



Bitdefender[®]

GravityZone

SECURITY ANALYST'S GUIDE

Bitdefender GravityZone Security Analyst's Guide

Publication date 2020.04.15

Copyright© 2020 Bitdefender

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.



Table of Contents

- 1. About GravityZone 1
- 2. GravityZone Protection Layers 2
 - 2.1. Antimalware 2
 - 2.2. Advanced Threat Control 3
 - 2.3. HyperDetect 4
 - 2.4. Advanced Anti-Exploit 4
 - 2.5. Firewall 4
 - 2.6. Content Control 4
 - 2.7. Network Attack Defense 4
 - 2.8. Patch Management 5
 - 2.9. Device Control 5
 - 2.10. Full Disk Encryption 5
 - 2.11. Security for Exchange 6
 - 2.12. Sandbox Analyzer 6
 - 2.13. Endpoint Detection and Response (EDR) 7
 - 2.14. Endpoint Risk Analytics (ERA) 7
 - 2.15. Email Security 7
 - 2.16. Security for Storage 7
 - 2.17. GravityZone Protection Layers Availability 8
- 3. GravityZone Architecture 9
 - 3.1. Security Server 9
 - 3.2. Security Agents 9
 - 3.2.1. Bitdefender Endpoint Security Tools 9
 - 3.2.2. Endpoint Security for Mac 11
 - 3.3. Sandbox Analyzer Architecture 12
 - 3.4. EDR Architecture 14
- 4. Getting Started 15
 - 4.1. Connecting to Control Center 15
 - 4.2. Control Center at a Glance 16
 - 4.2.1. Table Data 17
 - 4.2.2. Action Toolbars 18
 - 4.2.3. Contextual Menu 19
 - 4.3. Changing Login Password 20
 - 4.4. Managing Your Account 20
- 5. Monitoring Dashboard 23
 - 5.1. Refreshing Portlet Data 24
 - 5.2. Editing Portlet Settings 24
 - 5.3. Adding a New Portlet 24
 - 5.4. Removing a Portlet 25
 - 5.5. Rearranging Portlets 25
- 6. Investigating Incidents 26
 - 6.1. The Incidents Page 26



6.1.1. Filtering Security Events	27
6.1.2. Viewing the List of Security Events	31
6.1.3. Investigating a Security Event	35
6.2. Blocklisting Files	77
6.3. Searching Security Events	79
6.3.1. The Query Language	80
6.3.2. Running Queries	82
6.3.3. Favourite Searches	84
6.3.4. Predefined queries	85
7. Notifications	86
7.1. Notification Types	86
7.2. Viewing Notifications	87
7.3. Deleting Notifications	88
7.4. Configuring Notification Settings	89
8. Using Reports	91
8.1. Report Types	91
8.1.1. Computer and Virtual Machine Reports	92
8.1.2. Exchange Server Reports	102
8.2. Creating Reports	105
8.3. Viewing and Managing Scheduled Reports	107
8.3.1. Viewing Reports	108
8.3.2. Editing Scheduled Reports	109
8.3.3. Deleting Scheduled Reports	110
8.4. Taking Report-Based Actions	110
8.5. Saving Reports	111
8.5.1. Exporting Reports	111
8.5.2. Downloading Reports	111
8.6. Emailing Reports	112
8.7. Printing Reports	112
9. User Activity Log	113
10. Getting Help	114
10.1. Bitdefender Support Center	114
A. Appendices	116
Glossary	117



1. ABOUT GRAVITYZONE

GravityZone is a business security solution built from ground-up for virtualization and cloud to deliver security services to physical endpoints, 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 blacklisting 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
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Endpoint Risk Analytics (ERA)
- Email Security

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.



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.



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. 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, analyze their behavior and report any subtle system changes that is indicative of malicious intent.

Sandbox Analyzer automatically submits suspicious files residing on the managed endpoints, yet hidden to signature-based antimalware services. Dedicated heuristics embedded in the Antimalware on-access module from Bitdefender Endpoint Security Tools trigger the submission process.

The Sandbox Analyzer service is able to prevent unknown threats from executing on the endpoint. It operates in either monitoring or blocking mode, allowing or denying access to the suspicious file until a verdict is received. Sandbox Analyzer automatically resolves discovered threats according to the remediation actions defined in the security policy for the affected systems.

Additionally, Sandbox Analyzer allows you to manually submit samples directly from Control Center, letting you decide what to do further with them.

2.13. Endpoint Detection and Response (EDR)

Endpoint Detection and Response is an event correlation component, capable of identifying advanced threats or in-progress attacks. As part of our comprehensive and integrated Endpoint Protection Platform, EDR 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 EDR 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.

2.14. Endpoint Risk Analytics (ERA)

Endpoint Risk Analytics (ERA) identifies, assesses and remediates Windows endpoints weaknesses via security risk scans (on-demand or scheduled via policy), taking into account a vast number of indicators of risk. Once you have scanned your network with certain indicators of risk, you will obtain an overview of your network risk status via **Risk Management** dashboard, available from the main menu. You will be able to resolve certain security risks automatically from GravityZone Control Center, and view recommendations for endpoint exposure mitigation.

2.15. Email Security

Through Email Security you can control email delivery, filter messages, and apply company-wide policies, to stop targeted and sophisticated email threats, including Business Email Compromise (BEC) and CEO fraud. Email Security requires account provisioning to access the console. For more information, refer to the [Bitdefender Email Security User Guide](#).

2.16. 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.

2.17. 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](#)
- [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. 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](#)

3.2.1. 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
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Endpoint Risk Analytics (ERA)

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:

-

- 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.

3.2.2. 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. Sandbox Analyzer Architecture

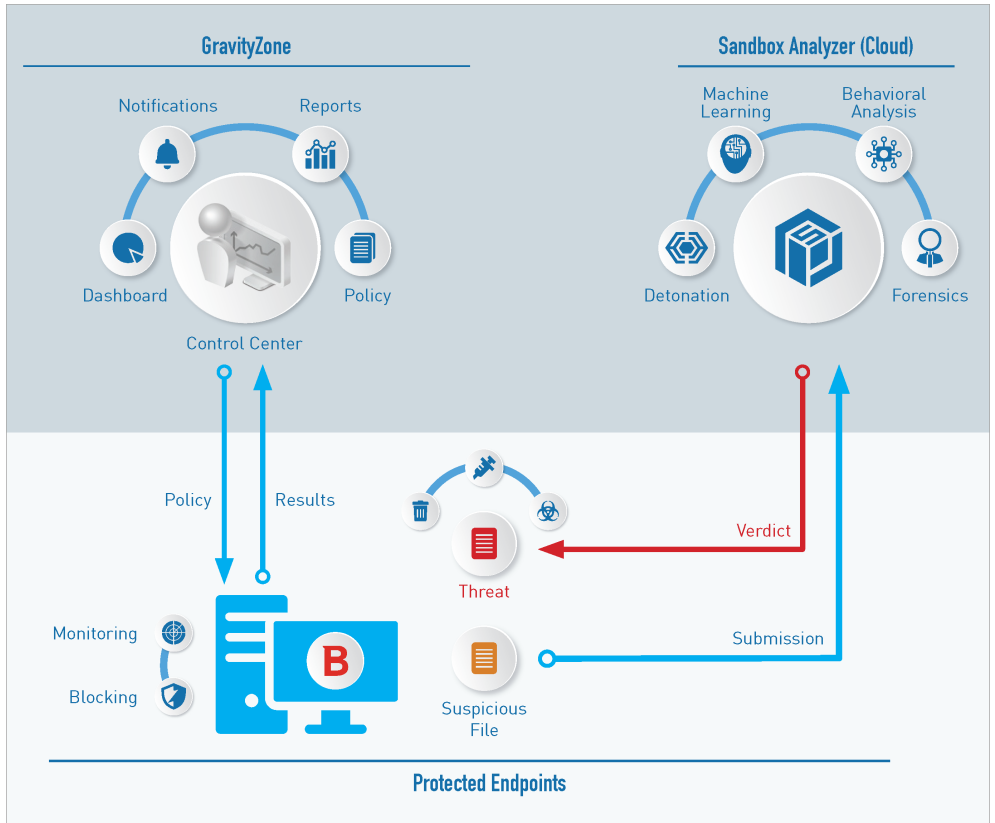
Bitdefender Sandbox Analyzer provides a powerful layer of protection against advanced threats by performing automatic, in-depth analysis of suspicious files which are not yet signed by Bitdefender antimalware engines.

Sandbox Analyzer contains the following components:

- **Sandbox Analyzer Portal.** This component is a hosted communication server used for handling requests between endpoints and the Bitdefender sandbox cluster.
- **Sandbox Analyzer Cluster.** This component is 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.



The Sandbox Analyzer architecture

Once the Sandbox Analyzer service is activated from Control Center on endpoints:

1. The Bitdefender security agent starts to submit suspicious files that match the protection rules set in the policy.
2. After the files are analyzed, a response is sent back to the Portal and further to the endpoint.
3. If a file is detected as dangerous, the user gets notified and a remediation action is taken.

The analysis results are preserved by file hash value in the Sandbox Analyzer database. When a previously analyzed file is submitted from a different endpoint,



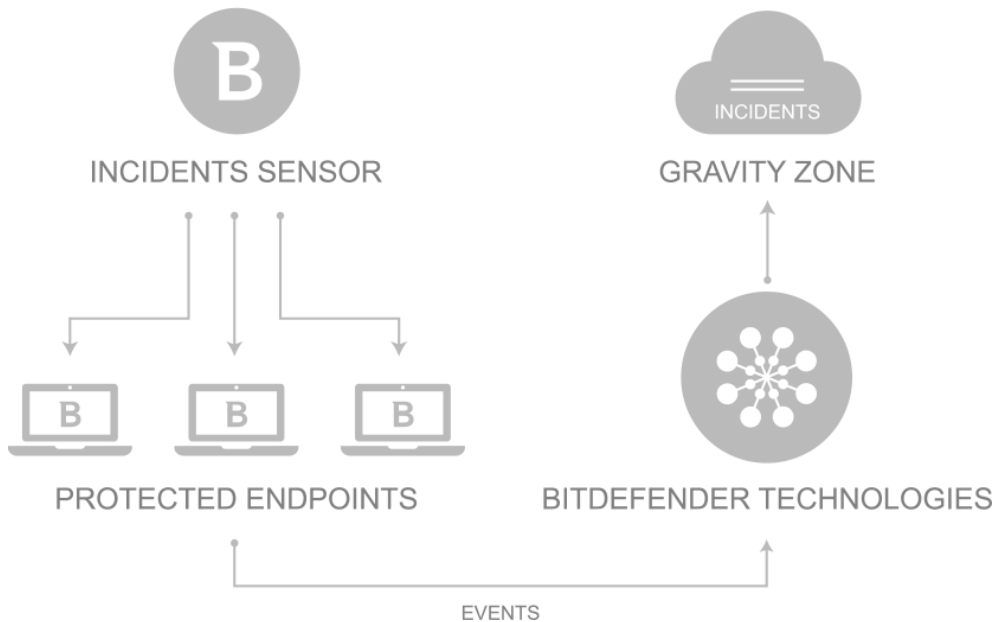
a response is immediately sent back as the results are already available in the database.

3.4. EDR Architecture

To identify advanced threats and in-progress attacks, EDR requires hardware and operating system data. Some of the raw data is processed locally, while machine learning algorithms in the Security Analytics, perform more complex tasks.

EDR contains two major components:

- The Incidents Sensor, which collects process data, and reports endpoint and application behavior data.
- The Security Analytics, a back-end component part of the suite of Bitdefender technologies used to interpret metadata collected by the Incidents Sensor.



EDR flow from endpoint to Control Center

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:

1. Open your web browser.
2. Go to the following address: <https://gravityzone.bitdefender.com>
3. If you use **GravityZone credentials**:
 - a. Enter the email address of your account and click **Next**.
 - b. Enter the password of your account and click **Next**.
 - c. Enter the six-digit code from Google Authenticator as part of the two-factor authentication.
 - d. Click **Continue** to log in.

If you use **single sign-on**:

- a. When first logging in, enter the email address of your account and click **Next**. GravityZone will redirect you to the authentication page of your identity provider.
- b. Authenticate with the identity provider.

- c. The identity provider will redirect you back to GravityZone and you will automatically log in to Control Center.

Next time, you will log in to Control Center with just your email address.

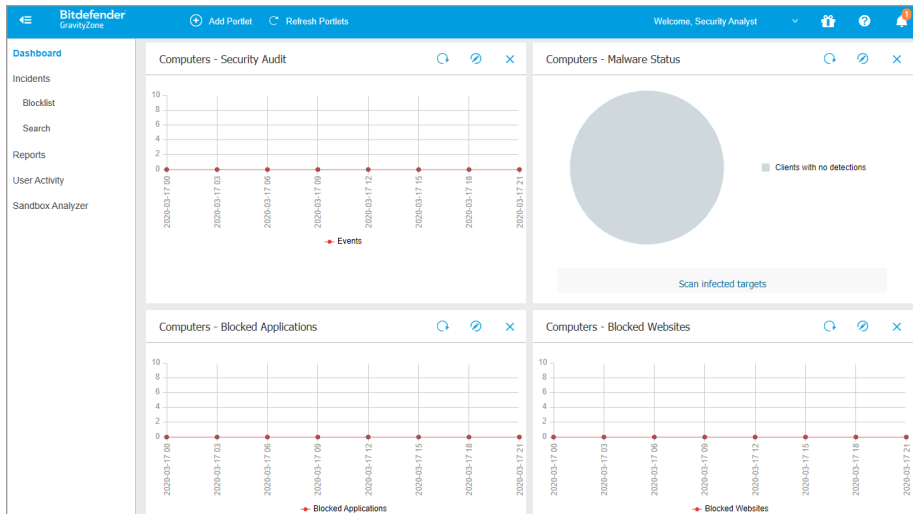
At the first login, you have to agree to Bitdefender Terms of Service. Click **Continue** to start using GravityZone.

Note

- If you have forgotten your password, use the password recovery link to receive a new password. You must provide the email address of your account.
- If your account Portlet uses single sign-on, but GravityZone asks you for a password, contact your administrator for assistance. In the meantime, log in with your previous password or use the password recovery link to receive a new password.

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.

+ Add Download Delete Refresh			
Report name	Type	Recurrence	View report
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/> Malware Activity Report	Malware Activity	Weekly	No report has been generated yet

First Page Page 1 of 1 Last Page 20 1 items

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.

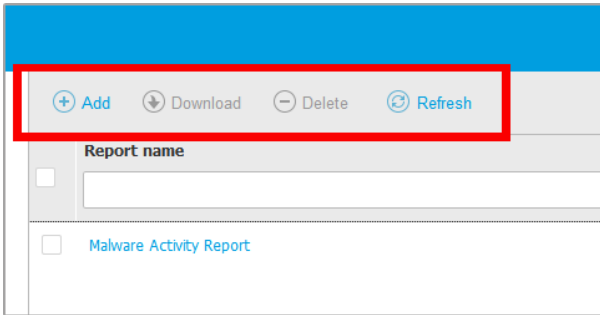
This may be needed when you spend more time on the page.

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:

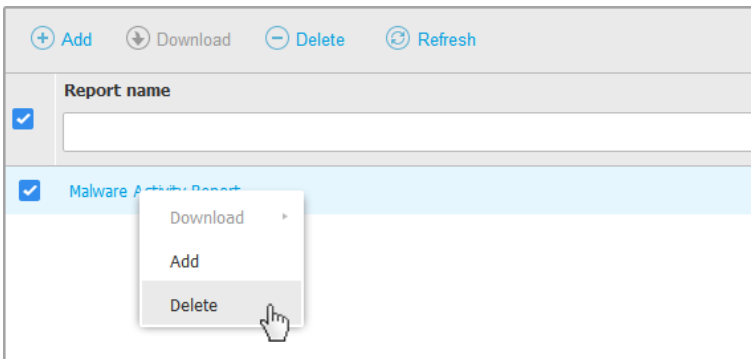
- Create a new report.
- Download a scheduled report.
- Delete a scheduled report.



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

4.3. Changing Login Password

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

It is recommended to do the following:

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

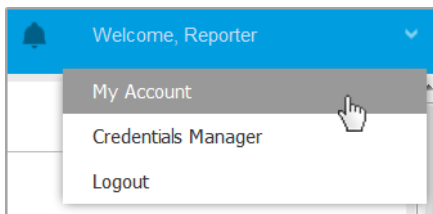
To change the login password:

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.
 - **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. 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 app on a mobile device, link it to your GravityZone account, then use it with each Control Center login. Google Authenticator generates a six-digit code each 30 seconds. To complete the Control Center login, after entering the password, you will need to provide the Google Authenticator six-digit code.



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:

- a. Go to **My account > Two-factor authentication** and click **Enable**.
- b. A dialog box opens. Click the appropriate link to download and install Google Authenticator on your mobile device.
- c. On your mobile device, open Google Authenticator.
- d. 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 Google Authenticator on a new device and provide the secret key to link it to your GravityZone account.

- e. Enter the six-digit code in the **Google Authenticator code** field.
- f. Click **Enable** to complete the feature activation.

**Note**

Your Company Administrator may turn two-factor authentication mandatory for all GravityZone accounts. In this case, you will be asked at login to configure your 2FA. At the same time, you will not be able to deactivate 2FA for your account as long as this feature is enforced by your Company Administrator.

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

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

**Note**

You cannot delete your own account.

5. MONITORING DASHBOARD

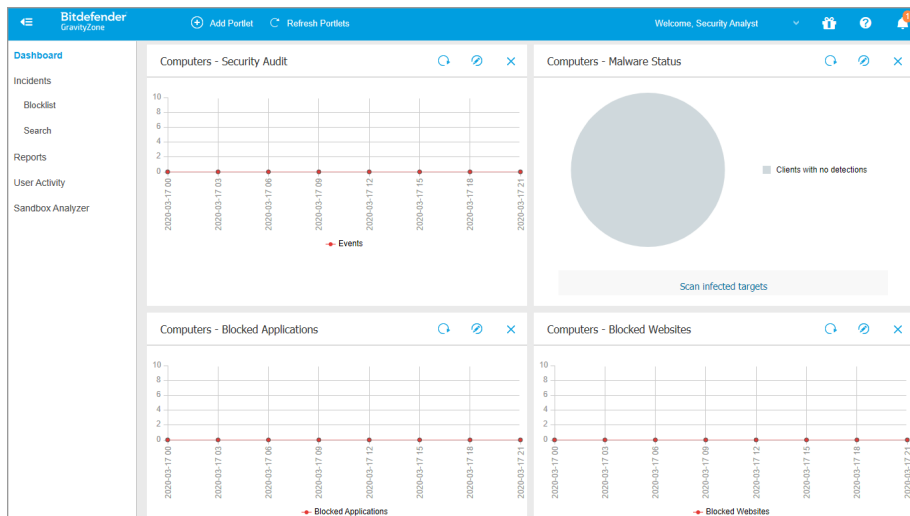
The Control Center dashboard is a customizable visual display providing a quick security overview of all protected endpoints and network status.

It is composed of two sections:

- Dashboard network status bar
- Dashboard portlets

The Dashboard network status bar updates you with the number of opened or in-progress incidents, threatened assets (endpoints) and detected threats in your network. Use this information to glance over unresolved network items. Click **View** to access the **Incidents** page. For more information, refer to [“Investigating Incidents” \(p. 26\)](#).

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. 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.


5.2. 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.


5.3. 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:
 - 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. 91).
4. Under the **Targets** tab, select the network objects and groups to include.
 5. Click **Save**.

5.4. 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.

5.5. 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.



Note

You can move portlets only within the positions already taken.

6. INVESTIGATING INCIDENTS

The **Incidents** section helps you filter, investigate and take actions on all security events detected by Incidents Sensor over a specific time interval.

The **Incidents** section contains the following pages:

- **Incidents**: allows viewing and investigating security events.
- **Blocklist**: manages blocked files involved in security events.
- **Search**: provides options for querying the security events database.

6.1. The Incidents Page

Use the **Incidents** page to filter and manage security events.

Score	Date	Status	ID	Endpoint	Attack type	Alerts
90	Created at 12:57	Open	3	LEV-ENDPOINT2	Other	20
90	Created at 13:27	Open	2	LEV-ENDPOINT2	Other	28
90	Created at 13:27	Open	1	LEV-ENDPOINT2	Other	28

Incidents page overview

This page contains the following areas:

1. **Investigate** and **Review** tabs, containing corresponding incident categories.

2. **Overview** bar, listing the open incidents, top alerts, used attack techniques, and affected devices.
3. **Filters**, providing multiple filtering criteria for security events.
4. **List of security event cards**, displaying the list of events according to the applied filters.



Note

This feature no longer provides support for Internet Explorer.

This is what you can do from the **Incidents** page:

- [Filter security events](#)
- [View the list of security events](#)
- [Open and investigate a security event](#)

6.1.1. Filtering Security Events

Use filters to refine your search when analyzing security events.

OPEN INCIDENTS		TOP ALERTS		TOP TECHNIQUES		TOP AFFECTED DEVICES	
High	3	ATC.Malicious	3	Modify Registry	3	LEV-ENDPOINT2	3
Medium	0	CertUtil Process	2	PowerShell	3		
Low	0	PowerShell Command	2	Command-Line Interface	3		

Score	Date	Status	ID	Endpoint	Attack type	Alerts
100-30	Select...	Open	Search...	Search...	Choose...	20
90	Created at 12:57	Open	3	LEV-ENDPOINT2	Other	20

Security events filtering options

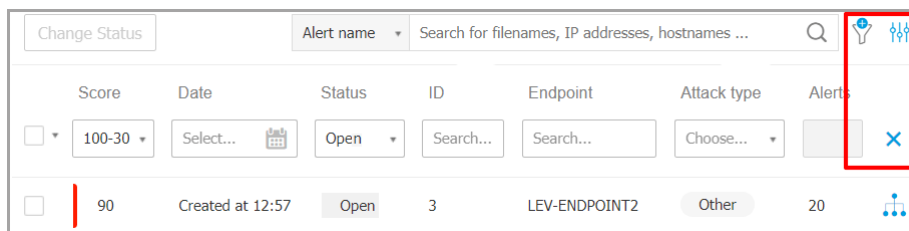
1. GravityZone groups security events under two categories, available as tabs in the **Incidents** page. Click the tab you want for viewing the appropriate list of security events:

- Investigate:** displays all suspicious incidents requiring investigation, upon which no action was taken yet. Here you can find all reported endpoint activity that may represent a threat and needs your attention.
- Review:** includes security events identified as threats by GravityZone prevention modules and applied with the predefined policy actions. In certain cases, these incidents require taking an action, or you may want to review them for further analysis.

2. Fully customizable grid with multiple filtering options.

The Filters Grid

The **Incidents** page allows you to choose what incidents to display by customizing the filters grid.





Filters Grid

- Show/Hide Columns** button to add or remove filter columns. The page will update automatically, loading the security event cards with information matching the added columns.
- Show/Hide Filters** button to show or hide the filters bar.
- Clear Filters** button to reset all filters.

Find details of the available filtering options in the following table:

Filtering Option	Details
Score	The confidence score is a number between 100 and 10, indicating how potentially dangerous a security event is. The higher the score,



Filtering Option	Details
	<p>the more certain the event is dangerous. It provides context based on the attack indicators, and ATT&CK Techniques, if applicable.</p> <p>To filter by confidence score, drag the slider bar to the chosen values. Or, you can use the number fields below the slider bar. Click OK to confirm the score selection.</p>
Date	<p>To filter by date:</p> <ol style="list-style-type: none"> 1. Click the  calendar icon or the Date field to open the date configuration page. 2. Select the time frame when the incident occurred: <ul style="list-style-type: none"> • Click the From and To tabs to select the dates defining the time interval. <p style="text-align: center;"> Note You can specify the exact time for the start and end dates, using the hours and minutes fields below the calendar.</p> <ul style="list-style-type: none"> • You can also select a predetermined time frame, relative to the current time (the last 7 up-to 90 days). 3. Click OK to apply the filter.
Status	<p>Filter the incidents by their current status by checking one or more of the status options available in the Status drop-down menu:</p> <ul style="list-style-type: none"> • Open: for uninvestigated security events • Investigating: for security events under investigation • False Positive: for security events labeled as false alarm • Closed: for security events with closed investigation
ID	<p>Narrow the incident list by searching a specific security event ID number.</p>
Endpoint	<p>Narrow the incident list by searching a specific endpoint name from your managed network.</p>

Filtering Option	Details
Attack Type	The attack type is a dynamic list of the most common types of attack, which changes based on the attack indicators found in the listed security events.
Alerts	The Alerts column displays the number of alerts triggered per incident.
Endpoint OS	This option filters the security events by operating system of involved endpoints.

To search for more elements that are not visible in the filter grid, select one of the search options from the **Search** drop-down menu:

- **Alert name** - 3 to 1000 max. characters.
- **ATT&CK Technique** - 100 maximum characters.
- **Endpoint IP** - 45 maximum characters.
- **MD5** - 32 maximum characters.
- **SHA256** - 64 maximum characters.
- **Node name** - 360 maximum characters.
- **Username** - 1000 maximum characters.

The page will update automatically, loading only the security event cards matching the searched element. For a more granular search, you can create search queries in the [Search page](#).

Filtering incidents from the Overview bar

You can also filter the incidents list by selecting values in the **Overview** bar:

- If you click a value in the **OPEN INCIDENTS** section it will display only the incidents with the selected level of severity.
- If you click a value in the **TOP ALERTS** section it will populate the search field with the alert name and display only the incidents where the alert was detected.
- If you click a value in the **TOP TECHNIQUES** section it will populate the search field with the technique name and display only the incidents where the technique was detected.

- If you click a value in the **TOP AFFECTED DEVICES** section, it will display only the incidents affecting the selected device.

6.1.2. Viewing the List of Security Events

The **Incidents** page displays a list of security events matching the selected filters. By default, there are 20 events per page, bundled by date. The page auto-refreshes at regular intervals, as EDR triggers new events.

Important

All security events older than 90 days are automatically deleted from both **Investigate** and **Review** sections, and also from the security events repository.

To navigate through the page, use the arrow keys, scroll wheel, or click the scroll bar. Change the number of displayed events at the bottom of the page. You can go up to 100 events per page.


Each security event entry is listed in a rich card format, providing an overview of each incident, with information based on the selected filters.

Note

Check the left-border color for quickly assessing the confidence level (low, medium or high).



Security Event Card

- If you click the corresponding  **View Graph** button of a security event card, it will [open it in a new page](#), where you can analyze the incident in detail and take appropriate actions.
- If you click on a security event card, it will open a side quick view panel with information about the selected incident.

#1
Reported

INCIDENT DETAILS

Incident ID: #1
 Status: Open
 Created On: 16 Jan 2020, 13:27:05
 Last Updated on: 16 Jan 2020, 13:27:05
 Endpoint: LEV-ENDPOINT2
 Artifacts Involved: 45

DETECTION

Confidence Score: 90
 Incident Trigger: user.exe(PID:3584)

ScriptFileWrittenByPowershell

A suspicious script was written by powershell.exe or another process with powershell.exe as parent which could indicate lateral movement.

Detected By: EDR
 Detected on: 16 Jan 2020, 13:26
 Severity: Low

ATTACK INFO

Attack Type: Other

View Graph **View Events**

Quick View of Incident Details

- Click the **View Graph** button to access the graphic visualization of the incident.
- Click the **View Events** button to access the incident's timeline.
- If you select the check box of any security event card, it will activate the **Change Status** button, allowing you to change the current status of the incident.



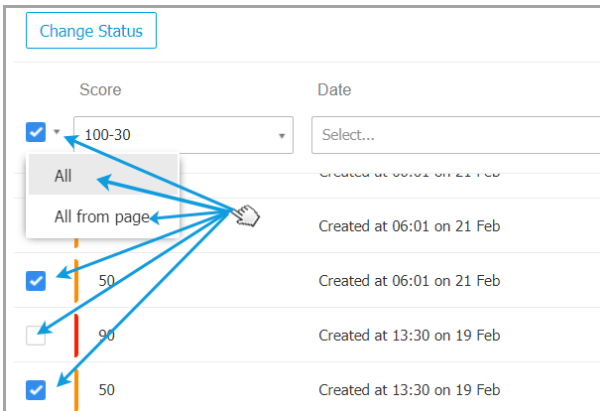
90 Created at 12:57 Open 3 LEV-ENDPOINT2 Other 20

Changing the Status of Security Events

The investigation status helps you keep track of incidents that have already been investigated, and marked as closed or false positive, incidents that are currently under investigation, and open, or new incidents that have yet to be analyzed.

You can choose to change the status of one or multiple security events at a time:

1. Check the boxes of the security event cards that will undergo a status change.



Selecting Security Event Cards

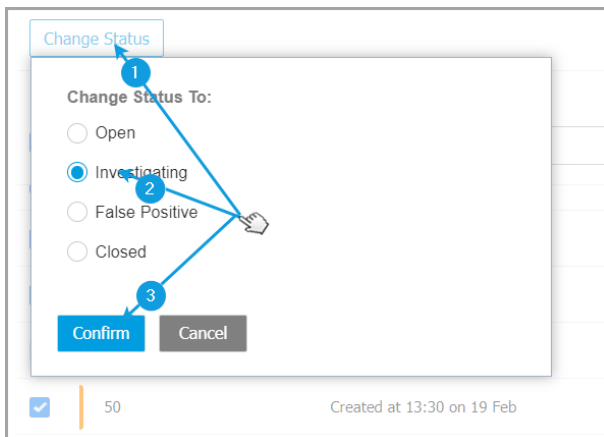
You can select them individually or by using the bulk selection options in the drop-down menu.



Note

You can also browse through several security event pages while keeping your selection.

2. Click the **Change Status** button and select the desired options:



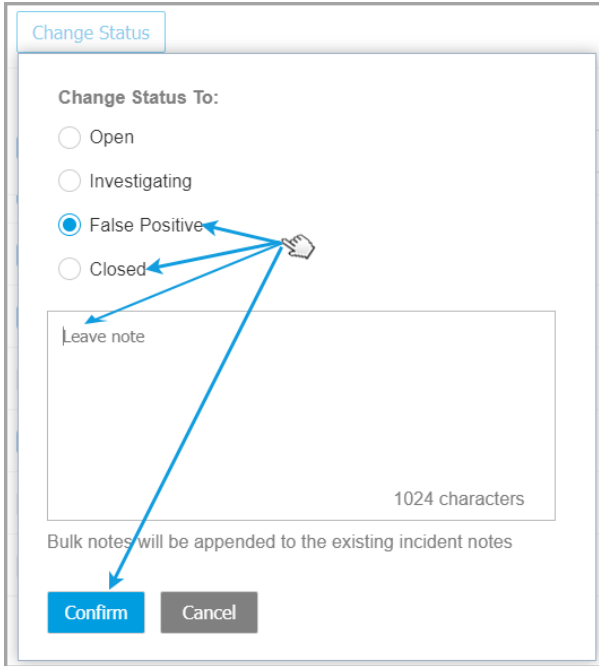
Changing the Status of Security Event

- **Open** - when the security event is not yet under investigation.
- **Investigating** - when you have started to investigate the event.
- **False Positive** - when you analyzed the event and identified it as a false positive.
- **Closed** - when you have done investigating.



Note

A box will open when changing the status of events to **False Positive** or **Closed**, where you can leave a note on the reasons for changing the event status, for later consultation.



Leaving Note for False Positive and Closed events




Note

The note will be appended to the ones already existing inside the filtered incidents.

3. Click **Confirm** to apply the selected status option.

6.1.3. Investigating a Security Event

In the **Incidents** page, identify the security event you want to analyze and click the  **View Graph** button to display it in a new page.



Each security incident has a dedicated page containing detailed information about the sequence of events (displayed in the graph as linked security event nodes) that led to triggering the incident, and provides options to take remediation actions.

Security Incident Page

1. Graph tab

The Graph displays the security incident and its consisting elements, highlighting the Critical Path of the incident and displaying the details of the node that triggered the incident in the **Node Details** panel.

2. Events tab

The Events tab displays filterable detected system events and alerts, and their corresponding event descriptions.

3. Incident Info panel

This panel contains collapsible sections with details like incident ID, current status, timestamp when it was created and last updated, number of involved artifacts, trigger name and attack info.

4. Remediation panel

This panel includes collapsible sections with actions taken automatically by GravityZone and recommended steps you can follow to mitigate the incident.

5. Notes clipboard

Clicking the **Notes** button opens a clipboard where you can add notes on the current incident which you may read when you revisit the incident at a later time.

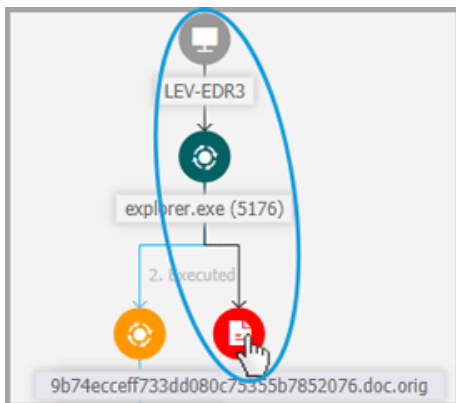
6. Incident status bar

The status bar offers details on the ID of the incident, the time and date it was generated, status, incident trigger and the endpoint it affects. Clicking the **Back** button will take you back to the main **Incidents** page.

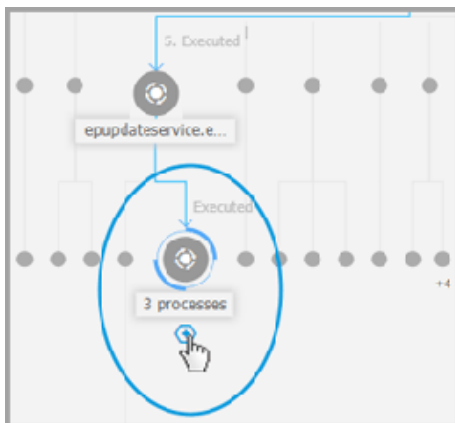
Security Event Nodes

This is what you need to know about security event nodes:

- Each node represents a specific element involved in the investigated incident.
- All nodes that make the critical path are shown by default in detail when you open the incident, while the other elements are faded out, to avoid cluttering the view.
 - Hovering over a node that is not part of the critical path will highlight it and show the path to the point of origin, without breaking the **Critical Path**.



- Three or more same action type event nodes spawning from a parent node are grouped into an expandable cluster-node.



- Only nodes without child elements will be hidden from the incident graph when the cluster-node is collapsed.
- Nodes where suspicious activity has been detected will not be added to the cluster-node.
- Clicking a node will display the following details:

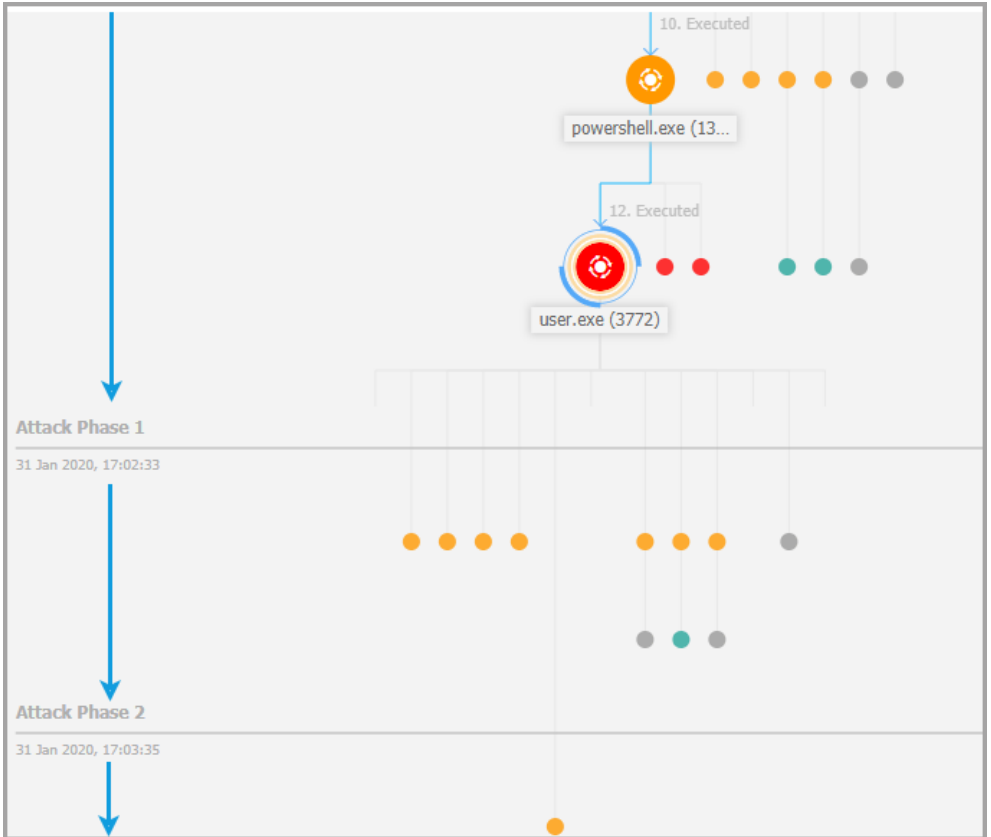
- It will highlight in blue the path to the endpoint node along with all the other involved elements.
- A side panel with expandable sections that provide detailed information of the selected node, alerts in case detections are triggered, available actions and recommendations. Refer to “[Node Details](#)” (p. 50) for more information.
- Nodes are linked by arrow-lines indicating the course of actions that occurred on the endpoint during the incident. Each line is labeled with the action name and its chronological number.

The following elements of an incident can be represented as nodes:

Node Type	Description
Endpoint	Displays endpoint details and patch management status.
Domain	Shows information about the domain host and its endpoints.
Process	Shows details about the process role in the current incident, file information, process executions details, network presence and further investigation options.
File	Shows details about the file role in the current incident, file information, network presence and further investigation options.
Registry	Displays Registry information and the parent process details.

Graph

The **Graph** provides an interactive graphical representation of the investigated incident and its context, highlighting the sequence of elements directly involved in triggering it, known as the **Critical Path** of the incident, as well as all the other elements involved, which are faded out by default. In case of complex incidents that evolve over time, the graphic displays every single stage of the attack.



Staged Attack

The Graph includes filtering options that allow the customization of the incident graphic to improve visualization, features to navigate the incident map, and details panels with more information about each element.

The screenshot displays the Bitdefender GravityZone interface. At the top, there is a navigation bar with a 'Back' button, a shield icon, and the following information: '#901 Reported', 'Date 25 Feb 2020', 'Status Open', and 'Endpoint LEV-ENDPOINT2'. The main area is divided into two sections. On the left, a process execution graph shows a sequence of events: 'user.exe (368)' at the bottom, followed by 'powershell.exe (35...)', 'poc_ctc_gambit.exe...', and 'explorer.exe (5700)', all leading to 'LEV-ENDPOINT2' at the top. A blue oval highlights the path from 'user.exe' to 'explorer.exe'. On the right, a 'Graph' tab is selected, showing details for 'user.exe Process Execution'. The 'ALERTS' section indicates 'PROCESS DETECTED AS MALWARE BY ANALYSIS' with a severity of 'High'. Below this, several alerts are listed: 'Suspicious File Drop', 'ScriptFileWrittenByPowershell', and 'Behavior.BatDropped.1'. The 'INVESTIGATION' section shows 'NETWORK PRESENCE' with '4 endpoints' and 'First Seen: 07 Aug 2019, 13:35'. A 'FURTHER ANALYSIS' section indicates 'Sandbox Analysis completed'. Four blue callout numbers are present: '1' points to the 'user.exe' node, '2' points to the filter icon, '3' points to the navigator icon, and '4' points to the graph details panel.

The Graph Tab

- 1. Critical Path
- 2. Filters Menu
- 3. Navigator Menu
- 4. Node Details Panel

Critical Path

The **Critical Path** is the sequence of linked security events that have led up to setting off an alert, starting from the point of entry in the network down to the event node that triggered the incident. The critical path of the incident is highlighted by default in the graph, along with all consisting event nodes on it, while the other elements are minimized.

The trigger node easily stands out from the rest of the elements in the graph, being surrounded by additional highlight features (two orange circles), and a related info

panel is displayed by default alongside the incident graph, providing detailed trigger node information.

The screenshot displays a process execution graph on the left and a detailed alert panel on the right. The graph shows a critical path starting from 'user.exe (7368)' (labeled 1), which executed 'powershell.exe (35...)' (labeled 16), which then executed 'poc_ctc_gambit.ex...' (labeled 13), which finally executed 'explorer.exe (5700)' (labeled 6). The path ends at 'LEV-ENDPOINT2'. A blue arrow labeled 2 points to the 'user.exe' node, which is highlighted with a red circle. A blue arrow labeled 3 points to the 'poc_ctc_gambit.ex...' node. The alert panel on the right is titled 'user.exe Process Execution' and contains the following information:

- ALERTS** (4 total)
 - PROCESS DETECTED AS MALWARE BY ANALYSIS
 - ATC.Malicious
- Advanced Threat Control has labeled user.exe as a potential threat to your system.
- Detected By: ATC
- Detected on: 25 Feb 2020, 13:23
- Severity: High
- Suspicious File Drop (+)
- ScriptFileWrittenByPowershell (+)
- Behavior.BatDropped.1 (+)

INVESTIGATION

- NETWORK PRESENCE
 - 4 endpoints | First Seen: 07 Aug 2019, 13:35
- FURTHER ANALYSIS
 - Sandbox Analysis completed

Critical Path

1. Trigger Node
2. Node Details panel with information grouped in categories and collapsible sections
3. Faded out nodes indirectly involved in the incident



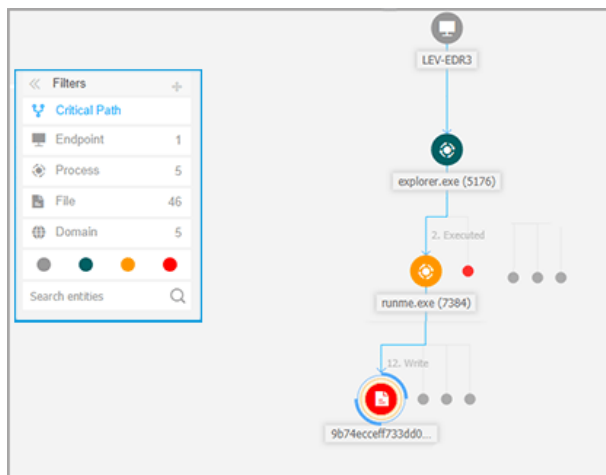
Note

Clicking any other element than the trigger node will break the critical path and highlight the path to origin, from the selected node upstream to endpoint node.

Filters

The **Filters** menu provides you with enhanced filtering capabilities, allowing full manipulation of the incident graph, by highlighting the elements based either on their type or relevance, or by hiding them to make the incident more compact and easier to analyze.

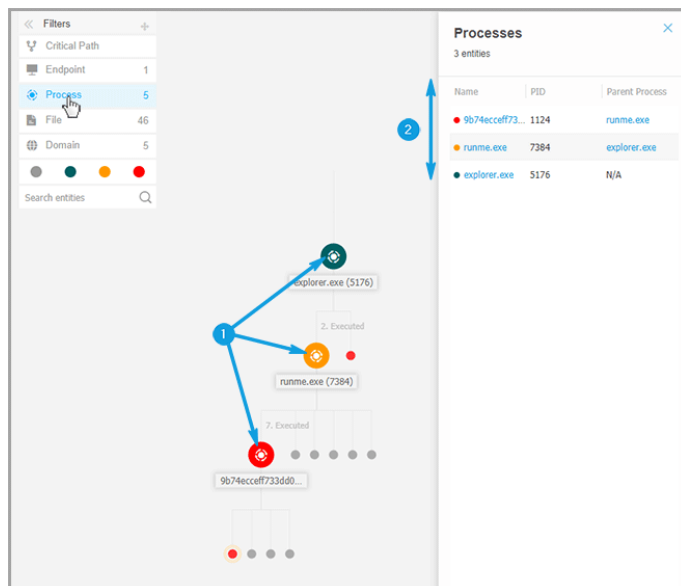
Click and hold the **+ Drag** icon to position the floating Filters panel anywhere inside the incident graph.



Incident Graph Filters

When selecting an element-type filter:

1. The incident graphic zooms out and highlights all the elements of the selected type, while the elements of different type are faded out.
2. It instantly opens a panel with the list of all the highlighted elements.



Note Selecting an element from the displayed list will highlight it in the incident graphic, and open a details panel with information related to that element. Only one filter can be applied at a time.

Filtering options include:

- **Critical Path:** It highlights the critical path of the incident of compromise.
- **Endpoint:** It highlights the endpoints affected by the incident.
- **Process:** It highlights all process-type nodes involved in the incident.
- **File:** It highlights file-type nodes involved in the incident.
- **Domain:** It highlights all domain-type nodes involved in the incident.
- **Registry:** It highlights all registry-type nodes involved in the incident.

- **Element Relevance:** You can also filter elements by their importance inside the incident.
 - ● **Neutral node:** Elements with no direct impact in the security incident.
 - ● **Important node:** Elements with relevant role in the security incident.
 - ● **Origin node:** Entry point of the attack inside the network.
 - ● **Suspicious node:** Elements with suspicious behavior, directly involved in the security incident.
 - ● **Malicious node:** Elements that caused damage to your network.

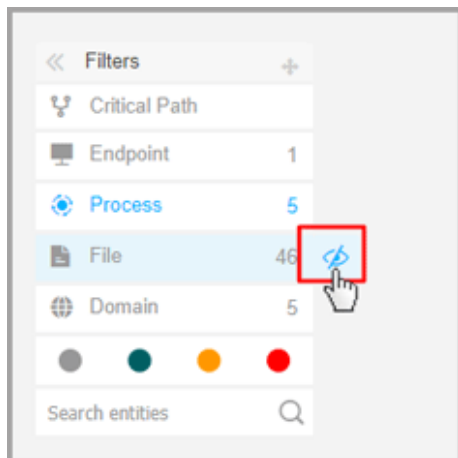
**Note**

Hovering over any of the color filters displays how many elements with same relevance are involved in the incident.

- **Search entities:** You can search names or file extensions of incident components in the search field and the results will be displayed in the side panel.

If no filters are selected, the incident graph is reset to its default state, with endpoint, origin and trigger elements highlighted, while the other elements are faded out.

You can also hide certain elements from the incident graph by clicking the **Show/Hide** button displayed when positioning the mouse over filters of the type: File, Domain, and Registry.



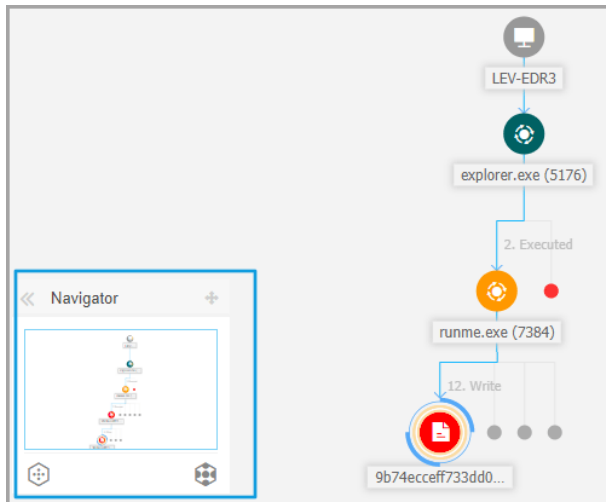
Hiding an element type redraws the incident graph by removing all corresponding elements, even if they are zoomed out, excepting the trigger node and nodes with child elements.

Navigator

The **Navigator** enables you to quickly move through the incident graph and explore all displayed elements by using the mini-map and the different levels of visualization.

Click and hold the **+ Drag** icon to position the floating Navigator panel anywhere inside the incident graph.

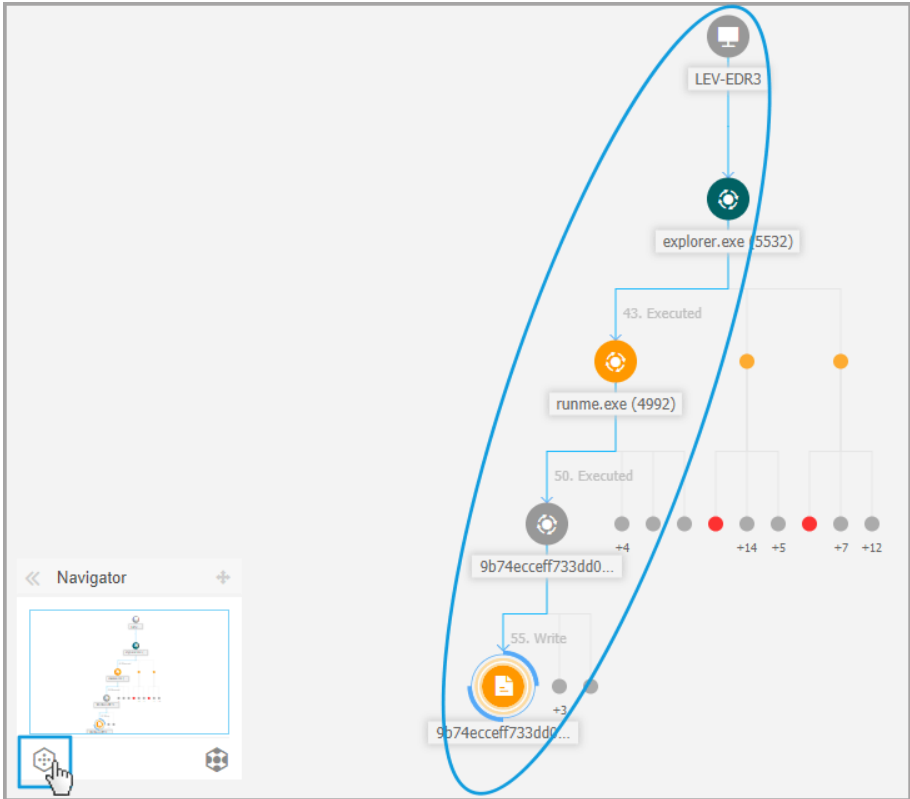
The **Navigator** is collapsed by default. When expanding it, the menu will display the miniaturized version of the entire incident map, and action buttons to adjust the level of visualization.



Navigator

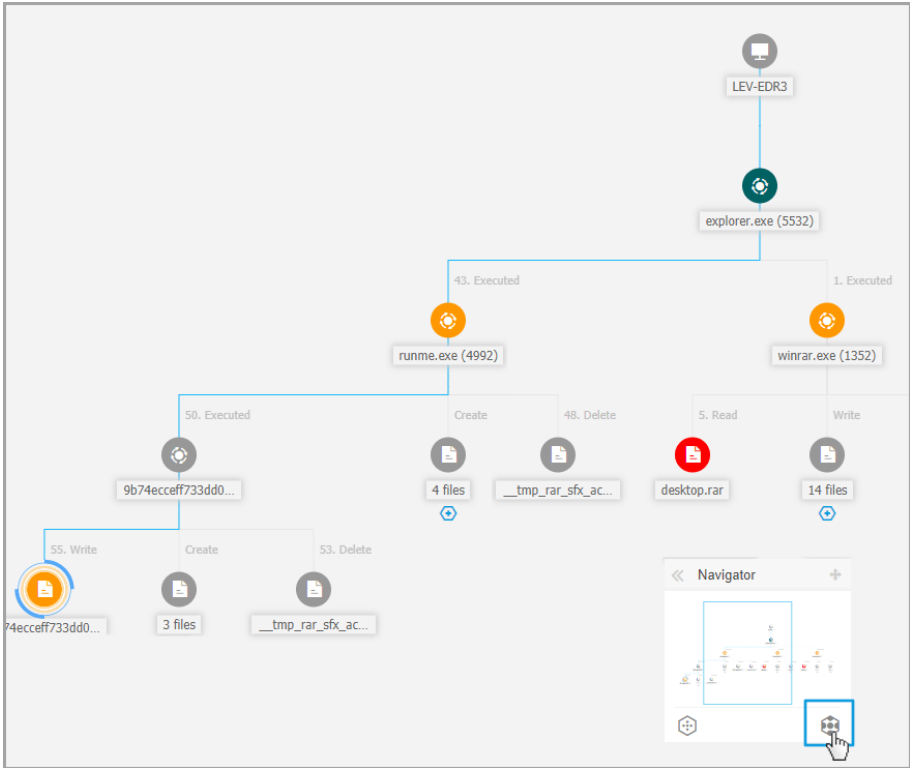
The **Navigator** menu provides two action buttons to adjust how you visualize the incident graph, the **Fewer Details** button, and **More Details** button.

When you click the **Fewer Details** button, the graph is set to its default state, highlighting only the critical path of the incident.



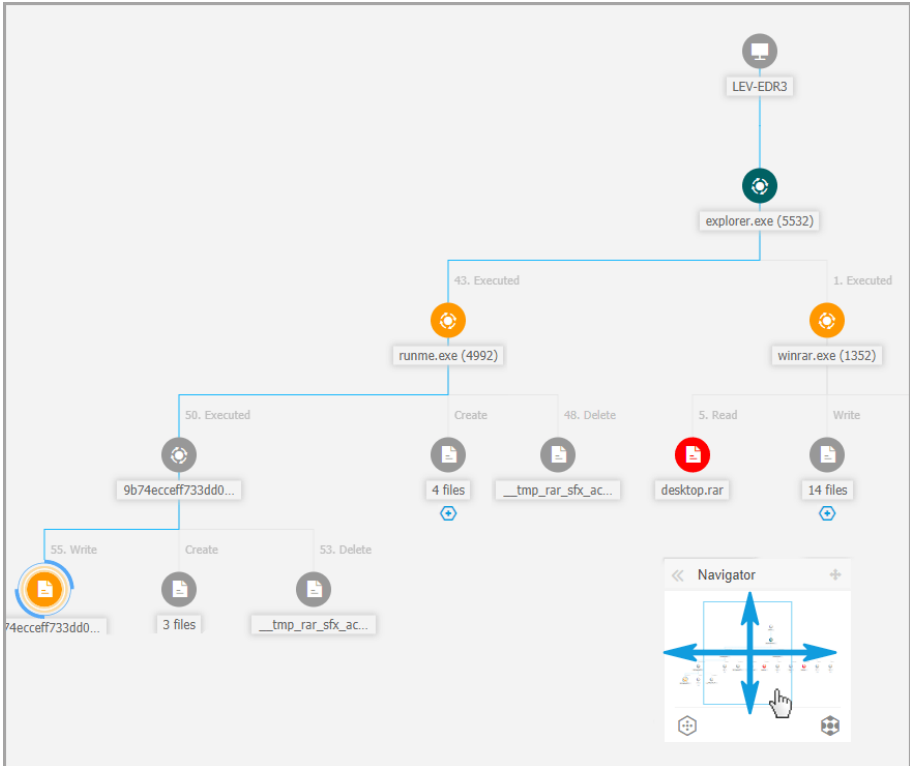
Overview Visualization

When you click the **More Details** button, all the incident graph elements are expanded, highlighting every node and node clusters.



Zoomed-in Visualization

When the incident is zoomed-in and all elements are highlighted the graph may often expand beyond screen limits. In this case hold and drag the map selector within the navigator mini-map to easily slide to the desired incident map area, or simply drag the graph area to the desired direction.



Mini-map Selector

Node Details

The **Node Details** panel includes sections with detailed information of the selected node, including preventive or remediation actions you can take to mitigate the incident, details on the type of detection and alerts detected on the node, network presence, process execution details, additional recommendations to manage the security event, or actions to further investigate the element.

To view this information and take actions within the panel, select a node within the security event map.



Node Details Panel

1. You can collapse or expand the **Node Details** panel by clicking the **Collapse** button.
2. You can easily navigate the information displayed in the **Node Details** panel by clicking the icons of each of the four major categories:
 - **ALERTS**
 This section displays one or multiple detections triggered on the selected node, including details about the Bitdefender technology that included the element in the incident, the reason that triggered the detection, detection name, and the date when it has been detected.
 - **INVESTIGATION**
 This section displays date stamps for the initial detection and all the endpoints where this element was spotted.

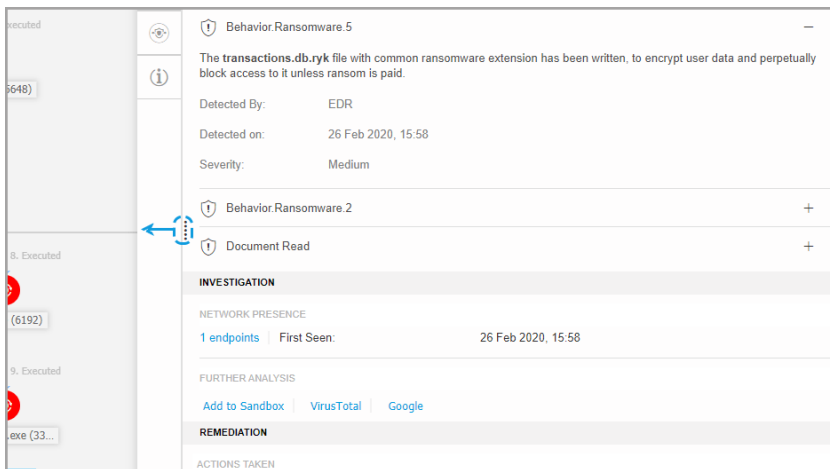
- **REMIEDIATION**

This section displays actions taken automatically by GravityZone, actions you can take immediately to mitigate the threat, as well as detailed recommendations for each alert detected on the selected node to assist you in mitigating the incident and increase the security level of your environment.

- **INFO**

This section displays general information about each file, and specific information depending on the type of node selected.

3. You can drag the **Node Details** panel towards the center of the screen to easily go through its contents.



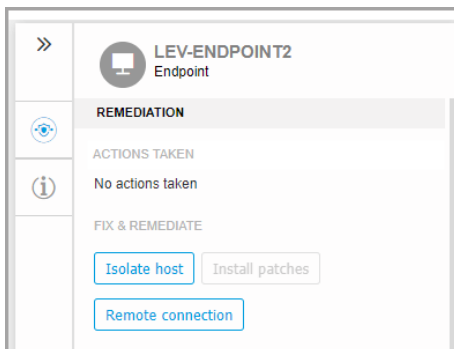
Expanded Panel

Details Panel for Endpoint Nodes

The **Node Details** panel for endpoints includes two categories:

- **REMIEDIATION**

Displays info about the actions taken automatically by GravityZone to mitigate threats and actions you can take:



- **Isolate host** - Use this remediation solution to isolate the endpoint from the network.
- **Install patches** - Use this action to install a missing security patch on the target endpoint. This option is visible only with the Patch Management module, an add-on available with a separate license key. Refer to [Patch Install](#) for more information.
- **Remote Connection** - Use this action to to establish a remote connection to the endpoint involved in the current incident and run a number of custom shell commands directly on its operating system, for mitigating the threat instantly or collecting data for further investigation.

Clicking this button will display the [Remote Connection](#) window.

● DEVICE INFO

Displays general information about the affected endpoint, such as endpoint name, IP address, operating system, pertaining group, state, active policies, and a link that opens a new window where full endpoint details are displayed.

The screenshot displays the 'LEV-ENDPOINT2 Endpoint' details panel. It is organized into sections: 'DEVICE INFO', 'ENDPOINT DETAILS', and 'PATCH INFORMATION'. The 'ENDPOINT DETAILS' section lists various attributes such as FQDN, IP, OS, Infrastructure, Group, State, Last seen, and Active Policy. The 'PATCH INFORMATION' section includes a warning about patch management license availability, last checked status, and patch status.

ENDPOINT DETAILS	
FQDN:	lev-endpoint2
IP:	10.17.44.116
OS:	Windows 10 Pro
Infrastructure:	Computers and Groups
Group:	Custom Groups
State:	Online
Last seen:	Online
Active Policy:	forSandbox

PATCH INFORMATION	
ⓘ Patch Management license not available	
Last Checked:	Never
Patch status:	Unknown ↻

It also provides with information such as the number of installed patches, failed patches, or any missing security and non-security patches. In addition, you can generate an endpoint patch status report. This section is provided on demand for the target endpoint.

You can take the following actions within the panel:

- View patch information for target endpoint. To view patch details, click **Refresh** inside this section.
- View patch status report for target endpoint. To generate the report, click **View endpoint patch status report**.

Details Panel for Process Nodes

The **Node Details** panel for process nodes includes four categories:



- **ALERTS**

Displays one or multiple detections triggered on the selected node, including details about the Bitdefender technology that included this entity in the incident, the reason that triggered the detection, detection name, and the date when it has been detected. The description for each alert follows the latest MITRE standards.

»

acro32.exe
Process Execution

4

ALERTS

PROCESS DETECTED AS **MALWARE** BY ANALYSIS

Gen:Illusion.Slingshot.PowerShell.10.2010 — 100

HyperDetect has detected unwanted activity in your system, caused by this file.

Detected By: Hyper detect

Detection Level: Normal

Detected on: 26 Feb 2020, 15:58

Severity: High

⋮

- Behavior.Ransomware.5 +
- Behavior.Ransomware.2 +
- Document Read +

- **INVESTIGATION**

Displays date stamps for the initial detection and all the endpoints where this element was spotted.



The screenshot shows a sidebar on the left with navigation icons. The main content area displays the following information:

- Process Execution:** **acro32.exe** (with a red circular icon)
- INVESTIGATION:** NETWORK PRESENCE
- 1 endpoints** | First Seen: 26 Feb 2020, 15:58
- FURTHER ANALYSIS:** Add to Sandbox | VirusTotal | Google

To view this list, click the number shown in the **endpoints** field and a new window will pop up.

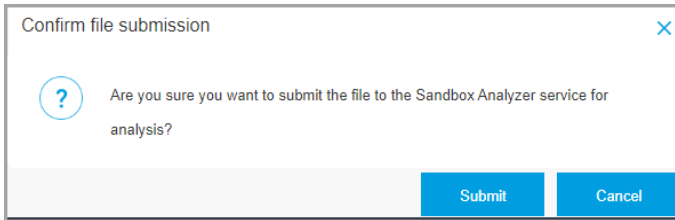
The 'Endpoints' window displays the following details:

- File Name: 9b74ecccff733dd080c75355b7852076.doc.orig
- Table with columns: Endpoint, File Name, Path, First Seen
- Table entry: LEV-EDR3 | 9b74ecccff733dd080c75355b78... | c:\users\admin\desktop\9b74ec... | 28 August 2019, 13:31:38
- Page navigation: First Page | Page 1 of 1 | Last Page | 20 | 1 items
- OK button

This section also provides external analysis through internal components and third-party solutions.

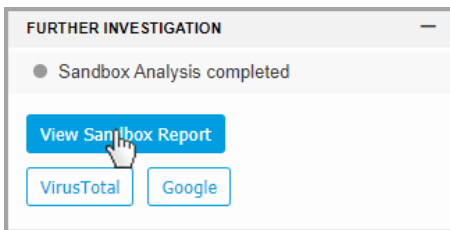
The following actions are available:

- **Add to Sandbox** - Use this action to generate a Sandbox Analyzer report. Choosing **Add to Sandbox** prompts you with a screen to confirm file submission.



After confirmation, you are automatically redirected to the submission screen.

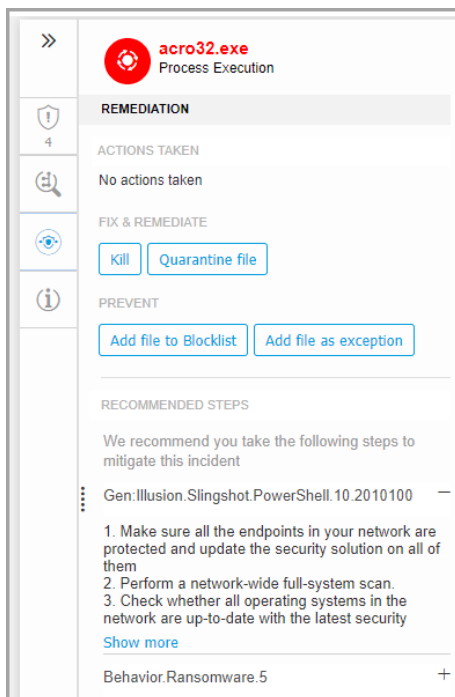
When the analysis is completed, click the **View Sandbox Report** button to open the full report.



- **VirusTotal** - Use this action to submit a file externally for analysis.
- **Google** - Use this action to search the hash value of a file.

- **REMIEDIATION**

Displays info about the actions taken automatically by GravityZone to mitigate threats and actions you can take:

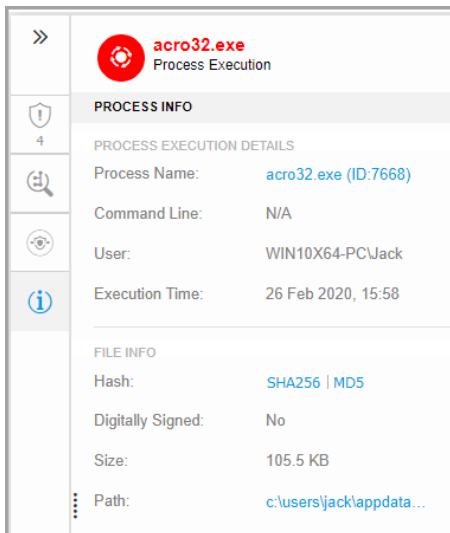


- **Kill** - Use this action to stop a process execution. This action creates a kill process task visible in the process execution bar. `System32` and Bitdefender processes are excluded from this action.
- **Quarantine file** - Use this action to store the item in question and prevent it from executing its payload. This action requires the Firewall module to be installed on the target endpoint.
- **Add file to Blocklist** - Manage blocked items in the [Blocklist](#) section.
- **Add file as Exception** - Use this option to exclude legitimate activity on a specific policy. When you choose this action, a configuration window prompts you to select the policy where you want to add an exception. Manage exclusion under **Policies > Antimalware > Settings**.

It also provides detailed recommendations for each alert detected on the selected node to assist you in mitigating the incident and increase the security level of your environment.

- **PROCESS INFO**

Displays details about the selected process node, including process name, executed command line, user, time of execution, file origin and path, hash value, or digital signature.



The screenshot displays a details panel for a process named 'acro32.exe'. The panel is organized into several sections:

- Process Execution:** Shows the process name 'acro32.exe' and its ID 'ID:7668'.
- PROCESS INFO:** A header section for the process details.
- PROCESS EXECUTION DETAILS:** A section containing:
 - Process Name:** acro32.exe (ID:7668)
 - Command Line:** N/A
 - User:** WIN10X64-PC\Jack
 - Execution Time:** 26 Feb 2020, 15:58
- FILE INFO:** A section containing:
 - Hash:** SHA256 | MD5
 - Digitally Signed:** No
 - Size:** 105.5 KB
 - Path:** c:\users\jack\appdata...

You can copy the hash value to clipboard by clicking the available hashing algorithms within the **Hash** field and then **Copy to Clipboard**, and use it to add a file hash value to **Blocklist**. For more information, refer to [Blocklisting Files](#).

Details Panel for File Nodes

The **Node Details** panel for file nodes includes four categories:

- **ALERTS**

Displays one or multiple detections triggered on the selected node, including details about the Bitdefender technology that included this entity in the incident, the reason that triggered the detection, detection name, and the date when it

has been detected. The description for each alert follows the latest MITRE standards.

The screenshot shows the alert details for a file named 'cv.docm'. It includes an 'ALERTS' section with a count of 1, a description 'FILE DETECTED AS MALWARE BY ANALYSIS', and a specific detection by 'Proton.VB.Vexillum.1.419.3000001'. A detailed description states: 'HyperDetect has detected unwanted activity in your system, caused by this file.' Below this, a table lists the detection details:

Detected By:	Hyper detect
Detection Level:	Aggressive
Detected on:	26 Feb 2020, 15:58
Severity:	High

- **INVESTIGATION**

Displays date stamps for the initial detection and all the endpoints where this element was spotted.

The screenshot shows the investigation details for the file 'cv.docm'. It features an 'INVESTIGATION' section with a count of 1. Under 'NETWORK PRESENCE', it shows '1 endpoints' and 'First Seen: 26 Feb 2020, 15:58'. The 'FURTHER ANALYSIS' section contains links for 'Add to Sandbox', 'VirusTotal', and 'Google'.

To view this list, click the number shown in the **endpoints** field and a new window will pop up.

Endpoint	File Name	Path	First Seen
LEV-EDR3	9b74ecceff733dd080c75355b78...	c:(users\admin)\desktop\9b74ec...	28 August 2019, 13:31:38

This section also provides external analysis through internal components and third-party solutions.

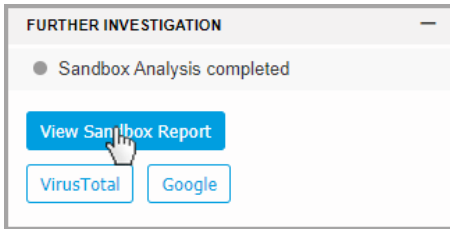
The following actions are available:

- **Add to Sandbox** - Use this action to generate a Sandbox Analyzer report. Choosing **Add to Sandbox** prompts you with a screen to confirm file submission.

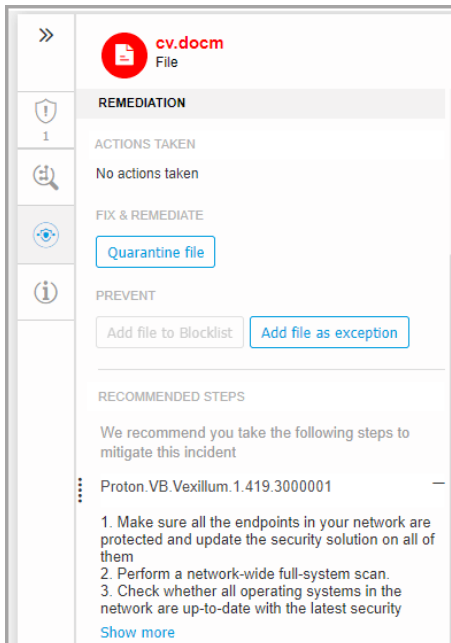
Are you sure you want to submit the file to the Sandbox Analyzer service for analysis?

After confirmation, you are automatically redirected to the submission screen.

When the analysis is completed, click the **View Sandbox Report** button to open the full report.



- **VirusTotal** - Use this action to submit a file externally for analysis.
- **Google** - Use this action to search the hash value of a file.
- **REMIEDIATION**
Displays info about the actions taken automatically by GravityZone to mitigate threats and actions you can take:

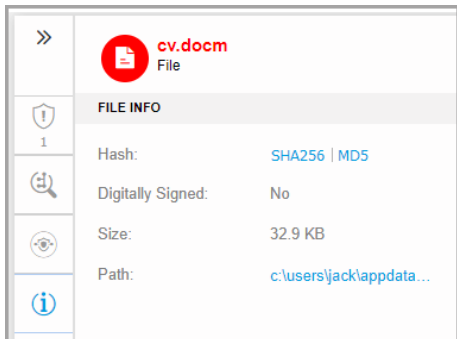


- **Quarantine file** - Use this action to store the item in question and prevent it from executing its payload. This action requires the Firewall module to be installed on the target endpoint.
- **Add file to Blocklist** - Manage blocked items in the [Blocklist](#) section.
- **Add file as Exception** - Use this option to exclude legitimate activity on a specific policy. When you choose this action, a configuration window prompts you to select the policy where you want to add an exception. Manage exclusion under **Policies > Antimalware > Settings**.

It also provides detailed recommendations for each alert detected on the selected node to assist you in mitigating the incident and increase the security level of your environment.

● FILE INFO

Displays details about the selected file node, including file origin and path, hash value, or digital signature.



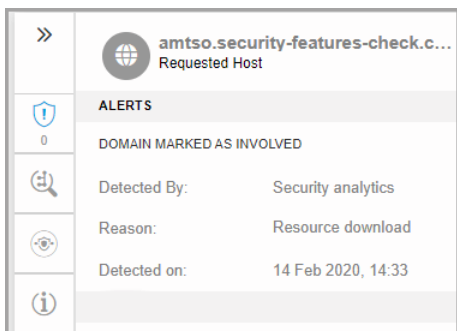
You can copy the hash value to clipboard by clicking the available hashing algorithms within the **Hash** field and then **Copy to Clipboard**, and use it to add a file hash value to **Blocklist**. For more information, refer to [Blocklisting Files](#).

Details Panel for Domain Nodes

The **Node Details** panel for domain nodes includes four categories:

- **ALERTS**

Displays the severity of the domain as marked by the Bitdefender technology that included this entity in the incident, the reason that triggered the detection, and the date when it has been detected.



- **INVESTIGATION**



Displays date stamps for the initial detection and all the endpoints where this element was spotted.

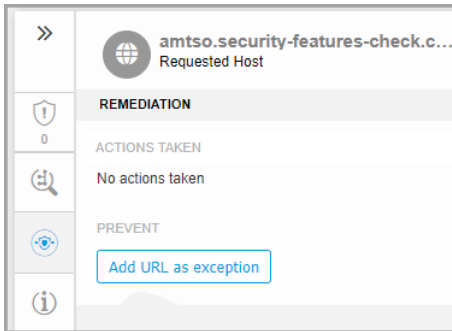
The screenshot shows a sidebar with navigation icons and a main panel. The main panel displays a globe icon, the text "amtso.security-features-check.c...", and "Requested Host". Below this is a section titled "INVESTIGATION" with a shield icon and a "0" count. Underneath is "NETWORK ACTIVITY" with a magnifying glass icon and the text "6 endpoints | First Seen: 28 Aug 2019, 16:30".

To view this list, click the number shown in the **endpoints** field and a new window will pop up.

The "Endpoints" window has a title bar with a close button. Below the title bar, it shows "File Name: 9b74ecceff733dd080c75355b7852076.doc.orig". A table follows with columns: "Endpoint", "File Name", "Path", and "First Seen". The table contains one row: "LEV-EDR3", "9b74ecceff733dd080c75355b78...", "c:\users\admin\desktop\9b74ec...", and "28 August 2019, 13:31:38". Below the table is a pagination bar: "First Page", "Page 1 of 1", "Last Page 20", and "1 items". An "OK" button is in the bottom right corner.

- **REMIEDIATION**

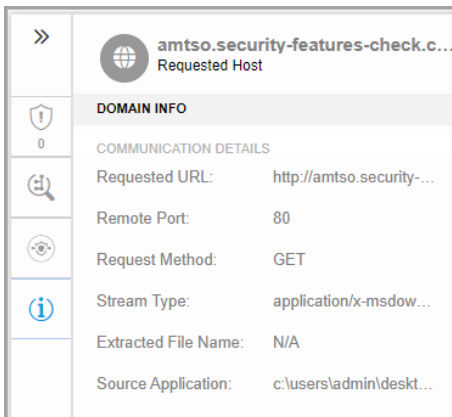
Displays info about the actions taken automatically by GravityZone to mitigate threats and actions you can take:



- **Add URL as Exception** - Use this option to exclude legitimate activity on a specific policy. When you choose this action, a configuration window prompts you to select the policy where you want to add an exception. Manage exclusion under **Policies > Antimalware > Settings**.

- **DOMAIN INFO**

Displays details about the selected domain node, including requested URL, port used, request method, stream type, extracted file name, source application.



Details Panel for Registry Nodes

The **Node Details** panel for registry nodes includes three categories:

- **ALERTS**

Displays the severity of the registry manipulation as marked by the Bitdefender technology that included this entity in the incident, the reason that triggered the detection, the date when it has been detected, and registry type.

>>	<p>POC-To-Delete Registry</p>
 0	ALERTS
<p>REGISTRY DETECTED AS IMPORTANT BY ANALYSIS</p>	
	<p>Detected By: Security analytics</p>
	<p>Reason: Registry write</p>
	<p>Detected on: 14 Feb 2020, 14:33</p>
	<p>Registry Type: Startup or Autorun</p>

- **REMIEDIATION**

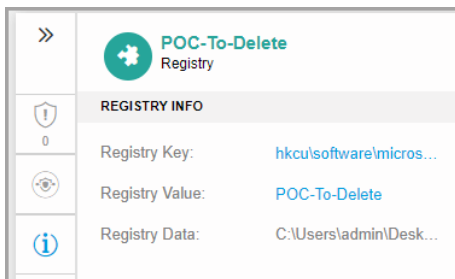
Displays info about the actions taken automatically by GravityZone.

>>	<p>POC-To-Delete Registry</p>
 0	REMIEDIATION
<p>ACTIONS TAKEN</p>	
	<p>No actions taken</p>

The **REMIEDIATION** section for registry nodes does not provide any user action option.

- **REGISTRY INFO**

Displays details about the selected registry node, including registry key, value and data.



You can click the registry key and value to copy it to clipboard for further analysis purposes.

Events

Use the **Events** tab to view how the sequence of events unfolded into triggering the currently investigated incident. This window displays the correlated system events and alerts detected by GravityZone technologies such as EDR, Network Attack Defense, Anomaly Detection, Advanced Anti-Exploit, Windows Antimalware Scan Interface (AMSI).

Every complex event has a detailed description explaining what was detected and what might happen if the artifact is used for malicious purposes, in accordance with the latest MITRE techniques and tactics.

Events Tab

1. Use the filtering options to display all events, or either only system events or complex events (alerts).
2. Click the **More details** button to expand each event and have access to additional information.

Incident Info

This panel contains collapsible sections with details like incident ID, current state, time and date when it was created and last updated, number of involved artifacts, trigger name and attack info.



The screenshot displays the Bitdefender GravityZone interface for incident #901. The top navigation bar includes 'Back', 'Reported', 'Date: 25 Feb 2020', 'Status: Open', and 'Endpoint: LEV-ENDPOINT2'. The main area shows a flowchart of the incident's execution path: LEV-ENDPOINT2 (computer icon) -> explorer.exe (5700) (green gear icon) -> poc_ctc_gambit.ex... (red gear icon) -> powershell.exe (35...) (orange gear icon) -> user.exe (7368) (red gear icon). The 'user.exe (7368)' node is highlighted with a red circle. The right-hand 'INCIDENT DETAILS' panel shows: Incident ID: #901, Status: Open, Created On: 25 Feb 2020, 13:23:57, Last Updated on: 25 Feb 2020, 13:23:57, Endpoint: LEV-ENDPOINT2, Artifacts Involved: 26. The 'DETECTION' section lists: Confidence Score: 90, Incident Trigger: user.exe(PID:7368), ATC.Malicious, and a note: 'Advanced Threat Control has labeled user.exe as a potential threat to your system.' It also shows 'Detected By: ATC', 'Detected on: 25 Feb 2020, 13:23', and 'Severity: High'. The 'ATTACK INFO' section shows 'Attack Type: Other'.

Incidents Info Panel

The panel also includes the alerts detected on the element that triggered the incident.

Remediation

The **Remediation** panel provides you insightful information about what corrective actions were taken automatically by GravityZone in case of attacks blocked by technologies such as Advanced Threat Control (ATC), HyperDetect, Antimalware, as well as recommended steps you may follow in order to mitigate the incident and to increase the security level of your system.



The screenshot displays the Bitdefender GravityZone interface. On the left, a process graph shows the execution flow: LEV-EDR3 (grey) → explorer.exe (5532) (green) → runme.exe (4992) (orange) → 9b74ecceff733dd0... (grey) → 9b74ecceff733dd0... (orange). The graph includes event details like '43. Executed' and '50. Executed'. On the right, the 'Remediation' panel is open, showing '6 actions taken' and a list of 'ACTIONS TAKEN AUTOMATICALLY' (Deleted File, Deleted Registry Value) and 'RECOMMENDED STEPS' (ScreenCaptureModuleLoaded, Suspicious File Drop). Two blue arrows labeled '1' and '2' point to the automatic actions and recommended steps respectively.

Remediation Panel

1. Actions taken automatically by GravityZone.
2. Recommendations to further mitigate the incident and boost security.



Note

The recommended steps correspond to the alerts detected on the node that triggered the investigated incident.

Notes

The **Notes** section allows you to add a note for tracking recent changes and ease incident ownership change.

Notes Clipboard

1. To leave a note for the current event, click the **Notes** button to display a new window.
2. Enter your message in this window (maximum 1024 characters).

Incident Status Bar

The incident status bar provides security event tags that can help you detect key information about the involved network endpoints.

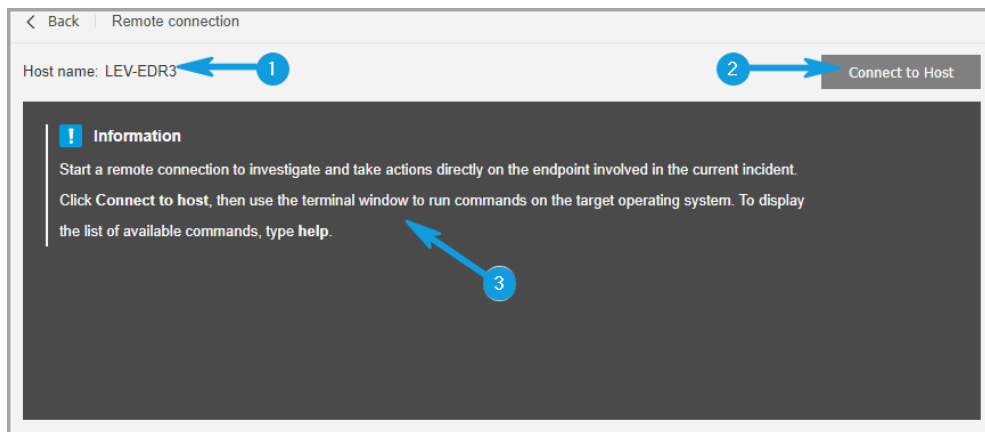
Incident Status Bar

1. Incident ID - the id number of the incident under investigation and if the incident is either blocked or reported only.
2. Detection timestamp - the date and time the incident was triggered.
3. Incident status - the current incident status.
4. Incident Trigger - the name of the element that generated the incident.
5. Endpoint - the name of the target endpoint.

Clicking the **Back** button takes you back to the main **Incidents** page.

Remote Connection

Use this tab to establish a remote connection to the endpoint involved in the current incident and run a number of custom shell commands directly on its operating system, for cancelling the threat instantly or collecting data for further investigation.



Remote Connection tab

The **Remote Connection** tab contains the following items:

1. The name of the endpoint involved in the current security event
2. The button controlling the remote connection (connect / disconnect)
3. The terminal window

Terminal Session Prerequisites

- The version of Bitdefender agent installed on the endpoint supports the Remote Connection feature.
- The endpoint must be powered-on and online.
- The endpoint must have Windows OS.
- GravityZone is able to communicate with the endpoint.
- Your GravityZone account must have manage permissions for the target endpoint.

Creating a Remote Connection

This is how the remote connection works:

1. Start the live session by clicking the **Connect to Host** button.
The connection status will be displayed next to the endpoint name.

If the connection fails, an error message will be displayed in the terminal window.



Note

You can open maximum five terminal session with the same endpoint simultaneously.

2. Once connected, the terminal displays the list of available commands and their description. Type the command that you want in the terminal window followed by `Enter`.

To learn more about a command, type `help` followed by the command name (for example, `help ps`).

3. The terminal displays the command output, when the command is successful. If the endpoint fails to complete the command execution, the command will be discarded.

The command history is logged in the terminal window. However, you can view the previously typed commands by pressing the arrow keys.

4. To end the connection, click the **End Session** button.

The terminal session expires automatically after five minutes of inactivity.

By navigating outside the **Remote Connection** tab while connected to an endpoint will also end the terminal session.

Terminal Session Commands

EDR terminal session commands are custom-built shell commands, platform independent, using a generic syntax. Find hereinafter the list of available commands you can use on endpoints through the terminal session:

- `ps`
 - **Description:** Displays information about the current running processes on the target endpoint, such as process ID (PID), name, path or memory usage.
 - **Syntax:** `ps`
 - **Aliases:** `tasklist`
 - **Parameters:** -
- `kill`

- **Description:** Terminates a running process or application on the target endpoint by its PID. Use the `ps/tasklist` command to obtain the PID.
- **Syntax:** `kill [PID]`
- **Aliases:** -
- **Parameters:** `[PID]` - the ID of a process from the target endpoint.
- `ls (dir)`
 - **Description:** Displays information about all files and folders from the specified directory, such as name, type, size and modify date. Allows wildcards to specify the path. For example:
 - `C:\Users\admin\Desktop\s*` all contents of Desktop folder starting with "s"
 - `C:\Users\publ??` lists all contents of specified path, with any last two letters.
 - **Syntax:** `ls [path]`
 - **Aliases:** `dir`
 - **Parameters:** `[Path]` - the path to a file or folder on the target endpoint.
- `rm (del, delete)`
 - **Description:** Deletes files and folders from the specified path on the target endpoint.
 - **Syntax:** `rm [path]`
 - **Aliases:** `del/delete`
 - **Parameters:** `[Path]` - the path to a file or folder on the target endpoint.
- `reg query`
 - **Description:** Returns all information (name, type and value) for the specified registry key path.
 - **Syntax:** `reg query [keypath] [/k] [keyname] [/v] [valuename]`
 - **Aliases:** -
 - **Parameters:** -

- `keypath`- returns all registry keys information from the specified path.
- `/k [keyname]` - filters the registry keys results by a specific key name. You can also use wildcards (*, ?) to filter for a wider range of names.
- `/v [valuename]` - filters the registry values by a specific value name. You can also use wildcards (*, ?) in the value name to filter a wider range of names.

- `reg add`
 - **Description:** Adds a new registry key or value. Overwrites a registry value, if it already exists. When overwriting registry information, you must specify all defined parameters.
 - **Syntax:** `reg add [keyname] [/v] [valuename] [/t] [datatype] [/d] [data]`
 - **Aliases:** -
 - **Parameters:**
 - `[keyname]` - the registry key name.
 - `/v [valuename]` - the registry value name. It also require adding at least `/d [data]` parameter.
 - `/t [datatype]` - the registry value data type. You can add one of the following data types:
`REG_SZ, REG_MULTI_SZ, REG_DWORD, REG_BINARY,`
`REG_DWORD_LITTLE_ENDIAN, REG_LINK,`
`REG_FULL_RESOURCE_DESCRIPTOR, REG_EXPAND_SZ`
When unspecified, the `REG_SZ` type is assigned by default.
When the type is set to `REG_BINARY`, registry data are interpreted as hex values.

- `reg delete`
 - **Description:** Deletes a registry key or its values.
 - **Syntax:**
`reg delete [keyname] [/v] [valuename]`

```
reg delete [keyname] [/va]
```

– **Aliases:** -

– **Parameters:**

[keyname] - deletes the registry key and all its values.

/v [valuename] - deletes the specified registry value.

/va - deletes all values of the specified registry key.

- cd

– **Description:** Changes the working directory to the specified path. This command requires, as parameter, the path to a drive or folder from the target endpoint.

– **Syntax:** cd [path]

– **Aliases:** -

– **Parameters:** [Path] - the path to a file or folder on the target endpoint.

- help

– **Description:** Without specifying a parameter, help lists all available commands along with a short description. When entering help followed by a parameter, it displays the complete syntax of that command, short description and usage example.

– **Syntax:** help [command]

– **Aliases:** -

– **Parameters:** command name (for example: cd, kill, ls, ps)

- clear (cls)

– **Description:** Clears up the terminal window and displays prompt with the current working folder.

– **Syntax:** clear

– **Aliases:** cls

– **Parameters:** -

6.2. Blocklisting Files

In the **Blocklist** page you can view and manage items by their hash values. View activity records in [User Activity Log](#).

Type	File Hash	Source Type	Source Info	File Name
<input type="checkbox"/> MD5	77e864a40d175cbd380c7185b2f9026c	Incident	#6	user.exe
<input type="checkbox"/> SHA256	c893b6baef3610e9812317f4411ea6df29afb718cf22d583a...	Incident	#6	user.exe

Blocklist page

In a data table, you can view the following details for each item:

- File type:
 - MD5
 - SHA256
- File Hash Value
- Source Type:
 - Incident
 - Import
 - Manual
- Source Info
- File Name
- Company

Add hash values to the existing Blocklist:

1. Copy the hash value from [File Info](#).



2. Choose from **MD5** or **SHA256** and paste the value in the box below.
Add a note if required.
3. Click **Save**.

Add hash value window



Important

Incidents Sensor will block any binary whose hash value has been added to **Blocklist** from starting a process.

Import hash records to the existing Blocklist. To import a CSV file:

1. Click **Import CSV**.
2. Browse for your CSV file and click **Save**.

Import CSV window

You may also import local CSV files from your device into the **Blocklist** page, but first you must make sure your CSV is valid.

To create a valid CSV file for import you must populate the first three columns with the following data:

1. The first column of the CSV must contain the Hash type: either `md5` or `sha256`.
2. The second column must contain corresponding hexadecimal hash values.
3. The third column may contain optional string information related to the **Source Info** column in the **Blocklist** page.



Note

Information corresponding to the other columns in the **Blocklist** page will be filled in automatically, upon [importing the CSV file](#).

6.3. Searching Security Events

The **Search** page allows you to go through past events based on complex criteria.

Search page overview

To view the events you are interested in, you must build queries using the query language available in GravityZone.

The **Search** page provides the following options:

- A [search bar for entering queries](#), displaying the list of query terms by categories when clicked, and an autocomplete assistant.
- [Saving favorite searches](#) for later use.
-
- A **Get Started** section with a link to the [query language Syntax Help](#).
- [Predefined queries](#), designed for useful security event search cases.

6.3.1. The Query Language

The query language provides the vocabulary (fields and operators) and the syntax with which you can build queries. You can find them described herein.

Click the **Syntax Help** link and select the **Query Language** tab to view its contents.

Fields

The query field is the same with the field in GravityZone database. Fields stand for entities such as file paths, file hashes, hostnames, or domain names.

Any field may have one or more values, representing the state of the field at a specific time. Values are of different types of data, depending on the meaning of the field.

Operators

Operators allow you to create relationships between fields to build searching criteria. You can use the following operators:

Operator	Example	Description
:	fieldCategory.option: value1	Compares the query field value with values of the same field in the database.
" "	fieldCategory.option: "value1 value2"	Strings enclosed in quotation marks are treated together, as a phrase.
()	fieldCategory1.option: value1 AND (fieldCategory2.option: value2 OR	Groups query terms.

Operator	Example	Description
	<code>fieldCategory3.option: value3)</code>	
AND	<code>fieldCategory1.option: value1 AND fieldCategory2.option: value2</code>	Retrieves results that match all your query conditions.
OR	<code>fieldCategory1.option: value1 OR fieldCategory2.option: value2</code>	Retrieves results that match any of your query conditions.
AND NOT	<code>fieldCategory1.option: value1 AND NOT fieldCategory2.option: value2</code>	This operator is useful in complex queries and returns results not matching the specified term, apart from all the other conditions.
<code>_exists_</code>	<code>_exists_ fieldCategory.option</code>	Returns results that contain the specified field.
-	<code>fieldCategory.option: -value</code>	Use the minus sign (-) when the value must be excluded from the results.
?	<code>fieldCategory.option: ??_file.path</code>	Use a question mark (?) to match any single character in your field value.
*	<code>fieldCategory.option: file.*</code>	Use an asterisk (*) to match any field value.

Query Syntax

A query is a logical condition, or a series of conditions bound by operators, which have as results events from the EDR database.

All conditions must relate to fields. Some conditions require you to provide a value, while others not. For example, you don't need a value when you only ask if the field exists in the event details.

Queries may be from simple to complex. Complex queries may have nested queries (query in another query).

A valid field syntax consists of the field category followed by one of options in the **Query Language** section, and its corresponding value: `fieldCategory.option:value`.

For example, `file.path: "%system32%\com\svchost.exe"` is a rather simple query that searches all events that include `%system32%\com\svchost.exe`, and it consists in:

- A mandatory field category and related option (separated by a period):
`file.path`
- An operator: the colon (:) - to compare the field's value
- The searched value: `%system32%\com\svchost.exe`
- Quotation marks (" "), because the value contains special characters such as `<\>` and `<.>`

6.3.2. Running Queries

To run a query:

1. Type the query string in the field.

Clicking the **Search** field will display the list of search terms grouped by category. Select the term that you want to start creating your query.

As you type, Control Center assists you with autocomplete suggestions. Use the arrow keys to select a suggested option and then press **Enter** to add it to the query.

If you need more help, click the **Syntax Help** link.



Note

You can use nested queries to build complex searches.

2. To filter the events within a time frame, click the time field. You have several options to define it:
 - Only specific date.
Select a date in the **From** tab of the calendar.

- An exact time interval.
 - a. Select the start date in the **From** tab of the calendar.
 - b. Select the end date in the **To** tab.
 - A recent time interval from the available options.
 - Click **OK**.
3. Click **Search**, or press **Enter**.

You can view the matching events, together with their details, below your query.



Important

When you search the `detections.detection_type` query in the *Search* field, Control Center requires you complete it with an integer value ranging from 1 to 15 (i.e `detections.detection_type:1`).

Each value you put in corresponds to a certain detection type, as follows:

- a. `detections.detection_type:1` - Advanced Threat Control detection
- b. `detections.detection_type:2` - Antimalware static engines detection
- c. `detections.detection_type:3` - HyperDetect detection
- d. `detections.detection_type:4` - Advanced Threat Control suspicious event notification
- e. `detections.detection_type:5` - HyperDetect reported attack types detection
- f. `detections.detection_type:6` - Antimalware CMDLine Scanner detection
- g. `detections.detection_type:7` - Cross Technologies Correlation detection
- h. `detections.detection_name:8` - Network Attack Defense detection
- i. `detections.detection_type:9` - HyperDetect unreported attack types detection
- j. `detections.detection_type:10` - Sandbox Analyzer contained dynamic analysis detection
- k. `detections.detection_type:11` - Memory Buffer Register Scan detection
- l. `detections.detection_type:12` - URL detection

- m. `detections.detection_type:13` - Advanced Anti-Exploit detection
- n. `detections.detection_type:14` - User Behavior Analysis detection
- o. `detections.detection_type:15` - Antimalware Scan Interface detection

Control Center can display up to 10,000 events. If the query results contain more than 10,000 events, a message will appear on the screen. In this case, you need to refine your search.

6.3.3. Favourite Searches

As most queries are long, some are even hard to build or to remember. Instead of saving them into a file and copy-pasting them in GravityZone, you can save them directly in GravityZone, to have them at hand.

To save your query:

1. Enter the string in the **Search** field.
2. Click the ☆ icon at the right-end of the **Search** field.
3. When prompted to name it, type the name you want for your query.
4. Click **Add**.

Click the **Favourite Searches** link under the **Query** field to view your saved queries.

Further on, you have three options:

- Run the query.
- Edit the query name.
- Delete the query.

To run a saved query:

1. Click the **Favourite Searches** link.
2. Select your preferred query.

The saved string will be added to the **Search** field.





Note

If needed, edit the query string. Additionally, you can save the new search query to your Favourite Searches.

3. Use the company and calendar filters to refine the search.
4. Click **Search**.

When your list of queries needs adjustments, place the mouse over the saved query to reveal the inline options.


- Click the  **Edit** icon to rename the query.
- Click the  **Delete** icon if you no longer need the query.

6.3.4. Predefined queries

The **Search** page provides a few example of complex query searches, specific to security events investigations.

Predefined queries are grouped by security investigation category.

To launch a predefined query:

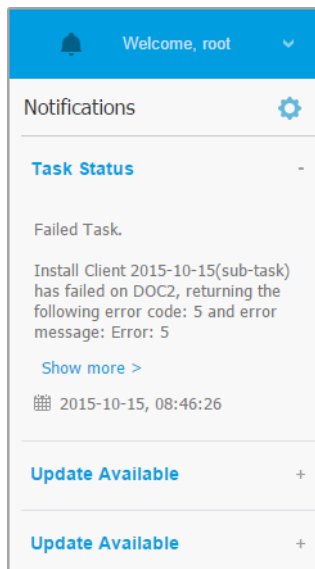
- Click the  icon next to the predefined query description.
- The query phrase will appear automatically in the **Search** bar. Fill in the specific details for the query terms.
- Click the **Search** button to run the query.

Note


You can anytime return to the **Get Started** options from the **Search** page, by clicking the **Get Started** link at the top-right side of the page.

7. 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  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.

7.1. 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.

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. 89).

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.


Missing Patch Issue

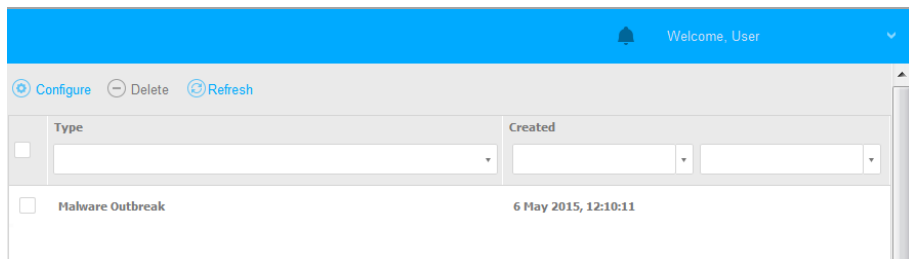
This notification occurs when endpoints in your network are missing one or more available patches.

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.

7.2. 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.

7.3. 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. 89).

7.4. 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




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. 86). 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.
- **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 **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**.

8. USING REPORTS

Control Center 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 effortlessly 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).

8.1. Report Types

Different report types are available for each endpoint type:

- [Computer and Virtual Machine Reports](#)
- [Exchange Reports](#)

8.1.1. 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, Advanced Anti-Exploit and ATC/IDS. 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.
- Company name.

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.

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



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.



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.



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.

Monthly License Usage

Click the numbers in each column to view details regarding each module and add-on available. You can easily customize the report by clicking the **Show/Hide Columns** button.

Email Security - Monthly License Usage

This report provides license usage for the Email Security service. All report intervals retrieve license usage information until the end of the previous day. For example, you generate a report on Monday, at 12 pm and set the interval

to **This month**. The report will provide license usage information until the end of Sunday.

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:

- Available protection layers
- Managed and unmanaged endpoints
- License type and status (additional license related columns are hidden by default)
- Infection status
- 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 [???](#).

- Threat type, such as adware, rootkit, downloader, exploit, host-modifier, malicious tools, password stealer, ransomware, 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
- 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.

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.



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

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.

8.1.2. 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.

8.2. 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. Click the  **Add** button at the upper side of the table. A configuration window is displayed.

Create Report

Details

Type: Antiphishing Activity

Name: * Antiphishing Activity Report

Settings

Now

Scheduled

Reporting Interval: Today

Show: All endpoints

Only endpoints with blocked websites

Delivery: Send by email at

Select Target

- CM

Selected Groups

Company

Generate **Cancel**

Report Options

3. Select the desired report type from the menu. For more information, refer to [“Report Types” \(p. 91\)](#)
4. Enter a suggestive name for the report. When choosing a name, consider the report type and target, and possibly the report options.
5. 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).
6. 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.
 7. 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.

8. **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.
9. **Select Target.** Scroll down to configure the report target. Select one or several groups of endpoints you want to include in the report.
10. 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.

8.3. 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.

8.3.1. 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” \(p. 111\)](#)

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.

8.3.2. 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 and 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 and 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.

8.3.3. 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.

8.4. Taking Report-Based Actions

While most reports only highlight the issues in your network, some of them also offer you several options to fix the issues found with just one click of a button.

To fix the issues displayed in the report, click the appropriate button from the Action Toolbar above the data table.

 **Note** You need **Manage Network** rights to perform these actions.

These are the available options for each report:

Malware Status

- **Scan infected targets.** Runs a preconfigured Full Scan task on the targets showing as still infected.

Update Status

- **Update.** Updates the target clients to their latest available versions.

Upgrade Status

- **Upgrade.** Replaces old endpoint clients with the latest generation of products available.

8.5. 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](#)

8.5.1. 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.

8.5.2. 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.

8.6. 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**.



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.

8.7. Printing Reports

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

9. 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
-

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.

10. GETTING HELP

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

10.1. 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.

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

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.