Bitdefender®

GravityZone

SECURITY ANALYST'S GUIDE

Bitdefender GravityZone
Security Analyst's Guide

Publication date 2021.01.31

Copyright© 2021 Bitdefender

Table of Contents

1. ABOUT GRAVITYZONE

GravityZone is a business security solution built from ground-up for virtualization and cloud to deliver security services to physical endpoints, mobile devices, virtual machines in private, public cloud and Exchange mail servers.

GravityZone is one product with a unified management console available in the cloud, hosted by Bitdefender, or as one virtual appliance to be installed on company's premises, and it provides a single point for deploying, enforcing and managing security policies for any number of endpoints and of any type, in any location.

GravityZone delivers multiple layers of security for endpoints and for Microsoft Exchange mail servers: antimalware with behavioral monitoring, zero day threat protection, application control and sandboxing, firewall, device control, content control, anti-phishing and antispam.

2. GRAVITYZONE PROTECTION LAYERS

GravityZone provides the following protection layers:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Advanced Anti-Exploit
- Firewall
- Content Control
- Patch Management
- Device Control
- Full Disk Encryption
- Security for Exchange
- Application Control
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Antimalware

The antimalware protection layer is based on signature scanning and heuristic analysis (B-HAVE, ATC) against: viruses, worms, Trojans, spyware, adware, keyloggers, rootkits and other types of malicious software.

Bitdefender's antimalware scanning technology relies on the following technologies:

- First, a traditional scanning method is employed where scanned content is matched against the signature database. The signature database contains byte patterns specific to known threats and is regularly updated by Bitdefender. This scanning method is effective against confirmed threats that have been researched and documented. However, no matter how promptly the signature database is updated, there is always a vulnerability window between the time when a new threat is discovered and when a fix is released.

- Against brand-new, undocumented threats, a second layer of protection is provided by **B-HAVE**, Bitdefender's heuristic engine. Heuristic algorithms detect malware based on behavioral characteristics. B-HAVE runs suspicious files in

a virtual environment to test their impact on the system and ensure they pose no threat. If a threat is detected, the program is prevented from running.

Scanning Engines

Bitdefender GravityZone is able to automatically set the scanning engines when creating security agent packages, according to the endpoint's configuration.

The administrator can also customize the scan engines, being able to choose between several scanning technologies:

1. **Local Scan**, when the scanning is performed on the local endpoint. The local scanning mode is suited for powerful machines, having security content stored locally.

2. **Hybrid Scan with Light Engines (Public Cloud)**, with a medium footprint, using in-the-cloud scanning and, partially, the local security content. This scanning mode brings the benefit of better resources consumption, while involving off-premise scanning.

3. **Central Scan in Public or Private Cloud**, with a small footprint requiring a Security Server for scanning. In this case, no security content set is stored locally, and the scanning is offloaded on the Security Server.

> **i Note**
> There is a minimum set of engines stored locally, needed to unpack the compressed files.

4. **Central Scan (Public or Private Cloud scanning with Security Server) with fallback* on Local Scan (Full Engines)**

5. **Central Scan (Public or Private Cloud scanning with Security Server) with fallback* on Hybrid Scan (Public Cloud with Light Engines)**

2.2. Advanced Threat Control

For threats that elude even the heuristic engine, another layer of protection is present in the form of Advanced Threat Control (ATC).

Advanced Threat Control continuously monitors running processes and grades suspicious behaviors such as attempts to: disguise the type of process, execute code in another process's space (hijack process memory for privilege escalation), replicate, drop files, hide from process enumeration applications, etc. Each

suspicious behavior raises the process rating. When a threshold is reached, an alarm is triggered.

2.3. HyperDetect

Bitdefender HyperDetect is an additional layer of security specifically designed to detect advanced attacks and suspicious activities in the pre-execution stage. HyperDetect contains machine learning models and stealth attack detection technology against threats such as: zero-day attacks, advanced persistent threats (APT), obfuscated malware, fileless attacks (misuse of PowerShell, Windows Management Instrumentation etc.), credential stealing, targeted attacks, custom malware, script-based attacks, exploits, hacking tools, suspicious network traffic, potentially unwanted applications (PUA), ransomware.

2.4. Advanced Anti-Exploit

Powered by machine learning, Advanced Anti-Exploit is a proactive technology that stops zero-day attacks carried out through evasive exploits. Advanced anti-exploit catches the latest exploits in real-time and mitigates memory corruption vulnerabilities that can evade other security solutions. It protects the most commonly used applications, such as browsers, Microsoft Office or Adobe Reader, as well as others that you may think of. It watches over system processes and protects against security breaches and hijacking existing processes.

2.5. Firewall

The Firewall controls applications' access to the network and to the Internet. Access is automatically allowed for a comprehensive database of known, legitimate applications. Furthermore, the firewall can protect the system against port scans, restrict ICS and warn when new nodes join a Wi-Fi connection.

2.6. Content Control

The Content Control module helps enforce company policies for allowed traffic, web access, data protection and applications control. Administrators can define traffic scan options and exclusions, schedule web access while blocking or allowing certain web categories or URLs, configure data protection rules and define permissions for the use of specific applications.

2.7. Network Attack Defense

The Network Attack Defense module relies on a Bitdefender technology focused on detecting network attacks designed to gain access on endpoints through specific techniques, such as: brute-force attacks, network exploits, password stealers, drive-by-download infection vectors, bots, and Trojans.

2.8. Patch Management

Fully integrated in GravityZone, Patch Management keeps operating systems and software applications up to date and provides a comprehensive view on the patch status for your managed Windows endpoints.

The GravityZone Patch Management module includes several features, such as on-demand / scheduled patch scanning, automatic / manual patching or missing patch reporting.

You can learn more about GravityZone Patch Management supported vendors and products from this KB article.

> **Note**
> Patch Management is an add-on available with a separate license key for all available GravityZone packages.

2.9. Device Control

The Device Control module allows preventing the sensitive data leakage and malware infections via external devices attached to endpoints by applying blocking rules and exceptions via policy to a vast range of device types (such as USB flash drives, Bluetooth devices, CD/DVD players, storage devices, etc.).

2.10. Full Disk Encryption

This protection layer allows you to provide full disk encryption on endpoints, by managing BitLocker on Windows, and FileVault and diskutil on macOS. You can encrypt and decrypt boot and non-boot volumes, with just a few clicks, while GravityZone handles the entire process, with minimal intervention from the users. Additionally, GravityZone stores the recovery keys needed to unlock volumes when the users forget their passwords.

> **i** **Note**
> Full Disk Encryption is an add-on available with a separate license key for all available GravityZone packages.

2.11. Security for Exchange

Bitdefender Security for Exchange provides antimalware, antispam, antiphishing, attachment and content filtering seamlessly integrated with the Microsoft Exchange Server, to ensure a secure messaging and collaboration environment and increase productivity. Using award-winning antimalware and antispam technologies, it protects the Exchange users against the latest, most sophisticated malware, and against attempts to steal users' confidential and valuable data.

> **!** **Important**
> Security for Exchange is designed to protect the entire Exchange organization to which the protected Exchange Server belongs. This means it protects all active mailboxes, including user/room/equipment/shared mailboxes.
> In addition to Microsoft Exchange protection, the license also covers the endpoint protection modules installed on the server.

2.12. Application Control

The Application Control module prevents malware, zero-day attacks and enhances security without impacting productivity. Application Control enforces flexible application whitelisting policies that identify and prevent the installation and execution of any unwanted, untrusted or malicious applications.

2.13. Sandbox Analyzer

Bitdefender Sandbox Analyzer provides a powerful layer of protection against advanced threats by performing automatic, in-depth analysis of suspicious files which are not signed by Bitdefender antimalware engines yet. The sandbox employs an extensive set of Bitdefender technologies to execute payloads in a contained virtual environment hosted by Bitdefender or deployed locally, analyze their behavior and report any subtle system changes that is indicative of malicious intent.

Sandbox Analyzer uses a series of sensors to detonate content from managed endpoints, network traffic streams, centralized quarantine and ICAP servers.

Additionally, Sandbox Analyzer allows sample manual submission and through API.

> **i** **Note**
> This module's functionality can be provided by Sandbox Analyzer Cloud and Sandbox Analyzer On-Premises. Sandbox Analyzer On-Premises is available with a separate license key.

2.14. Incidents

The Incidents feature is an event correlation component, capable of identifying advanced threats or in-progress attacks. As part of our comprehensive and integrated Endpoint Protection Platform, the Incidents feature brings together device intelligence across your enterprise network. This solution comes in aid of your incident response teams' effort to investigate and respond to advanced threats.

Through Bitdefender Endpoint Security Tools, you can activate a protection module called Incidents Sensor on your managed endpoints, to gather hardware and operating system data. Following a client-server framework, the metadata is collected and processed on both sides.

This component brings detailed information of the detected incidents, an interactive incident map, remediation actions, and integration with Sandbox Analyzer and HyperDetect.

2.15. Hypervisor Memory Introspection (HVI)

It is widely known that highly organized, profit-driven attackers seek unknown vulnerabilities (zero-day vulnerabilities), or use one-off, purpose-built exploits (zero-day exploits) and other tools. Attackers also use advanced techniques to delay and sequence attack payloads to mask malicious activity. Newer, profit-driven attacks are built to be stealthy and defeat traditional security tools.

For virtualized environments, the problem is now resolved, HVI protecting datacenters with a high density of virtual machines against advanced and sophisticated threats that the signature-based engines cannot defeat. It enforces strong isolation, ensuring real-time detection of the attacks, blocking them as they happen and immediately removing the threats.

Whether the protected machine is Windows or Linux, server or desktop, HVI provides insight at a level that is impossible to achieve from within the guest operating system. Just as the hypervisor controls hardware access on behalf of each guest virtual machine, HVI has intimate knowledge of both user-mode and kernel-mode in-guest memory. The result is HVI has complete insight into guest memory, and therefore full context. At the same time, HVI is isolated from the protected guests,

just as the hypervisor itself is isolated. By operating at the hypervisor level and leveraging the hypervisor functionalities, HVI overcomes technical challenges of traditional security to reveal malicious activity in datacenters.

HVI identifies attack techniques rather than attack patterns. This way, the technology is able to identify, report and prevent common exploitation techniques. The kernel is protected against rootkit hooking techniques that are used during the attack kill chain to provide stealth. User-mode processes are also protected against code injection, function detouring, and code execution from stack or heap.

> **Note**
>
> The HVI module may be available for your GravityZone solution with a separate license key.

2.16. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) is a network security solution that analyzes IPFIX traffic streams for the presence of malicious behavior and malware.

Bitdefender NTSA is meant to act alongside your existing security measures as a complementary safeguard that is capable of covering the blind spots that traditional tools do not monitor.

Traditional network security tools generally attempt to prevent malware infections by inspecting inbound traffic (via sandbox, firewalls, antivirus and so on). Bitdefender NTSA focuses solely on monitoring outbound network traffic for malicious behavior.

2.17. Security for Storage

GravityZone Security for Storage delivers real-time protection for leading file-sharing and network-storage systems. System and threat-detection algorithm upgrades happen automatically - without requiring any efforts from you or creating disruptions for end-users.

Two or more GravityZone Security Servers Multi-Platform perform the role of ICAP server providing antimalware services to Network-Attached Storage (NAS) devices and file-sharing systems compliant with the Internet Content Adaptation Protocol (ICAP, as defined in RFC 3507).

When a user requests to open, read, write, or close a file from a laptop, workstation, mobile, or other device, the ICAP client (a NAS or file-sharing system) sends a scan

request to Security Server and receives a verdict regarding the file. Depending on the result, Security Server allows access, denies access or deletes the file.

> **Note**
> This module is an add-on available with a separate license key.

2.18. Security for Mobile

Unifies enterprise-wide security with management and compliance control of iPhone, iPad and Android devices by providing reliable software and update distribution via Apple or Android marketplaces. The solution has been designed to enable controlled adoption of bring-your-own-device (BYOD) initiatives by enforcing usage policies consistently on all portable devices. Security features include screen lock, authentication control, device location, remote wipe, detection of rooted or jailbroken devices and security profiles. On Android devices the security level is enhanced with real-time scanning and removable media encryption. As a result, mobile devices are controlled and sensitive business information residing on them is protected.

2.19. GravityZone Protection Layers Availability

The GravityZone protection layers availability differs according to the endpoint's operating system. To learn more, refer to the GravityZone Protection Layers Availability KB article.

3. GRAVITYZONE ARCHITECTURE

The GravityZone solution includes the following components:

- Web Console (Control Center)
- Security Server
- HVI Supplemental Pack
- Security Agents

3.1. Security Server

The Security Server is a dedicated virtual machine that deduplicates and centralizes most of the antimalware functionality of antimalware agents, acting as a scan server.

3.2. HVI Supplemental Pack

The HVI pack ensures the link between the hypervisor and the Security Server on that host. This way, the Security Server is able to monitor the memory in use on the host it is installed, based on the GravityZone security policies.

> **Note**
> The HVI module may be available for your GravityZone solution with a separate license key.

3.3. Security Agents

To protect your network with Bitdefender, you must install the appropriate GravityZone security agents on network endpoints.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac
- GravityZone Mobile Client
- Bitdefender Tools (vShield)

3.3.1. Bitdefender Endpoint Security Tools

GravityZone ensures Windows and Linux physical and virtual machines protection with Bitdefender Endpoint Security Tools, an intelligent environment-aware security agent which adapts to the endpoint type. Bitdefender Endpoint Security Tools can

be deployed on any machine, either virtual or physical, providing a flexible scanning system, being an ideal choice for mixed environments (physical, virtual and cloud).

Protection Layers

The following protection layers are available with Bitdefender Endpoint Security Tools:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Firewall
- Content Control
- Network Attack Defense
- Patch Management
- Device Control
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Application Control

Endpoint Roles

- Power User
- Relay
- Patch Caching Server
- Exchange Protection

Power User

Control Center administrators can grant Power User rights to endpoint users via policy settings. The Power User module enables administration rights at user level, allowing the endpoint user to access and modify security settings via a local console. Control Center is being notified when an endpoint is in Power User mode and the Control Center administrator can always overwrite local security settings.

> ⚠ **Important**
> This module is available only for supported Windows desktop and server operating systems. For more information, refer to the GravityZone Installation Guide.

Relay

Endpoint agents with Bitdefender Endpoint Security Tools Relay role serve as communication proxy and update servers for other endpoints in the network. Endpoint agents with relay role are especially required in organizations with isolated networks, where all traffic is made through a single access point.

In companies with large distributed networks, relay agents help lowering the bandwidth usage, by preventing protected endpoints and security servers to connect directly to the GravityZone appliance.

Once a Bitdefender Endpoint Security Tools Relay agent is installed in the network, other endpoints can be configured via policy to communicate with Control Center through the relay agent.

Bitdefender Endpoint Security Tools Relay agents serve for the following purposes:

- Discovering all unprotected endpoints in the network.
- Deploying the endpoint agent inside the local network.
- Updating protected endpoints in the network.
- Ensuring the communication between Control Center and connected endpoints.
- Acting as proxy server for protected endpoints.
- Optimizing the network traffic during updates, deployments, scanning and other resource-consuming tasks.

Patch Caching Server

Endpoints with Relay role may also act as a Patch Caching Server. With this role enabled, Relays serve for storing software patches downloaded from vendor's websites, and distributing them to target endpoints in your network. Whenever a connected endpoint has software with missing patches, it takes them from the server and not from the vendor's website, thus optimizing the traffic generated and the network bandwidth load.

> ⚠ **Important**
> This additional role is available with a registered Patch Management add-on.

Exchange Protection

Bitdefender Endpoint Security Tools with Exchange role can be installed on Microsoft Exchange Servers with the purpose of protecting the Exchange users from email-borne threats.

Bitdefender Endpoint Security Tools with Exchange role protects both the server machine and the Microsoft Exchange solution.

3.3.2. Endpoint Security for Mac

Endpoint Security for Mac is a security agent designed to protect Intel-based Macintosh workstations and laptops. The scanning technology available is **Local Scan**, with security content stored locally.

Protection Layers

The following protection layers are available with Endpoint Security for Mac:

- Antimalware
- Advanced Threat Control
- Content Control
- Device Control
- Full Disk Encryption

3.3.3. GravityZone Mobile Client

GravityZone Mobile Client extends security policies with ease to on any number of Android and iOS devices, protecting them against unauthorized usage, riskware and loss of confidential data. Security features include screen lock, authentication control, device location, remote wipe, detection of rooted or jailbroken devices and security profiles. On Android devices the security level is enhanced with real-time scanning and removable media encryption.

GravityZone Mobile Client is exclusively distributed via Apple App Store and Google Play.

3.3.4. Bitdefender Tools (vShield)

Bitdefender Tools is a light agent for VMware virtualized environments that are integrated with vShield Endpoint. The security agent installs on virtual machines protected by Security Server, to allow you to take advantage of the additional functionality it provides:

- Allows you to run Memory and Process Scan tasks on the machine.
- Informs the user about the detected infections and actions taken on them.
- Adds more options for antimalware scan exclusions.

3.4. Sandbox Analyzer Architecture

Bitdefender Sandbox Analyzer provides a powerful layer of protection against advanced threats by performing automatic, in-depth analysis of suspicious files which are not yet signed by Bitdefender antimalware engines.

Sandbox Analyzer is available in two variants:

- Sandbox Analyzer Cloud, hosted by Bitdefender.
- Sandbox Analyzer On-Premises, available as a virtual appliance that can be deployed locally.

Sandbox Analyzer Cloud

Sandbox Analyzer Cloud contains the following components:

- **Sandbox Analyzer Portal** – a hosted communication server used for handling requests between endpoints and the Bitdefender sandbox cluster.
- **Sandbox Analyzer Cluster** – the hosted sandbox infrastructure where the sample behavioral analysis occurs. At this level, the submitted files are detonated on virtual machines running Windows 7.

GravityZone Control Center operates as management and reporting console, where you configure the security policies, view analysis reports and notifications.

Bitdefender Endpoint Security Tools, the security agent installed on endpoints, acts as a feeding sensor to Sandbox Analyzer.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises is delivered as a Linux Ubuntu virtual appliance, embedded into a virtual machine image, easy to install and configure through a command-line interface (CLI). Sandbox Analyzer On-Premises is available in OVA format, deployable on VMware ESXi.

A Sandbox Analyzer On-Premises instance contains the following components:

- **Sandbox Manager**. This component is the sandbox orchestrator. Sandbox Manager connects to the ESXi hypervisor via API and uses its hardware resources to build and operate the malware analysis environment.
- **Detonation virtual machines**. This component consists of virtual machines leveraged by Sandbox Analyzer to execute files and analyze their behavior. The

detonation virtual machines can run Windows 7 and Windows 10 64-bit operating systems.

GravityZone Control Center operates as management and reporting console, where you configure security policies and view analysis reports and notifications.

Sandbox Analyzer On-Premises operates the following feeding sensors:

- **Endpoint sensor**. Bitdefender Endpoint Security Tools for Windows acts as feeding sensor installed on endpoints. The Bitdefender agent uses advanced machine learning and neural network algorithms to determine suspicious content and to submit it to Sandbox Analyzer, including objects from centralized quarantine.

- **Network sensor**. Network Security Virtual Appliance (NSVA) is a virtual appliance deployable in the same virtualized ESXi environment as the Sandbox Analyzer instance. Network sensor extracts content from network streams and submits it to Sandbox Analyzer.

- **ICAP sensor**. Deployed on network attached storage (NAS) devices using ICAP protocol, Bitdefender Security Server supports content submission to Sandbox Analyzer.

In addition to these sensors, Sandbox Analyzer On-Premises supports manual submission and through API. For details, refer to **Using Sandbox Analyzer** chapter in the GravityZone Administrator's Guide.

4. GETTING STARTED

Bitdefender GravityZone solutions can be configured and managed via a centralized management platform named Control Center. Control Center has a web-based interface, which you can access by means of username and password.

4.1. Connecting to Control Center

Access to Control Center is done via user accounts. You will receive your login information by email once your account has been created.

Prerequisites:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+

- Recommended screen resolution: 1280 x 800 or higher

> **⊗ Warning**
> Control Center will not work / display properly in Internet Explorer 9+ with the Compatibility View feature enabled, which is equivalent with using an unsupported browser version.

To connect to Control Center:

At the first login, you have to agree to Bitdefender Terms of Service. Click **Continue** to start using GravityZone.

4.2. Control Center at a Glance

Control Center is organized so as to allow easy access to all the features. Use the menu bar in the upper area to navigate through the console.
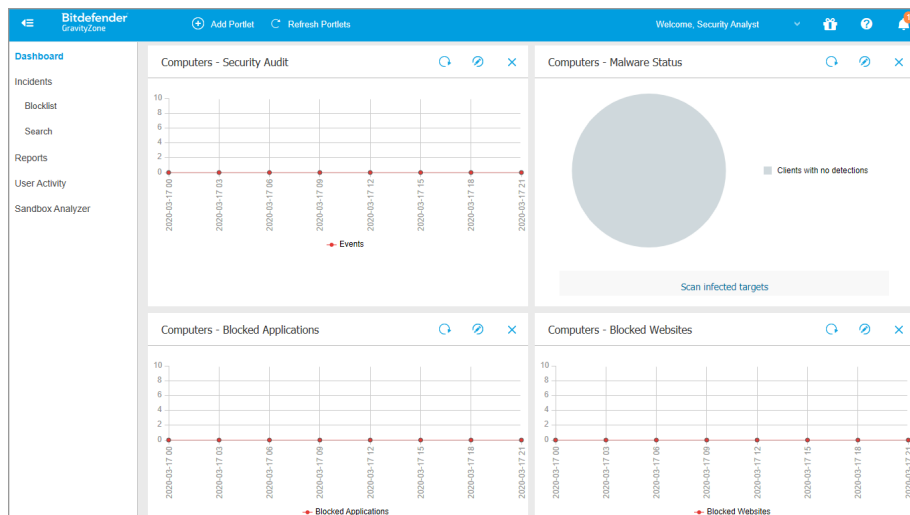
The Dashboard

Security Analysts can access the following sections from the menu bar:

Dashboard
View easy-to-read charts providing key security information concerning your network.

Reports
Get security reports concerning the managed clients.

User Activity
Check the user activity log.

By pointing to the username in the upper-right corner of the console, the following options are available:

- **My Account**. Click this option to manage your user account details and preferences.

- **Help & Support**. Click this option to find help and support information.

- **Feedback**. Click this option to display a form allowing you to edit and send your feedback messages regarding your experience with GravityZone.

- **Logout**. Click this option to log out of your account.

Additionally, in the upper-right corner of the console, you can find:

- The **Help Mode** icon, which enables a help feature providing expandable tooltip boxes placed on Control Center items. You will easily find out useful information regarding the Control Center features.

- The **Notifications** icon, which provides easy access to notification messages and also to the **Notifications** page.

4.2.1. Table Data

Tables are frequently used throughout the console to organize data into an easy-to-use format.

The Reports page

Navigating through Pages

Tables with more than 20 entries span on several pages. By default, only 20 entries are displayed per page. To move through the pages, use the navigation buttons at the bottom of the table. You can change the number of entries displayed on a page by selecting a different option from the menu next to the navigation buttons.

Searching for Specific Entries

To easily find specific entries, use the search boxes available below the column headers.

Enter the search term in the corresponding field. Matching items are displayed in the table as you type. To reset the table contents, clear the search fields.

Sorting Data

To sort data by a specific column, click the column header. Click the column header again to revert the sorting order.

Refreshing Table Data

To make sure the console displays the latest information, click the ⟳ **Refresh** button at the upper side of the table.

This may be needed when you spend more time on the page.

4.2.2. Action Toolbars

In Control Center, action toolbars allow you to perform specific operations pertaining to the section you are in. Each toolbar consists of a set of icons that is usually placed at the upper side of the table. For example, the action toolbar in the **Reports** section allows you to perform the following actions:

- ⊕ Create a new report.
- ⊕ Download a scheduled report.
- ⊖ Delete a scheduled report.
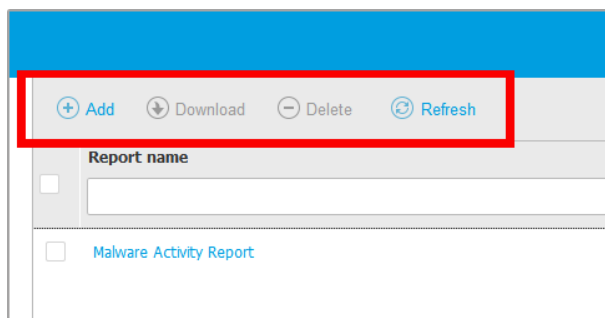
The Reports page - Action Toolbar

4.2.3. Contextual Menu

The action toolbar commands are also accessible from the contextual menu. Right-click the Control Center section you are currently using and select the command that you need from the available list.
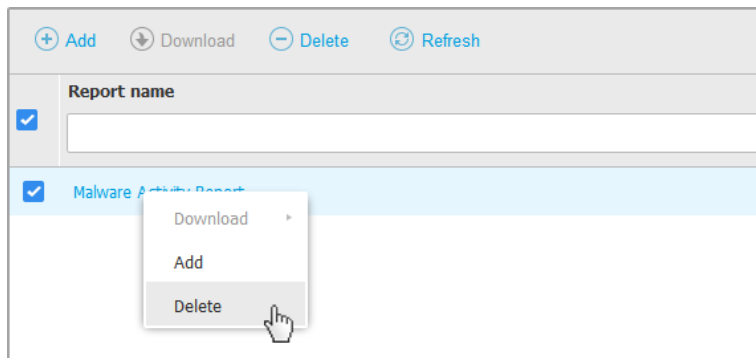
The Reports page - Contextual menu

4.2.4. Views Selector

If you work with different types of endpoints, you can find them organized in the **Network** page by type under several network views:

- **Computers & and Virtual Machines**: displays Active Directory groups and computers and also physical and virtual workstations outside Active Directory that are discovered in the network.

- **Virtual Machines**: displays the infrastructure of the virtual environment integrated with Control Center and all the containing virtual machines.

- **Mobile Devices**: displays users and the mobile devices assigned to them.

To select the network view that you want, click the views menu in the upper-right corner of the page.
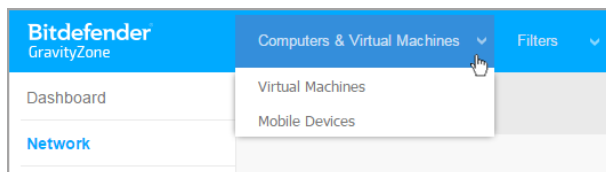
The Views Selector

> **Note**
> You will see only the endpoints you have permissions to view, permissions granted to you by the administrator who added your user to Control Center.

4.3. Changing Login Password

After your account has been created, you will receive an email with the login credentials.

Unless you use Active Directory credentials to access Control Center, it is recommended to do the following:

- Change the default login password first time you visit Control Center.
- Change your login password periodically.

To change the login password:

1. Click your username in the upper-right corner of the console and choose **My Account**.
2. Under **Account Details**, click **Change password**.
3. Enter your current password and the new password in the corresponding fields.
4. Click **Save** to apply the changes.

4.4. Managing Your Account

To check or change your account details and settings:

1. Click your username in the upper-right corner of the console and choose **My Account**.
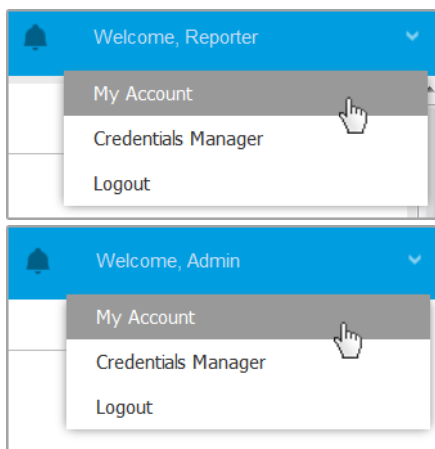
The User Account menu

2. Under **Account Details**, correct or update your account details. If you use an Active Directory user account, you cannot change account details.
    - **Username.** The username is the unique identifier of a user account and cannot be changed.
    - **Full name.** Enter your full name.
    - **Email.** This is your login and contact email address. Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important risk conditions are detected in the network.
    - A **Change password** link allows you to change your login password.

3. Under **Settings**, configure the account settings according to your preferences.
    - **Timezone.** Choose from the menu the timezone of your account. The console will display time information according to the selected timezone.
    - **Language.** Choose from the menu the console display language.
    - **Session Timeout.** Select the inactivity time interval before your user session will expire.

4. Under **Login Security**, configure two-factor authentication and check the status of the policies available to secure your GravityZone account. Company-wide set policies are read-only.

    To enable the two-factor authentication:

    a. **Two-factor authentication.** The two-factor authentication adds an extra layer of security to your GravityZone account, by requiring an authentication code in addition to your Control Center credentials.

        When first logging in to your GravityZone account you will be prompted to download and install the Google Authenticator, Microsoft Authenticator, or any two-factor TOTP (Time-Based One-Time Password Algorithm) authenticator - compatible with the standard RFC6238 on a mobile device, link it to your GravityZone account, then use it with each Control Center login. The authenticator app generates a six-digit code each 30 seconds. To complete the Control Center login, after entering the password, you will need to provide the six-digit code generated by the app.

        > **Note**
        > You may skip this process three times, after which you will not be able to log in without two-factor authentication.

        To enable the two-factor authentication:

    i.   Click the **Enable** button under the **Two-factor authentication** message.

    ii.   In the dialog box, click the appropriate link to download and install the selected authenticator app on your mobile device.

    iii.   On your mobile device, open the app.

    iv. In the **Add an account** screen, scan the QR code to link the app to your GravityZone account.

You can also enter the secret key manually.

This action is required only once, to enable the feature in GravityZone.

> ⚠ **Important**
>
> Make sure to copy and save the secret key in a safe location. Click **Print a backup** to create a PDF file with the QR code and secret key. If the mobile device used for activating two-factor authentication is lost or replaced, you will need to install the autheticator app of choice on a new device and provide the secret key to link it to your GravityZone account.

    v.   Enter the six-digit code in the **Authenticator code** field.

    vi. Click **Enable** to complete the feature activation.

> ℹ **Note**
>
> Be aware that, if the currently configured 2FA is disabled for your account, this secret key will no longer be valid.

b. **Password expiration policy.** Regular changes to your password provide an added layer of protection against the unauthorized use of passwords, or limits the duration of unauthorized use. When enabled, GravityZone requires you to change your password no later than 90 days.

c. **Account lockout policy.** This policy prevents access to your account after five consecutive failed login attempts. This measure is to protect against brute-force attacks.

To unlock your account, you need to reset your password from the login page, or contact another GravityZone administrator.

5. Click **Save** to apply the changes.

> **Note**
> You cannot delete your own account.

5. MONITORING DASHBOARD

Proper analysis of your network security requires data accessibility and correlation. Having centralized security information allows you to monitor and ensure compliance with the organization security policies, quickly identify issues, analyze threats and vulnerabilities.

5.1. Dashboard

The Control Center Dashboard is a customizable visual display providing a quick security overview of all protected endpoints and network status.

Dashboard portlets display various real-time security information using easy-to-read charts, thus allowing you to quickly identify any issues that might require your attention.
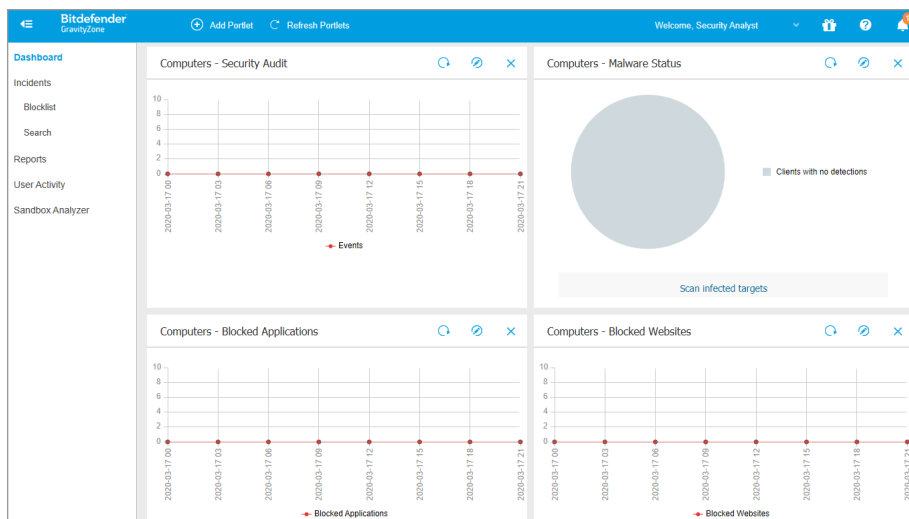
The Dashboard

This is what you need to know about dashboard portlets:

- Control Center comes with several predefined dashboard portlets.
- Each dashboard portlet includes a detailed report in the background, accessible with just one click on the chart.

- There are several types of portlets that include various information about your endpoint protection, such as update status, malware status, firewall activity.

  > **ⓘ Note**
  > By default, the portlets retrieve data for the current day and, unlike reports, cannot be set for longer intervals than one month.

- The information displayed via portlets refers to endpoints under your account only. You can customize each portlet's target and preferences using the **Edit Portlet** command.
- Click the chart legend entries, when available, to hide or display the corresponding variable on the graph.
- The portlets are displayed in groups of four. Use the vertical scroll bar or the up and down arrow keys to navigate between portlet groups.
- For several report types, you have the option to instantly run specific tasks on target endpoints, without having to go to the **Network** page to run the task (for example, scan infected endpoints or update endpoints). Use the button at the lower side of the portlet to take the available action.

The dashboard is easy to configure, based on individual preferences. You can edit portlet settings, add additional portlets, remove or rearrange existing portlets.

5.1.1. Refreshing Portlet Data

To make sure the portlet displays the latest information, click the ↻ **Refresh** button on its title bar.

To update the information for all the portlets at once, click the ↻ **Refresh Portlets** button at the top of the dashboard.

5.1.2. Editing Portlet Settings

Some portlets offer status information, while other report on security events in the last period. You can check and configure the reporting period of a portlet by clicking the ⊘ **Edit Portlet** icon on its title bar.

5.1.3. Adding a New Portlet

You can add other portlets to obtain the information you need.

To add a new portlet:

1. Go to the **Dashboard** page.

2. Click the ⊕ **Add Portlet** button at the upper side of the console. The configuration window is displayed.
3. Under the **Details** tab, configure the portlet details:
    *   Endpoint type (**Computers**, **Virtual Machines** or **Mobile Devices**)
    *   Type of background report
    *   Suggestive portlet name
    *   The time interval for the events to be reported

    For more information on available report types, refer to "Report Types" (p. 35).
4. Under the **Targets** tab, select the network objects and groups to include.
5. Click **Save**.

5.1.4. Removing a Portlet

You can easily remove any portlet by clicking the ⊗ **Remove** icon on its title bar. Once you remove a portlet, you can no longer recover it. However, you can create another portlet with the exact same settings.

5.1.5. Rearranging Portlets

You can rearrange dashboard portlets to better suit your needs. To rearrange portlets:

1. Go to the **Dashboard** page.
2. Drag and drop each portlet to the desired position. All other portlets between the new and old positions are moved to preserve their order.

> **i** **Note**
> You can move portlets only within the positions already taken.

6. NOTIFICATIONS

Depending on the events that might occur throughout your network, Control Center will show various notifications to inform you of the security status of your environment. The notifications will be displayed in the **Notification Area**, located in the right side of the Control Center.
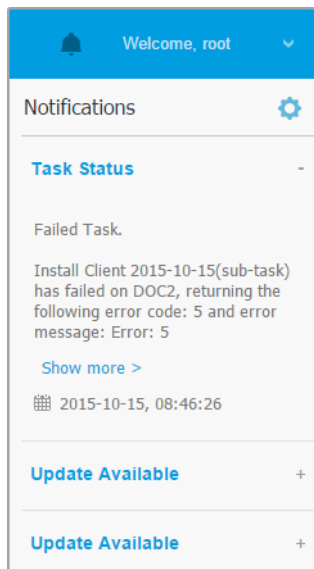
Notification Area

When new events are detected in the network, the [11] icon in the upper right corner of Control Center will display the number of newly detected events. Clicking the icon displays the Notification Area containing the list of detected events.

6.1. Notification Types

This is the list of available notifications types:

Malware Outbreak
    This notification is sent to the users that have at least 5% of all their managed network objects infected by the same malware.

Bitdefender GravityZone — unfollow the traditional

You can configure the malware outbreak threshold according to your needs in the **Notifications Settings** window. For more information, refer to "Configuring Notification Settings" (p. 32).

Threats detected by HyperDetect are out of the scope of this notification.

Advanced Anti-Exploit

This notification informs you when Advanced Anti-Exploit has detected exploit attempts in your network.

Login from New Device

This notification informs you that your GravityZone account was used to log in to Control Center from a device you have not used for this purpose before. The notification is automatically configured to be visible both in Control Center and on email and you can only view it.

Network Incidents event

This notification is sent each time the Network Attack Defense module detects an attack attempt on your network. This notification also informs you if the attack attempt was conducted either from outside the network or from a compromised endpoint inside the network. Other details include data about the endpoint, attack technique, attacker's IP, and the action taken by Network Attack Defense.

HyperDetect Activity

This notification informs you when HyperDetect finds any antimalware or unblocked events in the network. This notification is sent for each HyperDetect event and provides the following details:

- Affected endpoint information (name, IP, installed agent)
- Malware type and name
- Infected file path. For file-less attacks it is provided the name of the executable used in the attack.
- Infection status
- The SHA256 hash of the malware executable
- The type of the intended attack (targeted attack, grayware, exploits, ransomware, suspicious files and network traffic)
- Detection level (Permissive, Normal, Aggressive)
- Detection time and date

You can view details about the infection and further on investigate the issues by generating a **HyperDetect Activity** report right from the **Notifications** page. To do so:

1. In Control Center, click the 🔔 **Notification** button to display the Notification Area.

2. Click the **Show more** link at the end of the notification to open the **Notifications** page.

3. Click the **View report** button in the notification details. This opens the report configuration window.

4. Configure the report if needed. For more information, refer to .

5. Click **Generate**.

> ℹ️ **Note**
> To avoid spamming, you will receive maximum one notification per hour.

Missing Patch Issue

This notification occurs when endpoints in your network are missing one or more available patches.

You can view which endpoints are in this situation by clicking the **View report** button in notification details.

By default, the notification refers to security patches, but you may configure it to inform you of non-security patches as well.

New Incident

Password Expiration Enabled

This notification informs you when the password expiration is enabled on your account.

Password expiration reminder

This notification is sent daily, starting 10 days before your GravityZone password expires, to remind you that you need to change it. To quickly update the password, click the **My Account** button from the notification in Control Center.

Account Lockout Enabled
> This notification informs you when the account lockout is enabled on your account.
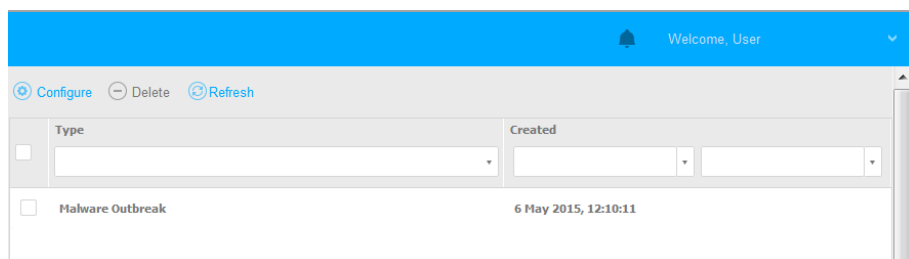
Account Locked Out
> This notification is sent via email to inform you that your account was locked out due to repeated login attempts with invalid passwords.

6.2. Viewing Notifications

To view the notifications, click the 🔔 **Notifications** button and then click **See All Notifications**. A table containing all the notifications is displayed.

The Notifications page

Depending on the number of notifications, the table can span several pages (only 20 entries are displayed per page by default).

To move through the pages, use the navigation buttons at the bottom of the table.

To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.

If there are too many entries, you can use the search boxes under the column headers or the filter menu at the top of the table to filter displayed data.

● To filter notifications, select the notification type you want to see from the **Type** menu. Optionally, you can select the time interval during which the notification was generated, to reduce the number of entries in the table, especially if a high number of notifications has been generated.

● To view the notification details, click the notification name in the table. A **Details** section is displayed below the table, where you can see the event that generated the notification.

6.3. Deleting Notifications

To delete notifications:

1. Click the 🔔 **Notification** button at the right side of the menu bar, then click **See All Notifications**. A table containing all the notifications is displayed.

2. Select the notifications you want to delete.

3. Click the ⊖ **Delete** button at the upper side of the table.

You can also configure notifications to be automatically deleted after a specified number of days. For more information, refer to "Configuring Notification Settings" (p. 32).

6.4. Configuring Notification Settings

The type of notifications to be sent and the email addresses they are sent to can be configured for each user.

To configure the notification settings:

1. Click the 🔔 **Notification** button at the right side of the menu bar and then click **See All Notifications**. A table containing all the notifications is displayed.

2. Click the ⊙ **Configure** button at the upper side of the table. The **Notification Settings** window is displayed.

Notifications Settings

> **ℹ Note**
> You may also access the **Notification Settings** window directly using the ⚙
> **Configure** icon from upper-right corner of the **Notification area** window.

3. Under **Configuration** section you can define the following settings:

   ●

   ● Additionally, you may send the notifications by email to specific recipients.
     Type the email addresses in the dedicated field, pressing `Enter` key after
     each address.

4. Under **Enable Notification** section you can choose the type of notifications you
   want to receive from GravityZone. You can also configure the visibility and
   sending options individually for each notification type.

   Select the notification type that you want from the list. For more information,
   refer to "Notification Types" (p. 28). While a notification type is selected, you
   can configure its specific options (when available) in the right-side area:

Visibility

- **Show in Control Center** specifies that this type of event is displayed in Control Center, with the help of 🔔 **Notifications** button.

- **Log to server** specifies that this type of event is also sent to the `syslog` file, in the case when a syslog is configured.

- **Send per email** specifies that this type of event is also sent to certain email addresses. In this case, you are required to enter the email addresses in the dedicated field, pressing `Enter` after each address.

Configuration

- **Use custom threshold** - allows defining a threshold for the occurred events, from which the selected notification is being sent.

  For example, the Malware Outbreak notification is sent by default to users that have at least 5% of all their managed network objects infected by the same malware. To change the malware outbreak threshold value, enable the option **Use Custom Threshold**, then enter the value that you want in the **Malware Outbreak Threshold** field.

- For **Security Server Status event**, you can select the Security Server events that will trigger this type of notification:
  - **Out of date** - notifies each time a Security Server in your network is outdated.
  - **Powered off** - notifies each time a Security Server in your network has been shut down.
  - **Reboot required** - notifies each time a Security Server in your network requires a reboot.

- For **Task Status**, you can select the status type that will trigger this type of notification:
  - **Any status** - notifies each time a task sent from Control Center is done with any status.
  - **Failed only** - notifies each time a task sent from Control Center has failed.

5. Click **Save**.

7. USING REPORTS

GravityZone allows you to create and view centralized reports on the security status of the managed network objects. The reports can be used for multiple purposes, such as:

- Monitoring and ensuring compliance with the organization's security policies.
- Checking and assessing the network security status.
- Identifying network security issues, threats and vulnerabilities.
- Monitoring security incidents.
- Providing upper management with easy-to-interpret data on network security.

Several different report types are available so that you can easily get the information you need. The information is presented as easy-to-read interactive charts and tables, allowing you to quickly check the network security status and identify security issues.

Reports can consolidate data from the entire network of managed network objects or from specific groups only. In this way, from a single report, you can find out:

- Statistical data regarding all or groups of managed network objects.
- Detailed information for each managed network object.
- The list of computers that meet specific criteria (for example, those that have antimalware protection disabled).

Some reports also allow you to quickly fix the issues found in your network. For example, you can effortless update all target network objects right from the report, without having to go and run an update task from the **Network** page.

All scheduled reports are available in Control Center but you can save them to your computer or email them.

Available formats include Portable Document Format (PDF) and comma-separated values (CSV).

7.1. Report Types

Different report types are available for each endpoint type:

- Computer and Virtual Machine Reports
- Exchange Reports
- Mobile Device Reports

7.1.1. Computer and Virtual Machine Reports

These are the available report types for physical and virtual machines:

Antiphishing Activity
Informs you about the activity of the Antiphishing module of Bitdefender Endpoint Security Tools. You can view the number of blocked phishing websites on the selected endpoints and the user that was logged in at the time of the last detection. By clicking the links from the **Blocked Websites** column, you can also view the website URLs, how many times they were blocked and when was the last block event.

Blocked Applications
Informs you about the activity of the following modules: Antimalware, Firewall, Content Control, Application Control, Advanced Anti-Exploit, ATC/IDS and HVI. You can see the number of blocked applications on the selected endpoints and the user that was logged in at the time of the last detection.

Click the number associated to a target to view additional information on the blocked applications, the number of events occurred, and the date and time of the last block event.

Blocked Websites
Informs you about the activity of the Web Control module of Bitdefender Endpoint Security Tools. For each target, you can view the number of blocked websites. By clicking this number, you can view additional information, such as:

- Website URL and category
- Number of access attempts per website
- Date and time of the last attempt, as well as the user that was logged in at the time of the detection.
- Reason for blocking, which includes scheduled access, malware detection, category filtering and blacklisting.

Data Protection
Informs you about the activity of the Data Protection module of Bitdefender Endpoint Security Tools. You can see the number of blocked emails and websites on the selected endpoints, as well as the user that was logged in at the time of the last detection.

Device Control Activity

Informs you about the events occurred when accessing the endpoints through the monitored devices. For each target endpoint, you can view the number of allowed / blocked access and read-only events. If events occurred, additional information is available by clicking the corresponding numbers. Details refer to:

- User logged on the machine
- Device type and ID
- Device vendor and product ID
- Date and time of the event.

Endpoint Encryption Status

Provides you with data regarding the encryption status on the endpoints. A pie chart displays the number of the machines compliant, respectively non-compliant with the encryption policy settings.

A table below the pie chart delivers details such as:

- Endpoint name.
- Full Qualified Domain Name (FQDN).
- Machine IP.
- Operating system.
- Device policy compliance:
  - **Compliant** – when the volumes are all encrypted or unencrypted according to the policy.
  - **Non-compliant** – when the volumes status is not consistent with the assigned policy (for example, only one of two volumes is encrypted or an encryption process is in progress on that volume).
- Device policy (**Encrypt** or **Decrypt**).
- Click the numbers in the Volumes Summary column to view information about each endpoint's volumes: ID, name, encryption status (**Encrypted** or **Unencrypted**), issues, type (**Boot** or **Non-boot**), size, Recovery Key ID.

Endpoint Modules Status

Provides an overview of the protection modules coverage over the selected targets. In the report details, for each target endpoint you can view which

modules are active, disabled or not installed, and also the scanning engine in use. Clicking the endpoint name will show up the **Information** window with details about the endpoint and installed protection layers.

By clicking the **Reconfigure Client** button, you can start a task to change the initial settings of one or several selected endpoints. For details, refer to Reconfigure Client.

Endpoint Protection Status
Provides you with various status information concerning selected endpoints from your network.

- Antimalware protection status
- Bitdefender Endpoint Security Tools update status
- Network activity status (online/offline)
- Management status

You can apply filters by security aspect and status to find the information you are looking for.

Firewall Activity
Informs you about the activity of the Firewall module of Bitdefender Endpoint Security Tools. You can see the number of blocked traffic attempts and blocked port scans on the selected endpoints, as well as the user that was logged in at the time of the last detection.

HyperDetect Activity
Informs you about the activity of the HyperDetect module of Bitdefender Endpoint Security Tools.

The chart in the upper side of the report page shows you the dynamics of the attack attempts over the specified period of time and their distribution by type of attack. Moving the mouse over the legend entries will highlight the associated attack type in the chart. Clicking the entry will show or hide the respective line in the chart. Clicking any point on a line will filter your table data according to the selected type. For example, if you click any point on the orange line, the table will display only exploits.

The details in the lower part of the report help you identify the breaches in your network and if they were addressed. They refer to:

- The path to the malicious file, or the detected URL, in the case of infected files. For file-less attacks it is provided the name of the executable used in

the attack, with a link to a details window which displays the detection reason and the malicious command line string.

- The endpoint on which the detection was made
- The protection module which detected the threat. As HyperDetect is an additional layer of the Antimalware and Content Control modules, the report will provide information about one of these two modules, depending on the type of detection.
- The type of the intended attack (targeted attack, grayware, exploits, ransomware, suspicious files and network traffic)
- The threat status
- The module protection level at which the threat was detected (Permissive, Normal, Aggressive)
- Number of times the threat was detected
- Most recent detection
- Identification as file-less attack (yes or no), to quickly filter the file-less attacks detections

> **i** **Note**
> A file may be used in more types of attacks. Therefore, GravityZone reports it for each type of attack it was involved in.

From this report, you can quickly resolve false positives, by adding exceptions in the assigned security policies. To do so:

1. Select as many entries in the table as you need.

   > **i** **Note**
   > File-less attack detections cannot be added to the exceptions list, due to the fact that the detected executable is not a malware itself, but can be a threat when using a malicious encoded command line.

2. Click the **Add exception** button at the upper side of the table.

3. In the configuration window, select the policies to which the exception should be added and then click **Add**.

   By default, related information for each added exception is sent to Bitdefender Labs, to help improving the detection capabilities of Bitdefender

products. You can control this action using the **Submit this feedback to Bitdefender for a better analysis** checkbox.

If the threat was detected by the Antimalware module, the exception will apply to both On-access and On-demand scanning modes.

> **i** **Note**
> You can find these exceptions in the following sections of the selected policies: **Antimalware > Settings** for files, and **Content Control > Traffic** for URLs.

Malware Status

Helps you find out how many and which of the selected endpoints have been affected by malware over a specific time period and how the threats have been dealt with. You can also see the user that was logged in at the time of the last detection.

Endpoints are grouped based on these criteria:

- Endpoints with no detections (no malware threat has been detected over the specified time period)

- Endpoints with resolved malware (all detected files have been successfully disinfected or moved to quarantine)

- Endpoints with unresolved malware (some of the detected files have been denied access to)

For each endpoint, by clicking the links available in the disinfection result columns, you can view the list of threats and paths to the affected files.

In this report, you can quickly run a Full Scan task on the unresolved targets, by clicking the **Scan infected targets** button from the Action Toolbar above the data table.

Network Incidents

Informs you about the activity of the Network Attack Defense module. A graph displays the number of the attack attempts detected over a specified interval. The report details include:
- Endpoint name, IP and FQDN
- Username
- Detection name
- Attack technique
- Number of attempts
- Attacker's IP

- Targeted IP and port
- When the attack was blocked most recently

Clicking the **Add exceptions** button for a selected detection automatically creates an entry in **Global Exclusions** from the **Network Protection** section.

Network Patch Status

Check the update status of the software that is installed in your network. The report reveals the following details:

- Target machine (endpoint name, IP and operating system).
- Security patches (installed patches, failed patches, missing security and non-security patches).
- Status and last modified time for checked-out endpoints.

Network Protection Status

Provides detailed information on the overall security status of the target endpoints. For example, you can view information about:

- Name, IP, and FQDN
- Status:
  - **Has issues** - the endpoint has protection vulnerabilities (security agent not up to date, security threats detected, etc.)
  - **No issues** - the endpoint is protected and there are no reasons for concern.
  - **Unknown** - the endpoint was offline when the report was generated.
  - **Unmanaged** - the security agent is not installed on the endpoint yet.
- Available protection layers
- Managed and unmanaged endpoints (the security agent is installed or not)
- License type and status (additional license related columns are hidden by default)
- Infection status (the endpoint is "clean" or not)
- Update status of the product and security content
- Software security patch status (missing security or non-security patches)

For unmanaged endpoints, you will view the **Unmanaged** status under other columns.

On-demand Scanning

Provides information regarding on-demand scans performed on the selected targets. A pie chart displays the statistics of successful and failed scans. The table below the chart provides details regarding the scan type, occurrence and last successful scan for each endpoint.

Policy Compliance

Provides information regarding the security policies applied on the selected targets. A pie chart displays the status of the policy. In the table below the chart, you can see the assigned policy on each endpoint and the policy type, as well as the date and the user that assigned it.

Sandbox Analyzer Failed Submissions

Displays all failed submissions of objects sent from the endpoints to Sandbox Analyzer over a specified time period. A submission is considered failed after several retry attempts.

The graphic shows the variation of the failed submissions during the selected period, while in the report details table you can view which files could not be sent to Sandbox Analyzer, the machine where the object was sent from, date and time for each retry, the error code returned, description of each failed retry and the company name.

Sandbox Analyzer Results (Deprecated)

Provides you with detailed information related to the files on target endpoints, which were analyzed in the sandbox over a specified time period. A line chart displays the number of the clean or dangerous analyzed files, while the table presents you with details on each case.

You are able generate a Sandbox Analyzer Results report for all analyzed files or only for those detected as malicious.

You can view:

- Analysis verdict, saying whether the file is clean, dangerous or unknown (**Threat detected / No threat detected / Unsupported**). This column shows up only when you select the report to display all analyzed objects.

  To view the complete list with file types and extensions supported by Sandbox Analyzer, refer to "Supported File Types and Extensions for Manual Submission" (p. 66).
- Threat type, such as adware, rootkit, downloader, exploit, host-modifier, malicious tools, password stealer, ramsomware, spam or Trojan.

- Date and time of the detection, which you can filter depending on the reporting period.
- Hostname or IP of the endpoint where the file was detected.
- Name of the files, if they were submitted individually, or number of analyzed files in case of a bundle. Click the file name or bundle link to view details and actions taken.
- Remediation action status for the submitted files (**Partial**, **Failed**, **Reported Only**, **Successful**).
- Company name.
- More information about the properties of the analyzed file is available by clicking the ⓑ **Read more** button in the **Analysis Result** column. Here you can view security insights and detailed reporting on the sample behavior.

Sandbox Analyzer captures the following behavioral events:
- Writing / deleting / moving / duplicating / replacing files on the system and on removable drives.
- Execution of newly-created files.
- Changes to the file system.
- Changes to the applications running inside the virtual machine.
- Changes to the Windows taskbar and Start menu.
- Creating / terminating / injecting processes.
- Writing / deleting registry keys.
- Creating mutex objects.
- Creating / starting / stopping / modifying / querying / deleting services.
- Changing browser security settings.
- Changing Windows Explorer display settings.
- Adding files to firewall exception list.
- Changing network settings.
- Enabling execution at system startup.
- Connecting to a remote host.
- Accessing certain domains.
- Transferring data to and from certain domains.
- Accessing URLs, IPs and ports through various communication protocols.
- Checking the indicators of virtual environment.
- Checking the indicators of monitoring tools.
- Creating snapshots.
- SSDT, IDT, IRP hooks.
- Memory dumps for suspicious processes.
- Windows API functions calls.

- Becoming inactive for a certain time period to delay execution.
- Creating files with actions to be executed at certain time intervals.

In the **Analysis Result** window, click the **Download** button to save to your computer the Behavior Summary content in the following formats: XML, HTML, JSON, PDF.

Security Audit

Provides information about the security events that occurred on a selected target. The information refers to the following events:

- Malware detection
- Blocked application
- Blocked scan port
- Blocked traffic
- Blocked website
- Blocked device
- Blocked email
- Blocked process
- HVI events
- Advanced Anti-Exploit events
- Network Attack Defense events

Security Server Status

Helps you evaluate the status of the target Security Servers. You can identify the issues each Security Server might have, with the help of various status indicators, such as:

- **Status**: shows the overall Security Server status.

- **Machine status**: informs which Security Server appliances are stopped.

- **AV status**: points out whether the Antimalware module is enabled or disabled.

- **Update status**: shows if the Security Server appliances are updated or whether the updates have been disabled.

- **Load status**: indicates the scan load level of a Security Server as described herein:

  - **Underloaded**, when less than 5% of its scanning capacity is used.

  - **Normal**, when the scan load is balanced.

- **Overloaded**, when the scan load exceeds 90% of its capacity. In such case, check the security policies. If all Security Servers allocated within a policy are overloaded, you need to add another Security Server to the list. Otherwise, check the network connection between the clients and Security Servers without load issues.

- **Near overload**, when the scan load is between 85 and 90% of the full scan capacity.

- **Near underload**, when the scan load is between 5 and 10% of its full scan load.

● **HVI protected VMs**: informs you of the virtual machines that are monitored and protected by HVI module.

● **HVI status**: points out whether the HVI module is enabled or disabled. HVI is enabled if both Security Server and Supplemental Pack are installed on host.

● **Connected Storage Devices**: informs how many ICAP-compliant storage devices are connected to Security Server. Clicking the number will display the list of storage devices, with details for each one: name, IP, type, date and time of the last connection.

● **Storage Scanning Status**: indicates if the Security for Storage service is enabled or disabled.

You can also view how many agents are connected to the Security Server. Further on, clicking the number of connected clients will display the list of endpoints. These endpoints may be vulnerable if the Security Server has issues.

Top 10 Detected Malware
Shows you the top 10 malware threats detected over a specific time period on selected endpoints.

> **i** **Note**
> The details table displays all endpoints which were infected by the top 10 detected malware.

Top 10 Infected Endpoints
Shows you the top 10 most infected endpoints by the number of total detections over a specific time period out of the selected endpoints.

> **ⓘ Note**
> The details table displays all malware detected on the top 10 infected endpoints.

Update Status

Shows you the update status of the security agent or Security Server installed on selected targets. The update status refers to product and security content versions.

Using the available filters, you can easily find out which clients have updated and which have not in the last 24 hours.

In this report, you can quickly bring the agents to the latest version. To do this, click the **Update** button from the Action Toolbar above the data table.

Upgrade Status

Shows you the security agents installed on the selected targets and whether a more recent solution is available.

For endpoints with old security agents installed, you can quickly install the latest supported security agent by clicking the **Upgrade** button.

> **ⓘ Note**
> This report is available only when a GravityZone solution upgrade has been made.

Virtual Machines Network Protection Status

Informs you of the Bitdefender protection coverage in your virtualized environment. For each of the selected machines, you can view which component resolves security issues:
- Security Server, for agentless deployments in VMware NSX and vShield environments, and for HVI
- A security agent, in any other situation

HVI Activity

Informs you about all attacks that HVI modules detected on the selected machines within a specific period of time.

The report also includes information about the date and time of the last detected incident that involved the monitored process, final status of the action taken against the attack, the user under which the process has started and the target machine.

Depending on the action taken, same process may be reported several times. For example, if a process once was killed and another time access was denied, you will see two entries in the report table.

For each process, when you click the last detection date, a separate log with all incidents detected since the process started will be displayed. The log reveals important information, such as the incident type and description, the source and target of the attack, and actions taken to remediate the problem.

In this report, you can quickly instruct the protection module to ignore certain events, which you consider are legitimate. To do this, click the **Add exception** button from the Action Toolbar above the data table.

> **Note**
> The HVI module may be available for your GravityZone solution with a separate license key.

HVI Third Party Tools Injection Status

Offers you a detailed status for each injection run on the target endpoints. The information includes:

- The name of the endpoint.
- The name of the injected tool.
- The IP address of the endpoint.
- The guest operating system.
- The trigger. This may be a memory violation, an on-demand task or a scheduled run.
- The number of successful runs. Clicking the number will pop up a window with the logs path and timestamp for each tool run. Clicking the icon in front of the path will copy it to Clipboard.
- The number of unsuccessful runs. Clicking the number will pop up a window where you can view the reason for failing and the timestamp.
- Last successful injection.

Injections are grouped by target endpoints. You can filter the report to view data only related to a specific tool by using the filtering options in the table's header.

> ℹ️ **Note**
> The HVI module may be available for your GravityZone solution with a separate license key.

Ransomware Activity

Informs you with regards to the ransomware attacks that GravityZone detected on the endpoints you manage, and provides you with the necessary tools to recover the files affected during the attacks.

The report is available as a page in Control Center, distinct from the other reports, accessible right from the GravityZone main menu.

The **Ransomware Activity** page consists of a grid that, for each ransomware attack, lists the following:

- The name, IP address and FQDN of the endpoint on which the attack took place
- The company to which the endpoint belongs
- The name of the user who was logged in during the attack
- The type of attack, respectively a local or a remote one
- The process under which the ransomware ran for local attacks, or the IP address from which the attack was initiated for remote ones
- Date and time of the detection
- Number of files encrypted until the attack was blocked
- The restore action status for all files on the target endpoint

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.

Additional information is available by clicking the number for files. You can view a list with the full path to the original and restored files, and the restore status for all files involved in the selected ransomware attack.

> ⚠️ **Important**
> The backup copies are available for maximum 30 days. Please mind the date and time until files may still be recovered.

To recover files from ransomware:

1. Select the attacks you want in the grid.

2. Click the **Restore files** button. A confirmation window shows up.

    A recovery task is being created. You can check its status in the **Tasks** page, just like for any other task in GravityZone.

If detections are the result of legitimate processes, follow these steps:

1. Select the records in the grid.

2. Click the **Add exclusion** button.

3. In the new window, select the policies to which the exclusion must apply.

4. Click **Add**.

    GravityZone will apply all possible exclusions: on folder, on proccess, and on IP address.

    You can check or modify them in the **Antimalware > Settings > Custom Exclusions** policy section.

> **i** **Note**
> Ransomware Activity keeps record of events for two years.

7.1.2. Exchange Server Reports

These are the available report types for Exchange Servers:

Exchange - Blocked Content and Attachments
Provides you with information about emails or attachments that Content Control deleted from the selected servers over a specific time interval. The information includes:

●   Email addresses of the sender and of the recipients.

    When the email has more recipients, instead of the email addresses, the report displays the recipients number with a link to a window containing the list of email addresses.

●   Email subject.

●   Detection type, indicating which Content Control filter detected the threat.

●   The action taken on the detection.

●   The server where the threat was detected.

Exchange - Blocked Unscannable Attachments

Provides you with information about emails containing unscannable attachments (over-compressed, password-protected, etc.), blocked on the selected Exchange mail servers over a specific time period. The information refers to:

- Email addresses of the sender and of the recipients.

  When the email is sent to more recipients, instead of the email addresses, the report displays the recipients number with a link to a window containing the list of email addresses.

- Email subject.
- The actions taken to remove the unscannable attachments:

  - **Deleted Email**, indicating that the entire email has been removed.
  - **Deleted Attachments**, a generic name for all actions that remove attachments from the email message, such as deleting the attachment, moving to quarantine or replacing it with a notice.

  By clicking the link in the **Action** column, you can view details about each blocked attachment and the corresponding action taken.

- Detection date and time.
- The server where the email was detected.

Exchange - Email Scan Activity

Shows statistics on the actions taken by the Exchange Protection module over a specific time interval.

The actions are grouped by detection type (malware, spam, forbidden attachment and forbidden content) and by server.

The statistics refer to the following email statuses:

- **Quarantined.** These emails were moved to the Quarantine folder.
- **Deleted/Rejected.** These emails were deleted or rejected by the server.
- **Redirected.** These emails were redirected to the email address supplied in the policy.
- **Cleaned and delivered.** These emails had the threats removed and passed through the filters.

An email is considered cleaned when all detected attachments have been disinfected, quarantined, deleted or replaced with text.

- **Modified and delivered.** Scan information was added to the emails headers and the emails passed through the filters.
- **Delivered without any other action.** These emails were ignored by Exchange Protection and passed through the filters.

Exchange - Malware Activity

Provides you with information about emails with malware threats, detected on the selected Exchange mail servers over a specific time period. The information refers to:

- Email addresses of the sender and of the recipients.

  When the email is sent to more recipients, instead of the email addresses, the report displays the recipients number with a link to a window containing the list of email addresses.

- Email subject.
- Email status after antimalware scan.

  By clicking the status link, you can view details about the detected malware and the action taken.

- Detection date and time.
- The server where the threat was detected.

Exchange - Top 10 Detected Malware

Informs you about the top 10 most detected malware threats in email attachments. You can generate two views containing different statistics. One view shows the number of detections by affected recipients and one by senders.

For example, GravityZone has detected one email with an infected attachment sent to five recipients.

- In the recipients view:
    - The report shows five detections.
    - The report details shows only the recipients, not the senders.
- In the senders view:
    - The report shows one detection.

– The report details shows only the sender, not the recipients.

Besides the sender/recipients and the malware name, the report provides you with the following details:

● The malware type (virus, spyware, PUA, etc.)

● The server where the threat was detected.

● Measures that the antimalware module has taken.

● Date and time of the last detection.

Exchange - Top 10 Malware Recipients
Shows you the top 10 email recipients most targeted by malware over a specific time interval.

The report details provide you with the entire malware list that affected these recipients, together with the actions taken.

Exchange - Top 10 Spam Recipients
Shows you the top 10 email recipients by the number of spam or phishing emails detected over a specific time interval. The report provides information also on the actions applied to the respective emails.

7.1.3. Mobile Devices Reports

> **Note**
> Malware protection and related reports are only available for Android devices.

This is the list of available report types for mobile devices:

Malware Status
Helps you find out how many and which of the target mobile devices have been affected by malware over a specific time period and how the threats have been dealt with. Mobile devices are grouped based on these criteria:

● Mobile devices with no detections (no malware threat has been detected over the specified time period)

● Mobile devices with resolved malware (all detected files have been removed)

● Mobile devices with existing malware (some of the detected files have not been deleted)

Top 10 Infected Devices

Shows you the top 10 most infected mobile devices over a specific time period out of the target mobile devices.

> **i** **Note**
> The details table displays all malware detected on the top 10 infected mobile devices.

Top 10 Detected Malware

Shows you the top 10 malware threats detected over a specific time period on the target mobile devices.

> **i** **Note**
> The details table displays all mobile devices which were infected by the top 10 detected malware.

Device Compliance

Informs you of the compliance status of the target mobile devices. You can see the device name, status, operating system and the non-compliance reason.

Device Synchronization

Informs you of the synchronization status of the target mobile devices. You can view the device name, the user it is assigned to, as well as the synchronization status, the operating system and the time when the device was last seen online.

Blocked Websites

Informs you about the number of attempts of the target devices to access websites which are blocked by **Web Access** rules, over a certain time interval.

For each device with detections, click the number provided in the **Blocked Websites** column to view detailed information of each blocked web page, such as:

- Website URL
- Policy component that performed the action
- Number of blocked attempts
- Last time when the website was blocked

Web Security Activity

Informs you about the number of attempts of the target mobile devices to access websites with security threats (phishing, fraud, malware or untrusted websites), over a certain time interval. For each device with detections, click the number provided in the Blocked Websites column to view detailed information of each blocked web page, such as:

- Website URL
- Type of threat (phishing, malware, fraud, untrusted)
- Number of blocked attempts
- Last time when the website was blocked

Web Security is the policy component which detects and blocks websites with security issues.

7.2. Creating Reports

You can create two categories of reports:

- **Instant reports.** Instant reports are automatically displayed after you generate them.
- **Scheduled reports.** Scheduled reports can be configured to run periodically, at a specified time and date. A list of all the scheduled reports is displayed in the **Reports** page.

> ⚠ **Important**
> Instant reports are automatically deleted when you close the report page. Scheduled reports are saved and displayed in the **Reports** page.

To create a report:

1. Go to the **Reports** page.
2. Choose the network objects type from the views selector.
3. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.

Computers and Virtual Machines Report Options

4. Select the desired report type from the menu. For more information, refer to "Report Types" (p. 35)

5. Enter a suggestive name for the report. When choosing a name, consider the report type and target, and possibly the report options.

6. Configure the report recurrence:

- Select **Now** to create an instant report.
- Select **Scheduled** to configure the report to be automatically generated at the time interval that you want:
  – Hourly, at the specified interval between hours.
  – Daily. In this case, you can also set the start time (hour and minutes).

- Weekly, in the specified days of the week and at the selected start time (hour and minutes).

- Monthly, at each specified day on the month and at the selected start time (hour and minutes).

7. For most report types you must specify the time interval to which the contained data is referring. The report will only display data from the selected time period.

8. Several report types provide filtering options to help you easily find the information you are interested in. Use the filtering options under **Show** section to obtain only the desired information.

   For example, for an **Update Status** report you can choose to view only the list of network objects that have not updated, or the ones that need to be restarted to complete the update.

9. **Delivery**. To receive a scheduled report by email, select the corresponding check box. Enter the email addresses that you want in the field below. By default, the email contains an archive with both report files (PDF and CSV). Use the check boxes in the **Attach files** section to customize what files and how to send them by email.

10. **Select Target**. Scroll down to configure the report target. Select one or several groups of endpoints you want to include in the report.

11. Depending on the selected recurrence, click **Generate** to create an instant report or **Save** to create a scheduled report.

    - The instant report will be displayed immediately after clicking **Generate**. The time required for reports to be created may vary depending on the number of managed network objects. Please wait for the requested report to be created.

    - The scheduled report will be displayed in the list on the **Reports** page. Once a report instance has been generated, you can view the report by clicking the corresponding link in the **View report** column on the **Reports** page.

7.3. Viewing and Managing Scheduled Reports

To view and manage scheduled reports, go to the **Reports** page.
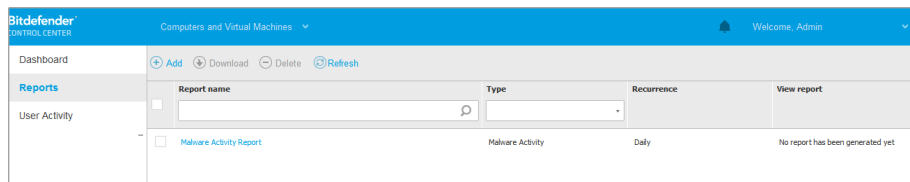
The Reports page

All scheduled reports are displayed in a table together with useful information about them:

- Report name and type
- Report recurrence
- Last generated instance.

> **Note**
> Scheduled reports are available only for the user who has created them.

To sort reports by a specific column, simply click the header of that column. Click the column header again to change the sorting order.

To easily find what you are looking for, use the search boxes or the filtering options below the column headers.

To clear a search box, place the cursor over it and click the ✕ **Delete** icon.

To make sure the latest information is being displayed, click the ↻ **Refresh** button at the upper side of the table.

7.3.1. Viewing Reports

To view a report:

1. Go to the **Reports** page.
2. Sort reports by name, type or recurrence to easily find the report you are looking for.
3. Click the corresponding link in the **View report** column to display the report. The most recent report instance will be displayed.

   To view all instances of a report, refer to "Saving Reports" (p. 59)

All reports consist of a summary section (the upper half of the report page) and a details section (the lower half of the report page).

● The summary section provides you with statistical data (pie charts and graphics) for all target network objects, as well as general information about the report, such as the reporting period (if applicable), report target etc.

● The details section provides you with information on each target network object.

> **ⓘ Note**
>
> ● To configure the information displayed by the chart, click the legend entries to show or hide the selected data.
>
> ● Click the graphic area (pie section, bar) you are interested in to view related details in the table.

7.3.2. Editing Scheduled Reports

> **ⓘ Note**
> When editing a scheduled report, any updates will be applied starting with the report's next recurrence. Previously generated reports will not be impacted by the editing.

To change the settings of a scheduled report:

1. Go to the **Reports** page.

2. Click the report name.

3. Change report settings as needed. You can change the following:

   ● **Report name.** Choose a suggestive name for the report to help easily identify what it is about. When choosing a name, consider the report type and target, and possibly the report options. Reports generated by a scheduled report are named after it.

   ● **Report recurrence (schedule).** You can schedule the report to be automatically generated hourly (by a certain hour interval), daily (at a certain start time), weekly (on a specific day of the week andf start time) or monthly (on a specific day of the month and start time). Depending on the selected schedule, the report will only include data from the last day, week or month, respectively.

   ● **Settings.**

– You can schedule the report to be automatically generated hourly (by a certain hour interval), daily (at a certain start time), weekly (on a specific day of the week andf start time) or monthly (on a specific day of the month and start time). Depending on the selected schedule, the report will only include data from the last day, week or month, respectively.

– The report will only include data from the selected time interval. You can change the interval starting with the next recurrence.

– Most reports provide filtering options to help you easily find the information you are interested in. When you view the report in the console, all information will be available, regardless of the selected options. If you download or email the report however, only the report summary and the selected information will be included in the PDF file. Report details will only be available in CSV format.

– You can choose to receive the report by email.

- **Select target.** The selected option indicates the type of the current report target (either groups or individual network objects). Click the corresponding link to view the current report target. To change it, select the groups or network objects to be included in the report.

4. Click **Save** to apply changes.

7.3.3. Deleting Scheduled Reports

When a scheduled report is no longer needed, it is best to delete it. Deleting a scheduled report will delete all the instances it has generated automatically to that point.

To delete a scheduled report:

1. Go to the **Reports** page.

2. Select the report you want to delete.

3. Click the ⊖ **Delete** button at the upper side of the table.

7.4. Saving Reports

By default, scheduled reports are automatically saved in Control Center.

If you need reports to be available for longer time periods, you can save them to your computer. The report summary will be available in PDF format, whereas report details will be available just in CSV format.

You have two ways of saving reports:

- Export
- Download

7.4.1. Exporting Reports

To export the report to your computer:

1. Choose a format and click either **Export CSV** or **Export PDF**.

2. Depending on your browser settings, the file may be downloaded automatically to a default download location, or a download window will appear, where you must specify the destination folder.

7.4.2. Downloading Reports

A report archive contains both the report summary and the report details.

To download a report archive:

1. Go to the **Reports** page.

2. Select the report you want to save.

3. Click the ⊕ **Download** button and select either **Last Instance** to download the last generated instance of the report or **Full Archive** to download an archive containing all the instances.

   Depending on your browser settings, the file may be downloaded automatically to a default download location, or a download window will appear, where you must specify the destination folder.

7.5. Emailing Reports

You can send reports by email using the following options:

1. To email the report you are viewing, click the **Email** button. The report will be sent to the email address associated with your account.

2. To configure the desired scheduled reports delivery by email:

   a. Go to the **Reports** page.

b. Click the desired report name.

c. Under **Settings > Delivery**, select **Send by email at**.

d. Provide the desired email address in the field below. You can add as many email addresses as you want.

e. Click **Save**.

> **i** **Note**
> Only the report summary and the chart will be included in the PDF file sent by email. Report details will be available in the CSV file.

The reports are sent by email as .zip archives.

7.6. Printing Reports

Control Center does not currently support print button functionality. To print a report, you must first save it to your computer.

8. USER ACTIVITY LOG

Control Center logs all the operations and actions performed by users. The user activity list includes the following events, according to your administrative permission level:

● Logging in and logging out
● Creating, editing, renaming and deleting reports
● Adding and removing dashboard portlets
● Starting, ending, canceling, and stopping troubleshooting processes on affected machines
● Editing authentication settings for the GravityZone accounts.

To examine the user activity records, go to the **User Activity** page and choose the network view that you want from the views selector.

The User Activity Page

To display recorded events that you are interested in, you have to define a search. Fill in the available fields with the search criteria and click the **Search** button. All the records matching your criteria will be displayed in the table.

The table columns provide you with useful information about the listed events:

● The username of who performed the action.

● User role.

● Action that caused the event.

● Type of console object affected by the action.

● Specific console object affected by the action.

● Time when the event occurred.

To sort events by a specific column, simply click the header of that column. Click the column header again to reverse the sorting order.

To view detailed information about an event, select it and check the section under the table.

9. GETTING HELP

For any problems or questions concerning GravityZone, contact an administrator.

9.1. Bitdefender Support Center

Bitdefender Support Center is the place where you will find all the assistance you need with your Bitdefender product.

You can use several resources to quickly find a solution or an answer:

● Knowledge Base Articles

● Bitdefender Support Forum

● Product Documentation

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

Knowledge Base Articles

The Bitdefender Knowledge Base is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the Bitdefender support and development teams, along with more general articles about virus prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The Bitdefender Knowledge Base for business products is available any time at http://www.bitdefender.com/support/business.html.

Bitdefender Support Forum

The Bitdefender Support Forum provides Bitdefender users with an easy way to get help and to help others. You can post any problem or question related to your Bitdefender product.

Bitdefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

Before posting your problem or question, please search the forum for a similar or related topic.

The Bitdefender Support Forum is available at http://forum.bitdefender.com, in 5 different languages: English, German, French, Spanish and Romanian. Click the **Business Protection** link to access the section dedicated to business products.

Product Documentation

Product documentation is the most complete source of information about your product.

The easiest way to reach the documentation is from the **Help & Support** page of Control Center. Click your username in the upper-right corner of the console, choose **Help & Support** and then the link of the guide you are interested in. The guide will open in a new tab of your browser.

A. Appendices

A.1. Sandbox Analyzer Objects

A.1.1. Supported File Types and Extensions for Manual Submission

The following file extensions are supported and can be manually detonated in 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 is able to detect the above-mentioned file types also if they are included in archives of the following types: `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. File Types Supported by Content Prefiltering at Automatic Submission

Content prefiltering will determine a particular file type through a combination which implies the object content and extension. That means that an executable having the `.tmp` extension will be recognized as an application and, if found suspicious, it will be sent to Sandbox Analyzer.

- Applications - files having the PE32 format, including but not limited to the following extensions: `exe, dll, com.`

- Documents - files having the document format, including but not limited to the following extensions: `xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm, dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf.`

- **Scripts:** `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.`

- **Archives:** `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.`

- **Emails (saved in the file system):** `eml, tnef.`

A.1.3. Default Exclusions at Automatic Submission

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

Glossary

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Antimalware Scanning Storm

An intensive use of system resources that occurs when antivirus software simultaneously scans multiple virtual machines on a single physical host.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Bootkit

A bootkit is a malicious program having the ability of infecting the master boot record (MBR), volume boot record (VBR) or boot sector. The bootkit remains active even after a system reboot.

Browser

Short for Web browser, a software application used to locate and display Web pages.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Downloader

It is a generic name for a program having a primary functionality of downloading content for unwanted or malicious purposes.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

Exploit

An exploit generally refers to any method used to gain unauthorized access to computers or a vulnerability in a system's security that opens a system to an attack.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Grayware

A class of software applications between legitimate software and malware. Though they are not as harmful as malware which affects the system's integrity, their behavior is still disturbing, driving to unwanted situations such as data theft and unauthorized usage, unwanted advertising. Most common grayware applications are spyware and adware.

Heuristic

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Keylogger

A keylogger is an application that logs anything you type.

Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they

are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Malware

Malware is the generic term for software that is designed to do harm - a contraction of 'malicious software'. It is not yet in universal usage, but its popularity as a general term for viruses, Trojan Horses, worms, and malicious mobile code is growing.

Malware signature

Malware signatures are snippets of code extracted from actual malware samples. They are used by antivirus programs to perform pattern-matching and detect malware. Signatures are also used to remove the malware code from infected files.

The Bitdefender Malware Signature Database is a collection of malware signatures updated hourly by the Bitdefender malware researchers.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Password stealer

A password stealer collects pieces of data that can be account names and associated passwords. These stolen credentials are then used for malicious purposes, like account takeovers.

Phishing

The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to

visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Ransomware

A malware that locks you out of your computer or blocks access to your files and applications. Ransomware will demand that you pay a certain fee (ransom payment) in return for a decryption key that allows you to regain access to your computer or files.

Report file

A file that lists actions that have occurred. Bitdefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited email.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Suspicious files and network traffic

Suspicious files are those with a doubtful reputation. This ranking is given by many factors, among which to name: existence of the digital signature, number of occurrences in computer networks, packer used, etc. Network traffic is considered suspicious when it deviates from the pattern. For example, unreliable source, connection requests to unusual ports, increased bandwidth usage, random connection times, etc.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

Targeted attacks

Cyber-attacks that mainly aim financial advantages or denigration of reputation. The target can be an individual, a company, a software or a system, well studied before the attack takes place. These attacks are rolled out over a long period of time and in stages, using one or more infiltration points. They are hardly noticed, most times when the damage has already been done.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has its own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.