

Bitdefender®

GravityZone Cloud

Table of Contents

1. 2022	6
1.1. December 2022 (Version 6.35.0-1)	6
1.1.1. Early Access	6
1.1.1.1. XDR Live Search	6
1.1.2. Improvements	6
1.1.2.1. Integrity Monitoring	6
1.1.2.2. XDR	6
1.1.2.3. Network Protection	6
1.1.3. Resolved issues	6
1.1.3.1. Integrity Monitoring	6
1.1.3.2. Integrations	7
1.1.3.3. GravityZone platform	7
1.2. November 2022 (Version 6.34.0-1)	7
1.2.1. Early Access	7
1.2.1.1. XDR Live Search	7
1.2.1.2. Unified Incidents	7
1.2.2. New features	8
1.2.2.1. Integrity Monitoring	8
1.2.2.2. GravityZone platform	8
1.2.2.3. Endpoint tags	8
1.2.2.4. Email Security	9
1.2.3. Improvements	10
1.2.3.1. GravityZone platform	10
1.2.3.2. XDR	10
1.2.3.3. Threats Xplorer	10
1.2.3.4. Public API	11
1.2.4. Resolved issues	11
1.2.4.1. Licensing	11
1.2.4.2. Threats Xplorer	11
1.2.4.3. GravityZone platform	11
1.2.5. Known issues	11
1.2.5.1. Integrity Monitoring	11
1.3. October 2022 (Version 6.32.0-2)	12
1.3.1. Improvements	12
1.3.1.1. EDR	12
1.4. September 2022 (Version 6.31.0-2)	12
1.4.1. Early Access	12
1.4.1.1. XDR Live Search	12
1.4.2. New features	12
1.4.2.1. Early Access programs	12
1.4.2.2. Remote troubleshooting	12
1.4.3. Improvements	12
1.4.3.1. XDR	12
1.4.3.2. Quarantine	13
1.4.3.3. GravityZone platform	13
1.4.3.4. Email Security	13
1.4.4. Resolved issues	13
1.4.4.1. API	13

1.5. August 2022 (Version 6.27.2-3)	13
1.5.1. New features	13
1.5.1.1. GravityZone platform	13
1.5.2. Improvements	14
1.5.2.1. GravityZone platform	14
1.5.2.2. XDR	14
1.5.2.3. Firewall	14
1.5.2.4. Advanced Anti-Exploit	14
1.5.2.5. Risk Management	14
1.5.3. Resolved issues	15
1.5.3.1. GravityZone platform	15
1.5.3.2. Configuration Profiles	15
1.5.3.3. Patch Management	15
1.6. August 2022 (Version 6.27.2-2)	15
1.6.1. Resolved issues	15
1.6.1.1. GravityZone platform	15
1.7. July 2022 (Version 6.27.2-1)	15
1.7.1. Improvements	15
1.7.1.1. XDR / EDR	15
1.7.1.2. Sensors Management	15
1.7.1.3. Risk Management	16
1.7.1.4. Network	16
1.7.1.5. Policies	16
1.7.2. Resolved issues	16
1.7.2.1. Quarantine	16
1.8. July 2022 (Version 6.26.2-2)	16
1.8.1. New features	16
1.8.1.1. Integrations	16
1.8.2. Improvements	16
1.8.2.1. XDR	16
1.8.2.2. Threats Xplorer	17
1.8.2.3. Licensing	17
1.8.2.4. Exclusions	17
1.8.2.5. GravityZone authentication	17
1.8.2.6. Sandbox Analyzer	18
1.8.2.7. Quarantine	18
1.8.2.8. Companies	18
1.8.2.9. Network	19
1.8.2.10. API	19
1.8.2.11. Localization	19
1.8.3. Resolved issues	19
1.8.3.1. GravityZone platform	19
1.8.3.2. API	19
1.8.3.3. Reports	19
1.8.3.4. Risk Management	19
1.9. June 2022 (Version 6.26.2-1)	19
1.9.1. New features	19
1.9.1.1. EDR	19
1.9.1.2. Licensing	19
1.9.2. Improvements	20

1.9.2.1. XDR	20
1.9.2.2. EDR	20
1.9.2.3. Exclusions	20
1.9.2.4. Maintenance Windows	21
1.9.2.5. Policies	21
1.9.3. Resolved issues	21
1.9.3.1. Device Control	21
1.9.3.2. GravityZone platform	21
1.10. May 2022 (Version 6.26.1-2 EFX)	21
1.10.1. Improvements	21
1.11. May 2022 (Version 6.26.1-2)	22
1.11.1. Improvements	22
1.11.2. Resolved issues	22
1.12. May 2022 (Version 6.26.1-1)	22
1.12.1. New features	22
1.12.2. Improvements	22
1.13. April 2022 (Version 6.24.0-3)	22
1.13.1. Improvements	22
1.13.1.1. GravityZone platform	22
1.13.1.2. Public API	23
1.14. April 2022 (Version 6.23.0-4)	23
1.14.1. New features	24
1.14.1.1. XDR in general availability	24
1.14.1.2. Threats Xplorer	25
1.14.2. Improvements	25
1.14.2.1. GravityZone platform	25
1.14.2.2. Threats Xplorer	25
1.14.2.3. Network Protection	25
1.14.2.4. Antimalware	25
1.14.2.5. Fileless Attack Protection	26
1.14.2.6. Configuration Profiles	26
1.14.2.7. Assignment Rules	26
1.14.2.8. Licensing	26
1.14.2.9. Security Audit	26
1.14.2.10. Network	26
1.14.2.11. Public API	27
1.14.2.12. Localization	27
1.14.2.13. Sandbox Analyzer	27
1.15. March 2022 (Version 6.22.0-1)	27
1.15.1. Improvements	27
1.16. February 2022 (Version 6.21.1-1)	28
1.17. January 2022 (Version 6.20.1-2)	29
1.18. January 2022 (Version 6.20.1-1)	29
1.18.1. Improvements	29
2. 2021	30
2.1. December 2021 (Version 6.19.1-1)	30
2.2. November 2021 (Version 6.18.1-2)	35
2.3. October 2021 (Version 6.18.1-1)	35
2.4. September 2021 (Version 6.16.1-7)	36
2.5. September 2021	37

2.6. August 2021	37
2.7. July 2021	37
2.8. June 2021	38
2.9. May 2021	41
2.10. April 2021	42
2.11. February 2021	43
3. 2020	46
3.1. November 2020	46
3.1.1. Resolved Issues	49
3.2. September 2020	50
3.3. March 2020	51
3.4. January 2020	54
4. 2019	55
4.1. November 2019	55
4.2. October 2019	56
4.3. June 2019	60
4.4. March 2019	63
4.5. February 2019	64

1. 2022

1.1. December 2022 (Version 6.35.0-1)

1.1.1. Early Access

1.1.1.1. XDR Live Search

- The **Endpoint name** filter is now available for **Live Search**. You can use it to perform a query on specific endpoints from a company.
- Multiple graphical elements have been modified to offer a better user experience.
- Actions taken in the **Live Search** page are now available in the **User Activity** records.

1.1.2. Improvements

1.1.2.1. Integrity Monitoring

- You can now create rules using different types of special characters.
- MITRE IDs have been added for events generated by default rules. They are displayed in the **Event details** window.
- When a data retention add-on expires, events are kept for only 7 days, if the Integrity Monitoring license is still active. Events generated before the data retention add-on expired are still available for the previous retention period.
- Performance improvements.

1.1.2.2. XDR

- Where applicable, the **Deactivate AWS account** response action is now also displayed as a recommended action in the incident Overview tab, in the **Action needed** section.

1.1.2.3. Network Protection

- You can now enable outbound traffic monitoring for Network Attack Defense over SFTP and SCP/SSH protocols on Linux machines. The new options are available on the **Network Protection > General** page in the policy settings. In addition, the **Scan SSL** option has been renamed to **Intercept Encrypted Traffic** and **Scan HTTP** has become **Scan HTTPS**.

1.1.3. Resolved Issues

1.1.3.1. Integrity Monitoring

- Fixed an issue that prevented caching mechanisms from working when querying the Bitdefender Global Protective Network to check if a process is trusted.
- Fixed an issue that prevented service events from being generated on SUSE Linux Enterprise Server (SLES) systems.
- Fixed an issue that prevented the use of the `mv` command to trigger folder rename events.

1.1.3.2. Integrations

- Fixed a Splunk integration issue that was causing empty "att_ck_id" fields in "new-incident" events.

1.1.3.3. GravityZone Platform

- You can now uninstall the **Integrity Monitoring**, **Patch Management**, and **Full Disk Encryption** modules after their corresponding license keys have expired.
- Fixed an issue that was preventing partners from enabling the **Command-Line Scanner** and **Antimalware Scan Interface Security Provider** features their customers if **Fileless Attack Protection** was not licensed in their own company.
- Fixed an issue that was causing EDR raw event submission to fail for endpoints configured to use a proxy.
- Fixed an issue that was causing endpoints with Patch Management installed to display the module as expired. The issue occurred after replacing the license key for the main product.

1.2. November 2022 (Version 6.34.0-1)

1.2.1. Early Access

1.2.1.1. XDR Live Search

- The **Company** filter is now available for Live Search. As an MSP, you can use it to perform a query on endpoints from a specific company.

1.2.1.2. Unified Incidents

- This feature correlates host-based EDR incidents with broader attacks detected by XDR, bringing both types of incidents in one place: the Incidents grid.
- Correlated incidents are displayed in their own column in the grid, in line with the parent incident. They are not listed as separate entries in the grid.
- A new notification type is now available, **Correlated incident**, informing you when an incident assigned to you is correlated with another incident.
- New columns are now available:
 - **Actions taken**: shows you whether an attack was blocked by other prevention technologies.
 - **Resources** and **Entities** : replace the former **Organization impact**. For more information, click an entity or a resource to open their specific side panel.
- Filters enhancements include multiple select for the **Companies** option and a new filter for **Correlated incidents**.
- **Views** offers you the option to save your current filter and column settings for later use. You can also name, rename, delete or add your views to the Favorites category. The default views are **All incidents** and **Assigned to you**.
- The **Incident - Suspicious activity status** and **Incident - Suspicious activity** portlets in **Monitoring > Dashboard** now reflect both EDR and XDR incidents. The dashboards count the parent incidents. Correlated incidents are not represented in the charts. Severity scores are grouped by: **High** (75 - 100), **Medium** (40 - 74) and **Low** (10 - 39).

1.2.2. New Features

1.2.2.1. Integrity Monitoring

Integrity Monitoring reviews and validates changes made on Windows and Linux endpoints to assess the integrity of multiple entities.

Integrity Monitoring operates based on default rules, provided by Bitdefender, and custom rules. These rules are available in the **Policies > Integrity Monitoring Rules** page of Control Center.

Based on these rules, Integrity Monitoring takes action when events are generated for files, folders, registry entries, users, services and installed software. These events are displayed on the **Reports > Integrity Monitoring Events** page of Control Center.

You can also create a portlet, as well as two types of reports based on Integrity Monitoring events:

- **Integrity Monitoring activity**, which displays events from the events page.
- **Integrity Monitoring configuration changes**, which displays **Bitdefender Trusted** as well as **Unapproved** events.

Integrity Monitoring also comes with hardcoded restrictors, which automate best practices to reduce alert fatigue and prevent a negative impact on performance.

Integrity Monitoring is available for all standard products, except for GravityZone EDR and Bitdefender FRAT. It is delivered as an add-on for products with a license key, and as a licensing option for monthly subscriptions.

By default, it stores the detected events for 7 days. In addition, it comes with a data retention add-on to store the events. You have three options from which can choose: 90 days, 180 days and 1 year of data retention.

1.2.2.2. GravityZone Platform

- **Raw Events** is a new feature that helps you filter which Windows or macOS events GravityZone processes. This feature becomes available in the **Configuration** tab if you have the following:
 - GravityZone Business Security Enterprise or Bitdefender EDR license
 - One of the storage add-on licenses: GravityZone EDR 90 days Data Retention Add-on, GravityZone EDR 180 days Data Retention Add-on, or GravityZone EDR 365 days Data Retention Add-on.
 - EDR or XDR module enabled

You can only send raw events to one feature at a time: either to a SIEM, to Advanced search, or to Bitdefender MDR.

1.2.2.3. 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. As a partner, you can manage endpoint tags only for your own company.

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.
- 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:

- GravityZone Business Security Premium
- GravityZone Business Security Enterprise
- GravityZone Security for Workstations
- GravityZone Security for Servers
- GravityZone EDR
- GravityZone Security for Physical Workstations
- GravityZone Security for Physical Servers
- GravityZone Security for Virtualized Environments VDI
- GravityZone Security for Virtualized Environments VS

1.2.2.4. Email Security

Sandbox for Email Security

The feature adds a powerful layer of protection to your user's email accounts, sending attachments in email messages to be analyzed in depth and await results before delivering the message .

Sandbox serves as a safe virtual environment for testing potentially malicious files. A real environment is simulated where threats are triggered and payloads are detonated, in order to analyze their behavior and identify malicious intent.

The technology provides:

- Advanced threat protection and zero-day exploit detection.
- Machine learning algorithms, behavior analysis, anti-evasion techniques and memory snapshot comparison to detect threats.
- The capacity to uncover malicious files, including threats designed for undetectable targeted attacks.
- Support for a broad range of file types.
- Dynamic analysis to detect and defeat advanced malware.

Microsoft Outlook Add-in for Email Security

This add-in enables users to report messages as spam or phishing attacks directly from their inbox.

If a message is reported, it will be sent to Bitdefender and analyzed. The information gathered will be used to improve detection and the overall effectiveness of the Email Security product.

1.2.3. Improvements

1.2.3.1. GravityZone Platform

- Emails sent to new GravityZone users now contain one-time links instead of temporary passwords. Users can use the links to create a new password and log in.
- The **Incident status** portlet in **Monitoring > Executive Summary** now groups incidents based on whether the attacks were blocked by prevention technologies or not. The new values for this portlet are: **Blocked attacks** and **Requires investigation**.
- You can now view in the endpoint details in **Network** when the Patch Management and Full Disk Encryption modules are expired and why.
- GravityZone now generates and sends email notifications when the license limit for Patch Management or Full Disk Encryption is about to be reached, has been reached or exceeded.
- You can now install the Microsoft Hyper-V Security Server for second generation VM hardware.
- You now have visibility over tasks created by other users in the same company. You cannot take actions on them, but you can sort and filter them by username in the new **Owner** column in the **Tasks** grid.
Users from child companies can view tasks created by their parent company only for entities within their own companies. They can also view the user from the parent company who has created the task. This scenario applies to both Customer and Partner type companies.
- Actions taken on your tasks, such as create, restart and delete, are now visible in the **Accounts > User Activity** page.
- The default period for trusted browsers with two-factor authentication (2FA) has been set to 7 days.

1.2.3.2. XDR

- A new response action is now available in the Incidents **Graph** and **Response** tabs: **Deactivate AWS account**. This action creates and applies a policy that deactivates the AWS user account and deletes the associated access keys.
- The **Sensors Management** feature now provides integration with **Google Workspace**. The new sensor collects and pre-processes activity and usage data related to Google Workspace accounts and services.
- Prerequisites for the **Active Directory** sensor have changed. With the exception of Global Object Access Auditing policies, all group policies in Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies must be set to audit all login events.
- The default retention period for alerts has changed to 90 days. Extend retention periods for alerts, incidents or raw events by enabling a different storage add-on: GravityZone EDR 180 days Data Retention Add-on or GravityZone EDR 365 days Data Retention Add-on.

1.2.3.3. Threats Xplorer

- The **Detection details** panel now includes the web address involved in the attack for each event that is based on the **Network Attack Defense** technology.
- Improved the exclusions mechanism for **LSASS Protection** events. Now when you add an exclusion from the **Detection details** panel, the necessary details are automatically configured in the **Configuration Profiles** page.

1.2.3.4. Public API

- API support is now available for the new Integrity Monitoring feature. The following methods have been updated: `getManagedEndpointDetails`, `getNetworkInventoryItems`, `createReconfigureClientTask`, `createPackage`, `createCompany`, `setMonthlySubscription`, `getLicenseInfo`, `getMonthlyUsage`, `getMonthlyUsagePerProductType`, `createReport`, `getReportsList`.

1.2.4. Resolved Issues

1.2.4.1. Licensing

- The **Patch Management** and **Full Disk Encryption** modules will now be disabled when applied to endpoints after the seat limit on the corresponding license keys has been reached.

1.2.4.2. Threats Xplorer

- The **Detection details** panel displayed the policy directly assigned to endpoints instead of the active policy at the moment of the detection applied through assignment rules.

1.2.4.3. GravityZone Platform

- 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.
- 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.
- Security fixes.

1.2.5. Known Issues

1.2.5.1. Integrity Monitoring

Windows

- Integrity Monitoring events are not generated for monitored entities that are modified by processes excluded from Advanced Threat Control scanning.
- Integrity Monitoring events are not generated for files that have been modified through Server Message Block (SMB).

Linux

- Integrity Monitoring is not compatible with 32-bit operating systems.
- Integrity Monitoring is not applicable for Bitdefender Security Container.
- Service events are not generated on SUSE Linux Enterprise Server (SLES) systems.
- Using `mv` command does not trigger folder rename events.

1.3. October 2022 (Version 6.32.0-2)

1.3.1. Improvements

1.3.1.1. EDR

The following features are generally available to all customers using Bitdefender EDR, GravityZone Endpoint Detection and Response, GravityZone Business Security Premium and GravityZone Business Security Enterprise:

- **Assignee** option to assign the incident to an analyst.
- **Priority** option to assign the incident a priority.
- **Incident history** button shows all actions taken on the incident, including assign and priority.

The above features are in the XDR Incident Overview and EDR Graph View pages as well as in the status bar of the incidents.

1.4. September 2022 (Version 6.31.0-2)

1.4.1. Early Access

1.4.1.1. XDR Live Search

- **Early Access** enrollment is now available for **Live Search**. With this feature you can directly search for events and system information from the online endpoints in your network, using OSquery, an SQL-compatible query system.

1.4.2. New Features

1.4.2.1. Early Access Programs

- **Early Access** allows you to try out specific products, features or functionalities that are still in development, by enrolling in beta programs. [Learn more](#)

1.4.2.2. Remote Troubleshooting

- Remote troubleshooting is now available for GravityZone Security for Containers.

1.4.3. Improvements

1.4.3.1. XDR

- Auto-complete functionality is now available when adding tags in **Incidents > Custom Rules**.
- The **Sensors Management** feature now provides integration with Azure Cloud. The new **Azure Cloud** sensor can collect and pre-process cloud activity data.
- A new filter is available for the **Status** column in the **Configuration > Sensor management** page.
- Integrations with Azure AD can now provide **Risky user** information in **Incidents > Graph**. Enable this functionality by setting up the Azure AD sensor with the **IdentityRiskyUser.Read.All** permission.
- Integrations with O365 now allow you to delete a suspicious email directly from **Incidents > Graph**.

1.4.3.2. Quarantine

- You can now filter and view quarantined items regardless of the time interval. Using the **Quarantined on** filter you can customize any interval that suits your needs.

1.4.3.3. GravityZone Platform

- You can now export the data displayed in the **Companies** page as a CSV file.
- A new filter is available for the **Product Status** column in the **Companies** page: you can select between companies with active, expired, trial or no licenses.
- Licensing information is now available for the **Full Disk Encryption** and **Patch Management** add-ons in the **My company**, **Edit Company** and **Companies** pages.
- The primary update location for endpoints and relays is now `https://update-cloud.2d585.cdn.bitdefender.net`. The previous location will still be used as a fallback. You can view the changes in the **General** and **Relay** sections of the policy under the **Update** tab.
- As GravityZone administrator, you can take ownership over policies created by users that have been deleted. The new **Take Ownership** is now available in the **Policies** page, and the **Created by** column has been renamed **Owner**.
- For user assignment rules, you can select organizational units (OUs) in Active Directory inventories as targets.
- The Network Protection Status report now indicates when the Full Disk Encryption and Patch Management modules are expired.

1.4.3.4. Email Security

- You can now activate the **Email Redaction** setting for your Email Security account. This will mask sensitive information when accessing emails through reports. [Learn more](#)

1.4.4. Resolved Issues

1.4.4.1. API

- `getNetworkInventoryItems` no longer returns an internal server error when users with no rights granted over their own company use the method for child companies.

1.5. August 2022 (Version 6.27.2-3)

1.5.1. New Features

1.5.1.1. GravityZone Platform

- Added the following features to Security for Amazon Web Services:
 - Sandbox Analyzer - companies can submit files, samples and URLs, and check their status.
 - HyperDetect - this module is activated from the policy. It detects advanced attacks and suspicious activities in the pre-execution stage.
 - Fileless Attack Protection - this feature prevents fileless malware attacks. The newly generated event is displayed by BEST. In addition, the event is also visible in the Security Audit Report.

- Antimalware Central Scan - this feature enables the Security Server in the **Packages** section.
- Advanced Anti-Exploit - this feature generates anti exploit events when the tool is run on a managed endpoint.
- Network Attack Defense - this feature focuses on detecting network attacks designed to gain access on endpoints through specific techniques. In addition, the event is visible in the **Notifications** section, if **Network incident events** are enabled.
- Incidents - this feature displays all suspicious incidents detected at endpoint level, that require investigation and upon which no action was taken yet.
- Endpoint Risk Analytics - you can see new information in the **Risk Management** dashboard and **Security Risks** after the risk scan task has successfully finished.

Note

All these features are also available for companies with an existing AWS integration.

1.5.2. Improvements

1.5.2.1. GravityZone Platform

- Installation packages are now kept even if the user that created them is deleted.

1.5.2.2. XDR

- The **Sensors Management** feature now provides integration with Microsoft Intune. The new **Microsoft Intune** sensor can be configured to collect and pre-process device-related data.
- Actions taken on incidents are now visible in **Accounts > User Activity**.

1.5.2.3. Firewall

- Port scan exclusions are now available. You can create IP-based exclusions to allow port scanning.

Note

This feature brings major changes to the Firewall technology used. We recommend testing this feature before deploying it to your endpoints.

1.5.2.4. Advanced Anti-Exploit

- The **LSASS process protection** option is now more customizable and provides details about possible exploits that may target Local Security Authority Server Service (LSASS). You can configure block or report actions in the policy, add exclusions for trusted processes in **Configuration Profiles** and view related user activity. The events are available in the security agent local interface.

1.5.2.5. Risk Management

- The **Endpoint Score** in the Top Devices at Risk widget now takes User Behavior Risks into account.

1.5.3. Resolved Issues

1.5.3.1. GravityZone Platform

- The option **The company manages endpoint security** is no longer disabled when editing partner companies with clients.
- Security fixes.

1.5.3.2. Configuration Profiles

- Users were unable to export exclusion lists from a GravityZone On-premises instance and import them in GravityZone Cloud.

1.5.3.3. Patch Management

- Patches for excluded products were incorrectly displayed in Control Center as failed.

1.6. August 2022 (Version 6.27.2-2)

1.6.1. Resolved Issues

1.6.1.1. GravityZone Platform

- Security fixes.

1.7. July 2022 (Version 6.27.2-1)

1.7.1. Improvements

1.7.1.1. XDR / EDR

- Added support for multi-value fields in the **Incidents > Search** section. This functionality is also present in the Details panel.
- Alert data is now available in the **Incidents > Search** section. The raw data is available in the **JSON** tab of the Details panel.
- Alerts now display the corresponding incident number.
- New fields have been added to **Incidents > Search**. The fields are either related to alert data or to resource information normally displayed in the Graph section of an incident.
- Added two new columns to the **Extended Incidents / Endpoint Incidents** tabs in the **Incidents** page: **Assigned to** and **Priority**.
- For the XDR **Incident Overview** and EDR **Graph View** pages, added the following items:
 - **Assignee** option to assign the incident to an analyst.
 - **Priority** option to assign the incident a priority.
 - **Notes** button providing a list of analyst notes.
 - **History** button providing a history of the incident.

1.7.1.2. Sensors Management

- The Sensors Management section now displays the setup steps at the top of the page.

- Re-designed authentication-related error messages for the O365, Azure AD and AWS sensors.

1.7.1.3. Risk Management

- Decommissioned endpoints no longer appear in Risk Management. The corresponding risk data is deleted and it no longer impacts risk-related reports and dashboards.

1.7.1.4. Network

- The **Restart machine** task is now available for all Security Server types in distributed environments.

1.7.1.5. 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.

1.7.2. Resolved Issues

1.7.2.1. Quarantine

- The **Restore** button is now available again for Exchange Quarantine.

1.8. July 2022 (Version 6.26.2-2)

1.8.1. New Features

1.8.1.1. Integrations

- You can now integrate GravityZone data into Microsoft Azure Sentinel, allowing automatic transfer of GravityZone events to the Microsoft platform.

1.8.2. Improvements

1.8.2.1. XDR

- Added a new response action to the Incidents **Graph** and **Response** tabs: **Mark user as compromised**. This action marks the user as compromised in Azure AD Identity Protection security tool. The Azure AD and Office 365 sensor requirements have been updated to reflect the type of permissions required for this response action.
- As a Partner, you can now view and deploy sensors for all managed companies under your account.
- As an MSP, you can collect investigation packages on endpoints from any company under your management.
- User activity records are now available for actions taken in the **Sensors Management** page.

1.8.2.2. Threats Xplorer

Threats Xplorer now provides you with enriched information about each security event and possible actions that you can take, all in a single view. The new **Detection details** panel is available when selecting any event from the grid and includes the following:

- Details about the threat such as threat type and name, the action taken, the detecting module, and others.
- Details about the detected object including the category and object-specific information like process ID, file path, URL, email subject, and others.
- Endpoint details such as endpoint name, type and risk score, the assigned policy, any existing vulnerabilities or misconfigurations, and others.
- Several investigation and remediation actions like scanning or isolating the endpoint, adding exclusions for files and processes or add detected objects to the **Blocklist**.
- The option to view all the security events on a specific endpoint within the last 24 hours.
- A link to a specific endpoint within the Network Inventory.

1.8.2.3. Licensing

- Bitdefender MDR Foundations is now available as an add-on to the Bitdefender Managed Detection and Response service.
- XDR is now available as an add-on. Additional licenses need to be enabled for each type of sensor platform. When reselling XDR, all types of sensor platforms will automatically be enabled for client companies.
- License trials now offer a maximum of 50 seats.
- New trial keys are now generated with 12 characters.
- Company Administrators can now enable or disable XDR sensor categories when the XDR add-on is enabled.
- Monthly Trial licenses now include XDR and all sensor categories.

1.8.2.4. Exclusions

- 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.

1.8.2.5. 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.

1.8.2.6. Sandbox Analyzer

- As a partner, you now can see submissions from other companies in the **Sandbox Analyzer** section of the Control Center main menu. Use the search box or the new drop-down list on the page to switch from the default view of your company's submissions to those from all direct companies or from a specific company.
- In the **Sandbox Analyzer > Manual Submission** section, you can select from the drop-down list a company on whose behalf to submit samples.
- Starting with this release, you can retrieve detailed Sandbox Analyzer HTML reports via API. The **Sandbox Analyzer Results** report, which contains only a summary, is no longer deprecated.

1.8.2.7. 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.
- The company selector is available in a new format as a customizable column and filter for partner companies.
- Added new time intervals for the quarantined items.
- Renamed a few elements on the page.

1.8.2.8. Companies

- Multiple graphical elements have been modified to offer a better user experience:
 - For companies that use multiple products, only the total number of products is displayed. You can use the arrow button on the left side of the screen to display all used products.
 - Multiple buttons have been redesigned, moved, or included under the **More actions** menu.
 - Improved the page navigation.
 - Added the **Settings** menu, which allows you to customize the information displayed for each company. The menu also provides additional features, including **Reset view**, **Compact View** and a search box to find specific columns.
- Several improvements have been made to the list of companies:
 - Added additional filters.
 - A new **Show or hide filters** button is available in the upper right side of the page.
 - You can customize the filters displayed on your screen by using the **More** menu or by removing individual filters using the Remove button.
 - A **Clear** button, allowing you to revert all filter settings to default.
 - Added several columns, providing access to additional company, product, and usage information.
 - Renamed License usage to Usage Breakdown and License validity to Expiry date for improved clarity.
- The information under **Company ID** has been moved to a new field called **Company hash**. Replacing it, will be the company's database ID, which mainly used for API requests.
- Companies now have two identifiers in Control Center:
 - **Company ID**, the company identifier in GravityZone Database. Use this ID when making API requests.

- **Company hash**, previously shown in Control Center as **Company ID**. Use the hash when changing the Bitdefender partner via Control Center.

1.8.2.9. Network

- Added two new tasks in the Network > Tasks section: **Isolate** and **Remove from isolation**.

1.8.2.10. API

- You can now use the Reports API to download Sandbox Analyzer HTML reports.
- Several methods under the Companies, Licensing and Network API have been updated to support the addition of the XDR add-on.

1.8.2.11. Localization

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

1.8.3. Resolved Issues

1.8.3.1. GravityZone Platform

- Companies are now suspended when reaching subscription end date.

1.8.3.2. API

- The 201 response status code is no longer handled as an error for the Event Push Service.

1.8.3.3. Reports

- In some situations, the **Security Audit** report did not include **Advanced Anti-Exploit** events.

1.8.3.4. Risk Management

- The **Devices** grid in Security Risks used to count all misconfigurations, regardless of whether they had been marked as **Ignore risks**.

1.9. June 2022 (Version 6.26.2-1)

1.9.1. New Features

1.9.1.1. EDR

- EDR alerts in the **Incidents > Search** section now display additional information in the **JSON** tab of the **Details panel**. The key-value pairs in this tab cannot be used for building queries. However, you can copy the entire data to clipboard for ease of access in your investigations.

1.9.1.2. Licensing

- Early Access Program licenses have been reworked:
 - You can now add the license on top of any other standalone license that includes EDR.
 - The license no longer has usage limitations.

Note

Previously generated Early Access Program licenses will be invalidated. Companies currently in the program will need to acquire a new license key.

1.9.2. Improvements

1.9.2.1. XDR

- Only the first two types of attacks are now visible in the **Summary** section of the incident **Overview** tab. You may expand the list to view all types of attacks.
- The **Resources** section inside the incident **Graph** has been redesigned:
 - The resources under the transition panel are now displayed as a list under each associated alert. The list displays groups of resources, organized by type, and includes the number of items for each type. The full resource details can be accessed from each alert panel.
 - The list of resources within the alert's details panel is now collapsible, making the details easier to observe.
 - All details gathered from an email are now grouped under a single resource. Along with the information aggregated from the previously existing resources (subject, URLs, and attachments) additional information will be made available:
 - Resource type: Email
 - Email Subject
 - Email ID
 - Received on
 - Sender
 - Receiver (to / cc / bcc lists)
 - Attachments
 - URLs
- **Remote Shell** is now available for Bitdefender XDR. You can find it in the incident **Graph** tab, in the details panel of endpoints or server nodes.
- **Network Sensor** details are now available in **Configuration > Sensors Management**.

1.9.2.2. EDR

- The EDR incident page has been redesigned:
 - A floating bar is now displayed above the **Critical path** of the incident and contains two functionalities: **Search entities** and **Incident trigger**.
 - The elements of the **Incident status** bar have been rearranged and the endpoint name is no longer displayed.

1.9.2.3. 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 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.

1.9.2.4. 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**.

1.9.2.5. Policies

- You can now scroll through sections inherited from another policy.

1.9.3. Resolved Issues

1.9.3.1. Device Control

- Creating a Device Control exclusion rule with multiple devices IDs, separated by commas or space, now correctly saves all information.

1.9.3.2. GravityZone Platform

- Security fixes.

1.10. May 2022 (Version 6.26.1-2 EFX)

1.10.1. Improvements

Remote troubleshooting

- The **Debug session** now contains a troubleshooting scenario for the **Endpoint Detection and Response(EDR)** module. Using this new option, you can gather specific logs that target EDR issues such as incidents not generated, false positives, missing incidents data, and others.
- The **Content Control (traffic scan and user control)** scenario now also covers **Firewall** issues and was renamed **Content Control and Firewall**.

Note

These changes are available for Windows systems.

1.11. May 2022 (Version 6.26.1-2)

1.11.1. Improvements

Threats Xplorer

- The detection events category and action taken have a new color design necessary for future developments.

1.11.2. Resolved Issues

Configuration Profiles

- The **Modules** column in the grid area was displaying the **Unknown** status instead of **All modules** (value "3") for exclusions coming from imported lists.

1.12. May 2022 (Version 6.26.1-1)

1.12.1. New Features

XDR

- You can now request a new sensor type by accessing **Configuration > Sensors Management > Add new > Need a different sensor?**

1.12.2. Improvements

XDR

- Now you can also access the **Remote Shell** feature from the **Network** section Action Toolbar. The option becomes available once you select at least one managed device in the list.

Network Protection

- The **Exclusions** table in the **General** page includes a **Remarks** column where you can add comments for existing or new rules.

1.13. April 2022 (Version 6.24.0-3)

1.13.1. Improvements

1.13.1.1. GravityZone Platform

- Two-factor authentication (2FA) becomes mandatory for all GravityZone Cloud accounts on April 12, 2022. From now on, when logging into Control Center, you need to enter a six-digit code from an authenticator app in addition to your GravityZone credentials.

If you do not use 2FA yet, you will be prompted to set it up in a configuration page. You can skip the configuration page up to 5 times.

Bitdefender supports any TOTP authenticator compatible with the standard RFC6238, installed on devices such as smartphones and computers. [Learn how to configure an authenticator on your smartphone or computer.](#)

This update comes with the following new options:

- **Remember this device**, on the Control Center login screen. Select this option to trust the device used for accessing Control Center and to skip entering the six-digit code. Different browsers on the same computer mean different devices.
- **Allow users to remember their device**, in the **Authentication** tab of the company settings. As an administrator, use this option to configure the time interval for skipping 2FA up to 90 days.
- **Forget all remembered devices** and **Forget current remembered device**, in the account settings, to reset those devices that skip 2FA when signing into GravityZone.

Two-factor authentication cannot be disabled. In case you forget your credentials or lose your authentication device, ask your administrator to reset 2FA from your account settings.

Note

Bitdefender does not enforce two-factor authentication (2FA) to GravityZone accounts using single sign-on (SSO).

Learn more about two-factor authentication and how to enable it from [this FAQ article](#).

1.13.1.2. Public API

- Enforcing two-factor authentication brings the following changes to the public API:
 - The API calls that had the parameter `enforce2FA` set to false are now automatically set to true for `createCompany` and `updateCompanyDetails` methods. This change does not return an error message.
 - The new optional parameter `skip2FAPeriod` is available for `createCompany` and `updateCompanyDetails` methods. This parameter allows you to configure the time interval in days for skipping two-factor authentication by specifying one of the values: 0, 1, 3, 7, 14, 30, 90. 0 (zero) means this option is disabled and the user must enter the six-digit code when logging into GravityZone.

1.14. April 2022 (Version 6.23.0-4)

Minimum requirements:

- Security agents: 7.5.1.177 (Windows), 7.0.3.1982 (Linux), 7.4.10.200020 (macOS)

Important

Starting April 12, 2022, two-factor authentication becomes mandatory for all GravityZone Cloud accounts. When signing in after this date, GravityZone will automatically prompt you to configure 2FA. If you are already using 2FA or logging in with an Identity Provider, this change will not affect you. [Read more](#).

A dedicated GravityZone update on April 12 will enforce two-factor authentication for existing users. The same update will bring a new option to remember the device used for signing in, which will allow skipping 2FA for a configurable time interval.

1.14.1. New Features

1.14.1.1. XDR In General Availability

eXtended Detection and Response (XDR) consolidates security-relevant endpoint detections with telemetry from non-endpoint sources such as network visibility, email security, identity and access management, or cloud security. XDR focuses on optimizing threat detection, investigation, and real-time threat hunting.

XDR provides advanced investigation tools such as:

- The **Overview** tab - Here you can evaluate the impact of an incident on your organization, and quickly act to contain threats.
- The **Graph** tab - Here you can analyze in detail the **Initial access**, **Exit points**, as well as the **interactions** between the multiple elements of your environment, and affected resources. Every graph element provides relevant information in their details panel, as well as specific mitigation actions. The **Graph** displays data correlated from endpoint, network, productivity, identity, and cloud sensors.
- The **Alerts** tab - Here you can see in detail all the security events that make an extended incident, and search for specific events by multiple criteria.
- The **Response** tab - Here you can view and take recommended actions to mitigate threats to your organization, and analyze actions already executed from within the incident graph.

XDR also includes new powerful investigation features such as:

- An advanced **Search** feature you can use to analyze any element or company resource involved in an incident. It provides:
 - Improved data visualization.
 - Automatic suggestions for field names, values and operators when typing queries.
 - Ability to save and name search queries: they will be displayed in the **Smart views** panel. You can also edit or delete them.
 - Ability to view more details about an event using the **Details** panel.
- An interactive full **Remote Shell** feature you can use to connect remotely to any endpoint in your environment, and take immediate action to minimize threats or perform advanced forensics.
- An **Investigation Package** feature you can use to collect data from any endpoint involved in an incident. You can download and analyze data such as BEST product logs, system info, registry files, Windows, macOS and Linux event logs.

To bring all these together, XDR uses advanced correlation engines to process data from multiple sources, such as:

- The **Incidents** sensor
- The **Network** sensor
- Productivity sensors:
 - The **0365 Mail** and **Audit** sensors
- Identity sensors:
 - The **Active Directory** sensor
 - The **Azure AD** sensor
- Cloud sensors:
 - The **AWS** sensor

Important

The **Network**, **Productivity**, **Identity**, and **Cloud** sensors, as well the **Remote Shell** feature require a separate license key for activation.

1.14.1.2. Threats Xplorer

Bitdefender introduces **Smart Views**, a brand-new GravityZone feature focused on optimizing user experience by adding a new level of personalization in **Threats Xplorer**. You can now create your own customized views or use predefined ones and quickly switch between them as needed. In a single view, you can customize filters, different time intervals, add or remove columns and scale their size.

1.14.2. Improvements

1.14.2.1. 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](#).
- The **Edit Company** page has been redesigned to match the **Add Company** and **My Company** pages, providing an improved overall company management experience.
- The package configuration page includes new privacy options in the **Miscellaneous** section.
- The list of supported internet browsers has updated. [Learn more](#).

1.14.2.2. Threats Xplorer

- The company selector is available in a new format as a customizable column and filter for partner companies. Furthermore, the improved filter now helps partners analyze detection events from multiple companies all at once.
- Added a new type of detection event for dynamic malware. This uses **Fileless Attack Protection** and **Windows Antimalware Scan Interface (AMSI)** technologies integration to detect various fileless threats.

1.14.2.3. 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 is 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.

1.14.2.4. 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.

1.14.2.5. 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.

1.14.2.6. 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.

1.14.2.7. Assignment Rules

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

1.14.2.8. Licensing

- The **License Usage Limit Has Been Reached or Exceeded** and **License Limit Is About To Be Reached** notifications now apply to Email Security mailboxes as well.

1.14.2.9. Security Audit

- The report now includes an enhanced graphical evolution of all security events that occurred on the selected target. You can view each available module as a single line in the graph and all modules in the graph legend.
- The exported report in PDF format now includes a new graph that details the evolution of the **Antimalware** security events.
- Added a new event type for AMSI detections.

1.14.2.10. 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.

1.14.2.11. Public API

- A new connector is available for sending events from GravityZone to SIEMs lacking HTTPS listeners. You can use the new DEB package to deploy the connector as a service. This provides easier installation, maintenance, and upgrades. [Learn more](#).

1.14.2.12. Localization

From now on GravityZone Control Center is available in Vietnamese.

1.14.2.13. Sandbox Analyzer

Security improvements to Cloud Sandbox.

1.15. March 2022 (Version 6.22.0-1)

1.15.1. Improvements

XDR

Important

Join the **Bitdefender Early Access Program** for the opportunity to access the **XDR** improvements, ahead of everyone else. Share your feedback with us and we'll make it a priority and tailor the product to your needs. Contact [Customer Support](#) to get the key to these locked features.

- The **Sensors Management** feature now provides integration with AWS. You can configure the new AWS sensor to collect and process configuration changes and actions taken by users, roles, or AWS services.
- **Extended Incidents** now display in graph the users involved in the interaction between two incident entities as an independent identity node, highlighted with a dotted link. The dotted transition also displays the direction, to make it easy to see if the user affects or is affected by the other elements it interacts with.
- The **Graph** offers support for forensic artifacts collected by the AWS sensor from your company's AWS service.
- When the same alert is spawned in multiple **Graph** interactions, this information is now shown in its details panel, to make it easier for you to investigate.

Licensing

- The **License Expires** notification comes with the following changes:
 - Recurrence: The notification will now be sent 90, 30, 7, and 1 day before expiration, each time containing specific content.
 - Content: Details include company information, product name, the expired license keys and useful URLs.

Note

For Partners, these changes apply only to notifications about their own licenses.

Configuration Profiles

- On the **Exclusions** page, you can add and remove columns from the grid.

Patch Management

- The **Patch Management** module for Linux now installs only on [supported distributions](#).
- Linux machines now display in the endpoint details page [explicit error messages for users](#) whenever a **Patch Scan** or **Patch Install** task fails.
- The **Patch Inventory** page displays the OS type column dynamically depending on the available endpoint types (Windows or Linux).

Assignment Rules

- For location-based rules, the maximum number of IP addresses you can add in the **DNS server address** category has been increased to 30. The character limit in the corresponding field has been extended to 480.

Public API

- The **Push API** now provides additional information:
 - `modules` events now inform you if the **Network Attack Defense** module is disabled or enabled on your endpoints.
 - `network-sandboxing` events now include the computer identifier and the IDs of your **Sandbox Analyzer** submissions.

1.16. February 2022 (Version 6.21.1-1)

Improvements

GravityZone platform

- The **User Activity** page now includes details about API operations such as editing, creating, and deleting API keys.
- You can now add descriptions to your API keys from the **API keys** section under **Account Menu > My Account**.
- New endpoint packages no longer have the **Device Control** module on by default.
- New privacy options have been added in the following section of the console: **Policies > General > Settings > Options**.

XDR

Important

Join the **Bitdefender Early Access Program** for the opportunity to access the XDR improvements, ahead of everyone else. Share your feedback with us and we'll make it a priority and tailor the product to your needs. Contact [Customer Support](#) to get the key to these locked features.

- The **Sensors Management** feature now provides integration with Active Directory. The new **Active Directory** sensor can be configured to collect and process user login information.
- The **Graph** offers support for forensic artifacts collected by the Active Directory sensor from your company's AD Domain Controllers.

The alerts resulted from interactions between incident elements offer additional data about involved entities and resources, displayed in their specific side panel.

- The **Security Analytics** sensor from the menu in the **Alerts** tab will be replaced by specific sensors that have triggered alerts.
- The **XDR Search** feature now provides automatic suggestions for fields, values and operators, which appear as you type. Syntax highlighting has been added for improved readability.

The new details panel shows further information about the events in the grid, and its data can be used to further refine your search. Support for Office 365 logs is now available.

1.17. January 2022 (Version 6.20.1-2)

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.

1.18. January 2022 (Version 6.20.1-1)

Minimum requirements:

- Security agents: 7.4.2.142 (Windows); 7.0.3.1927 (Linux); 7.4.8.200007 (macOS)

1.18.1. Improvements

XDR

We upgraded the visual mechanics of the **Extended Incidents Graph** to better represent the events that have occurred within the incident you are investigating.

- Triggered alerts that were displayed on both source and target nodes are now displayed as part of the interaction between them, thus eliminating duplicates.
- The interactions between nodes is displayed as a separate graph entity that shows all the company resources that were impacted in some way by the triggered alerts.

Important

Join the **Bitdefender Early Access Program** for the opportunity to access the XDR improvements, ahead of everyone else. Share your feedback with us and we'll make it a priority and tailor the product to your needs. Contact [Customer Support](#) to get the key to these locked features.

GravityZone platform

You can now view the names of Mac users logged into GravityZone via SSH. The new information is available in the **Network** section (**Users** tab in computer details) and in the **Network Protection Status** report.

2. 2021

2.1. December 2021 (Version 6.19.1-1)

Improvements

XDR

Important

Join the **Bitdefender Early Access Program** for the opportunity to access the XDR improvements, ahead of everyone else. Share your feedback with us and we'll make it a priority and tailor the product to your needs. Contact [Customer Support](#) to get the key to these locked features.

Search

We redesigned the **Search** feature, and now it provides:

- Enriched data, including raw events to help with investigation efforts
- An extended number of suggested fields for creating queries. A list of fields with predefined values is available [here](#).
- Customizable results grid with show/hide columns functionality
- New predetermined options for the **Date** field: **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom**.

Investigation Package

The new **Investigation Package** functionality enables the collection of forensic data from your environment without requiring a direct interaction with the endpoint involved in an incident.

This feature is designed to improve your SOC team's overall effectiveness by eliminating the time-consuming and labor-intensive task of manually collecting extra incident information from endpoints, allowing your team to mitigate and contain threats faster.

You can gather forensic data by using the **Collect Investigation Package** action from the **Details Panel** of any endpoint involved in an incident.

All investigation files are available for download in the **Investigation** tab of the endpoint's full details page.

Sensors Management

The new **Sensors Management** dashboard allows you to integrate sensors from all the major cloud service platforms, which enable GravityZone to gather and correlate data into highly-accurate extended incidents.

Currently in its early stages of development and production, this new feature provides integration with the Microsoft Office 365 platform, which will soon be followed by other integrations.

The feature provides integration with the **Microsoft Office 365** platform through the **Mail** and **Audit** sensors, which boost the detection capabilities by providing metadata about email traffic and content, as well as user and admin operations retrieved from the Microsoft 365 unified audit log.

All sensors be configured and managed as separate sensor integration instances or together as part of the same instance setup.

The **Sensors Management** dashboard is available as a new tab in the **Configuration** page.

Extended Incidents

The **Graph** went through a visual update designed to improve the investigation process. It now always indicates the origin of the incident in the **Initial Access** area, and all exfiltration and command & control activities in the **Exit Points** area.

The **Graph** also provides visual representation for new forensic artifacts collected and correlated from **Microsoft Office 365** sensors, namely nodes for O365 users and O365 Mail and Audit sensor integration instances.

The new **Overview** tab displays the most impactful events of an extended incident, condensed in three major areas:

- **Summary** - A synopsis of the entire incident, including data on initial access, tactics and techniques used by attackers, and affected organization assets
- **ATT&CK Tactics and Techniques** - All the identified MITRE ATT&CK tactics and techniques used in the incident
- **Highlights** - The critical alerts from the most impactful steps in the incident kill chain

Patch Management

Maintenance Windows

GravityZone introduces **Maintenance Windows** in **Configuration Profiles**, a new and powerful way to configure Patch Management settings outside policies. The Maintenance Windows feature provides 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. As a partner, you can create and modify maintenance windows for managed companies.

Upon this release, all Patch Management settings from existing policies will automatically be moved into maintenance windows, and then assigned to each policy accordingly. 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

- Starting with this version, you can no longer configure relays with Patch Caching Server role in the policies of other companies. The Relay and the policy must belong to the same company.
- 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.

Linux Support

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)

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.

Important

This feature will be operational with the next release of Bitdefender Endpoint Security Tools for Linux.

Threats Xplorer

The export functionality is now available in **Threats Xplorer**. You can use this new option to access and manage the centralized data outside GravityZone Control Center, according to your needs. The security events are exported in the widely available CSV format, making it easier to import in other software programs tailored for your business.

Reports**Antiphishing Activity Report**

The Antiphishing Activity 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.

Important

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 Report

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.

Licensing

- GravityZone now supports multiple standard products. Products added to the same company must be compatible.
- The **My Company** page has been reworked and restructured. The page now provides an improved overall company management experience.
- Notifications regarding reaching or exceeding a license limit or a license expiring have been modified. Changes include:
 - Notification recurrence
 - Customized information for companies with multiple licenses

Partners

Bitdefender MDR For MSPs

As a Managed Service Provider (MSP) you can now benefit of automatic provisioning and billing for the Managed Detection and Response (Bitdefender MDR) service, offering you and your customers protection through outsourced cybersecurity operations 24 hours a day, every day of the year. The Bitdefender MDR service combines cybersecurity for endpoints, network, and security analytics with the threat-hunting expertise of a SOC fully staffed by security analysts from global intelligence agencies.

This service is available in two flavors:

- **Bitdefender MDR Advice** - retain full control over end customer environments, with the MDR team acting as a trusted advisor, providing curated recommendations to equip your team to respond to customer incidents.
- **Bitdefender MDR Response** - benefit of a fully-managed threat hunting solution that includes state-of-the-art prevention and expert response. The Bitdefender MDR Customer Success Team (CST) will affect real-time changes in your customer's environments when security incidents are identified, based on a set of pre-approved actions you both agreed upon.

You can activate, deactivate, or switch between service flavors by editing the company details page.

Note

If you are a Bitdefender Partner, the Bitdefender MDR Service needs to be enabled by Bitdefender. If you are an MSP interested in Bitdefender MDR, please contact your Partner.

Companies

- The **New Company** and **Edit Company** pages have been improved. Managing and displaying company licenses has been updated to support multiple licenses.
- The **Licensing** section within the add / edit company flow for the **Monthly Subscription** license option now offers you easier activation and management of the products, add-ons, and services provided by Bitdefender.
- Use the new **Own use** section to enable add-ons and services for your own company, and the **Reselling** section to grant other partners the right to resell products, add-ons, and services.

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 **Maintenance Windows API**, the following methods have been added:
 - `createPatchManagementMaintenanceWindow`
 - `getMaintenanceWindowList`
 - `getMaintenanceWindowDetails`
 - `updatePatchManagementMaintenanceWindow`
 - `deleteMaintenanceWindow`
 - `assignMaintenanceWindows`
 - `unassignMaintenanceWindows`
- The **Companies**, **Network** and **Licensing APIs** have been modified as follows:
 - Functionality for the `getNetworkInventoryItems` and `getLicenseInfo` methods has been changed.
 - The `addProductKey` and `removeProductKey` methods has been added.
 - The `createCompany`, `setMonthlySubscription`, `getLicenseKey`, `getLicenseDetails`, and `getCompanyDetails` methods have been modified to

properly display multiple standard and add-on licenses, and include information and settings on Bitdefender MDR for MSPs.

Resolved Issues

EDR

Fixed an error that in some particular cases was preventing incidents from being generated.

Firewall

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

Configuration Profiles

- Exclusions imported from larger CSV files no longer go under All exclusions, but in your newly-created list.
- Exclusion lists created by the current user are now displayed only in the **My lists** section. They will no longer be added to the **Default exclusion lists**.

Partners

You can now search by company in **Add Company** page.

Known Issues

Partners

The **License key**, **License usage** and **License validity** columns in the **Companies** page will only display a company's first license key for standard products if the company has multiple base products.

2.2. November 2021 (Version 6.18.1-2)

Improvements

- Improvements made to back end code in preparation for future updates. Changes will have no direct impact on users.

Known Issues

- Starting with version 6.18.1-1, clicking the **License key**, **License validity**, **Subscription end date** or **Auto-renewal** column headers in the **Companies** page no longer reorders the list of companies.

2.3. October 2021 (Version 6.18.1-1)

Minimum requirements:

- Security agents: 7.3.2.44 (Windows); 7.0.3.1803 (Linux); 7.2.6.200017 (macOS)

Improvements

XDR

- XDR now includes a full interactive **Remote Shell** feature that enhances your SOC experts' investigation capabilities. It enables access to any endpoint in your environment, to gather forensic data and respond swiftly to mitigate and contain any suspicious activity. You can access this full interactive shell from the side details panel of any endpoint involved in an incident.
This added functionality is compatible with Windows, Linux, macOS.

Note

For now, the new **Remote Shell** functionality is available through the **Bitdefender Early Access Program**, which you may join by contacting [Bitdefender Enterprise Support](#).

The **Bitdefender Early Access Program** will provide exclusive access to many of the new GravityZone feature releases going forward.

Threats Xplorer

- **Threats Xplorer** now automatically retains the columns size selection and displays it accordingly when you return to the page. Additionally, we have also made several adjustments to the default columns size for better visibility.
- Added the new filter and column **SHA256** that helps you easily identify a file hash.

Partners

- The **New Company** page has been improved and the procedure to create a new company has been changed. For more information, refer to [Creating companies](#).
- **Trial companies** now start with a GravityZone Elite license equivalent and several add-ons, providing access to additional GravityZone features. For more information, refer to [this page](#).

2.4. September 2021 (Version 6.16.1-7)

Improvements

Platform

- A new option, **Automatically copy the label of the Relay to connected endpoints, if not specified otherwise**, is now available in the **Configuration > Network Settings** tab. This helps you to manage the labels according to your preferences and choose whether the endpoints connected to a relay should inherit its label or not.
- Agent packages names now include the product version.
- You can now find the GravityZone Cloud version under the **What's new** section .

Antimalware

- You can now automatically resume on-demand scan tasks using the **Resume scan after product update** option. To enable this select the option checkbox from the **Options > Miscellaneous** section when you create or edit a scan task.

Network Protection

- You can now enable **Scan SSL** for **RDP** protocols.

2.5. September 2021

Resolved Issues

Executive Summary

- In some situations, generating an **Executive Summary** report resulted in crashes for companies with an exceptionally high number of events.
- In some cases, generating the **Executive Summary** PDF file led to crashes. The issue is now fixed.
- The **Monitoring** section failed to display its subsections when hovering over it while the GravityZone menu was collapsed.

Policies

- The **Allow endpoints to send user login data to GravityZone** option was not properly inherited from the main policy.

2.6. August 2021

New Features

Executive Summary report

- The new report focuses on improving data accessibility while centralizing key security information from the **Executive Summary** page. You can easily export, schedule, and download the report from both the **Reports** and **Executive Summary** sections.

Improvements

GravityZone platform

- To help you monitor, analyze and quickly identify valuable information we are introducing **Executive Summary** as the new landing page for GravityZone Control Center. You can adjust this setting to your preference at any moment from the **My Account** section.

2.7. July 2021

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.

Improvements

Advanced Anti-Exploit

- **Advanced Anti-Exploit** feature is now available for Linux.

Network

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

2.8. June 2021

Minimum requirements:

- Security agents: : 7.2.1.60 (Windows)

Improvements

GravityZone platform

- Now you can view the names of all active users logged on endpoints running Windows. This feature brings changes in the following sections of Control Center:
 - **Network** – the Network grid includes a new searchable column named **Users** and the endpoint details window displays a dedicated tab also named **Users**.
 - **Reports** – the Network Protection Status report includes a searchable column named **Users**.
 - **Policies** – a new check box in **General > Settings > Options** allows you to enable data collection. The information sent by endpoints to GravityZone includes usernames, login time and the login method.

This feature can serve you in multiple ways:

- As a GravityZone administrator, you can use the provided information to reach out to the endpoint users in case you need their input.
- As a Security Analyst, you can correlate the information about the username with other events from GravityZone or 3rd party systems.
- As a partner, the user-related information is helpful in situations such as when you create a Monthly License Usage report for audit purposes.
- Renamed a few elements from the following sections:
 - **Threats Xplorer** - the columns **Device name** and **Device type** are now **Endpoint name** and **Endpoint type**.
 - **Network** - the column **Machine type** is now **Endpoint type**.
 - **Executive Summary** - the **Threats breakdown by machine type** widget is now **Threats breakdown by endpoint type**.
- **User Activity** page now informs if a user has logged in GravityZone from a third-party platform with which it is integrated.
- 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 disregard the 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.

You can use name patterns of any length.

Improved the offline machines cleanup rules so that you can now use the question mark (?) as wildcard and select targets that are offline for less than 24 hours.

EDR

- GravityZone extends the endpoint-based threat detection capabilities of the traditional EDR by incorporating network incidents, to successfully counter advanced threats no matter where they emerge in the infrastructure: on endpoints, network or in the cloud. This new EDR component combines the most advanced prevention capabilities, low overhead cross-technology correlation capabilities and Network Traffic Analytics to boost the cyber resilience of your organization.

In this new light, the **Incidents** page has been enriched with the **Extended Incidents** tab, to display all organization-wide incidents which require further investigation.

The new graphic representation of extended incidents makes it easy to view and investigate the evolution of a complex attack within your network:

- It includes a detailed timeline of events, displaying the network point of entry, evolution over time, lateral movement and communication with outside agents.

- It correlates events gathered by Endpoint Detection and Response and Network Traffic Analysis technologies.
- It associates extended incidents with any detected endpoint incident that makes a potential staged attack.
- Concurrently, if you are using a 3-rd party ticketing platform or a PSA solution, you will enjoy an enhanced experience through the new redirect links. Clicking on the embedded links will either:
 - direct you to the **Endpoint Details** page in GravityZone, when you are working on a security incident.
 - direct you to the **Incidents** section of that specific incident ID in GravityZone.

Threats Explorer

- The available filters now dynamically adjust to your company's license type. This way, you can quickly use search and filtering criteria relevant to your company and obtain better results.

Note

The filters and detection events are available up to 90 days after you change the protection layers. Following this period, the events are deleted and the filters automatically reflect the available features according to your license key.

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 ARM. The new downloader automatically detects the processor type and downloads and installs the right kit for that specific architecture.

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

- Network API: The result of the `GetNetworkInventoryItems` method now includes the `policyId` and `moveState` fields.

Resolved Issues

ERA

- An overflow of records in the CVEs inventory collection downturned the **Indicators of Risk** query.
- The **Risk Management** data removal step from the **Security Risks > Devices** section was skipped when BEST uninstall presented errors. The device still appeared to be present in the devices listed with vulnerabilities.
- Following a **Risk Scan**, the **Risk Management** module displayed users as having a high severity score, even if the human risks had been fixed through a previous Risk Scan.

Patch Management

- Previously installed patches were not displayed in GravityZone after manually rebooting a Virtual Machine.

MSP > Partners

- The **Reconfigure Task** failed when trying to add the **Exchange** module to endpoints from two different companies - with the same configuration - and displayed the error message "Task could not be created. Some task settings could not be applied to all selected product types".

2.9. May 2021

New Features

Threats Xplorer

Threats Xplorer offers you a highly increased visibility over the detected threats in your network and helps you perform a concise security analysis. The feature centralizes detection events from multiple GravityZone technologies and classifies them by category, threat type, remediation actions, and many others.

Threats Xplorer makes it easy to identify and analyze threats by providing you with:

- A wide variety of customizable columns with detailed information
- Diverse filtering and search criteria
- Detection events from various modules centralized in a single list
- Infinite scroll functionality for seamless interaction

Improvements

Executive Summary

Executive Summary now provides you with the possibility to explore multidimensional data, by browsing from a statistical level to a more granular and detailed view.

The new drill-down capability helps you navigate instantly from widgets to specific sections of the Control Center. Each section displays complex information in a customized way so that you can identify and analyze with ease the aspects you are interested in.

2.10. April 2021

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
- 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.

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.

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, GravityZone Business Security Enterprise Plus, and GravityZone Cloud Security for MSP.

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.

ERA

- The **App Vulnerabilities** details panel now allows you to view the devices impacted by a vulnerable application discovered in your environment.
When you select a vulnerable application and click the **View Devices** button it will take you to the **Devices** section and display a list of all impacted devices.

Email Security

- You will now know when the GravityZone Security for Email license expires. Just make sure to enable the notifications in the **Notifications** page.

EDR

- The **Incidents** page now displays suspicious events in the **Endpoint Incidents** tab, and events detected by prevention technologies, in the **Detected Threats** tab.

Public API

- Packages and Network APIs: Added the `productType` parameter to `createPackage` and `createReconfigureClientTask` methods. This parameter is optional and states the operation mode of the agent: EDR (Report only), or Detection and prevention.
- Event Push Service API:
 - The `taskType` parameter for **Troubleshooting activity** notification is now a string and can have the following values: `Gather Logs` and `Debug Session`.
 - Enforced TLS 1.2 encryption.
 - Enforced the use of an authorization header when selecting JSON-RPC format.

Resolved Issues**Patch Management**

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

2.11. February 2021

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.

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

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 (\).

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.

MSP & Partners

- Changing the product type in the company configuration page triggers a warning message that recommends users to reconfigure the security agents accordingly before the existing product expires on endpoints.

The new notification **Product type has changed** reminds users the same details and it is sent seven, three and one day before the grace period ends.

- The **Monthly License Trial** license type now includes Bitdefender EDR feature, so you can enjoy the full GravityZone experience.

Sandbox Analyzer

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

Reports

- The **Antiphishing Activity** report provides more clarity as it now includes the action taken on each event (**Blocked** or **Detected**), when clicking the number in the **Detected Websites** column. The action is also specified in the **Antiphishing event** notification.
- The **Security Audit** report includes a new event type, **Detected Website**, which is available in the report details and in the CSV file.

Resolved Issues

Packages

Fixed a minor issue where Customer companies could select another company in the network when creating an installation package.

MSP & Partners

Fixed an issue where Partner companies with **Monthly License Trial** could not create trial child companies because of missing **Product Type** options.

3. 2020

3.1. November 2020

New Features

Executive Summary

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

Bitdefender introduces **Executive Summary**, a feature specially designed to facilitate these aspects.

As part of the Control Center Dashboard, **Executive Summary** presents a concise security overview of all protected endpoints in your network. Composed mostly of widgets, it provides details about endpoint modules, detections and taken actions, threat types and techniques, your company risk score and many others.

Ransomware Mitigation

Vaccines give you immunity, but what happens when they come too late? Powered by proactive and award-winning detection technologies, **Ransomware Mitigation** offers an early solution to ransomware attacks. It detects the attack as it happens, blocks it regardless it was run locally or from a remote endpoint, and then recovers the files encrypted so far.

Find the **Ransomware Mitigation** settings under the Antimalware < **On-Execute** policy section.

After applying protection on endpoints:

- You will receive notifications whenever an attack takes place.
- You can view details about the ransomware attacks and recover encrypted files in the **Ransomware Activity** page.
- You will view such events in the **Security Audit** report.

Note

Available with GravityZone Business Security, GravityZone Advanced Business Security, GravityZone Business Security Premium, GravityZone Business Security Enterprise, GravityZone Cloud Security for MSP.

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.

Improvements

EDR

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

Incidents

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.

eXtended Detection and Response (XDR)

XDR successfully stops attacks and increases the cyber resilience of your organization. It combines the most advanced prevention capabilities, low overhead EDR (Endpoint Detection and Response) and Network Traffic Analytics. GravityZone extends the endpoint-based threat detection capabilities of a traditional EDR by incorporating network incidents (XDR) to successfully counter advanced threats no matter where they emerge in the infrastructure: on endpoints, network or in the cloud.

In this new light, the Incidents page has been enriched with the Extended Incidents tab to display all organization-wide incidents which require further investigation. The new graphic representation of extended incidents makes it easy to view and investigate the evolution of a complex attack within your network:

- It includes a detailed timeline of events, displaying the network point of entry, evolution over time, lateral movement and communication with outside agents
- It correlates events gathered by Endpoint Detection and Response and Network Traffic Analysis technologies
- It associates extended incidents with any detected endpoint incidents that make a potential staged attack

Note

Available with GravityZone Business Security Enterprise Plus

ERA

- The new **Industry Health Modifier**, an adjustment mechanism that increases the accuracy in calculating your overall company risk score by taking into account known CVEs discovered in your environment, which have already been exploited in your line of business.
- The new widgets displaying the number of scanned users and total devices that are being monitored.
- The **Top Human Risks** widget has been relabeled as **Top User Behavior Risks**.
- The **Top Vulnerable Users** widget has been relabeled as **Top Users by Behavior Risk**.

MSP & Partners

As a Bitdefender partner, you can now assign a certain product type for companies with monthly subscription. The following product types are available:

- Endpoint Security, the fully-featured security solution, with all modules available for deployment on endpoints.
- Bitdefender EDR, the lightweight EDR solution, which can run along any third-party endpoint protection platform. [Learn more](#).

A company, either Partner or Customer, may use in its network only one of the above-mentioned product types.

You can create installation packages, apply security policies, and generate reports based on the product type.

Notifications

The name of **License Usage Limit Has Been Reached or Exceeded** notification has been changed to **Deployments have reached or exceeded license limit** to better reflect its content.

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).

For more information and for the list of compatible features, refer to [Bitdefender support for macOS Big Sur](#).

Public API

- Added API support for handling product types in the following methods:
 - Companies API: `createCompany`
 - Licensing API: `setMonthlySubscription`, `getMonthlyUsagePerProductType`, `getLicenseInfo`.
Note that `getMonthlyUsage` is to be used only for the Endpoint Security product type.
 - Packages API: `createPackage`, `getPackageDetails`
 - Network API: `getNetworkInventoryItems`
- Companies API: Added the `industryModifier` indicator at `riskScore` in the `getCompanyDetails` method.
- Network API: Added `endpointName` as filtering option for the `getEndpointsList` method.
- Event Push Service API:
 - Enforced TLS 1.2 encryption for Event Push Service API.
 - Enforced the use of an authorization header when selecting JSON-RPC format.

Note

These enforcements are in place only for new users. Existing users benefit from a grace period and can make the necessary changes by the end of March 2021.

Find the details in the [API documentation](#).

3.1.1. Resolved Issues

Exchange Protection

In some cases, clients were missing Exchange credentials from Control Center.

Localization

Control Center in Korean displayed an improper string of characters in the PDF reports.

Removed Features

Security

Starting with this release, in keeping with industry standards and best practices, Bitdefender will disable obsolete communication protocols and ciphers (TLS 1.0 and 1.1) between agents and Control Center. For more information refer to [How to upgrade to TLS 1.2 and why it's crucial for Bitdefender Endpoint Security Tools functionality](#)

Known Issues

BEST installation

The following issues may arise when using Control Center with TLS 1.2 and an outdated BEST Linux agent:

- Download issues, when trying to install BEST either manually or remotely:
 - The kit generates some errors when downloading installation files
 - Install agent task does not show any status in Control Center
- Modify issues, when trying to download the package from the Update Server:
 - Reconfigure agent task status is not reported
- Removal issues:
 - No status is shown for the Uninstall task
 - After a successful uninstall, Control Center still shows the endpoint as being installed

3.2. September 2020

New Features

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).

Improvements

ERA

- New widgets in the **Risk Management** dashboard to show you how many users and devices were scanned across your network.

MSP & Partners

- As a Bitdefender Partner, you can now disable seat reservation for Partner companies. The option is available unless the company has minimum usage configured.
- As a Partner with monthly subscription, you will have access to a more detailed view of the GravityZone Security for Email activity in the dashboard of the companies under your direct management (Example: see the sender/receiver/attachments etc).
- Added an error message when trying to move a company with minimum usage under a Partner with fewer license seats.

Maintenance

- Forget about redeploying the agent to apply a fix from an update. Just run the new **Repair** task in the **Network** page.

Notifications

- The new notification **Partner Changed** informs you when a managed company has moved under a different Partner.
- **License Usage Limit Has Been Reached** now includes the list of the unlicensed endpoints within the past 24 hours due to license limit exceeding.

Public API

- EDR events are now available via Push API in JSON, CEF and Splunk formats. For this purpose, we added `new-incident` to `subscribeToEventTypes`. For more information, refer to the GravityZone [API documentation](#).
- `getInstallationLinks` and `downloadPackageZip` now provide full installation kits.
- As Bitdefender Partner, you can now remove slot reservation for all child companies with one API call. For this purpose, set the new parameter `removeReservedSlots` in `setMonthlySubscription`.

3.3. March 2020

New Features

Single sign-on (SSO)

Added single sign-on (SSO) authentication capability using the SAML 2.0 standard. The SSO options are available as follows:

- In the new **Configuration > Authentication Settings** page, for your company.
- In the **Companies** page, for companies you manage.
- In the **Accounts** page, for GravityZone users.

Incidents

The GravityZone Bitdefender Security bundle now includes the Incidents feature, where we provide the Root Cause Analysis of threats detected and blocked by our preventive technologies, with complex incident filtering options and graphic representation of incidents, as well as isolation, blocklisting, and remote connection capabilities.

Improvements

EDR

EDR introduces the Scan for IOC technology, enabling you to scan your environment for known indicators of compromise in real-time and generate detailed reports.

The Incidents page went through a significant visual and functional transformation, enhancing your experience when analyzing threats in your environment, as follows:

- The new **Overview** bar displays open incidents, top alerts, techniques and affected devices, as well as specific filtering capabilities
- The incidents list is now a fully customizable filterable grid with add/remove columns, for easier content management.
- The **Change Status** menu introduces the option to mark incidents as false-positive and leave bulk notes for later consultation.
- The detailed information for each incident, and their graphic representation and timeline, are now available in quick view mode.

- The **Graph** tab unravels a multi-phase representation of staged attacks, as well as in-graph search capabilities.
- The **Node Details** panel is now grouping information into more meaningful categories. Above that, the panel is fully expandable, to improve readability.

Endpoint Risk Analytics

- Endpoint Risk Analytics introduces the remediation of Common Vulnerability Exposures of applications currently installed in your environment.
- The **Risk Management** dashboard has been completely redesigned to improve visualization and enhance your experience while assessing the overall level of risk your company may be facing.
- The company risk score is now calculated by taking into account a wide list of indicators of risks and known application vulnerabilities, showing you its evolution in time.
- The new score breakdown, and top misconfigurations and vulnerable application widgets make it easier to see where your environment is more vulnerable to attacks and which devices are affected the most.
- The devices by severity widgets show you exactly how impacted by risks and vulnerabilities are the servers and workstations under your management.
- The new **Security Risks** page provides complex filtering options for indicators of risk, application vulnerabilities and devices. Risks in each category can be easily mitigated through the recommendations and actions provided in their Details Panel.
- The **Companies View** page is a new feature included in **Endpoint Risk Analytics for MSP**, providing a comprehensive overview of the overall risk faced by every company under your management, making it easy for you to assess and eliminate risks separately for each of your customers.

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.

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.

Network Inventory (MSP only)

- Partners (Company Administrator and Partner roles) are now able to move endpoints directly between the companies they manage by dragging and dropping endpoints in the **Network** page.
- More comprehensive error messages when moving companies under other Partners.

Firewall

We eased Firewall configuration with the new option to import and export rules.

Full Disk Encryption

You can now set rules to exclude drives from encryption.

Remote troubleshooting

- GravityZone introduces Bitdefender Cloud as a new storage option for collected logs.
- Remote troubleshooting is now available for Security Server Multi-Platform.
- You can now restart a troubleshooting session while maintaining its previous settings.

Monthly subscription trials

Two new trial options: **Monthly License Trial** (Partners only) and **Monthly Subscription Trial**. Trial companies have access to all features and add-ons available with GravityZone Cloud Security for MSP. The **Monthly License Trial** is valid for 45 days and covers 25 endpoints.

Reports

The Monthly License Usage report includes significant enhancements to simplify add-ons billing per usage:

- Displays usage and status for all add-ons, including the latest ones, such as Patch Management, Security for Virtualized Environments (Virtual Servers and Virtual Desktop Infrastructure), Advanced Threat Security, and Endpoint Detection and Response.
- Provides more information on each company's type and monthly subscription and each endpoint installed modules, like Network Attack Defense and Advanced Anti-Exploit.
- Includes the option to generate the report only for direct companies, ignoring their child companies.
- The report has some columns renamed. If you use the CSV file to extract usage information into external systems, please see the details [here](#).

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.

Two-factor authentication (2FA)

We moved the 2FA settings of your company in the new **Configuration > Authentication Settings** page.

What's New

Rushing to solve a problem and What's New stays in the way? No more. We wrapped it gently in a gift box next to the **Notifications** icon. It will showcase the new features in a compact side panel.

Amazon EC2 Integration

Added hourly billing support for the new EC2 instance types.

Event Push Service AP

- New agent-related events for all supported operating systems are now available via JsonRPC, CEF and Splunk. These events refer to agent installation/removal, endpoint move, and hardware ID changes.
- Added detection timestamps to antimalware (`av`) and Advanced Threat Control (`atc`) events. The field is named `BitdefenderGZDetectionTime`.

Removed Features

Reports

Removed the Malware Activity report. You can use the Security Audit report instead.

Dashboard

Removed the Malware Activity portlet.

Antimalware

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

Resolved Issues

Content Control

Policy inheritance did not work for specific web categories.

3.4. January 2020

Improvements

HyperDetect

Added the following details to the HyperDetect Activity notification:

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

Public API

Bitdefender Partners can now use the Companies API to enforce two-factor authentication. For this purpose, the following methods have been updated: `createCompany`, `updateCompanyDetails` and `getCompanyDetails`.

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.

For more information related to this subject, refer to this KB article [Windows XP and Windows Server 2003 support announcement](#).

4. 2019

4.1. November 2019

Improvements

Amazon EC2 integration

- GravityZone now replicates the instances inventory from region EU Stockholm.
- The hourly billing engine for AWS Marketplace subscribers now includes all newer EC2 instance types.


Endpoint Risk Analytics (ERA)

- Added new [Indicators of Risk](#):
 - Macro settings for Microsoft Office applications
 - Credential storage for several applications including some of the most popular browsers and email management tools out there
- Added new recommendations to better manage Local Group policies.

EDR

- Updated the **Add URL as exception** action button to change dynamically into **Add IP as exception**, when the domain node is an IP instead of an URL.

Network Inventory

- A new type of entities in Network Inventory: golden image 

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 hasn't granted the agent permissions such as access to the disk drive.

Public API

- You can now check the usage of the following features:
 - Security for Virtualized Environments (Virtual Servers, and VDI)
 - Advanced Threat Security (HyperDetect and Sandbox Analyzer)
 - Patch Management
 - GravityZone Security for Email
 - EDR

For this purpose, use the `getMonthlyUsage` method.

- The `getAccountsList` method now returns details about 2FA status.

Resolved Issues

EDR

- Incident graph was moving outside the display area when **Hide nodes** was used.
- **More details** button in **Navigator** menu no longer worked when closing the **Node Details** panel.
- Command lines were not displayed properly in the **Node Details** panel.
- Adding an exception for a domain node (by clicking the **Add URL as exception**) would not work when the domain was an IP/Mask instead of an URL.
- Clicking a notification for a new EDR incident was causing an error.

ERA

- **Indicators of Risk** lane was not loading in Full-screen mode.
- Some IOR rules were not being displayed properly in the **Device Risk Lane > Details** section.

Email Security

- Email addresses of previously deleted users were not available to new accounts.
- GravityZone Security for Email was unavailable to Partners when the Manage Companies rights were missing.
- Added links to guides in the **Help & Support** page.

Device Control

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

Localization

- Some texts and images were untranslated.

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.

Reports

- Duplicates of some scheduled reports were sent to email.

4.2. October 2019

Last revised: 2019-10-16

Minimum agent version: 6.6.11.159

Minimum Security Server Multi-Platform version: 6.1.71.8593

New Features

Email Security

New GravityZone Security for Email service with complete email flow control and protection against spam, targeted phishing and impersonation attacks. Email administration incorporates management and analytics tools.

GravityZone Security for Email management provides the following:

- Deployment through domain MX record redirect.
- Customizable policy engine to control email delivery and filter messages through a comprehensive rule builder.
- Company-wide quarantine.
- Connection rule configuration to monitor connection attempts to or from your mailboxes.
- Safe and Deny lists configuration for companies or individual users.
- Mailbox synchronization through Azure Active Directory and manual import.
- DNS record configuration with support for SPF, DKIM and DMARC.

The Analytics section delivers:

- Real-time visibility through email flow charts, rules triggered, and actions taken.
- Customizable reports for specific events.
- Scheduled reports and alerts for specific rules, actions or content

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.

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.

Improvements

EDR

The **Incidents** page went through a major visual and functional makeover, now providing enhanced investigation capabilities.

The **Graph** tab displays the critical path and all side elements in a fit-to-screen vertical tree. Plus:

- An interactive incident graph behavior with highlight of node and alternate path to endpoint on mouse-over, and same type elements grouped in expandable clusters.
- The **Filters** and **Navigator** floating menus that allow easy customization and navigation of the incident map.
- **New Node Details**, **Incident Info** and **Remediation** side panels with collapsible sections that provide information for each element, actions and recommendations to mitigate an attack.
- Suspicious and malicious nodes now display alerts in their details panel, describing what was detected and how it might be exploited, in accordance with MITRE tactics and techniques.

The **Remote Connection** tab is now available as an action button on the endpoint node's details panel.

- Anomaly Detection - a baselining module that spots anomalies in how the system is functioning
- Network Attack Defense – a new security layer that identifies network-specific breaches
- Advanced Anti-Exploit – a recently released security layer that detects the most evasive exploits
- AMSI - detections made by the Windows Antimalware Scan Interface (AMSI)

Two-factor authentication (2FA)

With this update, two-factor authentication is enabled by default when creating a company. When disabling 2FA, you will be prompted with a confirmation message before the changes come into effect.

Company accounts

MSP partners now have the option to add up to five custom fields in their **Monthly License Usage** report for storing third party or other custom data and facilitating billing automation.

A new page is now available under **Companies > Custom Fields**, with two sections where you can manage and import data for these fields. You can view the custom fields also when creating or editing a company.

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 new **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 Protection.
- **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.
- The **Indicators of Risk** (IOR) have been reclassified into new and more meaningful categories for increased efficiency in risk analysis and management.

Sandbox Analyzer

- 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**.

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. Plus, 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.

Reports

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

Policies

- MSP partners can enable GravityZone Security for Email and get the usage report via the public API.
- All GravityZone reports are now available via API as well.
- We have made some improvements here and there:
 - `createReconfigureClientTask` is updated with the latest changes
 - `getManagedEndpointDetails` returns all installed modules on a managed endpoint
 - `setMonthlySubscription` allows Bitdefender Partners to revoke seat reservation from companies with monthly licensing
 - `getQuarantineItemsList` has new filtering options

Resolved Issues

Policies

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

Notifications

Some partners were receiving daily **License Expires** email notifications against their notification settings. We added a new option to filter managed companies that may trigger such notifications.

4.3. June 2019

Last revised: 2019-07-17

Minimum BEST version: 6.6.11.159

Minimum Security Server Multi-Platform version: 6.1.71.8593

New Features

Endpoint Risk Analytics

This update brings Endpoint Risk Analytics, a brand-new feature designed for effectively identifying, assessing and remediating endpoint weaknesses. GravityZone exposes this new feature in the following areas:

- **Risk Management** policy section, including a risk scan scheduler.
- New **Risk scan** task available from the **Network** page.
- **Risk Management Dashboards**, providing several panels with risk information, one-click resolve action per endpoint and recommendations for exposure mitigation.

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 Applications, Endpoint Module Status reports.

Note

This security layer addresses Windows-based systems.

Antimalware

Implemented a new Load Balancing mechanism between endpoints, protected through BEST with Central Scan and Security Servers. You can now choose to distribute the load evenly between the assigned Security Servers.

Improvements

EDR

- Added full support for incidents detection and response actions, root cause analysis and MITRE events on Linux OS endpoints.
 - Enriched the **Search** section with several predefined queries, covering the most useful investigation scenarios.
- Improved security event visualization from the **Search** page:
- New panel in the Graph area displaying the actions and their states for the selected event node in a single view.
 - New **Further Investigation** section in the node details area, outlining the additional analysis through Sandbox, Virus Total and Google.

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.

Antimalware

- A major increase of the scanning speed in VDI environments due to the new scan cache sharing protocol between Security Servers. To benefit of this feature, enable port 6379 to allow traffic between Security Servers.
- Two new statuses for Security Server load: **Near overloaded** and **Near underloaded**.
- New custom exclusion types by file hash, certificate thumbprint, threat name, and command line.

- Ability to define custom exclusions by using wildcards:
 - Asterisk (*) for one or more characters.
 - Question mark (?) for a single character.
- New option to add folder exclusions for ATC/IDS. With this release, existing folder exclusions remain configured for On-Access and On-Demand scanning. To add ATC/IDS as well, you need to select the corresponding check box in the **Modules** column.

Security for Storage

You can now use a secured connection between Security Servers and the protected NAS servers, provided they use SSL over ICAP.

Usability

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

Update System

Replaced the Antimalware signatures with a new method to identify known and unknown malware, called **Security Content**.

Resolved Issues

Sandbox Analyzer

Analysis results from a manual submission could not be retrieved if the 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.

Network

Removed the ghost folders that appeared on some Partner accounts.

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 thumbprint exclusions are not available for ATC/IDS.

4.4. March 2019

Improvements

EDR

- **Live Response via Terminal Sessions**

Establish remote sessions with endpoints from GravityZone Control Center and execute commands in real-time on their operating system:

- Use the **Remote Connection** tab added to each incident page to establish a terminal session with the involved endpoint.
- Run commands on endpoint in the terminal session to remediate the threat immediately (delete files, terminate processes) or collect data for further investigation (list files, processes, registry keys information).

- **Leverage the network isolation action to all Windows operating systems**

The **Isolate** action for endpoint nodes in incident views is available now for both Windows desktop and server operating systems, whether if the Firewall module is available on the endpoint or not.

- **Better visibility on important incidents**

Two new tabs added to the **Incidents** page help you discriminate between incidents requiring immediate action and the threats already blocked by Bitdefender. All suspicious activity requiring action and investigation appears under **Investigate** tab, while the **Review** tab reveals threats contained by automatic block actions.

- **Select and edit multiple incidents at once**

New option to change the status of multiple incidents at the same time from the **Incidents** page. You can select multiple incidents while navigating through several entries, and then easily change their status using the **Bulk Operations** button.

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 now takes ownership for macOS boot drives encrypted with FileVault.

Sandbox Analyzer

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

Windows Defender ATP Integration

- A new and optimized integration flow based on Microsoft Azure Active Directory, replacing the existing one. If you have an active integration, follow these [guidelines](#).
- New event types (Process create, User session, and Network connections).
- Added response actions from Windows Defender Security Center (Trigger remote scan, Isolate machine).

Important

Future updates related to this integration will be available only for GravityZone Business Security Enterprise. If you want to receive these updates, consider upgrading your GravityZone solution.

Notifications

- You can now receive notifications for license usage on servers.
- Syslog events are now available in Common Event Format (CEF) via Event Push Service API.

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.

Usability

- Improvements in policy assignment and deployment troubleshooting.

Deprecated Features

- The **Malware Activity** report has become deprecated. The malware information from this report will be moved to another report in a future update.

Resolved Issues

- Corrected the error messages displayed when creating the AWS integration with incorrect ARN / external ID.
- Several minor bug fixes regarding GravityZone Control Center functionalities.

4.5. February 2019**Improvements****Sandbox Analyzer**

- New perspective on submissions
 - Advanced reporting interface, in the main menu, offering a single pane of glass view with all samples that were submitted to Sandbox Analyzer.

The info cards based interface adds detailed information about each submission like:

 - Sample name.
 - Submission time.

- Submission type – automatic or manual.
- Source – endpoint name.
- Analysis result – clean, infected or unsupported.
- Severity score – shows how dangerous the sample is.
- Files and processes involved into sample's actions.

Each card includes a link to a submission report, where you get even more data.

- While displaying all new submissions, the reporting interface shows the old manual submissions made before this update as well.
- In time, as adding more functionality to it, this reporting interface will replace the **Sandbox Analyzer Results** report, which from now on has the status deprecated.
- As MSP, you view in this interface only your own company submissions. Submissions of Customer companies are available in the **Sandbox Analyzer Results** report. Also, with this release, the **Sandbox Analyzer Detection** notification points to:
 - The new interface for submissions of your company.
 - The **Sandbox Analyzer Results** report for submissions of Customer companies.
- New manual submission options
 - You can use these new options when submitting samples:
 - Submit URLs.
 - Define command-line arguments for sample analysis.
 - Set a time limit for analysis execution, the number of reruns and the internet access during analysis.
 - Exclude samples previously analyzed.
 - The **Manual Submission** page is now accessible from the main menu and from the new reporting interface.
- User interface improvements at automatic submission in the security policy settings.

Public API

- HyperDetect events are now available in Event Push Service API.
- Improved the mechanism of generating API keys. You will notice significantly longer API keys. The existing API keys continue to work as before this update, but it is recommended to replace them with new ones.

Resolved Issues

- In some situations, GravityZone administrators could not modify security policies because the **Save** button was disabled.
- Improved the error message for AWS integration when using invalid ARN or ExternalID.
- Addressed a security issue that could affect manual submission to Sandbox Analyzer.
- Sometimes, Control Center was displaying inconsistent encryption status for the same endpoints.