Bitdefender

GravityZone On-Premises

Table of Contents

1. 2022

1.1. Version 6.30.1-3 (Third-Party Updates)

Release date: 2022.12.21

1.1.1. Resolved Issues

1.1.1.1. GravityZone Platform

- Security fixes.

1.2. Version 6.30.1-3

Release date: 2022.11.28

1.2.1. Resolved Issues

1.2.1.1. GravityZone Platform

- Fixed a few incorrect translations displayed in the GravityZone console.
- Security fixes.

1.3. Version 6.30.1-2

Release date: 2022.11.23

1.3.1. Resolved Issues

1.3.1.1. GravityZone Platform

- The GravityZone console with automatic product updates enabled became unresponsive during the update process of specific third-party software.
- Minor improvements and bug fixes.

1.4. Version 6.30.1-1

Release interval: 2022.11.23 - 2022.12.08

1.4.1. New Features

1.4.1.1. Endpoint Tags

You can now assign security policies to endpoints based on tags, in addition to the existing location and user rules. With this release, you can create, edit, delete, and assign tags manually or automatically.

We updated several areas in GravityZone Control Center to accommodate this feature:

- Endpoint tags are configurable in the new **Network** > **Tags Management** page.

- Tag rules are configurable under the new category **Endpoint Tag Rule** in the **Policies** > **Assignment Rules** page. Consequently, the previous **Tag** category has been renamed **Integration Tag**.
- The **Network** page includes a new button to assign and unassign tags to endpoints, and a new column that allows tag filtering.
- The **Accounts** > **User Activity** page records actions such as create, edit, delete, assign and unassign tags.

Endpoint tags are available with the following GravityZone products, based on yearly payment plans:

- GravityZone Business Security Premium
- GravityZone Business Security Enterprise
- GravityZone Security for Workstations
- GravityZone Security for Servers
- GravityZone Security for Endpoints Physical Workstations*
- GravityZone Security for Endpoints Physical Servers*
- GravityZone Security for Virtualized Environments VDI*
- GravityZone Security for Virtualized Environments VS*
- GravityZone Security for Virtual Environments per CPU*
- GravityZone EDR

* Following the April 2022 business portfolio revision, endpoint tags are available only with new license keys for these products. If you have a license for one of these products purchased before April 2022, you are not able to view and use endpoint tags.

1.4.2. Improvements

1.4.2.1. GravityZone Platform

- You now have visibility over tasks created by other GravityZone users. You cannot take actions on them, but you can sort and filter them by username in the new **Owner** column in the **Tasks** grid.
- Actions taken on your tasks, such as create, edit and delete, are now visible in the **Accounts** > **User Activity** page.
- You can now install the Microsoft Hyper-V Security Server for second generation VM hardware.
- Added support for new password security requirements for Security Server: 8 characters length, one digit, at least one upper case character, at least one lower case character and one special character.

> **Note**
> This requirement will become effective with the next Security Server Multi-Platform release. For more information, refer to Security Server Multi-Platform.

1.4.3. Resolved Issues

1.4.3.1. Licensing

- The **Patch Management** and **Endpoint Encryption** add-ons will now be disabled for all endpoints they are applied to after their expiration date has passed.

1.4.3.2. GravityZone Platform

- The GravityZone console was encountering communication issues with specific endpoints after a previously altered connection. This behavior resulted in inaccurately displayed policy and update changes.
- Fixed issue causing Antiphishing reports to display incorrect data for the current month. This issue occurred when the reporting interval was set for the last 2 or 3 months.
- The **Policy** tab in the endpoint details no longer displays the status "Cannot determine". The message appeared due to an issue with the cleanup rules that was fixed.
- In some cases, the GravityZone console page became unresponsive when creating a new maintenance window.
- Security fixes.

1.4.3.3. Security Server Multi-Platform (Embedded)

- Fixed an issue that prevented email credentials from being verified while using a Simple Mail Transfer Protocol (SMTP) server.

1.5. Version 6.29.3-1

Release date: 2022.10.06

1.5.1. Improvements

1.5.1.1. GravityZone Platform

- Staging updates are available to all customers using the GravityZone Business Security Enterprise solution. You can configure the updates in the **Configuration** > **Update** > **Components** > **Settings** pop-up window.

1.5.2. Resolved Issues

1.5.2.1. EDR

- Alerts generated by custom detections would be stuck in loading for users with only the Security Analyst role assigned.

1.5.2.2. GravityZone Platform

- Failed backups to network share no longer prevent further backups to be performed. This issue sometimes occurred when the user had insufficient rights to write files to the network share.
- Fixed an issue that prevented users from deleting staging product updates.
- Security fixes.

1.6. Version 6.29.2-1 (Third-Party Updates)

Release date: 2022.09.07

1.6.1. Resolved Issues

1.6.1.1. GravityZone Platform

- Security fixes.

1.7. Version 6.29.2-1

Release date: 2022.08.03

1.7.1. Resolved Issues

1.7.1.1. GravityZone Platform

- Security fixes.

1.8. Version 6.29.1-2

Release date: 2022.07.21

1.8.1. Resolved Issues

1.8.1.1. Network

- The **Restart machine** task failed on Security Servers deployed in VMware NSX environments.

1.8.1.2. Exclusions

- Antimalware exclusions from **Configuration Profiles** failed to apply to endpoints after update to version 6.29.1-1 due to a reconfiguration of the policy settings.

1.9. Version 6.29.1-1

Release interval: 2022.07.19 - 2022.08.02

1.9.1. Improvements

1.9.1.1. GravityZone Authentication

- The options and messages related to two-factor authentication (2FA) are now referring to “trusting the browser” rather than “remembering the device”, as the settings actually apply per browser. This addresses the scenario where a user might use a computer with multiple browsers to log in to GravityZone Control Center.
- Some buttons and options related to 2FA have been redesigned, alongside other minor visual changes.
- A new message informs you when you cannot log in to GravityZone Control Center because of an ongoing update.

1.9.1.2. Quarantine

The **Quarantine** page has a new modern design and includes the following changes:

- The views selector was redesigned into two new subsections that are available in the GravityZone menu under **Quarantine**.
- Filters and columns allow more control and customization. You can show or hide filters, add or remove columns and use a compact view.
- Added new time intervals for the quarantined items.
- Renamed a few elements on the page.

1.9.1.3. Exclusions

- You can now add exclusions to **Configuration Profiles** right from the **Blocked Applications** report. Use the new **Back** option at the top-left corner in **Configuration Profiles** to return to the report if needed.
- In **Configuration Profiles**, the contextual menu option **Assign to list** has been modified to **Edit list assignment**. The name of the corresponding configuration page also reflects this change.
- The **Exclusions** grid area in **Configuration Profiles** includes a new sortable column named **Added on**, which by default lists the exclusions in reverse chronological order. Only exclusions added after this GravityZone update will display date and time.
- Exclusions in **Configuration Profiles** and in the policy now support the `%SystemDrive%` variable.
- You can now use the asterisk (*) as wildcard for searching exclusions in the **Configuration Profiles** section.
- To accommodate Linux requirements, exclusions now support up to 4096 characters when defining paths in **Configuration Profiles** and in the policy. To apply this on Windows systems, make sure `MAX_PATH` is set to support this value on the target machines.
- Editing exclusions and list assignments now reflects in more detail in the **User Activity** section, with separate entries for the affected exclusions, lists, and policies.
- In **Policies** > **Configuration Profiles**, you can assign multiple exclusions to multiple lists by using the new **Assign to lists** option.
- Minor name changes to various buttons and options for more consistency.

1.9.1.4. Maintenance Windows

- New messages warn you when deleting maintenance windows assigned to policies, and when you remove the last maintenance window from a policy.
- You can now sort maintenance windows by name, status, modification time, users who last edited the window, permissions, and policies.
- The grid area in **Configuration Profiles** now displays the list of maintenance windows on multiple pages instead of a page with infinite scrolling.
- Minor text changes to the **Patch Management** section in the policy and in **Configuration Profiles**.

1.9.1.5. Policies

- The configuration page for location assignment rules now has the **Targets** section, where you can define specific folders within the network where you can apply a rule. If you do not enable **Targets**, the rule applies to the entire network.

- A new column added in the **Assignment Rules** grid indicates the status of existing rules:
  - **Running** – the rule is active and is applicable to the endpoints.
  - **No target** – the rule is not applied to the endpoints because it is missing targets.
- You can now scroll through sections inherited from another policy.

1.9.1.6. Network

- Added two new tasks in the Network > Tasks section: **Isolate** and **Remove from isolation**.
- The **Restart machine** task is now available for all Security Server types in distributed environments.

1.9.1.7. Localization

- From now on GravityZone Control Center is available in Japanese.

1.9.2. Resolved Issues

1.9.2.1. Reports

- In some cases, reports were displaying incorrect data due to inconsistencies with reporting intervals and time zones.
- In some situations, the **Security Audit** report did not include **Advanced Anti-Exploit** events.

1.9.2.2. GravityZone Platform

- Security fixes.

1.10. Version 6.28.1-4

Release date: 2022.06.14

1.10.1. Resolved Issues

GravityZone platform

- New scheduled database backups to network locations failed after updating the console to version 6.28.1-1.
- When using policy assignment rules endpoints migrated to a new host continued to use the Security Server of the initial host.
- The embedded Security Server failed to run properly with a specific set of licenses.
- Security fixes.

1.11. Version 6.28.1-3

Release date: 2022.05.25

1.11.1. Resolved Issues

GravityZone platform

- Fixed a few incorrect translations displayed in the GravityZone console.
- Security fixes.

1.12. Version 6.28.1-1

Release interval: 2022.04.14 - 2022.05.03

Minimum requirements:

- Security agents: 7.5.1.177 (Windows), 7.0.3.1986 (Linux), 7.4.10.200020 (macOS)

1.12.1. Improvements

1.12.1.1. GravityZone Platform

- Bitdefender has launched a new product portfolio. We have changed several product names to offer a better representation of our current vision. Learn more.
- Two-factor authentication is easier to use with the new **Remember this device** option on the login screen, which allows you to skip entering the six-digit code for a certain time interval. You can enable this option and configure the interval in the **Configuration** > **Miscellaneous** section.
- The list of supported internet browsers has been updated. Learn more.

1.12.1.2. Patch Management

GravityZone extends support for patch scanning and installation to Linux endpoints. For a unified experience, you can use the same maintenance windows and the same policies as for Windows.

Supported Linux distributions for this feature:

- CentOS
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise (SLE)

For the entire list of requirements, refer to Patch Management.

For the list of error messages received in GravityZone Control Center when **Patch Scan** or **Patch Install** fails, refer to this topic.

> **Note**
> Unlike for Windows, Patch Management for Linux endpoints does not require Relay role to use the Patch Caching Server role. Instead, the security agent downloads the updates directly from vendors' websites.

1.12.1.3. Fileless Attack Protection

The new integration with **Windows Antimalware Scan Interface (AMSI)** technology provides an additional level of protection against dynamic malware such as script-based attacks.

- The **Command-Line Scanner** option allows you to detect fileless attacks at pre-execution stage.
- The **Antimalware Scan Interface Security Provider** option allows you to scan content (scripts, files, URLs etc.) sent by other services that require a security vendor to analyze it before accessing, running, or writing it to the disk.

1.12.1.4. Configuration Profiles

- Bitdefender introduces a series of improvements to the **Exclusions** section:
  - The ability to import and export exclusion lists in the CSV format.
  - The ability to edit exclusions inline and delete or export them in bulk. You can also export selected exclusions.
  - The ability to sort exclusions and a new pagination system for easier navigation.
  - A new option in the **Blocked Applications** report to add exclusions to lists.
  - Improved performance when using filters.
- In the **Patch Management** section, you can now add multiple custom hostnames or IP addresses for Patch Caching Servers, separated by semicolon (;). The total limit is 256 characters.

1.12.1.5. Antimalware

You can now scan the memory of a process using the new **Process memory** option available in the **On-Access Scanning** > **Settings** section of the policy.

1.12.1.6. Network Protection

- The **Content Control** module is now available for Windows servers and Citrix virtual apps and desktops. For existing clients, the module is available through the **Reconfigure Client** task, while new clients need the installation packages configured accordingly. Learn more. Content Control on Windows servers requires Bitdefender Endpoint Security Tools version 7.5.1.177 or later.
- The Network Attack Defense module for macOS systems in now supported in GravityZone. The next versions of Endpoint Security for Mac will ensure compatibility between endpoints and GravityZone.
- On Windows servers, the Network Attack Defense module extends its capabilities on Windows servers beyond RDP connections and it scans web traffic as well when used with the new Content Control capability.

1.12.1.7. Security Audit

Added a new event type for AMSI detections.

1.12.1.8. Assignment Rules

For location rules, we increased the maximum number of DNS servers addresses to 30, and the field length to 480 characters.

1.12.1.9. Network

- The **Endpoint details** page displays more explicit messages when users have not approved Full Disk Access and Network extension for Endpoint Security for Mac components.
- New endpoint packages no longer have the **Device Control** module on by default.

1.12.1.10. Localization

From now on GravityZone Control Center is available in Vietnamese.

1.12.1.11. Sandbox Analyzer

Security improvements to Cloud Sandbox.

1.12.2. Resolved Issues

1.12.2.1. GravityZone Platform

- Fixed an issue that prevented Security Server packages for Hyper-V and Citrix from being published for offline environments.
- Fixed an issue that prevented the online GravityZone instance from correctly validating newly-created mirror archives.
- Fixed an issue that prevented the online GravityZone instance from connecting to the Windows shared location via the Server Message Block (SMB) protocol.
- Fixed an issue that prevented the online GravityZone instance from mounting SMBv1 shares.
- Fixed an issue that prevented the online GravityZone instance from removing the temporary `.bddltmp` extension when downloading kit files.
- Fixed an issue that prevented the online GravityZone instance from publishing Bitdefender Endpoint Security Tools Linux v7 packages.
- Fixed an issue that caused the online GravityZone instance to remount shares when running `gzou-target` scripts.
- Fixed an issue that caused the online GravityZone instance to display errors after starting the web service.
- Fixed an issue that prevented the GravityZone Control Center to display the hash of infected files in the **Antimalware event** notification.
- Security fixes.

1.12.3. Known Issues

1.12.3.1. Network

When having a version of Endpoint Security for Mac higher than **7.6.12.x** and a version of GravityZone older than **6.28.x**, the following issues may occur in Control Center:

- In the **Computer Details > Protection** tab of the macOS endpoints, **Primary scan engine** displays **None** instead of **Local Scan**.
- When assigning the **Repair client** task to a folder group containing a macOS endpoint with such a version, you receive the following message: **Task could not be created. Unknown operating system of repair task target**.

1.13. Version 6.27.1-5 (Third Party Updates)

Release date: 2022.03.29

1.13.1. Resolved Issues

GravityZone platform

- Security fixes.

1.14. Version 6.27.1-5

Release date: 2022.03.08

1.14.1. Resolved Issues

GravityZone platform

- Security fixes.

1.15. Version 6.27.1-4

Release date: 2022.02.02

Resolved Issues

GravityZone platform

- The **Dashboard** icon was missing from the collapsed menu after updating Control Center to version 6.27.1-1.
- In some situations, Control Center prevented users from saving newly configured policy settings. The issue occurred when having an exceptionally high number of processes in **Application Control** and trying to add exclusions for each of them to the policy.
- In some cases, fixing a disk usage issue using System Status resulted in GravityZone console failing to download endpoint packages.

Configuration Profiles

- The GravityZone console prevented users from adding new exclusion rules when editing preexisting exclusion lists.

Notifications

- The **Antimalware event** notification incorrectly displayed the **Scan Engines Type** value. This behavior occurred only in notifications sent per email.

1.16. Version 6.27.1-3 (Third Party Updates)

Release date: 2022.01.28

Resolved Issues

GravityZone platform

- Security fixes.

1.17. Version 6.27.1-3

Release date: 2022.01.27

Resolved Issues

Deployment

- The remote installation for endpoints failed after updating GravityZone Control Center to version 6.27.1-2.

GravityZone platform

- Security fixes.

1.18. Version 6.27.1-2

Release date: 2022.01.18

Resolved Issues

GravityZone platform

- Endpoint names are no longer clickable in the **Endpoint Protection Status** report for GravityZone users with Security Analyst role. Previously, clicking endpoint names resulted in Control Center session expiration for such users.
- Security fixes.

2. 2021

2.1. Version 6.27.1-1 (Third Party Updates)

Release date: 2021.12.14

Resolved Issues

GravityZone platform

- Security fixes.

2.2. Version 6.27.1-1

Release interval: 2021.12.07 - 2021.12.13

Minimum requirements:

- Security agents: 7.4.1.111 (Windows), 7.0.3.1903 (Linux)

Improvements

Patch Management

- GravityZone introduces **Maintenance windows** in **Configuration Profiles**, a new and powerful way to configure Patch Management settings outside policies. Maintenance windows provide you with higher control over patch scanning and patch installation than before, with expanded scheduling options.
  In the policy, the old Patch Management module is replaced with a simple interface that allows you to assign the maintenance window you want. You can assign the same maintenance window, created by you or other users, to multiple policies.
  Upon this release, all Patch Management settings from existing policies will automatically be moved into maintenance windows, which then will be assigned to those policies. So, no worries there, your previous hard work is in safe hands.
  The Maintenance windows feature requires a valid license with Patch Management.
  Read more about Maintenance Windows

  > **Important**
  > The option **Auto-restart machine after (hours)** for Patch Management has been migrated from **Endpoint Restart Notification** section in the policy settings to the new option **System restarts automatically after a specific number of minutes** in the maintenance window settings. Under the new option, the restart interval has been set to maximum 60 minutes, regardless of any previous value.

- **Going beyond Windows...** We are currently developing Patch Management for certain Linux distributions, such as SUSE, RHEL, and CentOS. Although you have the option to install Linux patches, we recommend you wait until the feature is fully released in March 2022. Otherwise patches will have no visibility in GravityZone.

Reports

- **Antiphishing Activity**: The report is now capable of organizing Antiphishing detections and affected endpoints based on different criteria. The new features focus on underlining possible security issues in your network while helping you achieve an effortless analysis. The report now includes:
  - **Top 10 domains blocked on endpoints**, which details the most frequently detected domains.
  - **Top 10 affected endpoints**, which informs you about the endpoints that have the most Antiphishing detections.
  - **Affected endpoints**, which presents the total number of endpoints with at least one detection.
  - **Total detections**, which provides the total number of phishing detections on all endpoints.

  > **Note**
  > After this update, the last instance of the scheduled report will no longer be available in the **View report** column. To access the archive containing all instances, select the report, click **Download**and then select **Full archive** from the drop-down menu.

- **Security Audit**: The new improvements simplify the analysis of Antimalware detections in the Security Audit report. The report now classifies the Antimalware detections and affected endpoints based on different criteria as follows:
  - **Top 10 malware by number of endpoints**, which details the most frequent Antimalware detections.
  - **Top 10 endpoints by number of Antimalware detections**, which informs you about the endpoints that have the most Antimalware detections.
  - **Endpoints**, which presents the total number of endpoints with at least one Antimalware detection.
  - **Detections**, which provides the total number of Antimalware detections on all endpoints.

Notifications

- License expires notifications have been modified to offer more comprehensive license information.

Public API

- The **Incidents API** has new methods for managing custom rules: `getCustomRulesList`, `createCustomRule`, and `deleteCustomRule`.
- Patch Management is now available through API. For the **Patch Management API**, the following methods have been added: `createPatchManagementMaintenanceWindow`, `getMaintenanceWindowList`, `getMaintenanceWindowDetails`, `updatePatchManagementMaintenanceWindow`, `deleteMaintenanceWindow`, `assignMaintenanceWindows` and `unassignMaintenanceWindows`.

Resolved Issues

Firewall

- Firewall rules are now being imported from GravityZone if the protocol is set to ICMP.

Platform

- Exclusions lists from Configuration Profiles now display correct information after importing CSV files.

2.3. Version 6.26.4-2

Release date: 2021.11.15

Resolved Issues

GravityZone platform

- Security fixes.

2.4. Version 6.26.4-1 (Third Party Updates)

Release date: 2021.10.12

Resolved Issues

GravityZone platform

- Security fixes.

2.5. Version 6.26.4-1

Release date: 2021.09.28

Resolved Issues

Configuration Profiles

- GravityZone Control Center failed to delete the exclusions list unless the page was refreshed.

GravityZone platform

- Security fixes.

2.6. Version 6.26.3-1

Release date: 2021.09.14

Resolved Issues

GravityZone platform

- Security fixes.

Policies

- The **Allow endpoints to send user login data to GravityZone** option was not properly inherited from the main policy.
- The **Power User** password was no longer recognized after adding a new exclusion in the **Configuration Profiles** section.

Network

- The **Full scan** logs available in the **Scan Logs** tab were not properly displayed resulting in a blank page when opened. The issue affected only a small group of endpoints.

2.7. Version 6.26.2-1

Release date: 2021.08.24

Resolved Issues

Product

- An incorrect cleanup was triggered while publishing a new repository version.

2.8. Version 6.26.1-1 (Third Party Updates)

Release date: 2021.08.17

Resolved Issues

- Security fixes.

2.9. Version 6.26.1-1

Release interval: 2021.08.05 - 2021.07.19

New Features

Container Protection

Bitdefender protection is now available for container environments. Container Protection monitors both the operating system on the host and running containers, providing server workload EDR and anti-exploit and antimalware scanning services based on licensing.

The feature offers visibility into Linux server and container workload malicious activity in real time and a clear understanding of attack risk exposure at each stage of the attack. It detects complex attacks early with Linux native exploit detection technology and performs threat-hunting campaigns using the GravityZone EDR event search. Once licensed, you can deploy Container protection through two solutions:

- **Best for Linux v7** deployed directly on a container host.
- A Security Container instance deployed on a separate container that protects both the host and its managed containers.

This new feature comes with a new report, **Security Container Status**, which helps you identify any issues that a specific Security Container might have, with the help of various indicators such as Update Status, Upgrade Status and more.

A new notification is also available, **Security Container Status Update**, informing you when the product update status changes for a Security Container installed in your network.

Advanced Anti-Exploit

Advanced Anti-Exploit is now available for Linux.

Improvements

Network

- **Virtual Machines** view renamed into **Cloud Workloads**.
- **Containers** group added under **Cloud Workloads** containing container hosts and container endpoints.
- Physical and VM container hosts now visible under **Computers and Virtual Machines**.

Reports

- **Monthly License Usage** report now contains Container Protection information.

Configuration Profiles

The **Configuration Profiles** section under **Policies** enables you to create and manage customized exclusion rule lists, and assign them to your company policies, thus enabling you to scale the usage of exclusions across your network more accurately, to lower the rate of false-positive events and improve system performance.

Every exclusion rule you create can be assigned to one or multiple exclusion lists, and every list can be assigned to one or more policies. Furthermore, you can assign multiple exclusion lists to the same policy, for maximum flexibility.

EDR

We fine-tuned the formula for how we calculate the Severity Score, to make it more accurate, by taking into account a wider range of parameters, and incident escalation. We also added new mechanics that allow us to update the formula on-the-fly with new parameters from our evolving correlation technologies.

2.10. Version 6.25.1-2

Release interval: 2021.07.06 - 2021.07.20

Improvements

GravityZone platform

- From now on you can view the usernames of all the active users logged-on an endpoint. The new option is available on Windows and offers support for multiple users logged on an endpoint.
  The newly-introduced users data will become accessible under multiple GravityZone pages:
  - **Network** - where a new searchable column for logged-on users will be displayed in the Network Inventory and a new tab for logged-on users will be added in the Endpoint Details page.
  - **Reports** - where a new default and searchable column will be displayed in the Network Protection Status report.
  - **Policies** - where a new option allows you to control whether endpoints send data regarding user logon sessions such as: username, logon time or logon method.

  This will serve you in multiple ways:
  - As an admin, you can use the usernames in the network and/or reports to be able to reach out to the user in case their input is needed.
  - As a Security Analyst, you can correlate the information about the username with other events from GravityZone or third-party systems.

  Minimum version of Bitdefender Endpoint Security Tools: 7.2.1.60.

- Renamed a few elements from the Network section: the column **Machine type** is now **Endpoint type**.
- The cleanup rules for offline machines are now more flexible:
  - Name patterns can contain the question mark (?) as wildcard.
  - Name patterns can have any length and no longer require a letter at the beginning. For example, you can use only the asterisk (*) to match any machine name.
  - You can select targets that are offline for less than 24 hours or more than 90 days. The cleanup rules will run hourly for machines offline less than a day, and daily for the other ones.
  - The target selection now covers Active Directory inventory as well.

Report Builder

- GravityZone Elite and GravityZone Ultra customers can now use Report Builder. Available under **Reports > Queries**, this feature allows you to create detailed query-based reports, with a higher level of customization than the predefined ones. See GravityZone documentation for details regarding Report Builder requirements, installation and operation.

Antimalware

- The **Malware Status** report has now the option for exporting report details to PDF.

HyperDetect

- The **HyperDetect Activity** report now includes the exact name of the detected threat and the file hash.

Deployment

- The **Network > Packages** section now includes **macOS downloader**, which will make it easier for you to install the security agent on different Mac architectures, whether they are Intel x86 or M1. The new downloader automatically detects the processor type and downloads and installs the right kit for that specific architecture.

VMware Integration

- Enhanced vCenter authentication by allowing you to configure the retry limit interval and the maximum number of retries before your account gets locked out due to invalid credentials.

Localization

- From now on GravityZone is also available in Turkish.

Product documentation

- A unified self-service support experience with the new online help center. All GravityZone help content that was included in PDF guides, knowledge base articles and release notes, is now under one roof, in a more digestible format. Currently it is available only in English, localizations will follow soon.

Public API

- Reports API: The `createReport` method has a new parameter - `detailedExport`, for including also the report details in the PDF file.

Resolved Issues

Patch Management

- Previously installed patches were not displayed in GravityZone after manually rebooting a virtual machine.

2.11. Version 6.24.1-1

Release date: 2021.05.25

Resolved Issues

GravityZone platform

- Security fixes.
- An HTTP redirect issue prevented the download of kits, updates and patches from Bitdefender servers.
- A limitation of the GravityZone VA operating system caused the security agents updates to fail.

Packages

- Some icons did not accurately indicate the supported OS platforms for GravityZone modules (Windows servers & workstations, Linux or macOS).

2.12. Version 6.23.1-1

Release date: 2021.04.21

New Features

EDR for Everyone

A lightweight Endpoint Detection and Response solution for Windows-based systems, powered by top-notch machine learning and cloud scan technologies, with low resource footprint, easy deployment and maintenance, which can run alongside any third-party endpoint protection platform.

This lightweight solution includes technologies from state of the art GravityZone features such as:

- Endpoint Detection and Response
- Fileless Attack Protection
- Network Attack Defense
- Advanced Threat Control (ATC)
- Sandbox Analyzer
- Endpoint Risk Analytics

> **Note**
> Available as Bitdefender EDR, a standalone solution.

2.12.1. Improvements

GravityZone platform

- Control Center leaves the old blue theme behind and comes with a couple of readability and usability improvements such as:
  - Replaced the scroll bar from the main menu with the More button to reveal additional items.
  - Increased the font size for lower screen resolutions.
  - Removed the top blue bar to make room for actual data.
  - Increased the contrast to the top banner for alerts.
- The **Update Security Server** task has two options now, for each type of update you can run, when available:
  - Feature update, for installing the Bitdefender new features, improvements and fixes, and security fixes
  - OS update, for upgrading the operating system of the Security Server VA

    Note
    Run the task with this option to bring the OS of the Security Server to Ubuntu 20.04 LTS, the only supported version until new upgrade.
- The grid in the **Network** page now includes new columns and several improvements, designed to help you better identify and find endpoints in the inventory:
  - **Name.** It can now display the MAC address appended to the hostname, to uniquely identify endpoints that may have the same hostname or IP address.
    You need to enable this option in the **Configuration** > **Network Settings** > **Network Inventory settings** page.
  - **Machine type.** It shows whether the endpoint is a server or a workstation.
  - **OS type.** It displays the type of operating system installed on the endpoint.
  - **OS version.** It shows the version of the operating system installed on the endpoint.
  - **Last seen.** It now allows you to filter endpoints that were online in the last 24h, 7 days or 30 days.
- **Virtual Machines** view of Network Inventory has now become **Cloud Workloads** view.
- When creating an installation package in the **Packages** page, you have now the option to choose the operation mode of the security agent:
  - **Detection and prevention**, which allows you to choose the modules to include in the package, and to enable their full capabilities.
  - **EDR (Report only)**, which creates an EDR package with a predefined list of modules, their functionality being limited to report-only actions. The package includes the following modules:
    - Advanced Threat Control (ATC)
    - EDR Sensor
    - Network Protection (Content Control, Network Attack Defense)

    Note
    Available only with GravityZone Business Security Enterprise, and GravityZone Business Security Enterprise Plus.
- Updated the wizard at the **Install Security Server** task with new requirements.
- Removed the option to scan the endpoint before agent installation to speed up the installation process. Nevertheless, it is recommended to run a scan task as soon as possible after the agent installed on the endpoint.

VMware integration

- Improved the performance of GravityZone processors and decreased CPU usage when synchronizing VMware inventory in high load environments.

Security for Storage

- Storage Antimalware notification now includes information about the Security Server and security content versions.

Sandbox Analyzer On-premises

- Files detected on the ICAP server as malicious are now sent to Sandbox Analyzer to remove the doubt of a false positive.

Ransomware Mitigation

- The **Ransomware Activity** page now links to the endpoint details page when clicking an endpoint name.

Security Telemetry

- New options for configuring Security Telemetry:
  - **Bypass validation of the SSL certificate on HTTP collector**, in case your HTTP collector uses a self-signed SSL certificate.
  - Granular event type selection, if you are interested in sending to the SIEM only certain types of events.

2.12.2. Resolved Issues

Active Directory integration

- When an endpoint joined in Active Directory changed its SSID, Control Center was still displaying the old entity as managed, and not the new one.

Patch Management

- Completed **Patch install** tasks could not be deleted from the **Tasks** page, returning the error "Items you selected cannot be deleted”.

2.13. Version 6.22.1-1

Release date: 2021.03.29

Resolved Issues

Security for Mobile

Apple Push Notification service (APNs) no longer supports the legacy binary protocol after March 31, 2021. All communication with Apple servers via MDM will be handled by the HTTP/2 protocol from this date forward.

This GravityZone update addresses the changes to APNs, and it is mandatory for the Security for Mobile to continue functioning. After the update, you need to configure your network firewall to allow traffic to `api.push.apple.com:443`, instead of `gateway.push.apple.com`, through ports `2195` and `2196`.

> **Note**
> The changes in APNs affects only the communication between GravityZone and Apple servers. GravityZone Mobile Client is not affected, and you do not need to update it.

2.14. Version 6.20.1-1

Release date: 2021.03.02

Minimum requirements:

- Security agents: 6.6.24.337 (Windows); 6.2.21.133 (Linux); 4.16.6.200156 (macOS)

New Features

Apple M1 support

Added support for Apple M1 processors. A separate installation package for endpoints, named **macOS kit (Apple M1)**, is available for download in the **Network > Packages** section. The previous **Mac kit** has been renamed **macOS kit (Intel x86)** and is only compatible with Intel-based Macs.

The following protection modules are supported on M1-based systems:

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

Support for other features will be added in time.

> **Important**
> After downloading the new macOS kit for Apple M1, you must publish it in **Update > Components**, otherwise the security agent installation on endpoints will fail.

> **Note**
> New kits will not install on OS X El Capitan (10.11). For details about the end of support for this legacy macOS version, refer to this topic.

Improvements

Network Inventory

New options to avoid duplicates of cloned endpoints are available in **Configuration > Network Settings**:

- Select **Applies to cloned physical endpoints that are joined in Active Directory** to resolve cloned HDD drives from decommissioned machines.
- Select **Applies to cloned virtual endpoints that are joined in Active Directory** to resolve clones created using VMware Instant Clones.

Resolved Issues

Policies

Addressed a situation where inherited security policy sections were editable after migrating to a GravityZone license without the Application Control module.

Network Inventory

Fixed an issue where Oracle Linux 7 machines imported from VMware NSX-T environments were displayed as Windows endpoints.

2.15. Version 6.19.1-1

Release date: 2021.01.25

Improvements

Antimalware

Added a new wildcard option when defining custom exclusions for files, folders, and processes. You can now use double asterisks (**) for replacing any character, including path separators (\). For example, with `**\example.txt` you can match any file named `example.txt`, regardless its location on the endpoint.

The option is available in both Control Center and Power User policy settings, under **Antimalware > Settings > Custom Exclusions** section.

> **Note**
> The single asterisk (*) substitutes zero or more characters between the path delimiters (\).

Sandbox Analyzer

Increased the length limit for detonated URLs from 500 to 1000 characters.

Resolved Issues

Patch Management

The status of patches requiring reboot after installation was not displayed in Control Center if the endpoints were rebooted manually.

Security for Mobile

An issue at the MDM module of the Communication Server caused mobile devices to stop synchronizing about a week after their enrollment in GravityZone.

GravityZone Platform

- The Security Audit report was no longer displaying Firewall events.
- Security fixes

3. 2020

3.1. Version 6.18.1-1

Release period: 2020.11.24 - 2020.12.07

Minimum requirements:

- Security agents: 6.6.22.311 (Windows); 6.2.21.106 (Linux); 4.14.96.200096 (macOS)

Improvements

EDR & Incidents

The new **Custom Detection Rules** functionality enables you to create rules to detect common events and generate incidents specific to your environment, which otherwise GravityZone may not flag as suspicious through its prevention and threat intelligence technologies. This enhances EDR's capabilities of raising alerts and triggering incidents to stop possible breaches in the early stages of an attack.

You can now:

- Create your own detection rule
- View and filter by alerts and incidents generated by a custom rule
- View details of any rule in the dedicated side panel
- Perform multiple actions, including edit, delete, duplicate or ignore a custom rule
- Import list of rules
- Receive notifications each time a new incident is triggered by a custom rule
- Add and filter tags easily maintain your created custom rules

Added the option to update your Linux EDR modules via product update when you configure policies, for a tighter change control configuration and update staging process.

The `new-incident` Syslog notification now includes more information for logging EDR incident data to an external software platform such as SIEM or SOAR. Make sure to re-check any existing correlation you are currently using and/or add the new information about incidents in the search queries that are running on your SIEM.

Relabeled the tabs inside the **Incidents** page as **Endpoint Incidents** and **Detected Threats**.

> **Note**
> Tabs availability may differ in your product, according to your license.

Security Telemetry

We now offer you the possibility to obtain raw security data from your endpoints right into a SIEM solution. Use this feature if you need a deeper analysis and correlation of the security events in your network.

Because we care about system performance and a low footprint of exported data, we are filtering out redundant information.

Check out the new **General > Security Telemetry** section of the security policy to enable and configure this feature, and the endpoint's Information page to verify the connection status between the endpoint and the SIEM.

> **Note**
> Available only for Windows endpoints and Splunk via HTTPS (TLS 1.2 or higher required).
>
> Security Telemetry requires EDR available in GravityZone Ultra.

Ransomware Mitigation

You have now the option to restore the files encrypted in a ransomware attack, on-demand. Select this option in the policy, for the endpoints where you need more control over. In case of an attack, check the **Ransomware Activity** page, from where you can view the affected files and then run a restore task.

This option is available for 30 days from the event.

Sandbox Analyzer On-premises

You can now enable sample submission through proxy to local instances in the **Sandbox Analyzer > Infrastructure** page. To set up a proxy, go to **Configuration > Proxy**.

Endpoint Protection

Following the deprecation of macOS kernel extensions, Bitdefender added support for the new EndpointSecurity and NetworkExtension APIs. These ensure the compatibility between Endpoint Security for Mac, GravityZone Control Center and endpoints running macOS Big Sur (11.0). More information is available with Endpoint Security for Mac-related documentation.

Platform

- New **Repair** task to quickly fix issues that other way would require agent reinstall.
- The options which provide more control over the data you send to Bitdefender are now available in the **Miscellaneous** section of the agent package configuration window as well.
- Several content improvements.

Public API

- The agent kit download link is now available via the `getInstallationLinks` method.
- The full version of the agent kit may now be retreived via the `downloadPackageZip` method.
- The new `endpointName` filtering option in the `getEndpointsList` method allows you to better find the endpoints in your network.
- The instant report is now accessible by email via the `createReport` method.

Resolved Issues

Sandbox Analyzer

In some situations, Sandbox Portal returned a 404 error when trying to access cached reports after seven days.

Security for Mobile

iOS devices enrollment in MDM failed when the Identity and Profile Signing certificate password contained bash special characters.

Platform

- The automatic updates system was generating the "GravityZone is unable to complete" error repeatedly, although no updates were available.
- Deleted blocked detections remained displayed in the report graph.
- Control Center was displaying the Dashboard portlets in a single row when the resolution was higher than 1080p and browser scaling was at 125%.
- Offline updates failed if the HTTP traffic for GravityZone was disabled.
- Changing the NTP server address in the **Control Center > Configuration** page had no effect.

3.2. Version 6.17.3-1

Release date: 2020.09.11

Resolved Issues

Security

Addressed a vulnerability discovered recently.

3.3. Version 6.17.2-1

Release date: 2020.08.12

Resolved Issues

Policies

- Policy assignment rules failed to apply on endpoints when the list of hostnames or IPs ended with semicolon (;).

Network Inventory

- In certain cases, GravityZone incorrectly reported the endpoint license status.

Reports

- The **Malware Status** report incorrectly listed unresolved detections as deleted.

General

- Fixed a Communication Server crash caused by invalid events.

3.4. Version 6.14.1-1

Release date: 2020.05.12

Important
Important

One of our main concerns is to support security engineers during the COVID-19 pandemic and keep network security measures stable. Therefore, we have decided to postpone Advanced Anti-Exploit technology enforcement until June 30.

Improvements

Update System

More options to update GravityZone components (security agents, Security Servers). You can configure GravityZone Update Server to download updates from the Bitdefender Servers, a custom update location, or both. The option is available in the **Update > Components > Settings** window.

3.5. Version 6.13.1-1

Release date: 2020.04.23

Improvements

Infrastructure

Added a CDN as the default updates delivery location. Configure your network firewall to allow traffic from and to `update-onprem.2d585.cdn.bitdefender.net`. For details, refer to GravityZone (on-premises) communication ports.

3.6. Version 6.12.1-1

Release Date: 2020.04.07

Minimum requirements:

- Security agents: 6.6.17.241 - Windows, 6.2.21.63 - Linux, 4.11.64.200064 - macOS
- Security Server: 6.1.75.9595 - Multi-Platform, 6.1.70.9793 - NSX-V

Improvements

Antimalware

You can now configure Security Servers' cache sharing so that you can enable/disable it or restrict it to Security Servers from the same network. Not to worry about bandwidth consumption between sites anymore. The settings are available in the **Configuration > Security Servers Settings** page.

Firewall

Added the option to import and export rules.

Full Disk Encryption

You can now set rules to exclude drives from encryption.

Remote Troubleshooting

- Remote troubleshooting is now available for all Security Server versions.
- You can now restart a troubleshooting session while maintaining its previous settings.

System Status

Automatic repair capability for metrics encountering issues on any appliance in your environment is now available at the click of a button.

Installation

Easily remove installed security solutions from your environment when upgrading to a full product license. The feature is ON by default and will remove any existing security software that creates conflicts when installing the BEST protection modules.

Dashboard

- View portlets in a single scrolling page and update all the information at once using the **Refresh Portlets** button.
- Added time filtering for the Endpoint Protection Status, Policy Compliance and Update Status portlets.

Notifications

The Antimalware Event notification now includes details about the scan type, security content version and scan engine type.

Removed Features

Reports

Removed the Malware Activity report. Consider using the Security Audit report as an alternative.

Dashboard

Removed the Malware Activity portlet.

Antimalware

Removed support for scanning Mapped Network drives when On-Demand Device Scanning is used.

3.7. Version 6.11.1-1

Release Date: 2020.01.22

Improvements

HyperDetect

Added the following details to the HyperDetect Activity notification:

- Parent process name
- Parent process ID
- Command line (if available)

Removed Features

Installation Kits for Windows Legacy

We removed all options to download installation kits for Windows legacy versions such as Windows XP, Windows Vista, Windows Server 2003 and Windows Server 2008.

Past events in User Activity, where **Action** is **Published** and **Area** is **Endpoint Kit**, will display **N/A** instead of the kit name.

For more information related to this subject, refer to these KB articles:

- Windows XP and Windows Server 2003 end of support
- Windows XP, Windows Vista, Windows Server 2003 and Server 2008 Support announcement

4. 2019

4.1. Version 6.10.1-1

Release Date: 2019.12.02

Improvements

Network Inventory

- A new type of entities in Network Inventory: golden images.
  Mark the endpoints you use for creating clones and avoid duplicates in Network Inventory. Keep track of your golden images by using the available filters.

  > **Important**
  > This feature is disabled by default. To enable it, select **Avoid duplicates of cloned endpoints** in **Configuration > Network Settings**.

- More relevant messages in Control Center when Mac clients have issues. For example, now you know if macOS has not granted the agent permissions such as access to the disk drive.

Resolved Issues

Network Inventory

Endpoints appeared duplicated in Network Inventory due to system cloning. We introduced a new entity in Network Inventory, called golden image, to avoid such situations. For details, check the Improvements section.

Antimalware

In certain scenarios, Security Servers were not displayed in the drop-down list from the **Antimalware > Security Servers** section of the policy.

Device Control

Deleting a Device Control exclusion from the policy also deleted the first item in the list.

4.2. Version 6.9.1-1

Release date: 2019.11.05

Minimum requirements:

- Security agents: Windows - 6.6.14.198
- Security Server: Multi-Platform - 6.1.73.9218

New Features

Network Attack Defense

A brand-new powerful technology focused on detecting network attack techniques designed to gain access on specific endpoints, such as brute-force attacks, network exploits, password stealers.

The Network Attack Defense settings are available under the new **Network Protection** policy section. A specific notification informs you about incidents in your network, while the **Network Incidents** report will provide more insight about these detections.

> **Note**
> To use the **Network Attack Defense** module, you need to install it on endpoints. For existing installations, run a **Reconfigure Client** task with **Network Attack Defense** selected. For new deployments, edit the installation package to include this module.

Sandbox Analyzer On-premises

Your own Sandbox Analyzer from Bitdefender is here! Born from the Cloud-based version, the new Sandbox Analyzer On-premises is delivered as a virtual appliance deployable on an ESXi hypervisor. The built-in installer allows easy deployment and configuration while the integration with GravityZone console provides a single interface for management.

The Sandbox Analyzer On-premises release is packed with the following features and capabilities:

- Virtual appliance packaging with built in graphical installer
- Out of the box integration with GravityZone console for management, configuration and deployment
- Integrated with various sensors capable for feeding samples from various sources: network streams, ICAP traffic, file system
- Unified reporting interface for both Sandbox Analyzer On-premises and Sandbox Analyzer Cloud
- Detailed detonation reports containing information about malware classification, behavior analysis or timeline view
- Support for custom detonation environments (golden images)
- Sample re-analysis using different configuration options
- REST based API for integration with third-party security solutions.

For more details, visit the Sandbox Analyzer dedicated webpage.

Remote Troubleshooting

The endpoint information page includes a new **Troubleshooting** tab, from where you can collect basic and advanced logs remotely. You can start a debug session, so that GravityZone collects the logs while the issue is reproducing. This will help our technical support specialists to perform an in-depth analysis of the issue and provide a resolution faster.

You can save the collected data on a network share, on the target endpoint or on both.

Localization

From now on we speak Chinese!

妈妈说：“今天能完成的事，不要留到明天。”

儿子回答："好吧，把全蛋糕给我，我今天都吃光了吧。"

Seriously now, you can switch the GravityZone interface to Simplified Chinese, if you please.

System Status

Control Center now includes the **System Status** section, which displays real-time status information for the main metrics of your GravityZone environment.

Improvements

Security

We have added the option to create a VPN cluster for a more secure communication between the services on the GravityZone appliances. You can enable this option from the GravityZone appliance menu.

Deployment

- Integrating new modules to deployed agents is like playing with modeling clay. We have made the reconfiguring process more flexible.
- You can choose to install Bitdefender security agents without removing the security software from other vendors. This means zero protection gap and faster deployment. Just remember, you're doing this at your own risk. Some security solutions may affect the Bitdefender installation. Once you are protected by Bitdefender, you can manually remove any previously installed security solution.

Network Inventory

Goodbye to unused virtual machines from your network inventory. The **Configuration** page offers you the option to schedule automatic cleanup tasks.

Policies

- The new Antimalware **> On-Execute** section covers Advanced Threat Control and Fileless Attack Protectiont.
- **Network Protection**, another new policy section, exposes the new Network Attack Defense technology and shields the Content Control features.
- Content Control went through a big transformation as well:
  - The old **Traffic**, **Web**, **Data Protection**, and **Applications** sections have been re-organized into new **General**, **Content Control**, and **Web Protection** sections.
  - The new **Network Attacks** section exposes the **Network Attack Defense** technology and its settings.
  - The new **Global Exclusions** option, in the **General** section, replaces the previous separated **Traffic Scan** and **Antiphishing** exclusions. During update, the existing policies will be automatically migrated to the new global exclusions.
  - **Network Protection** replaces the previous **Content Control** module in the **Inheritance Rules** settings.
  - The GravityZone reports keep tracking the Content Control features, but also include information on Network Attack Defense.
  - Location-based policies are now aware of the hostname, too. You can to define assignment rules based on endpoint's hostname.

Advanced Anti-Exploit

- Three new detection techniques are available: VBScript Generic, Shellcode EAF (Export Address Filtering), and Emerging Exploits. These detections will be present from now on in the Security Audit and Blocked Applications reports.
- User Activity now includes logs related to Advanced Anti-Exploit.

Patch Management

Added the option to limit reboot postpones at maximum 48 hours from new patches installation. When the set amount of time expires, endpoints will automatically reboot. Endpoint users will receive a notification regarding this action.

You can find this new option in the policy, under the **Notifications > Endpoint Restart Notification** modular settings.

Sandbox Analyzer Cloud

- Results from detonation analysis are available with new information-rich reports in HTML format. These reports contain details such as: malware classification, process-level view, network activity, timeline view, registry keys and mutex objects accessed, file systems modifications, IOC attributes.
- The **Filters** area is expanded by default, so it is easier for first-time users to discover all the options available with the submission cards.
- Under the **Submission Type** filtering category, the **Automatic** option has been renamed to **Endpoint Sensor**.

> **Note**
> These features are available for Sandbox Analyzer On-premises too.

HVI

- Added network connection details to forensic information. HVI reports details such as active connections, IP addresses, and ports involved, when it detects an attack in user space.
- HVI now prevents malicious DLL files from being loaded inside a protected process.

> **Note**
> These options are available in the **HVI > User Space** policy settings.

Notifications

- Added **Blocked Devices** notification that alerts you whenever a blocked device connects to the endpoint. This notification is configurable from **Notification Settings**.
- The **Antimalware** notification is now triggered during the scan, each time a malware event is detected.

Reports

The **Endpoint Modules Status** report now includes information on Sandbox Analyzer and HyperDetect.

Integrations

Added compatibility with NSX-T 2.5, which includes agentless antimalware scanning for Linux virtual machines.

Public API

- All GravityZone reports are now available via API as well.
- We have made some improvements here and there:
  - `createReconfigureClientTask` entered the Network API
  - `getManagedEndpointDetails` returns all installed modules on a managed endpoint
  - `getInstallationLinks` returns the installation links for a package
  - `getQuarantineItemsList` has new filtering options
- Sandbox Analyzer On-premises provides various API methods for monitoring detonation infrastructure, managing sample submission and downloading analysis reports. For details, refer to Public API.

Resolved Issues

Policies

Disabling the **Endpoint Issues Visibility** option in the **Notifications** policy section does not disable sub-features as well.

Automatic Update

Automatic product updates failed to start when configuring certain time zones and intervals.

Network

The **Mobile Devices** view failed to display the Active Directory inventory when creating an integration with the option **Sync to Custom Groups** enabled.

Known Issues

Sandbox Analyzer

- The HTML reports accessible in the Sandbox Analyzer section are available only in English.
- Sandbox Analyzer On-premises supports only golden images in English for building detonation virtual machines.

4.3. Version 6.8.1-21

Release Date: 2019.07.30

Improvements

Upgraded Database Servers

At Bitdefender, we are continuously improving GravityZone, world's best-in-class cybersecurity solution. This time, we enhanced the performance of GravityZone Database Server by upgrading MongoDB, the database management system they use. The MongoDB upgrade also brings some security and operational improvements.

> **Warning**
> Before proceeding with the update, we strongly advise you to take snapshots of all GravityZone appliances.

4.4. Version 6.7.1-1

Release date: 2019.07.02

Minimum requirements:

- Security agents: Windows - 6.6.11.159
- Security Server: Multi-Platform - 6.1.71.8593

New Features

Advanced Anti-Exploit

Powered by machine learning, this new proactive technology 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 existing solutions.

This security layer is pre-configured with the recommended security settings and you can customize it from the Antimalware **> Advanced Anti-Exploit** policy section.

You can view Advanced Anti-Exploit events in the **Security Audit**, **Blocked Application**, **Endpoint Modules Status** reports.

> **Note**
> This security layer addresses Windows-based systems.

Improvements

Antimalware

- Improved custom exclusions:
  - Ability to use wildcards when defining custom exclusions.
  - Added more exclusion types: file hash, certificate thumbprint, threat name, and command line.
  - New field for adding notes or remarks for each exclusion.
  - Added the option to add ATC/IDS exclusions on folders.
- Technology improvements to Central Scan:
  - Security Server cache sharing technology is now available. With this implementation, Security Servers will share scanning cache information with each other, leading to significant scanning speed performance increase in virtualized environments.
    To benefit of this feature, enable port 6379 to allow traffic between Security Servers.

    > **Note**
    > Cache sharing works only between Security Servers of the same type. For example, Security Server Multi-Platform shares its cache only with other Security Servers Multi-Platform.

  - Implemented a new Load Balancing mechanism between endpoints protected through Bitdefender Endpoint Security Tools with Central Scan, and Security Servers. You can now choose to distribute load evenly between the assigned Security Servers.
  - Improved load status reporting for Security Servers help you assess the scalability of Security Servers in your environment. The **Security Server Status** report now include two new states: **Near overloaded** and **Near underloaded**.

Sandbox Analyzer

- Expanded the list of supported file types that can be automatically submitted to Sandbox Analyzer.
- Added content pre-filtering capabilities for submitting files to the Sandbox Analyzer. This functionality is configurable in a new policy section.
- Added error messages for failed detonations in the submission card section on the **Sandbox Analyzer** page.

Security for Storage

- You can now use secured connection between Security Servers and the protected NAS servers, provided they use SSL over ICAP. Load your security certificate in the **Configuration > Certificates > Endpoint - Security Server communication** section of Control Center.

Usability

- Optimized the Control Center workspace with the new display modes of the menu: expanded, collapsed (icon view) and hidden.

Reports

- The **Network Protection Status** report has been enriched with more granular statuses for license (**Expired**, **Pending**, **Trial**) and endpoint management (**Unmanaged**).

Update system

- Replaced the antimalware signatures with a new method to identify known and unknown malware, called **Security Content**.
- Security Server updates are now published using update rings.

Public API

- **General**: Through this new endpoint you can now get the API key details.
- **Network**:
  - Added the option to create a scan task using the MAC address of the endpoint.
  - Added the `companyId` field in the results of the `getManagedEndpointDetails` method.
  - You can now reset the label for an endpoint using the `setEndpointLabel` method.
  - Introduced the `assignPolicy` method.

Resolved Issues

Sandbox Analyzer

- Analysis results from a manual submission could not be retrieved if proxy was in place.

Update system

- In Control Center, weekly recurrence for antimalware updates was resetting upon return, if set only on Sunday. This was only a display issue, the setting being sent correctly to the security agent.

Antimalware

- Security Server Load Balancing – Equal distribution mode had limited functionality. The scan load was not distributed equally between Security Servers.

Known Issues

Antimalware

- The new custom exclusion types are not available for custom scanning tasks from the **Network** page.
- The following exclusion types for ATC/IDS are available only for Windows desktop operating systems:
  - Process with wildcards
  - File hash
  - Detection name
  - Detection name with wildcards
  - Command-line
- Certificate hash (thumbprint) exclusions are not available for ATC/IDS.

4.5. Version 6.6.1-2

Release date: 2019.05.14

Improvements

Update system

GravityZone comes with a more flexible update system, which offers greater control over the update process. Among improvements, you can notice:

- Requirements validation before installation
- Progress tracking for each appliance from Control Center
- Update synchronization across appliances
- Automatic resume of the update, if interrupted by appliance reboot or crash
- Integrity checks when modifying the GravityZone infrastructure
  Starting with this update, installation of GravityZone roles requires using the same major and minor version numbers of GravityZone, for both the image file and the deployment.
  This requirement applies both when you reinstall an existing role, or when you extend your GravityZone deployment.
  The GravityZone version number consists of these sequences: `major.minor.patch`. For example, at version 6.5.3-1, 6 major version is 6, minor version is 5, and patch version is 3-1.

  Important
  You need to run this update manually. **Automatic update** is suspended due to the changes being made to the update system itself.

4.6. Version 6.5.5-1

Release date: 2019.04.09

New Features

Integration with NSX-T

- Agentless security with antimalware capability for your NSX-T Data Center 2.4, through the Guest Introspection service platform.

Integration with BitdefenderNetwork Traffic Security Analytics (NTSA)

- You can now integrate GravityZone with NTSA and smoothly navigate to NTSA console by a single click in GravityZone Control Center.

Improvements

Full Disk Encryption

- Encryption on macOS is now performed by FileVault for the boot drive and by the diskutil command-line utility for the non-boot drive.
- GravityZone takes ownership for macOS boot drives encrypted with FileVault.

Sandbox Analyzer

- You can now submit password-protected archives from the **Manual Submission** page.

Security for Virtualized Environments

- Effortless host maintenance with the new behavior of Security Server Multi-Platform, configurable in the security policy. When maintenance starts, Security Server is automatically shut down or migrated to another host, depending on the affinity rules. Migration is possible even on hosts with another Security Server in place.

Report Builder

- The Report Builder roles Database and Processors are delivered with the GravityZone appliance.

Reports

- The malware status reported by endpoints is now more accurately calculated and displayed in GravityZone reports and portlets:
  - The **Still Infected** status has been changed to **Unresolved**.
  - Removed the reporting interval options containing "last" ("last week" or "last 2 months") from scheduled reports.

> **Note**
> This change affects all existing scheduled reports. You may need to edit your scheduled reports and select another reporting interval option.

Security for Mobile

- Added support for push notifications through the Firebase Cloud Management (FCM) service on Android.

Resolved Issues

- Addressed a rare out-of-sync Control Center issue that occurred in certain GravityZone environments with Replica Set. Control Center was resynchronized after restarting the Communication Server services.
- Some security issues and minor bug fixes regarding GravityZone Control Center functionalities.

Deprecated Features

- The **Malware Activity** report has become deprecated. For now, you can continue to use this report as before. At the same time, Bitdefender plans to improve the reporting of malware information in a future GravityZone update.