Bitdefender

GravityZone

РУКОВОДСТВО АНАЛИТИКА ПО БЕЗОПАСНОСТИ

Bitdefender GravityZone
Руководство аналитика по безопасности

Дата публикации 2021.02.03

Правовое положение

Bitdefender

Содержание

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).**

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

Решение GravityZone включает в себя следующие компоненты:

- Веб-Консоль (Control Center)
- Security Server
- Дополнительный пакет HVI
- Агенты безопасности

3.1. 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.

3.2. 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.

3.3. 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)

3.3.1. 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).

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
- 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.

3.3.2. 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

3.3.3. 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.

3.3.4. 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.

3.4. 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 Bitdefender могут быть сконфигурированы и управляться через централизованную платформу, называемую 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

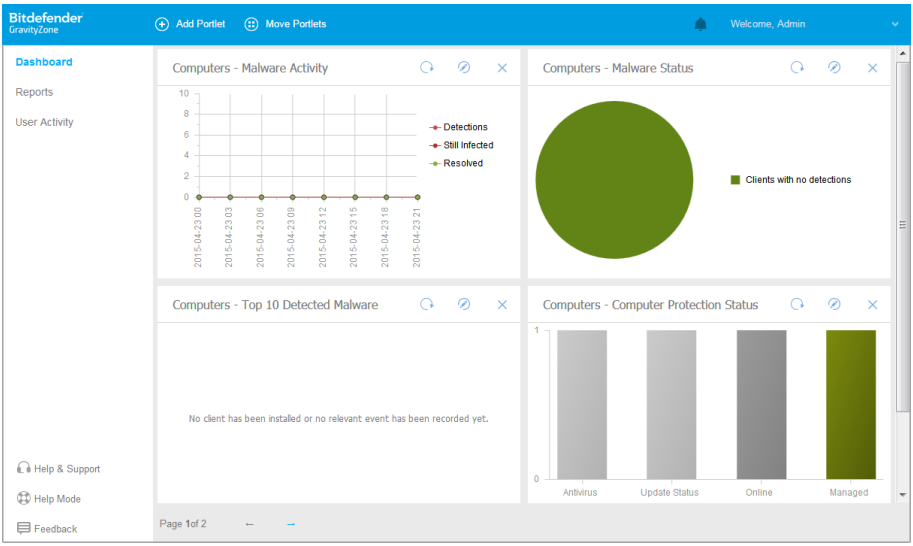
Предупреждение
Control Center не будет работать должным образом / отображаться в Internet Explorer 9 и выше с включенным режимом совместимости, что эквивалентно использованию неподдерживаемой версии браузера.

Подключение к Control Center:

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

4.2. Интуитивно понятная Control Center

Control Center организована таким образом, чтобы обеспечить легкий доступ ко всем функциям. Используйте панель меню в верхней части для навигации по консоли.



Информационная панель

Аналитики безопасности могут получить доступ к следующим разделам из панели меню:

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

Отчеты
Получение отчетов о безопасности по управляемым клиентам.

Активность пользователя
Проверьте журнал активности пользователя.

Наведя на имя пользователя в правом верхнем углу консоли, следующие опции могут быть доступны:

- **Моя учетная запись**. Выберите этот параметр, чтобы управлять своими реквизитами пользователя и настройками.
- **Помощь & Поддержка**. Выберите данную опцию, чтобы получить информацию о помощи и поддержке.

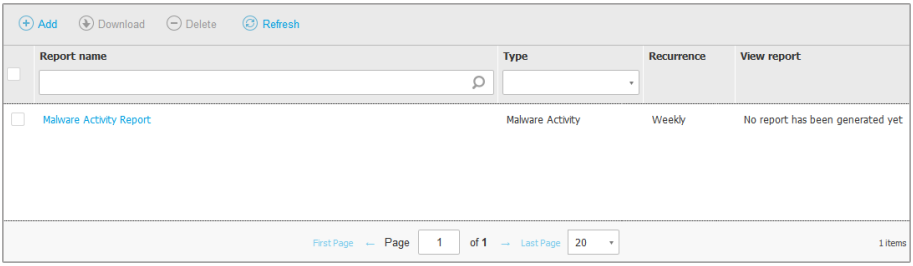
- **Обратная связь**. Нажмите эту опцию, чтобы отобразить форму, позволяющую редактировать и отправлять сообщения обратной связи относительно вашей работы с GravityZone.
- **Выход**. Выход из учетной записи.

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

- Значок **Режим справки** , который позволяет использовать систему подсказок, обеспечивающую расширенные подсказки по элементам Control Center. Здесь вы легко найдете полезную информацию, касающуюся функций Control Center.
- Значок **Уведомления** , который обеспечивает легкий доступ к уведомлениям и странице **Уведомления** .

4.2.1. 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

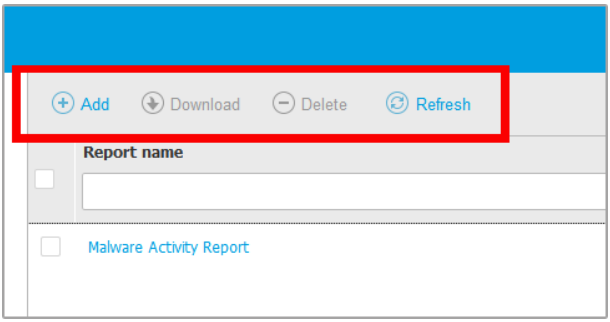
Чтобы убедиться, что консоль отображает последнюю информацию, нажмите кнопку **Обновить** в верхней части таблицы.

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

4.2.2. 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:

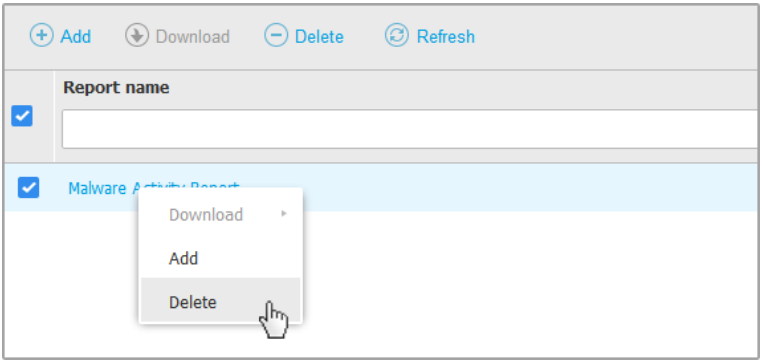
- Создать новый отчет.
- Загрузить отчет по расписанию.
- Удалить отчет по расписанию.



Страница отчетов - Панель Инструментов.

4.2.3. 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.



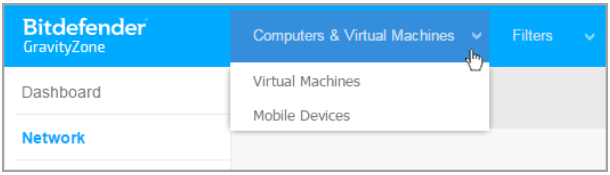
Страница отчетов - Контекстное меню

4.2.4. 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. 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:

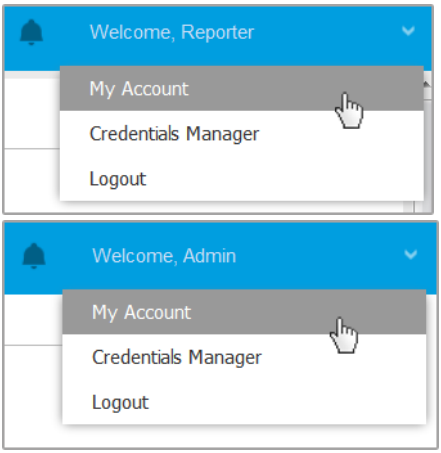
1. Нажмите на ваше имя пользователя в правом верхнем углу консоли и выберите **Мой аккаунт**.

2. В **Account Details** нажмите **Change password**.
3. Введите текущий пароль и новый пароль в соответствующие поля.
4. Нажмите **Сохранить**, чтобы сохранить изменения.

4.4. 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.

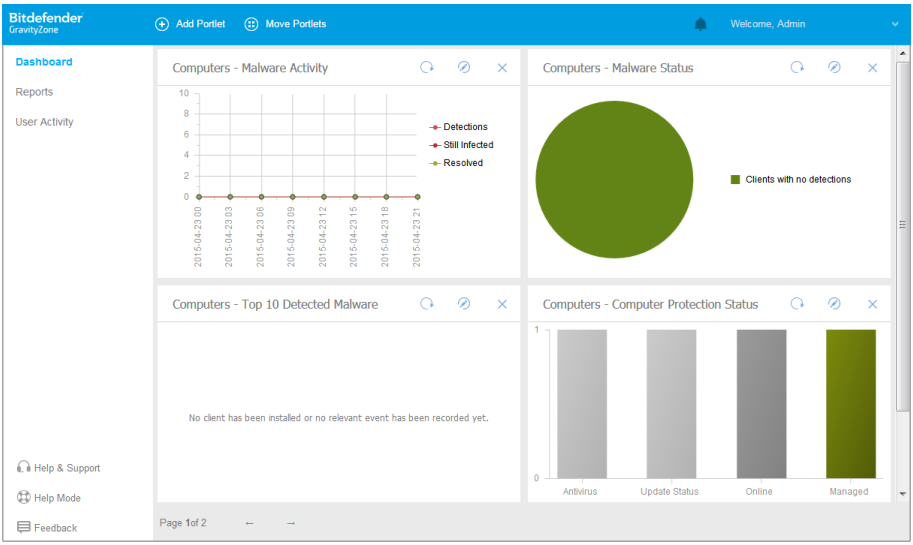
5. ИНФОРМАЦИОННАЯ ПАНЕЛЬ МОНИТОРИНГА

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.

5.1. 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.

5.1.1. 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.

5.1.2. 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.

5.1.3. 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. 41).
4. В разделе **Цели** выберите сетевые объекты и группы для включения.
5. Нажмите **Сохранить**.

5.1.4. 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.

5.1.5. Расположение портлетов

Вы можете расположить портлеты информационной панели по вашему усмотрению. Чтобы изменить расположение портлетов:

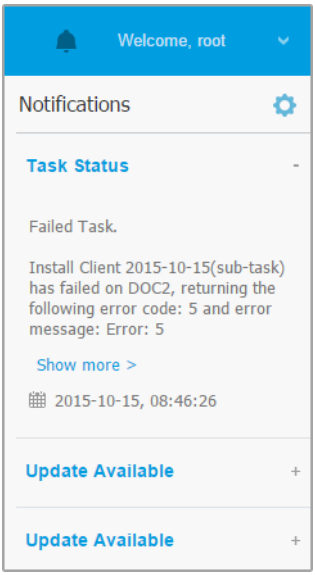
1. Перейдите на страницу **Панель инструментов**.

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.

6. 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.

6.1. 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. 37).

Угрозы, обнаруженные HyperDetect, выходят за рамки этого уведомления.

Advanced Anti-Exploit

Это уведомление информирует вас, когда Advanced Anti-Exploit обнаружил попытки использования в вашей сети.

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.

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.

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

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. 62).
5. Нажмите **Создать**.

Примечание
Чтобы избежать спама, вы будете получать максимум одно уведомление в час.

Ошибка патча отсутствует

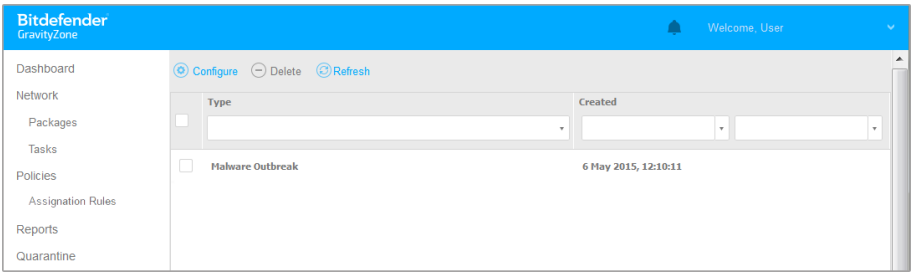
Это уведомление появляется,когда в конечных точках вашей сети отсутствуют 1 или 2 доступных патча.

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.

6.2. 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.

6.3. 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.

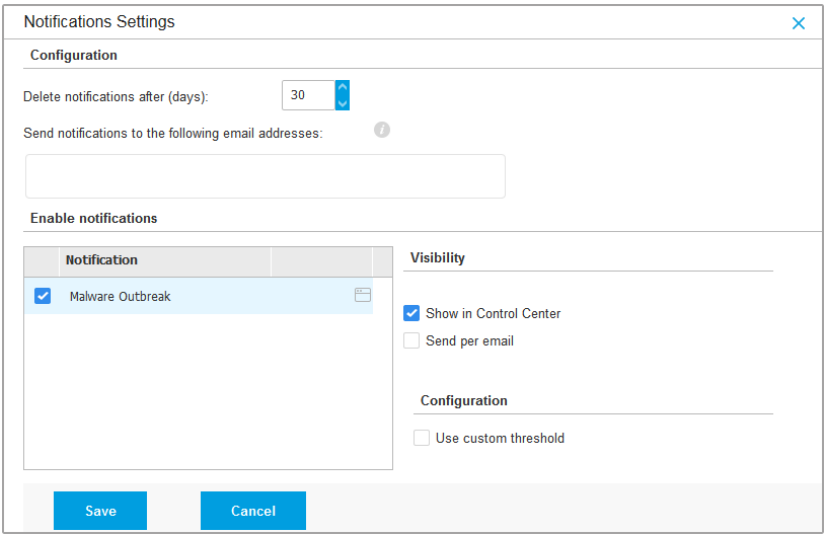
Вы также можете настроить уведомления для автоматического удаления после определенного количества дней. Для получения более подробной информации, обратитесь к «Настройка параметров уведомлений» (p. 37).

6.4. 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:
   -
   - 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. 33). 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.
- **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 **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**.

7. 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).

7.1. Типы отчетов

Различные типы отчетов доступны по каждому типу конечных точек:

- Отчеты по компьютерам и виртуальным машинам
- Отчеты Exchange
- Отчеты по мобильным устройствам

7.1.1. 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.

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. 75).

- 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.

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.

7.1.2. 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.

7.1.3. 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.

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.

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

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.

7.2. Создание отчетов

Вы можете создать две категории отчетов:

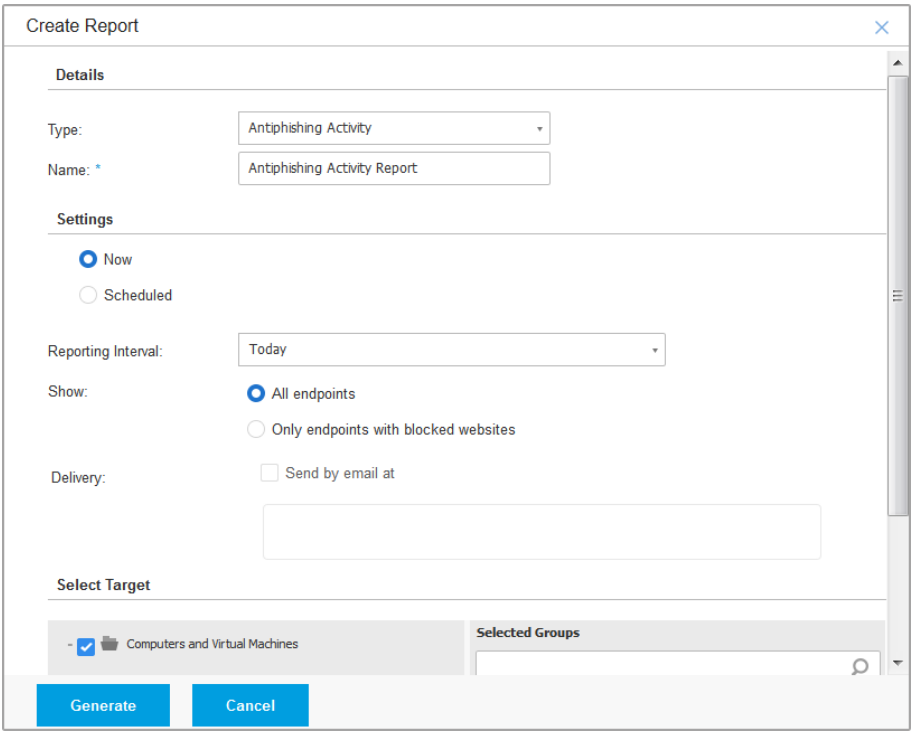
- **Мгновенные отчеты.** Мгновенные отчеты автоматически отображаются сразу после их создания.
- **Отчеты по расписанию.** Запланированные отчеты могут быть настроены на периодический запуск в заданные дату и время. Список всех запланированных отчетов отображается на странице **Отчеты**.

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. 41)
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.

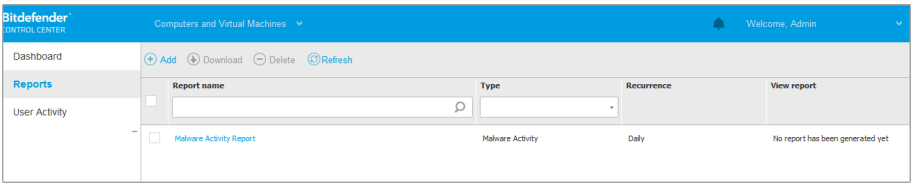
   Например, для отчета **Статус обновления** вы можете выбрать для просмотра только список сетевых объектов, которые не обновлены, или те, которые должны быть перезагружены для завершения обновлений.
9. **Доставка**. Чтобы получить отчет по расписанию по электронной почте, установите соответствующий флажок. 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**.

7.3. 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.

7.3.1. 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. 68)

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.

7.3.2. 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.

7.3.3. 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.

7.4. 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

7.4.1. 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.

7.4.2. 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.

7.5. 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.

7.6. Печать отчетов

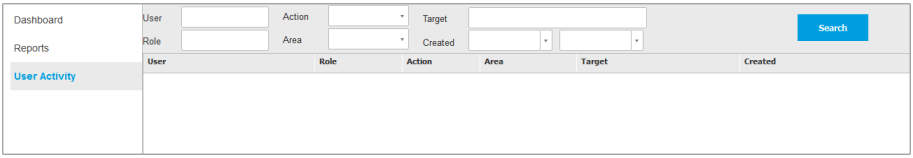
Control Center в настоящее время не поддерживает функцию печати. Чтобы напечатать отчет, необходимо сначала сохранить его на свой компьютер.

8. 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
- Запуск, завершение, отмена и остановка процессов устранения неполадок на зараженных компьютерах
- Редактирование параметров аутентификации для учетных записей GravityZone.

Чтобы изучить записи действий пользователей, перейдите в раздел **User Activity** 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.

9. ПОЛУЧЕНИЕ СПРАВКИ

По любым вопросам или проблемам в отношении GravityZone, обратитесь к администратору.

9.1. 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.

A. Приложения

A.1. Объекты Sandbox Analyzer

A.1.1. 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.1.2. 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.1.3. Исключения По Умолчанию в Автоматической Отправке

asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.

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.