрешения из доступных вариантов. Пожалуйста, обратите внимание, что доступно множество разрешений, которые могут варьироваться в зависимости от типа устройства:
   - **Разрешенное**: устройство можно использовать на конечной точке.
   - **Блокированное**: устройство не может быть использовано на конечной точке. В этом случае, каждый раз, когда устройство подключается к конечной точке, агент безопасности покажет уведомление о том, что это устройство заблокировано.

     Важно
     Подключенные устройства, ранее заблокированные, не разблокируются автоматически путем изменения разрешения на **Разрешено** . Пользователь должен перезагрузить систему или повторно подключить устройство, чтобы иметь возможность использовать его.

   - **Только чтение**: может быть использована только функция чтения на данном устройстве.
   - **Пользователь**: позволяет создавать разные разрешения для каждого типа используемого порта, таких как Firewire, ISA Plug & Play, PCI, PCMCIA, USB, т.д. В этом случае, отображается список компонентов, доступных для выбранного устройства, и вы можете установить желаемые разрешения для каждого компонента.

     Например, для внешних накопителей вы можете заблокировать только порты USB и позволить использовать все остальные порты.



Политики компьютеров и виртуальных машин - Управление устройствами - Правила

Исключения

После установки правил разрешений для разных типов устройств, вы можете исключить определенные устройства или типы устройств из этих правил.

Вы можете задать исключения для устройств:

- По ID устройства (или аппаратного ID), для обозначения определенных устройств, которые вы хотите исключить.
- По ID модели (или PID), для определения диапазона устройств, произведенных одним производителем.

Чтобы создать правила исключений для устройств:

1. Перейдите в **Управление устройством > Исключения**.
2. Включите опцию **Исключения**.
3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.
4. Выберите способ, который вы хотите использовать для добавления исключений:
   - **Вручную**. В этом случае, вы должны ввести идентификатор каждого устройства или ID продукта, который вы хотите исключить, если у вас есть под рукой список соответствующих идентификаторов:

a. Выберите тип исключения (по ID модели или по ID устройства).
b. В поле **Исключения**, введите идентификаторы, которые вы хотите исключить.
c. В поле **Описание** введите имя, которое поможет вам определить устройство или набор устройств.
d. Выберите тип разрешения для указанных устройств (**Разрешено** или **Заблокировано**).
e. Нажмите **Сохранить**.

Примечание
Можно вручную настроить исключения подстановочных знаков на основе идентификатора устройства, используя синтаксис `подстановочные знаки: deviceID` . Используйте знак вопроса (?), чтобы заменить один символ, и звездочку (*), чтобы заменить любое количество символов в `идентификаторе устройства` . Например, для `Подстановочные знаки:PCI\VEN_8086*` все устройства, содержащие строку `PCI\VEN_8086` в своих ID будут исключены из правил политики.

- **С обнаруженного устройства**. В этом случае, вы можете выбрать идентификаторы устройств или идентификаторы моделей для исключения из списка всех обнаруженных устройств в вашей сети (в отношении только управляемых конечных точек):
  a. Выберите тип исключения (по ID модели или по ID устройства).
  b. В таблице **Исключения** выберите идентификатор, который вы хотите исключить:
     – Для идентификаторов устройств (Hardware ID), выберите каждое устройство, которое необходимо исключить из списка.
     – Для идентификаторов моделей (PID), выберите одно устройство, чтобы исключить все устройства, имеющие тот же ID модели.
  c. В поле **Описание** введите имя, которое поможет вам определить устройство или набор устройств.
  d. Выберите тип разрешения для указанных устройств (**Разрешено** или **Заблокировано**).
  e. Нажмите **Сохранить**.

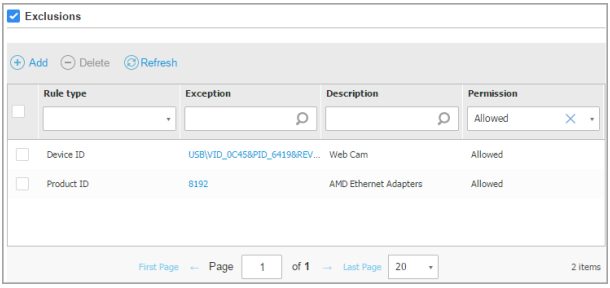
Важно

- Устройства, уже подключеные к конечным точкам, будут обнаружены Bitdefender Endpoint Security Tools только после перезапуска соответствующих конечных точек.
- Подключенные устройства, ранее заблокированные, не разблокируются автоматически путем установки разрешения на **Разрешено** . Пользователь должен перезагрузить систему или повторно подключить устройство, чтобы иметь возможность использовать его.

Все исключенные устройства появятся в таблице **Exclusions**.

Чтобы удалить исключение:

1. Выберите его в таблице.
2. Нажмите кнопку ⊕ **Удалить** в верхней части таблицы.



Политики компьютеров и виртуальных машин - Управление устройствами - Исключения

7.2.10. Ретранслятор

Примечание

Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- Linux

В этом разделе вы можете задать настройки связи и обновлений для конечных точек с ролью ретранслятора.

Настройки объединены в следующие разделы:

- Коммуникации
- Обновления

Коммуникации

Вкладка **Связь** содержит настройки прокси-сервера для связи между ретрансляторами и компонентами GravityZone.

При необходимости, вы можете самостоятельно настроить связь между выбранными конечными точками-ретрансляторами и облачным сервисом Bitdefender/GravityZone, используя следующие параметры:

- **Сохранить настройки установки**, чтобы использовать параметры прокси-сервера, определенные в установочном пакете.
- **Использовать прокси, определенный в общем разделе**, чтобы использовать параметры прокси-сервера, определенные в текущей политике в разделе **Общее > Настройки**.
- **Не использовать**, когда конечные точки не связываются с конкретными компонентами Bitdefender через прокси-сервер.

Обновления

Этот раздел позволяет настроить параметры обновлений для конечных точек с ролью ретранслятора:

- В разделе **Обновление** вы можете настроить следующие параметры:
  - Интервал времени проверки ретранслятором наличия обновлений.
  - Расположение папки на ретрансляторе, куда обновления продукта и сигнатур будут загружаться и зеркалироваться. Если вы хотите задать конкретную папку загрузки, введите ее полный путь в соответствующем поле.

    Важно
    Рекомендуется задать специальную папку для обновлений продукта и сигнатур. Избегайте выбора папки, содержащей систему или личные файлы.

- **Определить пользовательское место обновления**. По умолчанию, обновления для агентов-ретрансляторов располагаются на локальном

сервере обновлений GravityZone. Вы можете указать другие источники обновлений, указав IP-адрес или имя одного или нескольких серверов обновлений в сети, а затем настроить приоритеты их использования кнопками вверх и вниз, отображаемые при наведении мыши. Если первый источник обновлений недоступен, будет использован следующий в списке и так далее.

Чтобы задать пользовательское месторасположение обновлений:

1. Включите опцию **Определить пользовательские места обновления**.
2. Введите адрес нового сервера обновлений в поле **Добавить локацию**. Используйте один из следующих вариантов синтаксиса:
   - `update_server_ip:port`
   - `update_server_name:port`

   По умолчанию используется порт 7074.
3. Если конечная точка-ретранслятор общается с локальным сервером обновлений через прокси-сервер, выберите **Использовать прокси**. Настройки прокси-сервера, заданные в разделе **Общее > Настройки**, будут учтены.
4. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.
5. Используйте стрелки ⌃ вверх / ⌄ вниз в колонке **Действие**, чтобы установить приоритет использования источников обновлений. Если первый источник обновлений недоступен, будет использован следующий в списке и так далее.

Чтобы удалить папку из списка, нажмите соответствующую кнопку ⊗ **Удалить**. Вы можете удалить источник обновлений по умолчанию (не рекомендуется).

7.2.11. Защита Exchange

Примечание
Этот модуль доступен для Windows для серверов.

Security for Exchange поставляется с очень гибкими настройками, которые позволяют защитить серверы Microsoft Exchange от таких угроз, как вредоносные программы, спам и фишинг. Защита Exchange, установленная на вашем почтовом сервере, позволяет вам также фильтровать сообщения,

содержащие вложения, или если содержание писем считается опасным, в соответствии с политиками безопасности вашей компании.

Чтобы сохранить нормальную производительность сервера, трафик электронной почты обрабатывается фильтрами Security for Exchange в следующем порядке:

1. Фильтрация спама
2. Управление контентом > Фильтрация контента
3. Управление контентом > Фильтрация вложений
4. Фильтрация вредоносных программ

Настройки Security for Exchange организованы в следующих разделах:

- Основные
- Защита от вредоносного ПО
- Антиспам
- Контроль контента

Основные

В этом разделе вы можете создавать и управлять группами учетных записей электронной почты, определять срок хранения объектов в карантине и блокировать определенных отправителей.

Группы пользователей

Control Center позволяет создавать группы пользователей, для которых могут применяться различные политики сканирования и фильтрации. Например, вы можете создать соответствующую политику для ИТ-отдела, отдела продаж или для менеджеров вашей компании.

Группы пользователей создаются глобально, независимо от политик или пользователей, которые их создали.

Для более легкого управления группами, Control Center автоматически импортирует группы пользователей из Windows Active Directory.

Чтобы создать пользовательскую группу:

1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Отобразится окно подробной информации.
2. Введите имя группы, ее описание и адреса электронной почты пользователей.

Примечание

- Для большого количества адресов электронной почты, вы можете скопировать и вставить список из текстового файла.
- Допустимые разделители: пробел, запятая, точка с запятой и ввод.

3. Нажмите **Сохранить**.

Пользовательские группы доступны для редактирования. Нажмите на название группы, чтобы открыть окно настроек, где вы можете изменить данные о группе или отредактировать список пользователей.

Чтобы удалить пользовательскую группу из списка, выберите группу и нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Примечание

Вы не можете редактировать или удалять группы Active Directory.

Настройки

- **Удалить помещенные на карантин файлы, чей срок больше чем (дней).** По умолчанию, файлы в карантине старше 30 дней удаляются автоматически. Для того, чтобы изменить период, введите новое значение в соответствующем поле.
- **Черный список подключений** Если эта опция включена, сервер Exchange отклоняет все письма из черного списка отправителей.

  Чтобы создать черный список:
  1. Нажмите на ссылку **Редактировать элементы в черном списке**.
  2. Введите адрес электронной почты, который вы хотите заблокировать. При редактировании списка вы также можете использовать специальные символы, чтобы задать домен или шаблон для адресов входящей электронной почты:
     - Звездочка (*) заменяет ноль, один или более символов.
     - Вопросительный знак (?) заменяет один любой символ.

     Например, если ввести `*@boohouse.com`, все адреса электронной почты из домена `boohouse.com` будут заблокированы.
  3. Нажмите **Сохранить**.

Проверка IP-адреса домена (Антиспуфинг)

Используйте этот фильтр, чтобы предотвратить подмену спамерами адресов электронной почты отправителей (спуфинг) и принятие электронной почты как доверенной. Вы можете указать IP-адреса, которым вы разрешаете отправку электронной почты в ваши почтовые домены, и, при необходимости, других известных почтовых доменов. Если появится сообщение от одного из перечисленных доменов, но IP-адрес отправителя не совпадет ни с одним из заданных IP-адресов, электронная почта будет отклонена.

Предупреждение

Не используйте этот фильтр, если вы используете смарт-хост, услугу почтовой фильтрации или фильтрующий шлюз электронной почты перед вашим сервером Exchange.

Важно

- Фильтр проверяет только почтовые подключения, не прошедшие проверку подлинности.
- Лучшие практики:
  - Рекомендуется использовать этот фильтр только на серверах Exchange, которые непосредственно используются в Интернет. Например, если у вас есть оба сервера Edge Transport и Hub Transport, настройте этот фильтр только на серверах Edge.
  - Добавьте в ваш список доменов все внутренние IP-адреса, которые могут отправлять почту по SMTP, не проходя проверку подлинности соединения. Это могут быть автоматизированные системы оповещения, сетевое оборудование, такое как принтеры и т.д.
  - На серверах Exchange, использующих Database Availability Groups, также добавьте в список доменов IP-адреса всех серверов с ролью Hub Transport и Mailbox.
  - Будьте осторожны при добавлении в разрешенные IP-адресов внешних почтовых доменов, которые не находятся под вашим управлением. Если вы не будете актуализировать список IP-адресов, сообщения электронной почты из некоторых доменов могут быть отклонены. Если вы используете резервный MX-сервер, вы должны добавить для всех внешних почтовых доменов его IP-адрес, с которого резервный MX-сервер переадресует сообщения электронной почты на ваш основной почтовый сервер.

Чтобы настроить фильтрацию антиспуфинга, выполните действия, описанные ниже:

1. Нажмите на флажок **Domain IP Check (Antispoofing)**, чтобы включить фильтр.
2. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.
3. Введите домен электронной почты в соответствующем поле.
4. Укажите диапазон доверенных IP-адресов, которые будут использоваться для ранее указанного домена, используя формат CIDR (IP/маска сети).
5. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. IP-адреса будут добавлены в таблицу.
6. Чтобы удалить диапазон IP-адресов из списка, нажмите соответствующую кнопку ⊗ **Удалить** в правой части таблицы.
7. Нажмите **Сохранить**. Домен будет добавлен к фильтру.

Чтобы удалить домен электронной почты из фильтра, выберите его в таблице антиспуфинга и нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Защита от вредоносного ПО

Модуль защиты от вредоносных программ защищает почтовые сервера Exchange от всех видов вредоносных угроз (вирусов, троянов, шпионских программ, руткитов, рекламного ПО, и т.д.), путем обнаружения зараженных или подозрительных объектов, попытками их лечения или путем изоляции инфицированных объектов, в соответствии с заданными действиями.

Сканирование на предмет вредоносных программ выполняется на двух уровнях:

- Транспортный уровень
- Хранилище Exchange

Сканирование на транспортном уровне

Bitdefender Endpoint Security Tools интегрируется с почтовыми транспортными агентами для сканирования всего почтового трафика.

По умолчанию, сканирование транспортного уровня включено. Bitdefender Endpoint Security Tools фильтрует трафик электронной почты, и, если требуется,

информирует пользователей о принятых мерах, добавляя текст в тело сообщения электронной почты.

Используйте флажок **Антивирусная фильтрация**, чтобы отключить или повторно включить эту функцию.

Чтобы настроить текст уведомления, нажмите на ссылку **Настройки**. Доступны следующие опции:

- **Добавить нижний колонтитул в отсканированные письма.** Выберите этот флажок, чтобы добавить сообщение в конце отсканированных писем. Чтобы изменить текст по умолчанию, введите ваше сообщение в текстовом поле ниже.
- **Замена текста.** Для писем, вложения которых были удалены или перемещены в карантин, может быть вложен файл-уведомление. Чтобы изменить текст уведомления по умолчанию, введите ваше сообщение в соответствующее текстовое поле.

Фильтрация вредоносного ПО основана на правилах. Каждое сообщение, доставленное почтовому серверу, проверяется на соответствие правилам фильтрации в порядке их приоритета, пока не будет найдено соответствие правилу. Затем почтовое сообщение обрабатывается в соответствии с действиями, заданными этим правилом.

Управление правилами фильтрации

Вы можете просмотреть все существующие правила в таблице вместе с информацией об их приоритетах, статусах и сферах действия. Правила отсортированы по приоритетности и первое правило обладает наивысшим приоритетом.

Любая antimalware-политика имеет правило по умолчанию, которое становится активным, как только включается фильтрация вредоносного ПО. Что вы должны знать о правиле по умолчанию:

- Это правило нельзя скопировать, удалить или отключить.
- Вы можете изменить только параметры сканирования и действия.
- Приоритет у правила по умолчанию всегда самый низкий.

Создание правил

Существуют два варианта создания правил фильтрации:

- Начните с настроек по умолчанию, выполнив следующие действия:
  1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы открыть окно конфигурации.

2. Настройте параметры правила. Для получения подробной информации относительно опций, обратитесь к опциям правил.
3. Нажмите **Сохранить**. Правило будет отображено первым в таблице.

- Используйте клон пользовательского правила в качестве шаблона, выполнив следующие действия:
  1. Выберите из таблицы требуемое правило.
  2. Нажмите кнопку **Скопировать** в верхней части таблицы, чтобы открыть окно конфигурации.
  3. Настройте параметры правила в соответствии с вашими потребностями.
  4. Нажмите **Сохранить**. Правило будет отображено первым в таблице.

Редактирование правил

Для редактирования существующего правила:

1. Нажмите на название правила, чтобы открыть окно конфигурации.
2. Задайте новые значения для опций, которые вы хотите изменить.
3. Нажмите **Сохранить**. Изменения вступят в силу после сохранения политики.

Установка приоритетов правил

Чтобы изменить приоритет правил:

1. Выберите правило, которое будет перемещаться.
2. Используйте кнопки **Вверх** или **Вниз** в верхней части таблицы, чтобы увеличить или уменьшить приоритет правила.

Удаление правил

Вы можете удалить одно или несколько пользовательских правил сразу. Все, что вам нужно сделать, это:

1. Отметьте флажками правила, которые будут удалены.
2. Нажмите кнопку **Удалить** в верхней части таблицы. После удаления правило нельзя восстановить.

Опции правил

Доступны следующие опции:

- **Основное.** В этом разделе вы должны задать имя для правила, иначе вы не сможете сохранить его. Выберите флажок **Активен**, если хотите, чтобы правило вступило в силу после сохранения политики.
- **Область действия правила** Вы можете ограничить применение правил только к определенной подгруппе писем, задав следующие параметры:

- **Применить к (направление).** Выберите направление почтового трафика, к которому будет применяться правило.
- **Отправители.** Вы можете применять правила для любого отправителя или только для определенных отправителей. Для определенного списка отправителей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Просмотрите выбранные группы в таблице справа.
- **Получатель** Вы можете применять правила для любого получателя или только для определенных получателей. Для определенного списка получателей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Вы можете просмотреть выбранные группы в таблице справа.

  Правило применяется если хотя бы один получатель соответствуют вашему выбору. Если вы хотите применять правило только в том случае, если все получатели находятся в выбранных группах, выберите **Выбрать всех получателей**.

  Примечание
  Адреса в полях **Cc** и **Bcc** также считаются в качестве получателей.

  Важно
  Правила, основанные на пользовательских группах, применяются только к серверам с ролями Hub Transport и Mailbox.

- **Параметры** Настройте параметры сканирования для сообщений электронной почты, соответствующих правилу:
  - **Типы отсканированных файлов** Используйте эту опцию, чтобы указать, какие типы файлов вы хотите просканировать. Вы можете сканировать все файлы (независимо от их расширения), только файлы приложений или определенные типы файлов, которые вы считаете опасными. Сканирование всех файлов обеспечивает наилучшую защиту, в то время как сканирование только приложений рекомендуется для быстрого сканирования.

    Примечание
    Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 610).

Если вы хотите сканировать файлы с определенными расширениями, у вас есть два варианта:
  - **Пользовательские расширения**, где вы должны указать только те расширения, которые будут проверяться.
  - **Все файлы, кроме определенных расширений**, где вы должны ввести только те расширения, которые будут пропущены при сканировании.
- **Максимальный размер вложения / тела письма (MB).** Установите этот флажок и введите значение в соответствующем поле, чтобы установить максимально допустимый размер прикрепленного файла или тела сообщения электронной почты, которые будут проверяться.
- **Максимальная глубина архива (уровней).** Установите флажок и выберите максимальную глубину архива из соответствующего поля. Чем ниже уровень глубины, тем выше производительность и ниже степень защиты.
- **Сканирование на наличие потенциально нежелательных приложений(PUA).** Установите этот флажок, чтобы просканировать возможность проникновения вредоносных или нежелательных приложений, таких как программы показа рекламы, которые могут установиться на системах без согласия пользователя, изменить поведение различных программных продуктов и снизить производительность системы.

- **Действия** Вы можете указать различные автоматические действия агента безопасности для файлов, в зависимости от типа обнаружения.

  Тип обнаружения делит файлы на три категории:
  - **Зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ).
  - **Подозрительные файлы.** Эти файлы опредеояются, как подозрительные с помощью эвристического анализа и других технологий Bitdefender. Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные).
  - **Не сканируемые файлы** Эти файлы не могут быть просканированы. Это могут быть файлы защищенные паролем, зашифрованные, перепакованные и другие.

  Для каждого типа обнаружения, вы можете выбрать действия по умолчанию или основные и альтернативные действия, если основные не

выполняются. Хотя это и не рекомендуется, можно изменить эти действия в соответствующих меню. Выберите действие, которое будет принято:

- **Дезинфицировать** Удаляет вредоносный код из инфицированных файлов и восстанавливает исходный файл. В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.
- **Отклонить / удалить письмо.** На серверах с ролью пограничного транспорта (Edge Transport), обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.
- **Удалить файл** Удаляет проблемные вложения без предупреждения. Желательно избегать использование этого действия.
- **Заменить файл.** удаляет проблемные файлы и вставляет текстовый файл, который уведомляет пользователя о принятых мерах.
- **Переместить файл в карантин.** Перемещает обнаруженные файлы в карантин и вставляет текстовый файл, который уведомляет пользователя о принятых мерах. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице **Карантин**.

  Примечание
  Пожалуйста, обратите внимание, что карантин для серверов Exchange требует дополнительное дисковое пространство на разделе, где установлен агент безопасности. Размер карантина зависит от количества хранящихся элементов и их размера.

- **Не предпринимать никаких действий** Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования. По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин.
- По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других

оставшихся правил. Если вы хотите продолжить проверку другими правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

Исключения

Если вы хотите, чтобы определенный трафик электронной почты был проигнорирован любыми правилами фильтрации, вы можете задать исключения из сканирования. Чтобы создать исключение:

1. Раскройте раздел **Исключения для правил защиты от вредоносных программ**.
2. Нажмите кнопку ⊖ **Добавить** в этом разделе на панели инструментов, которая открывает окно конфигурации.
3. Настройте параметры исключения. Для получения подробной информации относительно опций, обратитесь к опциям правил.
4. Нажмите **Сохранить**.

Сканирование хранилища Exchange

Защита Exchange использует службу Exchange Web Services (EWS) компании Microsoft, чтобы сканировать почтовые ящики Exchange и базы данных общих папок. Вы можете настроить модуль защиты от вредоносного ПО для регулярного запуска задач сканирования по запросу нужных баз данных, в соответствии с заданным графиком.

Примечание

- Сканирование по запросу доступно только для серверов Exchange, на которых установлена роль сервера почтовых ящиков (Mailbox).
- Пожалуйста, обратите внимание, что сканирование по запросу увеличивает потребление ресурсов и, в зависимости от опций сканирования и числа проверяемых объектов, может занимать значительное время.

Сканирование по запросу требует учетной записи администратора сервера Exchange (учетной записи службы), чтобы подменять пользователей Exchange и для получения доступа к целевым объектам, для сканирования почтовых ящиков и общих папок пользователей. Рекомендуется создать отдельную учетную запись для этой цели.

Учетная запись администратора Exchange должна соответствовать следующим требованиям:

- Она является членом группы Organization Management (Exchange 2016, 2013 и 2010)
- Она является членом группы Exchange Organization Administrators (Exchange 2007)
- Она имеет выделенный почтовый ящик.

Включение сканирования по запросу

1. В разделе **Сканировать задачи** нажмите на ссылку **Добавить учетные данные**.
2. Введите имя пользователя и пароль учетной записи службы.
3. Если электронная почта отличается от имени пользователя, необходимо также указать адрес электронной почты учетной записи службы.
4. Введите адрес (URL) Exchange Web Services (EWS) если автообнаружение Exchange не работает.

Примечание

- Имя пользователя должно включать имя домена, например, `user@domain` или `domain\user`.
- Не забудьте обновлять учетные данные в Control Center если они были изменены.

Управление задачами сканирования

В таблице задач сканирования отображаются все запланированные задачи и предоставляется информация об их назначении и периодичности.

Для создания задачи сканирования хранилища Exchange:

1. В разделе **Сканировать задачи**, нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы открыть окно конфигурации.
2. Настройте параметры задачи, как описано в следующем разделе.
3. Нажмите **Сохранить**. Задача будет добавлена в список и она вступит в силу сразу после сохранения политики.

Вы можете отредактировать задачу в любое время, нажав на имя задачи.

Чтобы удалить задачу из списка, выберите его и нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Параметры задачи сканирования

Задачи имеют ряд параметров, описание которых вы можете найти ниже:

- **Общее** Введите подходящее имя задачи.

  Примечание
  Вы можете просмотреть имя задачи во временной шкале Bitdefender Endpoint Security Tools.

- **Планировщик.** Используйте параметры планирования для настройки расписания сканирования. Вы можете установить время запуска задачи сканирования каждые несколько часов, дней или недель, начиная с указанной даты и времени. Для больших баз данных задача сканирования может занимать много времени и может повлиять на производительность сервера. В таких случаях вы можете настроить задачу остановки после определенного времени работы.
- **Цель** Выберите контейнеры и объекты, которые будут проверяться. Вы можете выбрать для сканирования: почтовые ящики, общие папки или и то, и другое. Кроме электронной почты, вы можете выбрать для сканирования другие объекты, такие, как **Контакты**, **Задачи**, **Фурнитура** и **Опубликовать элементы**. Кроме того, вы можете установить следующие ограничения на содержимое, которое будет проверяться:
  – Только непрочитанные сообщения
  – Только элементы с вложениями
  – Только новое, полученное в указанный промежуток времени

  Например, вы можете выбрать для сканирования только письма почтовых пользователей, принятые за последние семь дней.

  Выберите флажок **Исключения**, если вы хотите определить исключения при сканировании. Чтобы создать исключение, используйте поля из заголовков таблицы следующим образом:
  1. Выберите тип репозитория из меню.
  2. В зависимости от типа хранилища укажите объекты, которые должны быть исключены:

Тип хранилища	Формат объекта
Почтовый ящик	Адрес электронной почты
Общая папка	Путь к папке, начиная с корня каталога
База данных	Идентификатор базы данных

Примечание
Для получения идентификатора базы данных, используйте команду оболочки Exchange:
```
Get-MailboxDatabase | fl name,identity
```

Вы можете ввести только одну команду за один раз. Если у вас есть несколько объектов одного типа, вы должны задать столько правил, сколько элементов.

3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы сохранить исключение и добавить его в список.

Чтобы удалить правило исключения из списка, нажмите соответствующую кнопку ⊖ **Удалить**.

- **Параметры** Настройте параметры сканирования для сообщений электронной почты, соответствующих правилу:
  - **Типы отсканированных файлов** Используйте эту опцию, чтобы указать, какие типы файлов вы хотите просканировать. Вы можете сканировать все файлы (независимо от их расширения), только файлы приложений или определенные типы файлов, которые вы считаете опасными. Сканирование всех файлов обеспечивает наилучшую защиту, в то время как сканирование только приложений рекомендуется для быстрого сканирования.

    Примечание
    Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 610).

    Если вы хотите сканировать файлы с определенными расширениями, у вас есть два варианта:
    - **Пользовательские расширения**, где вы должны указать только те расширения, которые будут проверяться.
    - **Все файлы, кроме определенных расширений**, где вы должны ввести только те расширения, которые будут пропущены при сканировании.
  - **Максимальный размер вложения / тела письма (MB).** Установите этот флажок и введите значение в соответствующем поле, чтобы установить максимально допустимый размер прикрепленного файла или тела сообщения электронной почты, которые будут проверяться.
  - **Максимальная глубина архива (уровней).** Установите флажок и выберите максимальную глубину архива из соответствующего поля.

Чем ниже уровень глубины, тем выше производительность и ниже степень защиты.

– **Сканирование на наличие потенциально нежелательных приложений(PUA).** Установите этот флажок, чтобы просканировать возможность проникновения вредоносных или нежелательных приложений, таких как программы показа рекламы, которые могут установиться на системах без согласия пользователя, изменить поведение различных программных продуктов и снизить производительность системы.

- **Действия** Вы можете указать различные автоматические действия агента безопасности для файлов, в зависимости от типа обнаружения.

  Тип обнаружения делит файлы на три категории:

  – **Зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ).
  – **Подозрительные файлы.** Эти файлы опредеояются, как подозрительные с помощью эвристического анализа и других технологий Bitdefender. Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные).
  – **Не сканируемые файлы** Эти файлы не могут быть просканированы. Это могут быть файлы защищенные паролем, зашифрованные, перепакованные и другие.

  Для каждого типа обнаружения, вы можете выбрать действия по умолчанию или основные и альтернативные действия, если основные не выполняются. Хотя это и не рекомендуется, можно изменить эти действия в соответствующих меню. Выберите действие, которое будет принято:

  – **Дезинфицировать** Удаляет вредоносный код из инфицированных файлов и восстанавливает исходный файл. В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.
  – **Отклонить/ удалить электронную почту** Электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.

- **Удалить файл** Удаляет проблемные вложения без предупреждения. Желательно избегать использование этого действия.
- **Заменить файл.** удаляет проблемные файлы и вставляет текстовый файл, который уведомляет пользователя о принятых мерах.
- **Переместить файл в карантин.** Перемещает обнаруженные файлы в карантин и вставляет текстовый файл, который уведомляет пользователя о принятых мерах. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице **Карантин**.

  Примечание
  Пожалуйста, обратите внимание, что карантин для серверов Exchange требует дополнительное дисковое пространство на разделе, где установлен агент безопасности. Размер карантина зависит от количества и размера хранящихся писем.

- **Не предпринимать никаких действий** Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования. По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин.
- По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других оставшихся правил. Если вы хотите продолжить проверку другими правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

Антиспам

Модуль антиспама предлагает несколько защитных слоев против спама и фишинга, используя комбинации различных фильтров и механизмов, чтобы определить являются ли письма спамом или нет.

Примечание

- Антиспам-фильтрация доступна для:
  - Exchange Server 2016/2013 с ролями Edge Transport или Mailbox
  - Exchange Server 2010/2007 с ролями Edge Transport или Hub Transport

- Если у вас есть обе роли Edge и Hub в вашей структуре Exchange, рекомендуется включить антиспам-фильтрацию на сервере с ролью Edge Transport.

Фильтрация спама автоматически включена для входящих сообщений электронной почты. Используйте флажок **Антиспамовая фильтрация**, чтобы отключить или повторно включить эту функцию.

Антиспам-фильтры

Электронная почта проверяется на соответствие правилам фильтрации спама на основе групп отправителей и получателей, в порядке приоритета, до совпадения правила. Затем электронная почта обрабатывается в соответствии с параметрами правил и действия применяются над обнаруженным спамом.

Некоторые антиспам-фильтры настраиваются и вы можете контролировать их использование. Список дополнительных фильтров:

- **Charset Filter.** Многие спам-письма написаны на кириллице или иероглифами. Фильтр кодировки определяет подобные сообщения и отмечает их как SPAM.
- **Sexually Explicit Tagged Content.** Спам, который содержит информацию сексуального характера, будет содержать предупреждение SEXUALLY-EXPLICIT: в строке темы. Этот фильтр обнаруживает письма, помеченные как SEXUALLY-EXPLICIT: в строке темы, и помечает их как спам.
- **URL Filter.** Практически все спам-сообщения содержат ссылки на различные ресурсы. Как правило, эти ресурсы содержат еще больше рекламы и предлагают возможность купить вещи. Иногда они также используются для фишинга.

  Bitdefender имеет базу данных подобных ссылок. Фильтр URL-адреса сверяет каждую ссылку в сообщениях электронной почты с этой базой данных. Если обнаружено совпадение, сообщение помечается как спам.
- **Realtime Blackhole List (RBL).** Этот фильтр позволяет проверять почтовый сервер отправителя на сторонних RBL-серверах. Фильтр использует протокол DNSBL и серверы RBL для фильтрации спама на основе репутации почтовых серверов отправителей спама.

  Адрес почтового сервера извлекается из заголовка электронной почты и проверяется его достоверность. Если адрес принадлежит частному классу

(10.0.0.0, 172.16.0.0 до 172.31.0.0 или 192.168.0.0 до 192.168.255.0), он игнорируется.

Проверка DNS выполняется в домене d.c.b.a.rbl.example.com, где d.c.b.a это обратный IP-адрес сервера и rbl.example.com это сервер RBL. Если DNS-сервер отвечает, что домен является действительным, значит IP-адрес указан на сервере RBL и серверу присваивается определенный рейтинг. Этот рейтинг колеблется между 0 и 100, в зависимости от уровня доверия, который присваивается серверу.

Запрос отправляется для каждого RBL-сервера списком, и рейтинг, возвращаемый каждым из этих серверов, добавляется к промежуточному рейтингу. Когда рейтинг достигает 100, запросы больше не выполняются.

Если оценка RBL-фильтра 100 или выше, электронная почта считается спамом и применяются соответствующие меры. В противном случае, оценка спама вычисляется из результата RBL-фильтра и добавляется к глобальной спам-оценке электронной почты.

- **Heuristic Filter.** Разработанный Bitdefender, эвристический фильтр обнаруживает новые и неизвестные спам-угрозы. Фильтр автоматически обучается на больших объемах спама внутри антиспам-лаборатории Bitdefender. Во время обучения он учится различать спам и легитимные сообщения, распозновать новый спам на основе очень тонкого сходства, используя уже рассмотреную электронную почту. Этот фильтр предназначен для улучшения обнаружения спама на основаннии сигнатур при очень низком количестве ложных срабатываний.
- **BitdefenderОблачный запрос.** Bitdefender поддерживает постоянно развивающуюся базу данных "отпечатков" спам-почты в облаке. Запросы, содержащие характерные признаки, отправляются на облачные серверы и мгновенно проверяются, являются ли эти сообщения спамом. Даже если характерные признаки не найдены в базе данных, они сверяются с другими недавно полученными запросами, и при выполнении определенных условий, электронное сообщение может быть помечено как спам.

Управление правилами антиспама

Вы можете просмотреть все существующие правила в таблице вместе с информацией об их приоритетах, статусах и сферах действия. Правила отсортированы по приоритетности и первое правило обладает наивысшим приоритетом.

Любая антиспам-политика имеет правило по умолчанию, которое становится активным, как только включается антиспам-фильтрация. Что вы должны знать о правиле по умолчанию:

- Это правило нельзя скопировать, удалить или отключить.
- Вы можете изменить только параметры сканирования и действия.
- Приоритет у правила по умолчанию всегда самый низкий.

Создание правил

Чтобы создать правило:

1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы открыть окно конфигурации.
2. Настройте параметры правила. Для получения подробной информации относительно опций, обратитесь к «Опции правил» (p. 399).
3. Нажмите **Сохранить**. Правило будет отображено первым в таблице.

Редактирование правил

Для редактирования существующего правила:

1. Нажмите на название правила, чтобы открыть окно конфигурации.
2. Задайте новые значения для опций, которые вы хотите изменить.
3. Нажмите **Сохранить**. Изменения вступят в силу сразу после сохранения политики.

Установка приоритетов правил

Чтобы изменить приоритет правил, выберите правило, которое вы хотите изменить, и используйте стрелки ⊙ **Вверх** и ⊙ **Вниз** в верхней части таблицы. Вы можете переместить только одно правило за один раз.

Удаление правил

Если вы не хотите больше использовать правило, выберите правило и нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Опции правил

Доступны следующие опции:

- **Основное.** В этом разделе вы должны задать имя для правила, иначе вы не сможете сохранить его. Выберите флажок **Активен**, если хотите, чтобы правило вступило в силу после сохранения политики.
- **Область действия правила** Вы можете ограничить применение правил только к определенной подгруппе писем, задав следующие параметры:
  - **Применить к (направление).** Выберите направление почтового трафика, к которому будет применяться правило.

– **Отправители.** Вы можете применять правила для любого отправителя или только для определенных отправителей. Для определенного списка отправителей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Просмотрите выбранные группы в таблице справа.
– **Получатель** Вы можете применять правила для любого получателя или только для определенных получателей. Для определенного списка получателей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Вы можете просмотреть выбранные группы в таблице справа.

  Правило применяется если хотя бы один получатель соответствуют вашему выбору. Если вы хотите применять правило только в том случае, если все получатели находятся в выбранных группах, выберите **Выбрать всех получателей**.

  Примечание
  Адреса в полях **Cc** и **Bcc** также считаются в качестве получателей.

  Важно
  Правила, основанные на пользовательских группах, применяются только к серверам с ролями Hub Transport и Mailbox.

- **Настройки.** Выберите уровень безопасности, который лучше всего соответствует вашим потребностям (**Интенсивный**, **Нормальный** или **Рекомендуемый**) Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

  Кроме того, вы можете включить различные фильтры. Для получения более подробной информации об этих фильтрах, обратитесь к «Антиспам-фильтры» (p. 397).

  Важно
  RBL фильтр требует дополнительных настроек. Вы можете настроить фильтр после создания или редактирования правила. Для получения более подробной информации, обратитесь к«Настройка фильтра RBL» (p. 402)

  Для соединений, прошедших проверку подлинности, вы также можете выбрать сканированировать функцией антиспама или нет.
- **Действия.** Есть несколько действий, которые вы можете применить при обнаружении писем. Каждое действие, в свою очередь, имеет несколько

возможных вариантов или вторичных действий. Их описание приведено ниже:

Основные действия:

- **Доставить электронную почту.** Спам-почта будет достигать почтовых ящиков получателей.
- **Карантинная электронная почта** Электронная почта будет зашифрована и сохранена в папке карантина на сервере Exchange и не будет доставлена получателям. Вы можете управлять помещенной в карантин электронной почтой на странице **Карантин**.
- **Перенаправить письмо на.** Почта не будет доставлена оригинальному получателю, но будет доставлена на адрес, указанный в соответствующем поле.
- **Отклонить / удалить письмо.** На серверах с ролью пограничного транспорта (Edge Transport), обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.

Вторичные действия:

- **Интеграция с Exchange SCL.** Добавляет заголовок к спаму, позволяя серверу Exchange или Microsoft Outlook осуществлять действия в соответствии с механизмом - Уровень доверия спаму (SCL).
- **Отметьте тему письма как.** Вы можете добавить метку в тему письма, чтобы помочь пользователям фильтровать письма, обнаруженные в почтовом клиенте.
- **Добавить заголовок письма.** Добавляет заголовок к электронной почте, определенной как спам. Вы можете изменить имя заголовка и содержание, введя необходимые значения в соответствующих полях. Кроме того, вы можете использовать этот заголовок электронной почты, чтобы создать дополнительные фильтры.
- **Сохранить письмо на диск.** Копия спама сохраняется в виде файла в указанную папку. Укажите абсолютный путь к папке в соответствующем поле.

Примечание
Эта опция поддерживает только электронные письма в формате MIME.

  - **Архив к аккаунту** Копия обнаруженной электронной почты доставляется по указанному адресу электронной почты. Это действие добавляет указанный адрес электронной почты в СК (Bcc) список адресов электронной почты.
- По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других оставшихся правил. Если вы хотите продолжить проверку другими правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

Настройка фильтра RBL

Если вы хотите использовать фильтр RBL, вы должны указать список серверов RBL.

Чтобы настроить фильтр:

1. На странице **Антиспам**, нажмите на ссылку **Настройки**, чтобы открыть окно конфигурации.
2. Укажите в соответствующих полях IP-адрес DNS-сервера для отправки запроса, а также интервал тайм-аута для запроса. Если адрес DNS-сервера не настроен или DNS-сервер недоступен, фильтр RBL использует DNS-серверы системы.
3. Для каждого сервера RBL:
   a. Введите имя сервера или IP-адрес и уровень доверия, назначенный серверу, в полях заголовка таблицы.
   b. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.
4. Нажмите **Сохранить**.

Настройка белого списка отправителей

Вы можете снизить потребление ресурсов сервера, добавив известных отправителей электронной почты в списки надежных или ненадежных отправителей. Таким образом, почтовый сервер всегда будет принимать или отклонять письма, поступающие от этих отправителей. Например, у вас есть интенсивные связи по электронной почте с бизнес-партнером и чтобы быть уверенным, что вы получите все письма от него, вы можете добавить партнера в белый список.

Чтобы построить белый список надежных отправителей:

1. Нажмите ссылку **Белый список**, чтобы открыть окно конфигурации.
2. Выберите флажок **Отправитель Белый список**.

3. Введите адреса электронной почты в соответствующем поле. При редактировании списка вы также можете использовать специальные символы, чтобы задать домен или шаблон для адресов входящей электронной почты:
   - Звездочка (*) заменяет ноль, один или более символов.
   - Вопросительный знак (?) заменяет один любой символ.

   Например, если вы введете `*.gov`, все письма, поступающие от домена `.gov`, будут приняты.
4. Нажмите **Сохранить**.

Примечание
Используйте опцию **Черный список подключений** из раздела **безопасность электронной почты > Основное > Настройки**, чтобы добавить известных отправителей спама в черный список.

Контроль контента

Используйте модуль управления контентом для усиления защиты электронной почты, отфильтровав весь почтовый трафик, несовместимый с политикой компании (нежелательный или потенциально опасный).

Для общего контроля содержимого электронной почты, модуль включает в себя два варианта фильтрации электронной почты:

- Фильтрацию контента
- Фильтрацию вложений

Примечание
Фильтрация контента и Фильтрация вложений доступна для:
- Exchange Server 2016/2013 с ролями Edge Transport или Mailbox
- Exchange Server 2010/2007 с ролями Edge Transport или Hub Transport

Управление правилами фильтрации

Фильтры управления контентом основаны на правилах. Вы можете задать различные правила для различных пользователей и групп пользователей. Каждое сообщение, достигающее почтового сервера, сверяется с правилами фильтрации в порядке приоритета, пока не будет найдено соответствие

правилу. Затем почтовое сообщение обрабатывается в соответствии с действиями, заданными этим правилом.

Правила фильтрации содержимого предшествует правилам фильтрации вложений.

Правила фильтрации контента и вложений расположены в соответствующих таблицах, упорядоченных по приоритету, и первое правило имеет наивысший приоритет. Для каждого правила отображается следующая информация:

- Приоритет
- Имя
- Направление трафика
- Группы отправителей и получателей

Создание правил

Существуют два варианта создания правил фильтрации:

- Начните с настроек по умолчанию, выполнив следующие действия:
  1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы открыть окно конфигурации.
  2. Настройте параметры правила. Для получения подробной информации об опциях фильтрации конкретного контента и вложения, обратитесь к:
     – Опции правил фильтрации контента
     – Опции правил фильтрации вложений.
  3. Нажмите **Сохранить**. Правило будет отображено первым в таблице.
- Используйте клон пользовательского правила в качестве шаблона, выполнив следующие действия:
  1. Выберите нужное правило из таблицы.
  2. Нажмите кнопку **Скопировать** в верхней части таблицы, чтобы открыть окно конфигурации.
  3. Настройте параметры правил в соответствии с вашими потребностями.
  4. Нажмите **Сохранить**. Правило будет отображено первым в таблице.

Редактирование правил

Для редактирования существующего правила:

1. Нажмите на название правила, чтобы открыть окно конфигурации.
2. Задайте новые значения для опций, которые вы хотите изменить.
3. Нажмите **Сохранить**. Изменения вступят в силу после сохранения политики.

Установка приоритетов правил

Чтобы изменить приоритет правил:

1. Выберите правило, которое будет перемещаться.
2. Используйте кнопки **Вверх** или **Вниз** в верхней части таблицы, чтобы увеличить или уменьшить приоритет правила.

Удаление правил

Вы можете удалить одно или несколько пользовательских правил одновременно. Все, что вам нужно сделать, это:

1. Выберите правило, которое будет удалено.
2. Нажмите кнопку **Удалить** в верхней части таблицы. После удаления правило нельзя восстановить.

Фильтрация контента

Фильтрация контента позволяет фильтровать почтовый трафик на основе символьных строк, которые вы определили ранее. Эти строки сравниваются с темой письма или текстовым содержимым тела электронного письма. Фильтрация контента выполняет следующие задачи:

- Предотвращает поступление нежелательного содержимого электронной почты в почтовые ящики серверов Exchange.
- Блокирует исходящие сообщения электронной почты, содержащие данные конфиденциального характера.
- Архивирует электронную почту, удовлетворяющую заданным условиям, и доставляет ее на другой аккаунт электронной почты или сохраняет на диск. Например, вы можете сохранить письма, отправленные на адрес электронной почты поддержки вашей компании в папку на локальном диске.

Включение фильтрации контента

Если вы хотите использовать фильтрацию контента, выберите флажок **Контентная фильтрация**.

Для создания и управления правилами фильтрации контента, обратитесь к «Управление правилами фильтрации» (p. 403).

Опции правил

- **Основное.** В этом разделе вы должны задать имя для правила, иначе вы не сможете сохранить его. Выберите флажок **Активен**, если хотите, чтобы правило вступило в силу после сохранения политики.

- **Область действия правила** Вы можете ограничить применение правил только к определенной подгруппе писем, задав следующие параметры:
  - **Применить к (направление).** Выберите направление почтового трафика, к которому будет применяться правило.
  - **Отправители.** Вы можете применять правила для любого отправителя или только для определенных отправителей. Для определенного списка отправителей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Просмотрите выбранные группы в таблице справа.
  - **Получатель** Вы можете применять правила для любого получателя или только для определенных получателей. Для определенного списка получателей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Вы можете просмотреть выбранные группы в таблице справа.

    Правило применяется если хотя бы один получатель соответствуют вашему выбору. Если вы хотите применять правило только в том случае, если все получатели находятся в выбранных группах, выберите **Выбрать всех получателей**.

    Примечание
    Адреса в полях **Cc** и **Bcc** также считаются в качестве получателей.

    Важно
    Правила, основанные на пользовательских группах, применяются только к серверам с ролями Hub Transport и Mailbox.

- **Настройки.** Настройте выражения для поиска в сообщениях электронной почты, как описано ниже:
  1. Выберите часть электронной почты, которая должна быть проверена:
     - Тема электронной почты, отметив флажок проверки **Фильтровать по теме**. Все письма, которые содержат любое из выражений, введенное в соответствующей таблице, будут отфильтрованы.
     - Тело письма, выбрав флажок **Фильтровать по содержанию тела**. Все письма, которые содержат в теле письма любое из заданных выражений, будут отфильтрованы.
     - И тема, и тело письма, отметив оба флажка. Все письма, тема которых соответствует любому правилу из первой таблицы и тело письма, содержащее любое выражение из второй таблицы, будут отфильтрованы. Например:

Первая таблица содержит выражения: `Новостная рассылка` и `Еженедельный`. Вторая таблица содержит выражения: `Покупки`, `Цена` и `Предложение`.

Письмо с темой "Ежемесячное **новостная рассылка** от вашего любимого продавца часов" и телом письма, содержащим фразу "Мы рады представить вам наши новинки **Предложения** содержащие сенсационные часы в неотразимой **Ценой**.", совпадет с правилами и письмо будет отфильтровано. Если тема письма содержит "Новости от вашего продавца часов", электронное письмо не будет отфильтровано.

2. Создайте списки условий, используя поля в заголовках таблицы. Для каждого условия выполните следующие действия:
   a. Выберите тип выражения, которое будет использовано в поиске. Вы можете ввести точный текст или построить текстовые шаблоны с использованием регулярных выражений.

      Примечание
      Синтаксис регулярных выражений соответствует грамматике ECMAScript.

   b. Введите строку для поиска в поле **Expression**.

      Например:

      i. Выражение `5[1-5]\d{2}([\s\-]?\d{4}){3}` соответствует банковским картам с номерами, которые начинаются с цифр от 51 до 55, состоят из шестнадцати цифр в группах по четыре и группы могут разделяться пробелом или тире. Таким образом, любое письмо, содержащее номер карты в одном из следующих форматов: `5257-4938-3957-3948`, `5257 4938 3957 3948` или `5257493839573948`, будет отфильтровано.

      ii. Это выражение обнаруживает письма со словами `Лотерея`, `Наличные` и `награда`, найденными в этом порядке:

```
(lottery)((.|\n|\r)*)( cash)((.|\n|\r)*)( prize)
```

Чтобы обнаружить электронные письма, содержащие каждое из трех слов независимо от их порядка следования, добавьте три регулярных выражения с разным порядком слов.

iii. Это выражение обнаруживает электронные письма, которые включают три и более вхождений слова `Награда`:

```
(prize)((.|\n|\r)*)( prize)((.|\n|\r)*)( prize)
```

c. Если вы хотите дифференцировать заглавные и маленькие буквы в письме при сравнении текста, выберите флажок **Учитывать регистр**. Например, если отметить этот флажок, то `новостная рассылка` и `новостная рассылка` будут разными словами.

d. Если вы не хотите, чтобы выражение было частью других слов, выберите флажок **Целый мир**. Например, с выбранным флажком, выражение `Зарплата Анны` не будет совпадать с `Зарплата Марианы`.

e. Нажмите кнопку ⊕ **Добавить** в заголовке столбца **Действие**, чтобы добавить условие в список.

- **Действия.** Есть несколько действий, которые могут быть предприняты при обнаружении писем. Каждое действие, в свою очередь, имеет несколько возможных вариантов или вторичных действий. Их описание приведено ниже:

  Основные действия:

  – **Добавить электронную почту.** Обнаруженная электронная почта будет доставлена в почтовые ящики получателей.
  – **Карантин.** Электронная почта будет зашифрована, сохранена в папке карантина на сервере Exchange и не будет доставлена получателям. Вы можете управлять помещенной в карантин электронной почтой на странице **Карантин**.
  – **Отклонить.** Почта не будет доставлена оригинальным получателям, но будет доставлена на адрес, указанный в соответствующем поле.
  – **Отклонить / удалить письмо.** На серверах с ролью пограничного транспорта (Edge Transport), обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.

Вторичные действия:

- **Отметьте тему письма как** Вы можете добавить метку в тему письма, чтобы помочь пользователям отфильтровать обнаруженые письма в почтовом клиенте.
- **Добавьте заголовок к сообщениям электронной почты.** Вы можете добавить сообщению заголовок и значение обнаруженной почте, набрав желаемые значения в соответствующем поле.
- **Сохранить почту на диск.** Копия обнаруженной электронной почты сохраняется в виде файла в специальной папке на сервере Exchange. Если папка на сервере не существует, то она будет создана. Укажите абсолютный путь к папке в соответствующем поле.

  Примечание
  Эта опция поддерживает только электронные письма в формате MIME.

- **Архив к аккаунту** Копия обнаруженной электронной почты доставляется по указанному адресу электронной почты. Это действие добавляет указанный адрес электронной почты в CK (Bcc) список адресов электронной почты.

- По умолчанию, если сообщение соответствует условиям одного правила, его дальнейшая проверка на соответствие другим правилам не производится. Чтобы продолжить обработку другими правилами, снимите флажок **Если условия правила совпадают, прекратите обработку большего количества правил**.

Исключения

Если вы хотите, чтобы почтовый трафик для определенных отправителей или получателей доставлялся с любыми вложениями, вне зависимости от правил фильтрации, вы можете задать исключения в фильтрах.

Чтобы создать исключение:

1. Нажмите ссылку **Исключения** рядом с флажком **Фильтрация контента**. Это действие откроет окно конфигурации.
2. Введите адреса электронной почты доверенных отправителей и/или получателей в соответствующих полях. Любое письмо, приходящее от доверенного отправителя или отправляющееся доверенному получателю, будет исключено из фильтрации. При редактировании списка вы также

можете использовать специальные символы, чтобы задать домен или шаблон для адресов входящей электронной почты:
- Звездочка (*) заменяет ноль, один или более символов.
- Вопросительный знак (?) заменяет один любой символ.

Например, если вы введете `*.gov`, все письма, поступающие от домена `.gov`, будут приняты.

3. Для писем с несколькими получателями, можно выбрать флажок **Исключить электронную почту из фильтрации, только если все получатели являются доверенными**, чтобы применять исключение, только если все получатели электронной почты присутствуют в списке доверенных.
4. Нажмите **Сохранить**.

Фильтрация вложений

Модуль фильтрации вложений предоставляет функции фильтрации вложений электронной почты. Он может обнаружить вложения с определенными шаблонами имен или определенного типа. С помощью фильтрации вложений вы можете:

- Блокировать потенциально опасные вложения, такие как `.vbs` или `.exe` файлы или письма содержащие их.
- Блокировать вложения, имеющие оскорбительные выражения или электронные письма содержащие их.

Включение фильтрации вложений

Если вы хотите использовать фильтрацию содержимого, выберите флажок **Фильтрация вложений**.

Для создания и управления правилами фильтрации содержимого, обратитесь к «Управление правилами фильтрации» (p. 403).

Опции правил

- **Основное.** В этом разделе вы должны задать имя для правила, иначе вы не сможете сохранить его. Выберите флажок **Активен**, если хотите, чтобы правило вступило в силу после сохранения политики.
- **Область действия правила** Вы можете ограничить применение правил только к определенной подгруппе писем, задав следующие параметры:
  - **Применить к (направление).** Выберите направление почтового трафика, к которому будет применяться правило.

- **Отправители.** Вы можете применять правила для любого отправителя или только для определенных отправителей. Для определенного списка отправителей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Просмотрите выбранные группы в таблице справа.
- **Получатель** Вы можете применять правила для любого получателя или только для определенных получателей. Для определенного списка получателей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Вы можете просмотреть выбранные группы в таблице справа.

  Правило применяется если хотя бы один получатель соответствуют вашему выбору. Если вы хотите применять правило только в том случае, если все получатели находятся в выбранных группах, выберите **Выбрать всех получателей**.

  Примечание
  Адреса в полях **Cc** и **Bcc** также считаются в качестве получателей.

  Важно
  Правила, основанные на пользовательских группах, применяются только к серверам с ролями Hub Transport и Mailbox.

- **Настройки.** Перечислите файлы, которые разрешены или запрещены во вложениях электронной почты.

  Вы можете фильтровать вложения электронной почты по типу или по имени файла.

  Чтобы отфильтровать вложения по типу файла, выполните следующие действия:
  1. Выберите флажок **Определить по типу контента**.
  2. Выберите опцию обнаружения, которая больше всего подходит для ваших потребностей:
     - **Only the following categories**, когда у вас есть ограниченный перечень запрещенных типов файлов.
     - **Все, кроме следующих категорий**, когда у вас есть ограниченный перечень разрешенных типов файлов.
  3. Выберите интересующие вас категории типов файлов из списка доступных. Для получения подробной информации о расширениях каждой категории, обратитесь к «Фильтрация вложений по типу файлов» (p. 611).

Если вам необходимы только некоторые конкретные типы файлов, выберите флажок **Пользовательские расширения** и введите список расширений в соответствующем поле.

4. Выберите флажок **Включить определение истинного типа**, чтобы проверять заголовки файлов и правильно определять тип файла вложения при сканировании запрещенных расширений. Это означает, что расширение не может быть просто переименовано для обхода политики фильтрации вложений.

Примечание
Точное определение типа может быть ресурсоемким.

Чтобы отфильтровать вложения по имени, выберите флажок **Detect by Filename** и введите имена файлов, которые вы хотите отфильтровать, в соответствующем поле. При редактировании списка вы также можете использовать специальные символы, чтобы задать шаблоны:

– Звездочка (*) заменяет ноль, один или более символов.
– Вопросительный знак (?) заменяет один любой символ.

Например, если вы введете `database.*`, все файлы с именем `database`, независимо от их расширения, будут обнаружены.

Примечание
Если вы включите и определение типа содержимого, и имя файла (без точного определения типа), файл должен одновременно удовлетворять обоим условиям одновременно. Например, вы выбрали категорию **Мультимедиа** и ввели имя файла `test.pdf`. В этом случае любое письмо будет пропущено правилом, потому что файл PDF не является мультимедийным файлом.

Выберите флажок **Сканирование внутри архивов**, чтобы предотвратить сокрытие заблокированных файлов в простых архивах, таким образом обходя правило фильтрации.

Рекурсивное сканирование ведется внутри архивов и по умолчанию осуществляется до четвертого уровня глубины архива. Вы можете оптимизировать проверку, как описано ниже:

1. Выберите флажок **Максимальная глубина архива (уровни)**.

2. Выберите другое значение из соответствующего меню. Для лучшей производительности выберите наименьшее значение, для максимальной защиты выберите наибольшее значение.

Примечание
Если вы выбрали опцию **Сканирование внутри архивов**, проверяться будут все архивы.

- **Действия.** Есть несколько действий, которые вы можете предпринять при обнаружении вложений или электронной почты, содержащую их. Каждое действие, в свою очередь, имеет несколько возможных вариантов или вторичных действий. Их описание приведено ниже:

  Основные действия:
  - **Заменить файл.** Удаляет обнаруженные файлы и вставляет текстовый файл, который уведомляет пользователя о совершенных действиях.

    Чтобы настроить текст уведомлений:
    1. Нажмите **Настройки** рядом с флажком **Attachment filtering**.
    2. Введите текст уведомления в соответствующем поле.
    3. Нажмите **Сохранить**.
  - **Удалить файл.** Удаляет обнаруженные файлы без предупреждения. Желательно избегать использование этого действия.
  - **Отменить/Удалить электронную почту.** На серверах с ролью пограничного транспорта (Edge Transport) обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.
  - **Карантинная электронная почта** Электронная почта будет зашифрована и сохранена в папке карантина на сервере Exchange и не будет доставлена получателям. Вы можете управлять помещенной в карантин электронной почтой на странице **Карантин**.
  - **Перенаправить письмо на.** Почта не будет доставлена оригинальному получателю, но будет доставлена на адрес указанный в соответствующем поле.
  - **Доставить электронную почту.** Позволяет проходить электронной почте.

Вторичные действия:

- **Отметьте тему письма как** Вы можете добавить метку в тему письма, чтобы помочь пользователям отфильтровать обнаруженые письма в почтовом клиенте.
- **Добавьте заголовок электронной почты..** Вы можете добавить сообщению заголовок и значение обнаруженной почте, набрав желаемые значения в соответствующем поле.
- **Сохранить письмо на диск.** Копия обнаруженной электронной почты сохраняется в виде файла в специальной папке на сервере Exchange. Если папка на сервере не существует, то она будет создана. Укажите абсолютный путь к папке в соответствующем поле.

  Примечание
  Эта опция поддерживает только электронные письма в формате MIME.

- **Архив к аккаунту** Копия обнаруженной электронной почты доставляется по указанному адресу электронной почты. Это действие добавляет указанный адрес электронной почты в СК (Bcc) список адресов электронной почты.

- По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других оставшихся правил. Если вы хотите продолжить проверку другими правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

Исключения

Если вы хотите, чтобы почтовый трафик для определенных отправителей или получателей доставлялся с любыми вложениями, вне зависимости от правил фильтрации, вы можете задать исключения в фильтрах.

Чтобы создать исключение:

1. Нажмите **Исключния** рядом с флажком **Фильтрация вложений**. Это действие откроет окно конфигурации.
2. Введите адреса электронной почты доверенных отправителей и/или получателей в соответствующих полях. Любое письмо, приходящее от доверенного отправителя или отправляющееся доверенному получателю, будет исключено из фильтрации. При редактировании списка вы также

можете использовать специальные символы, чтобы задать домен или шаблон для адресов входящей электронной почты:
- Звездочка (*) заменяет ноль, один или более символов.
- Вопросительный знак (?) заменяет один любой символ.

Например, если вы введете `*.gov`, все письма, поступающие от домена `.gov`, будут приняты.

3. Для писем с несколькими получателями, можно выбрать флажок **Исключить электронную почту из фильтрации, только если все получатели являются доверенными**, чтобы применять исключение, только если все получатели электронной почты присутствуют в списке доверенных.
4. Нажмите **Сохранить**.

7.2.12. Шифрование

Примечание
Данный модуль доступен для:
- Windows для рабочих станций
- Windows для серверов
- ОС MAK

Модуль Encryption управляет полным шифрованием диска на конечных точках, используя BitLocker в Windows и FileVault и утилиту командной строки diskutil в macOS, соответственно.

При таком подходе GravityZone может обеспечить некоторые постоянные преимущества:

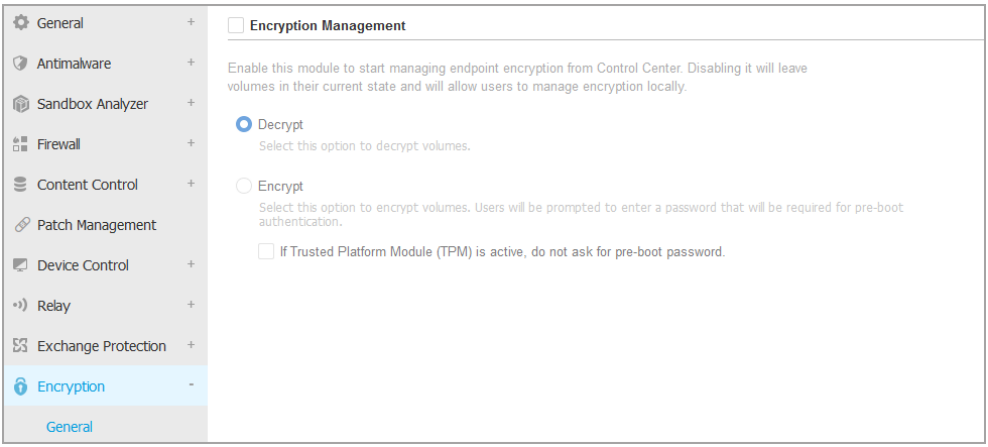
- Данные защищены в случае утери или кражи устройства.
- Обширная защита для самых популярных компьютерных платформ в мире, благодаря использованию рекомендуемых стандартов шифрования с полной поддержкой Microsoft и Apple.
- Минимальное влияние на производительность конечных точек благодаря встроенным средствам шифрования.

Модуль шифрования использует следующие решения:

- BitLocker версии 1. 2 и позднее на конечных точках Windows с доверенным платформенным модулем (TPM) для загрузочных и незагрузочных томов.

- BitLocker версии 1. 2 и позднее на конечных точках Windows без TPM для загрузочных и незагрузочных томов.
- FileVault на конечных точках macOS, для загрузочных томов.
- diskutil на конечных точках macOS, для незагрузочных томов.

Список операционных систем, поддерживаемых модулем шифрования, см. в Руководстве по установке GravityZone.



Страница шифрования

Чтобы начать управление шифрованием конечной точки из Control Center, установите флажок **Управление шифрованием** . Пока этот параметр включен, пользователи конечных точек не могут управлять шифрованием локально, а все их действия будут отменены. Отключение этого параметра оставит тома конечной точки в их текущем состоянии (зашифрованном или незашифрованном), и пользователи смогут управлять шифрованием на своих компьютерах.

Для управления процессами шифрования и дешифрования доступны три варианта:

- **Расшифровать** - расшифровывает тома и сохраняет их незашифрованными, когда политика активна на конечных точках.
- **Шифровать** - шифрует тома и сохраняет их в зашифрованном виде, когда политика активна на конечных точках.

В разделе «Шифрование» можно установить флажок **Если доверенный платформенный модуль (TPM) активен, не запрашивать пароль для шифрования** . Этот параметр обеспечивает шифрование на конечных точках Windows с TPM, не требуя пароль шифрования от пользователей. Подробнее см: «Шифрование томов» (p. 417).

- **Исключения**

GravityZone поддерживает метод шифрования Advanced Encryption Standard (AES) с 128 и 256-битными ключами в Windows и macOS. Фактический алгоритм шифрования зависит от конфигурации каждой операционной системы.

Примечание
GravityZone обнаруживает и управляет томами, зашифрованными вручную, с помощью BitLocker, FileVault и diskutil. Для того, чтобы начать управлять этими томами, агент безопасности предложит пользователям конечных точек изменить свои ключи восстановления. В случае использования других решений для шифрования, тома должны быть расшифрованы перед применением политики GravityZone.

Шифрование томов

Чтобы зашифровать тома:

1. Установите флажок **Управление шифрованием** .
2. Выберите опцию **Шифрование** .

Процесс шифрования начинается после того, как политика становится активной на конечных точках, с некоторыми особенностями в Windows и Mac.

Для Windows

По умолчанию агент безопасности предложит пользователям настроить пароль для запуска шифрования. Если на машине установлен функциональный TPM, агент безопасности предложит пользователям настроить персональный идентификационный номер (PIN) для начала шифрования. На экране предварительной загрузки и проверки подлинности пользователи должны вводить пароль или ПИН-код, настроенные на этом этапе, каждый раз, когда запускается конечная точка.

Примечание
Агент безопасности позволяет настраивать требования к сложности ПИН-кода, а также привилегии пользователей на изменение их ПИН-кода с помощью параметров групповой политики BitLocker (GPO).

Чтобы запустить шифрование без ввода пароля от пользователей конечной точки, установите флажок **Если модуль доверенной платформы (TPM) активен, не запрашивать пароль перед загрузкой** Этот параметр совместим с конечными точками Windows, которые имеют TPM и UEFI.

Когда флажок **Если модуль доверенной платформы (TPM) активен, не запрашивать пароль перед загрузкой** включен:

- На незашифрованной конечной точке:
  - Процесс шифрования без пароля.
  - Экран предварительной загрузки не появляется при запуске машины.
- На конечной точке зашифровано паролем:
  - Пароль удален.
  - Тома остаются зашифрованными
- Зашифрованная или незашифрованная конечная точка с TPM или без TMP не обнаружена или не работает:
  - Пользователю предлагается ввести пароль для шифрования.
  - Экран проверки подлинности перед загрузкой появляется при запуске машины.

Когда флажок **Если модуль доверенной платформы (TPM) активен, не запрашивать пароль перед загрузкой** отключен:

- Пользователь должен ввести пароль для шифрования.
- Тома остаются зашифрованными

На ОС Mac

Для того, чтобы запустить шифрование на загрузочных томах, агент безопасности предложит пользователям ввести свои системные учетные данные. Только пользователи, имеющие локальные учетные записи с правами администратора, могут включить шифрование.

Чтобы запустить шифрование на незагрузочных томах, агент безопасности предложит пользователям настроить пароль шифрования. Этот пароль будет необходим для разблокировки незагружаемого тома при каждом запуске компьютера. Если на компьютере несколько загрузочных томов,

пользователи должны настроить пароль шифрования для каждого из них.

Дешифровка томов

Чтобы дешифровать тома на конечных точках:

1. Установите флажок **Управление шифрованием** .
2. Выберите опцию **Дешифровка** .

Процесс расшифровки начинается после того, как политика становится активной на конечных точках, с некоторыми особенностями в Windows и Mac.

Для Windows
Тома расшифровываются без взаимодействия с пользователями.

На ОС Mac
Для загрузочных томов пользователи должны ввести свои системные учетные данные. Для незагрузочных томов пользователи должны ввести пароль, настроенный во время процесса шифрования.

В случае, если пользователи конечной точки забывают свои пароли шифрования, им нужны ключи восстановления для разблокировки компьютеров. Подробнее о получении ключей восстановления см. «» (p. 115).

Исключение разделов

Вы можете создать список исключений из шифрования, добавив определенные буквы дисков, метки и имена разделов и GUID раздела. Чтобы создать правило для исключения разделов из шифрования:

1. Установите флажок **Исключения**.
2. Нажмите **Тип** и выберите тип диска в выпадающем меню.
3. Введите значение диска в поле **Исключенные элементы** и примите во внимание следующие условия:
   - Чтобы ввести **Букву диска**, введите `D:` или вашу букву диска с двоеточием.
   - Для **Метки/имени** вы можете ввести любую метку, например `Работа`.
   - Для раздела **GUID** введите значение следующим образом: `\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\`.

4. Нажмите **Добавить**⊕, чтобы добавить исключение в список.

Чтобы удалить исключение, выберите и добавьте элемент и нажмите **Удалить** ⊗.

7.2.13. NSX

В этом разделе вы можете установить политику, которая будет использоваться в качестве профиля безопасности в NSX. Для этого:

1. Отметьте флажок **NSX**, чтобы задать его видимость также в веб-клиенте vSphere.
2. Введите ниже имя, по которому вы сможете идентифицировать политику для NSX. Это имя может отличаться от имени политики в GravityZone Control Center. В vSphere оно будет отображаться с префиксом `Bitdefender_`. Выберите это имя продумано, так как оно затем станет доступно только для чтения, после сохранения политики.

7.2.14. Защита хранилища

Примечание
Защита хранилищ доступна для защиты устройств сетевого хранилища (NAS) и систем обмена файлами, совместимых с протоколом адаптации контента Интернета (ICAP).

В данном разделе вы можете настроить Security Server как службу сканирования устройств NAS и систем обмена файлами, совместимых с ICAP, таких как Nutanix Files и Citrix ShareFile.

Security Server сканирует любые файлы, включая архивы, по запросу устройств хранения. В зависимости от настроек Security Server выполняет соответствующие действия с зараженными файлами, например, лечит или запрещает доступ.

Настройки объединены в следующие разделы:

- ICAP
- Исключения

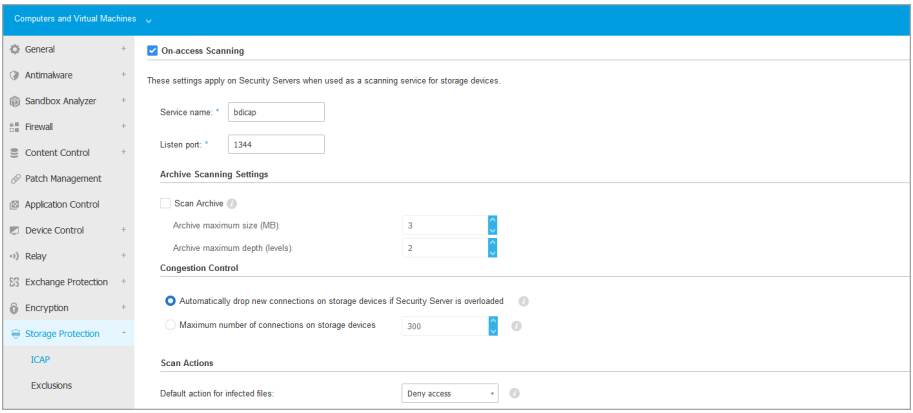
ICAP

Вы можете настроить следующие параметры для Security Server:

- Установите флажок **Сканирование при доступе** , чтобы включить модуль защиты хранилища. Необходимые настройки для связи между Security Server и устройствами хранения предварительно определены следующим образом:
  - Сервисное имя: `bdicap`.
  - Порт прослушивания: `1344`.
- В разделе **Настройки сканирования архива** установите флажок **Сканировать архив** , чтобы включить сканирование архива. Настройте максимальный размер и максимальную глубину сканируемых архивов.

  Примечание
  Если вы установите максимальный размер архива 0 (ноль), Security Server сканирует архивы независимо от их размера.

- В разделе **Контроль перегрузки** выберите предпочтительный способ управления соединениями на устройствах хранения в случае перегрузки Security Server:
  - **Автоматически сбрасывать новые подключения на устройствах хранения, если Security Server перегружен**. Когда один Security Server достиг максимального количества соединений, устройство хранения перенаправит избыток на второй Security Server.
  - **Максимально количество подключений на устройствах хранения**. По умолчанию установлен лимит в 300 подключений.
- В разделе **Действия сканирования** доступны следующие опции:
  - **Отказать в доступе** - Security Server отказывает в доступе зараженным файлам.
  - **Вылечить** - Security Server удаляет вредоносный код из зараженных файлов.



Политика - Защита хранилищ - ICAP

Исключения

Если вы хотите удалить определенные объекты из сканирования, установите флажок **Исключения**.

Вы можете определить исключения:

- По хэш - вы определяете исключаемый файл хэшем SHA-256.
- Подстановочным знаком - вы указываете исключенный файл по пути.

Настройка исключений

Чтобы добавить исключение:

1. Выберите тип исключения из меню.
2. В зависимости от типа исключения, укажите объект, который будет исключен, следующим образом:
   - **Хэш** - введите хэши SHA-256 через запятую.
   - **Подстановочный знак** - уточните абсолютный или относительный путь, используя подстановочные знаки. Символ звездочки (*) соответствует любому файлу в директории. Вопросительный знак (?) соответствует только одному символу.
3. Добавить описание для исключения.
4. Нажмите кнопку ⊕ **Добавить**. Новое исключения будут добавлены в список.

Чтобы удалить правило из списка, нажмите соответствующую кнопку ⊗ **Удалить**.

Импорт и экспорт исключений

Если вы намерены повторно использовать исключения в других политиках, вы можете выбрать их экспорт и импорт.

Чтобы экспортировать исключения:

1. Нажмите **Экспорт** в верхней части таблицы исключений.
2. Сохраните файл CSV на вашем компьютере. В зависимости от настроек вашего браузера, файл может автоматически загрузится или вам будет предложено сохранить его в определенное место.

Каждая строка в CSV-файле соответствует одному исключению, имеющему поля в следующем порядке:

```
<exclusion type>, <object to be excluded>, <description>
```

Доступные значения для полей в файле CSV:

Тип исключения:

`1`, для SHA-256 hash

`2`, для подстановочных

Исключаемый объект:

Хеш-значение или путь

Описание

Текст, помогающий определить исключение.

Пример исключений в файле CSV:

```
2,*/file.txt,text
2,*/image.jpg,image
1,e4b0c44298fc1c19afbf4c8996fb9227ae41e4649b934ca991b7852b855,hash
```

Чтобы импортировать исключения:

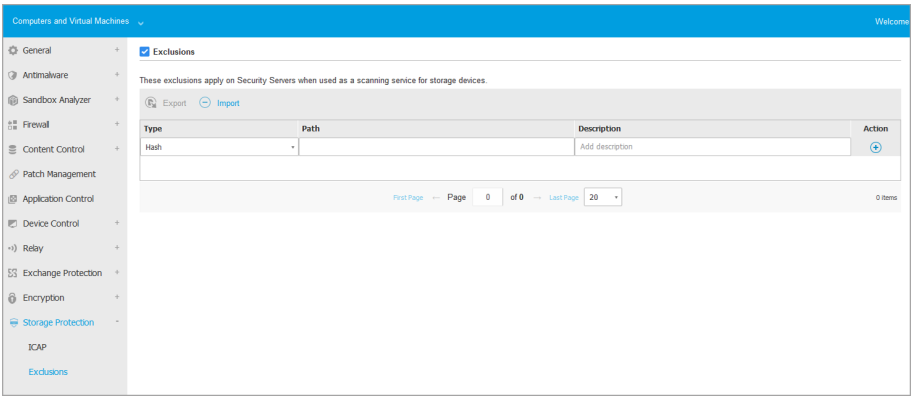
1. Нажмите **Импорт**. Откроется окно **Import Policy Exclusions**.
2. Нажмите **Добавить** и затем выберите файл CSV.

3. Нажмите **Сохранить**. Таблица заполняется корректными исключениями. Если файл CSV содержит недопустимые исключения, предупреждение информирует вас о соответствующих номерах строк.

Редактирование исключений

Чтобы редактировать исключение:

1. Кликните имя исключения в колонке **Путь** или в описании.
2. Редактируйте исключения
3. Нажмите `Выход` когда закончите.

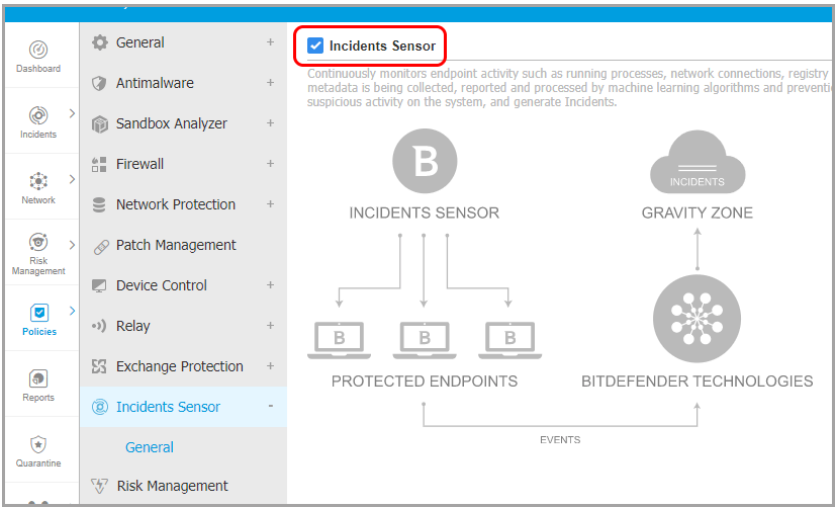


Политика - Защита хранилищ - ICAP

7.2.15. Инциденты Sensor

Постоянный контроль конечных точек, текущих процессов, подключения к сети, изменения реестра. Эти метаданные находятся в процессе сбора, предоставления и обработки при помощи алгоритмов машинного обучения и технологий предотвращения, позволяющих выявить подозрительное поведение.

Проверьте работу датчика инцидентов, чтобы сделать данный модуль доступным.



Инциденты Sensor

7.3. Политики мобильных устройств

Параметры политики можно настроить изначально при ее создании. Позже вы можете изменить их по мере необходимости в любое удобное время.

Чтобы настроить параметры политики:

1. Перейдите на страницу **Политики**.
2. Выберите **Мобильные устройства** из меню видов сетей.
3. Нажмите на имя политики. Откроется страница настройки политики.
4. Настройте необходимые параметры политики. Настройки организованы в следующие категории:
   - Основные
     - Подробная информация
   - Управление устройствами
     - Безопасность
     - Пароль
     - Профили

Вы можете выбрать категорию настроек, используя меню в левой части страницы.

5. Нажмите **Сохранить**, чтобы сохранить изменения и применить их на требуемых мобильных устройствах. Чтобы покинуть страницу политик без сохранения изменений, нажмите **Отменить**.

7.3.1. Основные

Категория **Основные** содержит описательную информацию о выбранной политике.

Подробная информация

На странице с подробной информацией отображаются общие сведения о политике:

- Название политики
- Пользователь, который создал политику
- Дата и время, когда политика была создана
- Дата и время последнего изменения политики

Вы можете переименовать политику, введя новое имя в соответствующем поле. Политики должны иметь подходящие имена, чтобы вы или другой администратор могли их быстро и просто идентифицировать.

Примечание
По умолчанию, только пользователь, создавший политику, может изменить ее. Чтобы внести изменения, владелец политики должен выбрать опцию **Разрешить другим пользователям изменять эту политику** на странице политик в разделе **Подробности**.

7.3.2. Управление устройствами

Настройки управления устройством позволяют задать параметры безопасности мобильных устройств, экран блокировки с паролем, а также несколько профилей для каждой политики мобильных устройств.

Настройки объединены в следующие разделы:

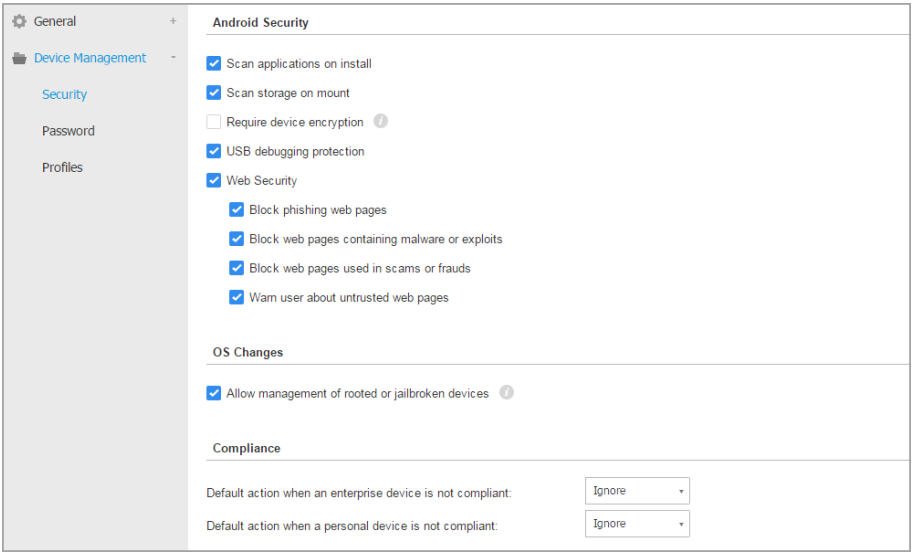
- Безопасность
- Пароль

- Профили

Безопасность

В этом разделе вы можете настроить различные параметры безопасности мобильных устройств, в том числе сканирование на предмет вредоносного ПО для Android-устройств, управление взломанными устройствами (root или jailbrake) или действия, которые необходимо предпринять для несовместимых устройств.

Важно
Сканирование на вредоносное ПО выполняется в облаке, поэтому мобильное устройство должно иметь доступ в Интернет.



Политики мобильных устройств - Настройки безопасности

Безопасность Android

- Выберите **Сканирование приложений при установке**, если вы хотите выполнять сканирование при установке нового приложения на управляемое мобильное устройство.

- Выберите **Сканирование хранилища при монтировании**, если вы хотите выполнять сканирование при каждой установке устройства хранения.

Предупреждение

Если вредоносная программа обнаружена, пользователю будет предложено удалить ее. Если пользователь не удалит обнаруженные вредоносные программы в течение одного часа после обнаружения, мобильное устройство объявляется несовместимым и действия для несовместимых устройств будут применены автоматически (игнорировать, запретить доступ, блокировать, стереть или отключить).

- Выберите **Требовать шифрование устройства**, чтобы запросить у пользователя активацию режима шифрования, доступного в ОС Android. Шифрование защищает данные, хранящиеся на Android-устройствах, в том числе учетные данные, настройки, загруженные приложения, медиа и другие файлы от несанкционированного доступа. Зашифрованные данные могут быть доступны на внешних устройствах только путем указания пароля разблокировки.

Важно

– Шифрование устройства доступно начиная с версии Android 3.0 и выше. Не все модели устройств поддерживают шифрование. Проверьте окно **Детали мобильного устройства** для получения информации о поддержке шифрования устройством.

– Шифрование может повлиять на производительность устройства.

Предупреждение

– Шифрование устройства является необратимым и единственный способ вернуться к незашифрованному состоянию это стереть устройство.

– Пользователи должны выполнить резервное копирование данных, прежде чем активировать шифрование устройства.

– Пользователи не должны прерывать процесс шифрования или они могут потерять часть или все свои данные.

Если вы включите эту опцию, то GravityZone Mobile Client будет постоянно отображать проблему, информирующую пользователя о необходимости активации шифрования. Пользователь должен нажать кнопку **Разрешить**, чтобы перейти к экрану шифрования и начать процесс. Если шифрование

не будет активировано в течение семи дней после уведомления, устройство станет несовместимым.

Чтобы включить шифрование на устройстве Android:

– Батарея должна быть заряжена более чем на 80%.
– Устройство должно быть подключено пока шифрование не завершится.
– Пользователь должен установить разблокировку паролем, соответствующим требованиям сложности.

Примечание

- Устройства Android используют тот же пароль для разблокировки экрана, что и для разблокировки зашифрованного содержимого.
- Шифрование требует пароль, PIN-код или снимок лица, чтобы разблокировать устройство, отключая другие параметры блокировки экрана.

Процесс шифрования может занять более часа, в течение которого устройство может перезагружаться несколько раз.

Вы можете проверить состояние шифрования хранилища для каждого мобильного устройства в окне **Детали мобильного устройства**.

- Устройства Android в режиме USB-отладки могут быть подключены к компьютеру через USB-кабель, что позволяет осуществлять расширенное управление приложениями и операционной системой. В этом случае безопасность мобильных устройств может быть под угрозой. Включенная по умолчанию опция **Защита от отладки USB**, предотвращает использование устройства в режиме USB-отладки. Если пользователь активирует USB-отладку, устройство автоматически становится несовместимым и над ним будут выполнены требуемые действия. Если выбрано действие **игнорировать** над несовместимыми устройствами, пользователь получит уведомление о небезопасных настройках.

  Тем не менее, вы можете запретить эту опцию для мобильных устройств, требующих работу в режиме USB-отладки (данный режим используется для разработки и тестирования мобильных приложений).

- Выберите **Веб-безопасность**, чтобы включить функции веб-безопасности на устройствах Android.

Модуль веб-безопасности сканирует в облаке каждый URL и возвращает GravityZone Mobile Client статус безопасности. Статус безопасности URL может быть: чистый, мошенничество, вредоносные программы, фишинг и ненадежный.

GravityZone Mobile Client может выполнять определенное действие в зависимости от состояния безопасности URL:

- **Блокировать фишинговую страницы**. Когда пользователь пытается получить доступ к фишинговому веб-сайту, GravityZone Mobile Client блокирует соответствующий URL и отображается страница с предупреждением.
- **Блокировка веб-страниц, содержащих вредоносные программы или эксплойты**. Когда пользователь пытается получить доступ к веб-сайту, который распространяет вредоносные программы или веб-эксплойты, GravityZone Mobile Client блокирует соответствующий URL и отображается страница с предупреждением.
- **Блокировать веб-страницы, используемые в мошенничестве или обмане**. Расширяет защиту от других видов мошенничества помимо фишинга (например поддельные escrows, поддельные пожертвования, социальные медиа угрозы и так далее). Когда пользователь пытается получить доступ к мошеннической веб-странице, GravityZone Mobile Client блокирует соответствующий URL и отображается страница с предупреждением.
- **Предупреждать пользователя о ненадежных веб-страницах**. Когда пользователь обращается к веб-сайту, который ранее был взломан для фишинговых целей или недавно был предупрежден о спаме или фишинговых письмах, будет отображено всплывающее сообщение без блокировки веб-страницы.

Важно
Функции веб-защиты работают только с Android 5 (и выше) и только с Chrome и встроенным Android-браузером.

Изменения ОС

Использование взломанных устройств (root или jailbroken), считается риском для безопасности корпоративных сетей, и такие устройства автоматически объявляются несовместимыми.

- Выберите **Разрешить управление рутованными или взломанными устройствами**, если вы хотите управлять взломанными устройствами (rooted или jailbroken) из Control Center. Обратите внимание, что такие устройства по умолчанию несовместимы и к ним будут автоматически применяться выбранные действия для несовместимых устройств, как только они будут обнаружены. Поэтому, чтобы иметь возможность применять к ним настройки политик безопасности или выполнять на них задачи, вы должны установить действие при несовместимости - игнорировать (Ignore).
- Если вы снимите флажок с **Разрешить управление рутованными или взломанными устройствами**, вы автоматически отключите связь со взломанными устройствами в сети GravityZone. В этом случае приложение GravityZone Mobile Client выведет сообщение о том, что устройство взломано (rooted/jailbroken). Пользователь может нажать кнопку OK, которая перенаправит его на экран регистрации. Как только устройство вернет первоначальный статус (unrooted / unjailbroken) или настройки политики позволят управление взломанными устройствами, оно может быть перезарегистрировано (с тем же маркером для устройств Android / с новым маркером для устройств iOS).

Совместимость

Вы можете настроить конкретные действия, которые будут автоматически применены к устройствам, обнаруженным как несовместимые, на основании типа владельца (предприятие или личное).

Примечание
При добавлении нового устройства в Control Center, вам будет предложено указать владельца устройства (предприятие или личное). Это позволит GravityZone управлять личными и корпоративными мобильными устройствами раздельно.

- Критерии несовместимости
- Действия для несовместимых устройств

Критерии несовместимости

Устройство определяется несовместимым в следующих ситуациях:

- **Устройства Android**

  - Устройство взломано (rooted).
  - GravityZone Mobile Client не является администратором устройства.
  - Вредоносные программы не удалены в течение одного часа после обнаружения.
  - Не выполняется политика:
    - Пользователь не установил пароль блокировки экрана в течение 24 часов после первого уведомления.
    - Пользователь не изменил пароль блокировки экрана в заданное время.
    - Пользователь не активировал шифрование устройства в течение семи дней после первого уведомления.
    - Режим USB-отладки включен на устройстве, при включенной опции политики защиты от USB-отладки.
- **Устройства iOS**
  - Устройство взломано (jailbroken).
  - GravityZone Mobile Client удален с мобильного устройства.
  - Не выполняется политика:
    - Пользователь не установил пароль блокировки экрана в течение 24 часов после первого уведомления.
    - Пользователь не изменил пароль блокировки экрана в заданное время.

Действие по умолчанию для несовместимых устройств

Когда устройство несовместимо, пользователю будет предложено исправить проблемы соответствия. Пользователь должен сделать необходимые изменения в течение определенного периода времени, в противном случае выбранное действие для несовместимых устройств будет применено (игнорировать, запретить доступ, блокировка, очистка или отключение).

Вы можете изменить действие для несовместимых устройств в политике безопасности в любое время. Новое действие будет применено к несовместимым устройствам как только политика будет сохранена.

Выберите из меню действие, соответствующее каждому типу владельца устройства, которое будет предпринято для несовместимых устройств:

- **Игнорировать**. Только уведомляет пользователя о том, что устройство не соответствует политике использования мобильного устройства.
- **Запретить доступ**. Блокирует доступ устройства к корпоративным сетям, удалив настройки Wi-Fi и VPN, но сохраняя все другие параметры, определенные в политике. Заблокированные настройки будут восстановлены, как только устройство станет совместимым.

  Важно
  Когда GravityZone Mobile Client запрещен как администратор устройства, устройство становится несовместимым и автоматически применяется действие **Запретить доступ**.

- **Блокировать**. Мгновенно блокирует экран устройства.
  - В Android экран блокируется паролем, созданным GravityZone, только если на устройстве не настроена блокировка экрана. Это не отменяет уже настроенную опцию блокировки экрана, такую как «Рисунок», «PIN-код», «Пароль», «Отпечаток пальца» или «Smart Lock».
  - На iOS, если устройство имеет блокировку экрана с паролем, устройство попросит его разблокировать.
- **Удалить**. Восстанавливает заводские настройки мобильного устройства, удаляя все пользовательские данные.

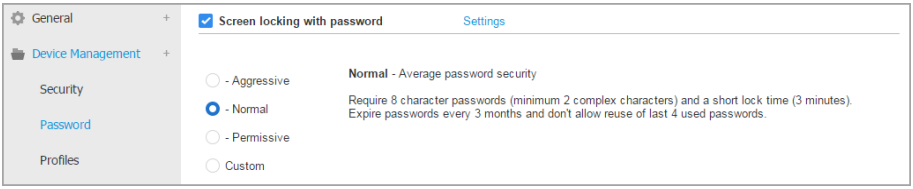
  Примечание
  Wipe не удаляет данные с установленных носителей (SD карты).

- **Связь прервана**. Устройство немедленно удаляется из сети.

  Примечание
  Чтобы опять зарегистрировать мобильное устройство, к которому было применено действие Unlink, необходимо добавить это устройство снова в Control Center. Затем устройство должно быть перерегистрировано с новым маркером активации. Перед повторной регистрацией устройства убедитесь, что условия, из-за которых устройство было отключено, отсутствуют или изменены параметры политик, которые позволяют управлять устройством.

Пароль

В этом разделе вы можете активировать блокировку экрана с функцией пароля, имеющегося в ОС мобильных устройств.



Политики мобильных устройств - Настройки защиты паролем

После включения этой функции, на экране устройства появится уведомление, которое предложит пользователю задать пароль разблокировки экрана. Пользователь должен ввести пароль, который соответствует критериям, заданным в политике безопасности. После того, как пароль будет установлен пользователем, все уведомления по этой проблеме будут удалены. Сообщение с предложением ввести пароль будет отображаться при каждой попытке разблокировать экран.

Примечание

Если пользователь не установит при запросе пароль, устройством можно будет пользоваться без пароля блокировки экрана до 24 часов после первого уведомления. В течение этого времени, сообщение с просьбой пользователю ввести пароль блокировки экрана, будет отображаться каждые 15 минут на экране.

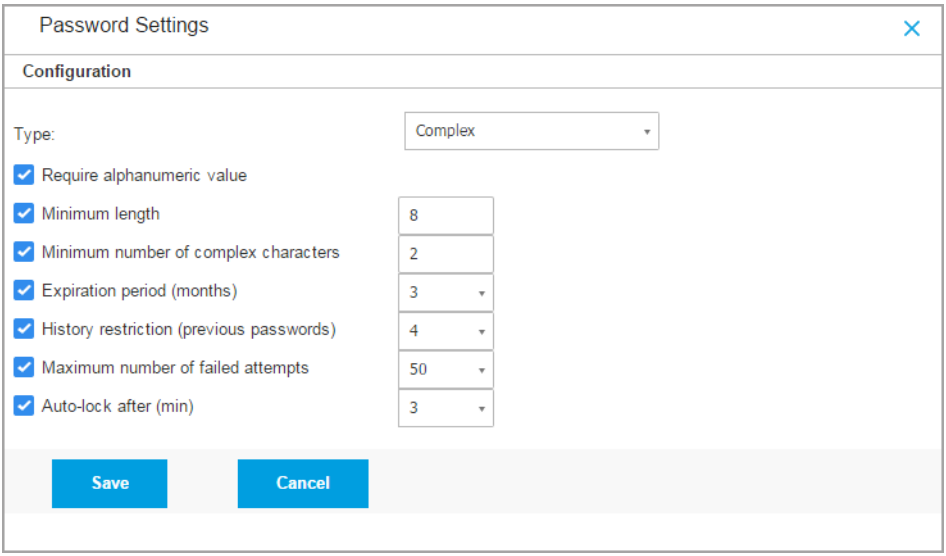
Предупреждение

Если пользователь не установит пароль в течение 24 часов после первого уведомления, мобильное устройство становится несовместимым и будет применяться действие для несовместимых устройств.

Для настройки параметров пароля блокировки экрана:

1. Выберите флажок **Блокировка экрана при помощи пароля**.
2. Выберите уровень безопасности, который лучше всего соответствует вашим потребностям (Интенсивный, Нормальный или Рекомендуемый). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

3. Для расширенной конфигурации, выберите уровень защиты **Пользователь**, а затем нажмите ссылку **Настройки**.



Политики мобильных устройств - Расширенные настройки защиты паролем

Примечание

Для просмотра требований к конфигурации пароля предопределенного уровня безопасности, выберите нужный уровень и нажмите ссылку **Настройки**. Если вы измените любую опцию, уровень безопасности пароля автоматически изменится на **Пользователь**.

Пользовательские настройки.

- **Тип**. Вы можете потребовать простые или сложные пароли. Критерии сложности пароля определены в ОС мобильных устройств.
  - На устройствах Android сложные пароли должны содержать по крайней мере одну букву, одну цифру и один специальный символ.

    Примечание

    Сложные пароли поддерживаются с Android 3.0 и более поздних версий.

– На iOS устройствах сложные пароли не допускают использование последовательных или повторяющихся символов (например, ABCDEF, 12345 или aaaaa, 11111).

В зависимости от выбранного варианта, когда пользователь устанавливает пароль экрана блокировки, операционная система проверяет и предлагает пользователю исправления, если необходимые критерии не выполняются.

- **Требовать буквенно-цифровое значение**. Требовать пароль, который содержит как буквы, так и цифры.
- **Минимальная длина**. Требовать пароль, который содержит минимальное количество символов, которое вы укажете в соответствующем поле.
- **Минимальное количество сложных символов**. Требовать пароль, который содержит минимальное количество не- буквенно-цифровых символов (например, @, # или $), которое вы укажете в соответствующем поле.
- **Период эксплуатации (месяцы)**. Заставить пользователя изменить пароль блокировки экрана через заданный интервал времени (в месяцах). Например, если ввести 3, пользователю будет предложено изменить пароль блокировки экрана через каждые три месяца.

Примечание
На устройствах Android эта функция поддерживается с версии 3.0 и в более поздних версиях.

- **Ограничение истории (предыдущие пароли)**. Выберите или введите значение в соответствующем поле, чтобы указать количество последних паролей, которые не могут быть повторно использованы. Например, если ввести 4, пользователь не сможет повторно использовать пароль, который соответствует одному из четырех предыдущих паролей.

Примечание
На устройствах Android эта функция поддерживается с версии 3.0 и в более поздних версиях.

- **Максимальное количество неудачных попыток**. Укажите, сколько раз пользователь может ввести неправильный пароль.

Примечание

На iOS устройствах, когда это число больше, чем 6: после шести неудачных попыток, время задержки суммируется, прежде чем пользователь сможет ввести пароль еще раз. Время задержки увеличивается с каждой неудачной попыткой.

Предупреждение

Если пользователь превышает максимальное число неудачных попыток, чтобы разблокировать экран, устройство будет стерто (все данные и настройки будут удалены).

- **Автоблокировка после (мин)**. Установите период бездействия (в минутах), после которого устройство автоматически блокируется.

Примечание

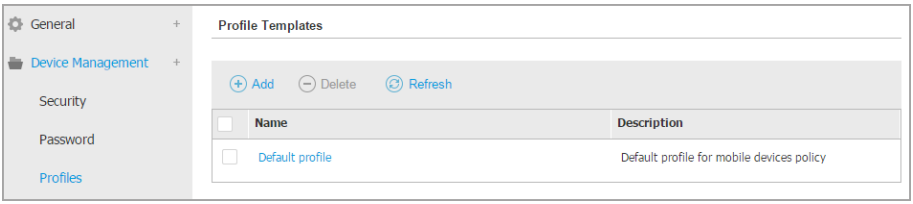
Устройства iOS имеют предопределенный список для автоматической блокировки и не позволяют применять пользовательские значения. При назначении политики, значения, несовместимые с параметрами автоматической блокировки устройства, будут заменены на более подходящий меньший период времени, доступный в списке. Например, если в политике автоблокировки указано три минуты, устройство автоматически будет заблокировано после двух минут бездействия.

При внесении изменений в политику, если вы выбираете более высокий уровень безопасности пароля блокировки экрана, пользователям будет предложено изменить пароль в соответствии с новыми критериями.

Если вы очистите опцию **Блокировка экрана при помощи пароля**, пользователям будет возвращен полный доступ к настройкам экрана блокировки на своем мобильном устройстве. Существующий пароль остается активным до тех пор, пока пользователь не решит изменить или удалить его.

Профили

В этом разделе вы можете создавать, изменять и удалять профили использования мобильных устройств. Использование профилей поможет вам настроить Wi-Fi, VPN и обеспечить контроль веб-доступа на управляемых мобильных устройствах.



Политики мобильных устройств - Шаблоны профилей

Вы можете настроить один или несколько профилей, но только один из них может быть активным на одном устройстве.

- Если настроить только один профиль, то профиль будет автоматически применен политикой для всех устройств.
- Если настроить несколько профилей, то политикой ко всем устройствам будет автоматически применен первый в списке.

Пользователи мобильных устройств могут просматривать назначенные профили и параметры, настроенные для каждого профиля в приложении GravityZone Mobile Client. Пользователи не могут изменять существующие настройки в профиле, но они могут переключаться между профилями, если доступно несколько из них.

Примечание
Для переключения профиля требуется подключение к сети Интернет.

Чтобы создать новый профиль:

1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится страница конфигурации профиля.
2. Настройте параметры профиля по мере необходимости. Для получения более подробной информации, обратитесь к:
   - «Подробная информация» (p. 439)
   - «Сети» (p. 439)
   - «Веб-доступ» (p. 443)
3. Нажмите **Сохранить**. Новый профиль будет добавлен к списку.

Чтобы удалить один или несколько профилей, отметьте их соответствующими флажками и нажмите кнопку ⊖ **Удалить** в правой части таблицы.

Чтобы изменить профиль, нажмите на его имя, измените настройки по мере необходимости и нажмите **Сохранить**.

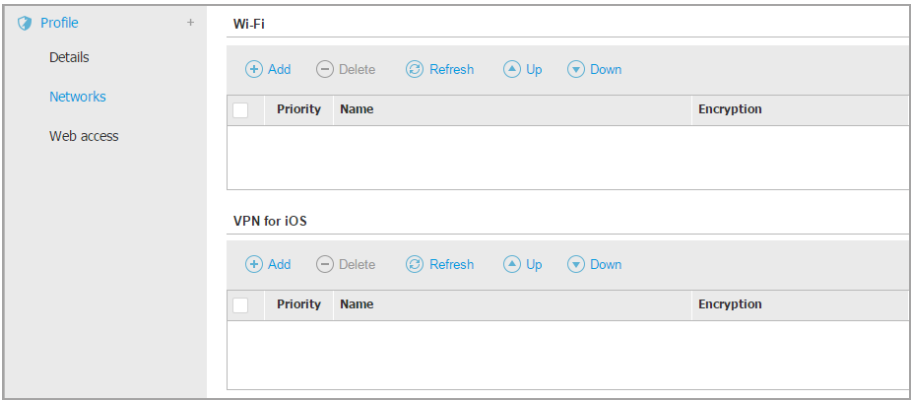
Подробная информация

Страница **Детали** содержит общую информацию о профиле:

- **Имя**. Введите имя профиля. Профили должны иметь подходящие имена, чтобы вы или другой администратор мог быстро определить их назначение.
- **Описание**. Введите подробное описание профиля. Эта опция может помочь администраторам легче определить назначение профиля из ряда других.

Сети

В этом разделе вы можете задать настройки одного или нескольких подключений к Wi-Fi и VPN. Настройки VPN доступны только для устройств под управлением iOS.



Политики мобильных устройств - Настройки подключений сетевых профилей

Важно
Перед настройкой подключений Wi-Fi и VPN убедитесь, что у вас есть вся необходимая информация (пароли, настройки прокси-сервера и т.д.).

Мобильные устройства, которым назначен соответствующий профиль, будут автоматически подключаться к определенной сети при ее доступности. Если создано несколько сетевых подключений, вы можете установить их приоритет,

учитывая то, что только одно подключение может быть использовано одновременно. Если первая сеть недоступна, то мобильное устройство будет подключаться ко второй сети и так далее.

Чтобы установить приоритет сети:

1. Отметьте флажком нужную сеть.
2. Используйте кнопки для задания приоритетов в правой части таблицы:
   - Нажмите кнопку **Вверх**, чтобы поднять приоритет выбранной сети.
   - Нажмите кнопку **Вниз**, чтобы понизить ее приоритет.

- **Wi-Fi**

  Вы можете добавить любое количество сетей Wi-Fi. Чтобы добавить сеть Wi-Fi:

  1. В разделе **Wi-Fi**, нажмите кнопку **Добавить** в правой части таблицы. Появится окно конфигурации.
  2. В разделе **Общее** вы можете настроить параметры соединения Wi-Fi:
     - **Имя (SSID)**. Введите имя новой сети Wi-fi.
     - **Безопасность**. Выберите опцию, соответствующую уровню сетевой безопасности Wi-Fi:
       - **Ограничения**. Выберите эту опцию если сеть Wi-Fi является публичной (не требуется учетных данных).
       - **Алгоритм для обеспечения безопасности сетей Wi-Fi (WEP)**. Выберите эту опцию, чтобы настроить Wireless Encryption Protocol (WEP) для подключения. Введите пароль для этого типа подключения в соответствующем поле ниже.
       - **WPA/WPA2 Personal**. Выберите эту опцию если сеть Wi-Fi защищена с помощью протокола Wi-Fi Protected Access (WPA). Введите пароль для этого типа подключения в соответствующем поле ниже.
  3. В разделе **TCP/IP** вы можете настроить параметры протокола TCP/IP для подключения к сети Wi-Fi. Каждое подключение Wi-Fi может использовать протокол версии IPv4 или IPv6, или оба.
     - **Настроить IPv4**. Если вы хотите использовать версию IPv4, выберите способ назначения IP-адресов из соответствующего меню:

DHCP: если IP-адрес назначается автоматически с помощью DHCP-сервера. При необходимости, укажите идентификатор клиента DHCP в следующем поле.

Отключен: выберите эту опцию, если вы не хотите использовать протокол версии IPv4.

– **Настроить IPv6**. Если вы хотите использовать протокол версии IPv6, выберите способ назначения IP-адресов из соответствующего меню:

DHCP: если IP-адрес назначается автоматически с помощью DHCP-сервера.

Отключен: выберите эту опцию если вы не хотите использовать протокол версии IPv6.

– **Серверы DNS**. Введите адрес по крайней мере одного DNS-сервера для сети.

4. В разделе **Представитель** настройте параметры прокси-сервера для подключения Wi-Fi. Выберите нужный способ настройки прокси-сервера из меню **Тип**:

   – **Выключить**. Выберите эту опцию если сеть Wi-Fi не имеет настроек прокси-сервера.

   – **Вручную**. Выберите эту опцию, чтобы вручную указать параметры прокси-сервера. Введите имя хоста прокси-сервера и порт, по которому он прослушивает подключение. Если прокси-сервер требует аутентификации, установите флажок **Аутентификация** и введите имя пользователя и пароль в последующих полях.

   – **Автоматически**. Выберите эту опцию для получения настроек прокси-сервера из Proxy Auto-Configuration (PAC), опубликованных в локальной сети. Введите адрес файла PAC в поле **URL**.

5. Нажмите **Сохранить**. Новое подключение Wi-Fi будет добавлено в список.

- **Настройка VPN для устройств iOS**

  Вы можете добавить любое количество подключений VPN. Чтобы добавить VPN:

  1. В разделе **VPN for iOS**, нажмите кнопку ⊕ **Добавить** в правой части таблицы. Появится окно конфигурации.

2. Задайте параметры VPN в окне **VPN Соединение**:

   Общее:

   – **Имя**. Введите имя подключения VPN.

   – **Шифрование**. Для данного типа подключения доступен протокол аутентификации **IPSec**, который требует пароль для проверки подлинности пользователя и аутентификации машины с общим секретным ключом.

   – **Сервер**. Введите адрес VPN-сервера.

   – **Пользователь**. Введите имя пользователя VPN.

   – **Пароль**. Введите пароль VPN.

   – **Название группы**. Введите имя группы.

   – **Выбрать**. Введите общий ключ.

   Представитель:

   В этом разделе вы можете настроить параметры прокси-сервера для подключения VPN. Выберите нужный способ настройки прокси-сервера из меню **Тип**:

   – **Выключить**. Выберите эту опцию если подключение VPN не имеет настроек прокси-сервера.

   – **Вручную**. Эта опция позволяет вручную указать параметры прокси-сервера:

     - **Сервер**: введите имя прокси-сервера.
     - **Порт**: введите номер порта прокси-сервера.
     - Если прокси-сервер требует аутентификации, установите флажок **Аутентификация** и введите имя пользователя и пароль в последующих полях.

   – **Автоматически**. Выберите эту опцию для получения настроек прокси-сервера из Proxy Auto-Configuration (PAC) файла, опубликованного в локальной сети. Введите адрес файла PAC в поле **URL**.

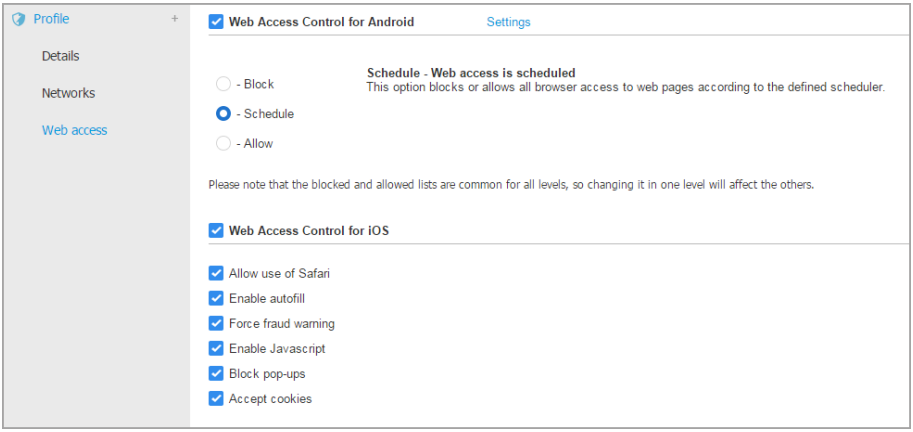
3. Нажмите **Сохранить**. Новое подключение VPN будет добавлено в список.

Чтобы удалить одну или несколько сетей, отметьте их соответствующими флажками и нажмите кнопку ⊖ **Удалить** в правой части таблицы.

Чтобы изменить сеть, нажмите на ее имя, измените настройки по мере необходимости и нажмите **Сохранить**.

Веб-доступ

В этом разделе вы можете настроить управление веб-доступом для устройств Android и iOS.



Политики мобильных устройств - Настройки профилей веб-доступа

- **Управление веб-доступом для Android.** Включите эту опцию для фильтрации веб-доступа Chrome и встроенного браузера Android. Вы можете установить временные ограничения на доступ к сети Интернет, а также разрешить или заблокировать доступ к определенным веб-страницам. Веб-страницы, заблокированные модулем управления веб-доступом, не будут отображаться в браузере. Вместо этого будет отображаться веб-страница по умолчанию, сообщающая пользователю о том, что запрашиваемая веб-страница была заблокирована модулем управления веб-доступом.

Важно
Управление веб-доступом для Android работает только с Android 5 (и выше) и только с Chrome и встроенным Android-браузером.

У вас есть три возможных варианта:

– Выберите **Разрешить**, чтобы всегда предоставлять доступ в интернет.
– Выберите **Блокировать**, чтобы всегда запрещать доступ в интернет.
– Выберить **Запланировать**, чтобы ввести временные ограничения на веб-доступ по подробному расписанию.

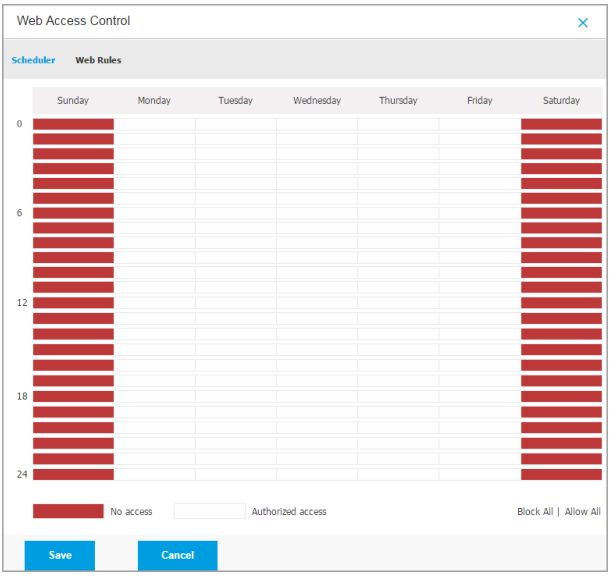
Также, если вы выберете разрешить или запретить веб-доступ, можно настроить исключения в этих действиях для целых веб-категорий или только для определенных веб-адресов. Нажмите **Настройки**, чтобы настроить расписание веб-доступа и исключения, следующим образом:

Проверка по расписанию

Чтобы ограничить доступ к сети Интернет еженедельно в определенное время:

1. Выберите из сетки временные интервалы, в течение которых вы хотите запретить доступ в Интернет.

   Можно щелчком мыши отметить отдельные клетки или нажать и расширить ее, чтобы задать более длительный период. Нажмите еще раз на клетку, чтобы изменить выбор.



Политики мобильных устройств - Расписание веб-доступа

Чтобы создать новый интервал, нажмите **Разрешить всем** или **Блокировать все**, в зависимости от типа ограничения, которое вы хотите реализовать.

2. Нажмите **Сохранить**.

Веб-правила

Вы также можете задать веб-правила по блокировке или разрешению определенных веб-адресов, переопределив существующие настройки модуля управления веб-доступом. Например, пользователи смогут получить доступ к определенной веб-странице, даже если веб-браузинг заблокирован модулем управления веб-доступом.

Чтобы создать веб-правило:

1. Выберите **Используйте исключения**, чтобы использовать веб-исключения.
2. Введите адрес, который вы хотите разрешить или запретить в поле **Веб-адрес**.
3. Выберите **Разрешить** или **Блокировать** из меню **Разрешение**.

4. Нажмите на кнопку ⊕ **Добавить** в правой части таблицы, чтобы добавить адрес в список исключений.
5. Нажмите **Сохранить**.

Чтобы изменить веб-правило:

1. Нажмите веб-адрес, который вы хотите отредактировать.
2. Измените существующий URL.
3. Нажмите **Сохранить**.

Чтобы удалить веб-правило:

1. Наведите курсор на веб-адрес, который вы хотите удалить.
2. Нажмите кнопку ⊗ **Удалить**.
3. Нажмите **Сохранить**.

Используйте маски, чтобы создать шаблоны веб-адресов:

– Звездочка (*) заменяет ноль или более символов.
– Вопросительный знак (?) заменяет только один символ. Вы можете использовать несколько вопросительных знаков, чтобы задать любую возможную комбинацию из определенного количества символов. Например, ??? заменяет любую комбинацию, состоящую из трех символов.

В следующей таблице, вы можете найти некоторые примеры синтаксиса для указания адресов веб-сайтов.

Синтаксис	Область применения
`www.example*`	Любой веб-сайт или веб-страница, начинающаяся с `www.example` (вне зависимости от расширения домена). Исключение не будет применяться к поддоменам указанного веб-сайта, например, `subdomain.example.com`.
`*example.com`	Любой веб-сайт, заканчивающийся на `example.com`, включая страницы и поддомены.

Синтаксис	Область применения
`*string*`	Любой веб-сайт или веб-страница, содержащие в адресе указанную строку.
`*.com`	Любой веб-сайт, имеющий доменное расширение `.com`, включая страницы и поддомены. Используйте этот синтаксис, чтобы исключить из сканирования целые домены верхнего уровня.
`www.example?.com`	Любой веб-адрес, начинающийся с `www.example?.com`, где ? заменяет один любой символ. Это могут быть сайты: `www.example1.com` или `www.exampleA.com` и др.

- **Управление веб-доступом для iOS.** Включите эту опцию, чтобы централизованно управлять настройками встроенного браузера iOS (Safari). Пользователи мобильных устройств больше не будут иметь возможность изменять соответствующие настройки на своем устройстве.
  - **Разрешить использование Safari**. Эта опция позволяет контролировать использование браузера Safari на мобильных устройствах. Отключение опции удаляет ярлык Safari из интерфейса iOS, тем самым предотвращая доступ пользователей к сети Интернет через Safari.
  - **Включить автозаполнение**. Отключите эту опцию если вы хотите предотвратить хранение данных форм браузером, которые могут включать конфиденциальную информацию.
  - **Предупреждение о мошенничестве** Выберите эту опцию для гарантированного уведомления пользователей при посещении мошеннических веб-страниц.
  - **Включить Javascript**. Отключите эту опцию если вы хотите, чтобы Safari игнорировал JavaScript на веб-сайтах.
  - **Блокировать всплывающие окна**. Выберите этот параметр, чтобы предотвратить автоматическое открытие всплывающих окон.
  - **Принять файлы cookies**. По умолчанию Safari разрешает файлы cookie. Отключите эту опцию если вы хотите защититься от хранения веб-сайтами просматриваемой информации.

Важно
Управление веб-доступом для iOS не поддерживается на iOS 13.

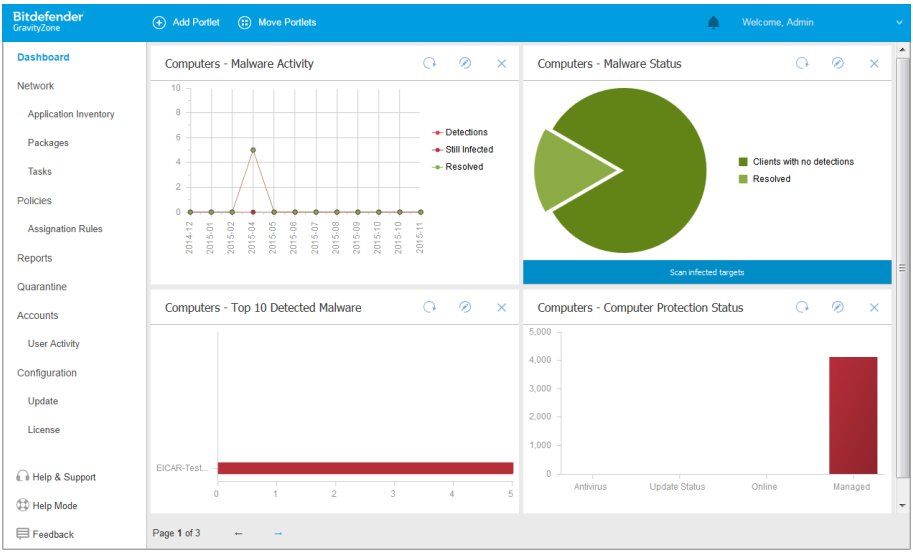
8. ИНФОРМАЦИОННАЯ ПАНЕЛЬ МОНИТОРИНГА

Правильный анализ сетевой безопасности требует наличия доступа к данным и их корреляции. Наличие централизованной информации о безопасности позволяет контролировать и обеспечивать соблюдение политик безопасности организации, быстро выявлять проблемы, анализировать угрозы и уязвимости.

8.1. Панель управления

Панель Control Center - настраиваемый визуальный дисплей, обеспечивающий быстрый обзор всех конечных точек и статуса сети.

Портлеты информационной панели отображают различную информацию о состоянии безопасности в реальном времени, используя простые графики, которые позволяют вам быстро выявить все проблемы, которые могут потребовать вашего вмешательства.



Информационная панель

Вот что вам нужно знать о портлетах информационной панели:

- Control Center поставляется с несколькими предопределенными портлетами информационной панели.
- Каждый портлет информационной панели включает в себя подробный отчет, создаваемый в фоновом режиме и доступный одним щелчком на графике.
- Есть несколько типов портлетов, которые содержат различную информацию о состоянии защиты конечных точек, такие как состояние обновлений, активность вредоносного ПО, активность файрвола.

Примечание
По умолчанию, портлеты получают данные за текущий день и, в отличие от отчетов, не могут быть установлены на более длительные промежутки времени, более чем один месяц.

- Информация, отображаемая с помощью портлетов, относится к конечным точкам только под вашей учетной записью. Вы можете настроить объекты каждого портлета и параметры с помощью команды **Изменить портлет**.
- Нажмите на нужной записи легенды диаграммы, в случае доступности, чтобы скрыть или отобразить соответствующие данные на графике.
- Портлеты отображаются в группах по четыре. Используйте вертикальную полосу прокрутки или клавиши со стрелками вверх и вниз для перемещения между группами портлетов.
- Для ряда типов отчетов, у вас есть возможность одновременно запускать нужные задачи на требуемых конечных устройствах, без необходимости переходить к разделу **Network**, чтобы запустить задачу (например, сканировать зараженные конечные точки или обновить конечные точки). Используйте кнопку выполнения доступных действий в нижней части портлета.

Информационную панель очень просто настроить с учетом индивидуальных предпочтений. Вы можете изменить настройки портлета, добавить дополнительные портлеты, удалить или отсортировать существующие портлеты.

8.1.1. Обновление данных портлета

Чтобы убедиться, что портлет отображает последнюю информацию, нажмите на кнопку **Обновить** в его заголовке.

Чтобы обновить информацию обо всех портлетах одновременно, нажмите кнопку **Обновить портлеты** в верхней части панели инструментов.

8.1.2. Редактирование настроек портлета

Некоторые портлеты содержат информацию о текущем статусе, в то время как другие содержат отчеты о событиях безопасности за последний период. Вы можете проверить и настроить периодичность отчетов портлета нажав значок в его заголовке.

8.1.3. Добавление нового портлета

Вы можете добавить другие портлеты для получения необходимой информации.

Чтобы добавить новый портлет:

1. Перейдите на страницу **Панель инструментов**.
2. Нажмите кнопку **Добавить портлет** в верхней части кансоли. Появится окно конфигурации.
3. В разделе **Подробная информация**, настройте детали портлета:
   - Тип конечной точки (**Компьютеры**, **Виртуальные машины** или **Мобильные устройства**)
   - Тип фонового отчета
   - Подходящее имя портлета
   - Интервал времени для событий, которые будут отображаться

   Для получения более подробной информации о доступных типах отчетов, обратитесь к «Типы отчетов» (p. 512).
4. В разделе **Цели** выберите сетевые объекты и группы для включения.
5. Нажмите **Сохранить**.

8.1.4. Удаление портлета

Вы можете легко удалить любой портлет, нажав значок **Удалить** в его заголовке. После того как вы удалите портлет, вы не сможете его восстановить. Тем не менее, вы сможете создать другой портлет с теми же настройками.

8.1.5. Расположение портлетов

Вы можете расположить портлеты информационной панели по вашему усмотрению. Чтобы изменить расположение портлетов:

1. Перейдите на страницу **Панель инструментов**.

2. Перетащите любой портлет в нужную позицию. Все остальные портлеты распределятся между новой и старой позицией, сохраняя свой порядок.

Примечание
Вы можете перемещать портлеты только в имеющиеся позиции.

9. РАССЛЕДОВАНИЕ ПРОИСШЕСТВИЙ

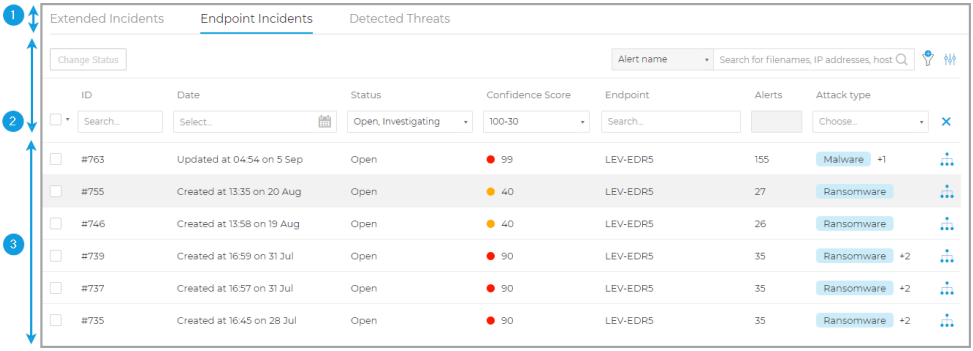
Раздел **Инциденты** позволяет фильтровать, расследовать и предпринимать действия по всем событиям безопасности, которые были обнаружены датчиком инцидентов за определенный промежуток времени.

Раздел **Incidents** содержит следующие страницы:

- **Инциденты** : позволяет просматривать и расследовать события безопасности.
- **Черный список**: управляет заблокированными файлами, участвующими в событиях безопасности.

9.1. Страница инцидентов

Используйте страницу **Инциденты** для фильтрации и управления событиями безопасности.



Обзор страницы инцидентов

Примечание
Доступность данных вкладок варьируется в зависимости от лицензии, которую включает в себя текущий план.

Эта страница содержит следующие области:

1. Панель окон с вкладками, включающими различные типы инцидентов:
   - **Обнаруженные угрозы**: отображает все события безопасности, идентифицированные как угрозы модулями предотвращения

GravityZone. Эти инциденты обнаруживают на конечных точках и обрабатывают с помощью действий, предусмотренных в политиках безопасности, применяемых к Вашей среде.

2. Параметры фильтрации для настройки Вашей сетки:
   - Нажмите кнопку **Показать/скрыть столбцы**, чтобы добавить или убрать столбцы фильтра.

     Страница обновится автоматически, загрузив карточки событий безопасности с информацией, соответствующей добавленным столбцам.
   - Нажмите кнопку **Показать/скрыть фильтры**, чтобы отобразить или скрыть панель фильтров.
   - Нажмите кнопку **Очистить фильтры**, чтобы сбросить все фильтры.
3. Сетка инцидентов отображает список событий безопасности, соответствующих выбранным фильтрам.

Примечание
Эта функция больше не обеспечивает поддержку Internet Explorer.

Панель обзора

Панель **Обзор** содержит список открытых инцидентов, главных предупреждений, затронутых устройств и другие соответствующие данные, чтобы дать Вам быстрое представление об общей ситуации, связанной с угрозами в Вашей среде.

Панель обзора

Примечание
Доступность и содержание панели **Обзор** могут отличаться в зависимости от лицензии, включенной в Ваш текущий план.

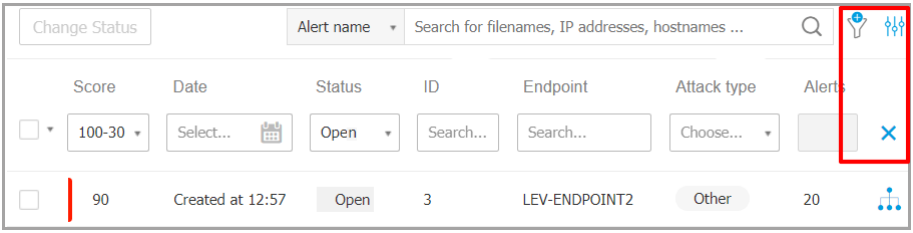
Фильтрация инцидентов из панели Обзор

Вы также можете отфильтровать список инцидентов, выбрав значения на панели

- Если щелкнуть значение в разделе **ОТКРЫТЫЕ ИНЦИДЕНТЫ**, оно отобразит только инциденты с выбранным уровнем серьезности.
- Если щелкнуть значение в разделе **ТОП ОПОВЕЩЕНИЙ**, оно заполнит поле поиска именем оповещения и отобразит только те случаи, когда оповещение было обнаружено.
- Если щелкнуть значение в разделе **ТОП МЕТОДОВ**, оно заполнит поле поиска названием метода и отобразит только те случаи, когда метод был обнаружен.
- Если нажать на значение в разделе **ТОП ЗАТРОНУТЫХ УСТРОЙСТВ**, оно отобразит только инциденты, влияющие на выбранное устройство.

9.1.1. Сетка фильтров

Страница **Инциденты** позволяет выбрать, какие инциденты отображать, настроив сетку фильтров.



Сетка фильтров

- Нажмите кнопку **Показать/скрыть столбцы**, чтобы добавить или убрать столбцы фильтра.

  Страница обновится автоматически, загрузив карточки событий безопасности с информацией, соответствующей добавленным столбцам.
- Нажмите кнопку **Показать/скрыть фильтры**, чтобы отобразить или скрыть панель фильтров.

- Нажмите кнопку ✕ **Очистить фильтры**, чтобы сбросить все фильтры.

Подробные сведения о доступных параметрах фильтрации приведены в следующей таблице:

Параметры фильтрации	Подробная информация
Рейтинг	Показатель достоверности - это число от 100 до 10, указывающее, насколько потенциально опасно событие безопасности. Чем выше число, тем больше уверенности в том, что событие опасно. Для фильтрации по доверительной шкале перетащите ползунок к выбранным значениям. Или вы можете использовать числовые поля под ползунком. Нажмите **OK**, чтобы подтвердить выбор оценки.
Дата	Чтобы фильтровать по дате: 1. Нажмите иконку календаря или поле **Дата**, чтобы открыть страницу конфигурации даты. 2. Выберите временной промежуток, когда произошел инцидент: • Перейдите на вкладки **с** и **до**, чтобы выбрать даты, определяющие временной интервал. **Примечание** Вы можете указать точное время для начала и завершения, используя поля часов и минут под календарем. • Вы также можете выбрать заранее определенный период относительно текущего времени. 3. Нажмите **OK** , чтобы применить фильтр.
Состояние	Отфильтруйте инциденты по их текущему состоянию, проверив один или несколько параметров статуса, доступных в выпадающем меню **Статус**: • **Открыть**: для неисследованных событий безопасности

Параметры фильтрации	Подробная информация
	• **Расследуемые** : для расследуемых событий безопасности • **Ложное срабатывание**: для событий безопасности, помеченных как ложная тревога • **Закрытые**: для событий безопасности с закрытым расследованием
Идентификатор	Сузьте список инцидентов, выполнив поиск определенного идентификационного номера события безопасности.
Конечная точка	Сузьте список инцидентов, выполнив поиск определенного имени конечной точки в управляемой сети.
Тип атаки	Тип атаки - это динамический список наиболее распространенных типов атак, который изменяется в зависимости от показателей атаки, обнаруженных в перечисленных событиях безопасности.
Оповещения	В столбце **Оповещения** отображается количество оповещений, вызванных за инцидент.
ОС конечной точки	Эта опция фильтрует события безопасности по операционной системе задействованных конечных точек.

Примечание
Параметры фильтрации могут варьироваться в зависимости от типа лицензионного ключа, включенного в Ваш текущий план.

Чтобы найти дополнительные элементы, которые не отображаются в сетке фильтра, выберите один из параметров поиска в выпадающем меню **Поиск**:

- **Имя оповещения** - от 3 до 1000 символов.
- **IP-адрес конечной точки** - не более 45 символов.
- **MD5** - максимум 32 символа.
- **SHA256** - максимум 64 символа.
- **Имя узла** - не более 360 символов.
- **Имя пользователя** - не более 1000 символов.

Страница обновится автоматически, загружая только карточки событий безопасности, соответствующие искомому элементу.

9.1.2. Просмотр списка событий безопасности

На странице **Инциденты** отображается список событий безопасности, соответствующих выбранным фильтрам.

По умолчанию на странице 20 событий, сгруппированных по дате. Страница автоматически обновляется через регулярные промежутки времени, пока **Датчик инцидентов** обнаруживает новые события.

Важно
Все события безопасности старше 90 дней автоматически удаляются из раздела **Угрозы**, а также из репозитория событий безопасности.

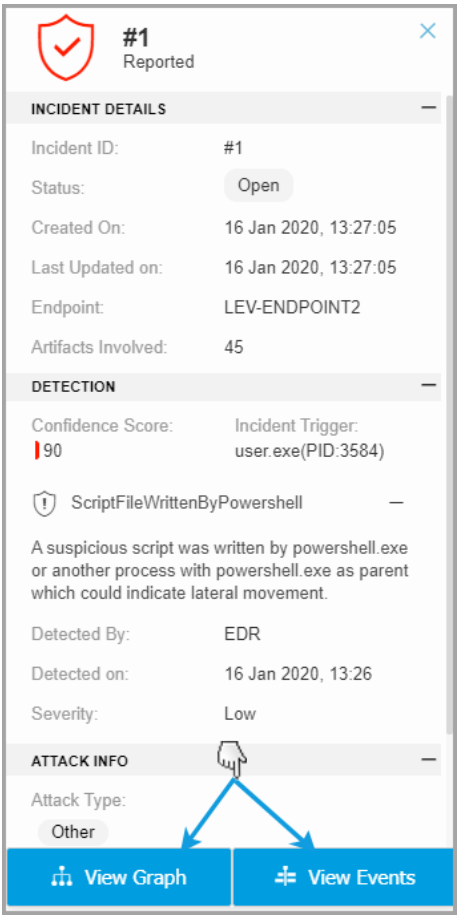
Для навигации по странице используйте стрелки, колесо прокрутки или нажмите на панель прокрутки. Измените количество отображаемых событий внизу страницы. Вы можете просматривать до 100 событий на странице.

Каждая запись события безопасности отображается в расширенном формате карты, предоставляя обзор каждого инцидента с информацией, основанной на выбранных фильтрах.

Примечание
Обратите внимание на цвет слева для того чтобы быстрее оценить достоверность события (низкий, средний или высокий).

Карта событий безопасности

- Если вы нажмете соответствующую кнопку **Посмотреть график** карты событий безопасности, она откроет ее на новой странице, где вы сможете детально проанализировать инцидент и предпринять соответствующие действия.
- Если щелкнуть карточку события безопасности, откроется боковая панель быстрого просмотра с информацией о выбранном инциденте.



Быстрый просмотр информации об инциденте

– Нажмите кнопку **Просмотреть график**, чтобы получить доступ к графической визуализации инцидента.

– Нажмите кнопку **Посмотреть события**, чтобы получить доступ к временной шкале инцидента.

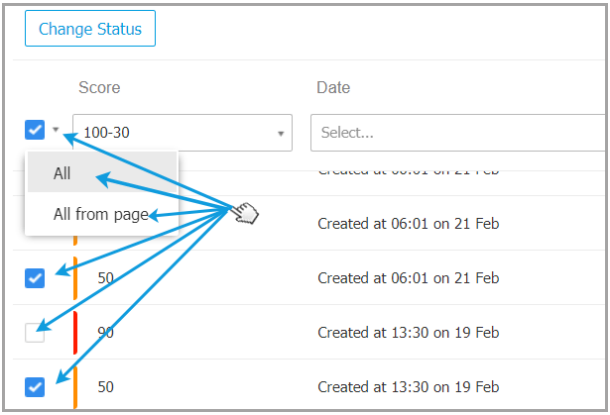
- Если вы установите флажок для любой карты событий безопасности, она активирует кнопку **Изменить статус**, позволяя вам изменить текущий статус инцидента.

Изменение статуса событий безопасности

Статус расследования помогает вам отслеживать инциденты, которые уже были расследованы и помечены как закрытые или ложно сработавшие, инциденты, которые в настоящее время расследуются, а также открытые или новые инциденты, которые еще предстоит проанализировать.

Вы можете изменить состояние одного или нескольких событий безопасности одновременно:

1. Установите флажки на карточках событий безопасности, у которых будет изменен статус.

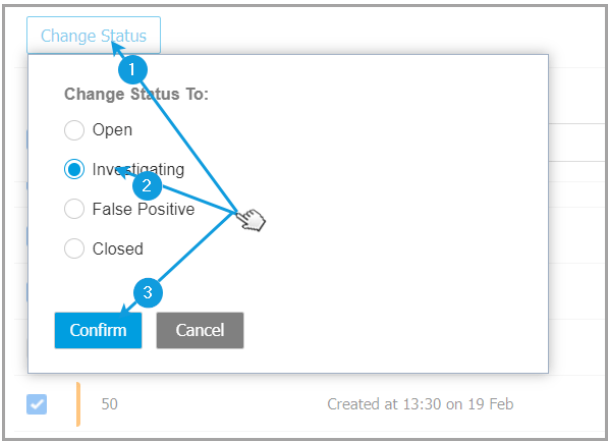


Выбор карт событий безопасности

Вы можете выбрать их по отдельности или с помощью опций массового выбора в выпадающем меню.

Примечание
Вы также можете просматривать несколько страниц событий безопасности, при сохранении своего выбора.

2. Нажмите кнопку **Изменить статус** и выберите нужные параметры:

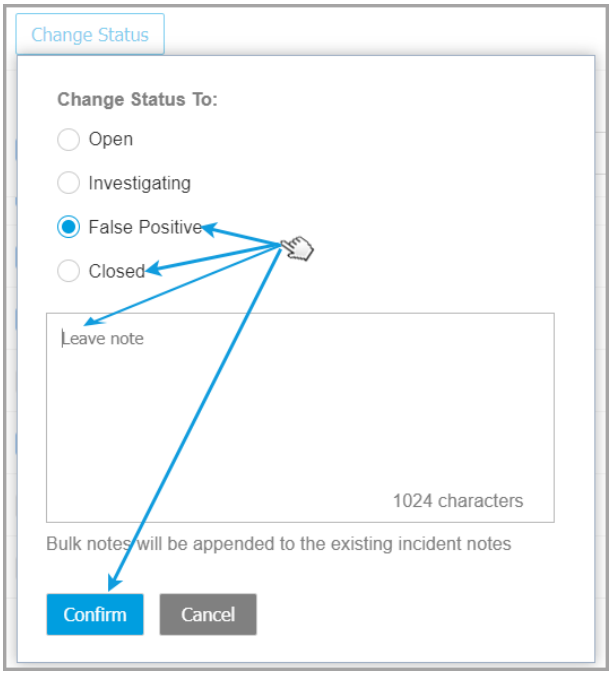


Изменение статуса события безопасности

- **Open** - когда событие безопасности еще не расследуется.
- **Расследовать** - когда вы начали расследование события.
- **Ложное срабатывание** - когда вы проанализировали событие и определили его как ложноположительное.
- **Закрыть**- когда вы закончили расследование события.

Примечание

При изменении состояния событий на **Ложное срабатывание** или **Закрытое** открывается окно, в котором можно оставить примечание о причинах изменения статуса события, для последующей консультации.



Оставить записку для закрытых событий и событий ложного срабатывания.

Примечание
Примечание будет добавлено к уже существующим внутри отфильтрованных инцидентов.

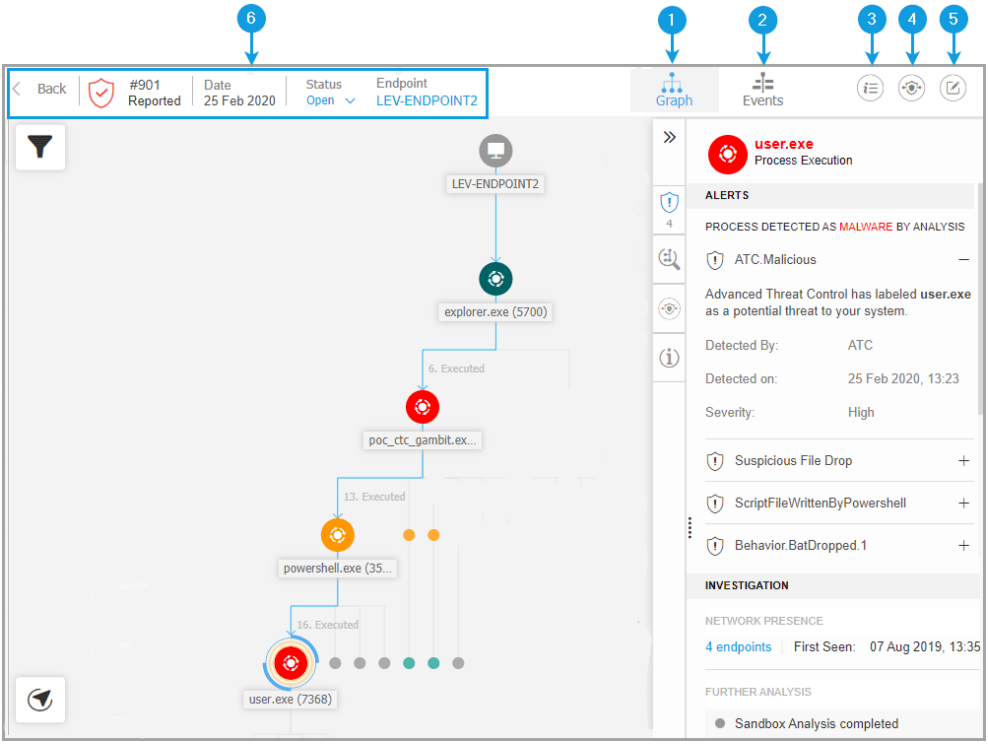
3. Нажмите **Confirm**, чтобы применить выбранную опцию статуса.

9.1.3. Обзор обнаруженных угроз

На странице **Инциденты** выберите событие безопасности, которое вы хотите проанализировать, и нажмите **Просмотреть график**, чтобы отобразить его на новой странице.

Каждый инцидент безопасности имеет отдельную страницу, содержащую подробную информацию о последовательности событий (отображаемых на графике в виде связанных узлов событий безопасности), которые

спровоцировали инцидент и предоставляет варианты действий по исправлению.



1. Вкладка «График»

   График отображает инцидент безопасности и составляющие его элементы, выделяя критический путь инцидента и отображая сведения об узле, который спровоцировал инцидент, на панели **Node Details**.

2. Вкладка «События»

   На вкладке «События» отображаются фильтруемые обнаруженные системные события и оповещения, а также соответствующие описания событий.

3. Панель информации об инциденте

   Эта панель содержит сворачиваемую область с такими деталями, как идентификатор инцидента, текущее состояние, временная отметка, когда он был создан и последний раз обновлялся, количество задействованных артефактов, имя триггера и информация об атаке.

4. Панель исправления

   Эта панель содержит сворачиваемую область с действиями, автоматически предпринимаемыми GravityZone, и рекомендуемыми действиями, которые можно выполнить, чтобы смягчить инцидент.

5. Заметки буфера обмена

   При нажатии кнопки **Notes** открывается буфер обмена, в который можно добавлять заметки о текущем инциденте, которые вы можете прочитать при повторном посещении инцидента позднее.

6. Строка состояния инцидента

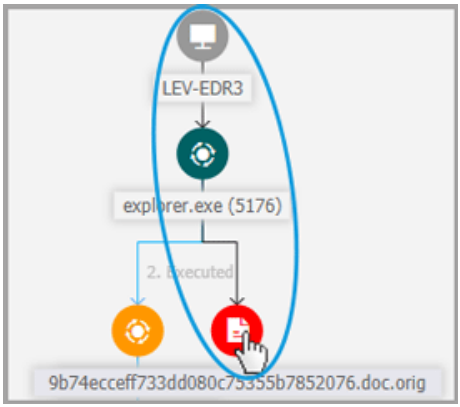
   Строка состояния содержит подробную информацию об идентификаторе инцидента, времени и дате его создания, статусе, триггере инцидента и конечной точке, на которую он влияет. Нажав кнопку **Back**, вы вернетесь на главную страницу **Incidents**.

Узлы событий безопасности

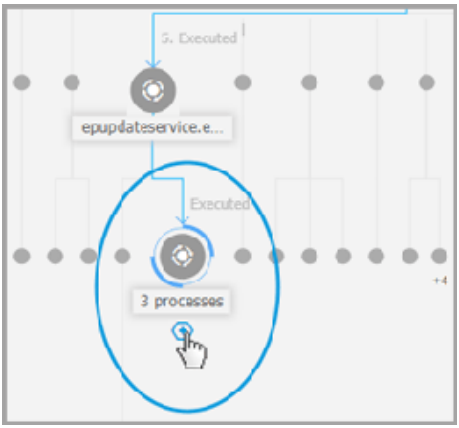
Вот что вам нужно знать об узлах событий безопасности:

- Каждый узел представляет определенный элемент, участвующий в расследуемом инциденте.

- Все узлы, составляющие критический путь, по умолчанию подробно отображаются при открытии инцидента, в то время как другие элементы постепенно исчезают, чтобы избежать загромождения.
  - Если навести курсор на узел, который не является частью критического пути, он будет выделен и покажет путь к исходной точке, не нарушая Critical Path.



- Три или более одинаковых узла событий типа действия, порождаемых родительским узлом, группируются в расширяемый узел кластера.



  - Только узлы без дочерних элементов будут скрыты от графика инцидентов, когда кластерный узел свернут.
  - Узлы, в которых была обнаружена подозрительная активность, не будут добавлены к узлу кластера.
- При нажатии на узел отобразятся следующие данные:
  - Он выделит синим цветом путь к узлу конечной точки вместе со всеми другими задействованными элементами.
  - Боковая панель с расширяемыми секциями, которые предоставляют подробную информацию о выбранном узле, предупреждениях в случае обнаружения сбоев, доступных действиях и рекомендациях. Обратитесь к «Сведения об узле» (p. 478) для получения дополнительной информации.
- Узлы связаны стрелками, указывающими ход действий, которые произошли в конечной точке во время инцидента. Каждая строка помечена именем действия и его хронологическим номером.

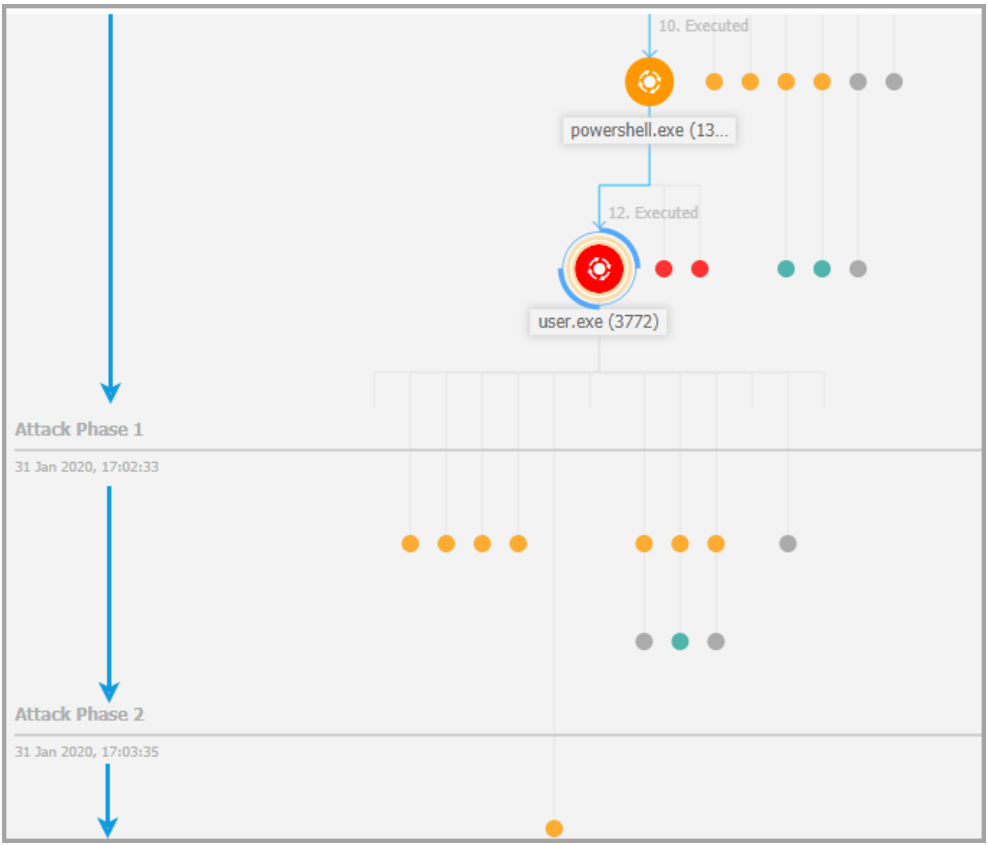
Следующие элементы инцидента могут быть представлены как узлы:

Тип узла	Описание
Конечная точка	Отображает сведения о конечной точке и статусе управления патчами.

Тип узла	Описание
Домен	Показывает информацию о хосте домена и его конечных точках.
Процесс	Отображает сведения о роли процесса в текущем инциденте, информацию о файле, сведения о выполнении процесса, присутствие в сети и дополнительные параметры расследования.
Файл	Показывает сведения о роли файла в текущем инциденте, информацию о файле, присутствие в сети и дополнительные параметры расследования.
Реестр	Отображает информацию Реестра и детали родительского процесса.

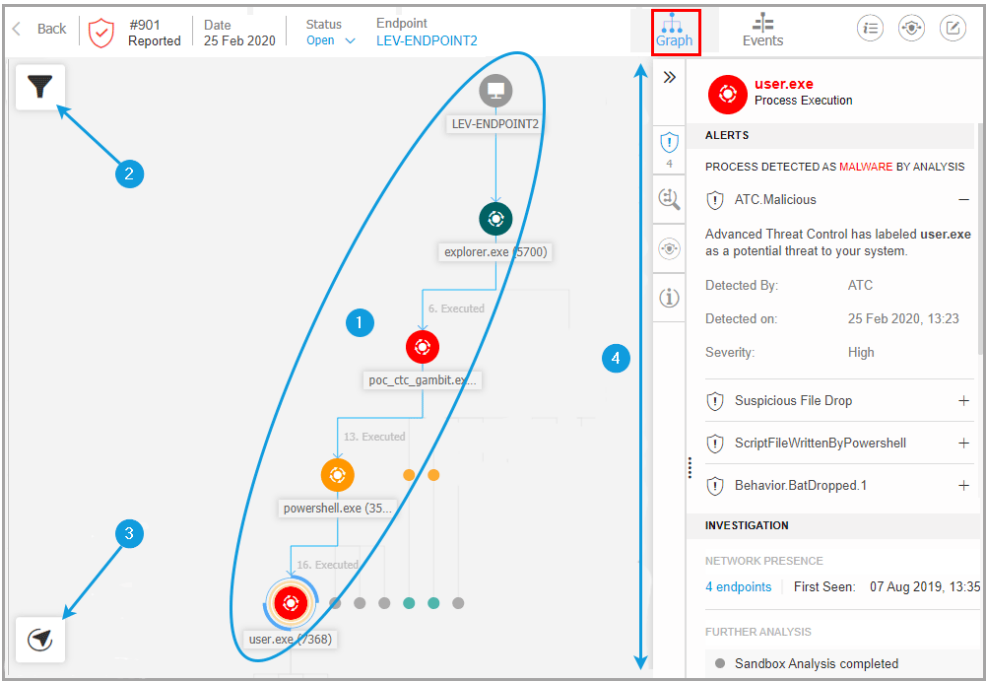
График

График предоставляет интерактивное графическое представление расследуемого инцидента и его контекста, выделяя последовательность элементов, напрямую участвующих в его инициировании, известную как **Критический путь** инцидента, а также всех других задействованных элементов, которые по умолчанию постепенно исчезают. В случае сложных инцидентов, которые развиваются с течением времени, на графике отображается каждый этап атаки.



Поэтапная атака

График включает параметры фильтрации, которые позволяют настраивать график инцидентов для улучшения визуализации, функций навигации по карте инцидентов и панели с подробной информацией о каждом элементе.



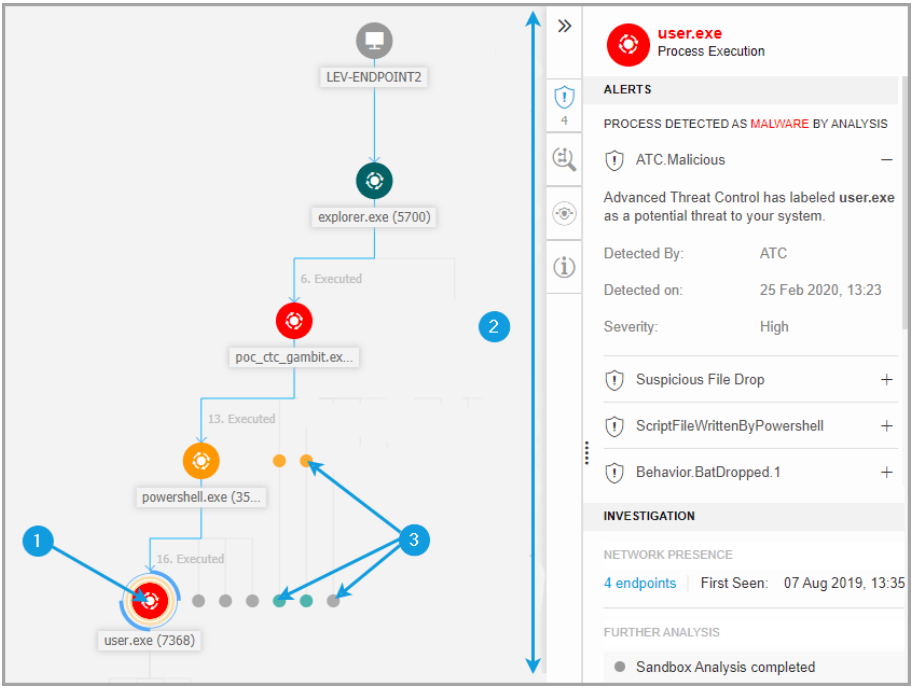
Вкладка «График»

1. Критический путь
2. Меню фильтров
3. Меню навигатора
4. Панель сведений об узле

Критический путь

Критический путь - это последовательность связанных событий безопасности, которые привели к отправке предупреждения, начиная с точки входа в сеть и заканчивая узлом события, который вызвал инцидент. Критический путь инцидента по умолчанию выделяется на графике вместе со всеми содержащимися на нем узлами событий, в то время как остальные элементы свернуты.

Триггерный узел легко выделяется на фоне остальных элементов графика, будучи окруженным дополнительными выделенными элементами (двумя оранжевыми кружками), и по умолчанию рядом с графиком инцидента отображается связанная информационная панель, предоставляя подробную информацию о триггерном узле.



Критический путь

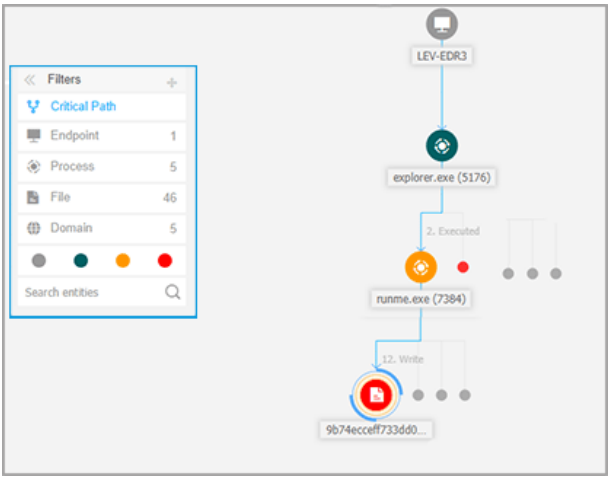
1. Триггерный узел
2. Панель сведений об узле с информацией, сгруппированной по категориям и разворачивающимся разделам
3. Постепенно исчезающие узлы, косвенно вовлеченные в инцидент

Примечание
Щелчок по любому другому элементу, кроме триггерного узла, нарушит критический путь и выделит путь к источнику, от выбранного узла выше до узла конечной точки.

Фильтры

Меню **Фильтры** предоставляет вам расширенные возможности фильтрации, позволяя полностью управлять графиком инцидента, выделяя элементы на основе их типа или релевантности, или скрывая их, чтобы сделать инцидент более компактным и простым для анализа.

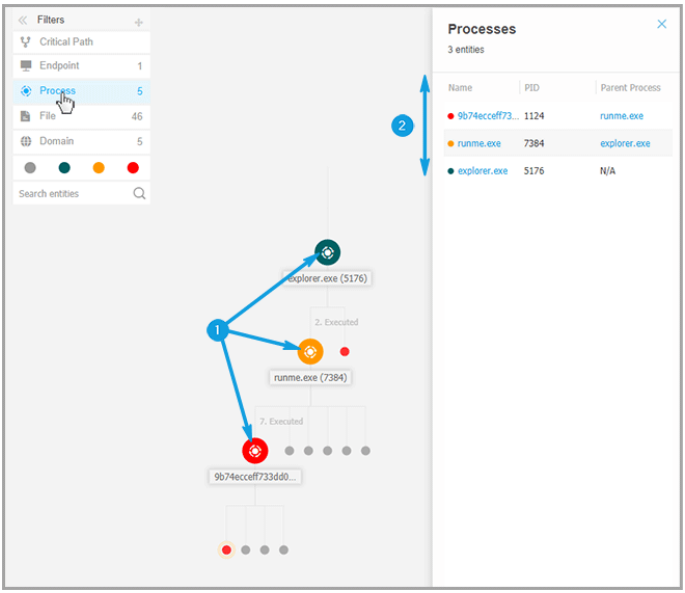
Нажмите и удерживайте значок **Перетащить**, чтобы расположить плавающую панель Фильтры в любом месте внутри графика инцидентов.



Фильтры графика инцидентов

При выборе фильтра типа элемента:

1. График инцидента сжимает и выделяет все элементы выбранного типа, в то время как элементы другого типа исчезают.
2. Он мгновенно открывает панель со списком всех выделенных элементов.



Примечание
Выбор элемента в отображаемом списке выделит его на графике инцидента и откроет панель сведений с информацией по этому элементу.
Только один фильтр может быть применен одновременно.

Параметры фильтрации включают в себя:

- **Критический путь**. Выделяет критический путь инцидента.
- **Конечная точка**. Выделяет конечные точки, затронутые инцидентом.
- **Процесс**: выделяет все узлы процессного типа, связанные с инцидентом.
- **Файл**. Выделяет узлы файлового типа, связанные с инцидентом.
- **Домен**. Выделяет все узлы доменного типа, связанные с инцидентом.
- **Реестр**. Выделяет все узлы реестрового типа, связанные с инцидентом.

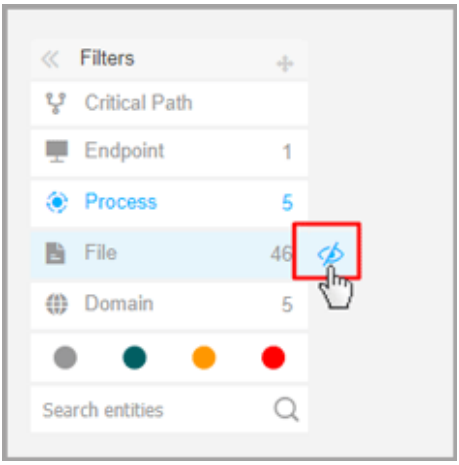
- **Релевантность элементов**. Вы также можете фильтровать элементы по их важности внутри инцидента.
  - **Нейтральный узел**: элементы без прямого воздействия на инцидент безопасности.
  - **Важный узел**: элементы с важной ролью в инциденте безопасности.
  - **Исходный узел**: Точка входа в атаку внутри сети.
  - **Подозрительный узел**: элементы с подозрительным поведением, напрямую связанные с инцидентом безопасности.
  - **Вредоносный узел**: элементы, которые нанесли ущерб вашей сети.

  Примечание
  Наведение курсора на любой из цветных фильтров отображает, какое количество элементов с одинаковой релевантностью вовлечено в инцидент.

- **Поиск объектов**. Вы можете искать имена или расширения файлов компонентов инцидента в поле поиска, и результаты будут отображаться на боковой панели.

Если фильтры не выбраны, график инцидентов сбрасывается до умолчания, при этом элементы конечной точки, источника и триггера подсвечиваются, а остальные элементы постепенно исчезают.

Вы также можете скрыть определенные элементы из графика инцидентов, нажав кнопку **Показать / Скрыть**, отображаемую при наведении указателя мыши на фильтры типа: Файл, Домен и Реестр.



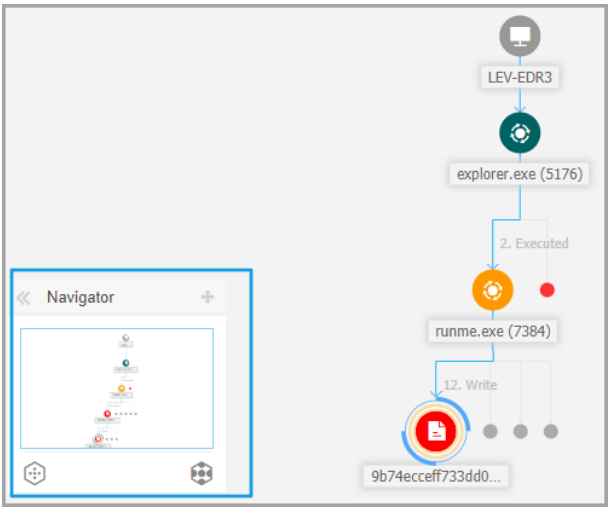
Скрытие типа элемента перерисовывает график инцидентов, удаляя все соответствующие элементы, даже если они сжаты, исключая триггерный узел и узлы с дочерними элементами.

Навигатор

Навигатор позволяет быстро перемещаться по графику инцидентов и исследовать все отображаемые элементы с помощью мини-карты и различных уровней визуализации.

Нажмите и удерживайте значок ✥ **Перетащить**, чтобы расположить плавающую панель Навигатор в любом месте внутри графика инцидентов.

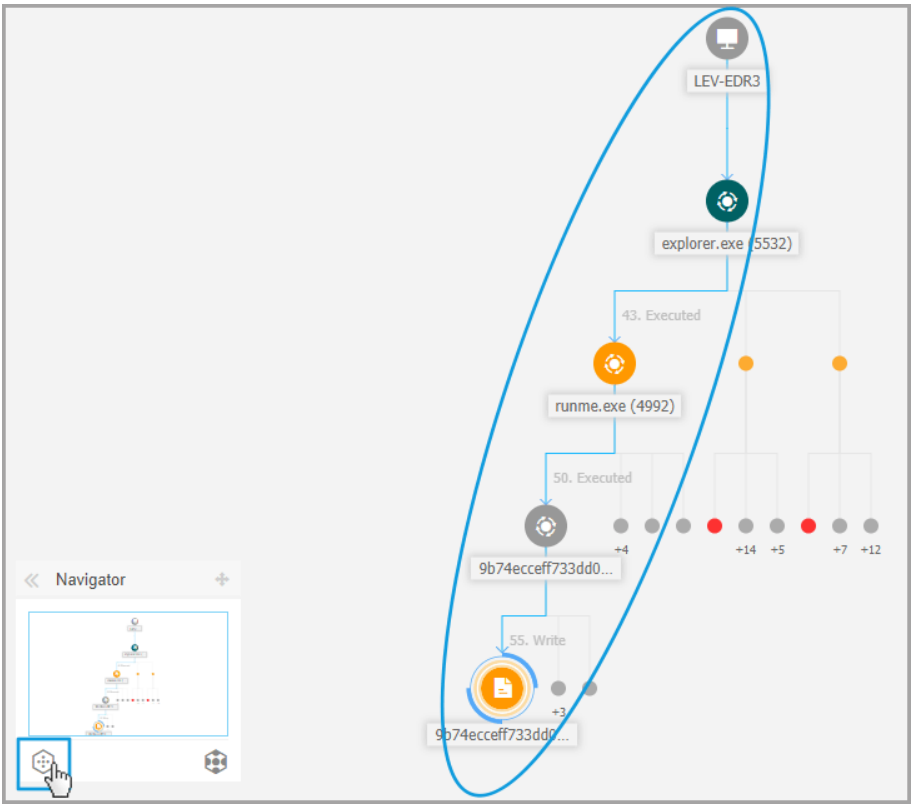
Навигатор свернут по умолчанию. При его расширении в меню будет отображаться миниатюрная версия всей карты инцидентов и кнопки действий для настройки уровня визуализации.



Навигатор

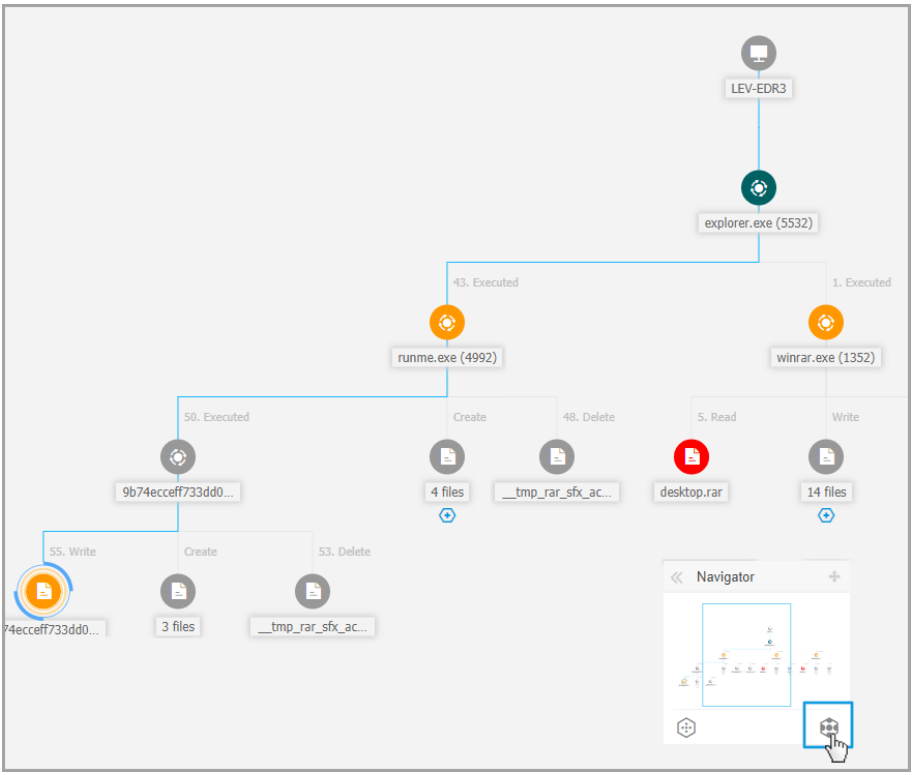
Меню **Навигатор** содержит две кнопки действий для настройки визуализации графика инцидентов: кнопка **Скрыть детали** и кнопка **Подробнее**.

Когда вы нажимаете кнопку **Меньше деталей**, график устанавливается в состояние по умолчанию, выделяя только критический путь инцидента.



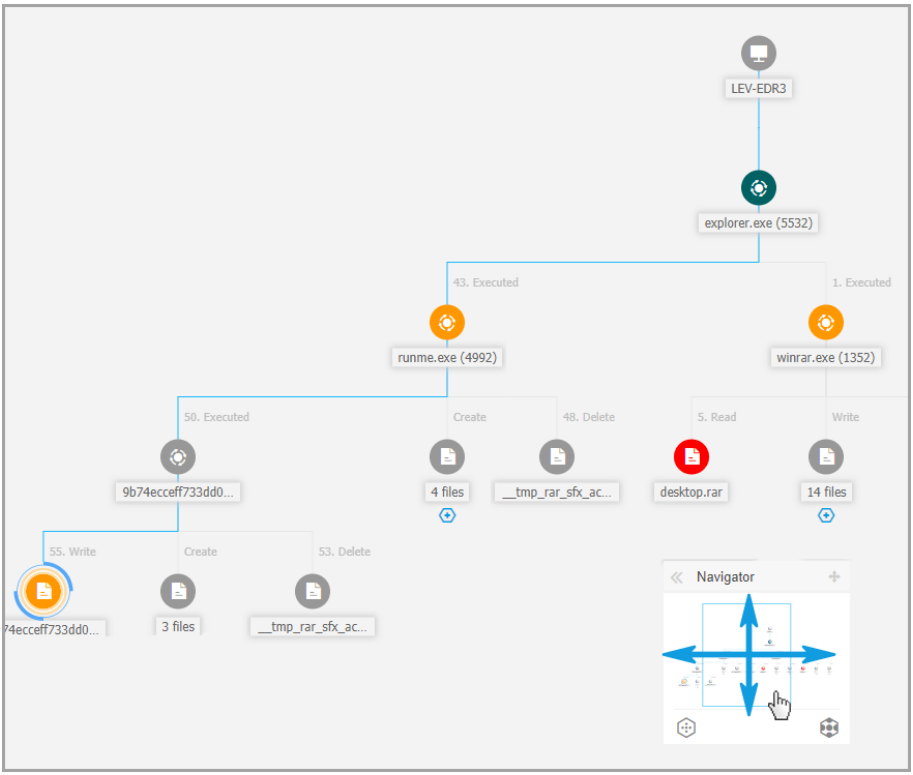
Обзорная визуализация

Когда вы нажмете кнопку **Подробнее**, все элементы графика инцидентов раскрываются, выделяя каждый узел и кластеры узлов.



Увеличенная визуализация

Когда инцидент увеличен и все элементы выделены, график часто может выходить за пределы экрана. В этом случае удерживайте и перетащите селектор карты на мини-карте навигатора, чтобы легко перемещаться в нужную область карты инцидентов, или просто перетащите область графика в нужное направление.

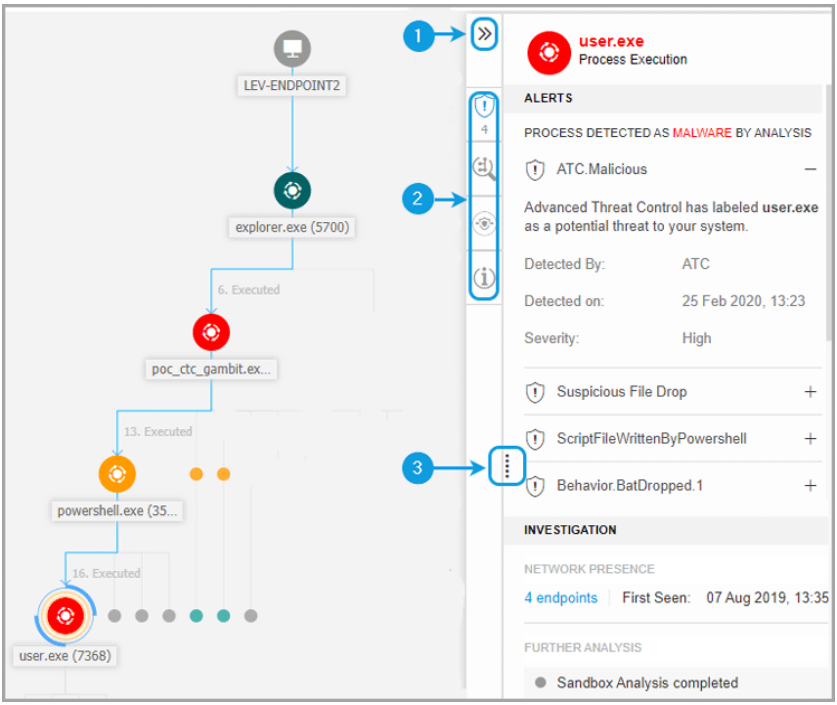


Селектор мини-карты

Сведения об узле

Панель **Сведения об узле** содержит разделы с подробной информацией о выбранном узле, включая действия по предотвращению или исправлению, которые можно предпринять для смягчения инцидента, подробности о типе обнаружения и обнаруженных оповещениях на узле, присутствии в сети, подробностях выполнения процесса, дополнительных рекомендациях по управлению событием безопасности или действиях для дальнейшего исследования элемента.

Чтобы просмотреть эту информацию и выполнить действия на панели, выберите узел на карте событий безопасности.



Панель сведений об узле

1. Вы можете свернуть или развернуть панель **Сведения об узле**, нажав кнопку **Свернуть**.
2. Вы можете легко ориентироваться в информации, отображаемой на панели **Сведения об узле**, щелкая иконки каждой из четырех основных категорий:
   - **ОПОВЕЩЕНИЯ**

     В этом разделе отображаются одно или несколько обнаружений, спровоцированных на выбранном узле, включая сведения о технологии Bitdefender, включившей элемент в инцидент, причину, по которой было спровоцировавшую обнаружение, имя обнаружения и дату, когда он был обнаружен.
   - **Исследование**

В этом разделе отображаются метки даты для начального обнаружения и все конечные точки, где был обнаружен этот элемент.

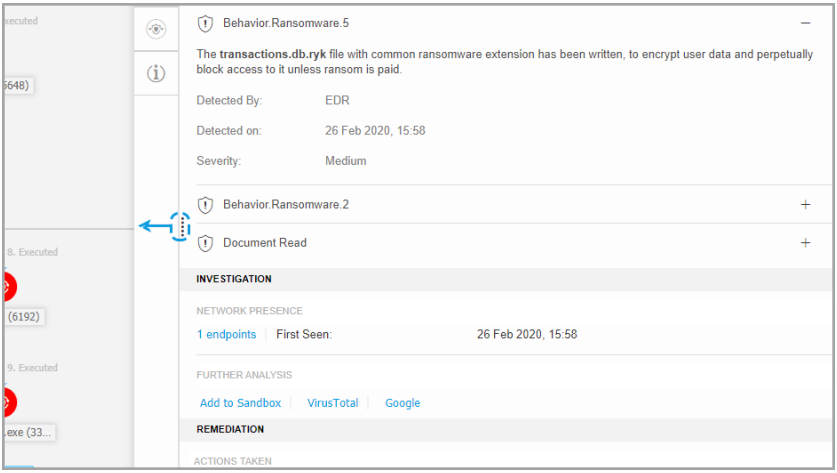
- **Исправление**

  В этом разделе отображаются действия, автоматически выполненные GravityZone, действия, которые вы можете предпринять немедленно для уменьшения угрозы, а также подробные рекомендации для каждого предупреждения, обнаруженного на выбранном узле, чтобы помочь вам в смягчении инцидента и повышении уровня безопасности вашей среды.

- **ИНФОРМАЦИЯ**

  В этом разделе отображается общая информация о каждом файле и конкретная информация в зависимости от типа выбранного узла.

3. Вы можете перетащить панель **Сведения об узле** по направлению к центру экрана, чтобы легко просмотреть его содержимое.



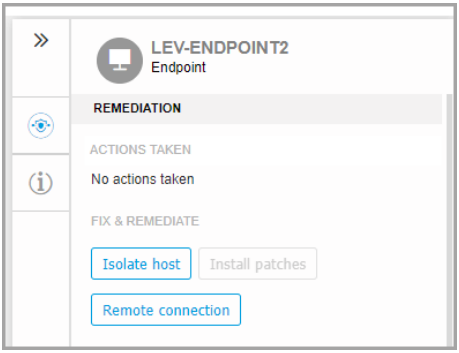
Расширенная панель

Панель сведений для узлов конечных точек

Панель **Сведения об узле** для конечных точек включает две категории:

- **Исправление**

Отображает информацию о действиях, автоматически предпринятых GravityZone для уменьшения угроз и действий, которые вы можете совершить:



– **Изолировать хост** - используйте это действие, чтобы изолировать конечную точку от сети.

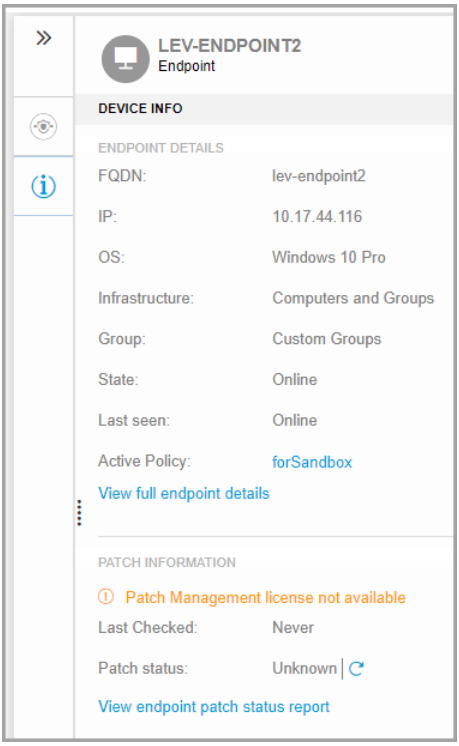
– **Установить патчи** - используйте это действие для установки отсутствующего патча безопасности на целевой конечной точке. Эта опция видна только с модулем Patch Management, надстройкой, доступной с отдельным лицензионным ключом. Обратитесь к Установке патча для получения дополнительной информации.

– **Remote Connection** - используйте это действие, чтобы установить удаленное подключение к конечной точке, участвующей в текущем инциденте, и выполнить ряд пользовательских команд оболочки напрямую в своей операционной системе для немедленного смягчения угрозы или сбора данных для дальнейшего расследования.

  При нажатии на эту кнопку отобразится окно Удаленное подключение.

- **ИНФОРМАЦИЯ ОБ УСТРОЙСТВЕ**

  Отображает общую информацию о затронутой конечной точке, такую как имя конечной точки, IP-адрес, операционная система, соответствующая группа, состояние, активные политики и ссылка, которая открывает новое окно, в котором отображаются полные сведения о конечной точке.



Также предоставляет вам такую информацию, как количество установленных исправлений, неисправных исправлений или отсутствующих исправлений по безопасности и не по безопасности. Кроме того, вы можете создать отчет о состоянии исправления конечной точки. Этот раздел предоставляется по запросу для целевой конечной точки.

На панели можно выполнить следующие действия:

– Просмотреть информацию об исправлениях для целевой конечной точки. Чтобы просмотреть сведения о патче, нажмите **Обновить** в этом разделе.

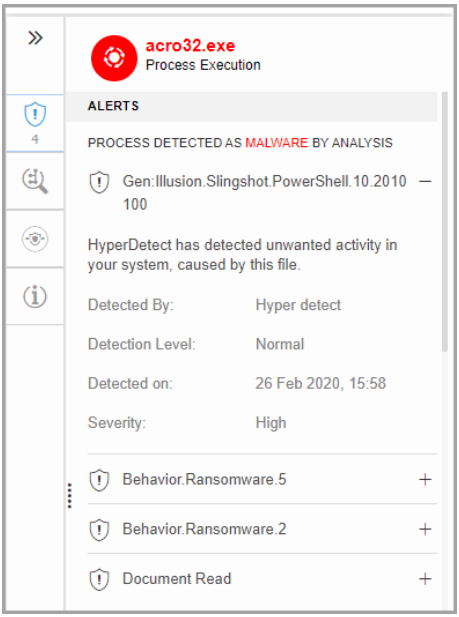
– Просмотреть отчет о состоянии исправления для целевой конечной точки. Чтобы сформировать отчет, нажмите **Просмотреть отчет о состоянии исправлений конечной точки**.

Панель сведений для узлов процесса

Панель **Сведения об узле** для узлов процесса включает четыре категории:

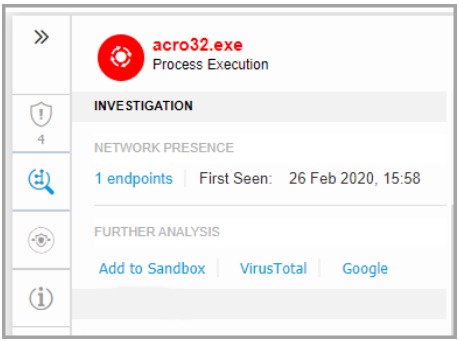
- **ОПОВЕЩЕНИЯ**

  Отображает одно или несколько обнаружений, инициированных на выбранном узле, включая сведения о технологии Bitdefender, которая включила этот элемент в инцидент, причину, по которой было инициировано обнаружение, имя обнаружения и дату, когда оно было обнаружено. Описание каждого предупреждения соответствует последним стандартам MITRE.

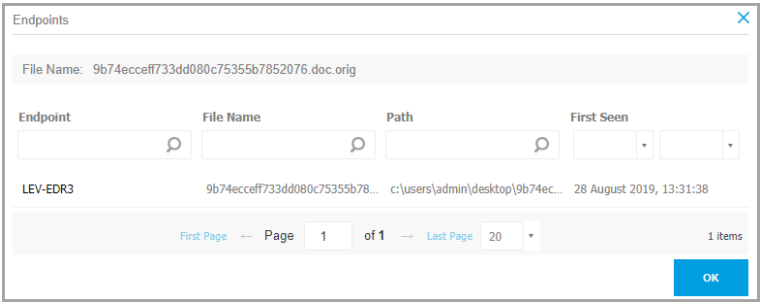


- **Исследование**

  Отображает метки даты для начального обнаружения и все конечные точки, где был обнаружен этот элемент.



Чтобы просмотреть этот список, щелкните число, указанное в поле **конечных точек**, и появится новое окно.

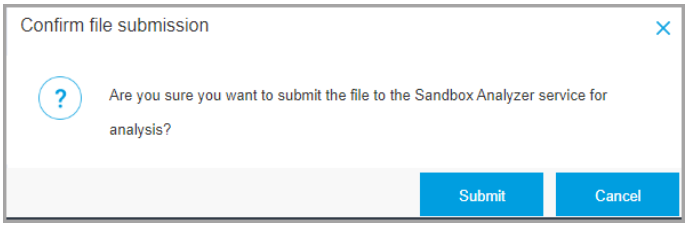


В этом разделе также представлен внешний анализ с помощью внутренних компонентов и сторонних решений.

Доступны следующие действия:

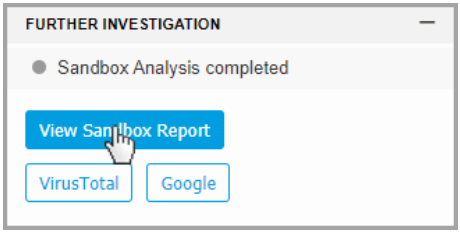
– **Добавить в песочницу** - используйте это действие для создания отчета Sandbox Analyzer.

  Выбор **Добавить в песочницу** предложит вам экран для подтверждения отправки файла.



После подтверждения вы будете автоматически перенаправлены к экрану представления.

По завершении анализа нажмите кнопку **Просмотреть отчет песочницы**, чтобы открыть полный отчет.

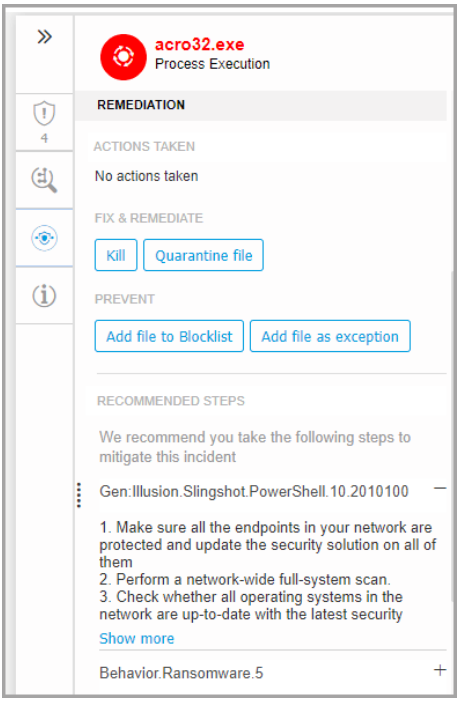


– **VirusTotal** - используйте это действие для внешней отправки файла на анализ.

– **Google** - используйте это действие для поиска хеш-значения файла.

- **Исправление**

  Отображает информацию о действиях, автоматически предпринятых GravityZone для уменьшения угроз и действий, которые вы можете совершить:



– **Завершить процесс** - используйте это действие, чтобы остановить выполнение процесса. Это действие создает задачу уничтожения процесса, видимую в панели выполнения процесса. `Процессы System32` и Bitdefender исключены из этого действия.

– **Файл карантина** - используйте это действие, чтобы сохранить рассматриваемый элемент и предотвратить размещение им полезных данных. Это действие требует, чтобы модуль брандмауэра был установлен на целевой конечной точке.

– **Добавить файл в Черный список** - управлять заблокированными элементами в разделе Черный список.

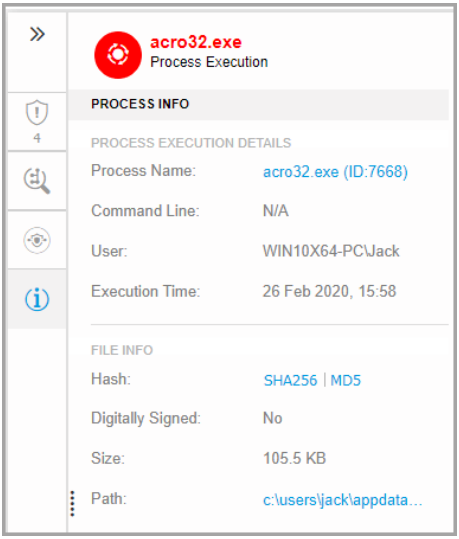
– **Добавить файл как исключение** - используйте эту опцию, чтобы исключить законную активность в определенной политике. Когда вы выбираете это действие, окно конфигурации предлагает вам выбрать

политику, в которую вы хотите добавить исключение. Управляйте исключениями в **Политика > Антивредоносное > Настройки**.

В данном разделе также содержится подробные рекомендации для каждого оповещения, обнаруженного на выбранном узле, чтобы помочь Вам смягчить инцидент и повысить уровень безопасности Вашей среды.

- **ИНФОРМАЦИЯ О ПРОЦЕССЕ**

  Отображает сведения о выбранном узле процесса, включая имя процесса, выполненную командную строку, пользователя, время выполнения, происхождение и путь файла, значение хеша, или цифровую подпись.



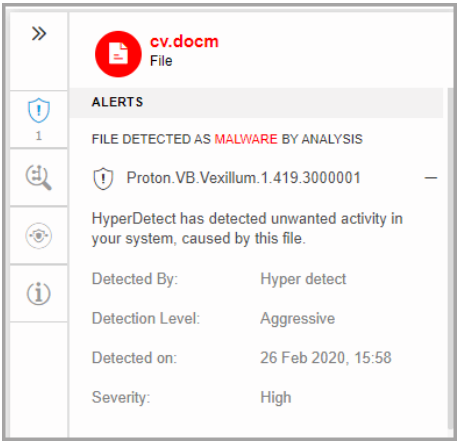
  Вы можете скопировать значение хеша в буфер обмена, щелкнув доступные алгоритмы хеширования в поле **Хэш**, а затем **Копировать в буфер обмена** и использовать его для добавления значения хэша файла в **Черный список**. Для получения дополнительной информации см. **Занесение файлов в Черный список** .

Панель сведений для файловых узлов

Панель **Сведения об узле** для файловых узлов включает четыре категории:

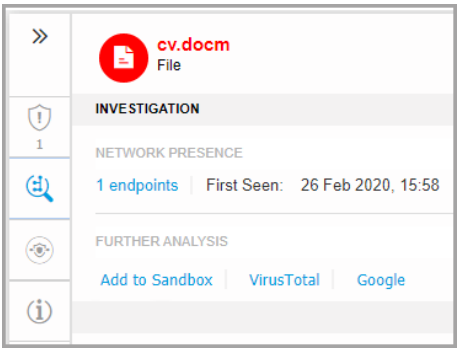
- **ОПОВЕЩЕНИЯ**

Отображает одно или несколько обнаружений, инициированных на выбранном узле, включая сведения о технологии Bitdefender, которая включила этот элемент в инцидент, причину, по которой было инициировано обнаружение, имя обнаружения и дату, когда оно было обнаружено. Описание каждого предупреждения соответствует последним стандартам MITRE.

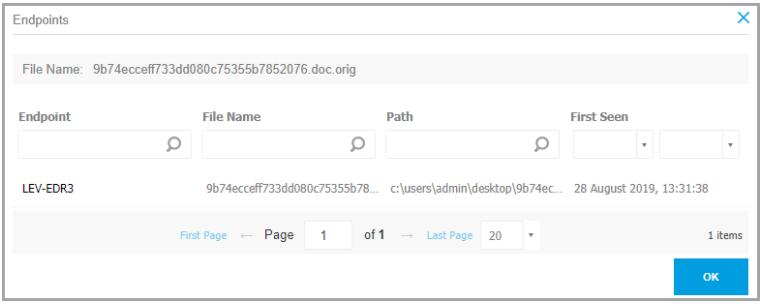


- **Исследование**

  Отображает метки даты для начального обнаружения и все конечные точки, где был обнаружен этот элемент.



Чтобы просмотреть этот список, щелкните число, указанное в поле **конечных точек**, и появится новое окно.

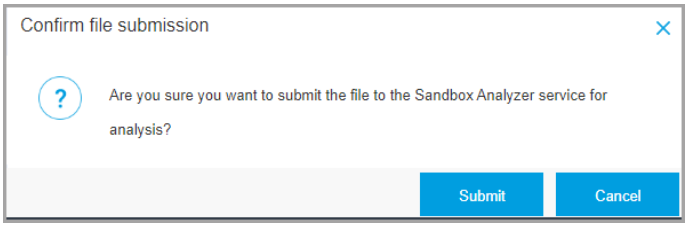


В этом разделе также представлен внешний анализ с помощью внутренних компонентов и сторонних решений.

Доступны следующие действия:

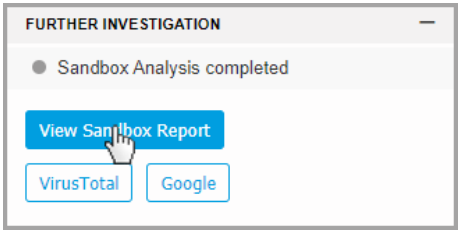
– **Добавить в песочницу** - используйте это действие для создания отчета Sandbox Analyzer.

  Выбор **Добавить в песочницу** предложит вам экран для подтверждения отправки файла.



После подтверждения вы будете автоматически перенаправлены к экрану представления.

По завершении анализа нажмите кнопку **Просмотреть отчет песочницы**, чтобы открыть полный отчет.

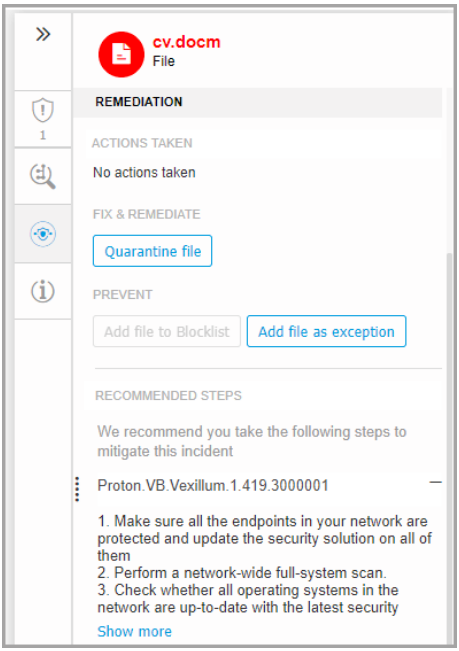


– **VirusTotal** - используйте это действие для внешней отправки файла на анализ.

– **Google** - используйте это действие для поиска хеш-значения файла.

- **Исправление**

  Отображает информацию о действиях, автоматически предпринятых GravityZone для уменьшения угроз и действий, которые вы можете совершить:



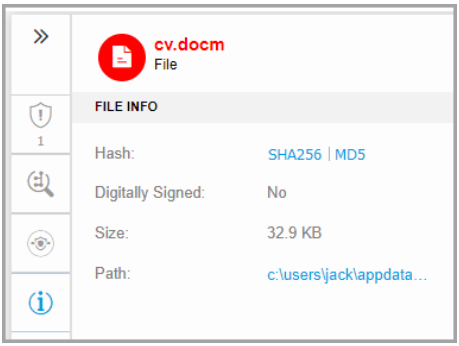
– **Добавить файл в Черный список** - управлять заблокированными элементами в разделе Черный список.

– **Добавить файл как исключение** - используйте эту опцию, чтобы исключить законную активность в определенной политике. Когда вы выбираете это действие, окно конфигурации предлагает вам выбрать политику, в которую вы хотите добавить исключение. Управляйте исключениями в **Политика > Антивредоносное > Настройки**.

В данном разделе также содержится подробные рекомендации для каждого оповещения, обнаруженного на выбранном узле, чтобы помочь Вам смягчить инцидент и повысить уровень безопасности Вашей среды.

- **Информация о файле**

  Отображает сведения о выбранном файловом узле, включая происхождение и путь к файлу, значение хеша, или цифровую подпись.



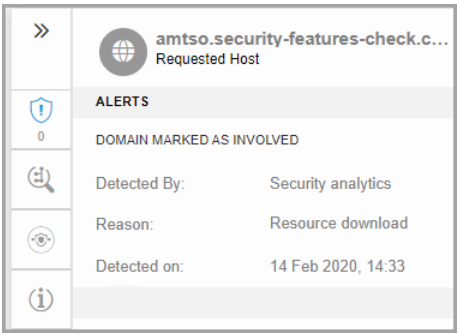
Вы можете скопировать значение хеша в буфер обмена, щелкнув доступные алгоритмы хеширования в поле **Хэш**, а затем **Копировать в буфер обмена** и использовать его для добавления значения хэша файла в **Черный список**. Для получения дополнительной информации см. **Занесение файлов в Черный список** .

Панель сведений для узлов домена

Панель **Сведения об узле** для узлов домена включает четыре категории:

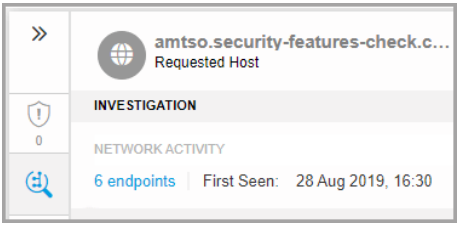
- **ОПОВЕЩЕНИЯ**

  Отображает серьезность домена, отмеченную технологией Bitdefender, которая включала эту сущность в инцидент, причину, которая вызвала обнаружение, и дату, когда она была обнаружена.

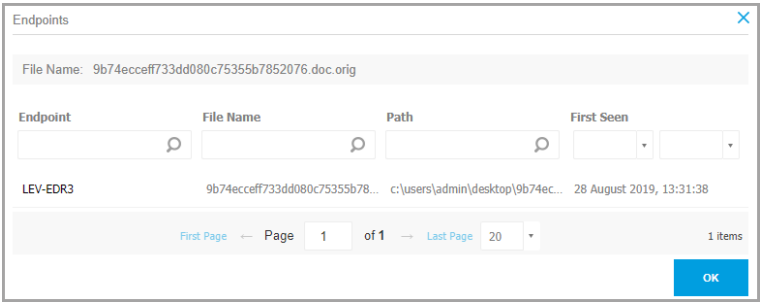


- **Исследование**

  Отображает метки даты для начального обнаружения и все конечные точки, где был обнаружен этот элемент.

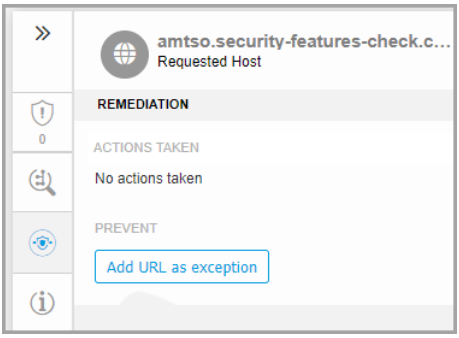


Чтобы просмотреть этот список, щелкните число, указанное в поле **конечных точек**, и появится новое окно.



- **Исправление**

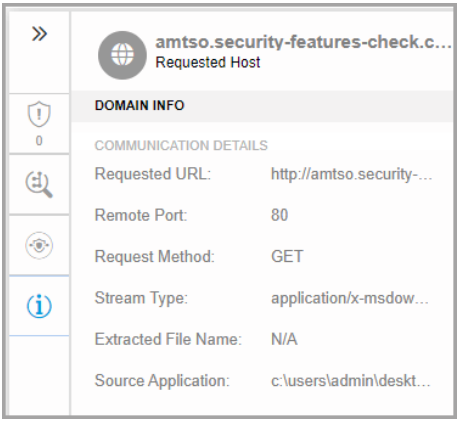
  Отображает информацию о действиях, автоматически предпринятых GravityZone для уменьшения угроз и действий, которые вы можете совершить:



– **Добавить URL как исключение** - используйте эту опцию, чтобы исключить законную активность в определенной политике. Когда вы выбираете это действие, окно конфигурации предлагает вам выбрать политику, в которую вы хотите добавить исключение. Управляйте исключениями в **Политика > Антивредоносное > Настройки**.

- **ИНФОРМАЦИЯ О ДОМЕНЕ**

  Отображает сведения о выбранном узле домена, включая запрошенный URL-адрес, используемый порт, метод запроса, тип потока, имя извлеченного файла, исходное приложение.

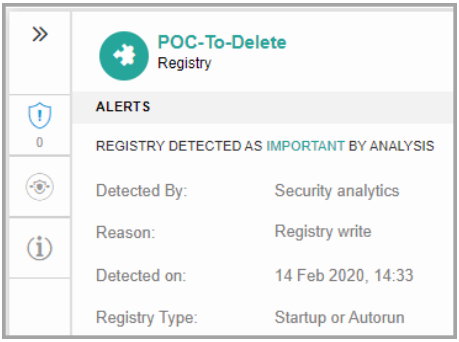


Панель сведений для узлов реестра

Панель **Сведения об узле** для узлов реестра включает три категории:

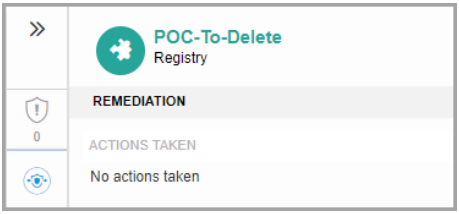
- **ОПОВЕЩЕНИЯ**

  Отображает степень серьезности манипулирования реестром, отмеченную технологией Bitdefender, которая включала эту сущность в инцидент, причину, которая вызвала обнаружение, дату, когда оно было обнаружено, и тип реестра.



- **Исправление**

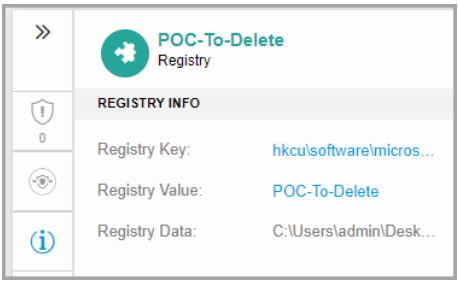
  Отображает информацию о действиях, выполненных автоматически GravityZone.



  Раздел **ИСПРАВЛЕНИЕ** для узлов реестра не предоставляет никаких опций пользовательских действий.

- **ИНФОРМАЦИЯ О РЕЕСТРЕ**

Отображает подробную информацию о выбранном узле реестра, включая ключ реестра, значение и данные.

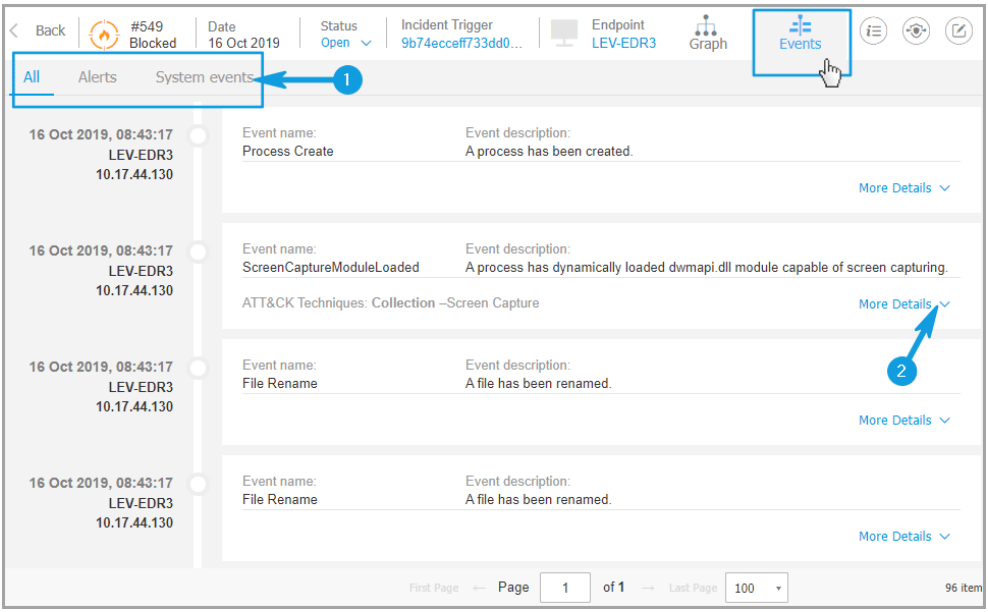


Вы можете щелкнуть ключ реестра и значение, чтобы скопировать его в буфер обмена для дальнейшего анализа.

События (Events)

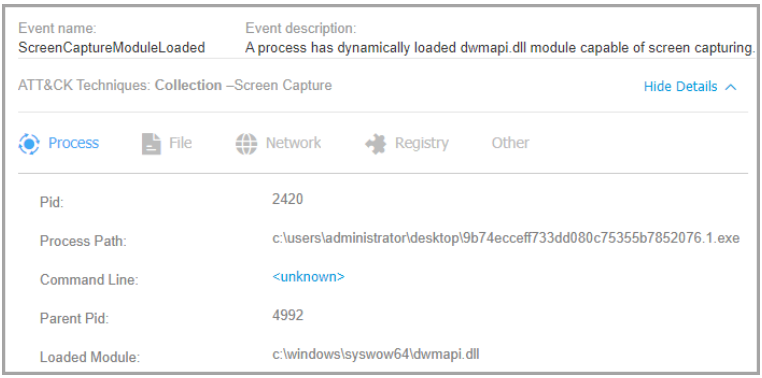
Используйте вкладку **События**, чтобы увидеть, как разворачивалась последовательность событий, спровоцировавшая расследуемый инцидент. В этом окне отображаются коррелированные системные события и предупреждения, обнаруженные с помощью технологий GravityZone, таких как Network Attack Defense, Anomaly Detection (обнаружение аномалий), Advanced Anti-Exploit (расширенная защита от эксплойтов), Windows Antimalware Scan Interface (AMSI) (интерфейс сканирования вредоносных программ Windows).

Каждое сложное событие имеет подробное описание, объясняющее, что было обнаружено и что может произойти, если артефакт используется в злонамеренных целях в соответствии с новейшими технологиями и тактиками MITRE.



Вкладка «События»

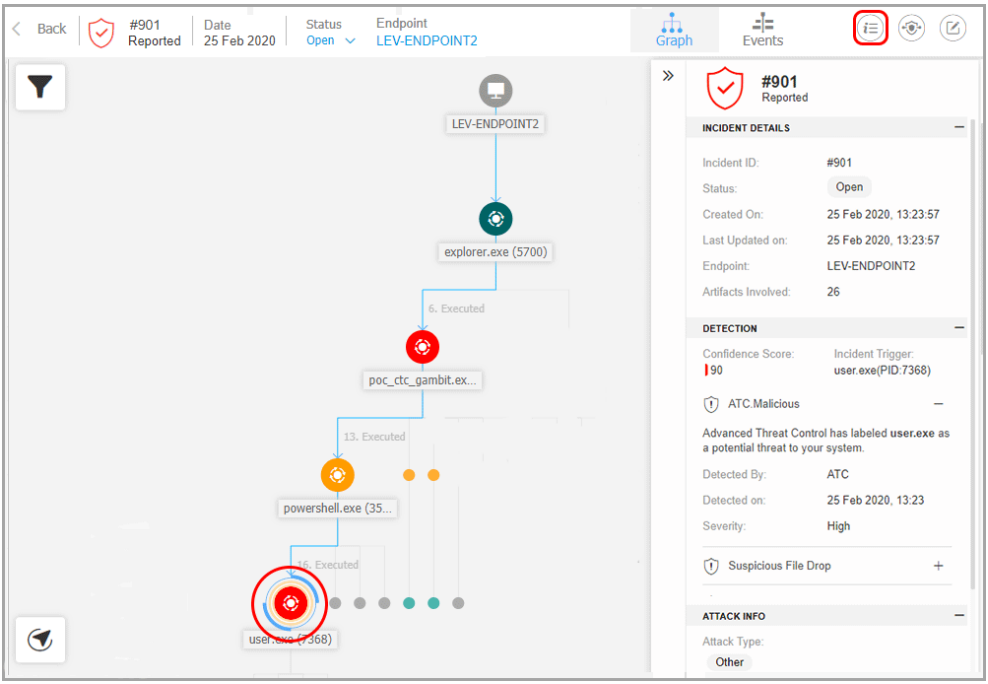
1. Используйте параметры фильтрации для отображения всех событий или только системных событий или сложных событий (предупреждений).
2. Нажмите кнопку **Подробнее**, чтобы развернуть каждое событие и получить доступ к дополнительной информации.



Сведения об инциденте

Эта панель содержит сворачиваемую область с такими деталями, как идентификатор инцидента, текущее состояние, время и дата его создания и последнего обновления, количество задействованных артефактов, имя триггера, описание и информация об атаке.

В этом разделе Вы можете получить доступ к расширенному инциденту, включающему в себя произошедшее на конечных точках, как пример.

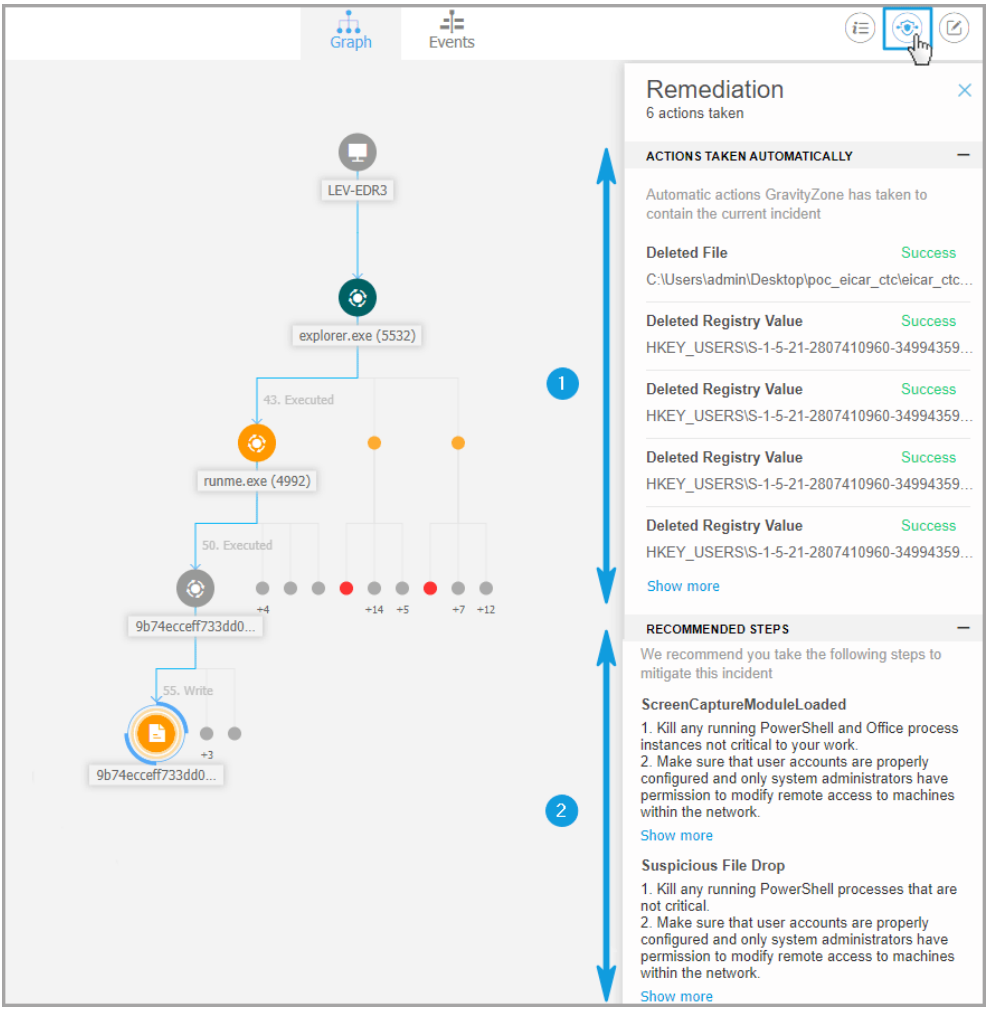


Панель сведений об инцидентах

Панель также содержит предупреждения, обнаруженные на элементе, который спровоцировал инцидент.

Восстановление

Панель **Исправление** предоставляет вам полезную информацию о том, какие корректирующие действия были предприняты GravityZone автоматически в случае атак, заблокированных такими технологиями, как Advanced Threat Control (ATC), HyperDetect, Antimalware, а также рекомендуемые действия, которые вы можете выполнить, чтобы смягчить инцидент и повысить уровень безопасности вашей системы.



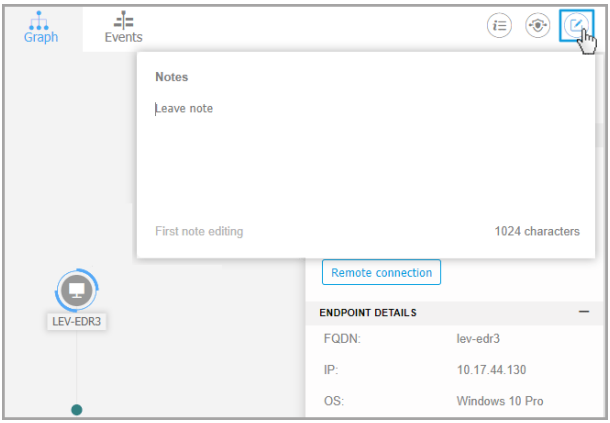
Панель исправления

1. Действия, выполняемые автоматически GravityZone.
2. Рекомендации по дальнейшему смягчению инцидента и повышению безопасности.

Примечание
Рекомендуемые шаги соответствуют предупреждениям, обнаруженным на узле, который вызвал расследуемый инцидент.

Примечания

В разделе **Заметки** можно добавить заметку для отслеживания последних изменений и упрощения смены владельца инцидента.

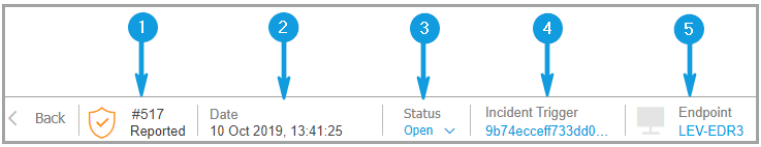


Заметки буфера обмена

1. Чтобы оставить заметку для текущего события, нажмите кнопку **Заметки** , чтобы открыть новое окно.
2. Введите ваше сообщение в этом окне (максимум 2048 символа).

Панель статуса инцидента

Строка статуса инцидента содержит теги событий безопасности, которые могут помочь вам обнаружить ключевую информацию о задействованных конечных точках сети.



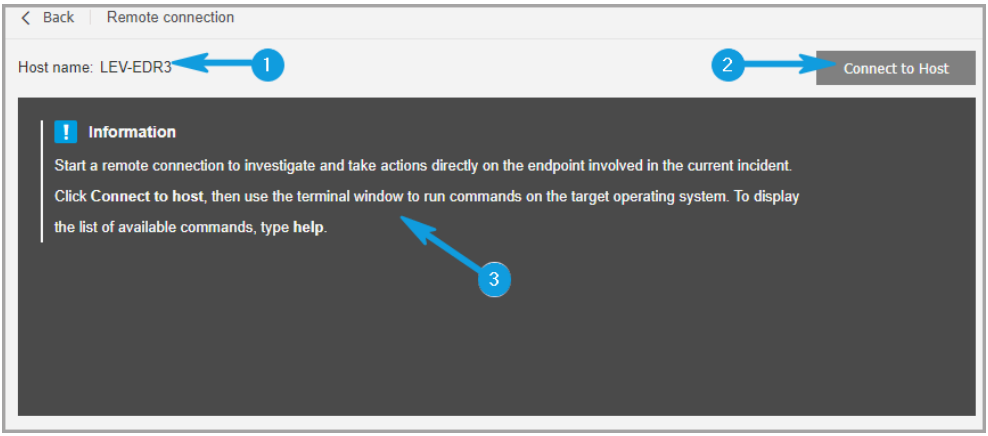
Панель статуса инцидента

1. Идентификатор инцидента - идентификационный номер расследуемого инцидента, только для заблокированного и сообщенного инцидента.
2. Отметка времени обнаружения - дата и время, когда произошел инцидент.
3. Статус инцидента - текущий статус инцидента.
4. Триггер инцидента - имя элемента, который инициировал инцидент.
5. Конечная точка - имя целевой конечной точки.

Нажав кнопку **Назад**, вы вернетесь на главную страницу **Инцидентов** .

Удаленное подключение

Используйте эту вкладку, чтобы установить удаленное соединение с конечной точкой, участвующей в текущем инциденте, и выполнить ряд пользовательских команд оболочки напрямую в своей операционной системе для мгновенной отмены угрозы или сбора данных для дальнейшего расследования.



Вкладка «Удаленное подключение»

На вкладке **Удаленное подключение** содержатся следующие элементы:

1. Имя конечной точки, участвующей в текущем событии безопасности
2. Кнопка управления удаленным подключением (подключить / отключить)
3. Окно терминала

Предварительные условия терминальной сессии

- Версия агента Bitdefender, установленного на конечной точке, поддерживает функцию удаленного подключения.
- Конечная точка должна быть включена и подключена к сети.
- На конечной точке должна быть установлена ОС Windows.
- GravityZone может связываться с конечной точкой.
- Ваша учетная запись GravityZone должна иметь разрешения на управление целевой конечной точкой.

Создание удаленного соединения

Удаленное соединение работает следующим образом:

1. Начните сеанс в реальном времени, нажав кнопку **Подключиться к хосту** .

Состояние соединения будет отображаться рядом с именем конечной точки.

Если соединение не установлено, в окне терминала появится сообщение об ошибке.

Примечание
Вы можете открыть максимум пять терминальных сессий с одной и той же конечной точкой одновременно.

2. После подключения терминал отображает список доступных команд и их описание. Введите нужную команду в окне терминала и нажмите `Enter`.

   Чтобы узнать больше о команде, введите `help`, а затем имя команды (например, `help ps`).

3. Терминал отображает результат команды, когда команда выполнена успешно.

   Если конечной точке не удается завершить выполнение команды, команда будет сброшена.

   История команд записывается в окно терминала. Однако, Вы можете просмотреть ранее введенные команды, нажимая клавиши со стрелками.

4. Чтобы отключиться, нажмите кнопку **Завершить сессию**.

   Сеанс терминала истекает автоматически через пять минут бездействия.

   Навигация за пределами вкладки **Удаленное подключение** при подключении к конечной точке также завершит сеанс терминала.

Команды для сеанса терминала

EDR команды для сеанса терминала - это пользовательские команды, независимые от платформы и использующие общий синтаксис. Здесь и далее приведен список доступных команд, которые Вы можете использовать на конечных точках через сеанс терминала:

- `ps`
  - **Описание**: отображает информацию о состоянии запущенных процессов на выбранной конечной точке, такую как идентификатор процесса (PID), имя, путь или использование памяти.

  - **Синтаксис**: `ps`
  - **Псевдонимы**: `Список задач`
  - **Параметры**: -
- `kill`
  - **Описание**: Завершает работу процесса или приложения на выбранной конечной машине по его PID. Используйте команду `ps/tasklist` для сбора PID,
  - **Синтаксис**: `kill [PID]`
  - **Псевдонимы**: -
  - **Параметры**: `[PID]` - идентификатор процесса на выбранной конечной точке.
- `ls (dir)`
  - **Описание**: Отображает информацию о всех файлах и папках из указанного каталога, такую как имя, тип, размер и дату изменения. Позволяет подстановочным знакам указывать путь. Например:

    `C:\Users\admin\Desktop\s*` все содержимое папки Desktop начиная с "s"

    `C:\Users\publ??` перечисляет все содержимое по указанному пути, с любыми последними двумя буквами.
  - **Синтаксис**: `ls [path]`
  - **Псевдонимы**: `dir`
  - **Параметры**: `[Path]` - путь к файлу или папке на выбранной конечной точке.
- `rm (del, delete)`
  - **Описание**: Удаляет файлы и папки по указанному пути на выбранной конечной точке.
  - **Синтаксис**: `rm [path]`
  - **Псевдонимы**: `del/delete`

  - **Параметры**: `[Path]` - путь к файлу или папке на выбранной конечной точке.

- `reg query`
  - **Описание**: отображает всю информацию (имя, тип, значение) указанного пути к ключу реестра.
  - **Синтаксис**: `reg query [keypath] [/k] [keyname] [/v] [valuename]`
  - **Псевдонимы**: -
  - **Параметры**:
    - `keypath`- отображает всю информацию о ключах реестра по указанному пути.
    - `/k [keyname]` - фильтр отображает ключи реестра по указанному имени ключа. Также Вы можете использовать шаблоны (*,?) для фильтрации более широкого диапазона имён.
    - `/v [valuename]` - фильтр отображает значения реестра по указанному имени значения. Также Вы можете использовать подстановочные знаки (*,?) для фильтрации более широкого диапазона имён.

- `reg add`
  - **Описание**: добавляет новый ключ реестра или значение. Перезаписывает значение, если оно уже существует. При перезаписи данных реестра необходимо указать все определенные параметры.
  - **Синтаксис**: `reg add [keyname] [/v] [valuename] [/t] [datatype] [/d] [data]`
  - **Псевдонимы**: -
  - **Параметры**:
    - `[keyname]` - имя ключа реестра.
    - `/v [valuename]` - имя значения реестра. Также требует добавления параметра /d [data]

- `/t [datatype]` - тип данных значения реестра. Вы можете добавить один из следующих типов данных:

  `REG_SZ, REG_MULTI_SZ, REG_DWORD, REG_BINARY, REG_DWORD_LITTLE_ENDIAN, REG_LINK, REG_FULL_RESOURCE_DESCRIPTOR, REG_EXPAND_SZ`

  Если тип не указан явно, то тип `REG_SZ` назначается по умолчанию.

  Если тип установлен как `REG_BINARY`, данные реестра интерпретируются в шестнадцатеричном виде.

- `reg delete`
  - **Описание** : Удаляет ключ реестра или его значения.
  - **Синтаксис**:

    ```
    reg delete [keyname] [/v] [valuename]
    reg delete [keyname] [/va]
    ```

  - **Псевдонимы**: -
  - **Параметры**:

    `[keyname]` - удаляет ключ реестра и все его значения.

    `/v [valuename]` - удаляет указанное значение реестра.

    `/va` - удаляет все значения указанного раздела реестра.

- `cd`
  - **Описание** : Изменяет рабочий каталог согласно указанному пути. Данная команда в качестве параметра требует путь к диску или каталогу на целевой конечной машине
  - **Синтаксис**: `cd [path]`
  - **Псевдонимы**: -
  - **Параметры**: `[Path]` - путь к файлу или папке на выбранной конечной точке.

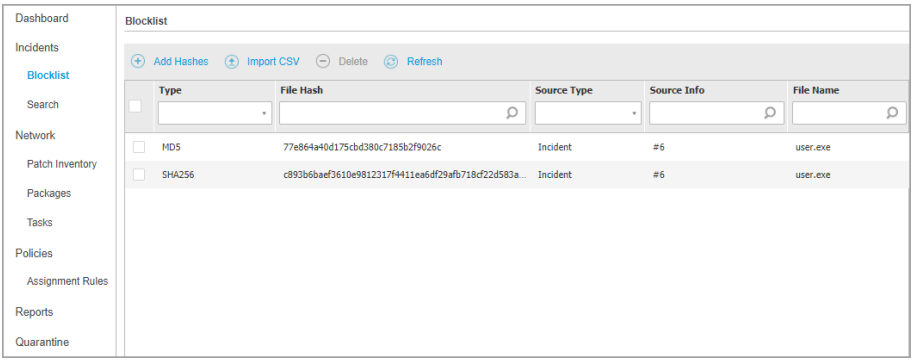
- `помощь`

- **Описание** : Без указания параметра, в справке перечисляются все доступные команды вместе с кратким описанием. При введении help с параметром, она отобразит полный синтаксис команды, краткое описание и пример использования.
- **Синтаксис**: `help [command]`
- **Псевдонимы**: -
- **Параметры**: имя команды (например: `cd, kill, ls, ps`)

- `clear (cls)`
  - **Описание** : Очищает окно консоли и показывает текущий рабочий каталог.
  - **Синтаксис**: `clear`
  - **Псевдонимы**: `cls`
  - **Параметры**: -

9.2. Занесение в черный список

На странице **Черный список** вы можете просмотреть и управлять компонентами в зависимости от хэш-значения. Просмотрите записи активности в Журнале активности пользователя .



Страница «Черный список»

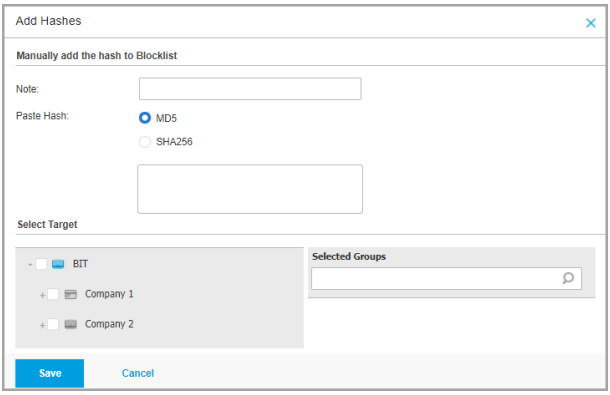
В таблице данных вы можете просмотреть следующие детали для каждого компонента:

- Типы файлов
  - MD5
  - SHA256
- Хэш-значение файлов
- Тип источника:
  - Инцидент
  - Импорт
  - Ручной режим
- Информация об источнике
- Имя файла
- Компания

Добавить хэш-значения к существующему Черному списку:

1. Скопировать хэш-значение из **Информация о файле**.
2. Выберите **MD5** или **SHA256** и вставьте значение в поле ниже.

   Если требуется, добавьте заметку.
3. Нажмите **Сохранить**.



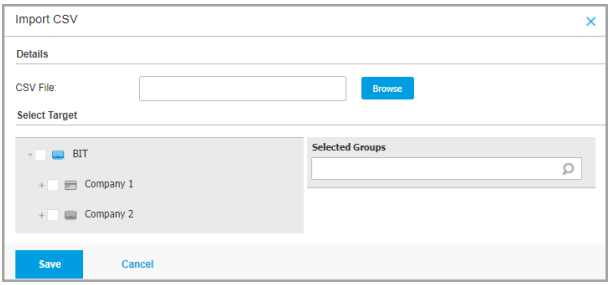
Добавить окно хэш-значения

Важно

Датчик инцидентов заблокирует любой двоичный файл, хеш-значение которого было добавлено в **Черный список**, от запуска процесса.

Импортировать записи хешей в существующий черный список. Чтобы импортировать файл CSV:

1. Нажмите **Импортировать CSV**.
2. Найдите файл CSV и нажмите **Сохранить** .



Окно импорта CSV

Вы также можете импортировать локальные файлы CSV со своего устройства на страницу **Черный список** , но сначала вы должны убедиться, что ваш CSV действителен.

Для создания действительного файла CSV для импорта, вы должны заполнить первые три столбца следующими данными:

1. Первый столбец CSV должен содержать тип хэша: `md5` или `sha256`.
2. Второй столбец должен содержать соответствующие шестнадцатеричные хеш-значения.
3. Третий столбец может содержать необязательную строковую информацию, относящуюся к столбцу **Подробности об источнике** на странице **Черный список**.

Примечание
Информация, соответствующая другим столбцам на странице **Черный список**, будет заполнена автоматически при импорте CSV файла.

10. ИСПОЛЬЗОВАНИЕ ОТЧЕТОВ

Control Center позволяет создавать и просматривать централизованные отчеты о состоянии безопасности управляемых сетевых объектов. Отчеты можно использовать для различных целей:

- Отслеживать и обеспечивать соблюдение политик безопасности предприятия.
- Проверять и оценивать статус безопасности сети.
- Выявлять проблемы безопасности сети, угрозы и уязвимости.
- Отслеживание инцидентов безопасности.
- Использовать функции управления высокого уровня с четким и удобным представлением данных о безопасности.

Доступно несколько различных типов отчетов, так что вы сможете легко получить необходимую информацию. Информация представлена в удобочитаемых интерактивных графиках и таблицах, что позволяет быстро проверить статус безопасности сети и выявить любые угрозы.

В отчетах можно объединить данные управляемых объектов всей сети или отдельных групп. Таким образом, в одном отчете будут содержатся следующие сведения:

- Статистические данные по всем группам управляемых объектов сети.
- Подробная информация по каждому управляемому объекту сети.
- Список компьютеров, которые отвечают определенным критериям (например, те, на которых отключена защита от вредоносных программ).

Некоторые отчеты также позволяют быстро исправить ошибки, найденные в сети. Например, вы можете легко обновить данные о всех выбранных сетевых объектах прямо из отчета, без необходимости переходить и запускать задачу обновления в разделе **Сеть**.

Все запланированные отчеты доступны в Control Center, но вы можете сохранить их на ваш компьютер или отправить по электронной почте.

Доступные форматы включают Portable Document Format (PDF) и comma-separated values (CSV).

10.1. Типы отчетов

Различные типы отчетов доступны по каждому типу конечных точек:

- Отчеты по компьютерам и виртуальным машинам
- Отчеты Exchange
- Отчеты по мобильным устройствам

10.1.1. Отчеты по компьютерам и виртуальным машинам

Следующие типы отчетов доступны для физических и виртуальных машин:

Антифишинговая активность

Информирует вас об активности антифишингового модуля Bitdefender Endpoint Security Tools. Вы можете просмотреть количество заблокированных фишинговых веб-сайтов на выбранных конечных устройствах и пользователей, которые были зафиксированы во время последнего обнаружения. Нажав на ссылку в колонке **Заблокированные сайты**, вы также сможете просмотреть URL веб-сайтов, сколько раз они были заблокированы и когда было последнее событие блокировки.

Заблокированные приложения

Информирует вас об активности следующих модулей: Защита от вредоносного ПО, Брандмауэр, Контроль контента, Контроль приложений, Advanced Anti-Exploit, ATC/IDS и HVI. Вы можете просмотреть количество заблокированных приложений на выбранных конечных точках и пользователей, которые были зарегистрированы во время последнего обнаружения.

Щелкните номер, связанный с целью, чтобы просмотреть дополнительную информацию о заблокированных приложениях, количестве произошедших событий и дате и времени последнего события блока.

На основании этого отчета вы можете быстро настроить модули защиты, чтобы разрешить выбранному приложению работать в конечной точке назначения:

- Нажмите кнопку **Добавить исключение**, чтобы определить исключения в следующих модулях: Защита от вредоносных программ, ATC, Управление контентом , брандмаузер и HVI. Появится окно подтверждения, уведомляющее о новом правиле, что приводит к изменению существующей политики для этой конкретной конечной точки.
- Нажмите кнопку **Добавить правило**, чтобы определить правило для приложения или процесса в Управлении приложениями. В окне конфигурации примените правило к существующей политике.

Сообщение проинформирует вас о том, что новое правило приведет к изменению политики, назначенной для определенной рабочей станции. В отчете также отображается количество попыток доступа, и то, работает ли модуль в тестовом режиме или в рабочем режиме.

Заблокированные веб-сайты

Информирует вас об активности модуля управления веб-доступом Bitdefender Endpoint Security Tools. Для каждого объекта вы можете просмотреть количество заблокированных веб-сайтов. Нажав на цифру вы можете просмотреть дополнительную информацию, например:

- URL веб-сайта и категория
- Количество попыток доступа на веб-сайт
- Дата и время последней попытки, а также пользователь, который был зафиксирован в момент обнаружения.
- Причина блокировки, которая включает в себя запланированный доступ, обнаружение вредоносных программ, категории фильтрации и черные списки.

Защита данных

Информирует вас об активности модуля защиты данных Bitdefender Endpoint Security Tools. Вы можете увидеть количество заблокированных сообщений электронной почты и веб-сайтов на выбранных конечных точках, а также пользователей, которые были зафиксированы во время последнего обнаружения.

Активность управления устройствами

Информирует вас о событиях, произошедших при доступе конечных точек через контролируемые устройства. Для каждой конечной точки вы можете просмотреть количество разрешенных / заблокированных попыток доступа и событий только для чтения. Если события произошли, то дополнительную информацию вы сможете получить, нажав на соответствующие цифры. Подробности содержат информацию о:

- Регистрации пользователя на машине
- Типе устройства и его ID
- Разработчике устройства и ID модели
- Дате и времени события.

Состояние шифрования конечных точек

Предоставляет вам данные о состоянии шифрования на конечных точках. Круговая диаграмма отображает количество систем отвечающих, и , соответственно, не отвечающих требованиям настройки политики шифрования.

Таблица ниже в виде круговой диаграммы предоставляет такие данные, как:

- Имя конечного пользователя.
- Полное доменное имя (FQDN).
- IP-адрес рабочей станции
- Операционная система.
- Согласование политики устройства:
  - **Совместимость** - когда все тома шифруются или незашифрованы в соответствии с политикой.
  - **Не совместимо** - когда статус томов не соответствует назначенной политике (например, зашифрован только один из двух томов или процесс шифрования выполняется на этом томе в текущий момент).
- Политика устройства (**Шифрование** или **Дешифровка**).
- Чтобы просмотреть информацию о томах каждой конечной точки кликайте цифры в столбце Общие данные по томам: идентификатор, имя, состояние шифрования (**Зашифровано** или **Незашифровано**), Проблемы, тип (**Загрузка** или **Не загружается**), размер, идентификатор ключа восстановления.

Состояние модулей конечной точки

Содержит обзор охвата модулей защиты по выбранным целям. В деталях отчета для каждого пользователя вы можете посмотреть, какие модули активны, отключены или не установлены, а также используемый механизм сканирования. При нажатии на имя конечного пользователя (компьютера) отображается окно **Информация** с информацией о конечном пользователе (компьютере) и установленных уровнях защиты.

Нажав кнопку **Реконфигурировать клиента**, Вы можете запустить задачу по изменению начальных настроек одной или нескольких выбранных конечных точек. Для получения большей информации перейдите по Настройка клиента.

Состояние защиты конечных точек

Предоставляет вам различную информацию о состоянии выбранных конечных точек в вашей сети.

- Состояние защиты от вредоносного ПО
- Состояние обновления Bitdefender Endpoint Security Tools
- Состояние сетевой активности (online/offline)
- Состояние управления

Вы можете применять фильтры по показаниям безопасности и состоянии, чтобы найти необходимую информацию.

Активность файрвола

Информирует вас об активности модуля файрвола Bitdefender Endpoint Security Tools. Вы можете увидеть количество блокировок трафика и блокировок сканирования портов на выбранных конечных точках, а также пользователей, которые были зафиксированы и обнаружены.

активность по обнаружению гипервизора

Информирует вас об активности модуля HyperDetect Bitdefender Endpoint Security Tools.

Диаграмма в верхней части страницы отчета показывает динамику попыток атаки за указанный период времени и их распределение по типу атаки. Перемещая курсор над элементами таблицы вы будете видеть соответствующий тип атаки в диаграмме. При нажатии на запись будет отображаться или скрываться соответствующая строка на диаграмме. Кликнув по любому параметру, вы отфильтруете данные таблицы в соответствии с выбранным параметром. Например, если вы нажмете любую точку на оранжевой линии, таблица отобразит только эксплойты.

В нижней части отчета будет отображаться информация о выявленных нарушениях в вашей сети и о том, были ли они рассмотрены. Они относятся к:

- Путь к вредоносному файлу или обнаруженному URL-адресу в случае зараженных файлов. Для атак, не содержащих файлы, назначается имя исполняемого файла, используемого в атаке, и ссылка на окно информации, в котором отображена причина обнаружения и вредоносная командная строка.
- Конечная точка, на которой было выполнено обнаружение

- Модуль защиты, который обнаружил угрозу. Поскольку Hyper Detect является дополнительным уровнем модулей Защиты от вредоносных программ и контента, в отчете появится только один из этих двух модулей, в зависимости от типа обнаружения.
- Тип предполагаемой атаки (целевая атака, нежелательная программа, эксплойты, программы-вымогатели, подозрительные файлы и сетевой трафик)
- Состояние угрозы
- Уровень защиты модуля, на котором обнаружена угроза (Рекомендуемый, Нормальный, Интенсивный)
- сколько раз была обнаружена угроза
- Последнее обнаружение
- Идентификация атаки в качестве не содержащей файлы (да или нет) для быстрой фильтрации обнаруженных атак.

Примечание
Файл может использоваться для различных типов атак. Поэтому GravityZone сообщает об этом для каждого типа атаки, в которой было принято участие.

На основе этого отчета вы можете с легкостью распознать ложные срабатывания, добавив исключения в назначенную политику безопасности. Для этого:

1. Выберите необходимое количество записей в таблице.

   Примечание
   В список исключений нельзя добавить обнаружение без файлов, в силу того, что обнаруженный исполняемый файл не является вредоносной программой, но может представлять угрозу при использовании вредоносной закодированной командной строки.

2. Нажмите кнопку **Добавить исключение** в верхней части таблицы.
3. В окне конфигурации выберите политики, к которым следует добавить исключение, и нажмите **Добавить** .

   Соответствующая информация для каждого добавленного исключения по умолчанию отправляется в Bitdefender Labs, чтобы помочь улучшить

возможности обнаружения продуктов Bitdefender. Вы можете управлять этим действием с помощью флажка **Отправить отзыв в Bitdefender для детального анализа** .

Если угроза была обнаружена модулем защиты от вредоносных программ, это исключение будет применяться как к режимам проверки доступа, так и по требованию.

Примечание
Данные исключения можно найти в следующих разделах выбранных политик: **Защита от вредоносных программ > настройки** для файлов и **Контроль контента > Трафик** для URL-адресов.

Состояние активности вредоносного ПО

Помогает вам узнать сколько и какие из выбранных конечных точек были затронуты вредоносным ПО в течении определенного периода времени и какие меры были приняты. Вы также можете просмотреть пользователя, который был зарегистрирован во время последнего обнаружения.

Конечные точки группируются по следующим критериям:

- Конечные точки без каких-либо срабатываний (вредоносные угрозы не были обнаружены за указанный период времени)
- Конечные точки, вылеченные от вредоносных программ (все обнаруженные файлы были успешно вылечены или перемещены в карантин)
- Конечные точки с неразрешенным вредоносным ПО (доступ к некоторым обнаруженным файлам запрещен)

Для каждой конечной точки, нажав ссылки, доступные в колонках результатов лечения, вы сможете просмотреть список угроз и путей к поврежденным файлам.

В этом отчете вы можете запустить задачу полной проверки для неразрешенных целей, нажав кнопку **Сканировать зараженные цели** в Панели инструментов над таблицей данных.

Отчет об инцидентах

Информирует вас о деятельности модуля Network Attack Defense. График отображает количество попыток атаки, обнаруженных за указанный интервал. Детали отчета включают в себя:

- Имя конечной точки, IP и полное доменное имя (FQDN)

- Имя пользователя
- Имя обнаружения
- Техника атаки
- Количество попыток
- IP-адрес атакующего
- Целевой IP и порт
- Когда была произведена ближайшая блокировка атаки

При нажатии кнопки **Добавить исключения** для выбранного обнаружения автоматически создается запись в **Глобальных исключениях** из раздела **Защита сети**.

Статус сетевого патча

Проверка статуса обновлений ПО, которое установлено в вашей сети. Отчет передает следующие детали:

- Целевой компьютер (имя конечной точки, IP и операционная система).
- Исправления безопасности (установленные исправления, сбойные исправления, отсутствующие исправления безопасности и исправления, не связанные с безопасностью).
- Состояние и время последнего изменения для проверенных конечных точек.

Состояние защиты сети

Содержит подробную информацию об общем состоянии безопасности выбранных конечных точек. Например, вы можете просмотреть информацию о:

- Имя, IP и FQDN
- Статус:
  - **Возникли проблемы** - конечная точка имеет уязвимости защиты (агент безопасности не обновлен, обнаружены угрозы безопасности и пр.)
  - **Проблем нет** - конечные точки защищены, и нет повода для беспокойства.
  - **Нет данных** - при создании отчета конечные точки недоступны.
  - **Неуправляемо** - агент безопасности пока еще не установлен на конечных точках.

- Доступные уровни защиты
- Управляемые и неуправляемые конечные точки (с установленными агентами безопасности и без)
- Статусе и типе лицензии (дополнительные столбцы, связанные с лицензиями, по умолчанию скрыты)
- Статус инфекции (очищена ли конечная точка)
- Состоянии обновления продукта и механизмов защиты
- Состоянии исправлений безопасности ПО (недостающие исправления связанные и не связанные с безопасностью)

Для неуправляемых конечных точек, в других столбцах вы увидите статус **Неуправляемый**

Сканирование по запросу

Предоставляет информацию о сканировании по запросу, проведенному на выбранных объектах. Круговая диаграмма будет отображать статистику успешных и неудачных проверок. Таблица под графиком будет содержать подробную информацию о типах сканирования, инцидентах и последнем успешном сканировании по каждой конечной точке.

Соблюдение политик

Предоставляет информацию о политиках безопасности, применяемых на выбранных объектах. Круговая диаграмма будет отображать состояние политики. В таблице под графиком вы сможете увидеть политики и их типы, назначенные каждой конечной точке, а также дату и пользователей, которые их назначили.

Sandbox Analyzer ошибки подчинения

Отображает все неудачные попытки перемещения объектов, отправленных с конечных точек, в Sandbox Analyzer за определенный период времени. Приписывание считается неудачным после нескольких попыток повтора.

На графике показано изменение неудачных перемещений в течение выбранного периода, в то время как в таблице сведений о отчетах вы можете просмотреть, какие файлы не могли быть отправлены в Sandbox Analyzer, систему, с которой был отправлен объект, дату и время повторения каждой попытки, ошибку которую выдал код, описание каждой неудачной попытки и название компании.

Результаты Sandbox Analyzer (устарело)

Предоставляет подробную информацию о файлах на целевых конечных точках, которые были проанализированы в песочнице в течение определенного периода времени. В линейной диаграмме отображается количество чистых или опасных анализируемых файлов, в то время как в таблице представлены данные о каждом событии.

Вы можете создать отчет о результатах работы Sandbox Analyzer для всех проанализированных файлов или только для тех, которые были идентифицированы, как вредоносные.

Вы можете просмотреть:

- Примите решение о том, указав, является ли файл чистым, опасным или неизвестным (**Обнаружена угроза** / **Не обнаружено угрозы** / **Неподдерживаемый**). Этот столбец отображается только при выборе отчета для отображения всех проанализированных объектов.

  Чтобы просмотреть полный список типов файлов и расширений, поддерживаемых Sandbox Analyzer, см. «Поддерживаемые Типы и Расширения Фалов для Отправки Вручную» (p. 614).
- Тип угрозы, такой как рекламное ПО, руткит, загрузчик, эксплойт, модификатор хоста, вредоносные инструменты, программа для кражи паролей, программа-вымогатель, спам или троян.
- Дата и время обнаружения, вы можете фильтровать эти данные в зависимости от отчетного периода.
- Имя хоста или IP конечной точки, где был обнаружен файл.
- Имя файлов, если они были отправлены индивидуально, или количество проанализированных файлов в случае групповой отправки. Нажмите ссылку на имя файла или ссылку для просмотра деталей и действий.
- Статус действия обезвреживания файлов (**Частичный** , **Не удалось** , **Только отчетная информация** , **Успешно**).
- Название компании.
- Более подробную информацию о свойствах анализируемого файла можно получить, нажав **Подробнее** в столбце **Результат анализа** . Здесь вы можете просмотреть сведения о безопасности и подробные отчеты о поведении образцов.

Sandbox Analyzer обращает внимание на следующие поведенческие события:

- Запись / удаление / перемещение / дублирование / замена файлов в системе и на съемных дисках.

- представление недавно созданных файлов.
- Изменения в файловой системе.
- Изменения в приложениях, запущенных внутри виртуальной машины.
- Изменения в панели задач Windows и в меню «Пуск».
- Создание / завершение / вброс процессов.
- Запись / удаление ключей реестра.
- Создание объектов мьютекса.
- Создание / запуск / остановка / изменение / запрос / удаление служб.
- Изменение настроек безопасности браузера.
- Изменение настроек экрана проводника Windows.
- Добавление файлов в список исключений брандмауэра.
- Изменение сетевых настроек.
- Включение выполнения при запуске системы.
- Подключение к удаленному хосту.
- Доступ к определенным доменам.
- Перенос данных в определенные области и из них.
- Доступ к URL-адресам, IP-адресам и портам через различные протоколы связи.
- Проверка индикаторов виртуальной среды.
- Проверка индикаторов инструментов мониторинга.
- Создание моментальных снимков.
- SSDT, IDT, IRP-захваты.
- Сброс памяти для подозрительных процессов.
- Вызов функций API Windows.
- Становится неактивным в течение определенного периода времени, чтобы отложить выполнение.
- Создание файлов с действиями, которые должны выполняться через определенные промежутки времени.

В окне **Результаты анализа** нажмите кнопку **Загрузить**, чтобы сохранить на своем компьютере содержимое сводки поведения в следующих форматах: XML, HTML, JSON, PDF.

Этот отчет будет поддерживаться в течение ограниченного периода времени. Рекомендуется вместо этого использовать карточки отправления для сбора необходимой информации по анализируемым образцам. Карточки отправления доступны в разделе **Sandbox Analyzer** в главном меню Control Center.

Аудит безопасности

Предоставляет информацию о событиях безопасности, произошедших на выбранном объекте. Информация относится к следующим событиям:

- Обнаружение вредоносного ПО
- Заблокированное приложение
- Заблокированное сканирование порта
- Заблокированный трафик
- Заблокированный веб-сайт
- Блочное устройство
- Заблокированная электронная почта
- Заблокированный процесс
- HVI События
- События Advanced Anti-Exploit
- Network Attack Defense события

Статус Security Server

Помогает оценить состояние серверов Security Server. Вы можете определить возникшие проблемы каждого Security Server с помощью различных индикаторов состояния, таких как:

- **Статус**: показывает общий статус Security Server.
- **Статус машины**: сообщает, какие устройства Security Server остановлены.
- **Статус Антивируса**: указывает, включен или отключен модуль защиты от вредоносных программ.
- **Статус обновления**: показывает, что устройства Security Server обновлены или обновления были отключены.
- **Статус загрузки**: указывает на уровень нагрузки при сканировании на Security Server, как описано ниже:
  - **Неполная**, при использовании менее чем 5% от его возможностей сканирования.
  - **Нормальная**, когда нагрузка сканирования является сбалансированной.
  - **Полная**, когда нагрузка сканирования превышает 90% от его мощности. В этом случае необходимо проверить политики безопасности. Если все Security Server, выделенные в рамках политики, перегружены, необходимо добавить еще один Security

Server в список. В противном случае, проверьте сетевое соединение между клиентами и серверами Security Server без нагрузки.

- **защищенные HVI виртуальные машины** : информирует вас о виртуальных машинах, которые контролируются и защищаются модулем HVI.
- **Статус HVI** : указывает, включен ли или отключен модуль HVI. HVI разрешен, если и Security Server и Дополнительный пакет устанавливается на хосте.
- **Подключенные устройства хранения данных**: показывает, сколько ICAP-совместимых устройств хранения данных подключены к Security Server. Нажатие на число отобразит список устройств хранения данных и соответствующие детали для каждого устройства: имя, IP, тип, дату и время последнего подключения.
- **Состояние сканирования хранилища**: показывает, включена ли службаSecurity for Storage.

Также вы можете узнать, сколько агентов подключено к Security Server. Далее, кликая на количество подключенных клиентов можно увидеть список конечных точек. Эти конечные пользователи (компьютеры) могут быть уязвимыми, если у Security Server есть проблемы.

Топ-10 обнаруженных вредоносных программ

Показывает Топ-10 вредоносных программ, обнаруженных в течение определенного периода времени на отдельных конечных точках.

Примечание
Таблица с подробной информацией будет отображать все конечные точки, которые были заражены Топ-10 обнаруженных вредоносных программ.

Топ-10 зараженных конечных точек

Показывает Топ-10 самых зараженных конечных устройств от общего числа обнаружений, в течении определенного периода времени.

Примечание
Таблица с подробной информацией будет отображать все обнаруженные вредоносные программы на Топ-10 зараженных конечных точках.

Состояние обновления

Показывает статус обновления агента безопасности или Security Server, установленного на выбранных объектах. Состояние обновления относится к версиям продукта и механизмов защиты.

Используя имеющиеся фильтры, вы можете легко выяснить, какие клиенты были обновлены и какие нет за последние 24 часа.

В этом отчете вы можете быстро обновить агентов до последней версии. Для этого нажмите на значок **Обновить** на панели инструментов действия над таблицей данных.

Состояние обновления версии продуктов

Показывает доступность новых версий агентов безопасности, установленных на выбранных объектах.

На конечных точках с устаревшими агентами безопасности вы можете быстро установить последнюю версию поддерживаемого агента, нажав кнопку **Обновление**.

Примечание
Этот отчет доступен только тогда, когда решение GravityZone обновлено.

Состояние сетевой защиты виртуальных машин

Информирует об обхвате защиты Bitdefender в вашей виртуальной среде. Для каждой из выбранных машин, вы можете увидеть, какие проблемы безопасности компонентов были решены:

- Security Server для размещения без агентов в средах VMware NSX и vShield, а также для HVI
- Агент по безопасности, в любой другой ситуации

Активность HVI

Информирует вас обо всех атак, которые HVI модули обнаружили на выбранных машинах в течение определенного периода времени.

В отчете также содержится информация о дате и времени последнего обнаруженного инцидента, привлекшего собой контролируемый процесс, окончательное состояние действий, предпринятых против нападения, пользователь от имени которого начался процесс и целевая машина.

В зависимости от предпринятых действий, об одном и том же процессе может быть сообщено несколько раз. Например, если процесс когда-то

был принудительно завершен, а в другой раз в доступе было отказано, вы увидите две записи в таблице отчета.

Для каждого процесса, при нажатии на дату последнего обнаружения, будет отображаться отдельный журнал по всем инцидентам, обнаруженным с момента запуска процесса. Журнал содержит важную информацию, такую как тип инцидента и его описание, источник и цель атаки, а также действия, предпринятые для устранения этой проблемы.

В этом отчете вы можете быстро проинструктировать модуль защиты, чтобы игнорировать определенные события, которые вы считаете законными. Для этого нажмите кнопку **Добавить исключение** на панели инструментов действия над таблицей данных.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Статус ввода инструмента неизвестного HVI

Представляет подробные сведения о каждом запуске введения инструмента на конечных точках. Информация содержит:

- Имя конечной точки.
- Имя вводимого инструмента.
- IP-адрес конечной точки.
- Гостевая операционная система.
- Триггер. Это может быть сбой памяти, задача по требованию или запланированный запуск.
- Количество успешных запусков. При нажатии на номер появится окно с указанным путем журналов и указанным временем для каждого запуска инструмента. Щелчок значка перед путем скопирует его в буфер обмена.
- Количество неудачных запусков. Щелчок по номеру откроет окно, в котором вы сможете ознакомиться с причиной и временем сбоя.
- Последнее успешное введение.

Инструменты ввода группируются по целевым конечным точкам. При помощи параметров фильтрации в заголовке таблицы можно фильтровать

отчеты, чтобы просматривать данные, относящиеся только к определенному инструменту.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Активность вредоносных программ

Информирует Вас об атаках вымогателей, обнаруженных GravityZone на конечных точках, которыми Вы управляете, и предоставляет Вам необходимые инструменты для восстановления файлов, затронутых во время атак.

Отчет доступен в виде страницы в Control Center, отличной от других отчетов, доступных в главном меню GravityZone.

Страница **Активность вымогателей** состоит из сетки, в которой перечисляются действия, свойственные для каждой атаки:

- Имя, IP-адрес и полное доменное имя конечной точки относительно которой была совершена атака
- Компания, которой принадлежит конечная точка.
- Имя пользователя, вошедшего в систему во время атаки
- Тип атаки, локальный или дистанционный
- Процесс, в рамках которого программа-вымогатель выполняла локальные атаки, или IP-адрес, с которого была инициирована атака
- Дата и время обнаружения.
- Количество файлов, было зашифровано до тех пор, пока атаку не заблокировали
- Действия по восстановлению для всех файлов на целевой конечной точке.

Some details are hidden by default. Click the **Show/Hide Columns** button in the upper right side of the page to configure the details you want to view in the grid. If you have many entries in the grid, you can choose to hide filters using the **Show/Hide filters** button in the upper right side of the page.

Дополнительную информацию можно получить, нажав на номер файла. Вы можете просмотреть список с полным путем к исходным и

восстановленным файлам, а также статус восстановления для всех файлов, участвующих в выбранной атаке вымогателей.

Важно
Резервные копии доступны не более чем на 30 дней. Пожалуйста, обратите внимание на дату и время, пока существует возможность восстановления файлов.

Для восстановления файлов от программ-вымогателей:

1. Выберите необходимые Вам атаки в сетке.
2. Нажмите кнопку **Восстановить файлы**. Появится окно подтверждения.

   Создается задача по восстановлению. Вы можете проверить его статус на странице **Задачи**, как и для любой другой задачи в GravityZone.

Если обнаружение является результатом законных процессов, выполните следующие действия:

1. Выберите записи в сетке.
2. Нажмите на **Добавить исключения** кнопку.
3. В новом окне выберите политики, к которым должно применяться исключение.
4. Нажмите **Добавить**.

   Будут применены все возможные исключения: на папку, на процесс и на IP-адрес.

   Вы можете проверить или изменить их в разделе **Antimalware > Settings > Custom Exclusions** политики.

Примечание
Деятельность вымогателей отслеживается в течение 2 лет.

10.1.2. Отчеты сервера Exchange

Доступны следующие типы отчетов для серверов Exchange:

Exchange - Заблокированное содержимое и вложения
Содержит информацию о письмах или вложениях, которые модуль управления контентом удалил с выбранных серверов в течение определенного интервала времени. Информация содержит:

- Адреса электронной почты отправителей и получателей.

  Если электронное письмо содержит много получателей, вместо адресов электронной почты в отчете отображается количество получателей, являющееся ссылкой на окно, содержащее список адресов электронной почты.

- Тема Email.
- Тип обнаружения, указывающий, что фильтр управления контентом обнаружил угрозу.
- Действия предпринятые при обнаружении.
- Сервер, на котором была обнаружена угроза.

Exchange - Заблокированые несканируемые вложения

Содержит информацию о письмах, содержащих несканируемые вложения (сильно сжатые, защищенные паролем, и т.д.), заблокированные на почтовых серверах Exchange в течение определенного периода времени. Информация содержит:

- Адреса электронной почты отправителей и получателей.

  Если электронное письмо содержит много получателей, вместо адресов электронной почты в отчете отображается количество получателей, являющееся ссылкой на окно, содержащее список адресов электронной почты.

- Тема Email.
- Действия, выполненные при удалении несканируемых вложений:
  - **Удаленное письмо**, указывает, что все сообщение было удалено.
  - **Удаленные вложения**, общее название для всех действий, которые удаляют вложения из сообщений электронной почты, таких как удаление вложения, перемещение в карантин или перемещение с уведомлением.

  Нажав на ссылку в колонке **Действие**, вы сможете просмотреть подробную информацию о каждом заблокированном вложении и соответствующем предпринятом действии.

- Дату и время обнаружения.
- Сервер, на котором было обнаружено электронное письмо.

Exchange - сканирование активности электронной почты

Показывает статистику о действиях, предпринятых модулем защиты Exchange, в течении определенного интервала времени.

Действия сгруппированы по типу обнаружения (вредоносные программы, спам, запрещенные вложения и запрещенный контент) и по серверам.

Статистика показывает следующие состояния электронной почты:

- **Карантин.** Эти письма были перемещены в папку карантина.
- **Удалено/Отклонено** Эти письма были удалены или отклонены сервером.
- **Перенаправлено.** Эти письма были перенаправлены на адрес электронной почты, указанный в политике.
- **Очищено и доставлено** В этих письмах угрозы были удалены и пропущены через фильтры.

  Электронная почта считается очищенной, когда все обнаруженные вложения были вылечены, перемещены в карантин, удалены или замещены текстом.
- **Изменено и доставлено.** В заголовки этих писем была добавлена информация о сканировании и такие письма прошли через фильтры.
- **Доставлено без других действий.** Эти письма были проигнорированы защитой Exchange и пропущены через фильтры.

Exchange - Активность вредоносного ПО

Содержит информацию о письмах с вредоносным ПО, обнаруженных на выбранных почтовых серверах Exchange в течении определенного периода времени. Информация содержит:

- Адреса электронной почты отправителей и получателей.

  Если электронное письмо содержит много получателей, вместо адресов электронной почты в отчете отображается количество получателей, являющееся ссылкой на окно, содержащее список адресов электронной почты.
- Тема Email.
- Состояние электронного письма после сканирования на вредоносное ПО.

Нажав на ссылку состояния, вы сможете просматреть подробную информацию об обнаруженных вредоносных программах и действях над ними.

- Дату и время обнаружения.
- Сервер, на котором была обнаружена угроза.

Exchange - Топ-10 обнаруженных вредоносных программ

Сообщает вам о Топ-10 самых распространенных угроз, обнаруженных в почтовых вложениях. Вы сможете создать два представления, содержащие различные статистические данные. Один вид показывает количество обнаружений, затрагиваемых получателей и одного отправителя.

Например, GravityZone обнаружил одно письмо с зараженным вложением, отправленное пяти получателям.

- При просмотре получателей:
  - В отчете показано пять обнаружений.
  - В отчете подробно показаны только получатели, а не отправители.
- При просмотре отправителей:
  - В отчете показано одно обнаружение.
  - В отчете подробно показан только отправитель, а не получатели.

Кроме отправителя/получателей и имен вредоносных программ, отчет предоставляет вам следующие данные:

- Тип вредоносных программ (вирус, шпионские программы, PUA и т.д.)
- Сервер, на котором была обнаружена угроза.
- Меры, которые предпринял модуль защиты от вредоносных программ.
- Дату и время последнего обнаружения.

Exchange - Топ-10 получателей вредоносных программ

Показывает Топ-10 почтовых получателей, которые стали мишенью вредоносных рассылок в течение определенного интервала времени.

В отчете подробно предоставляется весь список вредоносных программ, которые затрагивают этих получателей, вместе с предпринятыми действиями.

Exchange - Топ-10 получателей спама

Показывает Топ-10 получателей электронной почты по числу спам- или фишинговых писем, обнаруженных в течение определенного интервала времени. Отчет содержит информацию о предпринятых действиях над соответствующими письмами.

10.1.3. Отчеты по мобильным устройствам

Примечание
Защита от вредоносного ПО и соответствующие отчеты доступны только для устройств Android.

Список типов отчетов, доступных для мобильных устройств:

Состояние активности вредоносного ПО

Помогает узнать, сколько и какие мобильные устройства были заражены вредоносным ПО в течение определенного периода времени и какие угрозы были обнаружены. Мобильные устройства сгруппированы на основе следующих критериев:

- Мобильные устройства без каких-либо обнаружений (вредоносные угрозы не были обнаружены за указанный период времени)
- Мобильные устройства, вылеченные от вредоносного ПО (все обнаруженные файлы были удалены)
- Мобильные устройства, содержащие вредоносное ПО (некоторые из обнаруженных файлов не были удалены)

Топ-10 зараженных устройств

Показывает Топ-10 самых зараженных мобильных устройств за определенный период времени из общего числа мобильных устройств.

Примечание
Таблица с подробностями отображает все обнаруженные вредоносные программы на Топ-10 зараженных мобильных устройств.

Топ-10 обнаруженных вредоносных программ

Показывает Топ-10 вредоносных программ, обнаруженных в течение определенного периода времени, на мобильных устройствах.

Примечание
Таблица с деталями отображает все мобильные устройства, которые были заражены обнаруженными Топ-10 вредоносными программами.

Совместимость устройств

Информирует вас о состоянии совместимости выбранных мобильных устройств. Вы можете увидеть имя устройства, состояние, операционную систему и причину несовместимости.

Для получения более подробной информации о требованиях совместимости, пожалуйста, проверьте «Критерии несовместимости» (p. 431).

Синхронизация устройств

Информирует вас о состоянии синхронизации мобильных устройств. Вы можете просмотреть имя устройства, пользователя, которому оно назначено, а также состояние синхронизации, операционную систему и время, когда устройство было последний раз онлайн.

Для получения более подробной информации, обратитесь к «Проверка статуса мобильных устройств» (p. 188).

Заблокированные веб-сайты

Информирует вас о количестве попыток доступа выбранных устройств к веб-сайтам, которые заблокированы по правилам **Веб доступ**, в течение определенного интервала времени.

Для каждого устройства с обнаружениями, нажмите на цифру, указанную в столбце **Заблокированные сайты**, для просмотра подробной информации о каждой заблокированной веб-странице, такой как:

- ссылка URL
- Компонент политики, который выполнил действие
- Количество заблокированных попыток
- Время, когда веб-сайт был заблокирован

Для получения более подробной информации о настройках политики веб-доступа, обратитесь к «Профили» (p. 437).

Активность веб-защиты

Информирует вас о количестве попыток доступа выбранных мобильных устройств к веб-сайтам с угрозами безопасности (фишинг, мошенничество,

вредоносные программы или ненадежные сайты) в течении определенного интервала времени. Для каждого устройства с обнаружениями нажмите на цифру, указанную в столбце Blocked Websites, для просмотра подробной информации о каждой заблокированной веб-странице, такой как:

- ссылка URL
- Тип угрозы (фишинг, вредоносные программы, мошенничество, ненадежный сайт)
- Количество заблокированных попыток
- Время, когда веб-сайт был заблокирован

Веб-безопасность является компонентом политики, которая обнаруживает и блокирует сайты с проблемами безопасности. Для получения более подробной информации о параметрах политики веб-безопасности, обратитесь к «Безопасность» (p. 427).

10.2. Создание отчетов

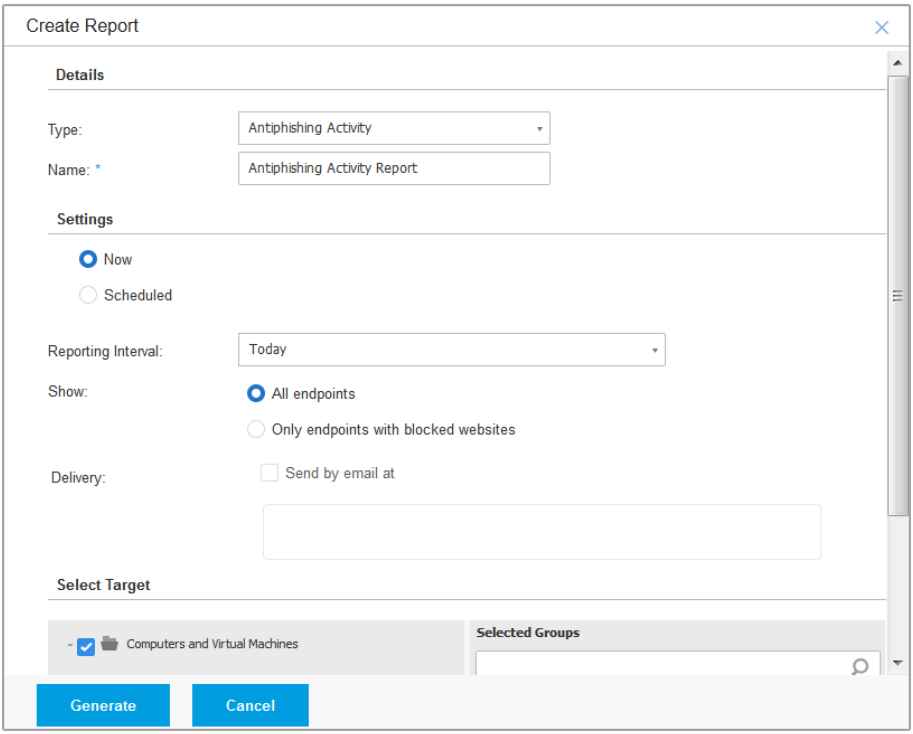
Вы можете создать две категории отчетов:

- **Мгновенные отчеты.** Мгновенные отчеты автоматически отображаются сразу после их создания.
- **Отчеты по расписанию.** Запланированные отчеты могут быть настроены на периодический запуск в заданные дату и время. Список всех запланированных отчетов отображается на странице **Отчеты**.

Важно
Мгновенные отчеты автоматически удаляются при закрытии страницы отчета. Запланированные отчеты сохраняются и отображаются на странице **Отчеты**.

Чтобы создать отчет:

1. Перейдите на страницу **Отчеты**.
2. Выберите тип объектов сети из меню видов сетей.
3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.



Опции отчета по компьютерам и виртуальным машинам

4. Выберите нужный тип отчета из меню. Для получения более подробной информации, обратитесь к«Типы отчетов» (p. 512)
5. Введите подходящее имя для отчета. При выборе имени учитывайте тип отчета, его назначение и возможности параметров отчета.
6. Настройка периодичности отчетов:
   - Нажмите **Сейчас**, чтобы создать мгновенный отчет.
   - Выберите **По расписанию**, чтобы настроить автоматическую генерацию отчета через желаемый интервал времени:
     – Почасовой, с указанием интервала между часами.

  - Ежедневный. В этом случае вы также можете установить время начала (часы и минуты).
  - Еженедельный, в указанные дни недели и в заданное время начала (часы и минуты).
  - Ежемесячный, в указанный день каждого месяца и в заданное время (часы и минуты).

7. Для большинства типов отчетов вам необходимо указать интервал времени, к которому относятся обрабатываемые данные. В отчете будут отображаться данные только за выбранный период времени.

8. Некоторые типы отчетов предоставляют возможность фильтрации, чтобы помочь вам легче найти интересующую вас информацию. Используйте параметры фильтрации в разделе **Показать** для получения только необходимой информации.

   Например, для отчета **Статус обновления** вы можете выбрать для просмотра только список сетевых объектов, которые не обновлены, или те, которые должны быть перезагружены для завершения обновлений.

9. **Доставка**. Чтобы получить отчет по расписанию по электронной почте, установите соответствующий флажок. Введите адрес электронной почты, который вы хотите, в поле ниже. По умолчанию, письмо содержит архив с двумя файлами отчета (PDF и CSV). Используйте флажки в разделе **Прикрепить файлы** для настройки - какие файлы и как отправлять их по электронной почте.

10. **Выберите цель**. Прокрутите вниз, чтобы выбрать объекты отчета. Выберите одну или несколько групп конечных точек, которые вы хотите включить в отчет.

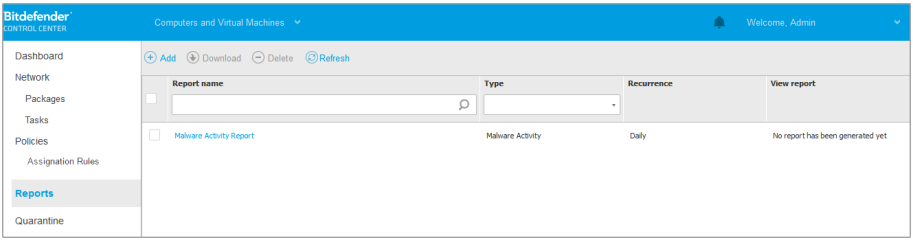
11. В зависимости от выбранной переодичности, нажмите **Создать**, чтобы создать мгновенный отчет или **Сохранить**, чтобы создать отчет по расписанию.

    - Мгновенный отчет будет отображен сразу после нажатия кнопки **Создать**. Время, необходимое для создания отчетов, варьируется в зависимости от количества управляемых объектов сети. Дождитесь завершения создания выбранного отчета.
    - Запланированный отчет будет отображаться в списке на странице **Отчеты**. После того, как экземпляр отчета был создан, вы можете

просмотреть отчет, нажав на соответствующую ссылку в колонке **Посмотреть отчет** на странице **Отчеты**.

10.3. Просмотр и управление отчетами по расписанию

Чтобы просматривать и управлять запланированными отчетами, перейдите на страницу **Отчеты**.



Страница отчетов

Все отчеты по расписанию отображаются в таблице вместе с полезной информацией о них:

- Имя и тип отчета
- Периодичность отчета
- Последний созданный экземпляр.

Примечание
Отчеты по расписанию доступны только для пользователя, который их создал.

Чтобы отсортировать отчеты по определенному столбцу, просто нажмите на заголовок нужного столбца. Щелкните заголовок столбца еще раз, чтобы изменить порядок сортировки.

Чтобы быстро найти то, что вы ищете, используйте окна поиска или параметры фильтрации под заголовками столбцов.

Чтобы очистить поле поиска, поместите в него курсор и нажмите на иконку × **Удалить**.

Чтобы быть уверенным, что отображается актуальная информация, нажмите кнопку **Обновить** в верхней части таблицы.

10.3.1. Просмотр отчетов

Чтобы просмотреть отчет:

1. Перейдите на страницу **Отчеты**.
2. Сортируйте отчеты по названию, типу или периодичности, чтобы быстрее найти нужный отчет.
3. Нажмите на соответствующую ссылку в колонке **Посмотреть отчет** для отображения отчета. Отобразится самый последний экземпляр отчета.

   Для просмотра всех экземпляров отчета, обратитесь к«Сохранение отчетов» (p. 541)

Все отчеты содержат краткое содержание (верхняя часть страницы отчета) и подробный раздел (нижняя часть страницы отчета).

- Раздел краткого содержания предоставляет вам статистические данные (круговые диаграммы и графики) для всех выбранных объектов сети, а также общую информацию об отчете, такую как отчетный период (если это применимо), цель отчета и т.д.
- Подробный раздел предоставляет вам информацию о каждом выбранном объекте сети.

Примечание

- Для настройки информации, отображаемой на графике, нажмите на записи легенды, чтобы показать или скрыть выбранные данные.
- Нажмите на графическую область (область круговой диаграммы, прямоугольной), которая вам нужна, чтобы посмотреть в таблице относящуюся к ней информацию.

10.3.2. Редактирование отчетов по расписанию

Примечание

При редактировании отчетов по расписанию, любые обновления будут применены, начиная со следующего запуска отчета. Изменения не затронут отчеты, сгенерированные ранее.

Чтобы изменить настройки отчетов по расписанию:

1. Перейдите на страницу **Отчеты**.

2. Нажмите на имя отчета.
3. Измените необходимые настройки отчета. Вы можете изменить следующее:
   - **Имя отчета.** Выберите подходящее имя для отчета, чтобы вам было проще понимать о чем он. При выборе имени учитывайте тип отчета, его назначение и возможности параметров отчета. Отчетам, которые генерируются по расписанию, имя дается позже.
   - **Периодичность отчетов (по расписанию).** Вы можете запланировать отчеты, чтобы они создавались каждый час (точный часовой интервал), ежедневно (в определенное время), еженедельно (в конкретный день недели и время) или ежемесячно (в конкретный день месяца и время). В зависимости от выбранного расписания, отчет будет включать только данные с последнего дня, недели или месяца соответственно.
   - **Настройки**
     - Вы можете запланировать отчет, чтобы он создавался автоматически каждый час (в определенный часовой интервал), ежедневно (в определенное время), еженедельно (в конкретный день недели и время) или ежемесячно (в конкретный день месяца и время). В зависимости от выбранного расписания, отчет будет включать только данные с последнего дня, недели или месяца соответственно.
     - Отчет будет включать только данные выбранного временного интервала. Вы можете изменить начальный интервал при следующем обращении.
     - Большинство отчетов предоставляют опции фильтрации, чтобы помочь вам легче найти нужную информацию. Когда вы просматриваете отчет в консоли, будет доступна вся информация, независимо от выбранных опций. Если вы загрузите или отправите отчет, в PDF файл будет включено только краткое содержание и выбранная информация. Подробные данные отчета будут доступны только в CSV формате.
     - Вы можете выбрать получение отчета по электронной почте.
   - **Выбрать цель.** Выбранная опция определяет тип объекта текущего отчета (как группы, так и индивидуального сетевого объекта). Нажмите на соответствующую ссылку, чтобы просмотреть объекты текущего

отчета. Чтобы изменить их, выберите нужные группы или сетевые объекты, которые будут включены в отчет.

4. Нажмите **Сохранить**, чтобы применить изменения.

10.3.3. Удаление отчета по расписанию

Если отчет по расписанию больше не нужен, его лучше удалить. Удаление отчета по расписанию удалит все его экземпляры, автоматически сгенерированные до этого момента.

Чтобы удалить отчет по расписанию:

1. Перейдите на страницу **Отчеты**.
2. Выберите отчет, который вы хотите удалить.
3. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

10.4. Выполнение действий, основанные на данных отчета

В то время, как большинство отчетов показывают проблемы в вашей сети, некоторые из них также предлагают вам несколько вариантов действий для решения найденных проблем, с помощью всего одного нажатия кнопки мыши.

Чтобы исправить проблемы, отображаемые в отчете, нажмите соответствующую кнопку на панели инструментов над таблицей данных.

Примечание
Вам нужны соответствующие права на **управление сетью**, чтобы выполнить данные действия.

Следующие опции доступны для каждого отчета:

Заблокированные приложения

- **Добавление Исключения**. Добавляет исключение в политику для предотвращения повторного блокирования модулей защиты.
- **Добавить**. Определяет правило для приложения или процесса в Контроле Приложений.

Активность HVI

- **Добавить исключение**. Добавляет исключение в политику, чтобы предотвратить повторный отчет об этом инциденте.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Состояние активности вредоносного ПО

- **Проверить зараженные цели**. Выполняет сконфигурированную задачу полной проверки объектов, которые все еще отображаются как зараженные.

Состояние обновления

- **Обновить**. Обновляет выбранных клиентов до последних доступных для них версий.

Состояние обновления версии продуктов

- **Обновить**. Заменяет старых клиентов конечных устройств на последние доступные версии продуктов.

10.5. Сохранение отчетов

По умолчанию, отчеты по расписанию автоматически сохраняются в Control Center.

Если вам необходимо более продолжительное время хранения отчетов, вы можете сохранить их на ваш компьютер. Сводный отчет будет доступен в формате PDF, в то время как сами подробные данные отчета будут доступны в формате CSV.

Существуют два способа сохранения отчетов:

- Экспортировать
- Загрузить

10.5.1. Экспорт отчетов

Чтобы экспортировать отчет на ваш компьютер:

1. Выберите формат и нажмите **Экспорт CSV** или **Экспорт PDF**.
2. В зависимости от настроек вашего браузера, файл может быть автоматически загружен в папку загрузки по умолчанию или окно загрузки запросит желаемое место, где вы должны указать папку назначения.

10.5.2. Загрузка отчетов

Архив отчетов содержит как сводный отчет (PDF), так и сами данные отчета (CSV).

Чтобы загрузить архив отчета:

1. Перейдите на страницу **Отчеты**.
2. Выберите отчет, который вы хотите сохранить.
3. Нажмите кнопку **Скачать** и выберите либо **Последний экземпляр**, чтобы загрузить последний сгенерированный отчет, либо **Полный архив**, чтобы загрузить архив, содержащий все отчеты.

   В зависимости от настроек вашего браузера, файл может быть автоматически загружен в папку загрузки по умолчанию или окно загрузки запросит желаемое место, где вы должны указать папку назначения.

10.6. Отправка отчетов

Вы можете отправлять отчеты по электронной почте, используя следующие параметры:

1. Чтобы отправить отчет, который вы просматриваете, по электронной почте, нажмите кнопку **Электронная почта**. Отчет будет отправлен на адрес электронной почты, связанный с вашей учетной записью.
2. Чтобы настроить расписание доставки отчетов по электронной почте:
   a. Перейдите на страницу **Отчеты**.
   b. Нажмите на название нужного отчета.
   c. Под **Настройки > Доставка**, выберите **Отправить по email** .
   d. Введите нужный адрес электронной почты в поле ниже. Можно добавить любое необходимое количество адресов электронной почты.
   e. Нажмите **Сохранить**.

Примечание
Только краткий отчет и график будут включены в файл PDF, отправляемый по электронной почте. Подробные данные отчета будут доступны в файле CSV.

Отчеты отправляются по электронной почте в виде архивов с расширением .zip.

10.7. Печать отчетов

Control Center в настоящее время не поддерживает функцию печати. Чтобы напечатать отчет, необходимо сначала сохранить его на свой компьютер.

11. КАРАНТИН

Карантин - это зашифрованная папка, которая содержит потенциально вредоносные файлы, такие как: подозрительно-вредоносные программы, подозрительно-зараженные программы или другие нежелательные файлы. Вирус, изолированный в карантинной зоне, не может причинить никакого вреда, так как его нельзя запустить или открыть для чтения.

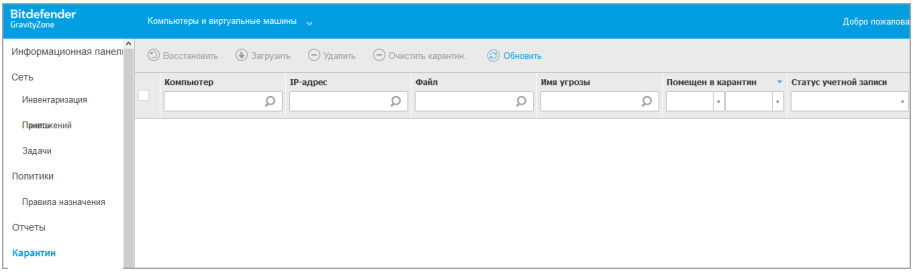
GravityZone перемещает файлы в карантин в соответствии с политикой, установленной на конечных точках. По умолчанию, файлы, которые не могут быть вылечены, отправляются в карантин.

Файлы карантина сохраняются локально на каждой конечной точке , за исключением сервера VMware vCenter, интегрированного с конечными точками vShield и с NSX, где они сохраняются на Security Server.

Важно
Карантин недоступен для мобильных устройств.

11.1. Просмотр карантина

Страница **Карантин** предоставляет подробную информацию о файлах в карантине со всех конечных точек, которыми вы управляете.



Страница карантина

Страница карантина состоит из двух панелей:

- Компьютеры и виртуальные машины, для файлов, обнаруженных непосредственно в файловой системе конечной точки.
- Серверы Exchange, для электронной почты и файлов, прикрепленных к электронной почте, обнаруженных на почтовых серверах Exchange.

Настройка отображения в верхней части страницы позволяет переключаться между этими панелями.

Информация о файлах, помещенных в карантин, отображается в виде таблицы. В зависимости от количества управляемых конечных точек, а также степени инфекции, таблица карантина может включать в себя большое количество записей. Таблица может содержать несколько страниц (по умолчанию, на странице отображается только 20 записей).

Для перемещения по страницам используйте кнопки навигации в нижней части таблицы. Чтобы изменить количество записей отображаемых на странице, введите другое значение в поле рядом с кнопками навигации.

Для лучшей наглядности данных, в которых вы заинтересованы, вы можете использовать поля поиска из заголовков столбцов, чтобы фильтровать отображаемые данные. Например, вы можете искать конкретную угрозу, обнаруженную в сети, или конкретный сетевой объект. Вы также можете нажимать на заголовки столбцов, чтобы отсортировать данные по определенному столбцу.

Чтобы быть уверенным, что отображается актуальная информация, нажмите кнопку **Обновить** в верхней части таблицы. Данная функция может быть полезной, если вы длительное время находитесь на странице.

11.2. Карантин компьютеров и виртуальных машин

По умолчанию файлы в карантине автоматически отправляются в Лаборатории Bitdefender для анализа исследователями Bitdefender. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить. Кроме того, файлы в карантине сканируются после каждого обновления баз данных сигнатур вредоносных программ. Очищенные файлы автоматически возвращаются на свое место. Данные возможности содержаться в каждой политике безопасности из раздела **Политики** и вы можете выбрать, следует ли сохранять файлы в карантине или лечить их. Для получения более подробной информации, обратитесь к «Карантин» (p. 310).

11.2.1. Просмотр подробной информации карантина

Таблица карантин предоставляет вам следующую информацию:

- Имя конечной точки, на которой угроза была обнаружена.

- IP-адрес конечной точки, на которой угроза была обнаружена.
- Путь к зараженному или подозрительному файлу на конечной точке, на которой он был обнаружен.
- Имя, которое дано вредоносной угрозе исследователями безопасности Bitdefender.
- Дата и время, когда файл был помещен в карантин.
- Состояние выбранного действия над перемещаемым в карантин файлом.

11.2.2. Управление файлами в карантине

В каждой среде параметры карантина отличаются:

- **Security for Endpoints** хранит файлы в карантине на каждом управляемом компьютере. Используя Control Center, у вас есть возможность, как удалять, так и восстанавливать отдельные файлы, помещенные в карантин.
- **Security for Virtualized Environments (Multi-Platform)** хранит файлы в карантине в каждой управляемой виртуальной машине. Используя Control Center, у вас есть возможность, как удалять, так и восстанавливать отдельные файлы, помещенные в карантин.
- **Security for Virtualized Environments (интегрированный с конечной точкой VMware vShield или NSX)** хранит файлы в карантине на устройстве Security Server. Используя Control Center, у вас есть возможность удалять файлы из карантина или сохранять их в выбранном местоположении.

Восстановление файлов из карантина

В отдельных случаях вам, возможно, потребуется восстановить файлы из карантина в их исходное местоположение или в другое место. Одна из таких ситуаций, когда вам необходимо восстановить важные файлы, хранящиеся в зараженном архиве, который был перемещен в карантин.

Примечание
Восстановление файлов из карантина возможно только в средах, защищенных Security for Endpoints и Security for Virtualized Environments (Multi-Platform).

Для восстановления одного или более файлов, помещенных в карантин:

1. Перейдите на страницу **Карантин**.
2. Выберите **Компьютеры и виртуальные машины** из меню просмотра в верхней части страницы.

3. Установите флажки, на соответствующих файлах в карантине, которые вы хотите восстановить.
4. Нажмите кнопку **Восстановить** в верхней части таблицы.
5. Выберите место, в которое вы хотите восстановить выбранные файлы (или оригинал, или другое место на компьютере).

   Если вы решите восстановить в другое место, необходимо ввести абсолютный путь в соответствующем поле.
6. Выберите **Автоматически добавлять исключения в политику**, чтобы исключить файлы, которые будут восстановлены при будущих проверках. Исключение распространяется на все политики, затрагивающие выбранные файлы, кроме политики по умолчанию, которая не может быть изменена.
7. Нажмите **Сохранить**, чтобы запустить задачу восстановления файлов. В колонке **Действие** вы можете наблюдать статус выполнения.
8. Запрашиваемое действие сразу же отправляется на объекты конечных точек или как только конечные точки появятся в сети.

   Вы можете просмотреть детали о выполнении действий на странице **Задачи**. После того, как файл будет восстановлен, соответствующая запись исчезнет из таблицы карантина.

Загрузка файлов из карантина

В виртуальных средах VMware, интегрированных с конечной точкой vShield или NSX, карантин сохраняется на Security Server. Если вы хотите изучить или восстановить данные из файлов в карантине, необходимо загрузить их из Security Server с помощью Control Center. Файлы в карантине загружаются в виде зашифрованного, защищенного паролем ZIP архива, чтобы предотвратить случайные вредоносные инфекции.

Чтобы открыть архив и извлечь его содержимое, вы должны использовать инструмент карантина - отдельное приложение Bitdefender, которое не требует установки.

Инструмент карантина доступен для следующих операционных систем:

- Windows 7 или новее
- Большинство дистрибутивов 32-разрядных Linux-систем с графическим интерфейсом пользователя (GUI).

Примечание
Пожалуйста, обратите внимание, что инструмент карантина не имеет интерфейса командной строки.

Предупреждение
Будьте осторожны при извлечении файлов из карантина, поскольку они могут заразить вашу систему. Рекомендуется извлекать и анализировать файлы из карантина на тестовой или изолированной системе, предпочтительно работающей на Linux. Вредоносные инфекции легче сдерживать в системах Linux.

Чтобы скачать файлы, помещенные в карантин, на компьютер:

1. Перейдите на страницу **Карантин**.
2. Выберите **Компьютеры и виртуальные машины** из меню просмотра в верхней части страницы.
3. Для фильтрации данных в таблице введите имя хоста или IP-адрес Security Server в соответствующем поле заголовка таблицы.

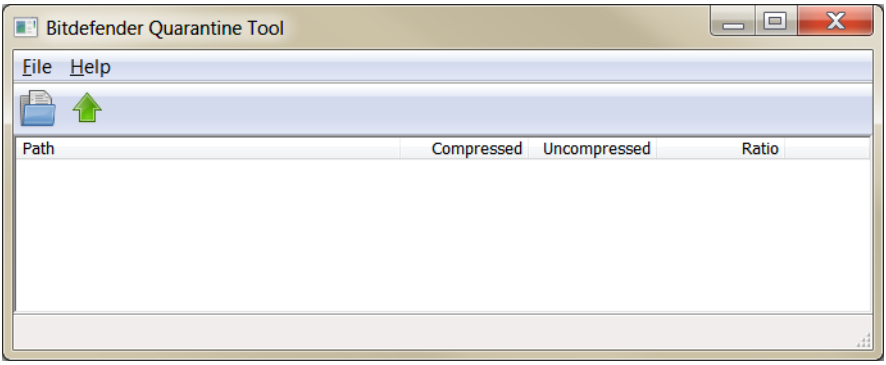
   Если карантин большой, чтобы просмотреть файлы, в которых вы заинтересованы, вам, возможно, потребуется применить дополнительные фильтры или увеличить количество файлов, отображаемых на странице.
4. Установите флажки на соответствующих файлах, которые вы хотите загрузить.
5. Нажмите кнопку **Скачать** в верхней части таблицы. В зависимости от настроек вашего браузера, вам будет предложено сохранить файлы в папку по вашему выбору, или файлы будут автоматически загружены в местоположение загрузок по умолчанию.

Чтобы получить доступ к восстановленным файлам:

1. Загрузите соответствующий инструмент карантина для вашей операционной системы со страницы **Помощь & Поддержка** или с одного из следующих адресов:
   - Инструмент карантина для Windows
   - Инструмент карантина для Linux

   Примечание
   Инструмент карантина для Linux заархивирован в файл `tar`.

2. Запустите исполняемый файл инструмента карантина.



Инструмент карантина

3. В меню **Файл** нажмите кнопку **Открыть** (CTRL+O) или нажмите **Открыть** для загрузки архива в инструмент карантина.

   Файлы организованы в архив виртуальной машиной, в которой они были обнаружены, и сохраняют свой оригинальный путь.
4. Перед извлечением архивированных файлов, если включено сканирование вредоносных программ на системе, убедитесь, что отключили его или настроили исключения сканирования для мест, куда вы будете извлекать файлы. В противном случае ваша программа обнаружения вредоносного ПО обнаружит их и применит меры к извлеченным файлам.
5. Выберите файлы, которые вы хотите извлечь.
6. В меню **Файл**, нажмите **Извлечь** (CTRL+E) или нажмите кнопку **Извлечь**.
7. Выберите папку назначения. Файлы будут извлечены в указанное место, сохраняя оригинальную структуру папок.

Автоматическое удаление файлов из карантина

По умолчанию файлы в карантине, созданные более 30 дней назад, удаляются автоматически. Этот параметр может быть изменен путем редактирования политики, назначаемой управляемым конечным точкам.

Чтобы изменить интервал автоматического удаления файлов, помещенных в карантин:

1. Перейдите на страницу **Политики**.
2. Найдите политику, назначенную конечным точкам, на которых вы хотите изменить настройку, и нажмите на ее имя.

3. Перейдите на страницу **Антивредоносное ПО > Настройки**.
4. В разделе **Карантин** выберите количество дней, после которого файлы будут удалены.
5. Нажмите **Сохранить**, чтобы применить изменения.

Руководство по удалению файлов из карантина

Если вы хотите вручную удалить файлы из карантина, вы должны сначала убедиться, что файлы, которые вы выбрали для удаления, больше не нужны.

В реальности весь файл может быть вредоносной программой. Если ваше исследование привело к такой ситуации, вы можете изучить карантин на предмет конкретной угрозы и удалить ее из карантина.

Чтобы удалить один или несколько файлов из карантина:

1. Перейдите на страницу **Карантин**.
2. Выберите **Компьютеры и виртуальные машины** из меню выбора в верхней части страницы.
3. Установите флажки на соответствующих файлах в карантине, которые вы хотите удалить.
4. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

   В колонке **Действие** вы можете наблюдать статус выполнения.

   Требуемое действие направляется на выбранные сетевые объекты сразу же или как только они появятся в сети. После того, как файл будет удален, соответствующая запись исчезнет из таблицы карантина.

Очистка карантина

Чтобы удалить все зараженные объекты:

1. Перейдите на страницу **Карантин**.
2. Выберите **Компьютеры и виртуальные машины** в меню видов.
3. Нажмите кнопку **Очистить Карантин**.

   Вы должны будете подтвердить ваши действия, нажав **Да**.

Все записи из таблицы карантина очищаются. Требуемое действие направляется на выбранные сетевые объекты сразу же или как только они появятся в сети.

11.3. Карантин серверов Exchange

Карантин Exchange содержит электронные письма и вложения. Модуль защиты от вредоносных программ отправляет в карантин вложения электронной почты, в то время как антиспам, фильтрация контента и вложений, отправляет в карантин все электронное письмо.

Примечание
Пожалуйста, обратите внимание, что карантин для серверов Exchange требует дополнительное дисковое пространство на разделе, где установлен агент безопасности. Размер карантина зависит от количества хранящихся элементов и их размера.

11.3.1. Просмотр подробной информации карантина

Страница **Карантин** предлагает вам подробную информацию об объектах в карантине из всех Exchange серверов в вашей организации. Информация доступна в таблице карантина и в окне описания каждого объекта.

Таблица карантин предоставляет вам следующую информацию:

- **Тема.** Тема сообщения на карантине.
- **Отправитель.** Адрес электронной почты отправителя, который отображается в поле заголовка электронной почты **From**.
- **Получатели.** Список получателей, которые отображаются в полях заголовков сообщений электронной почты **To** и **Cc**.
- **Реальные получатели.** Список отдельных адресов электронной почты пользователей, которым предназначалась доставка письма, прежде чем попасть в карантин.
- **Статус.** Состояние объекта после того, как он был просканирован. Статус показывает, помечено ли письмо как спам или содержит нежелательный контент, или вложение зараженно вредоносной программой, подозревается в инфицировании, нежелательное или несканируемое.
- **Имя вредоносного ПО.** Имя, данное вредоносной угрозе, исследователями безопасности Bitdefender.
- **Имя сервера.** Имя сервера, на котором угроза была обнаружена.
- **В карантине.** Дата и время, когда объект был помещен в карантин.

- **Статус действия.** Статус действий над объектами в карантине. Вы можете быстро просмотреть состояние действия - в обработке или действие не удалось выполнить.

Примечание

- Колонки **Реальные получатели**, **Имя вредоносного ПО** и **Имя сервера** скрыты по умолчанию от просмотра.
- Когда несколько вложений от одного адреса электронной почты отправлены в карантин, таблица карантина показывает отдельно каждое вложение.

Чтобы настроить детали параметров карантина, отображающихся в таблице:

1. Нажмите кнопку **Столбцы** в правой верхней части таблицы.
2. Выберите столбцы, которые вы хотите отобразить.

   Чтобы вернуться к просмотру столбцов по умолчанию нажмите кнопку **Сбросить**.

Вы можете получить более подробную информацию, нажав на ссылку **Тема**, соответствующую каждому объекту. Окно **Сведения об объекте** предоставляет вам следующую информацию:

- **Объект в карантине.** Тип объекта в карантине, который может быть как электронной почтой, так и вложением.
- **В карантине.** Дата и время, когда объект был помещен в карантин.
- **Статус.** Состояние объекта после того, как он был просканирован. Статус показывает, помечено ли письмо как спам или содержит нежелательный контент, или вложение зараженно вредоносной программой, подозревается в инфицировании, нежелательное или несканируемое.
- **Имя вложения.** Имя файла вложения обнаруженного защитой от вредоносных программ или модулем фильтрации вложений.
- **Имя вредоносного ПО.** Имя, данное вредоносной угрозе, исследователями безопасности Bitdefender. Эта информация доступна, только если объект был заражен.
- **Точка обнаружения.** Объект обнаружен или на транспортном уровне, или в почтовом ящике, или в общей папке хранилища Exchange.
- **Соответствующее правило.** Правило политики, определившее угрозу.

- **Сервер.** Имя сервера, где была обнаружена угроза.
- **IP отправителя.** IP-адрес отправителя.
- **Отправитель (От).** Адрес электронной почты отправителя, который отображается в поле заголовка электронной почты **От**.
- **Получатели.** Список получателей, которые отображаются в полях заголовков сообщений электронной почты **To** и **Cc**.
- **Реальные получатели.** Список отдельных адресов электронной почты пользователей, которым предназначалась доставка письма, прежде чем попасть в карантин.
- **Тема.** Тема сообщения на карантине.

Примечание
Знак многоточия в конце текста указывает, что часть текста опущена. В этом случае, наведите курсор мыши на текст, чтобы просмотреть его весь в виде всплывающей подсказки.

11.3.2. Объекты на карантине

Сообщения электронной почты и файлы, помещенные в карантин модулем защиты Exchange, хранятся локально на сервере в виде зашифрованных файлов. С помощью Центра управления вы имеете возможность восстановить помещенные в карантин сообщения электронной почты, а также удалять или сохранять любые файлы или электронные письма, помещенные в карантин.

Восстановление электронных писем из карантина

Если вы решили, что электронная почта в карантине не представляет угрозы, вы можете извлечь ее из карантина. Используя веб-службы Exchange, защитник Exchange-сервера отправляет электронное письмо, помещаемое в карантин, в виде вложения по электронной почте для уведомлений Bitdefender.

Примечание
Вы можете восстановить только электронные письма. Для восстановления вложения из карантина, вы должны сохранить его в локальную папку на сервере Exchange.

Для восстановления одного или нескольких писем:

1. Перейдите на страницу **Карантин**.
2. Выберите **Exchange** из меню выбора в верхней части страницы.
3. Установите флажки на соответствующих электронных письмах, которые вы хотите восстановить.
4. Нажмите кнопку **Восстановить** в верхней части таблицы. Появится окно **Восстановить учетные данные**.
5. Выберите учетные данные пользователя Exchange, уполномоченного отправлять восстановленные электронные письма. Если учетные данные, которые вы собираетесь использовать, новые, в первую очередь, вы должны их добавить в диспетчер учетных данных.

   Чтобы добавить необходимые учетные данные:

   a. Введите необходимую информацию в соответствующие поля заголовка таблицы:
      - Имя пользователя и пароль пользователя Exchange.

        Примечание
        Имя пользователя должно включать имя домена, например, `user@domain` или `domain\user`.

      - Адрес электронной почты пользователя Exchange, необходимый только тогда, когда адрес электронной почты отличается от имени пользователя.
      - Ссылка Exchange Web Services (EWS), необходимая если автообнаружение Exchange не работает. Это, как правило, происходит в случае с пограничными транспортными серверами в демилитаризованной зоне.

   b. Нажмите кнопку **Добавить** в верхней части таблицы. Новый набор учетных данных будет добавлен в таблицу.
6. Нажмите кнопку **Восстановить**. Появится окно подтверждения.

   Запрашиваемое действие сразу направляется на выбранные серверы. После того, как электронная почта восстанавливается, она также удаляется и из карантина, при этом соответствующая запись исчезает из таблицы карантина.

   Вы можете проверить состояние процесса восстановления в любом из этих разделов:

- **Статус действия** в столбце таблицы карантина.
- Страница **Сеть > Задачи**.

Сохранение файлов в карантине

Если вы хотите изучить или восстановить данные из карантина, вы можете сохранить файлы в локальную папку на сервере Exchange. Bitdefender Endpoint Security Tools расшифрует файлы и сохранит их в указанном месте.

Чтобы сохранить один или несколько файлов в карантине:

1. Перейдите на страницу **Карантин**.
2. Выберите **Exchange** из меню выбора в верхней части страницы.
3. Отфильтруйте данные в таблице для просмотра всех файлов, которые вы хотите сохранить, введя поисковые термины в полях заголовков столбцов.
4. Установите флажки, на соответствующих файлах в карантине, которые вы хотите восстановить.
5. Нажмите кнопку **Сохранить** в верхней части таблицы.
6. Введите путь к папке на сервере Exchange. Если папка на сервере не существует, то она будет создана.

   Важно
   Вы должны исключить эту папку из сканирования файловой системы, в противном случае файлы будут перемещены в карантин компьютеров и виртуальных машин. Для получения более подробной информации, обратитесь к «Исключения» (p. 312).

7. Нажмите **Сохранить**. Появится окно подтверждения.

   В колонке **Статус действия** вы можете наблюдать статус выполнения. Вы так же можете просматривать статус выполнения на странице **Сеть > Задачи**.

Автоматическое удаление файлов из карантина

По умолчанию, файлы в карантине старше 30 дней удаляются автоматически. Вы можете изменить эту настройку, отредактировав политику, назначенную управляемому серверу Exchange.

Чтобы изменить интервал автоматического удаления файлов, помещенных в карантин:

1. Перейдите на страницу **Политики**.
2. Нажмите на название политики, назначенной серверу Exchange, которая вам необходима.
3. Перейдите на страницу **Защита Exchange > Общие**.
4. В разделе **Настройки** выберите количество дней, после которого файлы будут удалены.
5. Нажмите **Сохранить**, чтобы применить изменения.

Руководство по удалению файлов из карантина

Чтобы удалить один или несколько объектов из карантина:

1. Перейдите на страницу **Карантин**.
2. Выберите **Exchange** из меню выбора.
3. Установите флажки на соответствующие файлы, которые вы хотите удалить.
4. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

   В колонке **Статус действия** вы можете наблюдать статус выполнения.

   Запрашиваемое действие сразу направляется на выбранные серверы. После того, как файл будет удален, соответствующая запись исчезнет из таблицы карантина.

Очистка карантина

Чтобы удалить все зараженные объекты:

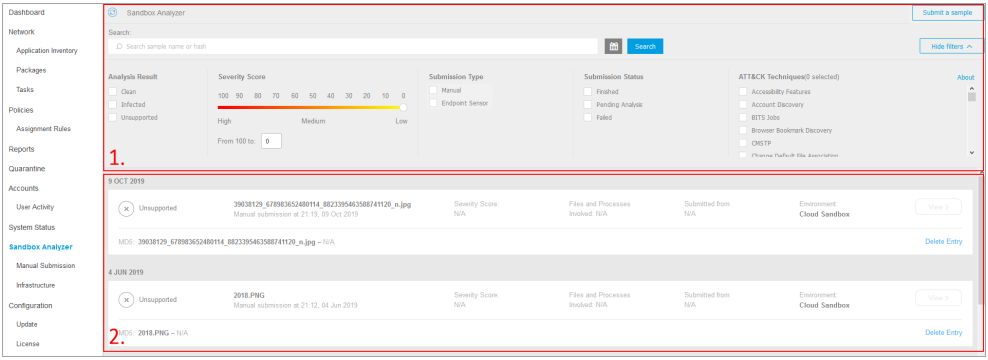
1. Перейдите на страницу **Карантин**.
2. Выберите **Exchange** в меню выбора.
3. Нажмите кнопку **Очистить Карантин**.

   Вы должны будете подтвердить ваши действия, нажав **Да**.

Все записи из таблицы карантина очищаются. Запрошенное действие немедленно отправляется объектам целевой сети.

12. ИСПОЛЬЗОВАНИЕ SANDBOX ANALYZER

Страница **Sandbox Analyzer** предоставляет собой единый интерфейс для просмотра, фильтрации и поиска автоматической и ручной отправки в среде песочницы. Страница **Sandbox Analyzer** состоит из двух областей:



Страница Sandbox Analyzer

1. **Область фильтрации** позволяет вам искать и фильтровать материалы по различным критериям: имя, хэш, дата, результат анализа, статус, среда детонации и техники MITRE's ATT&CK.
2. **Область карточек отправки** отображает все заявки в компактном формате с подробной информацией о каждой из них.

На странице Sandbox Analyzer вы можете сделать следующее:

- Фильтровать карточки отправки
- Просмотреть список отправленных объектов и подробную информацию об анализе
- Повторная отправка образцов на анализ с карты подачи
- Удалять карточки отправки
- Сделать ручную подачу

12.1. Фильтрация карточек отправки

Вот что вы можете сделать в области фильтров:

- Фильтровать заявки по различным критериям. Страница автоматически загрузит только карты событий безопасности, соответствующие выбранным критериям.
- Сбросьте фильтры, нажав кнопку **Очистить фильтры** .
- Скрыть вкладку фильтры, нажав кнопку **Скрыть фильтры** . Вы можете снова отобразить скрытые параметры, нажав **Показать фильтры** .

Вы можете фильтровать отправления Sandbox Analyzer по следующим критериям:

- **Пример имени и хэша (MD5)**. Введите в поле поиска часть или все имя или хэш искомого примера, а затем нажмите кнопку **Поиск** с правой стороны.
- **Дата**. Чтобы фильтровать по дате:
  1. Нажмите значок календаря , чтобы настроить временные рамки поиска.
  2. Определите интервал. Нажмите кнопки **ОТ** и **ДО** в верхней части календаря, чтобы выбрать даты, определяющие временной интервал. Вы также можете выбрать заранее определенный период из списка параметров справа относительно текущего времени (например, последние 30 дней).

     Вы также можете указать часы и минуты для каждой даты временного интервала, используя опции под календарем.
  3. Нажмите **OK** , чтобы применить фильтр.
- **Результат анализа**. Выберите один или несколько из следующих параметров:
  – **Очистить** - образец безопасен.
  – **Зараженный** - образец опасен.
  – **Неподдерживаемый** - образец имеет формат, который Sandbox Analyzer не может проверить. Чтобы просмотреть полный список типов файлов и расширений, поддерживаемых Sandbox Analyzer, см. «Поддерживаемые Типы и Расширения Фалов для Отправки Вручную» (p. 614).
- **Оценка серьезности**. Значение указывает, насколько опасен образец по шкале от 100 до 0 (ноль). Чем выше оценка, тем опаснее образец. Степень

серьезности применяется ко всем отправленным образцам, включая образцы со статусом **Чистый** или **Неподдерживаемый** .

- **Тип отправки**. Выберите один или несколько из следующих параметров:
  - **Вручную**. Sandbox Analyzer получил образец с помощью опции **Отправка вручную**.
  - **Датчик конечной точки**. Bitdefender Endpoint Security Tools отправил образец в Sandbox Analyzer на основе параметров политики.
  - **Датчик сетевого трафика** . Датчик сети отправил образец в локальный экземпляр Sandbox Analyzer на основе параметров политики.
  - **Централизованный карантин** . GravityZone отправил образец в локальный экземпляр Sandbox Analyzer на основе параметров политики.
  - **API**. Образец был передан в локальный экземпляр Sandbox Analyzer с помощью методов API.
  - **Датчик ICAP**. Security Server отправил образец в локальный экземпляр Sandbox Analyzer после сканирования сервера ICAP.
- **Сведения передачи**. Установите один или несколько из следующих флажков:
  - **Выполнено** - Sandbox Analyzer предоставил результат анализа.
  - **В ожидании анализа** - Sandbox Analyzer проверяет образец.
  - **Ошибка** - Sandbox Analyzer не смог проверить образец.
- **Среда**. Здесь перечислены виртуальные машины, доступные для детонации, включая экземпляр Sandbox Analyzer, размещенный в Bitdefender. Установите один или несколько флажков, чтобы просмотреть, какие образцы были взорваны в определенных условиях.
- **ATT&CK techniques**. Эта опция фильтрации объединяет базу знаний MITRE's ATT&CK если это применимо. Значения методов ATT&CK меняются динамически в зависимости от событий безопасности.

  Нажмите ссылку **О программе** , чтобы открыть ATT&CK Matrix в новой вкладке.

12.2. Просмотр подробностей анализа

На странице **Sandbox Analyzer** отображаются карточки отправки по дням, в обратном хронологическом порядке. Карточки для подачи содержат следующие данные:

- Результат анализа
- Имя образца
- Тип отправки
- Оценка серьезности
- Задействованные файлы и процессы
- Детонационная среда
- Значение хэша (MD5)
- ATT&CK techniques
- Статус отправки, когда результат недоступен

Каждая карта подачи содержит ссылку на подробный отчет об анализе HTML, если таковой имеется. Чтобы открыть отчет, нажмите кнопку **Вид** с правой стороны карточки.

Отчет в формате HTML предоставляет обширную информацию, организованную на нескольких уровнях, с описательным текстом, графикой и снимками экрана, которые иллюстрируют поведение образца в среде детонации. Вот что вы можете узнать из HTML-отчета Sandbox Analyzer:

- Общие данные об анализируемой выборке, такие как: название и классификация вредоносного ПО, данные о представлении (имя файла, тип и размер, хэш, время отправки и продолжительность анализа).
- Результаты поведенческого анализа, которые включают все события безопасности, зафиксированные во время детонации, организованы в секции. К событиям безопасности относятся:
  - Запись / удаление / перемещение / дублирование / замена файлов в системе и на съемных дисках.
  - представление недавно созданных файлов.
  - Изменения в файловой системе.
  - Изменения в приложениях, запущенных внутри виртуальной машины.
  - Изменения в панели задач Windows и в меню «Пуск».
  - Создание / завершение / вброс процессов.
  - Запись / удаление ключей реестра.
  - Создание объектов мьютекса.
  - Создание / запуск / остановка / изменение / запрос / удаление служб.

- Изменение настроек безопасности браузера.
- Изменение настроек экрана проводника Windows.
- Добавление файлов в список исключений брандмауэра.
- Изменение сетевых настроек.
- Включение выполнения при запуске системы.
- Подключение к удаленному хосту.
- Доступ к определенным доменам.
- Перенос данных в определенные области и из них.
- Доступ к URL-адресам, IP-адресам и портам через различные протоколы связи.
- Проверка индикаторов виртуальной среды.
- Проверка индикаторов инструментов мониторинга.
- Создание моментальных снимков.
- SSDT, IDT, IRP-захваты.
- Сброс памяти для подозрительных процессов.
- Вызов функций API Windows.
- Становится неактивным в течение определенного периода времени, чтобы отложить выполнение.
- Создание файлов с действиями, которые должны выполняться через определенные промежутки времени.

Важно
Доклады HTML доступны только на английском языке, несмотря на то, какой язык используется в GravityZone Control Center.

12.3. Повторное представление образца

Из области карточек отправки вы можете повторно отправить детонированные образцы в локальный экземпляр Sandbox Analyzer, не загружая их снова. Вы можете сделать это для образцов, ранее переданных в локальный экземпляр Sandbox Analyzer любым датчиком или методом, автоматически, вручную или через API.

Чтобы повторно отправить образец:

1. Нажмите **Повторно отправить для анализа** в карточке отправки.
2. В окне конфигурации сохраните настройки из предыдущей отправки или измените их следующим образом:

a. В разделе **Управление изображениями** выберите образ виртуальной машины, который вы хотите использовать для детонации.

b. В разделе **Конфигурации детонации** настройте следующие параметры:

   i. **Лимит времени для образца детонации (минуты)**. Выделите фиксированное количество времени для завершения анализа образца. Значение по умолчанию составляет 4 минуты, но иногда анализ может занять больше времени. По истечении настроенного интервала времени Sandbox Analyzer прерывает анализ и генерирует отчет на основе данных, собранных до этого момента. Если проверка прервана до полного завершения, анализ может содержать неточные результаты.

   ii. **Количество разрешенных повторных запусков**. В случае непредвиденных ошибок Sandbox Analyzer пытается взорвать образец, как настроено, до завершения анализа. Значение по умолчанию - 2. Это означает, что Sandbox Analyzer попытается еще два раза проверить образец в случае ошибки.

   iii. **Предфильтрация** . Выберите этот параметр, чтобы исключить из детонации уже проанализированные образцы.

   iv. **Доступ к интернету во время детонации**. Во время анализа некоторые образцы требуют подключения к Интернету для завершения анализа. Для лучшего результата, мы рекомендуем Вам оставить данную опцию включенной.

c. В разделе **Профиль детонации** настройте уровень сложности поведенческого анализа, влияя на пропускную способность Sandbox Analyzer. Например, если установлено значение **Высокое**, Sandbox Analyzer будет выполнять более точный анализ на меньшем количестве образцов за тот же интервал, чем на **Среднее** или **Низкое**.

3. Нажмите **Отправить повторно**.

После повторной отправки на странице **Sandbox Analyzer** отображается новая карта, и срок хранения данных для этого образца соответственно увеличивается.

Примечание
Параметр **Повторно отправить для анализа** доступен для образцов, которые все еще присутствуют в хранилище данных Sandbox Analyzer. Убедитесь, что

хранение данных настроено на странице параметров политики **Sandbox Analyzer > Sandbox Manager** .

12.4. Удаление карточек подачи

Чтобы удалить карточку отправки, которая Вам больше не нужна:

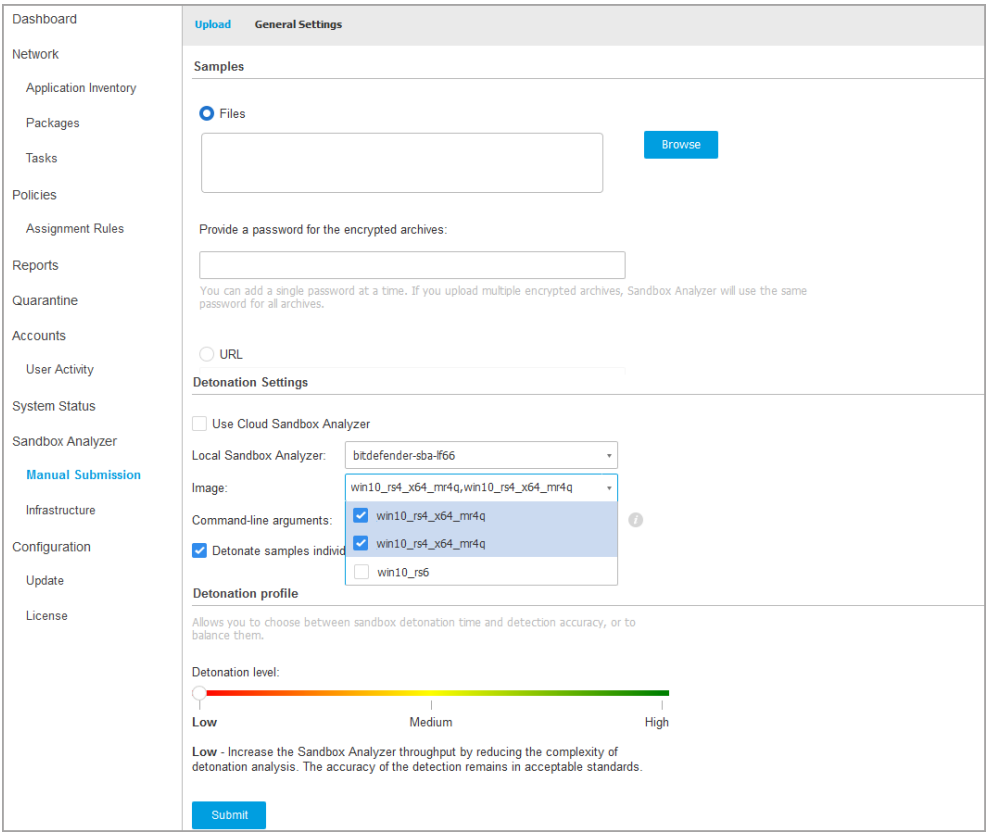
1. Перейдите к карточке отправки, которую Вы хотите удалить.
2. Нажмите **Удалить запись** в левой части карточки.
3. Нажмите **Да**, чтобы подтвердить выбор.

Примечание
Вы удалите только карту отправки, выполнив следующие действия. Информация об отправке по-прежнему доступна в отчете **Sandbox Analyzer Результаты (устарело)** . Однако этот отчет будет по-прежнему поддерживаться только в течение ограниченного периода времени.

12.5. Manual Submission

В **Sandbox Analyzer > Ручная отправка** Вы можете отправить образцы подозрительных объектов в Sandbox Analyzer, чтобы определить, являются ли они угрозами или безвредными файлами. Вы также можете перейти на страницу **Отправка вручную**, нажав кнопку **Отправить образец** в верхнем правом углу области фильтрации на странице Sandbox Analyzer.

Примечание
Sandbox Analyzer Ручное управление совместимо о всеми веб-браузерами, требуемыми Control Center, кроме Internet Explorer 9. Чтобы отправить объекты в Sandbox Analyzer, войдите в Control Center с помощью любого другого поддерживаемого веб-браузера, указанного в «Подключение к Control Center» (p. 21).



Sandbox Analyzer > ручная отправка

Чтобы отправить образцы в Sandbox Analyzer:

1. На странице **Загрузка** в разделе **Образцы** выберите тип объекта:
   a. **Файлы**. Нажмите кнопку **Просмотреть** выберите объекты, которые вы хотите представить для поведенческого анализа. Для архивов, защищенных паролем, Вы можете определить один пароль для каждой загрузки сеанса в специальном поле. В процессе анализа Sandbox Analyzer применяет указанный пароль ко всем отправленным архивам.

b. **URL**. Заполните соответствующие поля с любым URL, который вы хотите проанализировать. Вы можете отправить только один URL за сеанс.

2. В разделе **Параметры детонации** настройка параметров анализа для текущей сессии:

   - Sandbox Analyzer экземпляр, который вы хотите использовать. Вы можете выбрать либо экземпляр Cloud, либо экземпляр Sandbox Analyzer, установленный локально.

     Если вы решили использовать локальный экземпляр Sandbox Analyzer, вы можете выбрать несколько виртуальных машин, на которые вы можете отправить образец одновременно.

   - **Параметры командной строки**. Добавьте столько аргументов командной строки, сколько вы хотите, разделенных пробелами, чтобы изменить работу определенных программ, таких как исполняемые файлы. Параметры командной строки применяются ко всем отправленным образцам во время анализа.

   - **Детонировать образцы индивидуально**. Установите флажок, чтобы файлы из пакета были проанализированы один за другим.

3. В разделе **Профиль детонации** настройте уровень сложности поведенческого анализа, влияя на пропускную способность Sandbox Analyzer. Например, если установлено значение **Высокое**, Sandbox Analyzer будет выполнять более точный анализ на меньшем количестве образцов за тот же интервал, чем на **Среднее** или **Низкое**.

4. В разделе **Общие параметры** вы можете внести конфигурации, которые распространяются на все материалы руководства, независимо от сессии:

   a. **Лимит времени для образца детонации (минуты)**. Выделите фиксированное количество времени для завершения анализа образца. Значение по умолчанию составляет 4 минуты, но иногда анализ может занять больше времени. По истечении настроенного интервала времени Sandbox Analyzer прерывает анализ и генерирует отчет на основе данных, собранных до этого момента. Если проверка прервана до полного завершения, анализ может содержать неточные результаты.

   b. **Количество разрешенных повторных запусков**. В случае непредвиденных ошибок Sandbox Analyzer пытается взорвать образец, как настроено, до завершения анализа. Значение по умолчанию - 2.

Это означает, что Sandbox Analyzer попытается еще два раза проверить образец в случае ошибки.

c. **Предфильтрация** . Выберите этот параметр, чтобы исключить из детонации уже проанализированные образцы.

d. **Доступ к интернету во время детонации**. Во время анализа некоторые образцы требуют подключения к Интернету для завершения анализа. Для лучшего результата, мы рекомендуем Вам оставить данную опцию включенной.

e. Нажмите **Сохранить** чтобы сохранить изменения.

5. Вернитесь к разделу **Загрузка**.
6. Нажмите **Подтвердить**. Шкала загрузки показывает статус отправки.

   После представления, **Sandbox Analyzer** в разделе появится новая карта. Когда анализ будет завершен, карточка обеспечивает вердикт и соответствующие детали.

Примечание
Чтобы вручную отправить образцы к Sandbox Analyzer вы должны иметь права **Управления сетями**

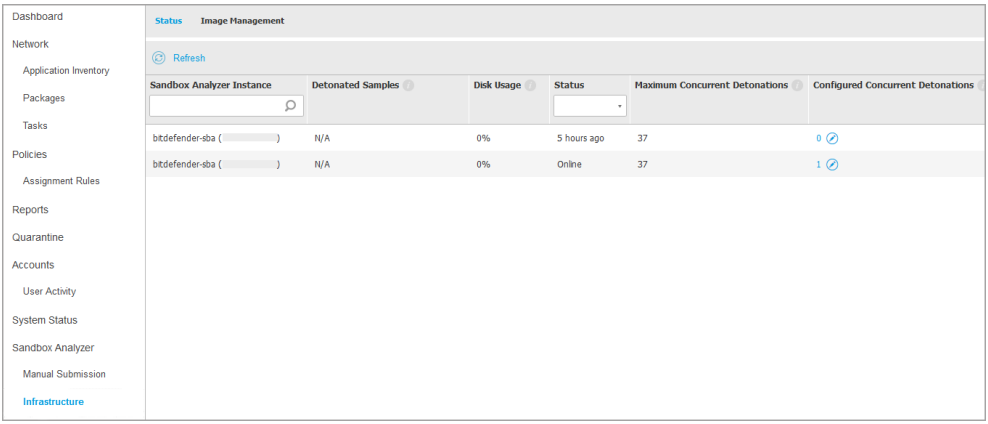
12.6. Инфраструктура управления Sandbox Analyzer

В разделе **Sandbox Analyzer > Инфраструктура**, вы можете выполнить следующие действия, связанные с Sandbox Analyzer экземпляр установлен локально:

- Проверьте статус экземпляра Sandbox Analyzer
- Настроить количество одновременных детонаций
- Проверить статус образов виртуальных машин
- Настроить и управлять образами виртуальных машин

12.6.1. Проверка статуса Sandbox Analyzer

После развертывания и настройки Sandbox Analyzer виртуального устройства на гипервизоре ESXi, вы можете получить информацию о локальных примерах Sandbox Analyzer в разделе **Статус** .



Sandbox Analyzer> Инфраструктура> Статус

В таблице приведены следующие данные:

- **Sandbox Analyzer имя экземпляра**. Каждое имя соответствует экземпляру Sandbox Analyzer установленному на один гипервизор ESXi. Вы можете установить анализатор песочницы на нескольких ESXi гипервизорах.
- **Сдетонировавшие образцы**. Значение указывает количество образцов, проанализированных с момента как экземпляр Sandbox Analyzer был лицензирован в первый раз.
- **Использование диска**. Процентаж указывает объем дискового пространства, используемого Sandbox Analyzer на хранилище данных.
- **Статус**. В этой колонке вы видите информацию о том, что данный Sandbox Analyzer экземпляр онлайн, оффлайн, не установлен, установка продолжается или установка не удалась.
- **Максимальное количество одновременных детонаций**. Значение показывает максимальное число виртуальных машин, которые Sandbox Analyzer может создать, чтобы взорвать образцы. В данный момент времени, одна виртуальная машина может выполнять одну детонации. Количество виртуальных машин определяется количеством аппаратных ресурсов на ESXi.
- **настройка одновременных детонаций**. Это фактическое количество виртуальных машин, созданных на основе имеющейся лицензий.

- **Использовать прокси-сервер**. Нажмите кнопку Вкл/Выкл, чтобы включить или отключить связь между экземплярами GravityZone Control Center и Sandbox Analyzer через прокси-сервер. Чтобы настроить прокси-сервер, перейдите в раздел **Configuration > Proxy** в главном меню Control Center. Если ни один прокси-сервер не установлен, Control Center не поддерживает данную функцию.

  Дополнительные сведения о конфигурации прокси-сервера см. в разделе **Установка защиты > установка и настройка GravityZone > Настройка параметров Control Center > прокси-сервер** в руководстве по установке GravityZone.

  Примечание
  Control Center использует этот прокси-сервер только для связи с экземплярами Sandbox Analyzer On-Premises. Для связи с облачным экземпляром Sandbox Analyzer Control Center использует прокси-сервер, настроенный на странице Sandbox Analyzer параметров политики.
  Этот прокси-сервер также отличается от того, который настроен на странице **Общие > настройки** параметров политики, которая обеспечивает связь между конечными точками и компонентами GravityZone.

Вы можете искать и фильтровать столбцы по имени и статусу экземпляра Sandbox Analyzer. Используйте кнопки в правом верхнем углу таблицы для обновления страницы, а также для отображения и скрытия фильтров и столбцов.

12.6.2. Настройка одновременных детонаций

В разделе **Status**, вы можете настроить количество одновременных детонаций, представляющее количество виртуальных машин, которые могут одновременно работать и детонировать образцы на Sandbox Analyzer. Количество одновременных детонаций зависят от аппаратных ресурсов и лицензий на распространение слотов между несколькими Sandbox Analyzer экземпляров.

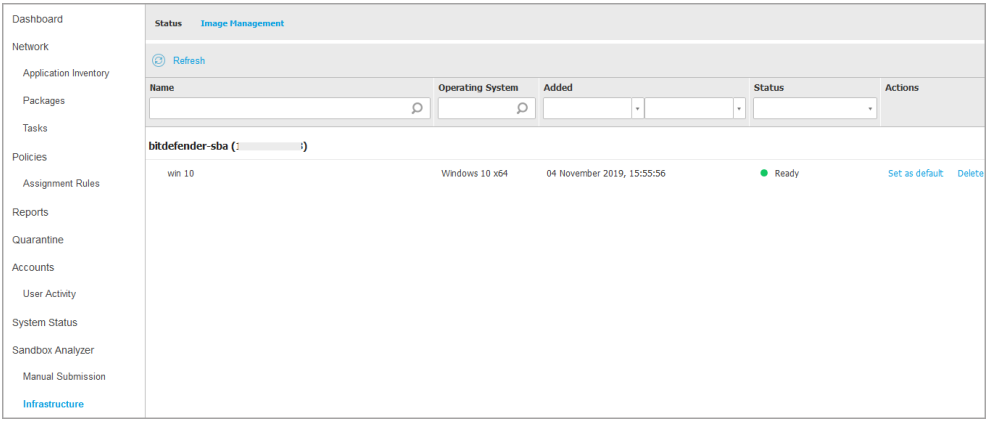
Чтобы настроить количество одновременных детонаций:

1. Нажмите на номер или значок **Edit** в столбце **Configured Concurrent Detonations**.

2. В новом окне укажите в соответствующем поле количество одновременных детонаций, которое вы хотите выделить в Sandbox Analyzer.
3. Нажмите **Сохранить**.

12.6.3. Проверка состояния VM.

Sandbox Analyzer использует образы виртуальных машин в средах детонации для выполнения поведенческого анализа представленных образцов. Вы можете проверить состояние виртуальной машины в **Image Management page**.



Sandbox Analyzer> Инфраструктура> Управление изображениями

В таблице приведены следующие данные:

- **Имя** для существующих образов виртуальных машин, как указано в консоли Sandbox Analyzer. Несколько образов виртуальных машин сгруппированы в одной песочнице анализаторе.
- **Операционная система** как указано в консоли Sandbox Analyzer.
- Время, когда виртуальная машина была добавлена.
- **Статус**. В этом разделе вы узнайте, является ли образ виртуальной машины новым и может быть подготовлен к детонации, готов ли к детонации или процесс подготовки не удалось.

- **Действия**. В этом разделе вы узнайте, что можно сделать с помощью образов виртуальных машин, в зависимости от их статуса: создание изображений для детонации, установка их в качестве среды детонации по умолчанию, или их удаление.

12.6.4. Настройка и управление VM

Строение детонации виртуальных машин

Чтобы взорвать образцы с помощью локального экземпляра в песочнице анализаторе, вам нужно построить специальные виртуальные машины. В разделе **Управление изображениями** вы можете создавать детонации виртуальных машин, если вы добавили образы виртуальных машин в песочнице анализаторе.

Примечание
Чтобы узнать, как добавить VM в Sandbox Analyzer консоли прибора, обратитесь к **Установка Sandbox Analyzer Виртуальное устройство** к разделу руководство по установке в GravityZone.

яЧтобы создать детонационные виртуальные машины, в столбце **Действия** выберите параметр **Создать образ** для образов виртуальных машин, имеющих статус: **Новое-требуется сборка**. Создание виртуальной машины обычно требуется от 15 до 30 минут, в зависимости от её размера. Когда сборка будет завершена, статус виртуальной машины изменения на **Готово**.

Настройка виртуальной машине по умолчанию

В Sandbox Analyzer может иметь несколько изображений и установлен и настроен на детонация виртуальных машин. В случае автоматического регистрации, Sandbox Analyzer будет использовать первый созданный образ виртуальной машины, чтобы взорвать образцы.

Вы можете изменить это поведение, настроив изображения виртуальную машину по умолчанию. Для этого нажмите кнопку **Установить по умолчанию** для предпочтительного образа виртуальной машины.

Удаление Виртуальных Машин

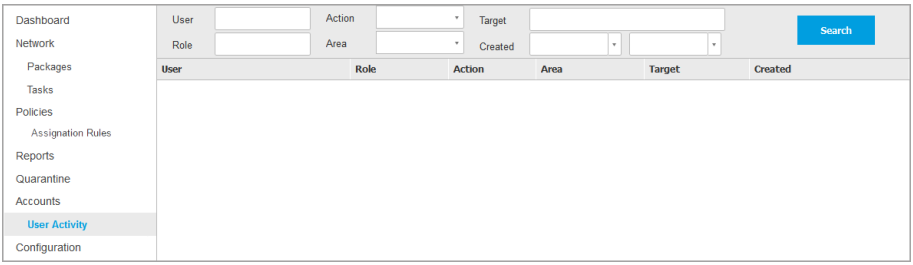
Чтобы удалить образ виртуальной машины в разделе **Управление изображениями** , выберите **Удалить** в колонке**Действия**. В окне подтверждения нажмите **Удалить изображение**.

13. ЖУРНАЛ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЯ

Control Center регистрирует все операции и действия, выполняемые пользователями. В зависимости от уровня ваших администраторских разрешений, список действий пользователя может включать в себя следующие события:

- Вход и выход (в/из аккаунта)
- Создание, редактирование, переименование и удаление отчетов
- Добавление и удаление портлетов информационной панели
- Создание, редактирование и удаление учетных данных
- Создание, изменение, загрузка и удаление сетевых пакетов
- Создание сетевых задач
- Запуск, завершение, отмена и остановка процессов устранения неполадок на зараженных компьютерах
- Создание, редактирование, переименование и удаление учетных записей пользователей
- Удаление или перемещение конечных точек между группами
- Создание, перемещение, переименование и удаление групп
- Удаление и восстановление файлов из карантина
- Создание, редактирование и удаление учетных записей пользователей
- Создание, редактирование и удаление правил доступа.
- Создание, редактирование, переименование, назначение и удаление политик
- Редактирование параметров аутентификации для учетных записей GravityZone.
- Создание, редактирование, синхронизация и удаление интеграции с Amazon EC2
- Создание, редактирование, синхронизация и удаление интеграций Microsoft Azure
- Обновление устройства GravityZone.

Чтобы изучить записи действий пользователей, перейдите на страницу **Аккаунты > Действия пользователя** и выберите требуемый вид сети из меню видов сетей.



Страница действий пользователя

Для отображения записанных событий, которые вас интересуют, вы должны задать искомые слова. Заполните имеющиеся поля критериями поиска и нажмите кнопку **Поиск**. Все записи, соответствующие вашим критериям, будут отображены в таблице.

В столбцах таблицы будут представлены полезные сведения о перечисленных событиях:

- Имя пользователя, который совершил действие.
- Роль пользователя.
- Действие, которое вызвало событие.
- Тип объекта консоли, затронутый действием.
- Конкретный объект консоли, затронутый действием.
- Время, когда произошло событие.

Чтобы отсортировать события по конкретному столбцу, просто нажмите на заголовок этого столбца. Щелкните заголовок столбца еще раз, чтобы изменить порядок сортировки.

Для просмотра подробной информации о событии, выберите его и проверьте раздел под таблицей.

14. ИСПОЛЬЗОВАНИЕ ИНСТРУМЕНТОВ

14.1. Ввод инструментов пользователя с HVI

Bitdefender HVI освобождает вас от бремени проблем,связанных с устранением неполадок, сбора данных для судебных экспертиз или выполнения регулярных задач по техническому обслуживанию на виртуальных машинах в среде Citrix, благодаря возможности быстро вводить сторонние инструменты внутри гостевой операционной системы. Эти операции выполняются при помощи Direct inspect API (не требуется TCP/IP-соединение), не беспокоя конечных пользователей. Для этой цели инструменты должны работать бесшумно.

GravityZone предоставляет 3 ГБ свободного пространства для сохранения инструментов в безопасности.

Для загрузки наборов инструментов в GravityZone:

1. Загрузите на компьютер последнюю версию набора инструментов.
2. Архивируйте комплект в ZIP-файл.
3. Перейдите к GravityZone Control Center и нажмите в нижнем левом углу страницы меню **Инструменты**. Будет отображена страница **Центр управления инструментами**.
4. Нажмите соответствующую кнопку загрузки в верхней части таблицы: **Загрузить инструмент Windows** или **Загрузить инструмент Linux**
5. Если средства предназначены для Windows, необходимо также выбрать соответствующую архитектуру компьютера из раскрывающегося меню.
6. Найдите ZIP-файл, выделите его и нажмите кнопку **Открыть**.

   Если размер файлов большой, возможно, придется подождать несколько минут, пока загрузка не будет завершена. По завершении работы инструмент будет добавлен в таблицу, а индикатор выполнения, расположенный над таблицей, будет информировать о доступном пространстве для дальнейших загрузок.

Наряду с именем инструмента в таблице отображены более полезные сведения, такие как:

- Операционная система и платформа, на которой запускается средство.
- Краткое описание инструмента. Вы можете изменить это поле по желанию.

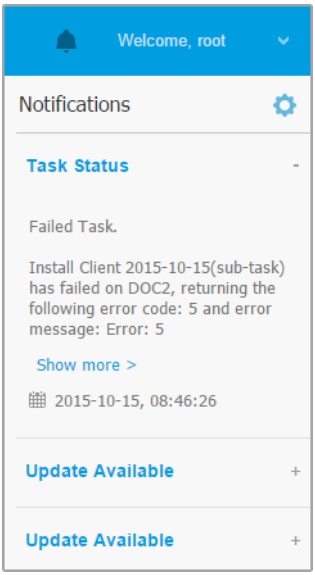
- Имя пользователя, загрузившего инструмент.
- Статус загрузки. Чтобы убедиться в успешной загрузке инструмента, проверьте это поле.
- Дата и время загрузки.

Затем можно запланировать время для введения средства, используя политики, или вводить их в любое время, запустив задачи на странице **Сеть**.

Если инструменты больше не используются, выделите их и нажмите в верхней части таблицы кнопку **Удалить**, чтобы удалить их. Подтвердите, нажав кнопку **Да**.

15. УВЕДОМЛЕНИЯ

В зависимости от событий, которые могут произойти в вашей сети, Control Center отобразит различные уведомления, чтобы проинформировать вас о состоянии безопасности вашей среды. Уведомления будут отображаться в **Область уведомлений**, расположенной в правой части Control Center.



Область уведомлений

Когда будут обнаружены новые события в сети, значок 11 в правом верхнем углу Control Center будет отображать количество недавно выявленных событий. Нажав на значок, отобразится область уведомлений, содержащая список обнаруженных событий.

15.1. Типы уведомлений

Список доступных типов уведомлений:

Вспышка вредоносного ПО

Это уведомление направляется пользователям при заражении не менее 5% устройств от числа всех управляемых объектов сети, зараженных одной и той же вредоносной программой.

Вы можете сконфигурировать порог срабатываний на вредоносное ПО в окне **Параметры уведомлений**. Для получения более подробной информации, обратитесь к «Настройка параметров уведомлений» (p. 588).

Угрозы, обнаруженные HyperDetect, выходят за рамки этого уведомления.

Доступные форматы системного журнала: JSON, CEF

Истечение срока действия лицензии

Это уведомление отправляется за 30, 7 и 1 день до истечения срока действия лицензии.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Доступные форматы системного журнала: JSON, CEF

Лимит использования лицензии достигнут

Это уведомление отправляется, когда все доступные лицензии использованы.

Доступные форматы системного журнала: JSON, CEF

Срок действия лицензии подходит к концу

Это уведомление отправляется, когда использовано 90% имеющихся лицензий.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Доступные форматы системного журнала: JSON, CEF

Достигнут лимит использования лицензий для серверов.

Это уведомление отправляется, когда количество защищаемых серверов достигает предела, указанного в вашем лицензионном ключе.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Доступные форматы системного журнала: JSON, CEF

Лимит лицензирования серверов почти достигнут.

Это уведомление отправляется, когда использовано 90% имеющихся серверных лицензий.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Доступные форматы системного журнала: JSON, CEF

Лимит использования лицензий Exchange достигнут

Это уведомление срабатывает каждый раз, когда количество защищаемых почтовых ящиков на сервере Exchange достигает предельного значения, указанного в лицензионном ключе.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Доступные форматы системного журнала: JSON, CEF

Не верные учетные данные пользователя Exchange

Данное уведомление отправляется, когда задача сканирования по требованию не может быть запущена на выбранном сервере Exchange из-за неправильных учетных данных пользователя Exchange.

Доступные форматы системного журнала: JSON, CEF

Состояние обновления версии продуктов

Это уведомление запускается еженедельно, если в сети обнаружены старые версии продукта.

Доступные форматы системного журнала: JSON, CEF

Доступно обновление

Это уведомление информирует вас о наличии новой версии GravityZone - нового пакета обновления или нового продукта.

Доступные форматы системного журнала: JSON, CEF

Подключение к сети Интернет

Это уведомление срабатывает, когда обнаружено изменение в подключении к сети Интернет следующими процессами:

- Проверка лицензии
- Получение запроса на подписание сертификата Apple
- Связь с мобильными устройствами Apple и Android

- Доступ к аккаунту MyBitdefender

Доступные форматы системного журнала: JSON, CEF

Соединение SMTP

Это уведомление отправляется каждый раз, когда Bitdefender GravityZone обнаруживает изменения, касающиеся подключения почтового сервера.

Доступные форматы системного журнала: JSON, CEF

Пользователи мобильных устройств без адресов электронной почты

Это уведомление отправляется после добавления мобильных устройств нескольким пользователям и когда у одного или нескольких выбранных пользователей отсутствует адрес электронной почты в учетной записи. Это уведомление предназначено, чтобы предупредить вас, что за пользователями, с неуказанными адресами электронной почты, не могут быть зарегистрированы мобильные устройства, закрепленые за ними, так как детали активации должны быть автоматически отправлены по электронной почте.

Для получения подробной информации о добавлении мобильных устройств нескольким пользователям, обратитесь к руководству по установке GravityZone.

Доступные форматы системного журнала: JSON, CEF

Резервное копирование базы данных

Это уведомление информирует вас о состоянии запланированного резервного копирования базы данных - успешное или неудачное. Если резервное копирование базы данных не удалось, уведомление также отобразит причину сбоя.

Для получения подробной информации о настройках резервного копирования базы данных GravityZone, обратитесь к руководству по установке GravityZone.

Доступные форматы системного журнала: JSON, CEF

Обнаружение вредоносного ПО на серверах Exchange

Это уведомление предупредит вас при обнаружении вируса на сервере Exchange в вашей сети.

Доступные форматы системного журнала: JSON, CEF

Advanced Anti-Exploit

Это уведомление информирует вас, когда Advanced Anti-Exploit обнаружил попытки использования в вашей сети.

Доступные форматы системного журнала: JSON, CEF

Событие о вредоносном ПО

Это уведомление предупредит вас при обнаружении вредоносного ПО на конечном устройстве в вашей сети. Данное уведомление создано для обнаружения зловредных программ и обеспечивает сведениями о поврежденных конечных точках (имя, IP), распознанных угрозах, версии подписи, времени обнаружения и типе сканирующего двигателя.

Доступные форматы системного журнала: JSON, CEF

Вне интеграции синхронизации

Это уведомление отправляется, когда существующая интеграция с виртуальной платформой не может синхронизироваться с GravityZone. В настройках уведомлений вы можете выбрать интеграцию, для которой желаете получать уведомления при возникновении ошибки синхронизации. Вы можете получить больше информации о статусе синхронизации в деталях уведомления.

Доступные форматы системного журнала: JSON, CEF

Событие Антифишинга

Это уведомление информирует вас каждый раз, когда агент конечного устройства блокирует несанкционированный доступ к известному фишинговому сайту. Это уведомление также содержит такие детали, как попытки конечного устройства получить доступ к небезопасным веб-сайтам (имя и IP-адрес), установленный агент или заблокированый URL.

Доступные форматы системного журнала: JSON, CEF

События межсетевого экрана

Данное уведомление информирует вас каждый раз, когда модуль межсетевого экрана установленного агента блокирует какие-нибудь сетевые приложения или попытки сканирования портов, в соответствии с применяемой политикой безопасности.

Доступные форматы системного журнала: JSON, CEF

События ATC/IDS

Это уведомление отправляется каждый раз, когда потенциально опасное приложение обнаружено и заблокировано на конечном устройстве в вашей сети. Вы найдете подробную информацию о типе приложения, имени и пути, а также ID родительского процесса и его путь, и командную строку, которая запустила процесс в данном случае.

Доступные форматы системного журнала: JSON, CEF

События контроля пользователя

Это уведомление срабатывает каждый раз, когда активность пользователя, такая как просмотр веб-страниц или используемое программное обеспечение, блокируется клиентом конечного устройства в соответствии с применяемой политикой безопасности.

Доступные форматы системного журнала: JSON, CEF

События защиты данных

Это уведомление формируется каждый раз, когда трафик блокируется на конечном устройстве в соответствии с правилами защиты данных.

Доступные форматы системного журнала: JSON, CEF

События модуля приложений

Это уведомление направляется каждый раз, когда модуль безопасности в установленном агенте отключается или включается.

Доступные форматы системного журнала: JSON, CEF

События состояния Security Server

Этот тип уведомлений содержит информацию об изменениях статуса определенного Security Server, установленного в вашей сети. Изменение статуса Security Server может быть вызвано следующими причинами: сервер выключается или включается, выполняется обновление продукта, обновляются механизмы защиты и требуется перезагрузка.

Доступные форматы системного журнала: JSON, CEF

Событие о перегрузке Security Server

Это уведомление отправляется, когда нагрузка при сканировании на Security Server в вашей сети превышает установленный порог.

Доступные форматы системного журнала: JSON, CEF

События регистрации продуктов

Это уведомление информирует вас, когда статус регистрации агента, установленного в вашей сети, изменяется.

Доступные форматы системного журнала: JSON, CEF

Аудит аутентификации

Это уведомление информирует вас, когда другая учетная записьGravityZone, исключая вашу собственную, была использована, чтобы войти в Control Center с нераспознанного устройства.

Доступные форматы системного журнала: JSON, CEF

Вход в систему с нового устройства

Это уведомление сообщает вам, что ваша учетная запись GravityZone была использована, чтобы войти в Control Center с устройства, которое вы не использовали для этих целей ранее. Уведомление автоматически настраивается таким образом, чтобы передаваться как в Control Center, так и по электронной почте и только вы сможете просмотреть его.

Доступные форматы системного журнала: JSON, CEF

Сертификат Истекает

Это уведомление информирует вас о том, что сертификат безопасности истекает. Уведомление направляется за 30, семь и один день до истечения срока действия.

Доступные форматы системного журнала: JSON, CEF

GravityZone Обновлен

Это уведомление отправляется, когда обновление GravityZone завершено. Если произошла ошибка, то обновление будет запущено снова в течение 24 часов.

Доступные форматы системного журнала: JSON, CEF

Статус задачи

Данное уведомление предупредит вас, когда статус задания изменен или только при завершении задания, в соответствии с вашими настройками.

Доступные форматы системного журнала: JSON, CEF

Сервер обновлений устарел

Это уведомление отправляется, когда сервер обновлений в вашей сети имеет устаревшие механизмы защиты.

Доступные форматы системного журнала: JSON, CEF

Событие сетевых инцидентов

Это уведомление отправляется каждый раз, когда модуль Network Attack Defense обнаруживает попытку атаки в вашей сети. Это уведомление также информирует вас о том, была ли предпринята попытка атаки извне сети или из скомпрометированной конечной точки в сети. Другие сведения включают данные о конечной точке, технике атаки, IP-адресе злоумышленника и действиях предпринятых Network Attack Defense.

Доступные форматы системного журнала: JSON, CEF

Обнаружено нарушение памяти

Это уведомление информирует вас, когда HVI обнаруживает атаку, нарушающую работу памяти защищенных виртуальных машин в среде Citrix Xen. Уведомление предоставит вам важные подробности, такие как имя и IP-адрес зараженной машины, описание инцидента, источник и цель атаки, меры, предпринятые для устранения угрозы, и время обнаружения.

Уведомления создаются в следующих случаях:

- Попытки использовать область памяти в других целях, отличных от намерений гипервизора, с помощью таблицы расширенния страниц (EPT).
- Попытки процессов внедрить код в другие процессы.
- Попытки изменить адреса процессов в таблицах перевода.
- Попытки изменить модель определенных регистров (MSR).
- Попытки изменить содержание определенных объектов драйверов или таблицы дескрипторов прерываний (IDT).
- Попытки загрузить в специальные контролируемые регистры (CR) недопустимые значения.
- Попытки загрузить в определенные расширенные регистры управления (XCR) недопустимые значения.
- Попытки изменить таблицу глобальных дескрипторов или таблицу дескрипторов прерываний.

Примечание

Функция HVI может быть доступна для вашего решения GravityZone с отдельным лицензионным ключом.

Доступные форматы системного журнала: JSON, CEF

Новое приложение в инвентаризации приложений

Это уведомление информирует вас, когда модуль Управления приложениями обнаружит новое приложение, установленное на контролируемых конечных точках.

Доступные форматы системного журнала: JSON, CEF

Sandbox Analyzer обнаружение

Это уведомление будет появляться каждый раз, когда Sandbox Analyzer обнаружит новую угрозу среди среди представленных файлов. Вам предоставляются такие данные, как имя хоста или IP-адрес конечной точки, время и дата обнаружения, тип угрозы, путь, имя, размер файлов и действия по исправлению, предпринятые для каждого из них.

Примечание

Вы не будете получать уведомления о чистых проанализированных образцах. Информация обо всех отправленных образцах доступна в отчете **Результаты Sandbox Analyzer (устарело)** и в разделе **Sandbox Analyzer**, в главном меню Control Center.

Доступные форматы системного журнала: JSON, CEF

активность по обнаружению гипервизора

Это уведомление информирует вас при обнаружении в сети любых вредоносных или незаблокированных событий. Это уведомление отправляется при каждом событии HyperDetect и содержит следующие данные:

- Сведения об уязвимой конечной точке (имя, IP-адрес, установленный агент)
- Тип и имя вредоносного по
- Зараженный путь к файлу. Для атак с меньшим количеством файлов предоставляется имя исполняемого файла, используемого в атаке.
- Состояние заражения
- Хэш SHA256 исполняемого вредоносного файла
- Тип предполагаемой атаки (целевая атака, нежелательная программа, эксплойты, программы-вымогатели, подозрительные файлы и сетевой трафик)

- Уровень обнаружения (Рекомендуемый, Нормальный, Интенсивный)
- Время и дата обнаружения

Доступные форматы системного журнала: JSON, CEF
Вы можете просматривать сведения об инфекции и продолжать изучать проблему, создав отчет **Активность HyperDetect** на странице **Уведомления**. Для этого:

1. В Control Center, нажмите кнопку **Уведомления** чтобы отобразить область уведомлений.
2. Нажмите ссылку **Показать больше** в конце уведомления, чтобы открыть страницу **Уведомления**.
3. Нажмите кнопку **Просмотр отчета** в деталях уведомлений. Это действие открывает окно конфигурации отчета.
4. Если необходимо, проведите конфигурацию отчета. Для получения более подробной информации, обратитесь к «Создание отчетов» (p. 534).
5. Нажмите **Создать**.

Примечание
Чтобы избежать спама, вы будете получать максимум одно уведомление в час.

Вне интеграции синхронизации

Это уведомление информирует вас о проблемах интеграции и невозможности синхронизации. Это может произойти из-за различных факторов, таких как измененные параметры интеграции или временной недоступности сервера.

Доступные форматы системного журнала: JSON, CEF

Ошибка патча отсутствует

Это уведомление появляется,когда в конечных точках вашей сети отсутствуют 1 или 2 доступных патча.

GravityZone автоматически отправляет уведомление, содержащее все результаты за последние 24 часа, до даты уведомления.

Вы можете просмотреть какая конечная точка находится в этой ситуации, нажав кнопку **Просмотреть отчет** в деталях уведомления.

По умолчанию уведомление отсылает к исправлениям безопасности, но вы можете настроить его так, чтобы оно также сообщало вам о исправлениях, не относящихся к безопасности.

Доступные форматы системного журнала: JSON, CEF

Новый инцидент

Это уведомление информирует Вас о появлении нового инцидента. После включения уведомления генерируются каждый раз, когда новый инцидент отображается в разделе **Инциденты** Центра управления. Соответствующее событие системного журнала содержит список релевантных элементов, извлеченных из сведений об инциденте, которые можно использовать для обогащения информации о безопасности и корреляций событий (SIEM). Для получения большей информации нажмите на **Название инцидента**.

Доступные форматы системного журнала: JSON, CEF

Хранение вредоносных программ

Это уведомление отправляется при обнаружении вредоносного ПО на устройстве хранения, совместимом с ICAP. Это уведомление создается при каждом обнаружении вредоносных программ и предоставляет сведения о зараженном устройстве хранения (имя, IP-адрес, тип), вредоносном ПО и времени обнаружения.

Доступные форматы системного журнала: JSON, CEF

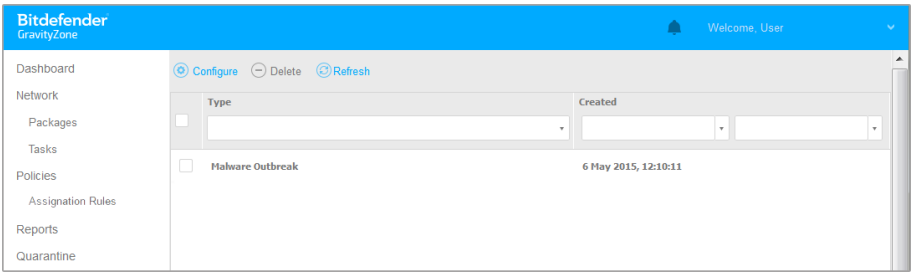
Заблокированные устройства

Это уведомление инициируется, когда к конечной точке подключается заблокированное устройство или устройство с разрешением только для чтения. Если одно и то же устройство подключается несколько раз в течение одного часа, в течение этого интервала отправляется только одно уведомление. Если устройство снова подключается через час, выдается новое уведомление.

Доступные форматы системного журнала: JSON, CEF

15.2. Просмотр уведомлений

Для просмотра уведомлений нажмите кнопку **Уведомления** и далее нажмите **Посмотреть все уведомления**. Появится таблица, содержащая все уведомления.



Страница уведомлений

В зависимости от количества уведомлений, таблица может занимать несколько страниц (по умолчанию отображается по 20 записей на странице).

Для перемещения по страницам используйте кнопки навигации в нижней части таблицы.

Чтобы изменить количество записей отображаемых на странице, введите другое значение в поле рядом с кнопками навигации.

Если записей слишком много, вы можете использовать поисковые поля под заголовками столбцов или меню фильтра в верхней части таблицы, чтобы отфильтровать отображаемые данные.

- Чтобы отфильтровать уведомления, выберите тип уведомлений, которые вы хотите увидеть, в меню **Тип**. По желанию, можно выбрать временной интервал, в течение которого уведомления были сгенерированы, чтобы уменьшить количество записей в таблице, особенно при большом количестве сгенерированных уведомлений.
- Для просмотра деталей уведомления, нажмите на его имя в таблице. Раздел **Подробная информация** отображается ниже таблицы, где вы можете увидеть событие, которое сгенерировало уведомление.

15.3. Удаление уведомлений

Чтобы удалить уведомления:

1. Нажмите кнопку **Уведомления** в правой части панели меню, затем нажмите **Просмотреть все уведомления**. Появится таблица, содержащая все уведомления.
2. Выберите уведомления, которые вы хотите удалить.

3. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

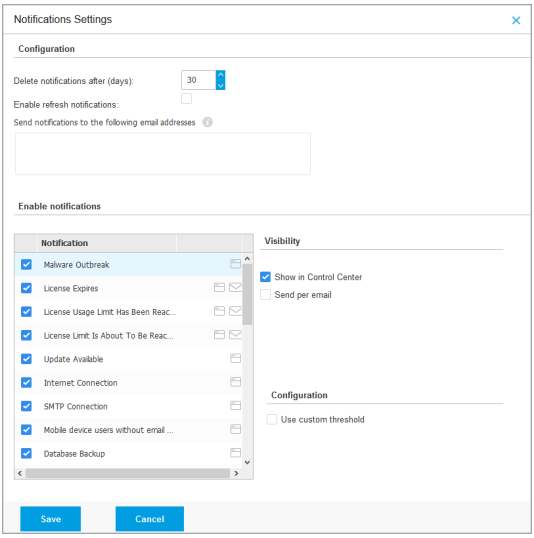
Вы также можете настроить уведомления для автоматического удаления после определенного количества дней. Для получения более подробной информации, обратитесь к «Настройка параметров уведомлений» (p. 588).

15.4. Настройка параметров уведомлений

Тип уведомлений для отправки и адреса электронной почты, на которые они отправляются, могут быть настроены для каждого пользователя.

Чтобы настроить параметры уведомлений:

1. Нажмите кнопку **Уведомления** в правой части панели меню, затем нажмите **Просмотреть все уведомления**. Появится таблица, содержащая все уведомления.
2. Нажмите кнопку Настроить в верхней части таблицы. Отобразится окно **Настройки уведомлений**.



Настройки уведомлений

Примечание
Вы также можете получить доступ к окну **Параметры уведомлений** напрямую, используя значок **Настроить** в правом верхнем углу окна **Область уведомлений**.

3. В разделе **Настройки** вы можете задать следующие настройки:
   - Автоматическое удаление уведомлений по истечении определенного периода времени. Установите любое желаемое число от 0 до 365 в поле **Удалить уведомления через (дней)** .
   - Отметьте флажок **Включите уведомления об обновлениях**, если вы хотите, чтобы область уведомлений автоматически обновлялась каждые 60 секунд.
   - Кроме того, вы можете отправлять уведомления определенным получателям по электронной почте. Введите адреса электронной почты в соответствующее поле, нажав `Enter` после каждого адреса.
4. В разделе **Включить уведомления** вы можете выбрать тип уведомлений, которые хотите получать от GravityZone. Вы также можете настроить видимость и параметры отправки индивидуально, для каждого типа уведомлений.

   Выберите желаемый тип уведомлений из списка. Для получения более подробной информации, обратитесь к «Типы уведомлений» (p. 576). Когда выбран тип уведомлений, вы можете настроить его конкретные параметры (если доступно) в правой части:

Видимость

- **Показ в Control Center** обозначает, что этот тип событий отображается в Control Center с помощью значка **Область уведомлений**.
- **Отправить журнал на сервер** обозначает, что данный тип событий также отправляется в файл `syslog`, в случае если syslog-сервер сконфигурирован.

  Чтобы узнать о том, как настроить syslog-серверы, обратитесь к Руководству по установке GravityZone.
- **Отправить по электронной почте** указывает, что этот тип событий будет также отправляться на некоторые адреса электронной почты.

В этом случае вы должны ввести адреса электронной почты в выделенном поле, нажав `Enter` после каждого адреса.

Конфигурация

- **Использовать пользовательский порог** - позволяет определить порог для количества произошедших событий, после которого выбранные уведомления будут отправлены.

  Например, уведомление о вспышках заражения вредоносным ПО отправляется по умолчанию пользователям, если не менее 5% всех управляемых объектов сети заражены одним и тем же вредоносным ПО. Чтобы изменить порог срабатывания о вспышках заражения, разрешите опцию **Использовать пользовательский порог**, затем введите желаемое значение в поле **Порог вспышки вредоносного ПО**.

- Для уведомления **Database Backup** вы можете выбрать только получение уведомлений о сбое резервного копирования. Оставьте эту опцию неотмеченной, если хотите получать уведомления о всех событиях, связанных с резервным копированием.

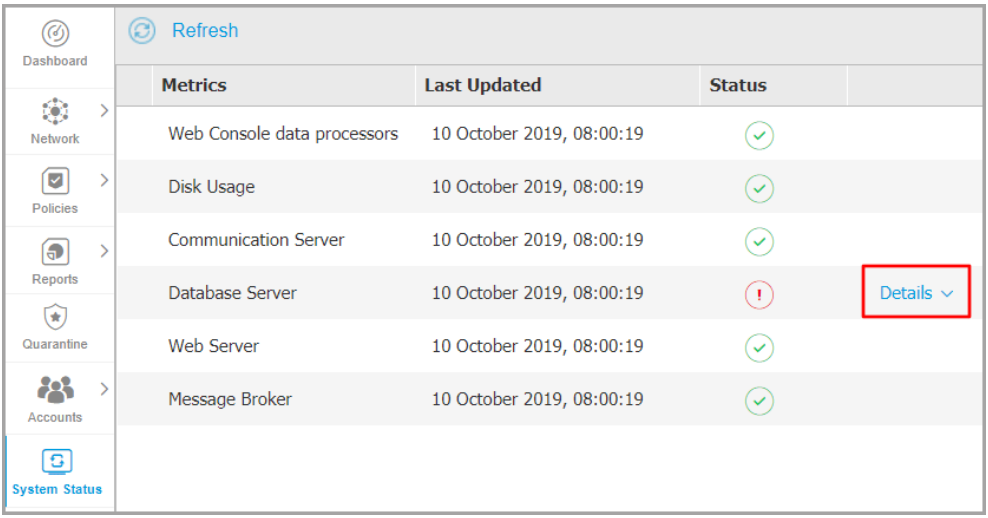
- Для **Статуса события Security Server** вы можете выбрать события Security Server, которые будут вызывать этот тип уведомления:
  - **Устарел** - уведомляет каждый раз, когда Security Server в вашей сети устарел.
  - **Powered off** - уведомляет каждый раз, когда Security Server в вашей сети выключен.
  - **Требуется перезагрузка** - уведомляет каждый раз, когда Security Server в вашей сети требует перезагрузки.

- Для **Статус задачи**, вы можете выбрать тип статуса, который будет вызывать следующий тип уведомлений:
  - **Любой статус** - уведомляет каждый раз, когда задача Control Center завершена с любым статусом.
  - **Только незавершенные** - уведомляет каждый раз, когда задача Control Center завершилась неудачей.

5. Нажмите **Сохранить**.

16. СТАТУС СИСТЕМЫ

На странице **Статус системы** отображается информация о состоянии работоспособности развертывания GravityZone, что упрощает просмотр при возникновении неполадок. На странице представлены системные показатели, их статус и когда они были обновлены в последний раз, все отображаются в виде сетки.



Страница статуса системы

В столбце **Показатели** отображаются все индикаторы, отслеживаемые GravityZone Control Center. Подробнее о каждой показатели и статусе сообщений см. В разделе «Процессоры данных» (p. 616).

В столбце **Последнее обновление** отображаются дата и время последней проверки состояния метрики.

В столбце **Статус** отображается состояние каждой метрики: **OK** или **Внимание**. **Статус** показателя обновляется каждые 15 минут или каждый раз, когда вы нажимаете кнопку **Обновить**

16.1. Состояние OK

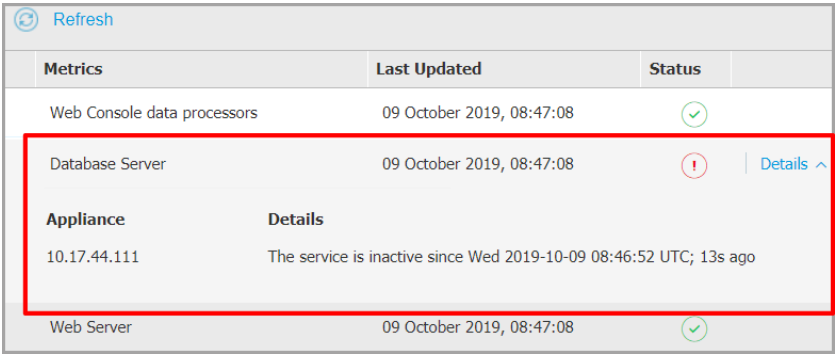
Статус OK указывает на то, что показатель ведет себя нормально. Никаких дополнительных подробностей в этом случае не отображается.

16.2. Статус учетной записи

Статус учетной записи отображает метрику, которую невозможно запустить при нормальных параметрах

В данном случае Вам следует понять, что произошло и выбрать текущие действия:

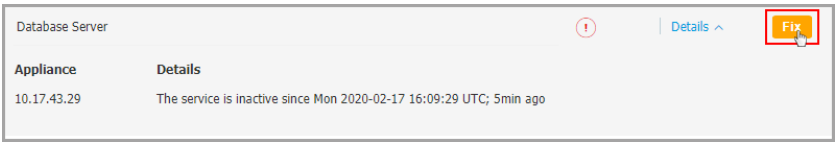
1. Нажмите кнопку **Подробности** чтобы развернуть дополнительную информацию, связанную с рассматриваемым параметром.



Детали параметров

- В разделе **Устройство** вы можете найти IP-адреса зараженных компьютеров.
- В разделе **Подробности** вы можете просмотреть информацию, относящуюся к каждому параметру.

2. Нажмите **Fix** для восстановления метрики и GravityZone сделает все за Вас.



Детали параметров

Статус метрики будет отвернут от **OK** до тех пор, пока он не будет исправлен.

Примечание
Для другой метрики, относящейся к делу, свяжитесь с Командой по поддержке предприятия.

16.3. Параметры

Страница **System Status** содержит сведения о следующих показателях:

- Процессоры данных веб-консоли
- Использование диска
- Коммуникационный Сервер
- Сервер базы данных
- Веб-сервис
- Брокер сообщений

Процессоры данных веб-консоли

Этот показатель отслеживает состояние процессоров данных, которые используются для компиляции данных, отображаемых в Control Center.

Сообщение о возможной проблеме статуса	Подробная информация
`Процессоры, которые вышли из строя на этом устройстве: <массив процессоров данных> .`	Один или несколько процессоров данных остановлены.

Сообщение о возможной проблеме статуса	Подробная информация
Виртуальное устройство не работает	Виртуальное устройство, использующее службы веб-консоли, остановлено.

Полный список процессоров, используемых Control Center, см. в «Процессоры данных» (p. 616).

Использование диска

Этот показатель отслеживает объем дискового пространства, используемого на каждом виртуальном устройстве, объем оставшегося свободного места, а также общее пространство на диске. Если какой-либо из дисков используется выше 80%, параметр отображает статус **Внимание**

Сообщение о возможной проблеме статуса	Подробная информация
Используемое место на диске (имя диска)	Один или несколько дисков используются свыше 80% их максимальной емкости.
Виртуальное устройство не работает	Указанное виртуальное устройство отключено.

Коммуникационный Сервер

Этот показатель отслеживает связь между агентами безопасности, установленными на ваших конечных точках, и сервером базы данных.

Сообщение о возможной проблеме статуса	Подробная информация
Служба неактивна <timestamp>	Данный сервис остановлен.

Сервер базы данных

Этот показатель отслеживает состояние базы данных GravityZone.

Сообщение о возможной проблеме статуса	Подробная информация
Служба неактивна <timestamp>	Сервис перестал работать на одном из устройств.
Виртуальное устройство не работает	Виртуальное устройство, использующее сервер базы данных, выключено.

Веб-сервис

Этот показатель отслеживает состояние веб-сервера, на котором размещается GravityZone Control Center.

Сообщение о возможной проблеме статуса	Подробная информация
Служба неактивна <timestamp>	Сервер перестал работать на одном из устройств.
Виртуальное устройство не работает	Виртуальное устройство, использующее этот сервер, выключено.

Брокер сообщений

Этот показатель отслеживает состояние службы брокера сообщений на устройствах с ролями веб-консоли и сервера связи.

Сообщение о возможной проблеме статуса	Подробная информация
Служба брокера сообщений не работает на этом устройстве	Сервис перестал работать на одном из устройств.
Не удалось установить сетевое соединение между устройствами	Связь между двумя приборами прервана.
Виртуальное устройство не работает	Виртуальное устройство, использующее этот сервис, отключено.

17. ПОЛУЧЕНИЕ СПРАВКИ

Bitdefender стремится предоставить своим клиентам быструю и качественную техподдержку. Если у вас возникли проблемы или если у вас есть какие-либо вопросы о продуктах Bitdefender, перейдите в наш Онлайн центр поддержки. В нем доступны ресурсы, с помощью которых можно быстро найти решение или ответ. Или при необходимости можно обратиться в службу поддержки клиентов Bitdefender. Представители службы поддержки быстро ответят на все вопросы и окажут необходимую помощь.

Примечание
В центре техподдержки можно найти информацию о предоставляемых услугах техподдержки, а также правилах их предоставления.

17.1. Центр поддержки Bitdefender

Bitdefender Центр поддержки это раздел, где вы найдете всю необходимую помощь по продуктам Bitdefender.

Доступные ресурсы можно использовать для быстрого нахождения решения или ответа:

- Статьи базы знаний
- Форум поддержки Bitdefender
- Документация по продукту

Также можно воспользоваться поисковой системой для получения дополнительных сведений о компьютерной безопасности, продуктах Bitdefender и самой компании.

Статьи базы знаний

База знаний Bitdefender - онлайн хранилище информации о продуктах Bitdefender. Здесь хранятся в удобном для доступа формате отчеты о результатах текущих операций по технической поддержке и исправлению ошибок, выполняемых службой поддержки и разработки Bitdefender, а также статьи по предотвращению заражения вирусами, управлению решениями Bitdefender с подробными разъяснениями, а также другая информация.

База знаний Bitdefender открыта для общего доступа с возможностью свободного поиска. Bitdefender содержит обширную информацию,

предоставляя клиентам необходимые технические сведения. Все действующие информационные запросы или отчеты об ошибках, поступающие от клиентов Bitdefender, могут быть найдены в базе знаний Bitdefender, такие как отчеты по исправлениям, устранению неполадок и информационные статьи, дополняющие файлы справок продуктов.

База знаний Bitdefender для бизнес-продуктов доступна в любое время - http://www.bitdefender.com/support/business.html.

Форум поддержки Bitdefender

Форум техподдержки Bitdefender предоставляет пользователям Bitdefender простой способ не только получить необходимую помощь, но и помочь другим. Можно опубликовать любую проблему или вопрос, связанные с продуктом Bitdefender.

Специалисты Службы технической поддержки Bitdefender отслеживают новые сообщения на форуме, что позволяет своевременно реагировать на все вопросы пользователей. На форуме также есть возможность получить ответ или узнать о способах решения проблемы от более опытных пользователей Bitdefender.

Перед публикацией своего сообщения о проблеме или вопроса, выполните поиск похожих или связанных тем на форуме.

Форум техподдержки Bitdefender доступен по адресу http://forum.bitdefender.com, на пяти различных языках: английском, немецком, французском, испанском и румынском. Нажмите ссылку **Защита бизнеса**, чтобы перейти в раздел продуктов для бизнеса.

Документация по продукту

Документация по продукту является самым полным источником информации о продукте.

Самый простой способ получить документацию - перейти на страницу **Справка и поддержка** в Control Center. Нажмите свое имя пользователя в верхнем правом углу консоли, выберите **Справка и поддержка** , а затем ссылку интересующего вас руководства. Руководство откроется на новой вкладке вашего браузера.

17.2. Обращение за помощью

Вы можете обратиться за помощью в наш онлайн Центр поддержки. Заполните контактная форма и примите.

17.3. Использование инструментов поддержки

Инструменты поддержки GravityZone созданы, чтобы помочь пользователям и специалистам поддержки упростить предоставление необходимой информации для устранения неполадок. Запустите инструмент поддержки на действующих компьютерах и отправьте архив с информацией о выявленных неполадках в представительство поддержки Bitdefender.

17.3.1. Использование инструмента поддержки на операционных системах Windows

Запуск приложения Инструмент поддержки

Чтобы создать журнал на зараженном компьютере, используйте один из следующих способов:

- Командная строка

  Для любых проблем с BEST, установленным на компьютере.

- Проблема с установкой

  Для ситуаций, когда BEST не установлен на компьютере и установка завершается неудачно.

Метод командной строки

Используя командную строку, вы можете собирать журналы прямо с зараженного компьютера. Этот метод полезен в ситуациях, когда у вас нет доступа к Центру управления GravityZone или компьютер не взаимодействует с консолью.

1. Откройте командную строку с правами администратора.
2. Перейдите в папку установки продукта. Путь по умолчанию:

   ```
   C:\Program Files\Bitdefender\Endpoint Security
   ```

3. Соберите и сохраните журналы, выполнив эту команду:

```
Product.Support.Tool.exe collect
```

Журналы по умолчанию сохраняются в `C: \ Windows \ Temp .`

При желании, если вы хотите сохранить журнал средства поддержки в произвольном месте, используйте путь к параметру:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Пример:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Пока команда выполняется, вы можете заметить индикатор выполнения на экране. Когда процесс завершен, в выходных данных отображается имя архива, содержащего журналы, и его местоположение.

Чтобы отправить журналы в службу поддержки Bitdefender Enterprise, перейдите в `C:\Windows\Temp` или в пользовательское местоположение и найдите архивный файл с именем `ST_[computername]_[currentdate]`. Прикрепите архив к заявке в службу поддержки для дальнейшего устранения неполадок.

Проблема с установкой

1. Чтобы загрузить Инструмент поддержки BEST, нажмите здесь.
2. Запустите исполняемый файл от имени администратора. Появится окно.
3. Выберите место для сохранения архива журналов.

   Пока журналы собираются, вы увидите на экране индикатор выполнения. Когда процесс завершен, в выходных данных отображается имя архива и его местоположение.

Чтобы отправить журналы в службу поддержки Bitdefender Enterprise, перейдите в выбранное местоположение и найдите архивный файл с именем `ST_[computername]_[currentdate]`. Прикрепите архив к заявке в службу поддержки для дальнейшего устранения неполадок.

17.3.2. Использование инструмента поддержки на операционных системах Linux

Для операционных систем Linux инструмент поддержки интегрирован в агент безопасности Bitdefender.

Для сбора информации о системе Linux с использованием инструмента поддержки, запустите следующую команду:

```
# /opt/BitDefender/bin/bdconfigure
```

используя следующие доступные опции:

- `--help` составить список всех команд инструмента поддержки
- `enablelogs` для включения журналирования продукта и коммуникационного модуля (все сервисы будут автоматически перезапущены)
- `disablelogs` для отключения журналирования продукта и коммуникационного модуля (все сервисы будут автоматически перезапущены)
- `deliverall` чтобы создать:
  - Архив, содержащий журналы продукта и модуля связи, доставленный в папку `/tmp` в следующем формате: `bitdefender_machineName_timeStamp.tar.gz`.

  После того как создан архив:

  1. При отключении журналирования вам будет выдан запрос. При необходимости службы автоматически перезапустятся.
  2. При удалении журналов вам будет выдан соответствующий запрос.
- `deliverall -default` предоставляет такую же информацию, как и в предыдущей опции, но действия по умолчанию будут отображены в логах без запроса пользователя (журналы отключены и удалены).

Вы также можете запустить команду `/bdconfigure` прямо из пакета [BEST_SHORT] (полный или загрузчик) без установки продукта.

Для сообщения о проблеме GravityZone, воздействующей на вашу систему Linux, выполните следующие шаги, используя ранее описанные опции:

1. Включите журналирование продукта и коммуникационного модуля.
2. Попытайтесь воспроизвести проблему.
3. Отключите журналы.
4. Создайте архив журналов.
5. Откройте обращение в службу поддержки, используя форму, которая доступна на странице **Помощь &Поддержка** в Control Center, с описанием проблемы и прикрепленным архивом журналов.

Инструмент поддержки для Linux предоставляет следующую информацию:

- `etc`, `var/log`, `/var/crash` (если доступно) и `var/epag` папки из папки `/opt/BitDefender`, которые содержат журналы и настройки Bitdefender
- Файл `/var/log/BitDefender/bdinstall.log` содержит информацию по установке
- Файл `network.txt`, который содержит информацию о сетевых настройках / о доступности машин
- Файл `product.txt`, включая содержимое всех файлов `update.txt` из `/opt/BitDefender/var/lib/scan` и полный рекурсивный список всех файлов из `/opt/BitDefender`
- Файл `system.txt`, который содержит общую системную информацию (версия дистрибутива и ядра, доступная оперативная память и свободное место на жестком диске)
- Файл `users.txt`, который содержит информацию о пользователе
- Другую системную информацию, касающуюся продукта, такую как внешнее сетевое взаимодействие процессов и использование процессора
- Системные журналы

17.3.3. Использование инструментов поддержки на операционных системах Mac

При отправке запроса в группу технической поддержки Bitdefender, необходимо предоставить следующую информацию:

- Подробное описание проблемы, с которой вы столкнулись.

- Скриншот (если возможно) сообщения об ошибке, которое появляется.
- Журнал инструмента поддержки.

Чтобы собрать информацию о Mac-системе с помощью инструмента поддержки:

1. Скачайте ZIP-архив, содержащий инструмент поддержки.
2. Извлеките файл **BDProfiler. Tool** из архива.
3. Откройте окно терминала.
4. Перейдите к папке, содержащей файл **BDProfiler.tool**.

   Например:

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. Добавьте разрешение на выполнение файла:

   ```
   chmod +x BDProfiler.tool;
   ```

6. Запустите инструмент.

   Например:

   ```
   /Users/Bitdefender/Desktop/BDProfiler.tool;
   ```

7. Нажмите `Y` и введите пароль, когда появится запрос ввода пароля администратора.

   Подождите пару минут, пока инструмент не закончит создание журнала. Полученный файл архива (**Bitdefenderprofile_ output. Zip**) появится на рабочем столе.

17.4. Контактная информация

Эффективное взаимодействие с клиентами является залогом успешного бизнеса. За последние 18 лет Bitdefender удалось завоевать бесспорный авторитет среди своих клиентов и партнеров за счет опережения их ожиданий и постоянного улучшения отношений с ними. Мы будем рады ответить на

все ваши вопросы и решить ваши проблемы – не стесняйтесь, обратитесь к нам за помощью.

17.4.1. Адреса веб-сайтов

Отдел продаж: enterprisesales@bitdefender.com
Центр поддержки:http://www.bitdefender.com/support/business.html
Документация: gravityzone-docs@bitdefender.com
Местные дистрибьюторы:http://www.bitdefender.com/partners
Партнерские программы: partners@bitdefender.com
Отдел по связям со СМИ: pr@bitdefender.com
Вирусная лаборатория: virus_submission@bitdefender.com
Спам-лаборатория: spam_submission@bitdefender.com
Сообщение о нарушениях: abuse@bitdefender.com
Веб-сайт: http://www.bitdefender.com

17.4.2. Местные дистрибьюторы

Местные дистрибьюторы Bitdefender готовы ответить на все вопросы коммерческого и общего характера, находящиеся в их компетенции.

Чтобы найти дистрибьютора Bitdefender в вашей стране:

1. Перейдите к http://www.bitdefender.com/partners.
2. Перейдите к **Поиск партнеров**.
3. Контактная информация местных дистрибьюторов Bitdefender будет отображена автоматически. Если это не произошло, выберите вашу страну, чтобы просмотреть информацию.
4. Если не удалось найти дистрибьютора Bitdefender в вашей стране, свяжитесь с нами по адресу электронной почты enterprisesales@bitdefender.com.

17.4.3. Офисы Bitdefender

Офисы компании Bitdefender готовы ответить на все вопросы коммерческого и общего характера, находящиеся в их компетенции. Ниже приведены адреса и контактная информация офисов.

США

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Телефон (продажи & техническая поддержка): 1-954-776-6262
Продажи: sales@bitdefender.com
Сайт: http://www.bitdefender.com
Центр поддержки: http://www.bitdefender.com/support/business.html

Франция

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Факс: +33 (0)1 47 35 07 09
Телефон: +33 (0)1 47 35 72 73
E-mail: b2b@bitdefender.fr
Веб-сайт: http://www.bitdefender.fr
Центр поддержки: http://www.bitdefender.fr/support/business.html

Испания

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Факс: (+34) 93 217 91 28
Телефон (office & sales): (+34) 93 218 96 15
Телефон (техническая поддержка): (+34) 93 502 69 10
Продажи: comercial@bitdefender.es
Веб-сайт: http://www.bitdefender.es
Центр поддержки: http://www.bitdefender.es/support/business.html

Германия

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte

Deutschland
Телефон (office & sales): +49 (0) 2304 94 51 60
Телефон (техническая поддержка): +49 (0) 2304 99 93 004
Продажи: firmenkunden@bitdefender.de
Веб-сайт: http://www.bitdefender.de
Центр поддержки: http://www.bitdefender.de/support/business.html

Великобритания и Ирландия

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Телефон (продажи & техническая поддержка): (+44) 203 695 3415
E-mail: info@bitdefender.co.uk
Продажи: sales@bitdefender.co.uk
Веб-сайт: http://www.bitdefender.co.uk
Центр поддержки: http://www.bitdefender.co.uk/support/business.html

Румыния

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Факс: +40 21 2641799
Телефон (продажи & техническая поддержка): +40 21 2063470
Продажи: sales@bitdefender.ro
Веб-сайт: http://www.bitdefender.ro
Центр поддержки: http://www.bitdefender.ro/support/business.html

Объединенные Арабские Эмираты

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Телефон (продажи & техническая поддержка): 00971-4-4588935 / 00971-4-4589186
Факс: 00971-4-44565047

Продажи: sales@bitdefender.com
Сайт: http://www.bitdefender.com
Центр поддержки: http://www.bitdefender.com/support/business.html

A. Приложения

A.1. Поддерживаемые типы файлов

Механизмы сканирования на наличие вредоносных программ, включенные в решения безопасности Bitdefender, могут сканировать все типы файлов, которые могут содержать угрозы. Список ниже включает наиболее распространенные типы файлов, которые анализируются.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp; xz; z; zip; zl?; zoo

A.2. Типы сетевых объектов и статусы

A.2.1. Типы сетевых объектов

Все типы сетевых объектов доступны в разделе **Сеть** и представлены соответствующими значками.

Ниже в таблице приведены значки и описание для всех доступных типов сетевых объектов.

Значок	Тип
	Сетевая группа
	Компьютер
	Компьютер ретранслятор
	Компьютер сервера Exchange
	Компьютер ретранслятор сервера Exchange
	Виртуальная машина
	Виртуальная машина ретранслятора
	Золотой образ
	Виртуальная машина сервера Exchange
	Виртуальная машина ретранслятор сервера Exchange
	Виртуальная машина с vShield
	Ретранслятор виртуальной машины с vShield
	Инвентаризация Nutanix
	Nutanix Prism
	кластер Nutanix
	Содержимое VMware
	VMware vCenter
	VMware дата-центр

Значок	Тип
	Пул ресурсов VMware
	Кластер VMware
	Содержимое Citrix
	XenServer
	Пул серверов Xen
	Инвентаризация Amazon EC2
	Интеграция Amazon EC2
	Amazon EC2 / Регион Microsoft Azure
	Amazon EC2 / Зона доступности Microsoft Azure
	Инвентаризация Microsoft Azure
	Инвентаризация Microsoft Azure
	Security Server
	Security Server с vShield
	Хост без Security Server
	Хост с Security Server
	VMware vApp
	Пользователь мобильного устройства
	Мобильное устройство

A.2.2. Состояние сетевых объектов

Каждый сетевой объект может находится в различных состояниях, в зависимости от состояния управляемости, проблем безопасности, подключения и так далее. Ниже в таблице приведены значки всех возможных состояний и их описание.

Примечание
Таблица ниже содержит несколько общих примеров возможных состояний. Аналогичные состояния могу применяться (одиночные или комбинированные) ко всем типам сетевых объектов, таких как сетевые группы, компьютеры и так далее.

Значок	Состояние
	Хост без сервера безопасности, отключен
	Виртуальная машина, офлайн, неуправляемая
	Виртуальная машина, онлайн, неуправляемая
	Виртуальная машина, онлайн, управляемая
	Виртуальная машина, онлайн, управляемая, с проблемами
	Виртуальная машина, Ожидает перезагрузки
	Виртуальная машина, приостановлена (Suspended)
	Виртуальная машина, удалена

A.3. Типы файлов приложений

Движки сканирования вредоносного ПО, включенные в решения безопасности Bitdefender, могут быть настроены на сканирование только файлов приложений (или программ). Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов.

Эта категория включает в себя файлы со следующими расширениями:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; iso; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; ps1; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk;

ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

A.4. Фильтрация вложений по типу файлов

Модуль управления контентом, предлагаемый Security for Exchange, может фильтровать вложения электронной почты в зависимости от типа файлов. Типы, доступные в Control Center, включают следующие расширения:

Исполняемые файлы

386; acm; ax; com; cpl; dll; drv; exe; flt; fon; lrc; ocx; scr; sys; vxd; x32

Образы

bmp; cal; dcx; drw; ds4; eps; gif; gx2; ico; img; jfif; jpe; jpeg; jpg; pat; pcx; pgm; png; psd; psp; rgb; sdr; sh3; shw; sym; tif; tiff; wpg

Мультимедиа

3g2; 3gg; asf; au; avi; mid; mmf; mov; mp3; mpeg; mpg; ogg; qt; ra; ram; rm; swf; wav; wpl

Архивы.

7z; ain; arc; arj; bz; bz2; cab; cpio; cru; crush; gz; hap; img; jar; lha; lzh; pak; ppz; rar; rpm; sit; snp; tar; tar.z; tb2; tbz2; tgz; ufa; z; zip; zoo

Электронные таблицы

fm3; ods; wk1; wk3; wks; xls; xlsx

Презентации

odp; pps; ppt; pptx

Документы

doc; docx; dtd; htm; html; odt; pcx; pdf; qxd; rtf; wks; wpf; ws; ws2; xml

A.5. Системные переменные

Некоторые из настроек, присутствующие в консоли, требуют указания путей на компьютерах. Желательно использовать системные переменные (в

соответствующих случаях), чтобы быть уверенным, что путь действителен для всех нужных компьютеров.

Ниже приведен список предопределенных системных переменных:

`%ALLUSERSPROFILE%`

Папка профиля All Users. Типовой путь:

`C:\Documents and Settings\All Users`

`%APPDATA%`

Папка Application Data вошедшего пользователя. Типовой путь:

`C:\Users\{username}\AppData\Roaming`

`%LOCALAPPDATA%`

Временные файлы приложений. Типовой путь:

`C:\Users\{username}\AppData\Local`

`%PROGRAMFILES%`

Папка Program Files. Типовой путь `C:\Program Files`.

`%PROGRAMFILES(X86)%`

Папка Program Files для 32-битных приложений (на 64-битных системах). Типовой путь:

`C:\Program Files (x86)`

`%COMMONPROGRAMFILES%`

Папка Common Files. Типовой путь:

`C:\Program Files\Common Files`

`%COMMONPROGRAMFILES(X86)%`

Папка Common Files для 32-битных приложений (на 64-битных системах). Типовой путь:

`C:\Program Files (x86)\Common Files`

`%WINDIR%`

Каталог Windows или SYSROOT. Типовой путь `C:\Windows`.

`%USERPROFILE%`

Путь к папке профиля пользователя. Типовой путь:

`C:\Users\{username}`

В macOS папка профиля пользователя соответствует домашней папке. При настройке исключений используйте `$HOME` or `~`.

A.6. Инструменты модуля Управления приложениями

Чтобы установить правила модуля Управления приложениями на основе хэш исполняемого файла или отпечатка сертификата, необходимо загрузить следующие инструменты:

- **Fingerprint**, чтобы получить пользовательское значение хэш.
- **Thumbprint**, чтобы получить пользовательское значение отпечатка сертификата.

Fingerprint

Нажмите здесь, чтобы загрузить исполняемый файл Fingerprint или перейдите к http://download.bitdefender.com/business/tools/ApplicationControl/

Чтобы получить хэш приложения:

1. Откройте окно **командной строки**.
2. Перейдите к местоположению инструмента Fingerprint. Например:

```
cd/users/fingerprint.exe
```

3. Чтобы отобразить хэш-значение приложения, выполните следующую команду:

```
fingerprint <application_full_path>
```

4. Вернитесь в Control Center и настройте правило на основе значения, которое вы получили. Для получения более подробной информации обратитесь к «Контроль приложений» (p. 367).

Thumbprint

Нажмите здесь, чтобы загрузить исполняемый файл Thumbprint или перейдите к http://download.bitdefender.com/business/tools/ApplicationControl/

Чтобы получить отпечаток сертификата:

1. Запустите **командную строку** от имени администратора.
2. Перейдите к местоположению инструмента Thumbprint. Например:

```
cd/users/thumbprint.exe
```

3. Чтобы отобразить отпечаток сертификата, выполните следующую команду:

```
thumbprint <application_full_path>
```

4. Вернитесь в Control Center и настройте правило на основе значения, которое вы получили. Для получения более подробной информации обратитесь к «Контроль приложений» (p. 367).

A.7. Объекты Sandbox Analyzer

A.7.1. Поддерживаемые Типы и Расширения Фалов для Отправки Вручную

Поддерживаются следующие расширения, которые могут быть проверены вручную в Sandbox Analyzer:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer может обнаруживать вышеупомянутые типы файлов, если они включены в архивы следующих типов: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

A.7.2. Типы Файлов Поддерживаемые Предварительной Фильтрацией Контента при Автоматической Отправке

Предварительная фильтрация контента определит конкретный тип файла с помощью комбинации, которая включает в себя содержимое объекта и расширение. Это означает, что исполняемый файл с расширением `.tmp` будет распознан как приложение и, если он окажется подозрительным, будет отправлен в Sandbox Analyzer.

- Приложения - файлы формата PE32, включая, но не ограничиваясь следующими расширениями: `exe, dll, com`.
- Документы - файлы формата документа, включая, но не ограничиваясь следующими расширениями: `xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm, dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf`.
- Сценарии: `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe`.
- Архивы: `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00`.
- Почту (сохраненную в файловой системе):`eml, tnef`.

A.7.3. Исключения По Умолчанию в Автоматической Отправке

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt`.

A.7.4. Рекомендуемые приложения для детонации виртуальных машин

Sandbox Analyzer On-Premises требует, чтобы определенные приложения были установлены на виртуальных машинах детонации, чтобы они открывали отправленные образцы.

Приложения	Типы файлов.
Пакет Microsoft Office	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx

Приложения	Типы файлов.
Adobe Flash Player	swf
Программа Adobe Acrobat Reader	pdf
Windows по умолчанию	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml

A.8. Процессоры данных

Имя	Подробная информация
Процессор пересылки запросов	Пересылает запросы процессора в различных средах
Аппаратный гипервизор VMware	Синхронизирует ресурсы VMware и другую информацию с GravityZone
Аппаратный гипервизор Citrix	Синхронизирует ресурсы Xen и другую информацию с GravityZone
Универсальный интегратор виртуализации	Синхронизирует ресурсы Nutanix, Amazon EC2 и Azure с GravityZone
Интегратор NTSA	Синхронизирует состояние интеграции Network Traffic Security Analytics (NTSA)и отправляет обновления лицензии на устройство (NTSA)

Имя	Подробная информация
Синхронизация инвентаризации компьютеров Active Directory	Синхронизирует инвентаризацию компьютеров Active Directory с GravityZone
Синхронизация инвентаризации групп Active Directory	Синхронизирует инвентаризацию групп Active Directory с GravityZone
Синхронизация импорта пользователей Active Directory	Синхронизирует учетные записи пользователей Active Directory с GravityZone (используется для связывания учетных записей AD с учетными записями GravityZone)
Синхронизация инвентаризации пользователей Active Directory	Синхронизирует инвентаризацию пользователей Active Directory с GravityZone
Процессор электронной почты	Выстраивает в очередном порядке электронные письма для отправки от GravityZone
Процессор отчетов	Обрабатывает отчеты и портлеты
Развертывание агента безопасности Windows	Задействование Bitdefenderагента безопасности для устройств Windows
Развертывание сервера безопасности	Развертывает виртуальные устройства безопасности
Использование лицензии	Управляет лицензиями установленных конечных точек
Процессор мобильных push-уведомлений	Отправляет push-уведомления на защищенные мобильные устройства
Развертывание агента безопасности Linux и macOS	Использует Bitdefender GravityZone безопасность предприятия для агента SVE на устройствах Linux и macOS
Комплекты конечных точек и средство обновления продукта	Загружает и публикует наборы конечных точек Bitdefender и обновления продуктов

Имя	Подробная информация
GravityZone Обновлен	Автоматически обновляет GravityZone при настройке. Обновляет версию для виртуальных устройств GravityZone
Package Cleaner	Удаляет неиспользуемые файлы
Процессор вопросов безопасности	Обрабатывает проблемы безопасности для элементов в разделе Сеть
Резервный процессор	Выполняет резервное копирование базы данных GravityZone
Процессор уведомлений	Отправляет уведомления пользователям
Процессор системных событий	Обрабатывает события из инфраструктуры (Application Control, Sandbox Analyzer, Serenity, SVA) или интеграций (Exchange, Nutanix, NSX)
Задача Дополнительного пакета HVI	Управляет установкой, обновлением и удалением дополнительного пакета HVI для хостов XEN
HVI Reboot Task Processor	Управляет задачами перезагрузки на хостах HVI
Состояние питания и состояние процессора	Вычисляет состояние питания и состояние подключения компьютеров и виртуальных машин
Процессор очистки автономных машин	Удаляет офлайн машины из сети
Выполнение* фоновых задач	Обрабатывает и запускает фоновые задачи

Глоссарий

Antimalware Scanning Storm

Интенсивное использование системных ресурсов, которое может происходить, когда антивирусное программное обеспечение сканирует одновременно нескольких виртуальных машин на одном физическом хосте.

IP-адрес

Сокращение от Internet Protocol – Интернет-протокол – маршрутизируемый протокол семейства TCP/IP, отвечающий за адресацию, маршрутизацию, фрагментацию и повторную компоновку IP-пакетов.

Windows Загрузчик

Это общее имя для программ, основная функция которых - загрузка содержимого для нежелательных или злонамеренных целей.

Архив

Диск, лента или каталог, содержащие резервные копии файлов.

Файл, содержащий один или несколько файлов в сжатом формате.

Браузер

Веб-браузер – приложение, которое находит и выводит на экран веб-страницы.

Буткит

Буткит - это вредоносная программа, способная заражать главную загрузочную запись (MBR), загрузочную запись тома (VBR) или загрузочный сектор. Буткит остается активным даже после перезагрузки системы.

Вирус

Программа или часть кода, которая загружается в ваш компьютер без вашего ведома и запускается без вашего участия. Многие вирусы также могут копировать себя. Все компьютерные вирусы создаются людьми. Очень легко написать простой вирус, который копирует себя снова и снова. Даже такой простой вирус очень опасен, так как он быстро использует всю свободную память и система зависает. Более опасные

вирусы могут передавать себя по сети и прорываться через системы защиты.

Вирусы-Вымогатели

Вредоносная программа, которая блокирует вас на вашем компьютере или блокирует доступ к файлам и приложениям. Вирусы-вымогатели будут требовать от вас определенную плату (выкуп) в обмен на ключ дешифрования, который позволяет получить доступ к вашему компьютеру или файлам.

Вредоносное ПО

Malware - обобщённый термин для программного обеспечения, который обозначает нанесения вреда - сокращение от "malicious software" (вредоносное программное обеспечение). Это не универсальное обозначение, но его популярность в качестве обобщённого термина для вирусов, троянских коней, червей и вредоносного мобильного кода постоянно растет.

Загрузочный вирус

Вирус, заражающий загрузочный сектор жесткого или гибкого диска. Попытка загрузиться с зараженной дискеты приводит к тому, что вирус активизируется в памяти. Каждый раз, когда вы загружаете систему с этого места, вирус будет активизироваться в памяти.

Загрузочный сектор:

Сектор в начале каждого диска, в котором хранится информация о структуре диска (размер сектора, размер кластера и т.д.) На загрузочном диске загрузочный сектор содержит программу, загружающую операционную систему.

Клавиатурный шпион (Keylogger)

Клавиатурные шпионы — это приложения, которые регистрируют все, что вводится с клавиатуры.

Клавиатурные шпионы по сути не являются вредоносным ПО. Их можно использовать в законных целях, например для контроля за действиями сотрудников или детей. Однако все чаще они используются кибер-мошенниками в злонамеренных целях (например, для сбора частных данных, таких как учетные данные и номера карт социального страхования).

Командная строка

В командной строке пользователь вводит нужные команды на специальном командном языке.

Лазейки в системе (Backdoor)

Брешь в защите системы, специально оставленная разработчиками или специалистами по сопровождению. Это не всегда делается со злым умыслом: например, в некоторых операционных системах предусмотрены учетные записи, которые могут использоваться персоналом службы технической поддержки или программистами разработчика.

Ложное срабатывание

Событие «ложного срабатывания» появляется, когда программа считает зараженным файл, который таковым на самом деле не является.

Макро-вирус

Компьютерный вирус, который кодируется как встроенный в документ макрос. Многие приложения, такие как Microsoft Word и Excel, поддерживают сложные макро-языки.

Эти приложения позволяют встраивать макросы в документ и эти макросы выполняются всякий раз, когда вы открываете документ.

Неэвристический анализ (Non-heuristic)

Этот метод проверки основан на использовании определенных сигнатур вирусов. Основное преимущество этого метода состоит в том, что его нельзя обмануть похожей на вирус программой, а, следовательно, не возникает ложное срабатывание.

Область уведомлений

Область уведомлений впервые появилась в операционной системе Windows 95. Она расположена на панели задач Windows обычно в нижней части экрана рядом с часами и содержит маленькие значки, обеспечивающие быстрый доступ к таким функциям, как факс, принтер, модем, регулировка громкости и т. д Чтобы просмотреть подробную информацию о программе и ее настройки, просто дважды щелкните мышкой на значке.

Обновления

Новая версия программного обеспечения или оборудования, разработанная на замену устаревшей версии этого продукта. Кроме того, многие обновления часто определяют, установлена ли на компьютере старая версия данного программного продукта. Если нет – обновление невозможно.

Bitdefender имеет свой собственный модуль обновления, который позволяет вручную проверять наличие обновлений или автоматически обновлять программные продукты.

Подозрительные файлы и трафик сети

Подозрительными являются файлы с сомнительной репутацией. Данное ранжирование определяется многими факторами, среди которых можно назвать: наличие цифровой подписи, количество вхождений в компьютерных сетях, используемый упаковщик и т. д. Сетевой трафик воспринимается как подозрительный, если он отклоняется от шаблона. Например, ненадежный источник, запросы на подключение к необычным портам, увеличение использования полосы пропускания, случайное время соединения и т. д.

Полиморфный вирус

Вирус, изменяющий свою форму всякий раз, заражая новый файл. Поскольку у таких вирусов нет бинарной закономерности, их трудно обнаружить.

Порт

Компьютерный интерфейс, с помощью которого подключается внешнее устройство. У персональных компьютеров есть несколько видов портов. Внутри корпуса есть несколько портов для подключения дисководов, монитора и клавиатуры. Снаружи есть порты для подключения модемов, принтеров, мыши и других внешних устройств.

В сетях на базе протоколов TCP/IP и UDP, порт – это конечная точка логического подключения. Номер порта указывает на его тип. Например, порт номер 80 используется для HTTP трафика.

Программа-шпион

Любого рода программа-шпион, которая тайно и без ведома пользователя - чаще всего в рекламных целях - собирает информацию о пользователе

во время его соединения с сетью Интернет. Шпионские программы обычно маскируют как скрытые компоненты бесплатных или условно бесплатных (shareware) приложений, которые можно скачать из сети Интернет, хотя следует отметить, что большинство бесплатных или условно бесплатных приложений не содержит программ-шпионов. Программа-шпион после своей установки отслеживает адреса в сети Интернет, к которым обращается пользователь, и тайно пересылает эту информацию третьим лицам. Программы-шпионы могут собирать информацию об адресах электронной почты, паролях и номерах кредитных карт.

Программы-шпионы аналогичны вирусам-троянам в том смысле, что и те и другие устанавливаются самими пользователями во время установки других программ. Жертвами программ-шпионов обычно становятся при скачивании известных программных продуктов из файлообменных сетей.

Действия программ-шпионов являются не только нарушением этики и конфиденциальности, но и кражей ресурсов компьютерной памяти и ресурсов канала соединения с сетью Интернет, за счет передачи информации программой-шпионом своему источнику при подключении пользователя к сети Интернет. За счет потребления памяти и системных ресурсов программами-шпионами, работа последних в фоновом режиме может приводить к неустойчивой работе системы и ее сбоям.

Протокол TCP/IP

Протокол управления передачей/интернет-протокол (Transmission Control Protocol/Internet Protocol) — набор сетевых протоколов, широко используемых в сети Интернет. Они объединяют в одну большую сеть множество взаимосвязанных сетей, состоящих из компьютеров с различной архитектурой и с различными операционными системами. Протокол TCP/IP включает в себя стандарты связи между компьютерами, общепринятые правила объединения сетей и маршрутизации трафика.

Расширение имени файла

Часть названия файла после точки, обозначающая тип данных, хранящихся в нем.

Многие операционные системы, такие как Unix, VMS и MSDOS используют расширения имен файлов. Обычно они состоят из трех букв, потому что устаревшие ОС не имеют поддержки более длинных расширений. Например, "c" текст программы на языке C (C source code), "ps" – язык PostScript, а "txt" – любой текстовый файл.

Рекламное ПО

Рекламное ПО часто устанавливается «в качестве нагрузки» к основным приложениям, которые предоставляются бесплатно, при условии, что пользователь соглашается установить adware-программу. Поскольку Adware-приложения обычно устанавливаются только после того, как пользователь принимает условия, содержащиеся в соответствующем лицензионном соглашении с указанием функций данного приложения, то их функционирование не является каким-либо нарушением прав пользователя.

Однако, всплывающие рекламные объявления могут причинять неудобства пользователю, а в некоторых случаях и ухудшать производительность системы. Кроме того, информация, собираемая некоторыми из этих приложений, может нарушить неприкосновенность частной жизни пользователей, которые не были в полной мере осведомлены об условиях лицензионного соглашения.

Руткит

Руткиты - это набор программных инструментов, позволяющих получить доступ к системе на уровне администратора. Термин впервые использовался для операционных систем UNIX и относился к инструментам перекомпиляции, которые позволяли получить права администратора, при этом их присутствие оставалось скрытым для системных администраторов.

Основной целью руткитов является скрытие процессов, файлов, логинов и журналов. Они также могут перехватывать данные с терминалов, сетевых соединений или перифирийных устройств, если их встроить в соотвествующее программное обеспечение.

По своей природе руткиты не вредоносны. Например, системы, а также некоторые приложения, скрывают важные файлы при помощи руткитов. Однако, чаще всего, их используют как вредоносные программы либо для скрытия присутствия в системе. При совмещении с вредоносными программами руткиты представляют серьезную угрозу для целостности и безопасности системы. Они могут отслеживать трафик, создавать бреши в системе, изменять файлы и журналы, избегая выявления.

Сигнатуры вредоносных программ

Сигнатуры вирусов представляют собой фрагменты кода, извлеченные из образцов настоящих вирусов. Они используются антивирусными

программами для поиска по шаблону и распознавания вредоносных программ. Сигнатуры также используются для удаления вредоносного кода из зараженных файлов.
База данных вирусных сигнатур Bitdefender представляет собой набор вирусных сигнатур, обновляемый каждый час специалистами Bitdefender по анализу вредоносных программ.

Слои защиты

GravityZone обеспечивает защиту при помощи ряда модулей и функций, которые можно назвать слоями защиты, делящимися на защиту на конечных точках или защиту ядра и на другие дополнения. Защита на конечных точках включает в себя антивредоносные программы, расширенный контроль угроз, расширенный Anti-Exploit, Firewall, контроль контента, контроль устройств, Network Attack Defense, Power user и Relay. Дополнения включают в себя слои защиты, такие как Security for Exchange и Sandbox Analyzer.

Для получения более подробной информации о слоях защиты, доступных для GravityZone решения, обращайтесь к «Уровни защиты GravityZone » (p. 2).

События (Events)

Действие или событие, обнаруженное программой. Событиями могут быть действия пользователя, например щелчок кнопкой мыши, или нажатие клавиши, или системные события, например, переполнение памяти.

Спам

"Мусорная" электронная почта или "мусорная" новостная рассылка. Более известна как нежелательная электронная почта.

Средство кражи паролей

Программа для кражи паролей собирает фрагменты данных, которые могут быть именами учетных записей и связанными с ними паролями. Эти украденные учетные данные затем используются для злонамеренных целей, таких как захват аккаунтов.

Сценарий

Еще один термин, обозначающий макрос или командный файл. Сценарий – это набор команд, выполняющихся без участия пользователя.

Троян

Вредоносная программа, маскирующаяся под безвредное приложение. В отличие от обычных вирусов, вирус класса Троян не копирует себя, однако, он может быть не менее разрушительным. Вирусы-трояны одни из наиболее опасных типов, обещающие избавить ваш компьютер от всех вирусов, но, на самом деле, загружают вирусы в компьютер.

Этот термин взят из поэмы Гомера «Илиада», где в одной из глав описывается как греки подарили своим врагам, жителям Трои, огромного деревянного коня, якобы в знак мира. Но после того, как троянцы втащили статую в город, греческие солдаты выскочили из полости в теле коня и открыли городские врата, после чего их соратники ворвались в Трою и захватили город.

Условно вредоносное ПО

Класс программных приложений между законным программным обеспечением и вредоносным ПО. Хотя они не так вредны, как вредоносное ПО, которое влияет на целостность системы, их поведение по-прежнему приводит к нежелательным ситуациям, таким как кража данных и несанкционированное использование, нежелательная реклама. Наиболее распространенными программными приложениями являются шпионское ПО и рекламное ПО .

Файл отчета

Файл, в котором перечислены совершенные действия. Bitdefender включает в отчеты путь к проверенным файлам, папки, количество проверенных архивов и файлов, а также сколько подозрительных и зараженных файлов обнаружено.

Файлы Cookie

В сфере интернет-технологий под файлами cookie подразумеваются небольшие файлы, содержащие информацию о компьютере, которую можно проанализировать и использовать для того, чтобы выяснить ваши интересы и предпочтения. Поэтому технология создания таких файлов набирает обороты и сейчас вы можете получать рекламу товаров, основанную на ваших интересах. Но это "палка о двух концах" - с одной стороны вы видите именно то, что может вам пригодиться. Но с другой – за вами постоянно следят и знают, на какой странице вы находитесь и на какой кнопке щелкаете мышкой. Понятно, почему сейчас так широко обсуждается конфиденциальность данных пользователей и многие

чувствуют себя ущемленными в своих правах, будучи уверенными, что их «считывают» как кассир в магазине считывает штрих-код на этикетке. Порой эта точка зрения кажется крайностью, но иногда она полностью отражает действительность.

Фишинг

Это действие, заключающееся в отправке пользователю электронного письма, якобы от имени реально существующей организации с целью получения обманным путем конфиденциальной информации, которая будет использоваться для кражи личных данных. В получаемом сообщении электронной почты пользователя, с помощью вложенной ссылки, приглашают посетить якобы официальный веб-сайт реально существующей организации, где его просят подтвердить или обновить личные данные (например, пароли и номера банковского счета, кредитной карточки, карточки социального обеспечения). Однако, на самом деле, такого рода веб-сайт является поддельным и создается для кражи конфиденциальной информации пользователей.

Целевые атаки

Кибер-атаки, которые в основном направлены на получение финансовой выгоды или порчу репутации. Целью может быть частное лицо, компания, программное обеспечение или система, данные о которых тщательно изучаются до проведения атаки. Такие атаки развертываются в течение длительного периода времени и поэтапно, используя одну или несколько точек проникновения. Они действуют незаметно и чаще всего обнаруживаются уже после нанесения повреждения.

Червь

Программа, которая распространяется по сети, копируя и отправляя себя дальше. Она не может присоединяться к другим программам.

Эвристический анализ (Heuristic)

Способ обнаружения новых вирусов, основанный на правилах. Этот способ проверки не связан напрямую с определенными сигнатурами вирусов. Преимущество эвристической проверки состоит в том, что новый вирус не может "обмануть" фильтр. Однако он может принять подозрительный код в обычных программах за вирус и вызвать так называемое «ложное срабатывание».

инструмент эксплуатации уязвимости

Эксплоитом обычно евзывают любой метод, используемый для получения несанкционированного доступа к компьютерам или к взлому безопасности системы, который открывает систему для атаки.