CHECK POINT

24 June 2026

EVENTS & AIOPS

Administration Guide

Contents

1. Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point Events & AIOps Administration Guide

Latest Version of this Document in English

Open the latest version of this document in a Web browser.

Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Feedback for Events & AIOps Administration Guide Please help us by sending your comments.

2. Revision History

Date	Description
17 June 2026	Added Appendix B - AIOps Metrics Repository *(on page 119)*.
28 May 2026	Updated Supported Asset Versions *(on page 62)*.
21 May 2026	Added Supported Asset Versions *(on page 62)* in prerequisites for AIOps on-boarding.
7 May 2026	Added Connectivity Requirements *(on page 63)* from user environment to enable data transmission to AIOps.
29 April 2026	Added AIOps **Alerts** table. See Appendix A - AIOps Alerts *(on page 111)*
7 April 2026	Updated product name and product grouping to align with the new Check Point strategic pillars and portal navigation. No functional changes were made. Infinity Events is now referred to as **Check Point Events & AIOps**.
12 March 2026	Added **Health Over Time** widget AIOps AIOps - Overview *(on page 70)* page.
27 January 2026	AIOps updates: • Added Insights *(on page 93)* page. • Added CloudGuard *(on page 87)* tab in **Asset Dashboard** page. • Added new widgets **Last Day Summary** and **Health Over Time** in AIOps - Overview *(on page 70)*.

Date	Description
6 August 2025	• Added these in the **Overview** page: ◦ Threat Prevention Attacks *(on page 20)* ◦ Overview Dashboard for MSPs *(on page 21)* • Updated Licensing the Product or Start a Trial *(on page 15)*.
28 July 2025	AIOps updates: • Updated AIOps onboarding procedure. See Onboarding AIOps (Automatic Mode) *(on page 62)*. • Updated Alerts *(on page 91)* page. • Updated widgets in Overview *(on page 70)* page.
21 May 2025	Added SASE to Supported Products *(on page 11)*.
17 April 2025	Added: • Threat Prevention dashboards. See Threat Prevention *(on page 98)*. • **Threat Prevention Summary** in Reports *(on page 40)*.
4 February 2025	Added AIOps - Introduction *(on page 61)*.
19 December 2024	Added the option to generate reports on demand. See: • Reports *(on page 40)* • Reports for MSPs *(on page 48)*
15 October 2024	Added Reports for MSPs *(on page 48)*.
21 August 2024	Updated Supported Products *(on page 11)*.

Date	Description
19 August 2024	Added Reports *(on page 40)*.
07 May 2024	• Updated Overview *(on page 17)*. • Added Log Ingestion *(on page 35)* page. • Added Adding a Search Query to Favorites.
26 April 2024	Added information about log retention duration in Logs *(on page 25)*.
18 March 2024	Updated the procedure to attach a contract to the product in Accessing the Events & AIOps Administrator Portal *(on page 13)*.
31 January 2024	Rebranded Horizon Events to Events & AIOps.
17 January 2024	Added the cloud license requirement in Licensing the Product or Start a Trial *(on page 15)*.
16 January 2024	Updated supported Check Point assets for AIOps - Introduction *(on page 61)*,
05 January 2024	Added information about AIOps - Introduction *(on page 61)*.
03 January 2024	Updated Accessing the Events & AIOps Administrator Portal *(on page 13)*: • Added the quick menu option to access Events & AIOps for MSSP accounts. • Updated the screenshots as per the new logos in the Check Point Portal.
14 September 2023	Updated Supported Products *(on page 11)*.

Date	Description
24 May 2023	Added API Support in Logs.
14 March 2023	Added new steps in Getting Started *(on page 13)*.
24 February 2023	Updated Overview *(on page 17)*.
16 February 2023	First release of this document.

3. Introduction to Events & AIOps

Topics:

Check Point Events & AIOps (formerly Infinity Events) is a centralized platform that provides a unified, intuitive interface for viewing and managing security events across a broad range of Check Point products. It streamlines event monitoring and investigation by presenting consolidated log data and standardized terminology, regardless of the product generating the event.

Related information

Supported Products *(on page 11)*

Key Use Cases *(on page 11)*

3.1. Supported Products

Events & AIOps integrates with the following Check Point solutions:

- On-premises Security Management Server
- Spark Management
- Smart-1 Cloud
- Endpoint Security
- Mobile Security
- Harmony Connect
- Browser Security
- Email Security
- SASE
- CloudGuard Posture
- WAF Application Security

3.2. Key Use Cases

Events & AIOps supports a variety of operational and security workflows, including:

- **Multi-Tenant Security Monitoring for MSPs**

  As a Managed Service Provider (MSP), you can monitor and analyze security events across all your managed accounts through a single unified interface, ensuring visibility and control at scale.

- **Event Source Attribution**

  Quickly identify which Check Point application was responsible for blocking or detecting a specific event, such as a URL, file, or connection attempt.

- **Unified Log Terminology**

  Events & AIOps harmonizes terminology across products to simplify investigations. For example, these actions are all referred to as **Block** in Events & AIOps:

  - Endpoint Security - **Block** or **Prevent**
  - Mobile Security - **Block**
  - Smart-1 Cloud - **Drop**

- **Report Generation and Scheduling**

  Generate PDF reports summarizing security activities.

  Reports can be:

  - Scheduled automatically (daily, weekly, monthly)
  - Delivered via email to stakeholders
  - Created for individual tenants or across MSP-managed environments

- **Log Ingestion Dashboard**

  Monitor and track log ingestion metrics and entitlement status per product through a dedicated dashboard. This helps to ensure:

  - Proper ingestion rates from various Check Point solutions
  - Visibility into quota consumption and entitlement usage
  - Early detection of ingestion or license issues

4. Getting Started

Topics:

To get started with Events & AIOps:

1. Creating an Account in the Check Point Portal *(on page)*.
2. Access the Events & AIOps Administrator Portal. *(on page 13)*
3. License the product. *(on page 15)*
4. Assign specific service roles to users *(on page 15)*.
5. View Logs.

4.1. Creating an Account in the Check Point Portal

Check Point Portal is a web-based interface that hosts the Check Point security SaaS services.

With Check Point Portal, you can manage and secure your IT infrastructures: networks, cloud, IoT, endpoints, and mobile devices.

To create an Check Point Portal account, see the Check Point Portal Administration Guide.

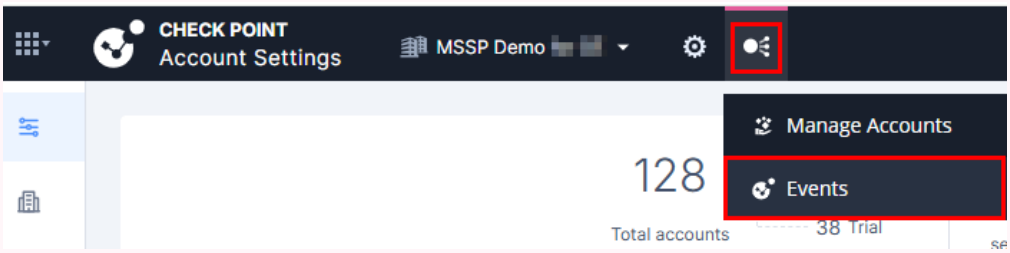
4.2. Accessing the Events & AIOps Administrator Portal

1. Sign in to *Check Point Portal*.

Note:

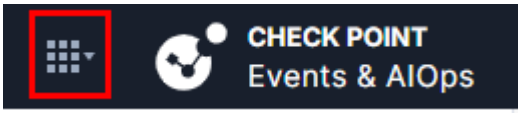
MSSP accounts can access the Events & AIOps Administrator Portal directly from the quick menu option at the top.

Click the  icon and then click **Events**.

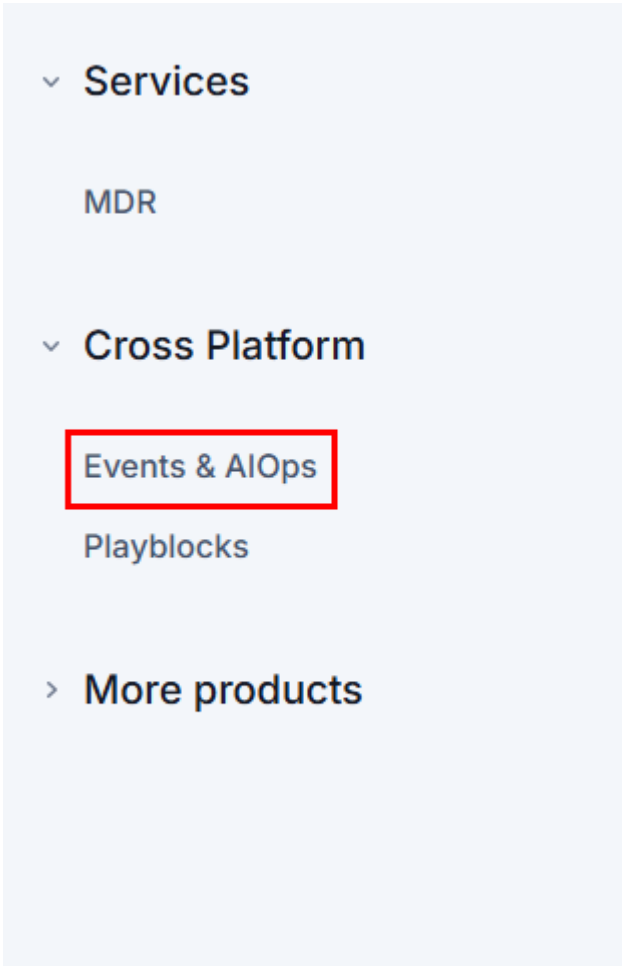


The Events & AIOps Overview *(on page 17)* page appears.

2. Click the **Menu** icon in the top left corner.

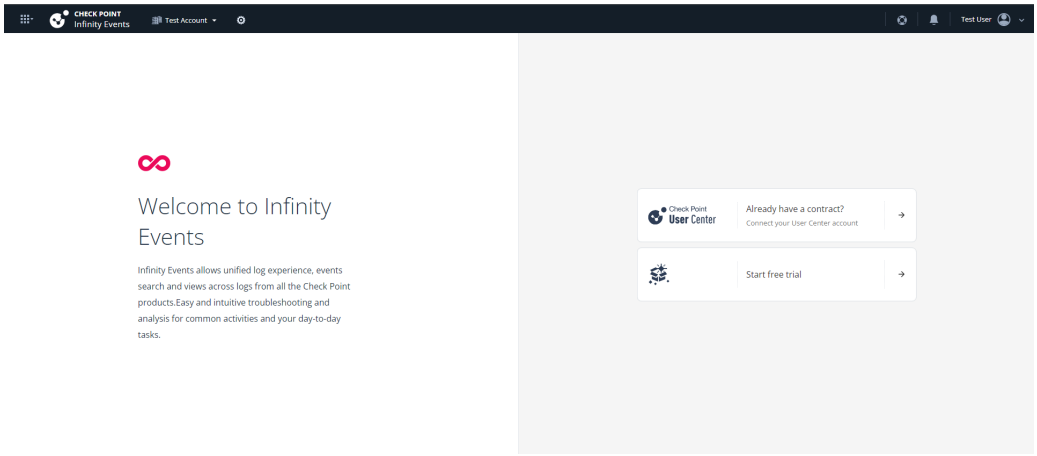


3. Under the **Cross Platform** section, click **Events & AIOps**.

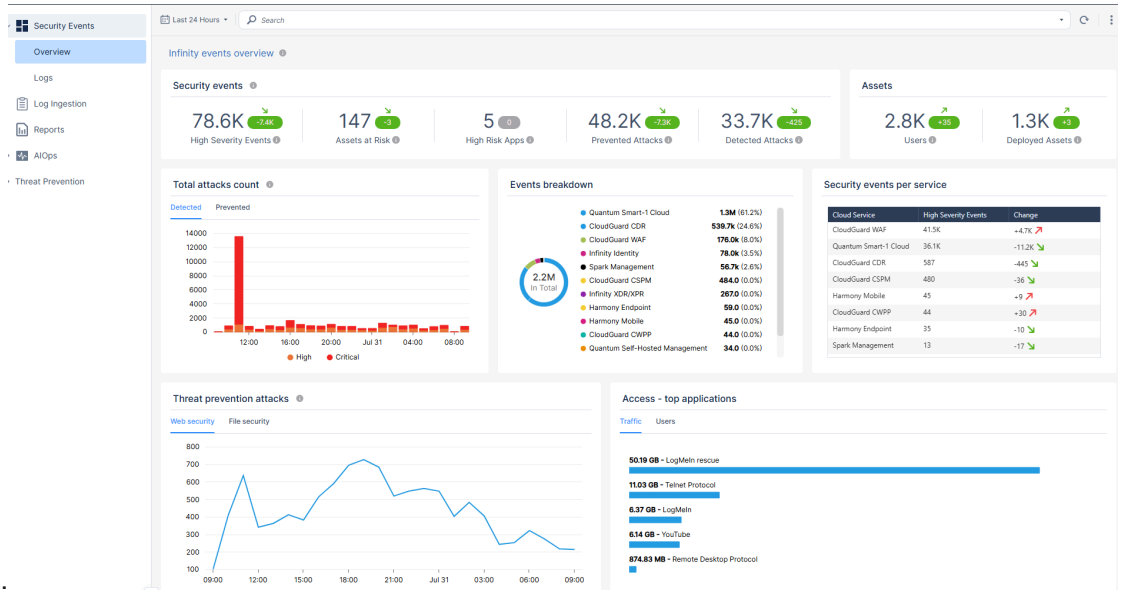


4. If you are accessing the portal for the time, select one of these.

- Add a license from your User Center Account
- Start a free trial (Valid for 30 days)



If you have already added a license from your User Center Account, the Overview *(on page 17)* page appears.



4.3. Licensing the Product or Start a Trial

To use Events & AIOps, you need a cloud license in addition to a licensed Check Point product subscription.

For details on product entitlements, log sharing via SmartConsole, and licensing FAQs, see sk182394.

4.4. Specific Service Roles

Events & AIOps supports specific service roles. For more information, see the **Specific Service Roles** section in the *Check Point Portal Administration Guide*.

To access **Specific Service Roles**, go to **Global Settings** > **Users** > **New** > **Add User** and expand **Specific Service Roles**.

Service Roles	Description
Admin	Can read and modify every administrative setting.
Read-Only	Provides full visibility across your Infinity Account.

5. Security Events

Topics:

5.1. Overview

The supported products are:

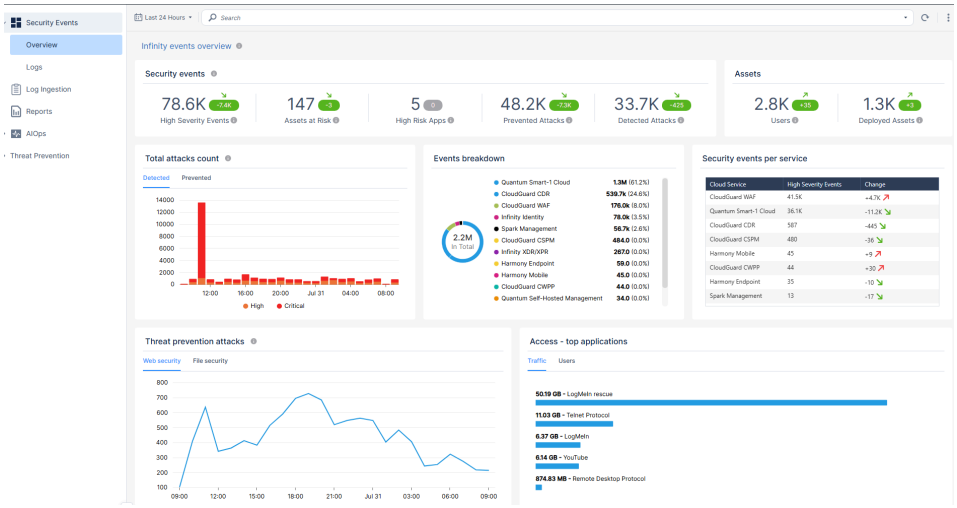
- On-premises Security Management Server
- Spark Management
- Smart-1 Cloud
- Endpoint Security
- Mobile Security
- Harmony Connect
- Browser Security
- Email Security
- SASE
- CloudGuard Posture
- WAF Application Security

For an MSP account, the **Overview** dashboard appears the same as for normal accounts, except that it provides options to view information for selected child accounts and includes a few additional widgets related to those child accounts. See Overview Dashboard for MSPs *(on page 21)*.

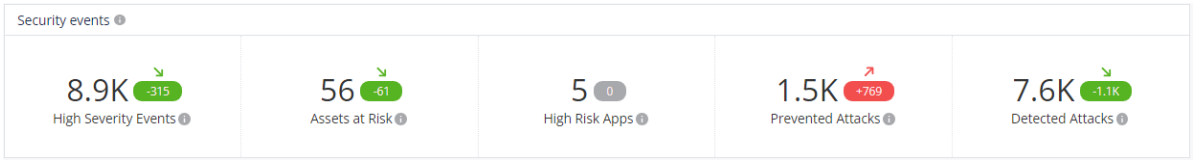
To view the Overview page:

1. Access the Events & AIOps Administrator Portal *(on page 13)*.
2. Click **Security Events** > **Overview**.

By default, the dashboard displays the overview for the last seven days.



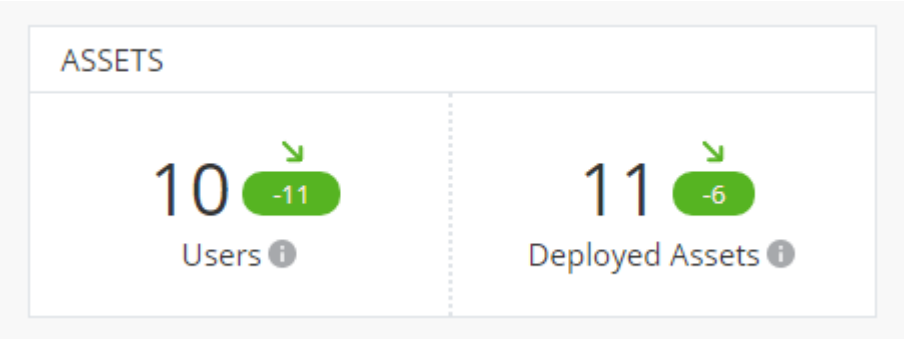
5.1.1. Security Events



The **Security events** widget shows:

- **High Severity Events** - The number of high severity events reported.
- **Assets at Risk** - The number of assets which reported critical events.
- **High Risk Apps** - The number of applications at High risk.
- **Prevented Attacks** - The number of security attacks prevented.
- **Detected Attacks** - The number of security attacks detected and not prevented.

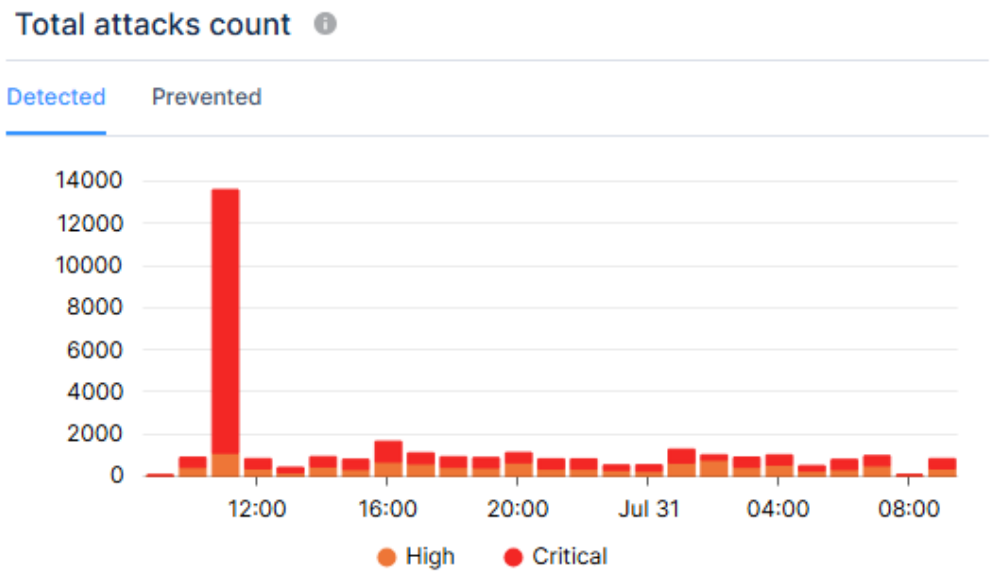
5.1.2. Assets



The **Assets** widget shows:

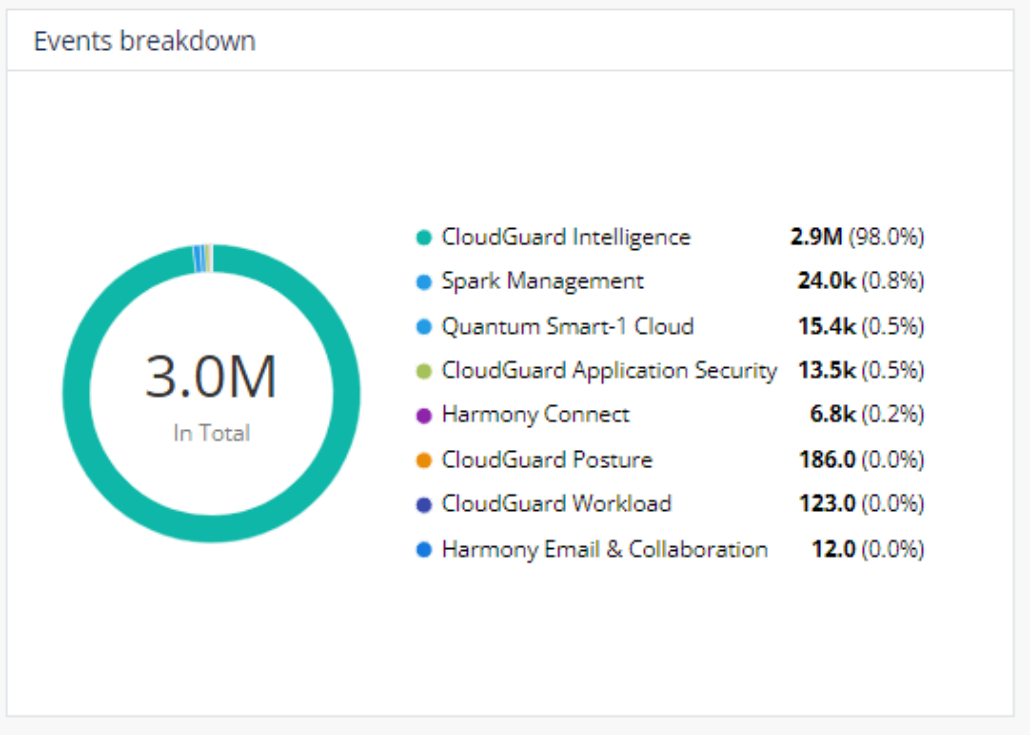
- **Users** - Number of users that reported events.
- **Deployed Assets** - Number of deployed assets.

5.1.3. Total Attacks Count



The **Total attacks count** widget shows the total number of attacks detected and prevented for the selected period, based on their severity.

5.1.4. Events Breakdown



The **Events breakdown** widget shows the number of events for each Check Point product.

5.1.5. Security Events Per Service

Security events per service

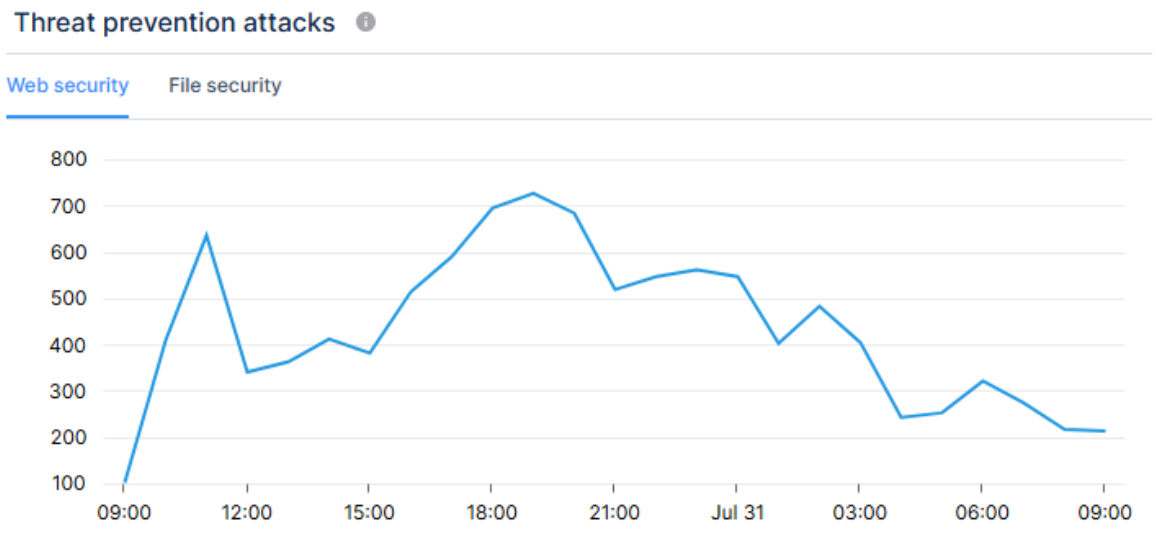
Cloud Service	High Severity Events	Change
CloudGuard Intelligence	6K	-682 ↘
CloudGuard Application Security	1.3K	+772 ↗
Quantum Smart-1 Cloud	1.2K	-24 ↘
CloudGuard Posture	186	-347 ↘
CloudGuard Workload	123	-31 ↘
Spark Management	30	-1 ↘
Harmony Email & Collaboration	12	-1 ↘
Harmony Connect	3	0
Harmony Browse	0	-6 ↘

The **Security events per service** widget shows:

- **High Severity Events** - Number of high severity events reported in each Check Point product.
- **Change** - The difference in the number of events reported in the current and previous time periods.

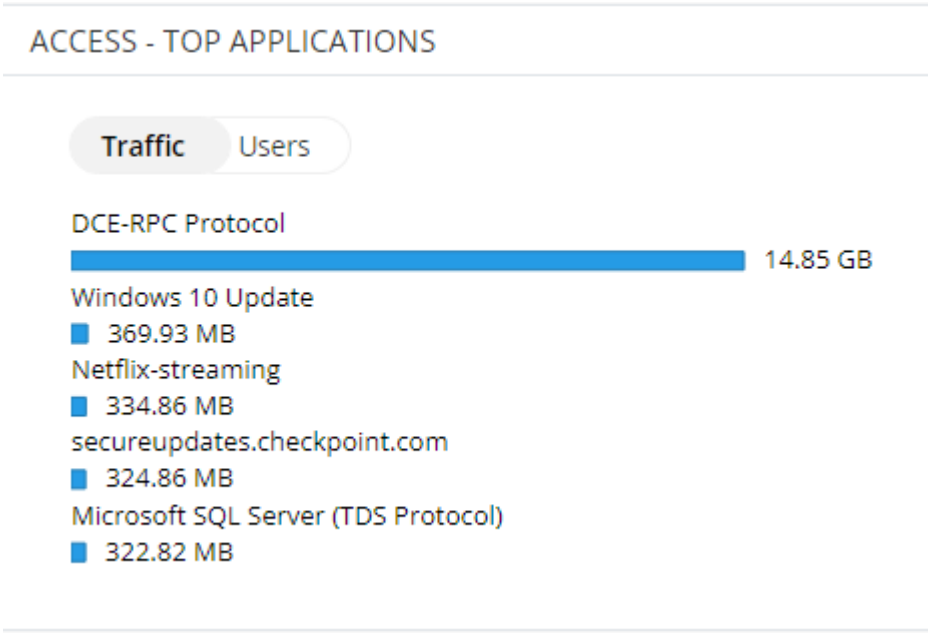
  For example, the selected time period is **Last 7 days** and the **Change** is **-411**. This means that 411 fewer events were reported in the last 7 days (11 Jan - 17 Jan) compared to the number of events reported in the previous 7 day period (4 Jan - 10 Jan).

5.1.6. Threat Prevention Attacks



The **Threat prevention attacks** widget shows the number of threat prevention events (detected and prevented) during the selected time period. To view Threat Prevention details, go to the Threat Prevention *(on page 98)* page.

5.1.7. Access - Top Applications



The **Top Applications** widget shows the internet data consumed by different users and applications such as Facebook or YouTube in the assets across Check Point products.

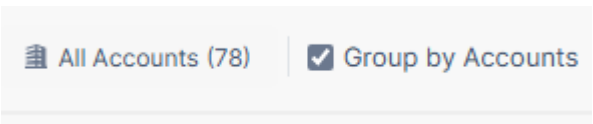
To view the data consumption by applications, click **Traffic**.

To view the data consumption by users, click **Users**.

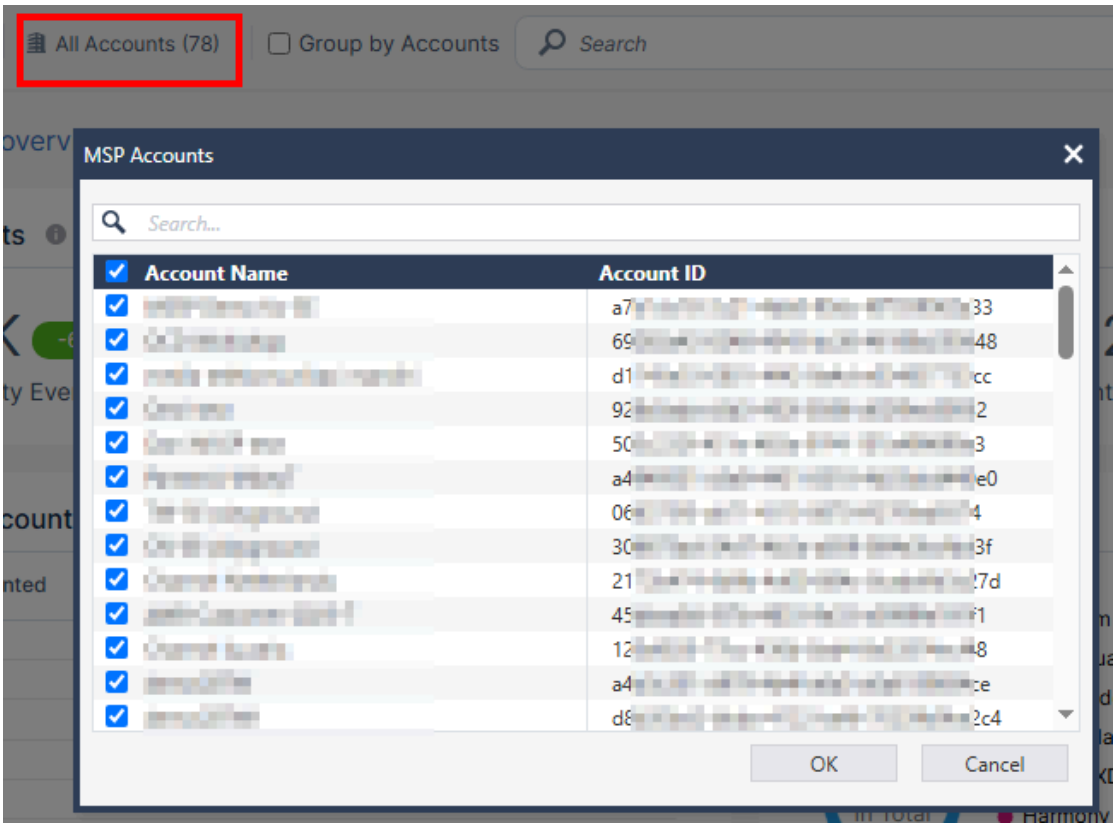
5.1.8. Overview Dashboard for MSPs

> **Note:**
>
> This section describes only the fields and widgets specific to MSP accounts.

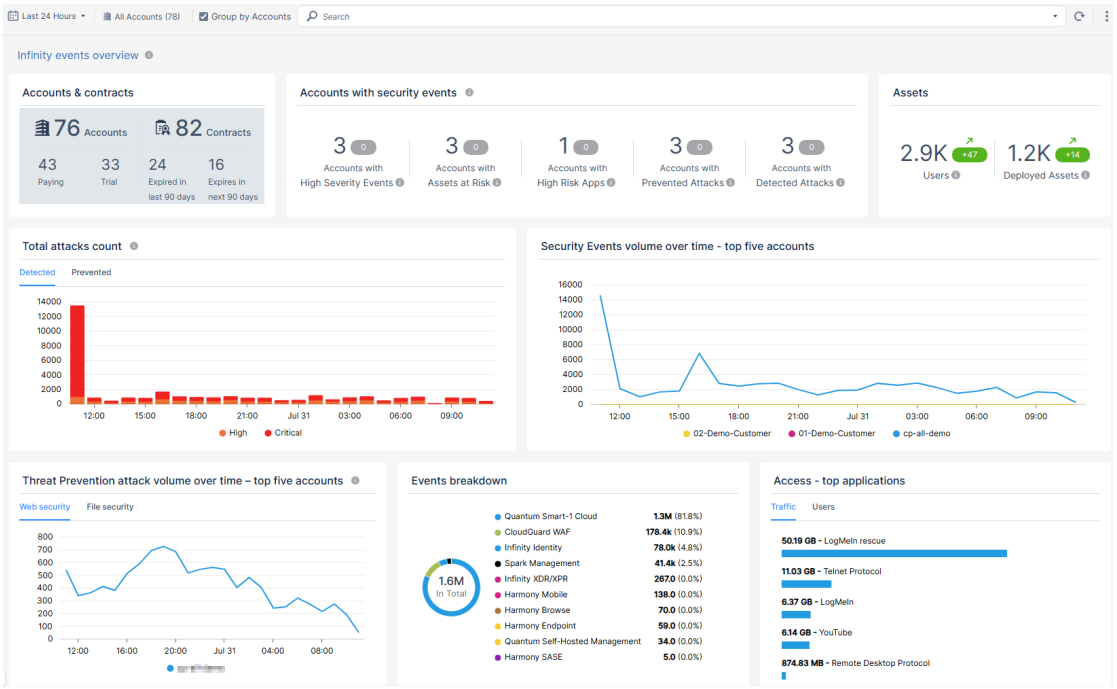
For Managed Service Providers (MSP) accounts, the **Overview** dashboard displays both standard and MSP-specific widgets. The data displayed depends on the selected accounts and whether the **Group by Accounts** option is enabled.



- To view data for specific MSP accounts, click **All Accounts** and select the required accounts.



- To group the data by accounts, select the **Group by Accounts** checkbox. When it is enabled, the dashboard shows the **number of accounts** in each widget, and not the number of events.



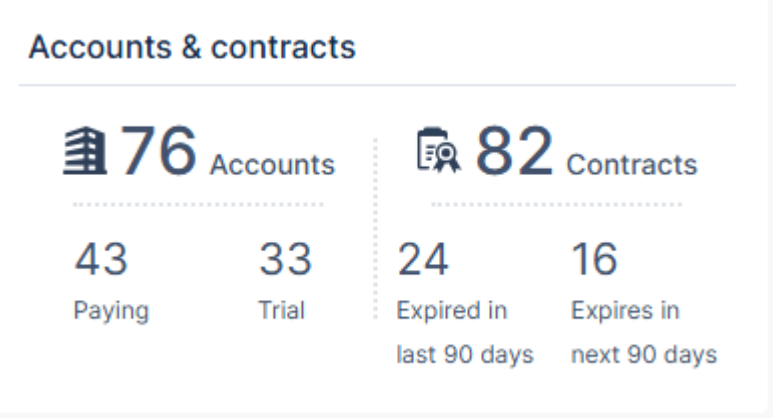
When the **Group by Accounts** checkbox is not selected, the dashboard shows the total number of events across all child accounts.

The MSP-specific widgets are described in the following sections.

5.1.8.1. Accounts and Contracts

Note:

The **Accounts & contracts** widget appears only when the **Group by Accounts** checkbox is selected.



The **Accounts & contracts** widget shows the summary of account types and contract statuses.

- **Accounts**

  Number of active and trial accounts.

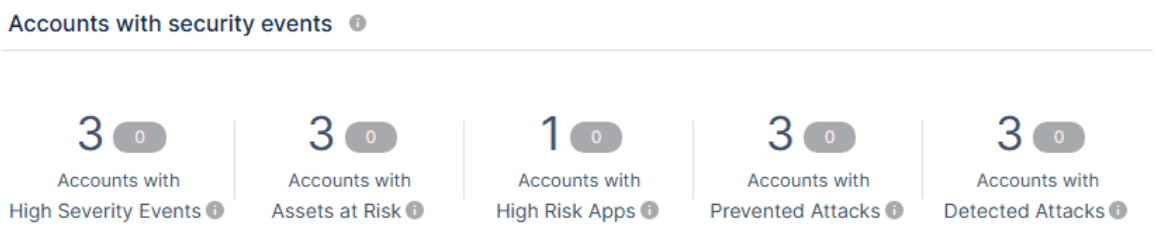
- **Contracts**

  Number of contracts expired and soon to expire in 90 days.

5.1.8.2. Accounts with Security Events

Note:

The **Accounts with security events** widget appears only when the **Group by Accounts** checkbox is selected.



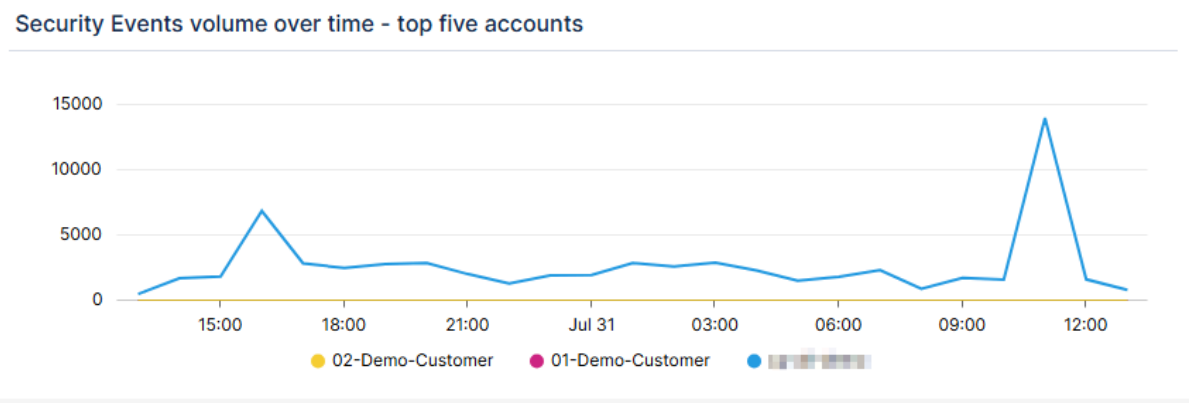
The **Accounts with security events** widget shows the number of accounts with:

- **High Severity Events** - The number of high severity events reported.
- **Assets at Risk** - The number of assets which reported critical events.
- **High Risk Apps** - The number of applications at High risk.
- **Prevented Attacks** - The number of security attacks prevented.
- **Detected Attacks** - The number of security attacks detected and not prevented.

5.1.8.3. Security Events Volume Over Time - Top Five Accounts

Note:

The **Security Events volume over time - top five accounts** widget appears only when the **Group by Accounts** checkbox is selected.

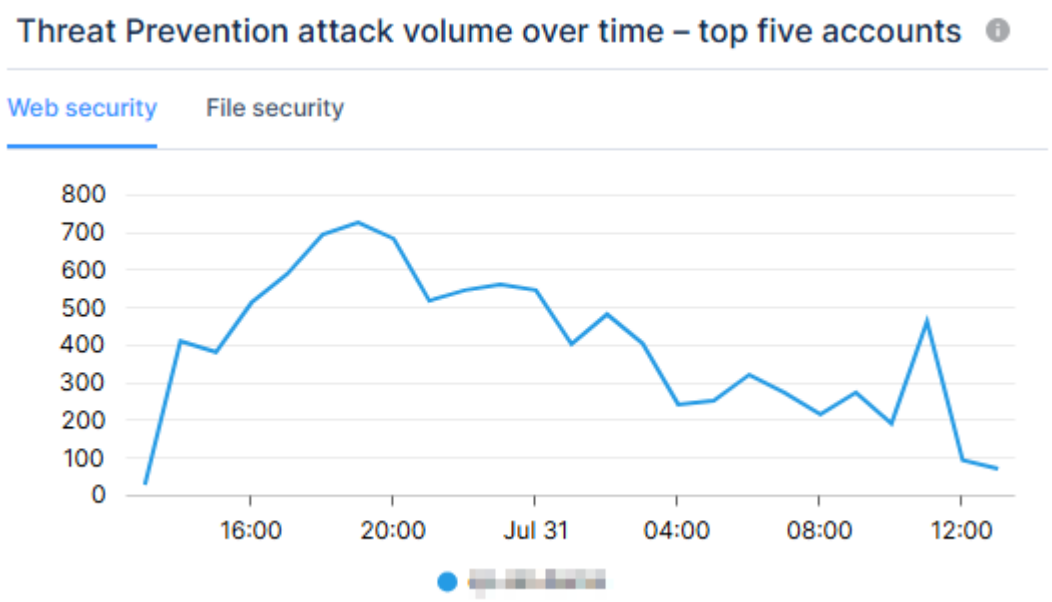


The **Security Events volume over time - top five accounts** widget shows the top five child accounts based on the number of security events.

5.1.8.4. Threat Prevention Attack Volume Over Time - Top Five Accounts

Note:

The **Threat Prevention attack volume over time - top five accounts** widget appears only when the **Group by Accounts** checkbox is selected.



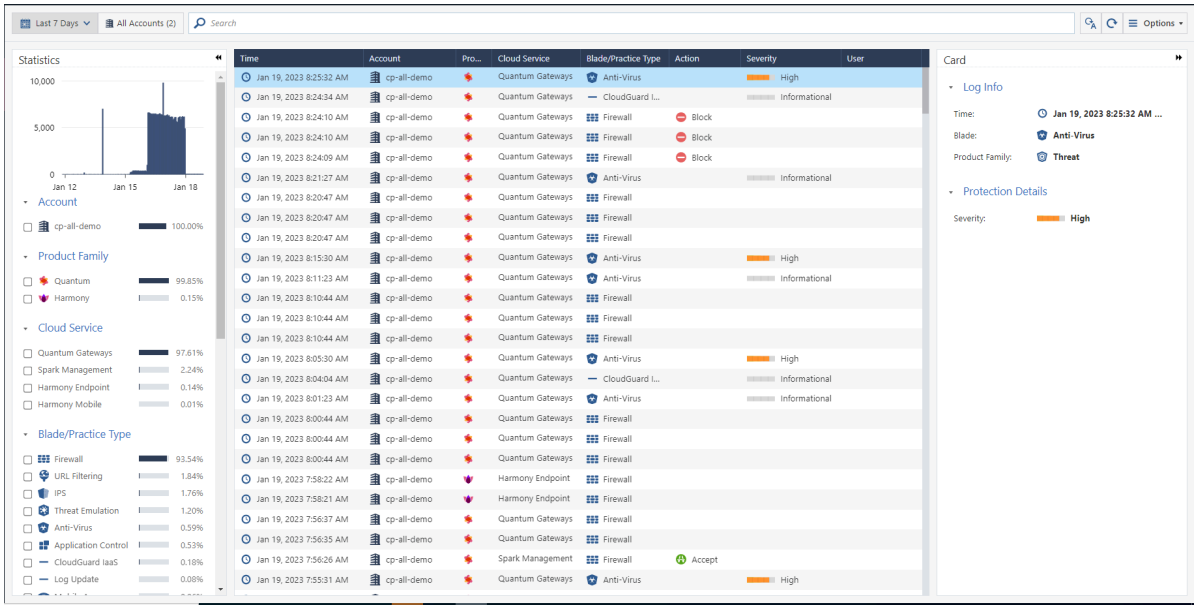
The **Threat Prevention attack volume over time - top five accounts** widget shows the top five child accounts based on the number of threat prevention events (detected and prevented). To view Threat Prevention details, go to the Threat Prevention *(on page 98)* page.

5.2. Logs

It shows:

- Statistics *(on page 27)*
- Logs Table *(on page 28)*
- Card *(on page 33)*

To view the **Logs** page, access Events & AIOps and click **Security Events** > **Logs**.



Note:

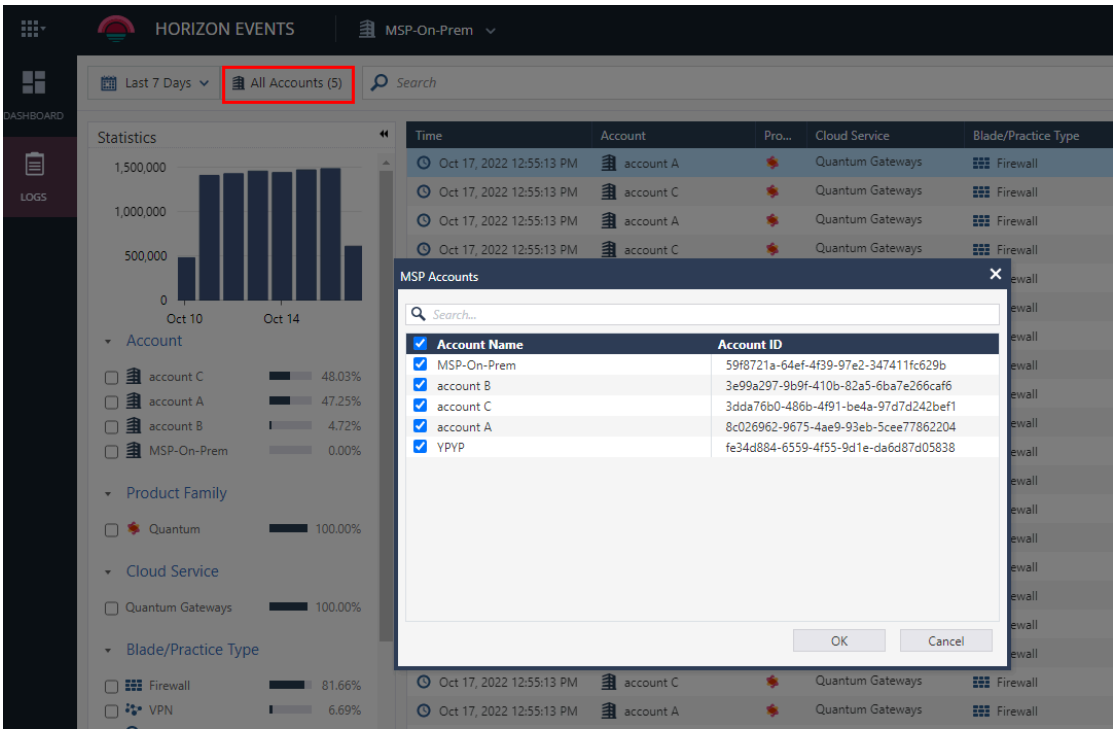
The default log retention duration is 90 days. To extend the duration to 180 days or 365 days, contact Check Point Support.

5.2.1. Viewing MSP Child Account Events

By default, the Logs Table *(on page 28)* shows events for all the child accounts of an MSP account.

1. In the **Logs** window, click **All Accounts**.

   The **MSP Accounts** window appears. By default, all child accounts are selected.



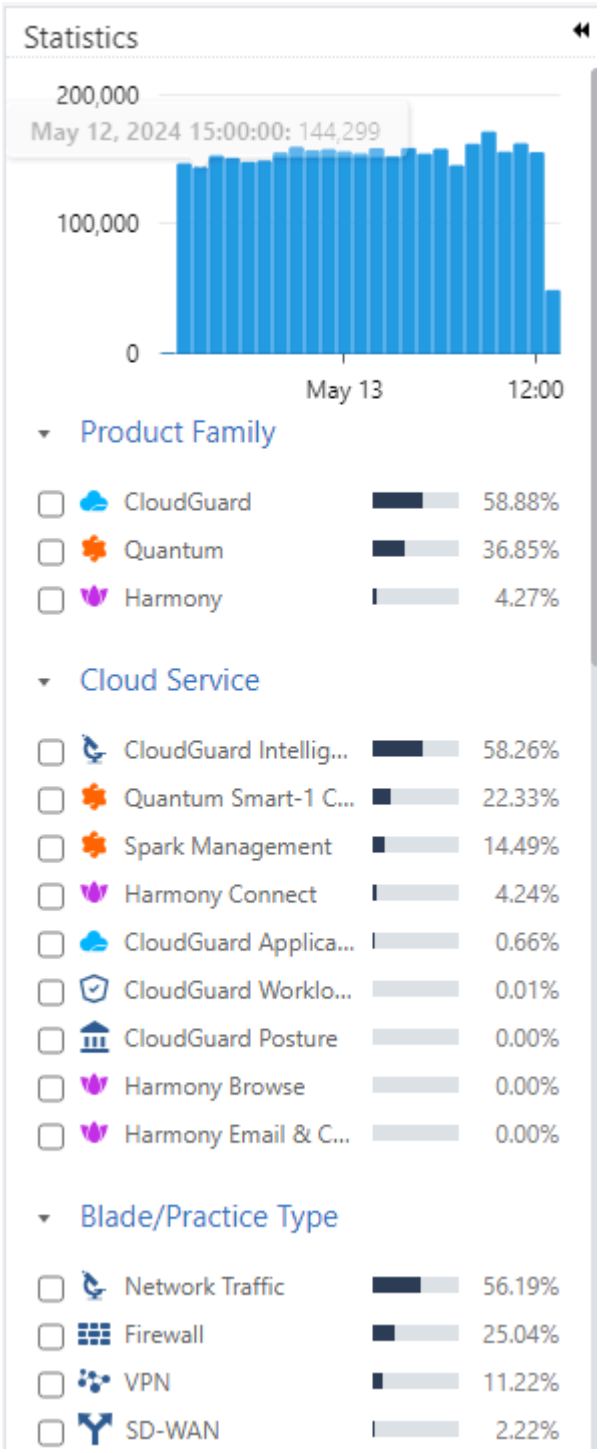
2. Select the checkbox for the required child account and deselect the others.

3. Click **OK**.

Note:

To manage child accounts under an MSP, go to **Global Settings** > **Account Management**.

5.2.2. Statistics

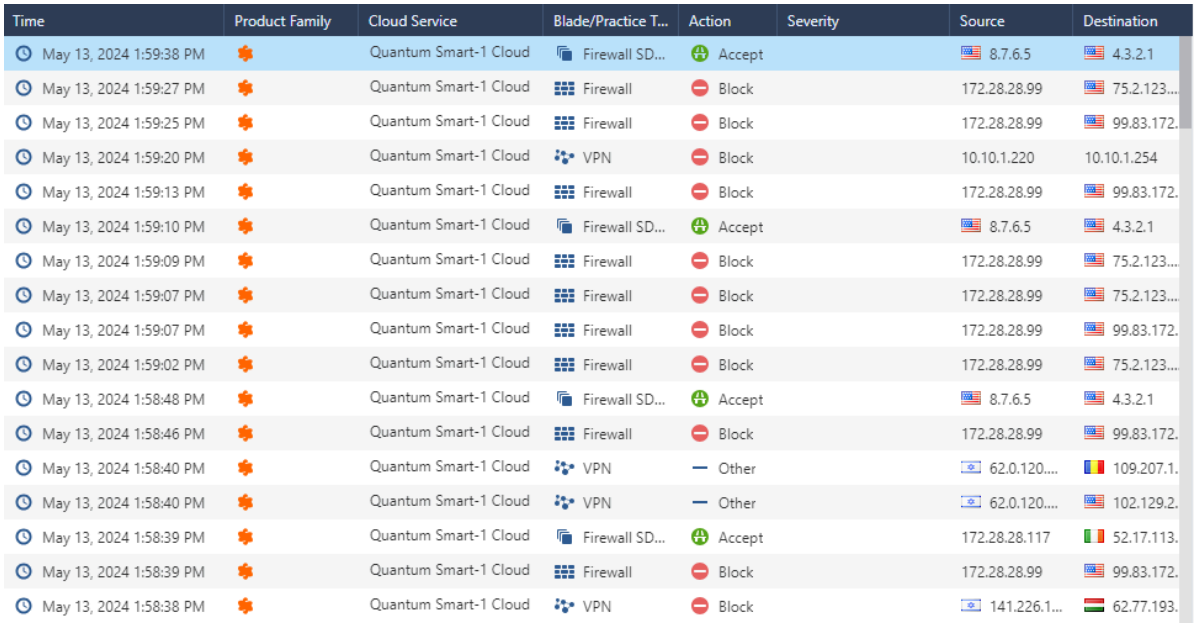


On the **Statistics** pane, you can:

- See a bar graph of the number of events for the selected time frame.
- Filter the event data in Logs Table *(on page 28)*. For example, you can filter the events data for a product family, an MSP child account and more.

> **Note:**
>
> As the logs for **Log Sharing** cloud service are distributed between **Quantum Smart-1 Cloud** and **Log Sharing**, the system may show inaccurate statistics in the **Cloud Service** section.

5.2.3. Logs Table



Time	Product Family	Cloud Service	Blade/Practice T...	Action	Severity	Source	Destination
May 13, 2024 1:59:38 PM		Quantum Smart-1 Cloud	Firewall SD...	Accept		8.7.6.5	4.3.2.1
May 13, 2024 1:59:27 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	75.2.123....
May 13, 2024 1:59:25 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	99.83.172.
May 13, 2024 1:59:20 PM		Quantum Smart-1 Cloud	VPN	Block		10.10.1.220	10.10.1.254
May 13, 2024 1:59:13 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	99.83.172.
May 13, 2024 1:59:10 PM		Quantum Smart-1 Cloud	Firewall SD...	Accept		8.7.6.5	4.3.2.1
May 13, 2024 1:59:09 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	75.2.123....
May 13, 2024 1:59:07 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	75.2.123....
May 13, 2024 1:59:07 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	99.83.172.
May 13, 2024 1:59:02 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	75.2.123....
May 13, 2024 1:58:48 PM		Quantum Smart-1 Cloud	Firewall SD...	Accept		8.7.6.5	4.3.2.1
May 13, 2024 1:58:46 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	99.83.172.
May 13, 2024 1:58:40 PM		Quantum Smart-1 Cloud	VPN	Other		62.0.120....	109.207.1.
May 13, 2024 1:58:40 PM		Quantum Smart-1 Cloud	VPN	Other		62.0.120....	102.129.2.
May 13, 2024 1:58:39 PM		Quantum Smart-1 Cloud	Firewall SD...	Accept		172.28.28.117	52.17.113.
May 13, 2024 1:58:39 PM		Quantum Smart-1 Cloud	Firewall	Block		172.28.28.99	99.83.172.
May 13, 2024 1:58:38 PM		Quantum Smart-1 Cloud	VPN	Block		141.226.1...	62.77.193.

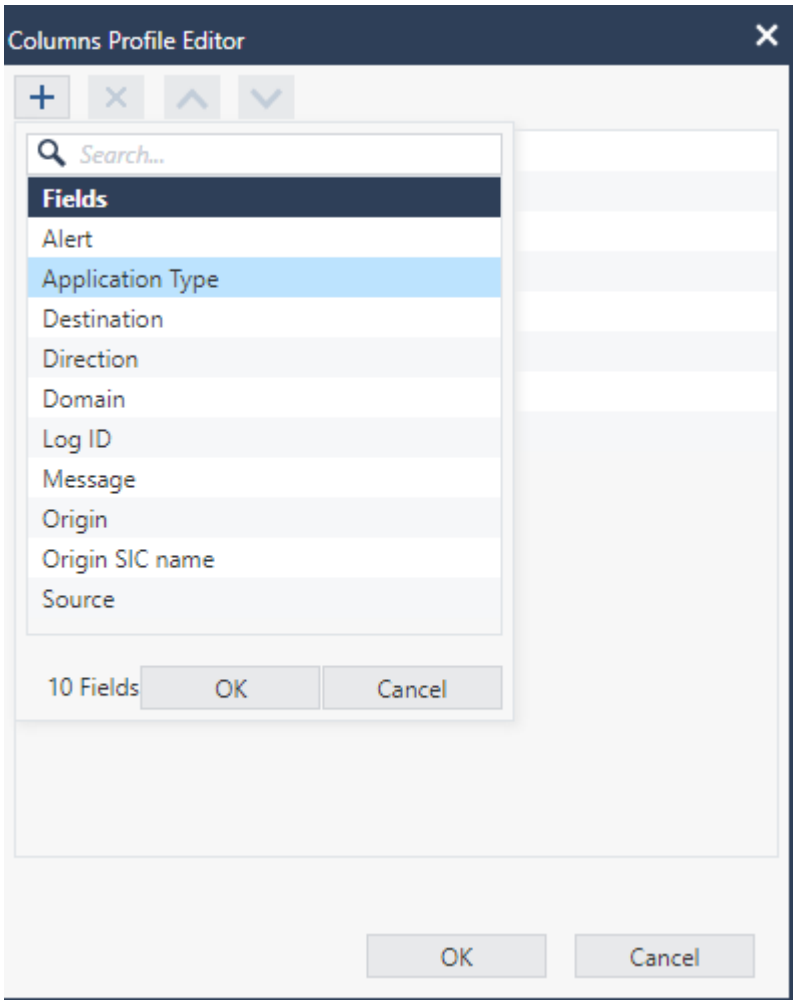
Field Name	Description
Default Fields	
Time	Time of the event.
Account	Account name.
Product Family	Check Point product family. For example, Quantum, Harmony or CloudGuard.
Cloud Service	The cloud service used by the Check Point product. For example, Quantum Gateways.
Blade/Practice Type	Software blade that triggered the event. For example, Firewall, VPN, Syslog.
Action	Action enforced on the event: • Accept • Block

Field Name	Description
	• Detect • Other
Severity	Severity of the event: • Critical • Informational • Low • Medium • High
User	User logged in at the time of the event.
Additional Fields	
Alert	Type of alert generated for the event. For example, spoof alert, mail.
Destination	Destination IP address.
Direction	Direction of the network traffic: • Inbound • Outbound
Domain	Domain name sent to DNS request.
Log ID	Unique identity for logs. Includes Type, Family, Product/Blade, Category.
Message	Message displayed for the security event. For example, *remote access client IP address and port were changed*.
Origin	Name of the first Security Gateway that reported this event.
Source	Source IP address.

5.2.4. Managing the Logs Table

1. To view the details of a specific log, double-click the row.
2. To view the default columns, right-click the table header row and click **Default**.
3. To modify the table columns, right-click the table header row and click **Columns Profile Editor**.
4. To add a new column to the table.

a. Click **+**.



b. Select the column from the list and click **OK**.

The new column appears in the Logs table and in the **Statistics** pane.

5. To remove a column from the table:
   a. Select the column you want to delete and click **X**.
   b. Click **OK**.

   The selected column is deleted from the Logs table and from the **Statistics** pane.

6. To sort the columns:

   a. Select the column:

      - To move the column higher in the order, click .
      - To move the column lower in the order, click

   b. Click **OK**.

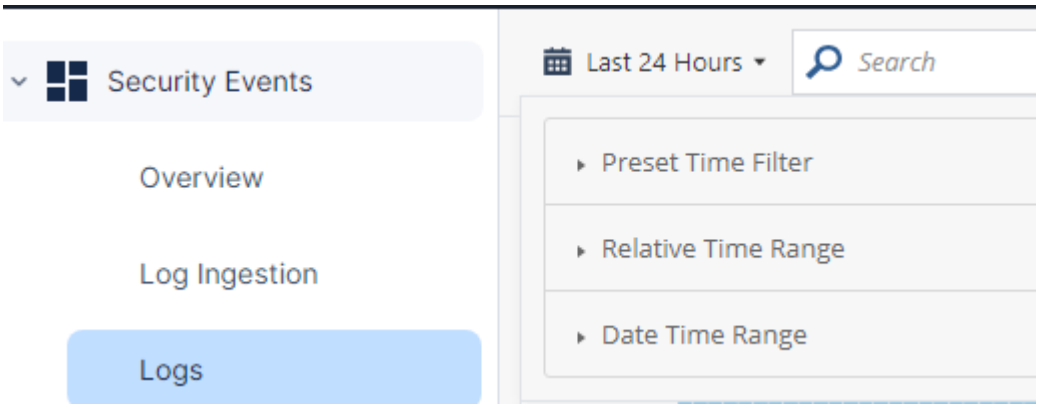
   The column position is updated in the Logs table and in the **Statistics** pane.

5.2.5. Viewing Logs for a Time Period

By default, the Logs table shows events for the last 7 days.

To view Logs table for a specified period, use one of these to set the time range:

- Preset Time Filter
- Relative Time Range
- Date Time Range



5.2.6. Searching for Events

You can search for events using free text or a filter.

1. To search using free text, in the **Search** field, enter the text and press **Enter**.

   For example, if you enter **Block**, the search results show all the blocked events.

2. To search using a filter, click the **Search** field, select a filter and enter the text.

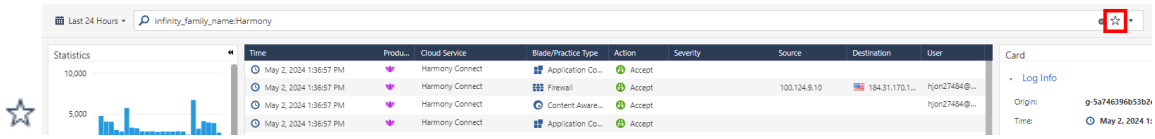
   For example, if the filter is **Blade/Practice Type** and text is **URL Filtering**, search as Blade/Practice Type:"URL Filtering".

   The search results show all events with **Blade/Practice Type** as **URL Filtering**.

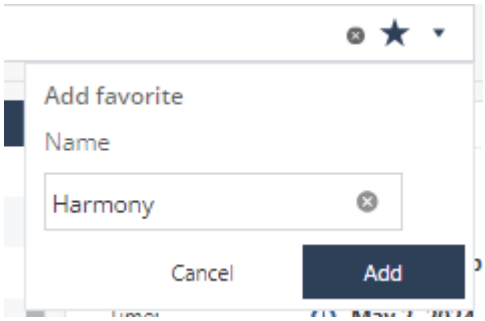
> **Note:**
>
> You can use logical operations AND, OR and NOT in the search.
>
> For example, **Block AND URL Filtering** shows the blocked events with **Blade/Practice Type** as **URL Filtering**.

5.2.7. Adding a Search Query to Favorites

1. Run the search query.
2. Click the icon at the end of the **Search** bar.

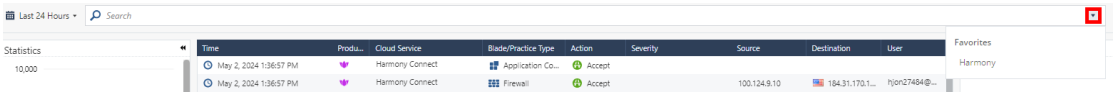


3. Enter a name for the query and click **Add**.



The query is added to the **Favorites** list.

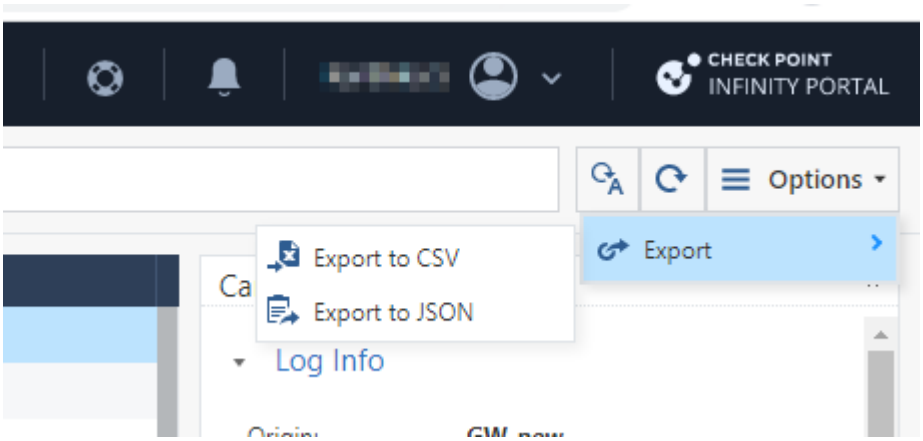
4. To view the **Favorites** list, click the drop-down in the **Search** bar.



5.2.8. Exporting Logs

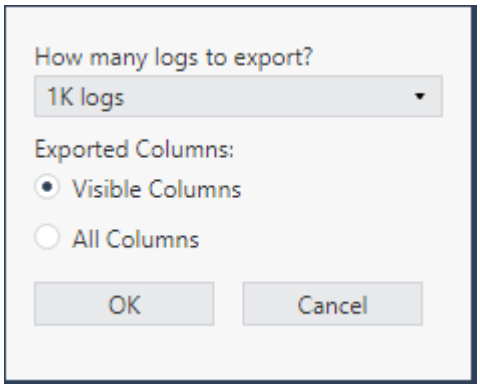
You can export events from the Logs table to a CSV file or to a JSON file.

1. In the **Logs** window, click **Options** > **Export**.



2. Select one of these output file formats.
   - Export to CSV
   - Export to JSON

3. Enter the information for these fields.
    - From **How many logs to export** list, select the number of logs you want to export.
    - In **Exported Columns**, select whether to export event data from **Visible Columns** or from **All Columns**.

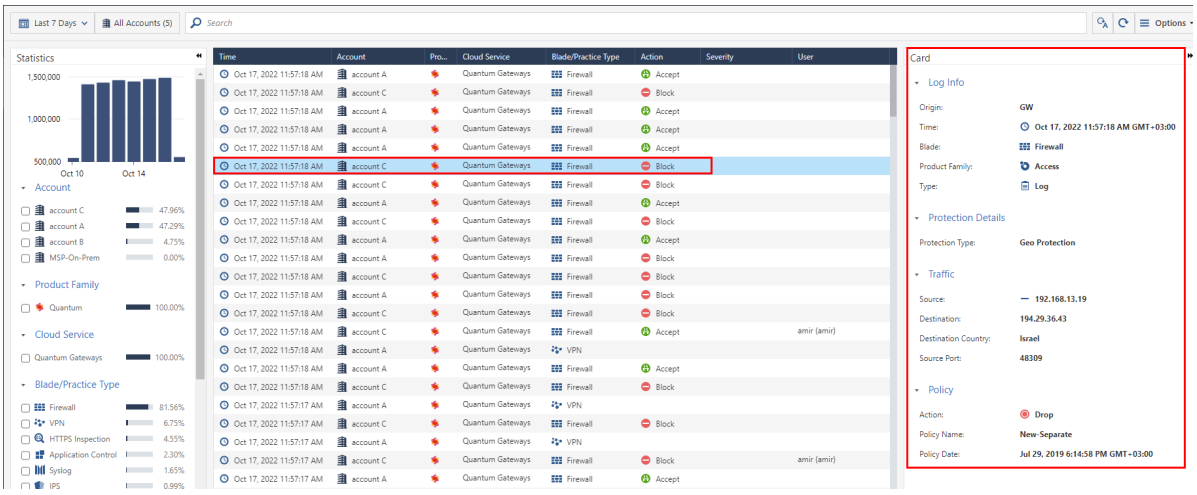


4. Click **OK**.

For CSV output, system generates an Excel sheet with the file name format: *Events_Logs_Date_Time.xls*. For JSON output, system generates a json file with name format: *Events_Logs_Date_Time.json*. Example, *Events_Logs_Oct_17_2022_01_48_24_PM*.

5.2.9. Card

The **Card** pane shows the details for the event selected in the Logs Table *(on page 28)*.



5.2.10. API Support-Events & AIOps

You can use REST APIs to query security event logs generated by Check Point products that are included in Events & AIOps.

1. Go to *Check Point API Reference*.
2. Click the **Infinity** tab.
3. In the **Events & AIOps API** widget, click **Open**.

6. Log Ingestion

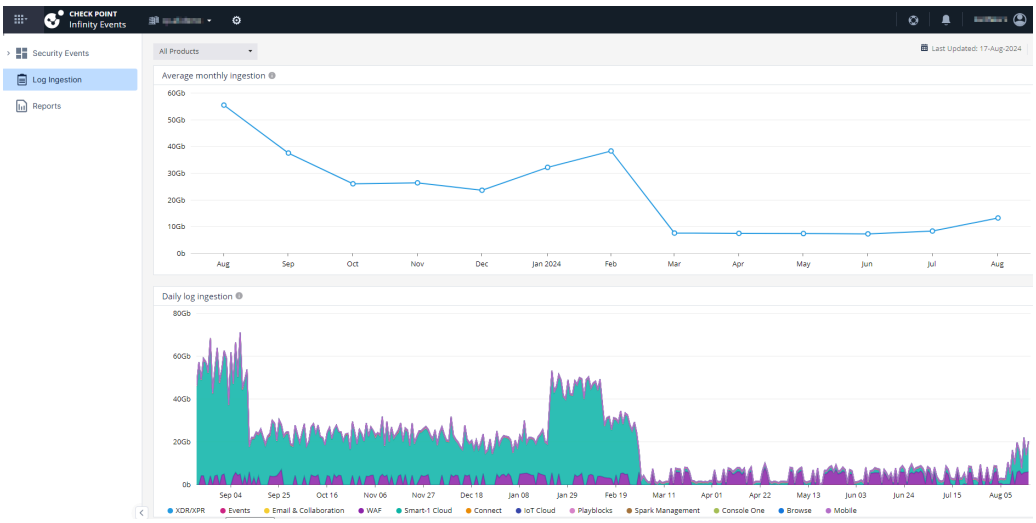
Topics:

The **Log Ingestion** page shows the volume of logs uploaded to Infinity Cloud Events by the Supported Products *(on page 11)*.

6.1. View the Log Ingestion page

By default, the page shows the **Average monthly ingestion** and **Daily log ingestion** data for all the supported products.

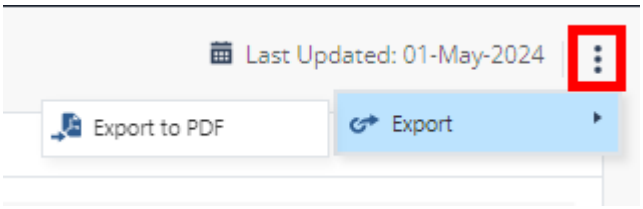
1. Access the Events & AIOps Administrator Portal *(on page 13)*.
2. Click **Log Ingestion**.



To view this information for a specific product, select the product from the drop-down list at the top-left corner.

6.2. Export the log ingestion details

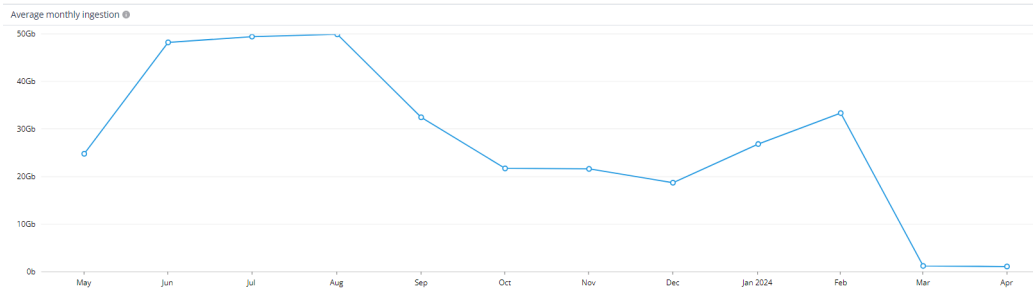
1. Click ⋮ at the top-right corner.



2. Click **Export** > **Export to PDF**.

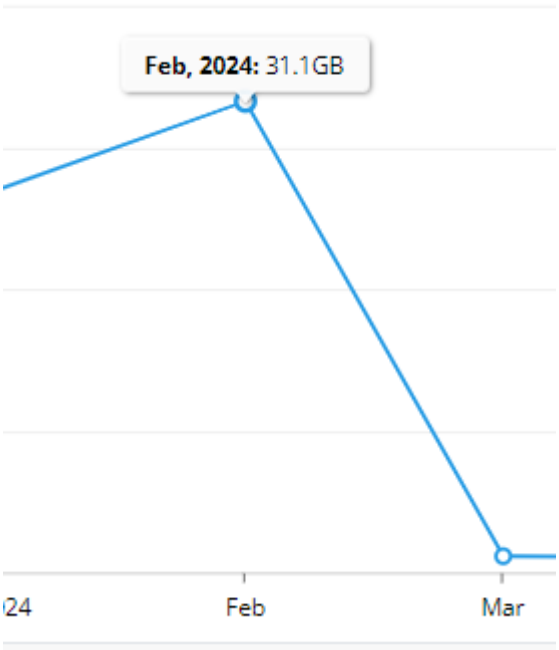
   The system generates a PDF with name format: *Ingestion_logs_last-year__Date_Time*

6.3. Average Monthly Ingestion



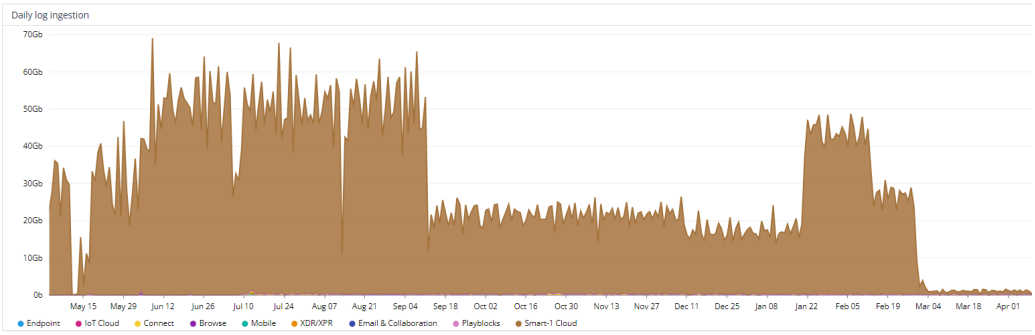
The **Average Monthly Ingestion** widget shows the average volume of logs uploaded to Infinity Cloud Events per month.

Hover over the month to view this information.

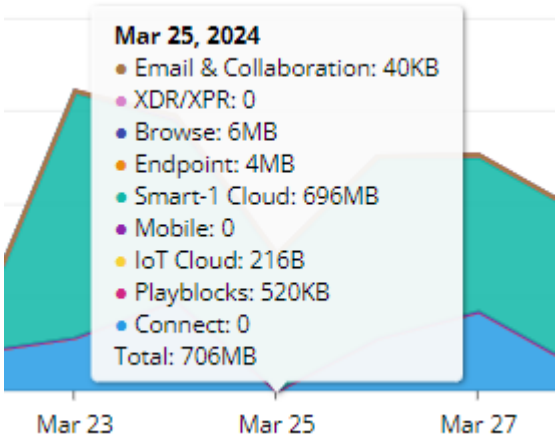


6.4. Daily Log Ingestion

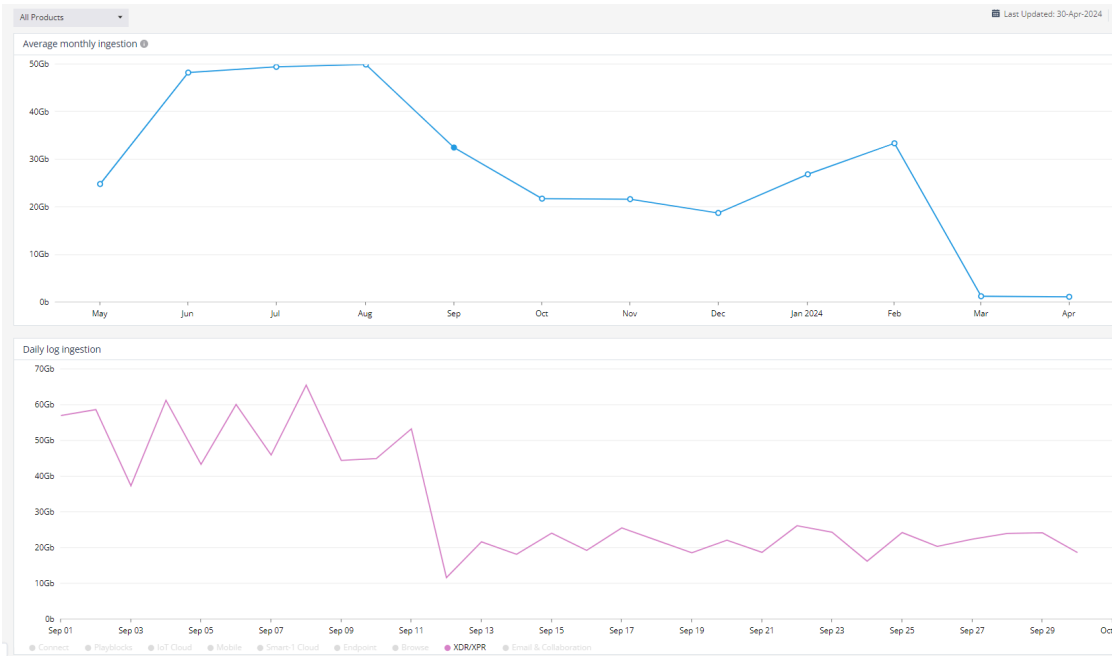
The **Daily Log Ingestion** widget shows the volume of logs that each product uploads to Infinity Cloud Events per day.



1. To view the volume of logs uploaded on a specific date, hover over the date.

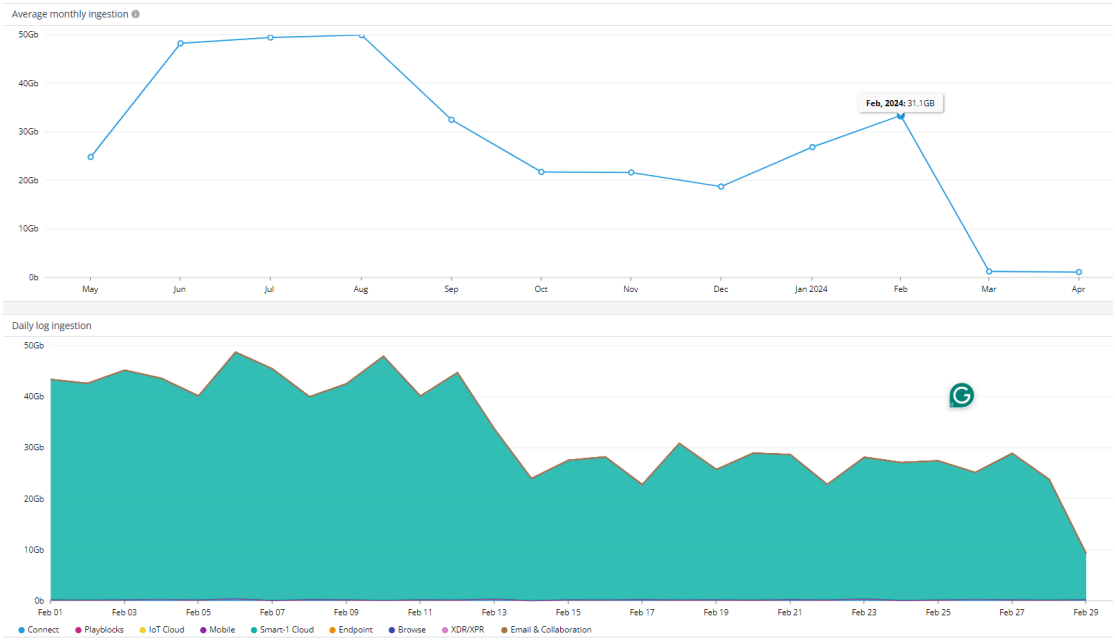


2. To view the daily log ingestion for a specific product, click the product name at the bottom.



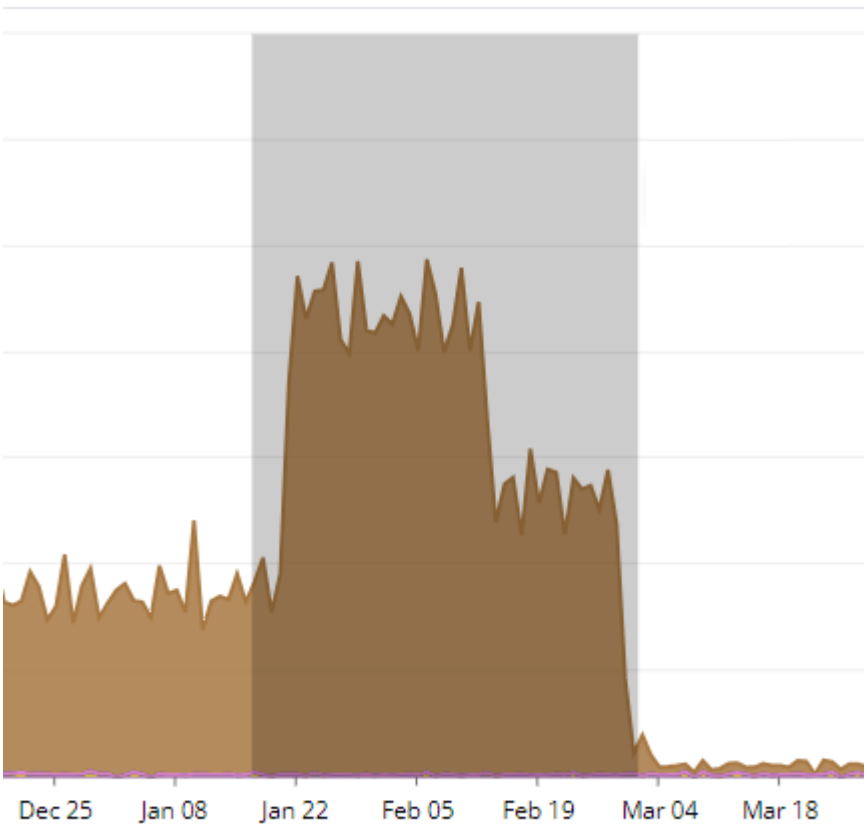
3. To view the daily log ingestion for a specific month, click the month in the **Average monthly ingestion** widget.

   The **Daily log ingestion** widget shows the volume of logs uploaded on each day of the selected month.

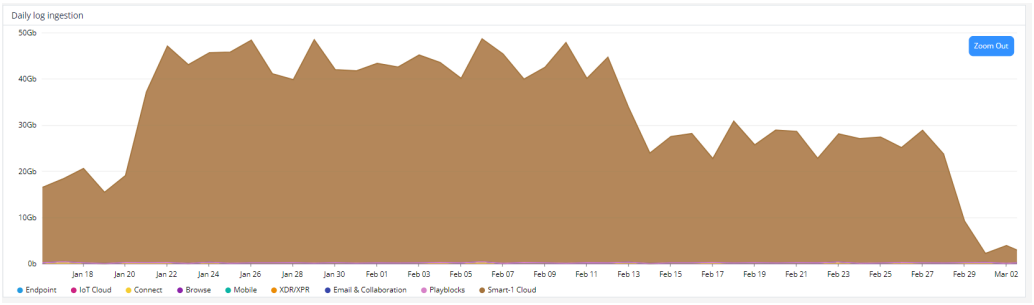


4. To view the volume of logs uploaded for a specific period:

   a. Press the mouse button and drag it over the required period.



The widget shows the daily log ingestion for the selected period.



b. To go back to the default view, click **Zoom Out**.

7. Reports

Topics:

Note:

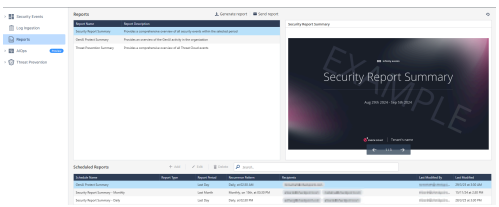
For MSPs, see Reports for MSPs *(on page 48)*.

The **Reports** page allows you to generate and send these reports:

- **Security Report Summary** - Provides an overview of security events for the Check Point products you are subscribed to in Check Point Portal.
- **GenAI Protect Summary** - Provides an overview of the GenAI activity in your organization.
- **Threat Prevention Summary** - Provides an overview of all Threat Prevention events for the Check Point products you are subscribed to in Check Point Portal.

You can generate the report on demand or create a schedule to generate the report and send it to the required recipients.

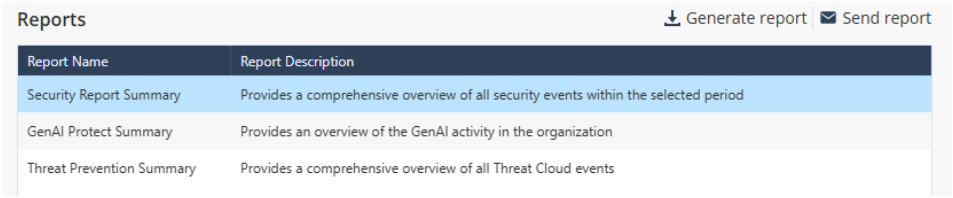
To view the **Reports** page, access the Events & AIOps Administrator Portal *(on page 13)* and click **Reports**.



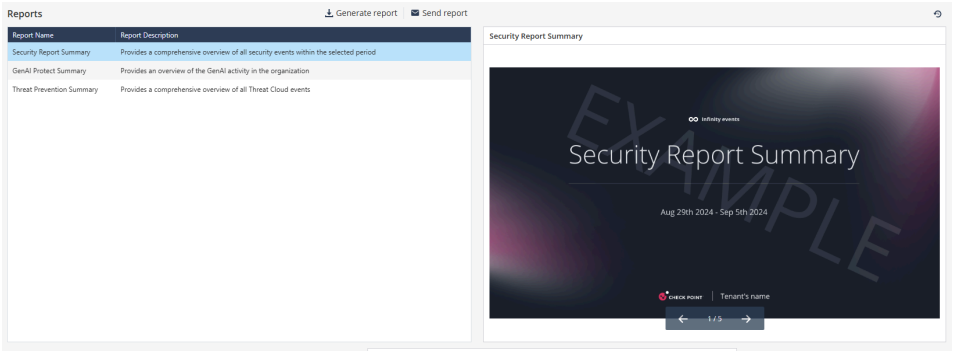
7.1. Generating Reports On Demand

From the **Reports** section, you can generate and download the Security Report Summary on demand.

1. Go to **Reports** and select the report template in the **Reports** section.

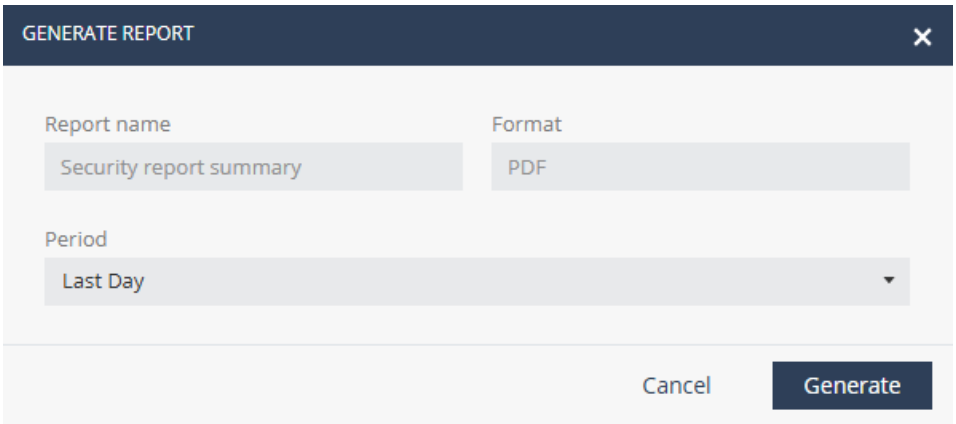


The system displays the sample report on the right side.



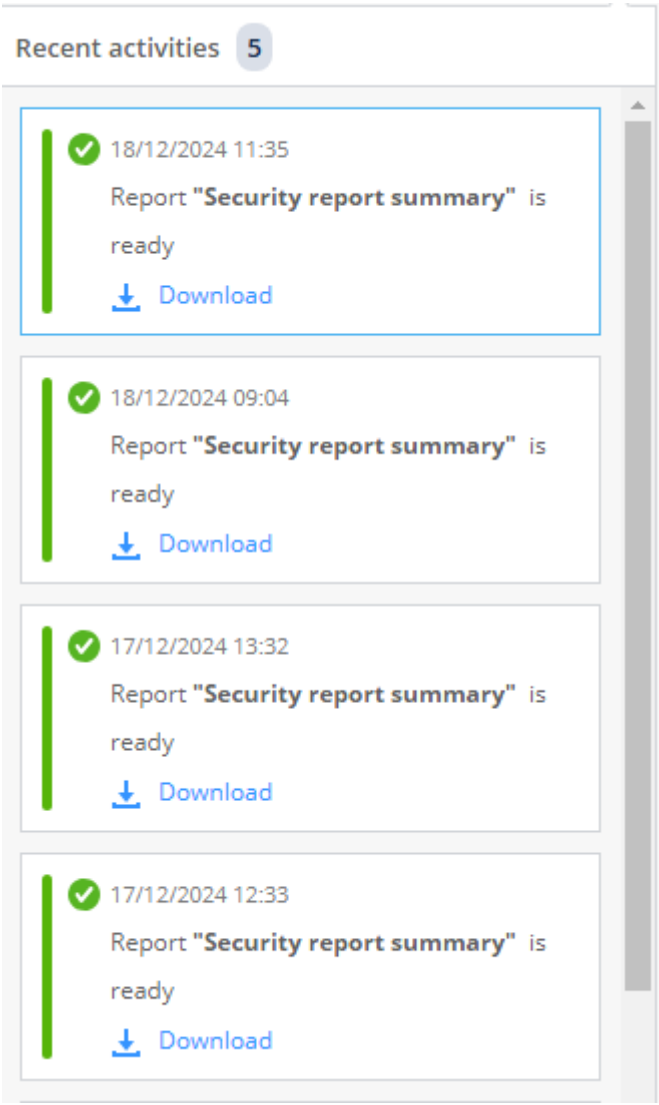
2. To generate the report, click **Generate report**.

   The **Generate Report** window appears.



3. From the **Period** list, select the time frame to generate the report.
   - **Last Day** - The system generates the report for the previous day.
   - **Last Week** - The system generates the report for the last seven days.
   - **Last Month** - The system generates the report for the last 30 days.
4. Click **Generate**.

   The **Recent activities** window appears and shows the report generation status.



Note:

The **Recent activities** window shows the download activities from the past seven days.

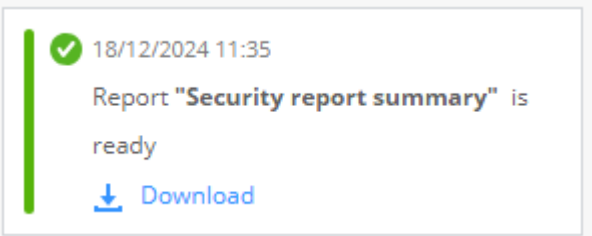
When the report is ready, the system downloads it automatically.

5. To download the report later:

   a. Click the icon at the top-right corner.

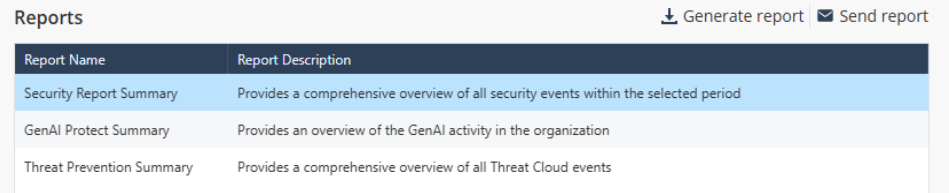
   The **Recent activities** window appears.

b. Click the **Download** link.



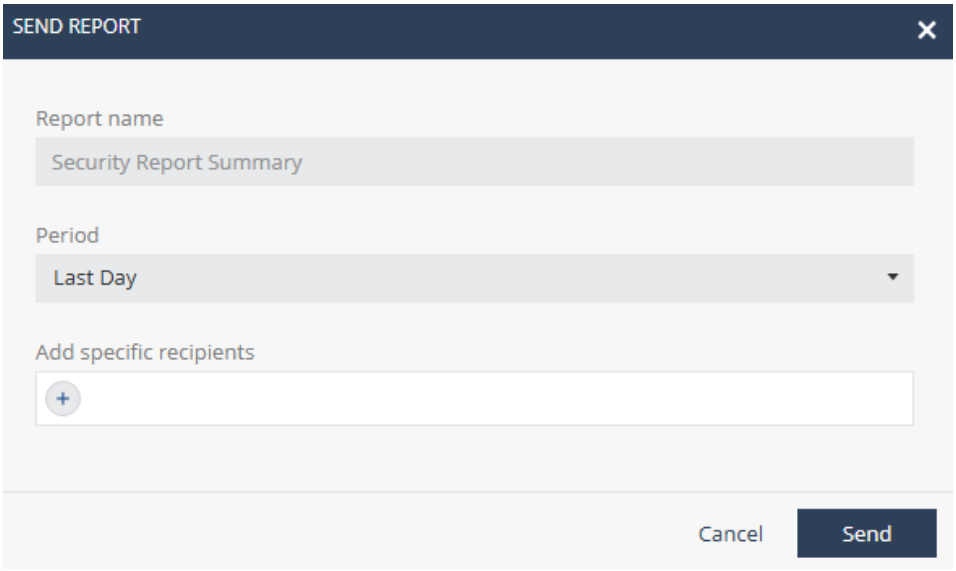
7.2. Sending Reports

1. Go to **Reports** and select the report template in the **Reports** section.



2. Click **Send report**.

   The **Send Report** window appears.



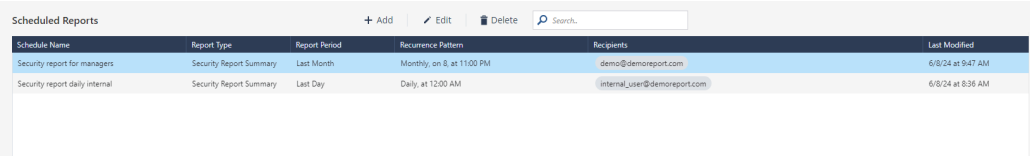
3. From the **Period** list, select the time frame to generate the report.
   - **Last Day** - The system generates the report for the previous day.
   - **Last Week** - The system generates the report for the last seven days.
   - **Last Month** - The system generates the report for the last 30 days.

4. In the **Add specific recipients** field, click **+** and select the recipients.

5. Click **Send**.

7.3. Scheduled Reports

From the **Scheduled Reports** section, you can schedule the generation of summary reports and email it to the required recipients.



The **Scheduled Reports** table shows:

Item	Description
Schedule Name	Name of the scheduled report.
Report Type	Type of the report: • Security Report Summary • GenAI Protect Summary • Threat Prevention Summary
Report Period	Time frame for which the report is generated: • **Last Day** - Generates the report for the previous day. • **Last Week** - Generates the report for the last seven days. • **Last Month** - Generates the report for the last 30 days.
Recurrence Pattern	Frequency, day(s) and time at which the report is sent, in your local time zone.
Recipients	Email addresses of the recipients to whom the report is sent.
Last Modified	Date and time when the scheduled report was last updated.

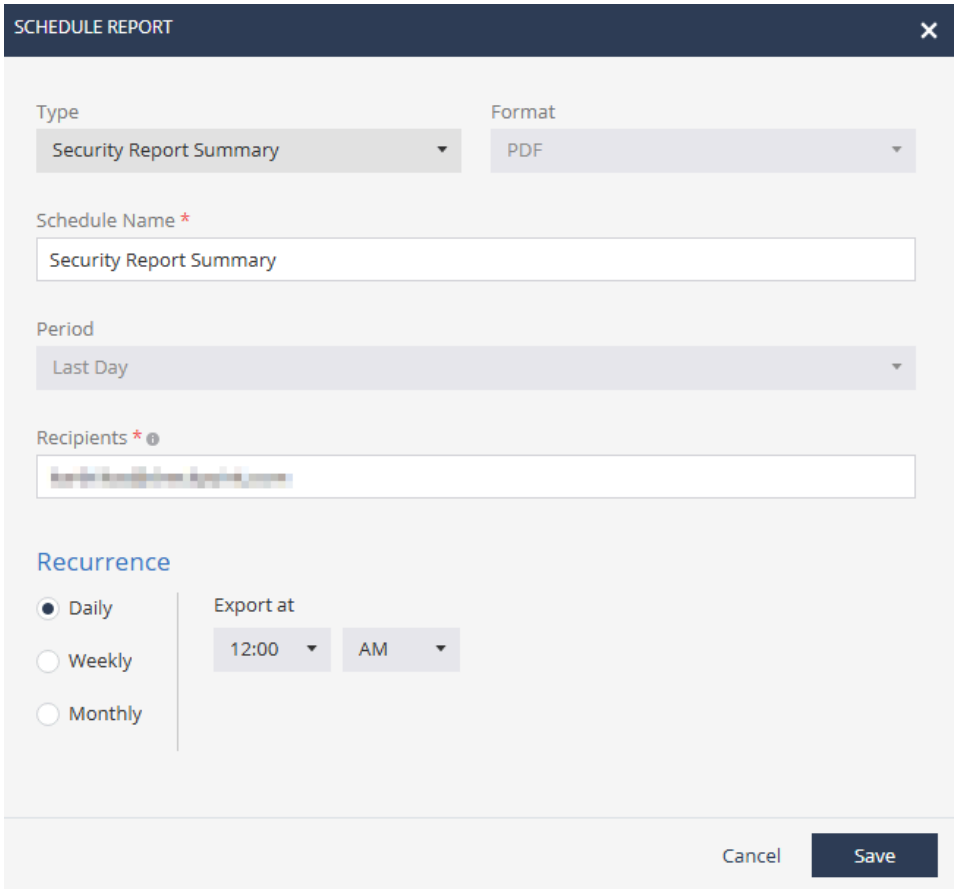
7.4. Adding a Scheduled Report

Important:

To add, edit or delete a scheduled report, you must have **Admin** role in **Global Roles** or in Specific Service Roles *(on page 15)*.

1. Go to **Reports**.
2. In the **Scheduled Reports** section, click **Add**.

   The **Schedule Report** window appears.



3. From the **Type** list, select the report type.
   - Security Report Summary
   - GenAI Protect Summary
   - Threat Prevention Summary
4. In the **Schedule Name** field, enter a name for the scheduled report.
5. From the **Period** list, select the time frame to generate the report.
   - **Last Day** - The system generates the report for the previous day.
   - **Last Week** - The system generates the report for the last seven days.
   - **Last Month** - The system generates the report for the last 30 days.

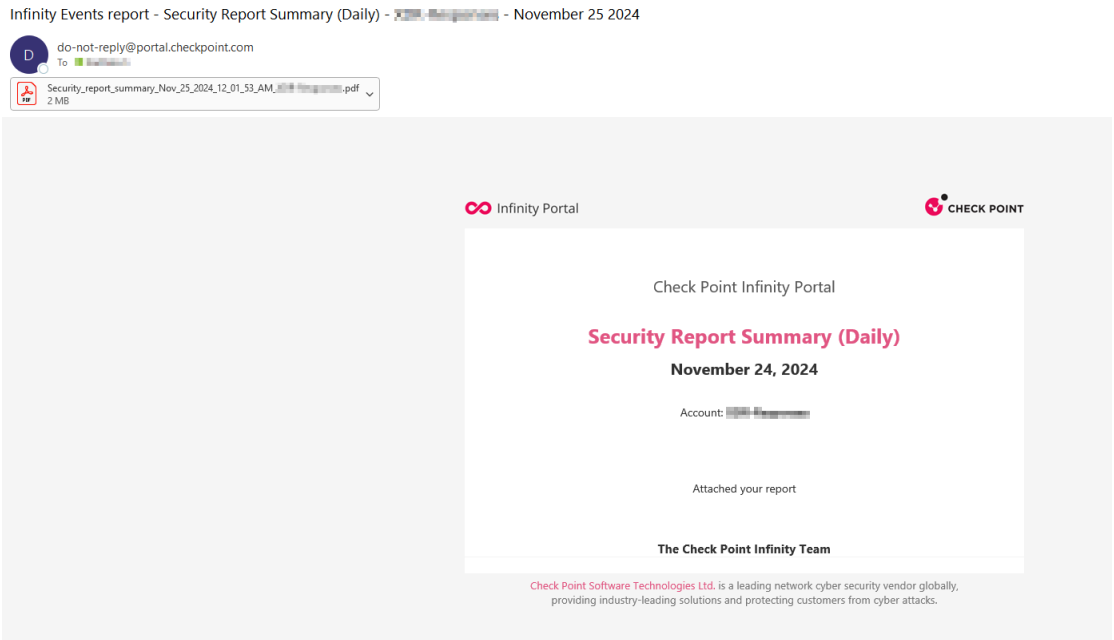
> **Note:**
>
> The **Period** field is enabled only when the **Recurrence** is **Weekly** or **Monthly**.

6. In the **Recipients** field, enter the email address of the recipients, separated by commas.
7. In the **Recurrence** section, configure the recurrence options.
    a. Select the frequency to send the report:
        - **Daily**
        - **Weekly** (You can select multiple days)
        - **Monthly** (You can select multiple dates)
    b. Under **Export at**, select the time to send the report.

> **Note:**
>
> The timezone is the local timezone of the administrator who scheduled the report.

8. Click **Save**.

The system sends the report in PDF format to the specified email addresses.



7.5. Managing Scheduled Reports

1. To edit a scheduled report.
    a. Select the scheduled report and click **Edit**.

    The **Edit Scheduled Report** window appears.

    b. Make the required changes and click **Save**.

2. To search for a scheduled report, enter the text in the **Search** box. Partial text search is supported.
3. To delete a scheduled report, select the report and click **Delete**.

8. Reports for MSPs

Topics:

Important:

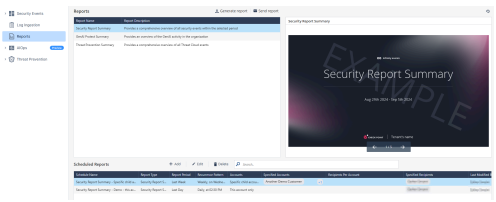
From this page, MSPs can schedule reports for child accounts within the same region. If a child account is located in a different region, you need to schedule the reports directly from that child account, as described in Reports *(on page 40)*.

The **Reports** page allows Managed Service Providers (MSP) administrators to generate these reports for their child accounts.

- **Security Report Summary** - Provides an overview of security events for the Check Point products you are subscribed to in Check Point Portal.
- **GenAI Protect Summary** - Provides an overview of the GenAI activity in your organization.
- **Threat Prevention Summary** - Provides an overview of all Threat Prevention events for the Check Point products you are subscribed to in Check Point Portal.

You can generate the report on demand or create a schedule to generate the report and send it to the required recipients.

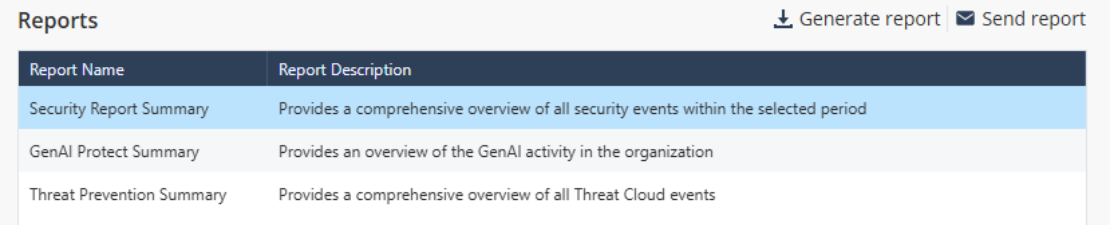
To view the **Reports** page, access the Events & AIOps Administrator Portal *(on page 13)* and click **Reports**.



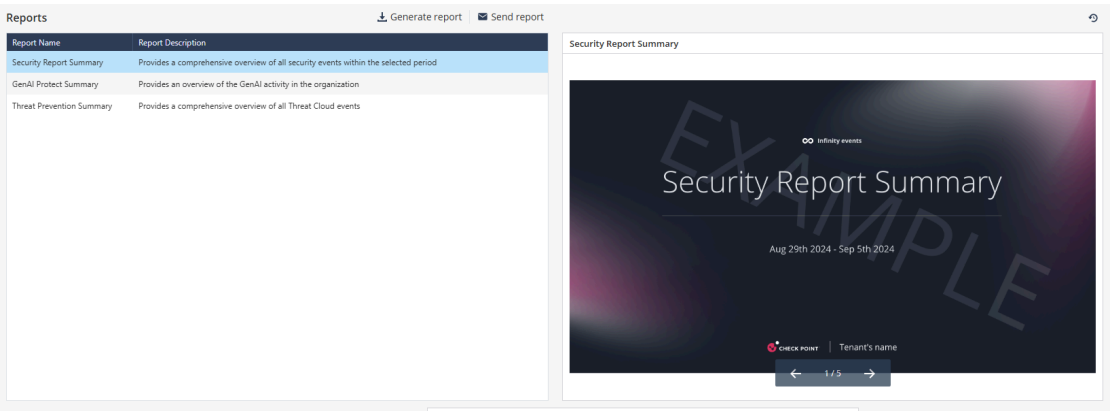
8.1. Generating Reports On Demand

From the **Reports** section, you can generate and download the Security Report Summary on demand.

1. Go to **Reports** and select the report template in the **Reports** section.

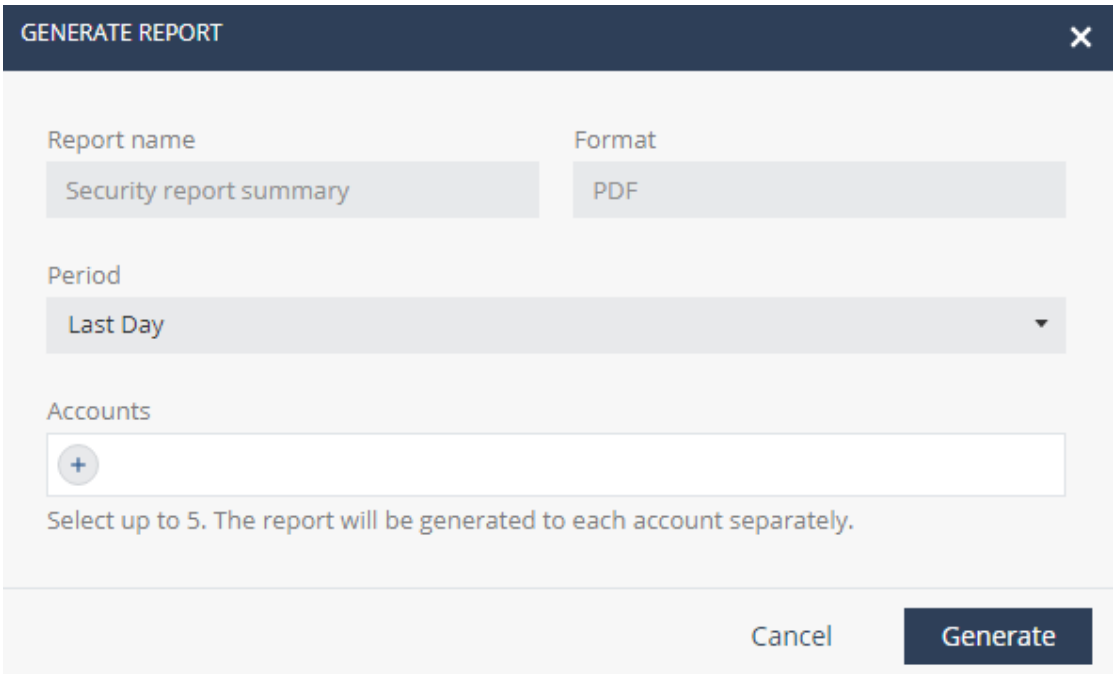


The system displays the sample report on the right side.



2. To generate the report, click **Generate report**.

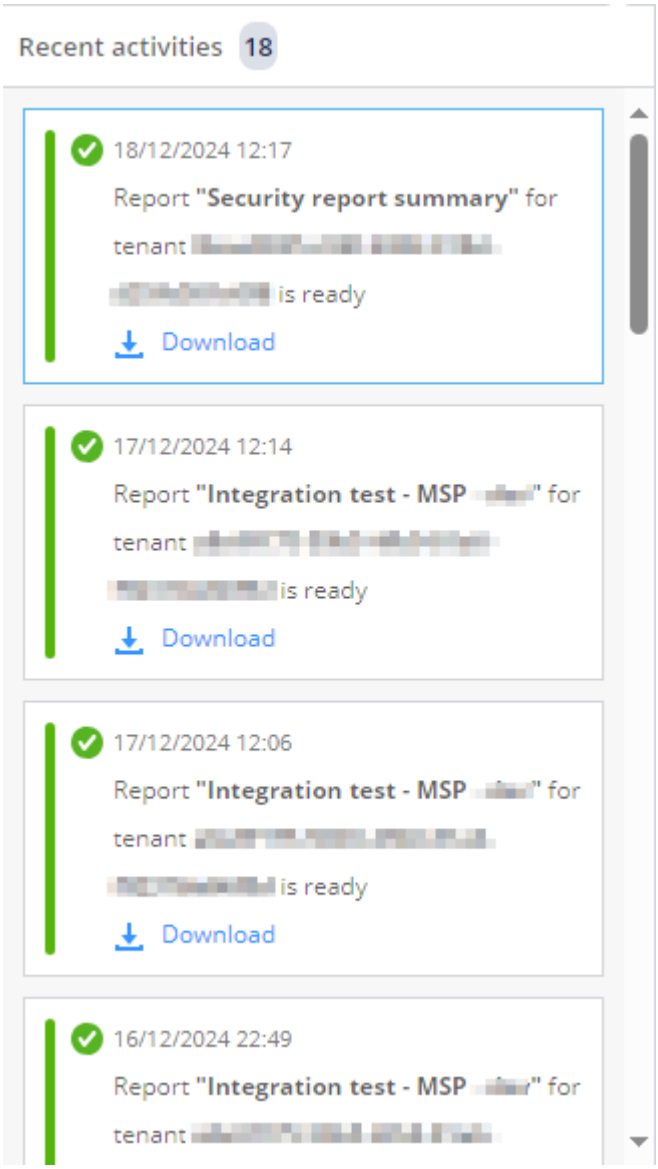
The **Generate Report** window appears.



3. From the **Period** list, select the time frame to generate the report.
    - **Last Day** - The system generates the report for the previous day.
    - **Last Week** - The system generates the report for the last seven days.
    - **Last Month** - The system generates the report for the last 30 days.
4. In the **Accounts** field, click **+** and then select the child accounts.

    You can select up to five accounts.
5. Click **Generate**.

    The **Recent activities** window appears and shows the report generation status.



Note:

The **Recent activities** window shows the download activities from the past seven days.

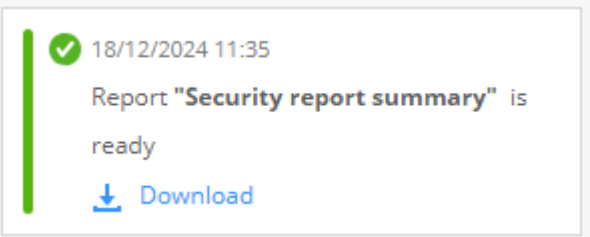
When the report is ready, the system downloads it automatically. If you selected multiple accounts, it downloads each report separately.

6. To download the report later:

   a. Click the icon at the top-right corner.

   The **Recent activities** window appears.

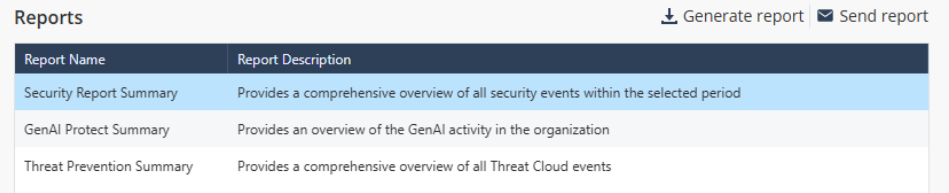
   b. Click the **Download** link.



8.2. Sending Reports

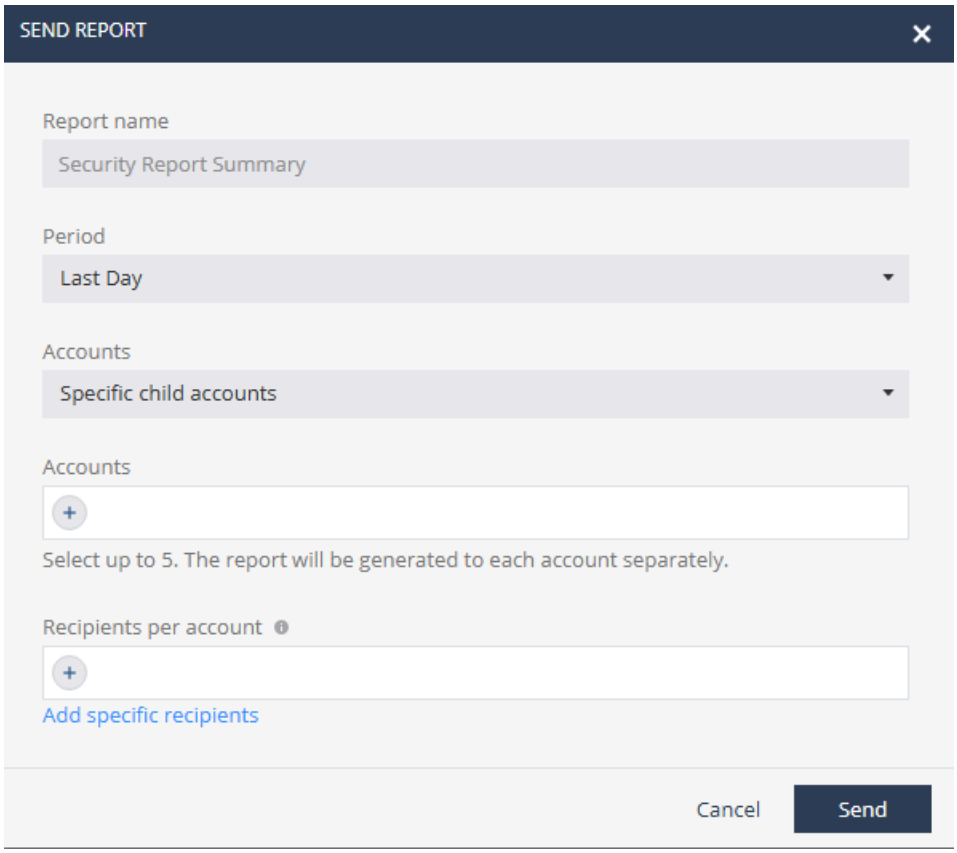
To send a report to specific users, follow these steps.

1. Go to **Reports** and select the report template in the **Reports** section.



2. Click **Send report**.

   The **Send Report** window appears.



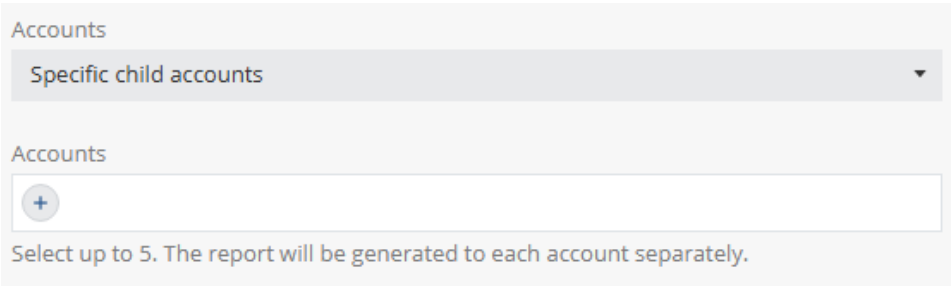
3. From the **Period** list, select the time frame to generate the report.
    - **Last Day** - The system generates the report for the previous day.
    - **Last Week** - The system generates the report for the last seven days.
    - **Last Month** - The system generates the report for the last 30 days.

4. From the **Accounts** list:

    - To send the report to recipients of specific child accounts:

        a. Select **Specific child accounts**.

        b. From the **Accounts** list, click **+** and select the child accounts you want to include.



        Each report will contain information specific to the individual child account.

5. From the **Recipients per account** list, click **+** and select the user roles of recipients in the account that receive the report.

- **Primary Admins** - Users with **Primary Administrator** role in **Global Roles** in the selected account.
- **Tenant Admins** - Users with **Admin** role in **Global Roles** or in **Specific Service Roles** in the selected account.
- **Read-Only** - Users with **Read-Only** role in **Global Roles** or in **Specific Service Roles** in the selected account.

> **Note:**
>
> If the account does not have any users with the selected role, the system will not send the report.

6. To send the report to specific recipients, click **Add specific recipients** and select the recipients.
   - To send the report only to recipients of MSP account:
     a. Select **This account only**.
     b. In the **Recipients** field, click **+** and select the user roles of recipients in the account that receive the report.
        - **Primary Admins** - Users with **Primary Administrator** role in **Global Roles** in the selected account.
        - **Tenant Admins** - Users with **Admin** role in **Global Roles** or in **Specific Service Roles** in the selected account.
        - **Read-Only** - Users with **Read-Only** role in **Global Roles** or in **Specific Service Roles** in the selected account.

        > **Note:**
        >
        > If the account does not have any users with the selected role, the system will not send the report.

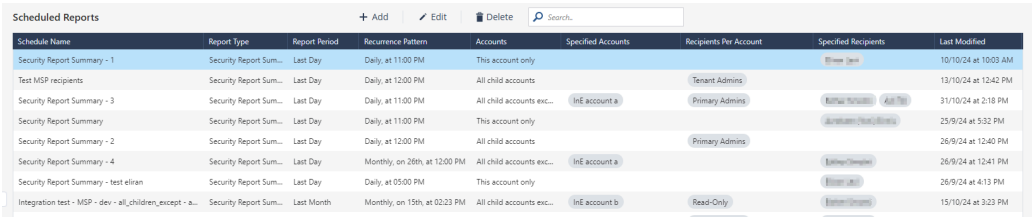
7. To send the report to specific recipients, click **Add specific recipients** and select the recipients.

   The report will include consolidated security events from both MSP account and all its child accounts.

8. Click **Send**.

8.3. Scheduled Reports

From the **Scheduled Reports** section, you can schedule the generation of summary reports and email it to the required recipients.



The **Scheduled Reports** table shows:

Item	Description
Schedule Name	Name of the scheduled report.
Report Type	Type of the report: • Security Report Summary • Threat Prevention Summary
Report Period	Time frame for which the report is generated: • **Last Day** - Generates the report for the previous day. • **Last Week** - Generates the report for the last seven days. • **Last Month** - Generates the report for the last 30 days.
Recurrence Pattern	Frequency, day(s) and time at which the report is sent, in your local time zone.
Accounts	Accounts to which the report is sent: • **This account only** - Report is sent only to the MSP account administrator or the configured MSP users. The report will include consolidated security events from both MSP account and all its child accounts. • **All child accounts** - Report is sent to recipients of all the child accounts. Each account will get report with its security events only. • **Specific child accounts** - Report is sent to recipients of the child accounts specified in the **Specified Accounts** column. • **All child accounts except** - Report is sent to recipients of all child accounts except the accounts specified in the **Specified Accounts** column.

Item	Description
Specified Accounts	Specified child accounts to which the report is sent / not sent.
Recipients Per Account	User roles of recipients in the account that receive the report.
Specified Recipients	Specific MSP users to whom all child account reports are sent.
Last Modified	Date and time when the scheduled report was last updated.

8.3.1. Scheduled Report Settings

Item	Description
Schedule Name	Name of the scheduled report.
Report Type	Type of the report: • Security Report Summary • Threat Prevention Summary
Report Period	Time frame for which the report is generated: • **Last Day** - Generates the report for the previous day. • **Last Week** - Generates the report for the last seven days. • **Last Month** - Generates the report for the last 30 days.
Recurrence Pattern	Frequency, day(s) and time at which the report is sent, in your local time zone.
Accounts	Accounts to which the report is sent:

Item	Description
	• **This account only** - Report is sent only to the MSP account administrator or the configured MSP users. The report will include consolidated security events from both MSP account and all its child accounts. • **All child accounts** - Report is sent to recipients of all the child accounts. Each account will get report with its security events only. • **Specific child accounts** - Report is sent to recipients of the child accounts specified in the **Specified Accounts** column. • **All child accounts except** - Report is sent to recipients of all child accounts except the accounts specified in the **Specified Accounts** column.
Specified Accounts	Specified child accounts to which the report is sent / not sent.
Recipients Per Account	User roles of recipients in the account that receive the report.
Specified Recipients	Specific MSP users to whom all child account reports are sent.
Last Modified	Date and time when the scheduled report was last updated.

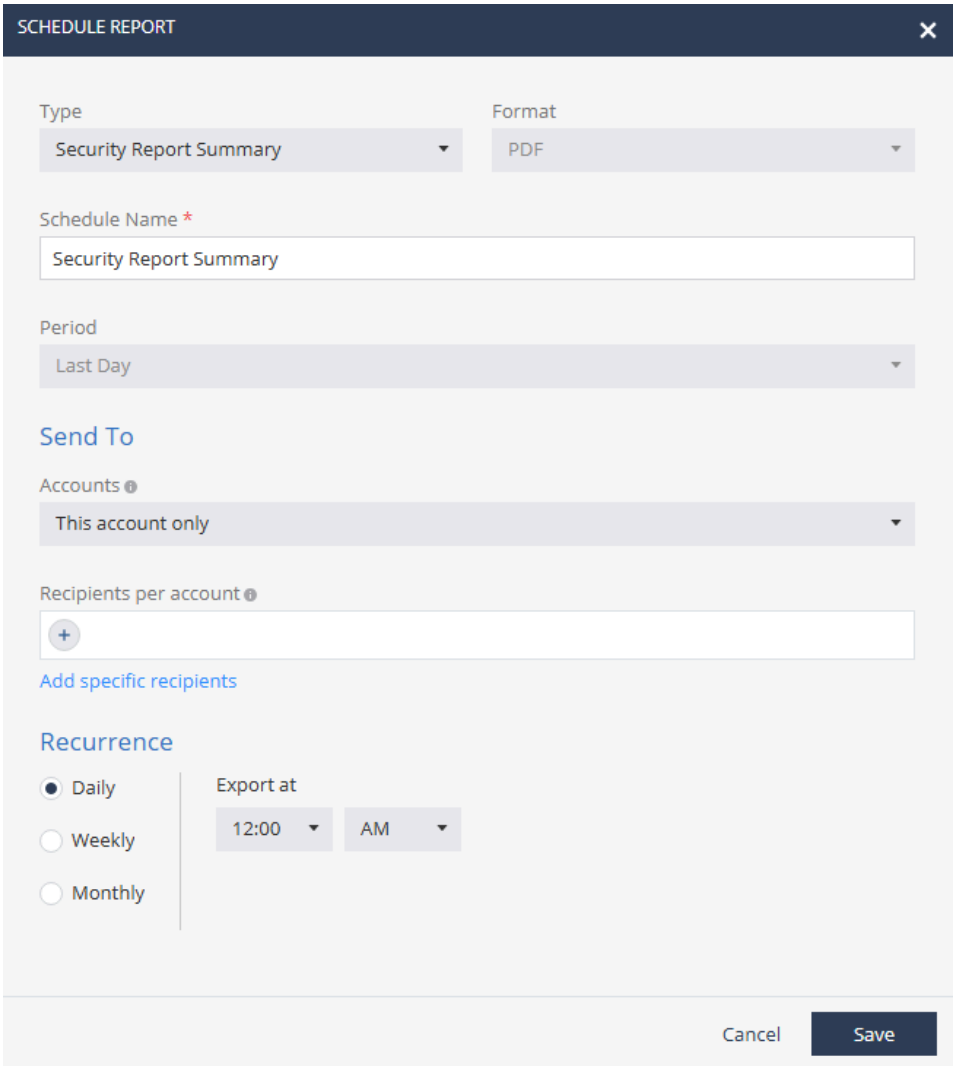
8.4. Adding a Scheduled Report

Important:

To add, edit or delete a scheduled report, you must have **Admin** role in **Global Roles** or Specific Service Roles *(on page 15)*.

1. Go to **Reports**.
2. In the **Scheduled Reports** section, click **Add**.

   The **Schedule Report** window appears.



3. From the **Type** list, select the report type.
    - Security Report Summary
    - Threat Prevention Summary
4. In the **Schedule Name** field, enter a name for the scheduled report.
5. From the **Period** list, select the time frame to generate the report.
    - **Last Day** - The system generates the report for the previous day.
    - **Last Week** - The system generates the report for the last seven days.
    - **Last Month** - The system generates the report for the last 30 days.

> **Note:**
>
> The **Period** field is enabled only when the **Recurrence** is **Weekly** or **Monthly**.

6. In the **Send To** section, configure recipient settings.

a. From the **Accounts** list:

- To send the security report only to the recipients of MSP account, select **This account only**.

  The report will include consolidated security events from both MSP account and all its child accounts.

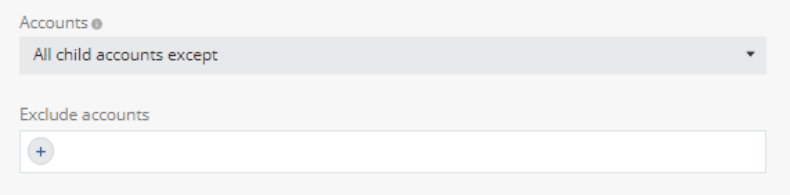
- To send the report to the recipients of all child accounts, select **All child accounts**.

  Each report will contain information specific to the individual child account.

  > **Note:**
  >
  > This includes both existing and new child accounts.

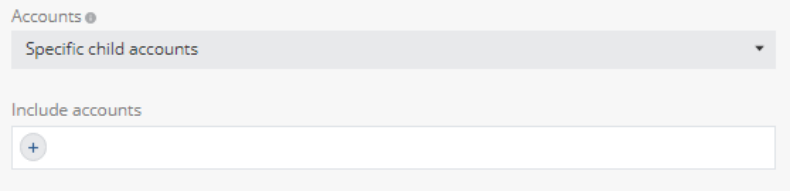
- To exclude recipients in some child accounts, select **All child accounts except**.

  From the **Exclude accounts** list, click **+** and select the child accounts you want to exclude.



- To send the report to recipients of specific child accounts, select **Specific child accounts**.

  From the **Include accounts** list, click **+** and select the child accounts you want to include.



b. From the **Recipients per account** list, click **+** and select the user roles of recipients in the account that receive the report.

- **Primary Admins** - Users with **Primary Administrator** role in **Global Roles** in the selected account.
- **Tenant Admins** - Users with **Admin** role in **Global Roles** or in **Specific Service Roles** in the selected account.
- **Read-Only** - Users with **Read-Only** role in **Global Roles** or in **Specific Service Roles** in the selected account.

> **Note:**
>
> If the account does not have any users with the selected role, the system will not send the report.

c. To send the report to specific users in the MSP account:

i. Click **Add specific recipients**.

ii. Click **+** and add the recipients.

These MSP users will receive the security reports of all the child accounts configured in **Accounts**.

7. In the **Recurrence** section, configure how often the report is sent.

a. Select the frequency to send the report:

- **Daily**
- **Weekly** (You can select multiple days)
- **Monthly** (You can select multiple dates)

b. Under **Export at**, select the time to send the report.

> **Note:**
>
> The timezone is the local timezone of the administrator who scheduled the report.

8. Click **Save**.

The system sends the report in PDF format to the email addresses of the selected account admins or users.

8.5. Managing Scheduled Reports

1. To edit a scheduled report.
    a. Select the scheduled report and click **Edit**.

       The **Edit Scheduled Report** window appears.

    b. Make the required changes and click **Save**.
2. To search for a scheduled report, enter the text in the **Search** box. Partial text search is supported.
3. To delete a scheduled report, select the report and click **Delete**.

9. AIOps

Topics:

AIOps - Introduction

Onboarding AIOps (Automatic Mode)

AIOps - Overview

Asset Dashboard

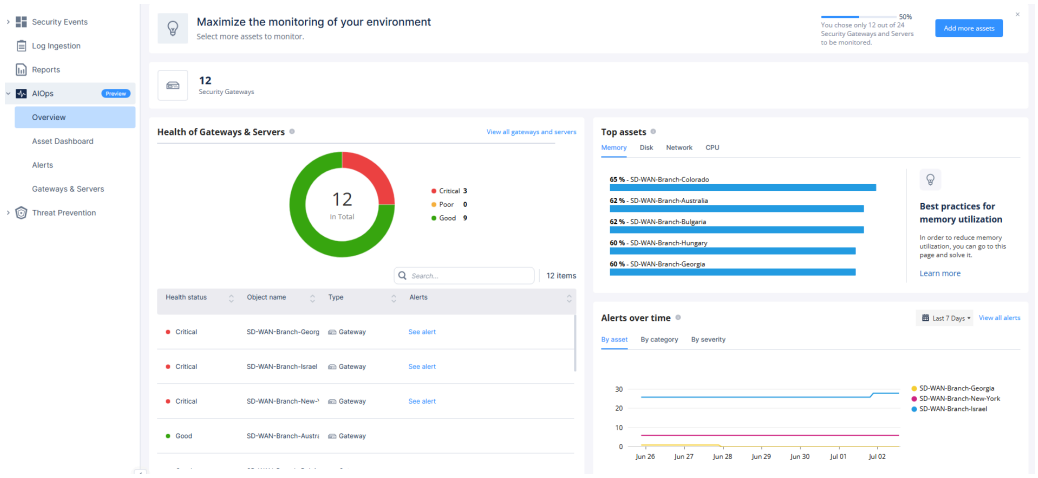
Alerts

Insights

Gateways & Servers

9.1. AIOps - Introduction

AIOps (formerly Infinity AIOps) allows you to monitor your Check Point assets and provides an overview of the monitored assets, assets dashboard and shows the alerts received for the assets.



9.1.1. Benefits

- A single location to view system resource utilization, network traffic and interfaces information of all your Check Point assets.
- Real-time data.
- Identify assets with low performance and/or high resource utilization.

9.1.2. Use Cases

- You have multiple Check Point assets and require a centralized location to monitor their resource utilization.
- You need to view the health status and alerts for the monitored assets, including non-resource related aspects.

9.2. Onboarding AIOps (Automatic Mode)

To monitor your assets with AIOps, you must connect your Security Management Server to your account in the Check Point Portal.

9.2.1. Prerequisites

1. Make sure you have installed the latest Web SmartConsole Package Take 146 or higher. For installation, see sk170314.
2. Creating an Account in the Check Point Portal *(on page)*.

9.2.1.1. Supported Asset Versions

The following table lists the asset versions supported for onboarding AIOps.

Asset	Supported Version
Security Management Server	R82 and later • R82 Jumbo Hotfix Accumulator, Take 25 or later • R81.20 Jumbo Hotfix Accumulator, Take 101 or later • AutoUpdate Packages: ◦ Web SmartConsole, Take 146 or higher Refer to sk170314 ◦ Gws_Onboard_AutoUpdate Take 50 or later
Multi-Domain Security Management Server (MDS)	From R82 and later, MDS can onboard it's Security Gateways but not the Security Management Server. For limitations, see sk182647.
Security Gateway	R81.20 and later

Asset	Supported Version
Supported Topologies • VSX Security Gateway, VSNext • ElasticXL Gateway • Cluster, ClusterXL	• Supported topologies are supported from R82 and later.
Cloud Firewall Gateway	R82 and later
Maestro Security Gateway	R82 and later

Note:

- Make sure that BUNDLE_QUID_AUTOUPDATE Take 57 or later is installed on all onboarded assets. If not, refer to sk181458-CPquid (QUID) Release Updates.
- For onboarding on earlier versions, see the **Non-Formal Onboarding** section in sk182647
- For product limitations, see sk182647.

9.2.1.2. Connectivity Requirements

To enable data transmission from the user environment to AIOps, ensure that outbound **HTTPS** connections are allowed to the following IP addresses and URLs.

9.2.1.2.1. Static IPs

Region	Portal URL	Static IP Addresses
CA	portal.checkpoint.com	• 166.117.123.221 • 99.83.217.236
AU	portal.checkpoint.com	• 15.197.214.233 • 3.33.222.204

Region	Portal URL	Static IP Addresses
IN	portal.checkpoint.com	• 15.197.167.248 • 3.33.187.244
US	portal.checkpoint.com	• 52.223.30.193 • 35.71.144.247
EU	portal.checkpoint.com	• 75.2.123.205 • 99.83.172.252

9.2.1.2.2. Check Point Portal URLs

Region	Portal URL	Cloud Infra GW	MaaS Mgmt Connect Tunnels Service
EU	portal.checkpoint.com	cloudinfra-gw.portal.checkpoint.com	maas-mgmt-connect-tunnels-service-2.portal.checkpoint.com
US	portal.checkpoint.com	cloudinfra-gw-us.portal.checkpoint.com	maas-mgmt-connect-tunnels-service-us-2.portal.checkpoint.com
AUS	ap.portal.checkpoint.com	cloudinfra-gw.ap.portal.checkpoint.com	maas-mgmt-connect-tunnels-service-ap-2.ap.portal.checkpoint.com

9.2.2. Onboarding Procedure

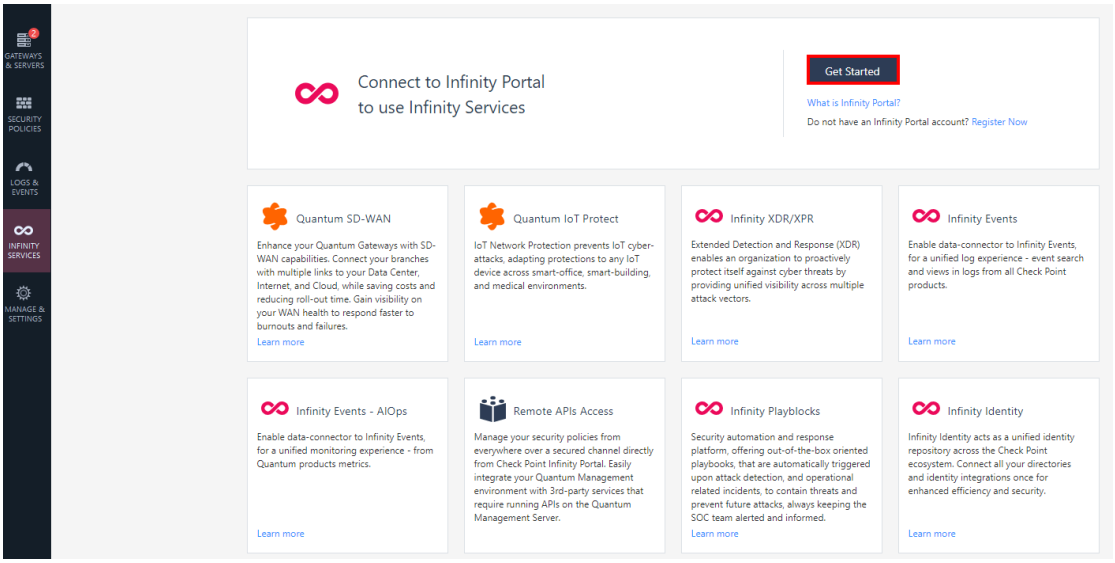
Automatic onboarding enables Security Gateways to securely connect to the Check Point Portal through the Gateways Connector.

Note: For more information, see sk180557.

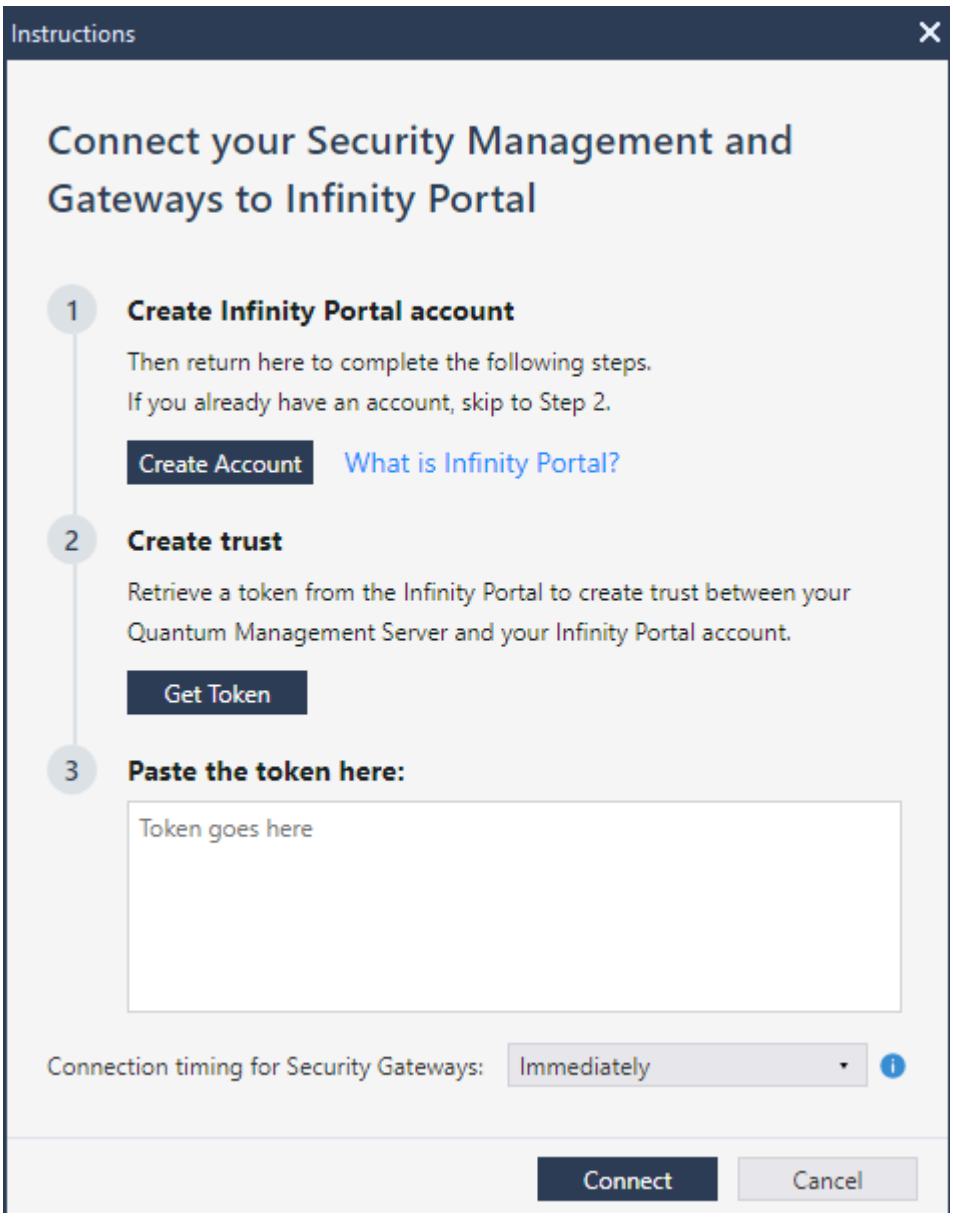
https://embed.app.guidde.com/playbooks/mE5jVcJfu8zX53qt2hE9CB

Onboarding AIOps in Smart Console - Procedure

1. Log in to SmartConsole.
2. Go to **Infinity Services** and click **Get Started**.

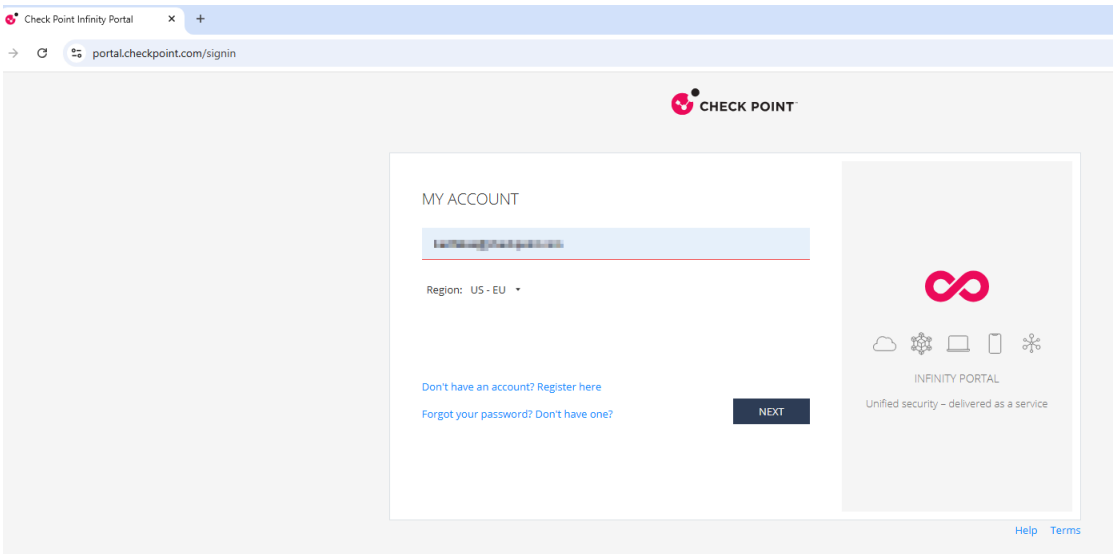


The **Instructions** window appears.



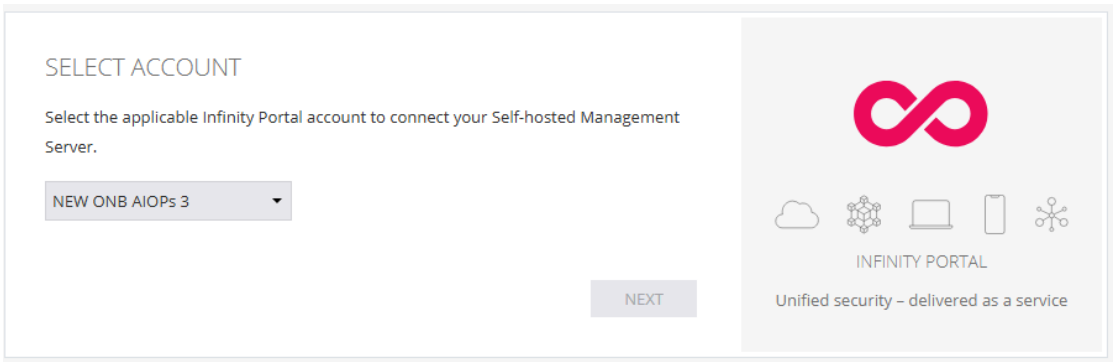
3. To connect your Security Management Server and Security Gateways to Check Point Portal, click **Get Token**.

   The Check Point Portal **Sign In** page appears.

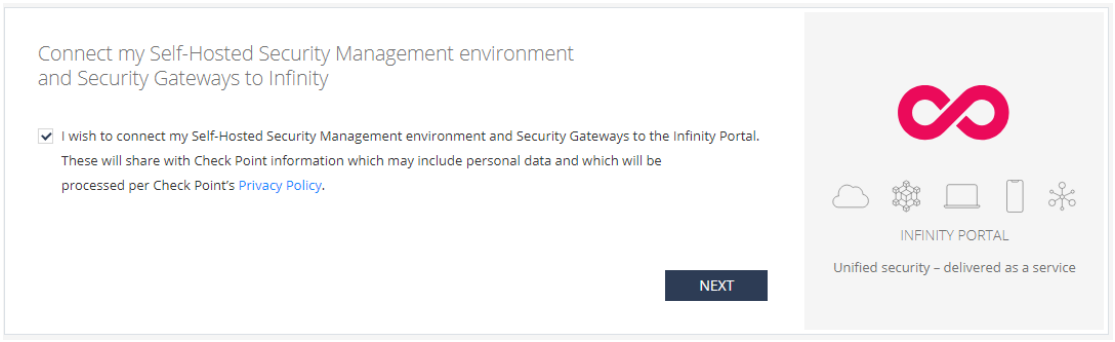


4. Click **Next**.

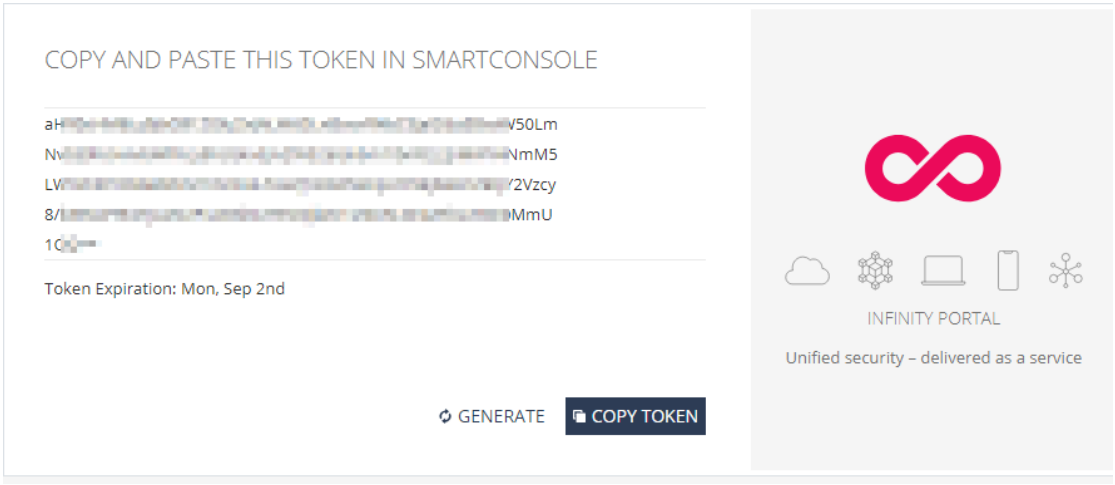
5. Select your Check Point Portal account and click **Next**.



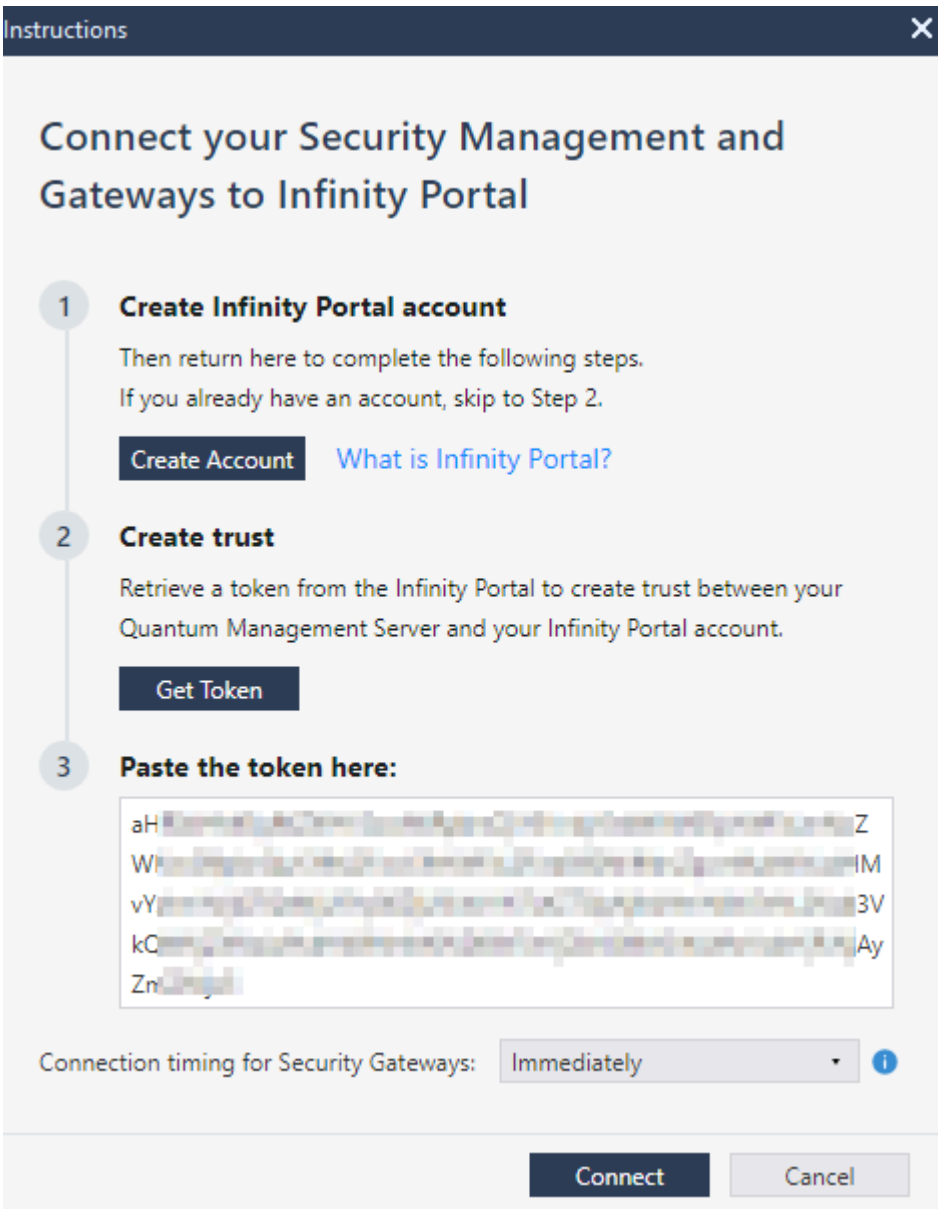
6. Accept the terms of service and click **Next**.



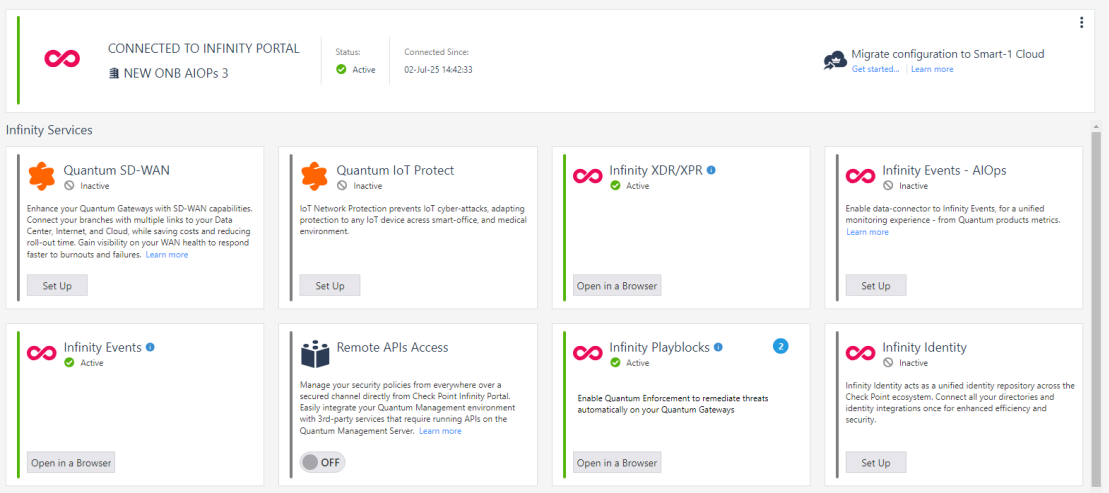
7. Click **Copy Token**.



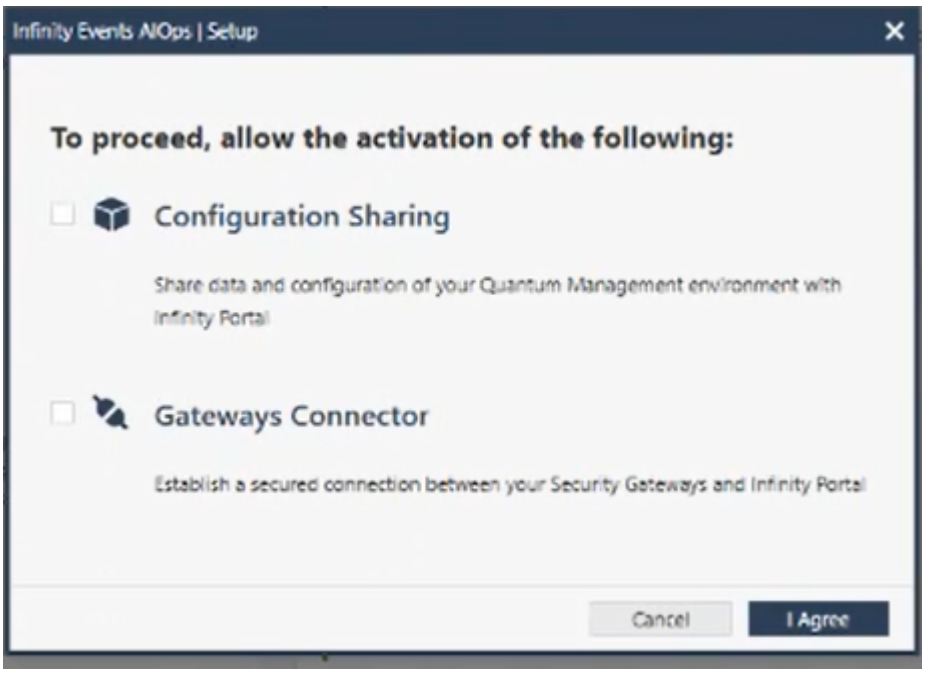
8. In the SmartConsole **Instructions** window, paste the token and click **Connect**.



When the Management Server is connected to your Check Point Portal account, the **Status** changes to **Active**.



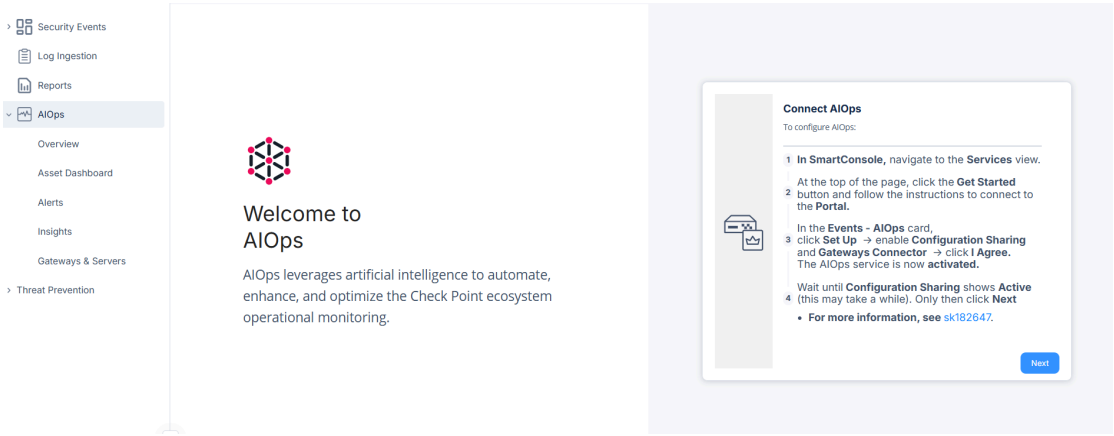
9. To activate AIOps, in the **Infinity Events - AIOps** widget, click **Set Up**.
10. In the dialog box, select **Configuration Sharing** and **Gateways Connector** and then click **I Agree**.



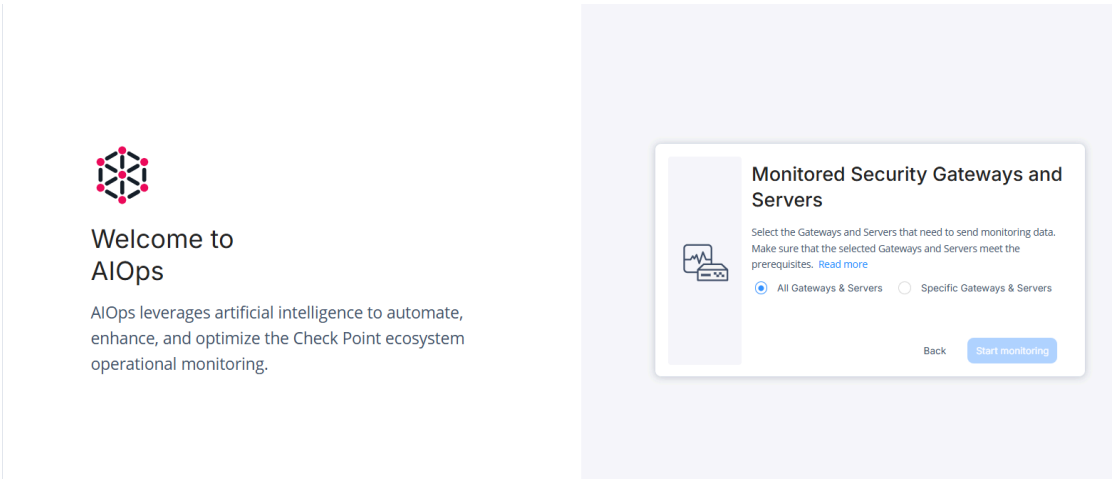
When the setup is completed, the status of **Infinity Events - AIOps** card becomes **Active**.

> **Note:**
>
> The initialization process may take some time. To monitor the progress, click the ⋮ icon on the top-right corner.

11. Log in to Check Point Portal and access the Events & AIOps Administrator Portal.
12. From the left navigation panel, click AIOps.



13. In the **Connect AIOps** widget, click **Next**.
14. In the **Monitored Security Groups and Servers** widget, select the required gateways and servers and then click **Start Monitoring**.

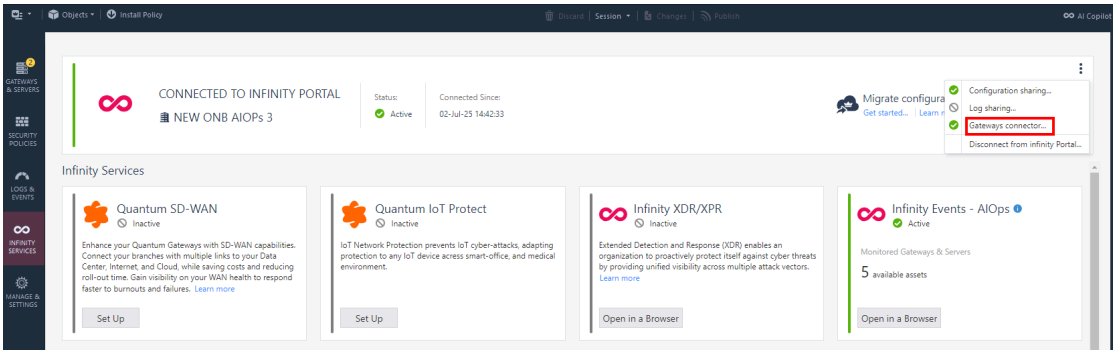


For guidance on common AIOps troubleshooting scenarios, see the **Troubleshooting** section in sk182647.

9.2.2.1. Disable the connection between gateways and Infinity Portal

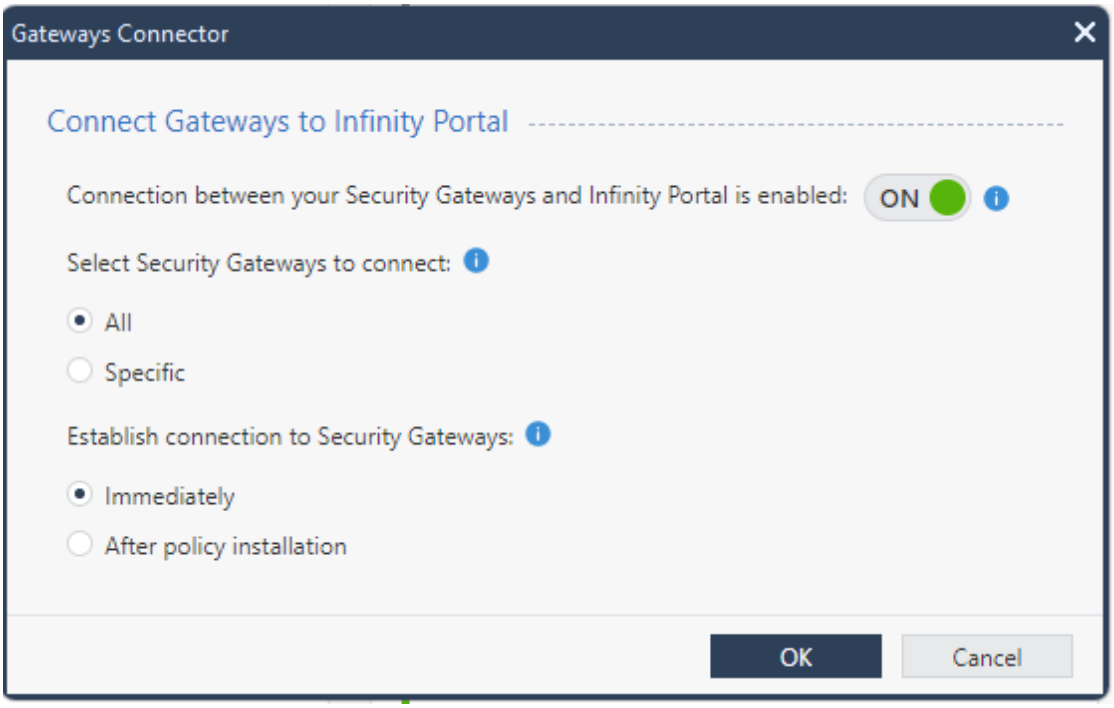
To disable the connection between Security Gateways and Check Point Portal:

1. Click the ⋮ icon on the top-right corner and click **Gateways connector**.



The **Gateways Connector** window appears.

2. Turn off the toggle button.



3. Click **OK**.

If you disable **Gateways Connector**, you need to set up **Infinity Events - AIOps** again.

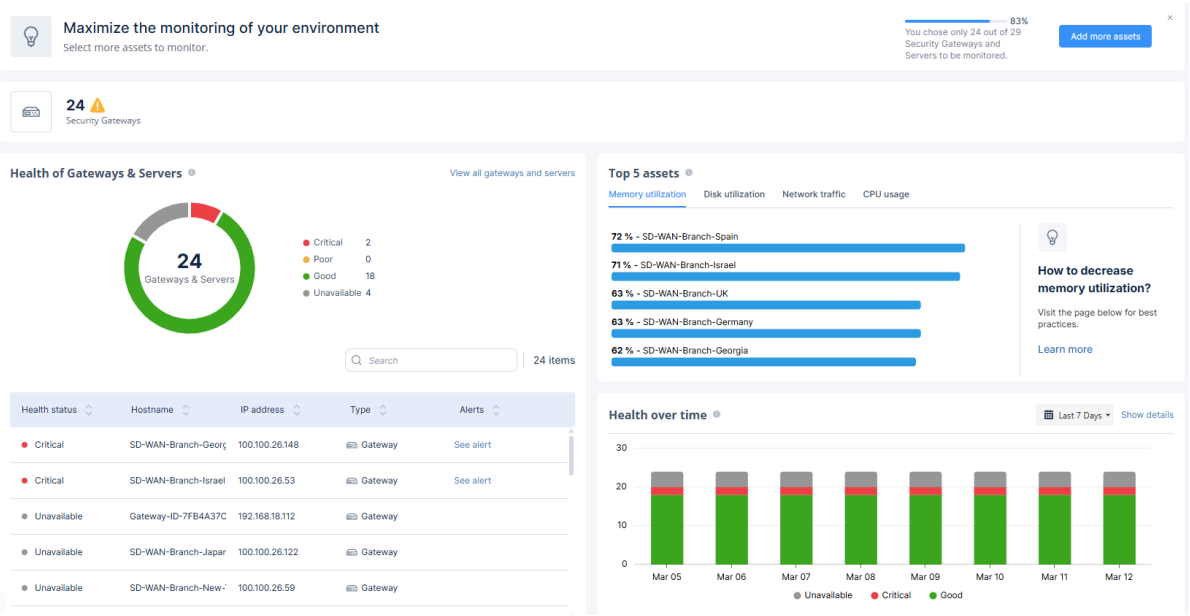
9.2.3. Known Limitations

For known limitations in AIOps, see sk182647.

9.3. AIOps - Overview

The **Overview** page under **AIOps** provides an overview of the monitored assets.

To view the **Overview** page, access the Events & AIOps Administrator Portal *(on page 13)* and go to **AIOps** > **Overview**.



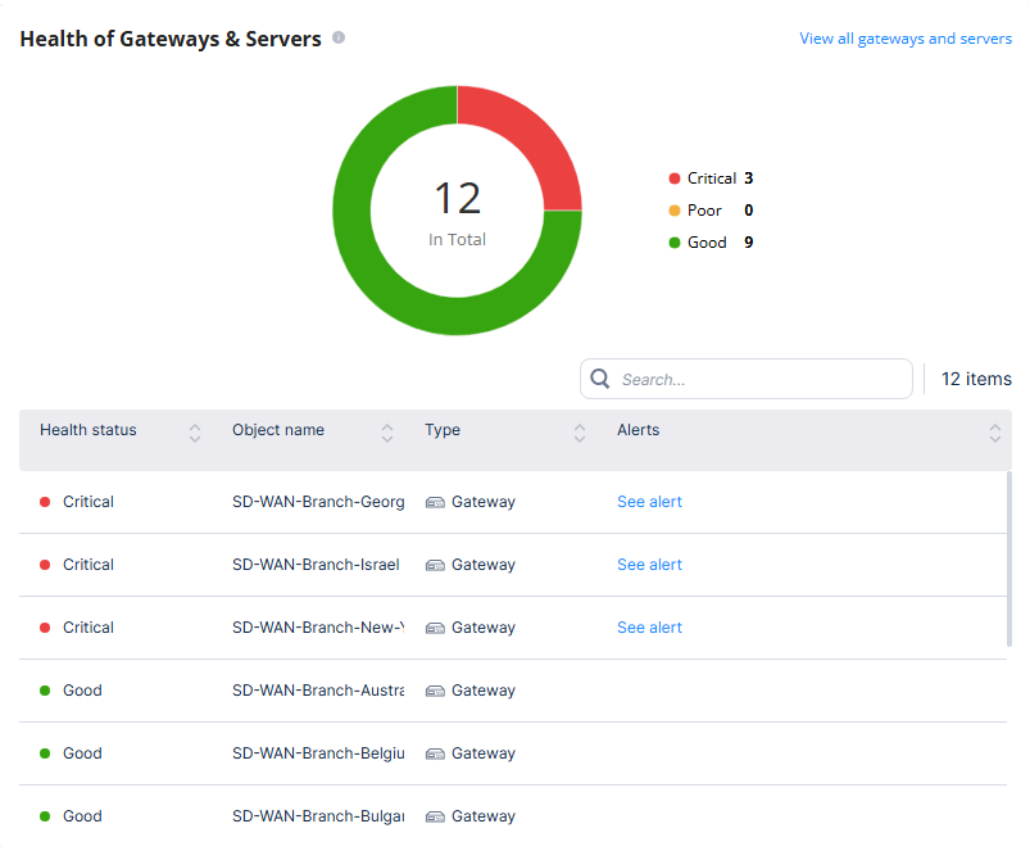
The top banner displays the number of connected and monitored assets. To connect more assets, click **Add more assets**. The Gateways & Servers *(on page 95)* page appears where you can add the assets.

Note:

This banner appears only when there are unconnected assets.

The number of physical assets connected in each asset type are shown below the banner.

9.3.1. Health of Gateways and Servers



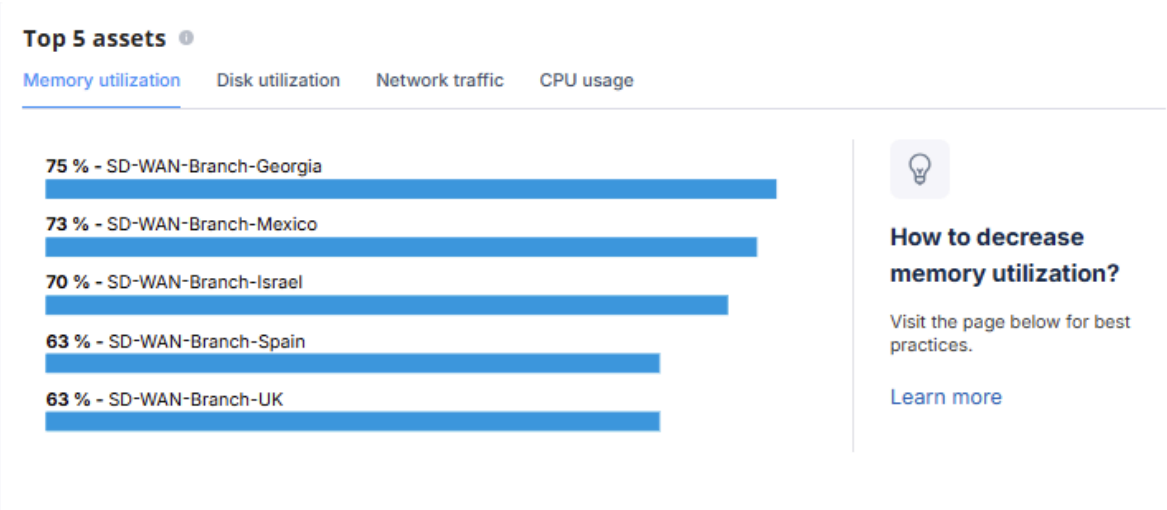
The **Health of Gateways & Servers** widget displays:

- A pie chart that shows the total number of physical and virtual assets connected and their health status according to the severity of alerts:
  - Good
  - Poor
  - Critical
  - Unavailable

  > **Note:**
  >
  > The pie chart shows the health status over the past five seconds.

- A table with the health status of specific Gateways & Servers and links to their associated alerts.

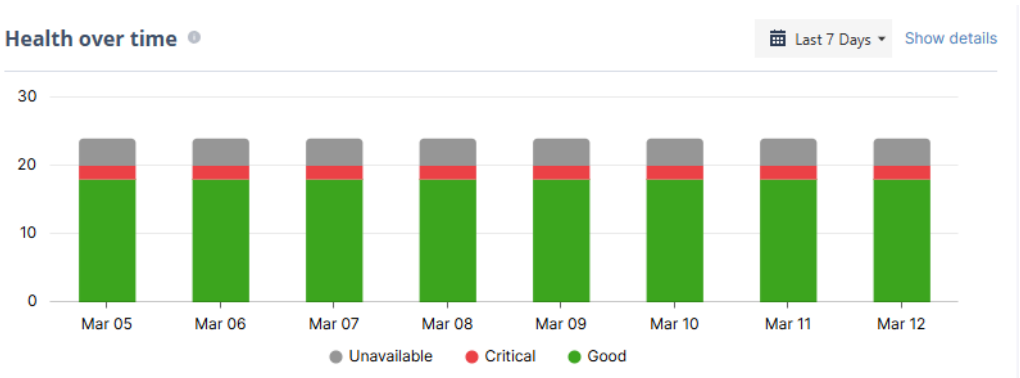
9.3.2. Top 5 Assets



The **Top 5 assets** widget displays the top five assets in these categories and provides the best practices to reduce resource utilization:

- **Memory utilization** - Top five assets with the highest memory utilization (RAM).
- **Disk utilization** - Top five assets with the highest disk space utilization.
- **Network traffic** - Top five assets that received the highest network traffic.
- **CPU usage** - Top five assets with the highest CPU usage.

9.3.3. Health Over Time

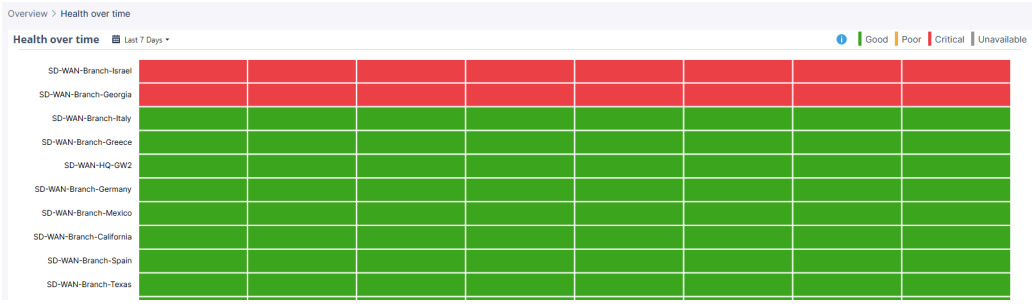


The **Health over time** widget displays the health status of monitored assets over a specific time period. The possible statuses are:

- Good
- Critical
- Unavailable

By default, the widget displays health status for the last **seven** days. You can select the time period from the top-right corner.

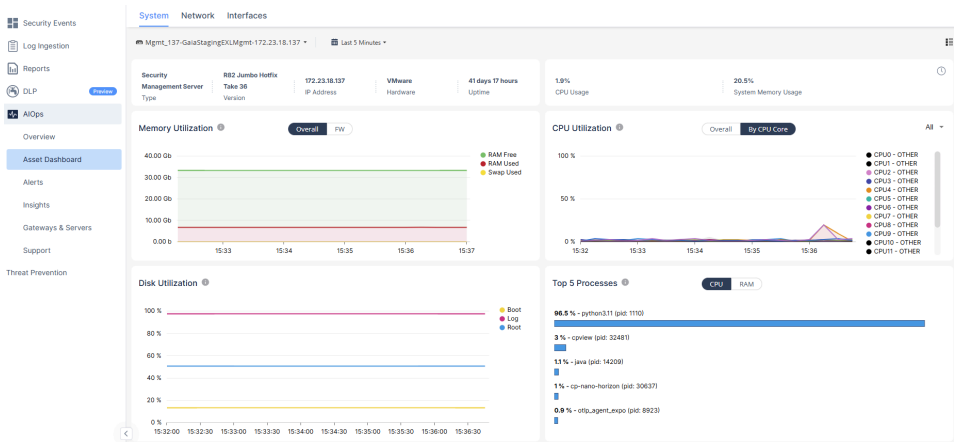
To view the health status of each asset, click the **Show details** link. The system displays the health status of all monitored assets for the selected time period.



9.4. Asset Dashboard

The **Asset Dashboard** page displays asset details in these categories:

- **System** - System resource utilization of assets. See System *(on page 75)*
- **Network** - Network traffic data of assets. See Network *(on page 78)*.
- **Interfaces** - Network interface data of assets. See Interfaces *(on page 81)*.
- **VPN** - VPN information of assets. See VPN *(on page 83)*.
- **Hardware** - Hardware information of assets. See Hardware *(on page 85)*.
- **CloudGuard** - CloudGuard information of assets. See CloudGuard *(on page 87)*.



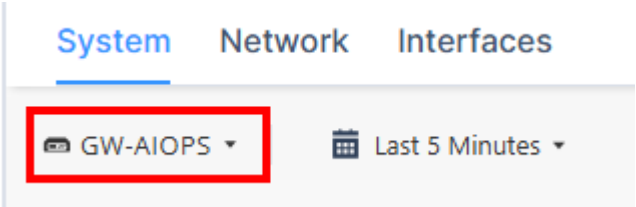
Note:

The tabs and widgets displayed depend on the supported asset types.

For supported asset types, see the **Prerequisites** section in sk182647.

To view the **Asset Dashboard** for a Check Point asset:

1. Access the Events & AIOps Administrator Portal *(on page 13)*.
2. Go to **AIOps** > **Asset Dashboard**.
3. Select the asset from the list at the top.



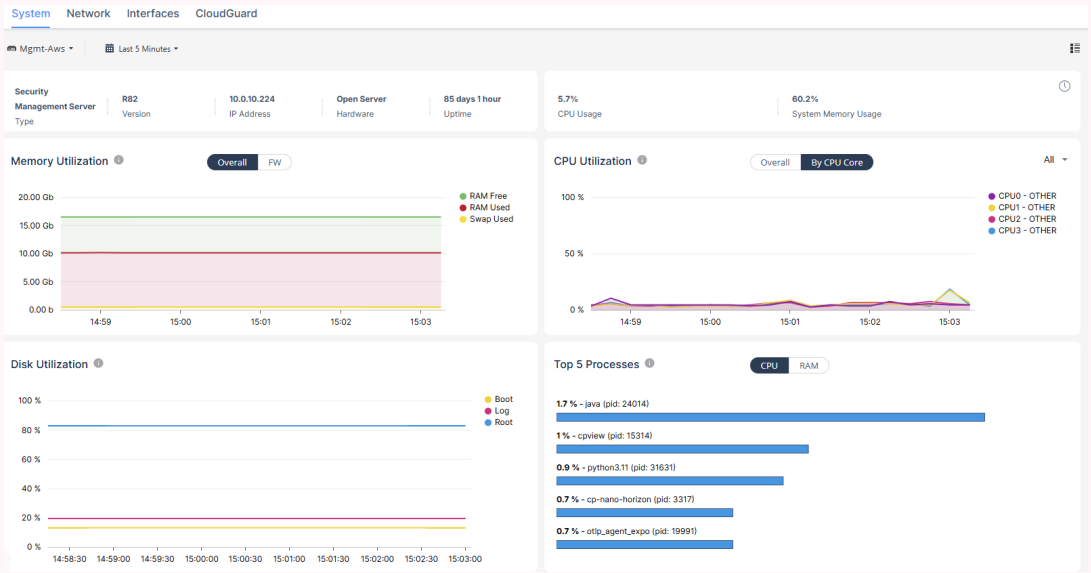
4. Click the icon and select the period for which you want to view the data. The default is **Last 5 Minutes**.

> **Note:**
>
> The widgets show data only for a maximum of 30 days.

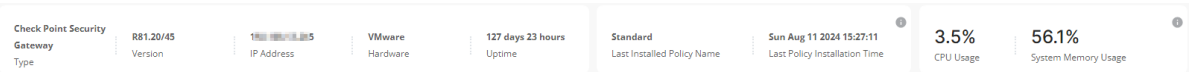
5. Select the required tab.

9.4.1. System

> **Note:**
>
> The widgets displayed depend on the asset type and version.



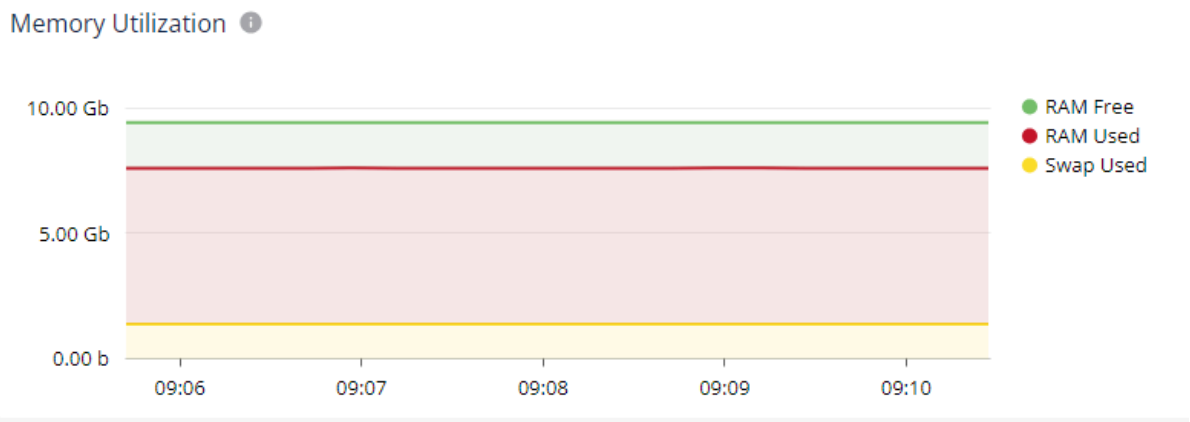
9.4.1.1. Asset Information



The **Asset Information** widget shows:

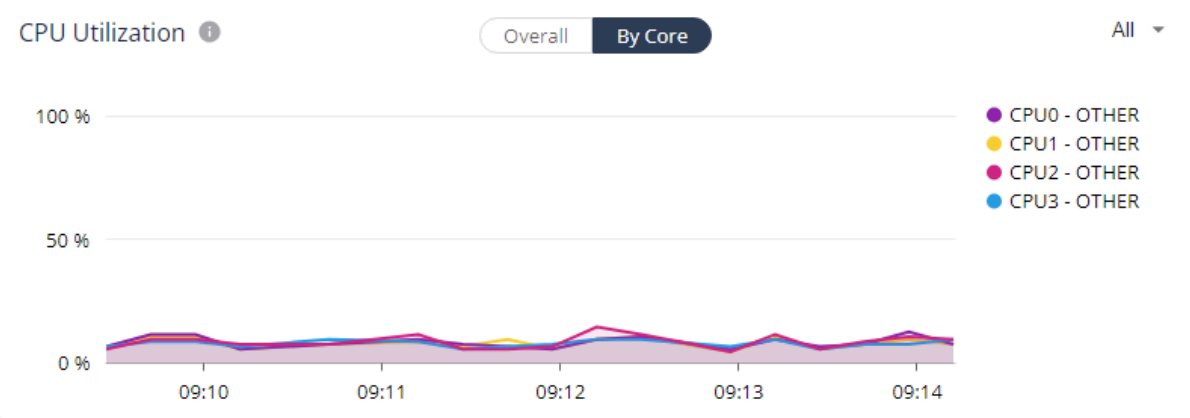
- Asset type
- Release version
- IP Address
- Hardware type
- Uptime
- Name of the last installed policy and its installation time
- CPU usage
- System memory usage

9.4.1.2. Memory Utilization



The **Memory Utilization** widget shows the RAM used for processes, swap, and the total RAM available.

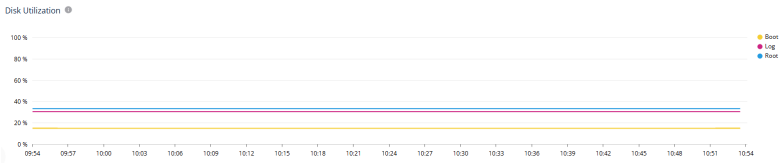
9.4.1.3. CPU Utilization



The **CPU Utilization** widget shows:

- **Overall** - The overall CPU used as a percentage of the total utilization.
- **By Core** - The CPU used as a percentage of the total utilization split by CPU cores.

9.4.1.4. Disk Utilization

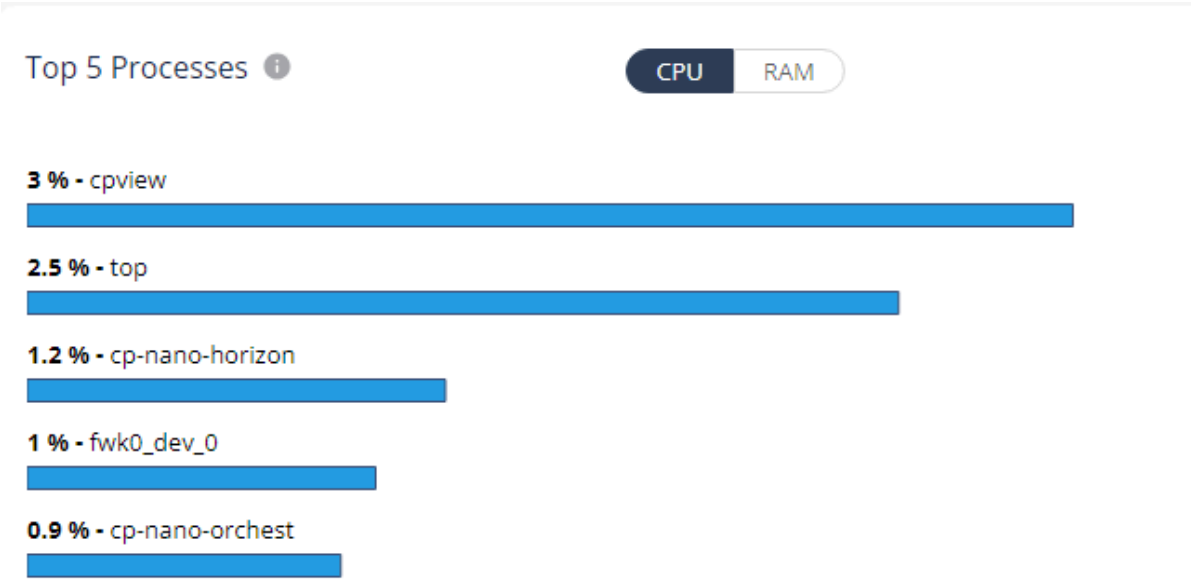


The **Disk Utilization** widget shows the disk space usage of all the mounted file systems as a percentage of the total utilization.

> **Note:**
>
> The partition may differ depending on the monitored asset type.

9.4.1.5. Top 5 Processes

> **Note:**
>
> This widget is supported only in R82 version and higher.



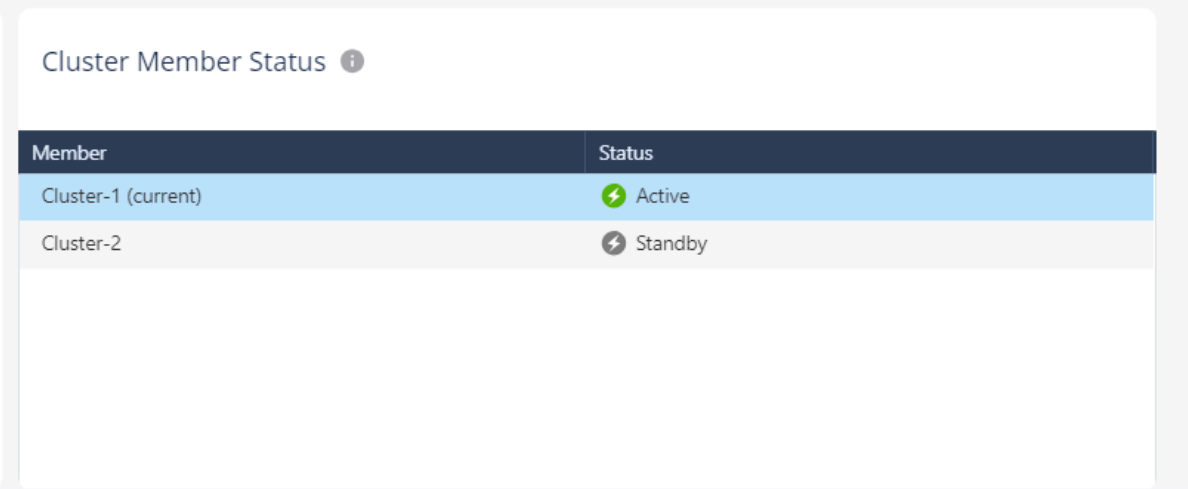
The **Top 5 Processes** widget shows:

- **CPU** - The top five processes with the highest CPU usage.
- **RAM** - The top five processes with the highest memory (RAM) usage.

9.4.1.6. Cluster Member Status

Note:

This widget is supported only in R82 version and higher.



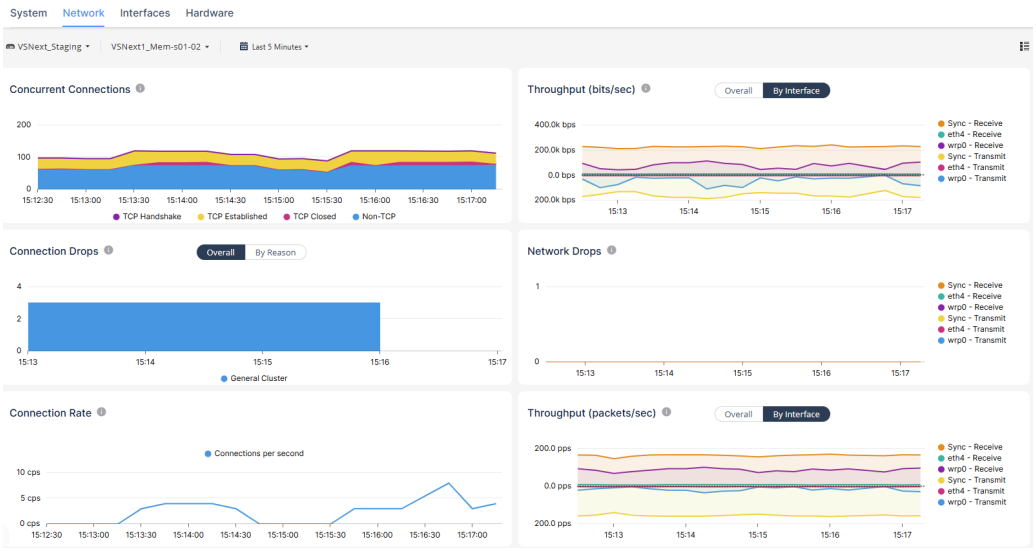
The **Cluster Member Status** shows the status of the cluster members:

- Active
- Standby
- Lost
- Down
- Initializing
- Ready
- Backup
- None

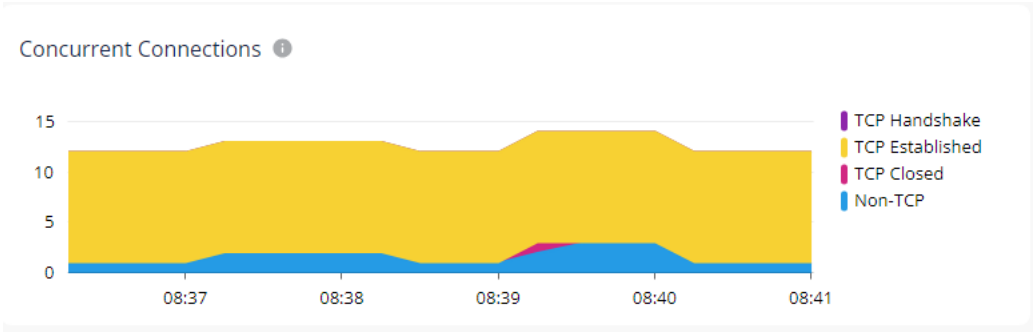
9.4.2. Network

Note:

The widgets displayed depend on the asset type and version.

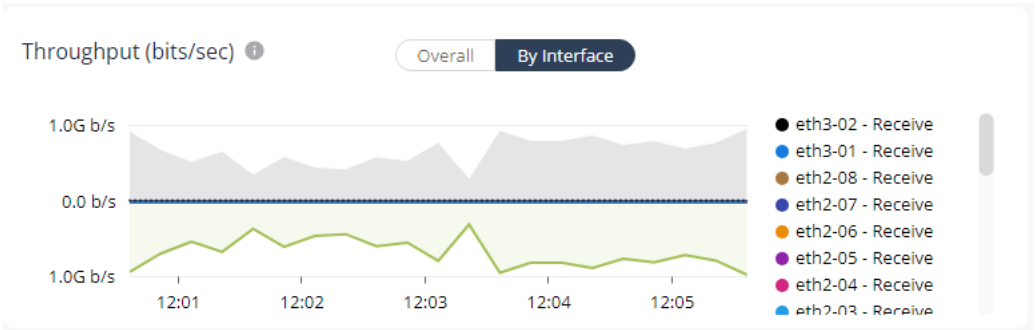


9.4.2.1. Concurrent Connections



The **Concurrent Connections** widget shows the total number of concurrent connections.

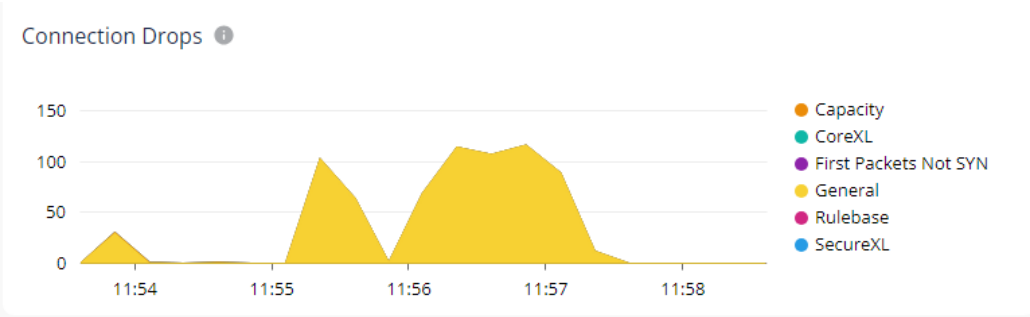
9.4.2.2. Throughput (bits/sec)



The **Throughput (bits/sec)** widget shows:

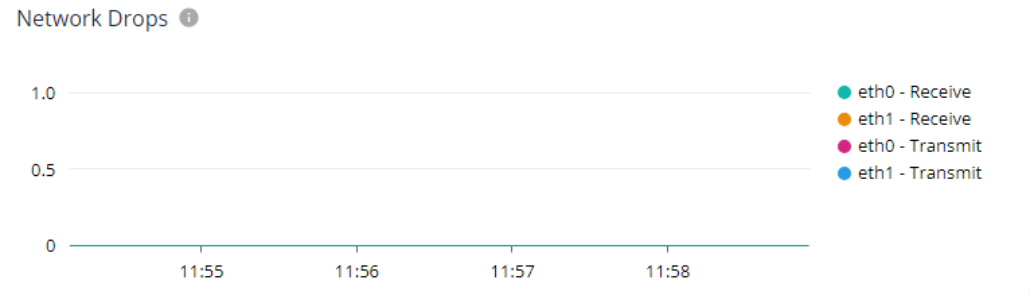
- **Overall** - The overall rate of successfully received and transmitted data over the communication channels.
- **By interface** - The rate of successfully received and transmitted data split by individual interfaces.

9.4.2.3. Connection Drops



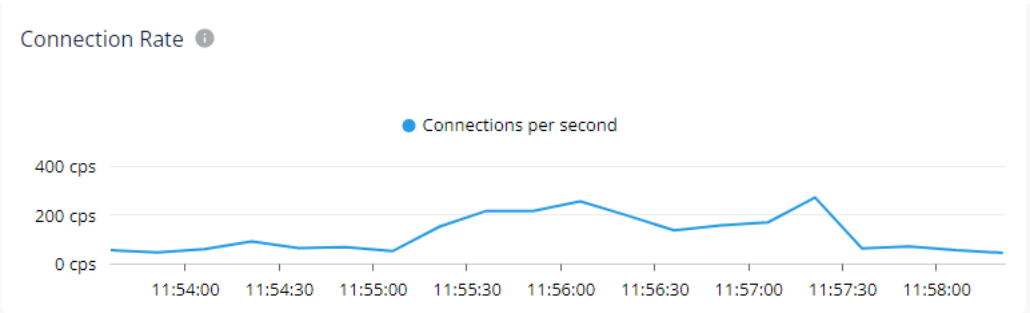
The **Connection Drops** widget shows the total number of connections dropped by Security Gateway Software Blades.

9.4.2.4. Network Drops



The **Network Drops** widget shows the total number of dropped packets received and transmitted since boot.

9.4.2.5. Connection Rate

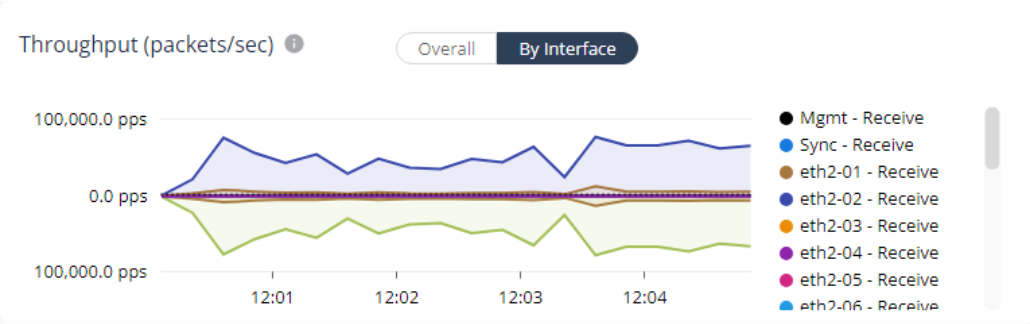


The **Connection Rate** widget displays the number of connections per second that were successfully forwarded by the gateway.

Note: Dropped connections are tracked separately in the **Connection Drops** widget. Both graphs measure traffic from the same pool of attempted connections. So it is expected that the dropped rate to exceed the sent rate under high load or when policy rules block significant traffic. This is not a measurement error. To assess overall

connection health, review both graphs together: sent + dropped connections = total attempted connection rate at any given time.

9.4.2.6. Throughput (packets/sec)



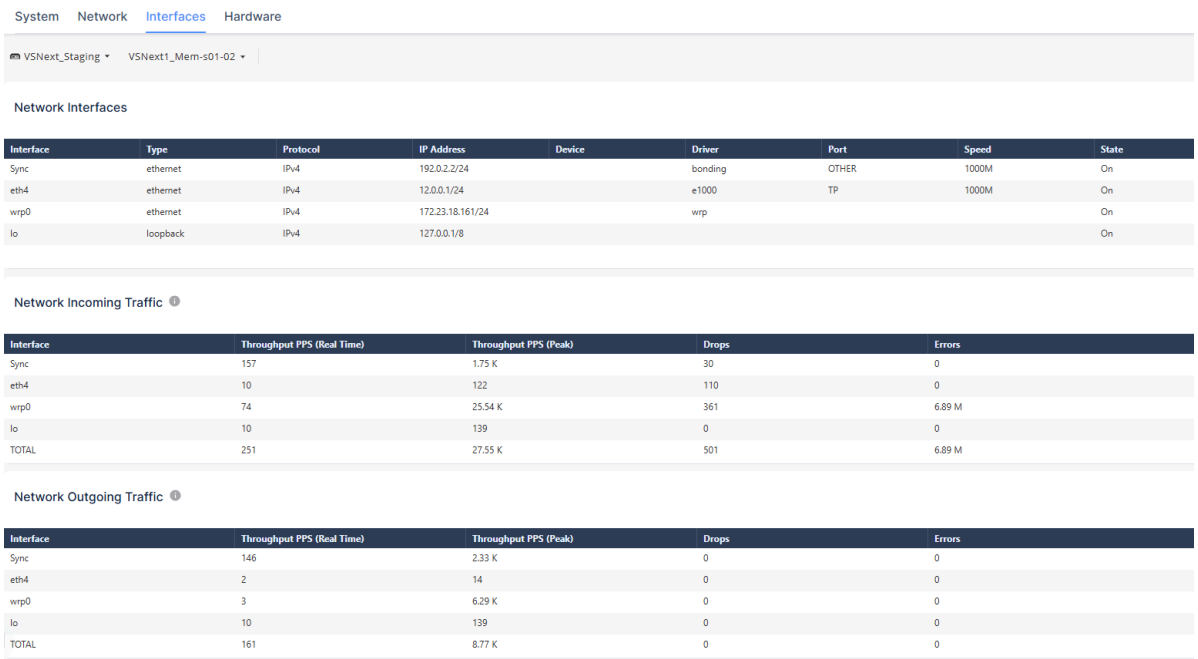
The **Throughput (packets/sec)** widget shows:

- **Overall** - The overall rate of successfully received and transmitted packets over the communication channels.
- **By interface** - The rate of successfully received and transmitted packets split by individual interfaces.

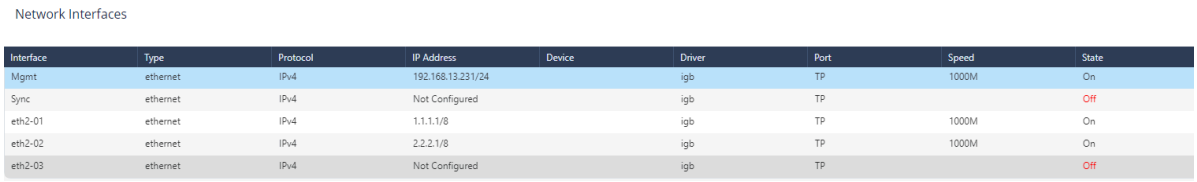
9.4.3. Interfaces

Note:

The widgets displayed depend on the asset type and version.



9.4.3.1. Network Interfaces


Network Interfaces

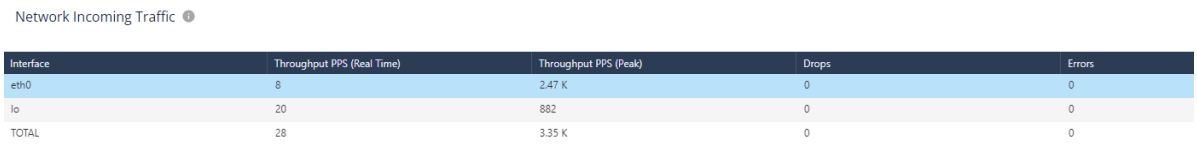
Interface	Type	Protocol	IP Address	Device	Driver	Port	Speed	State
Mgmt	ethernet	IPv4	192.168.13.231/24		igb	TP	1000M	On
Sync	ethernet	IPv4	Not Configured		igb	TP		Off
eth2-01	ethernet	IPv4	1.1.1.1/8		igb	TP	1000M	On
eth2-02	ethernet	IPv4	2.2.2.1/8		igb	TP	1000M	On
eth2-03	ethernet	IPv4	Not Configured		igb	TP		Off

The **Network Interfaces** table shows the IP address and state of the network interfaces.

The different parameters in the table are described below:

Column Name	Description
Interface	Name of the interface.
Type	Type of the network interface (ethernet / loopback).
Protocol	Network protocol used in the network.
IP Address	Asset IP address.
Device	Asset name provided by the Operating System.
Driver	Version of the network driver.
Port	Asset port number.
Speed	Network speed.
State	Asset network state (On/Off).

9.4.3.2. Network Incoming Traffic

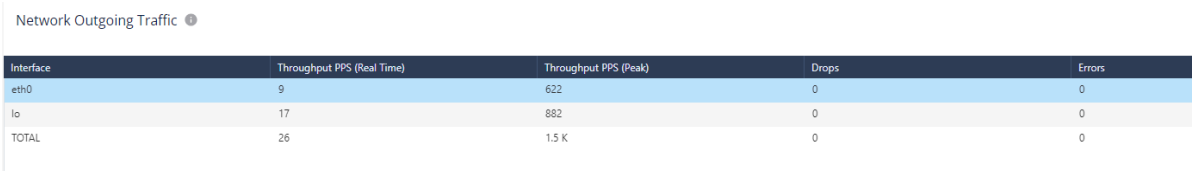

Network Incoming Traffic

Interface	Throughput PPS (Real Time)	Throughput PPS (Peak)	Drops	Errors
eth0	8	2.47 K	0	0
lo	20	882	0	0
TOTAL	28	3.35 K	0	0

The **Network Incoming Traffic** table shows:

Column Name	Description
Interface	Name of the interface.
Throughput PPS (Real Time)	The rate of packets successfully received over the communication channel (in packets per second).
Throughput PPS (Peak)	The maximal rate of packets successfully received for the network interface (in packets per second).
Drops	The total number of the dropped packets received since boot.
Errors	The total number of corrupted packets received since boot.

9.4.3.3. Network Outgoing Traffic


Network Outgoing Traffic

Interface	Throughput PPS (Real Time)	Throughput PPS (Peak)	Drops	Errors
eth0	9	622	0	0
lo	17	882	0	0
TOTAL	26	1.5 K	0	0

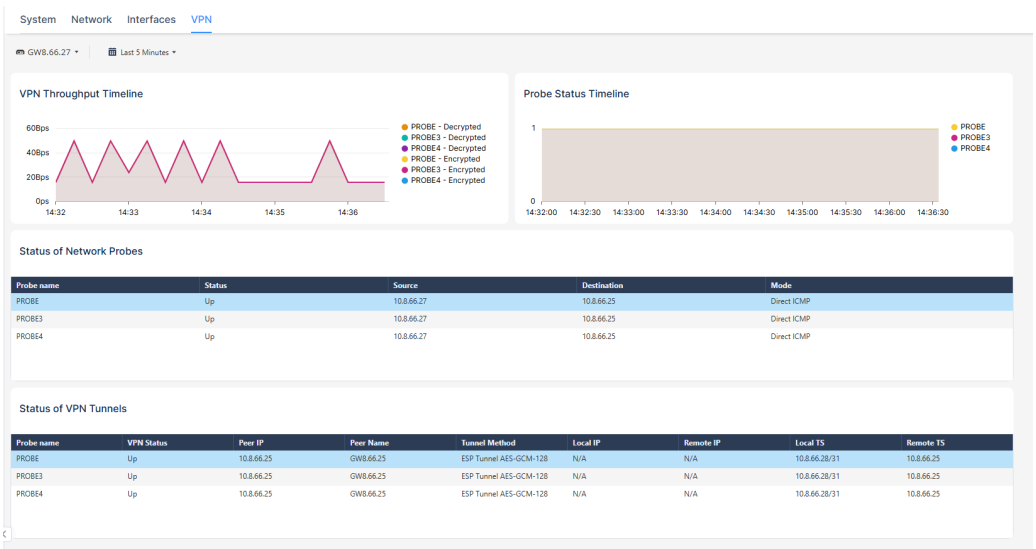
The **Network Outgoing Traffic** table shows:

Column Name	Description
Interface	Name of the interface.
Throughput PPS (Real Time)	The rate of packets successfully received over the communication channel (in packets per second).
Throughput PPS (Peak)	The maximal rate of packets successfully received for the network interface (in packets per second).
Drops	The total number of the dropped packets received since boot.
Errors	The total number of corrupted packets received since boot.

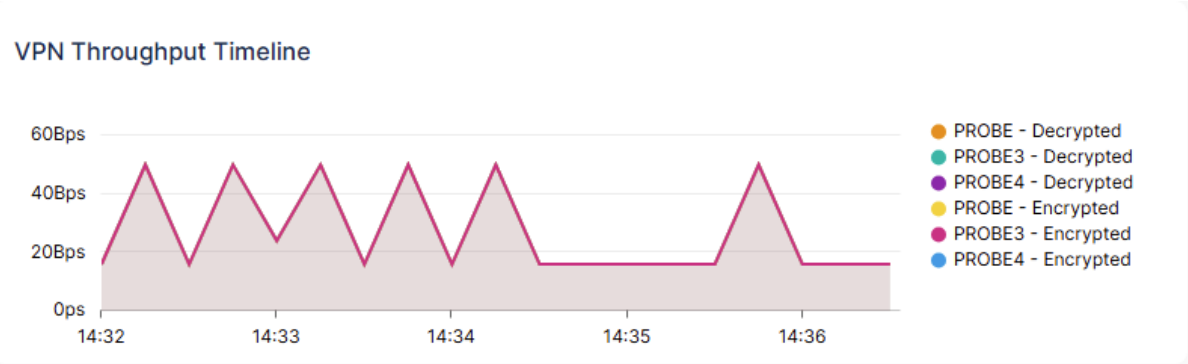
9.4.4. VPN

Note:

The **VPN** tab is optional and appears only when VPN probing is enabled. To monitor the status of your VPN Network Probes in R82 and higher, see sk181994.

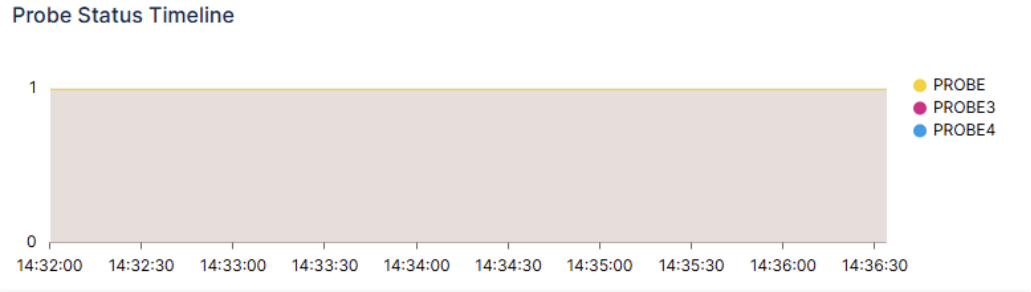


9.4.4.1. VPN Throughput Timeline



The **VPN Throughput Timeline** widget shows the rate of data transfer through the VPN.

9.4.4.2. Probe Status Timeline



The **Probe Status Timeline** widget shows the status of the VPN tunnel over time. For more information about Network Probes, see *R82 Site to Site VPN Administration Guide*.

9.4.4.3. Status of Network Probes

Status of Network Probes

Probe name	Status	Source	Destination	Mode
PROBE	Up	10.8.66.27	10.8.66.25	Direct ICMP
PROBE3	Up	10.8.66.27	10.8.66.25	Direct ICMP
PROBE4	Up	10.8.66.27	10.8.66.25	Direct ICMP

The **Status of Network Probes** widget shows the current status of VPN tunnel.

9.4.4.4. Status of VPN Tunnels

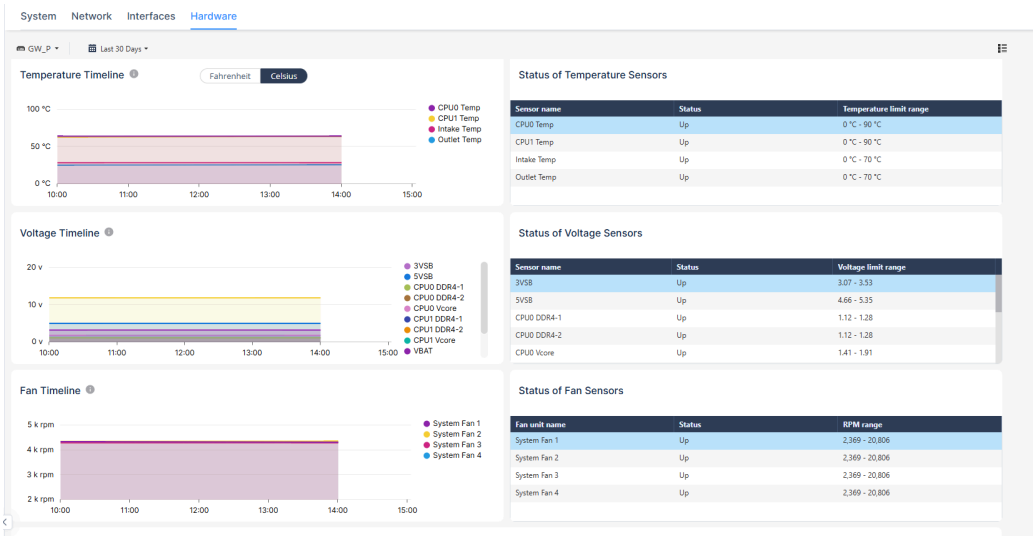
Status of VPN Tunnels

Probe name	VPN Status	Peer IP	Peer Name	Tunnel Method	Local IP	Remote IP	Local TS	Remote TS
PROBE	Up	10.8.66.25	GW8.66.25	ESP Tunnel AES-GCM-128	N/A	N/A	10.8.66.28/31	10.8.66.25
PROBE3	Up	10.8.66.25	GW8.66.25	ESP Tunnel AES-GCM-128	N/A	N/A	10.8.66.28/31	10.8.66.25
PROBE4	Up	10.8.66.25	GW8.66.25	ESP Tunnel AES-GCM-128	N/A	N/A	10.8.66.28/31	10.8.66.25

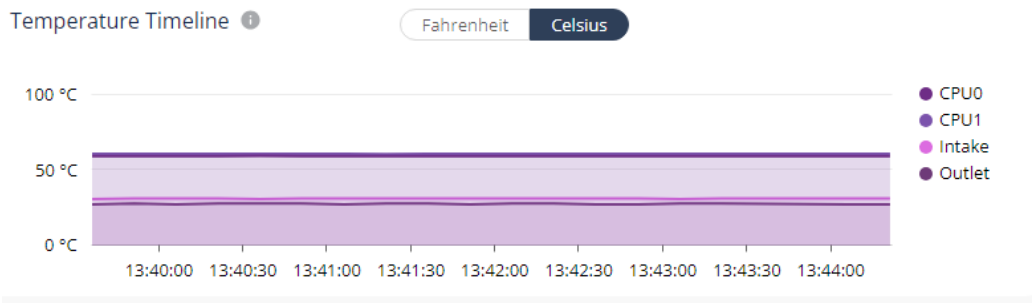
The **Status of VPN Tunnels** widget shows the status of current Site to Site VPN tunnels based on the configured Network Probes. For more information about Network Probes, see *R82 Site to Site VPN Administration Guide*.

9.4.5. Hardware

> **Note:**
>
> The **Hardware** tab and the widgets appear only for hardware assets (not for virtual machines).



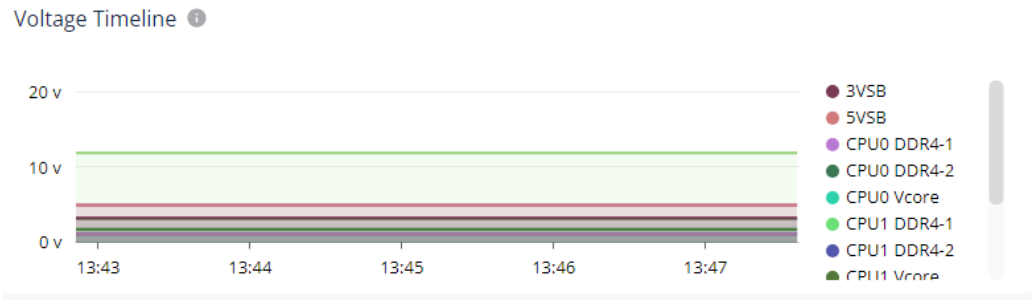
9.4.5.1. Temperature Timeline



The **Temperature Timeline** widget shows the current temperature of the sensor.

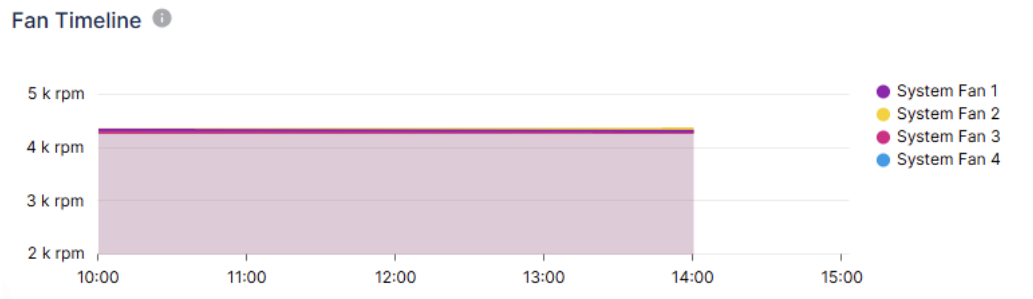
- CPU cores (CPU0 and CPU1)
- Incoming air (Intake)
- Outgoing air (Outlet)

9.4.5.2. Voltage Timeline



The **Voltage Timeline** widget shows the current voltage of the sensor.

9.4.5.3. Fan Timeline



The **Fan Timeline** widget shows the CPU fan speed over time.

9.4.5.4. Status of Temperature Sensors

Status of Temperature Sensors

Sensor name	Status	Temperature limit range
CPU0 Temp	Up	0 °C - 90 °C
CPU1 Temp	Up	0 °C - 90 °C
Intake Temp	Up	0 °C - 70 °C
Outlet Temp	Up	0 °C - 70 °C

The **Status of Temperature Sensors** widget shows the status of the temperature sensors.

9.4.5.5. Status of Voltage Sensors

Status of Voltage Sensors

Sensor name	Status	Voltage limit range
3VSB	Up	3.07 - 3.53
5VSB	Up	4.66 - 5.35
CPU0 DDR4-1	Up	1.12 - 1.28
CPU0 DDR4-2	Up	1.12 - 1.28
CPU0 Vcore	Up	1.41 - 1.91

The **Status of Voltage Sensors** widget shows the status of the voltage sensors.

9.4.5.6. Status of Fan Sensors

Status of Fan Sensors

Fan unit name	Status	RPM range
System Fan 1	Up	2,369 - 20,806
System Fan 2	Up	2,369 - 20,806
System Fan 3	Up	2,369 - 20,806
System Fan 4	Up	2,369 - 20,806

The **Status of Fan Sensors** widget shows the status of the fan sensors.

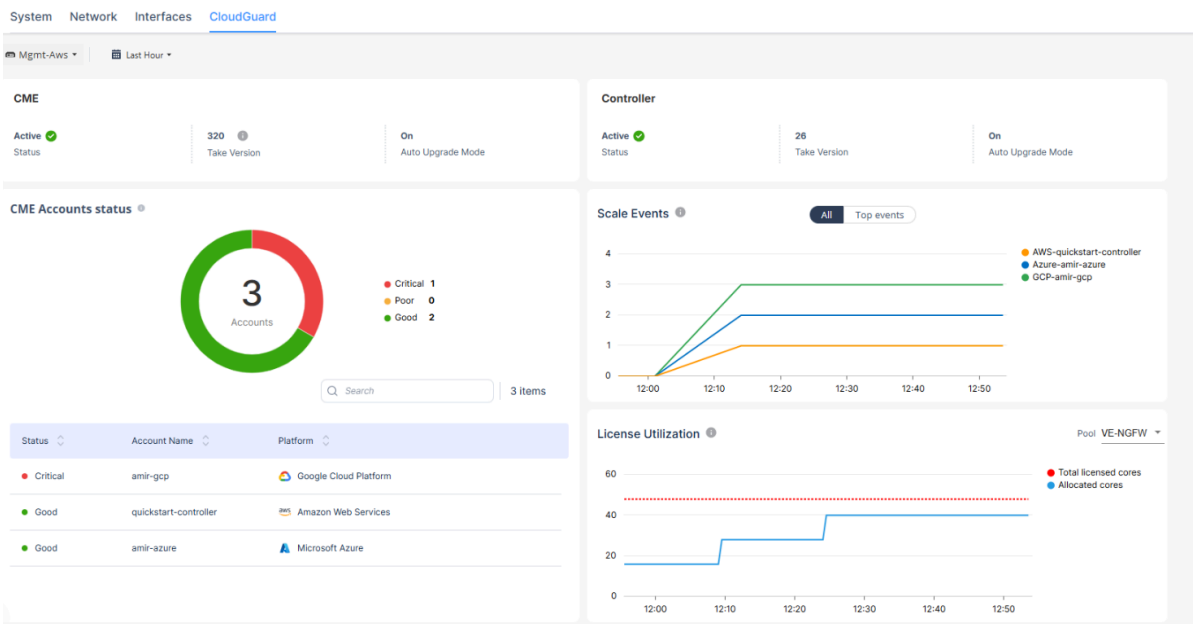
Note:

You can get data from the hardware sensors on Check Point appliances, in one of these ways:

- Directly on the Gaia Operating System - In Gaia Portal or Gaia Clish (see the *Gaia Administration Guide* for your version)
- With SNMP (see sk90860 and sk119232)
- With Skyline (see sk178566)

9.4.6. CloudGuard

In the **CloudGuard** tab, you can view the CloudGuard information for the asset.



Note:

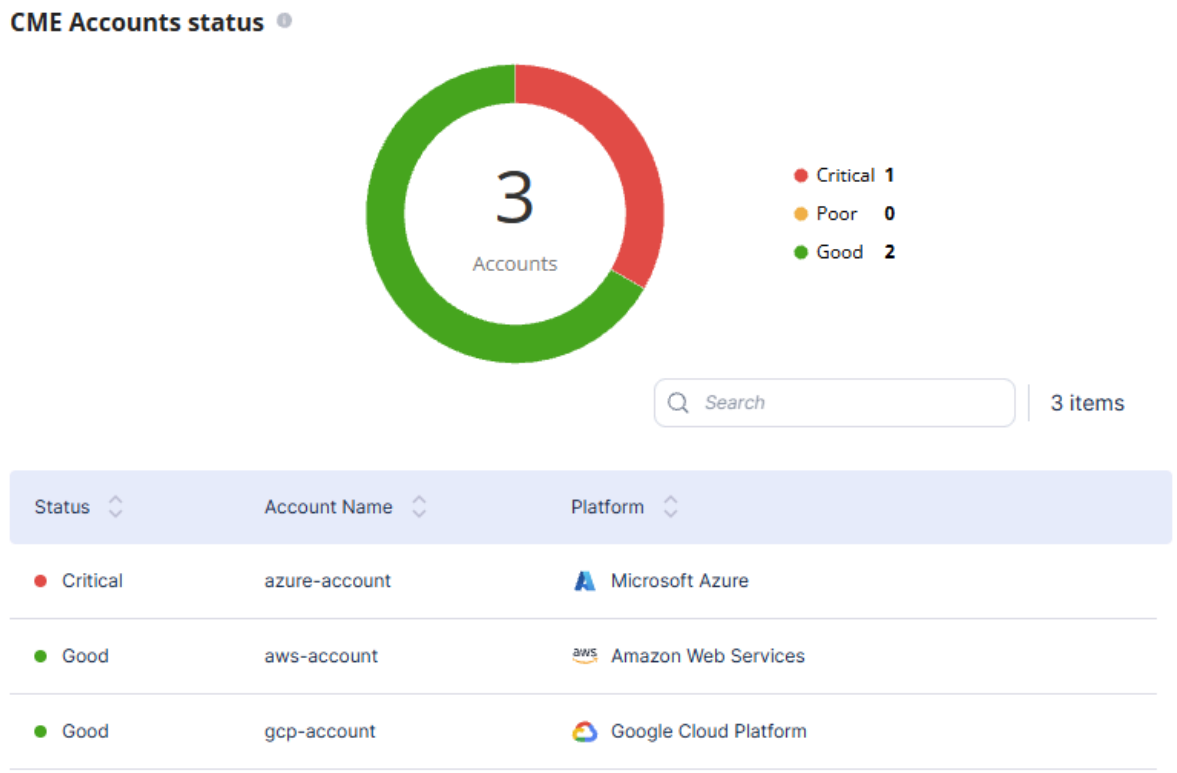
- The **CloudGuard** tab is displayed only for Management assets and not for Gateways.
- The widgets displayed in the **CloudGuard** tab depend on CloudGuard management components (CME, Controller, Central License) on the Management Server.

9.4.6.1. CME

The **CME** widget displays:

- **Status** - Status of the Cloud Management Extension (CME).
- **Take Version** - CME Take version
- **Auto Upgrade Mode** - Specifies whether **Auto Upgrade Mode** is enabled for CME.

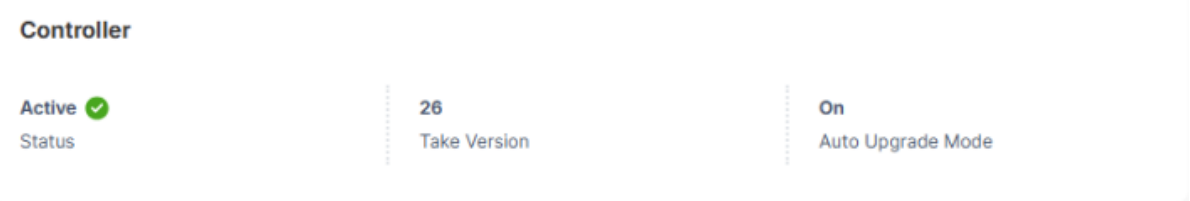
9.4.6.2. CME Accounts Status



The **CME Accounts status** widget displays:

- A pie chart that displays the total number of CME accounts and their health status.
- A table with health status of each CME account and the cloud provider (platform) associated with it.

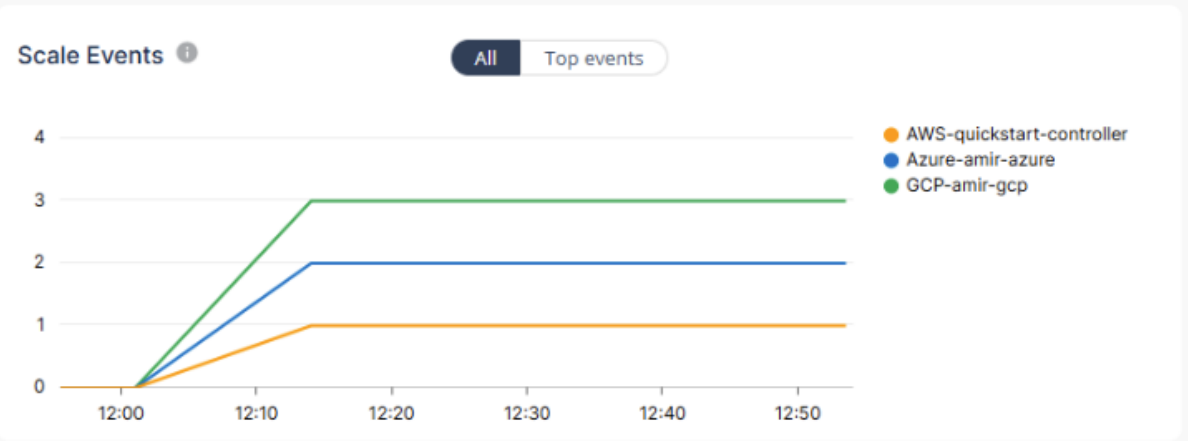
9.4.6.3. Controller



The **Controller** widget displays:

- **Status** - Status of the CloudGuard Controller.
- **Take Version** - CloudGuard Controller Take version
- **Auto Upgrade Mode** - Specifies whether **Auto Upgrade Mode** is enabled for CloudGuard Controller.

9.4.6.4. Scale Events



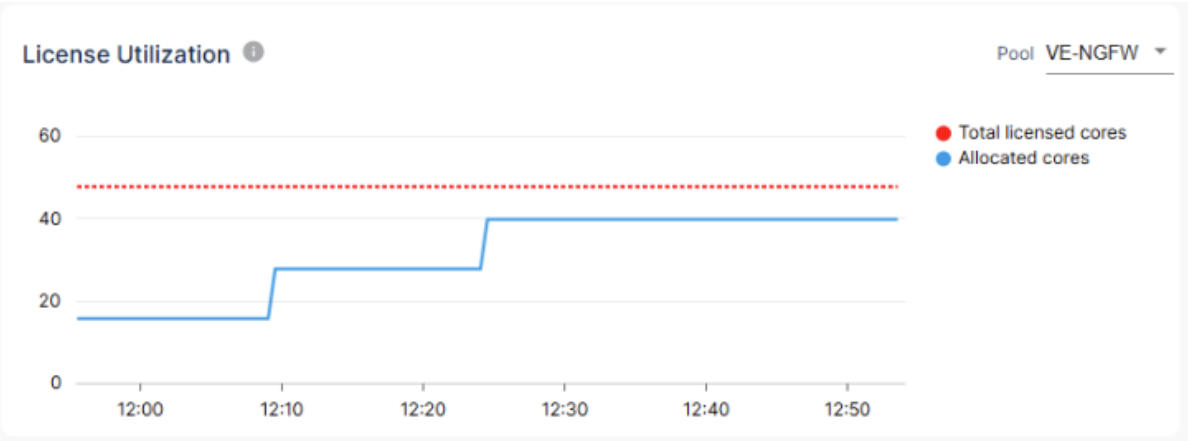
The **Scale Events** widget displays the scale-in and scale-out events over time:

- When the graph goes up, it indicates a **scale-out** event, where gateways are added to the Autoscaling Group.
- When the graph goes down, it indicates a **scale-in** event, where gateways are removed from the Autoscaling Group.

You can filter the widget to view:

- All scale events
- Top auto-scale events

9.4.6.5. License Utilization

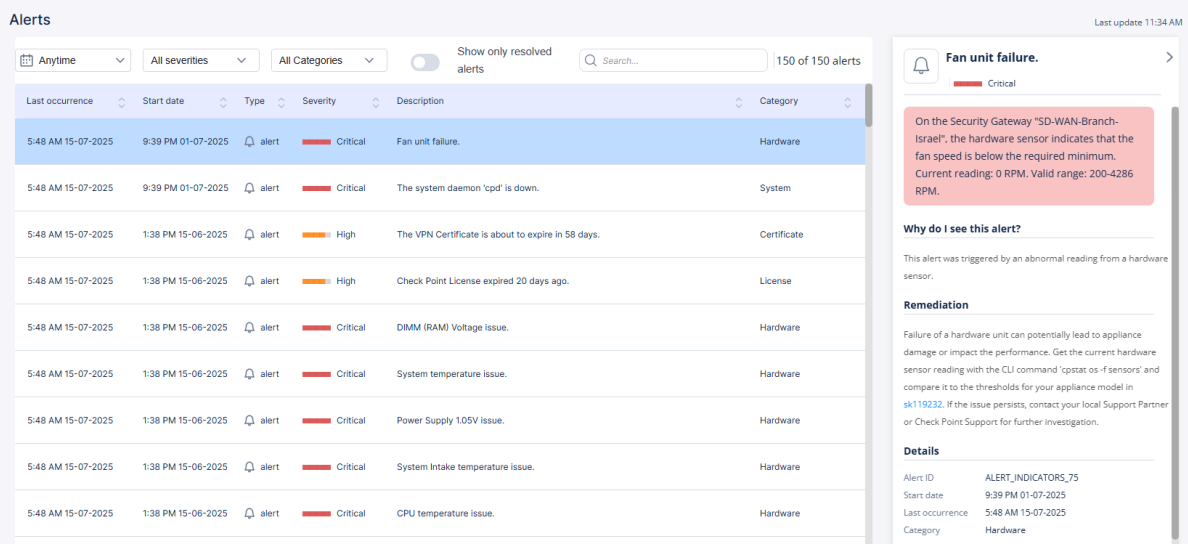


The **License Utilization** widget displays the number of allocated license cores over time compared to the total cores available in the license pool. You can select the license pool from the list at the top-right corner.

9.5. Alerts

The **Alerts** page shows the alerts received for the monitored assets.

To view the **Alerts** page, access the Events & AIOps Administrator Portal *(on page 13)* and go to **AIOps** > **Alerts**.



The **Alerts** table shows:

Item	Description
Last occurrence	Date and time when the alert most recently occurred.
Start date	Date and time when the alert started.
Type	Type of the alert: • Insight • Alert
Severity	Severity of the alert: • Critical • High • Medium • Info (For **Insights** type only)
Description	Details of the alert or insight.

Item	Description
	To view more information, click the row. A panel opens on the right side and displays additional details.
Category	Category of the alert.
Object name	Assets name from the Management Server.
Hostname	Host name defined by the user.
Originator	Component from which the alert originated.

You can filter the **Alerts** table by:

- Time frame
- Severity
- Category
- Resolved alerts

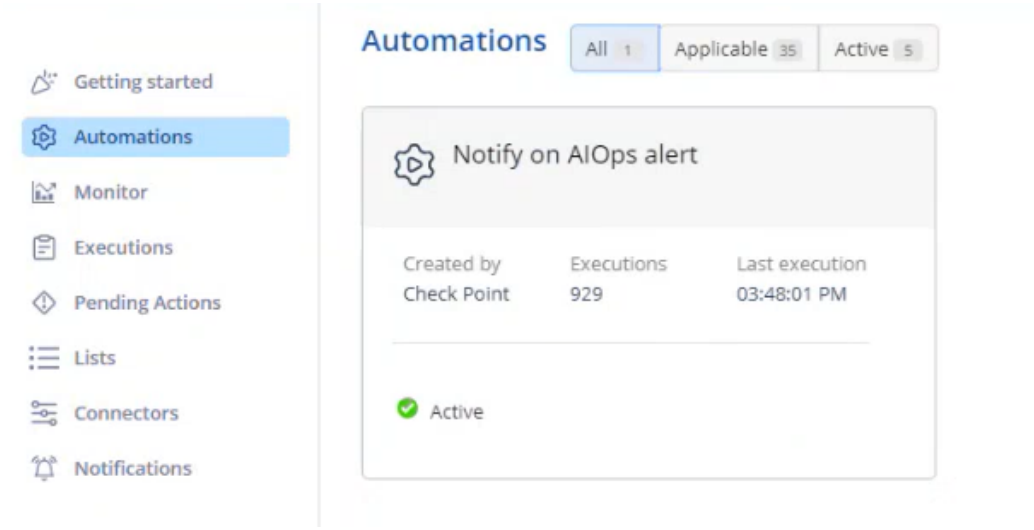
The **Last update** shows the time when the **Alerts** page was last updated.

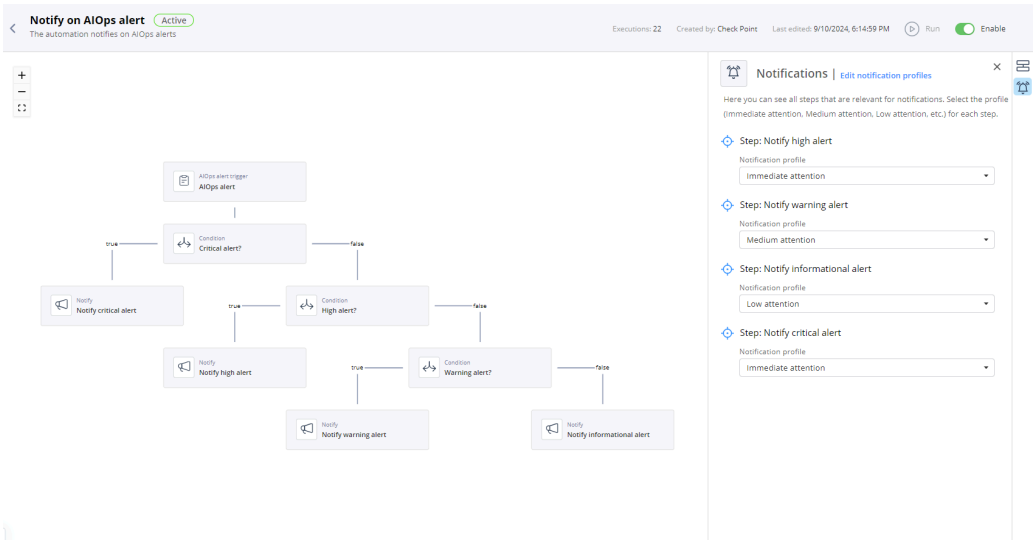
To search for a specific alert/insight, enter the value in the **Search** field.

For information on AIOps alerts and their descriptions, see Appendix A - AIOps Alerts *(on page 111)*.

9.5.1. Integration with Playblocks

AIOps is automatically integrated with Playblocks when you connect your Check Point Security Management Server with the Check Point Portal. This connection also activates the **Notify on AIOps alert** automation in Playblocks, to send notifications when alerts and insights are generated for the monitored assets.





Note:

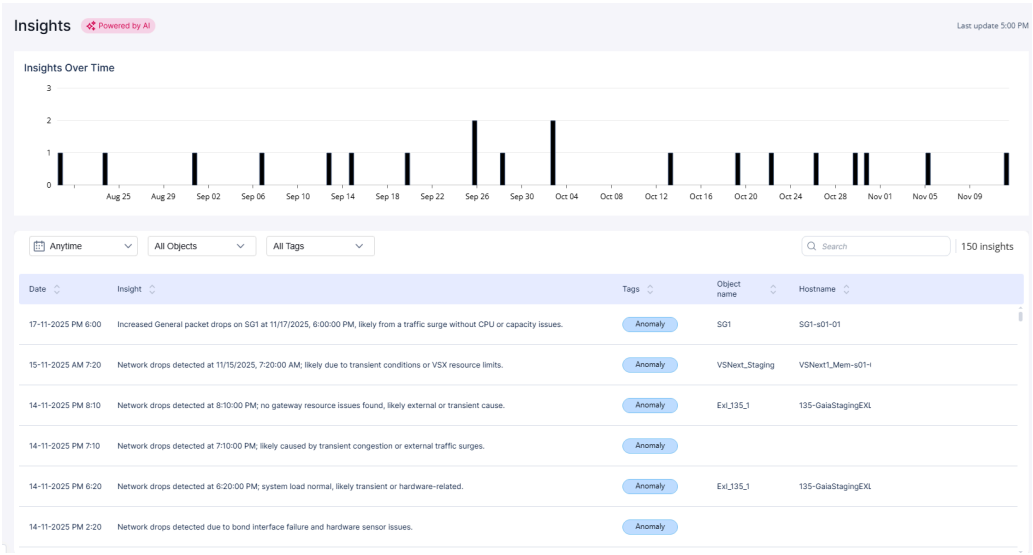
The **Notify on AIOps alert** automation treats all AIOps insights as **critical** alerts.

You can configure alert notification settings from the **Notifications** tab in Playblocks. For more information, see **Notifications** section in *Playblocks Administration Guide*.

9.6. Insights

Insights identify anomalies in system behavior or performance and provide recommendations to prevent future issues. They help improve system uptime.

The **Insights** page displays the AI generated insights for monitored assets. To view the **Insights** page, access the Events & AIOps Administrator Portal *(on page 13)* and go to **AIOps** > **Insights**.



- You can filter the **Insights** page by:
  - Time frame
  - Objects
  - Tags
- The **Last update** field shows the time when the **Insights** page was last updated.

9.6.1. Insights Over Time

The **Insights Over Time** widget displays the number of insights generated over a specific time period.

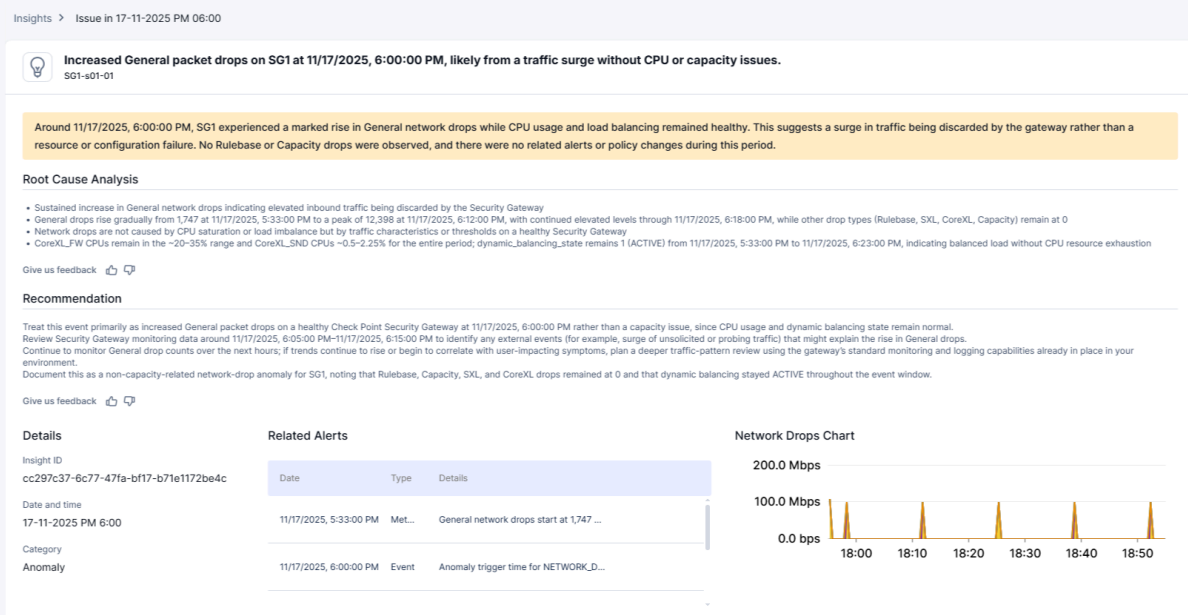
9.6.2. Insights Table

The **Insights** table shows:

Item	Description
Date	Date and time when the insight was generated.
Insight	Description of the insight.
Tags	Category of the insight.
Object name	Assets name from the Management Server.

Item	Description
Hostname	Host name defined by the user.

- To search for a specific insight, enter the value in the **Search** field.
- To view insights details, click the insight row. The system displays additional information about the selected insight.



Note:

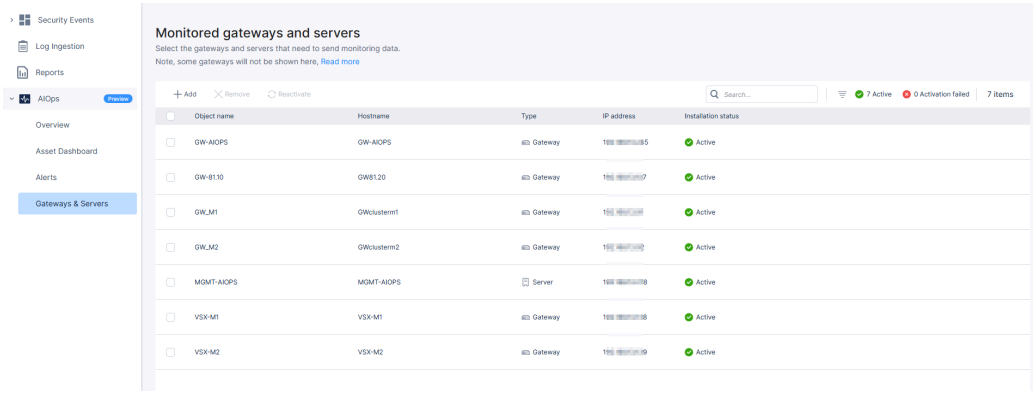
For details about Artificial Intelligence (AI) usage in Check Point products and services, see the following resources:

- Responsible AI
- AI FAQs

9.7. Gateways & Servers

The **Gateways & Servers** page shows all the monitored gateways and servers.

To view this page, access the Events & AIOps Administrator Portal *(on page 13)* and go to **AIOps** > **Gateways & Servers**.



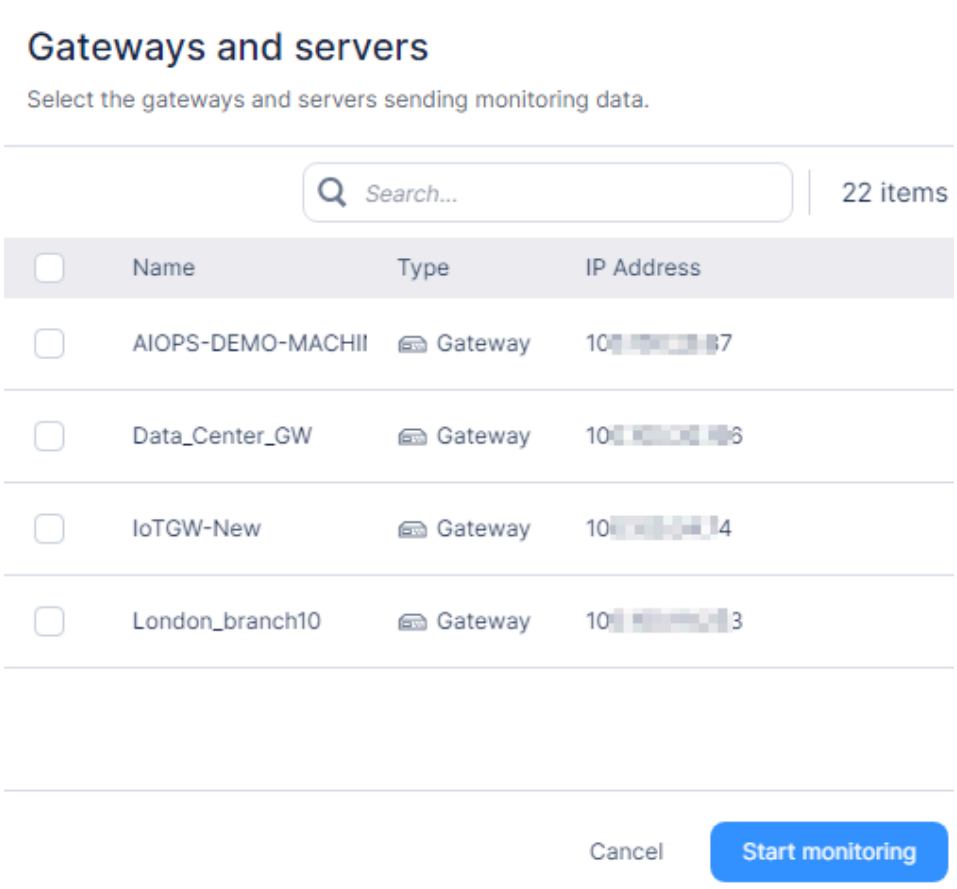
9.7.1. Adding an Asset

> **Note:**
>
> The **Add** option is enabled only if you have unmonitored assets.

To add an asset to AIOps:

1. Click **Add**.

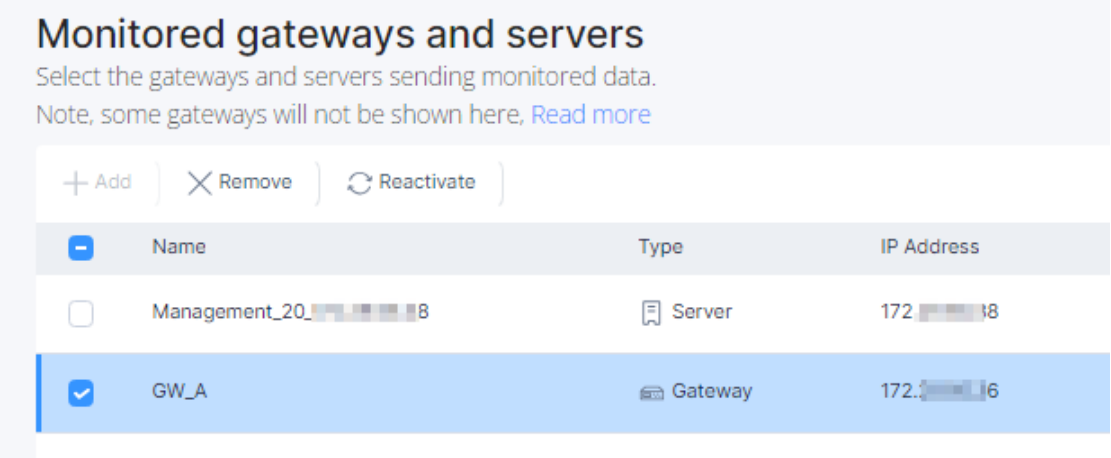
   The **Gateways and servers** window appears, that lists all your unmonitored assets.



2. Select the assets you want to add and click **Start monitoring**.

9.7.2. Removing an Asset

1. Select the asset and click **Remove**.



2. In the confirmation window, click **Remove**.

   AIOps stops monitoring the asset.

> **Note:**
>
> After an asset is removed, it will no longer appear on the **Asset Dashboard**. However, the system will still display the historical alerts received while the asset was being monitored.

9.7.3. Reactivating an Asset

To reactivate a monitored asset, see sk182647.

10. Threat Prevention

Topics:

The **Threat Prevention** dashboards allow you to view statistics of threat prevention events for the Check Point products you have subscribed to in Check Point Portal. These dashboard statistics highlight the effectiveness of threat prevention capabilities across each product.

The Threat Prevention dashboards are categorized into:

- Web Security dashboard *(on page 98)*
- File Security dashboard *(on page 104)*

Currently, the dashboard displays threat prevention events for:

- Smart-1 Cloud
- Endpoint Security
- Email Security

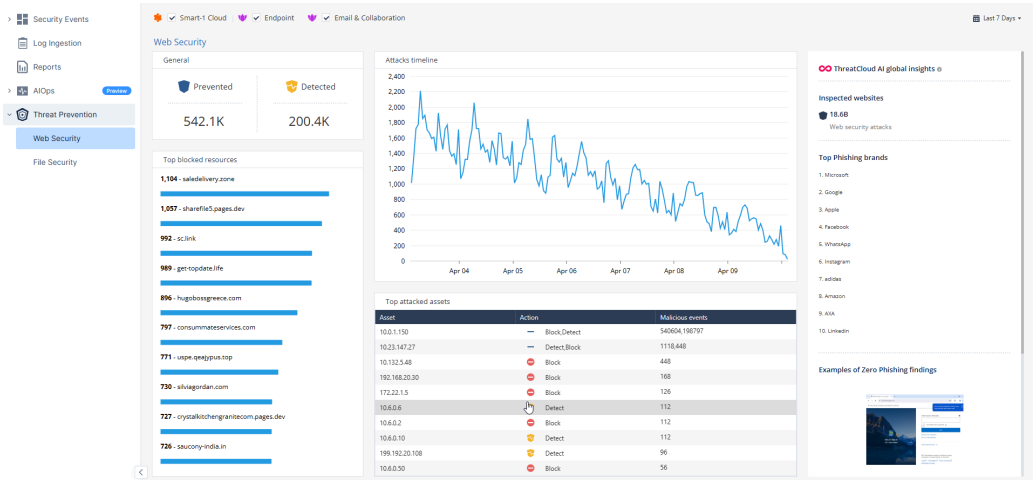
10.1. Web Security

The **Web Security** dashboard shows an overview of threat prevention events related to web security in the selected products.

Currently, the dashboard displays threat prevention events for:

- Smart-1 Cloud
- Endpoint Security
- Email Security

You can view the combined threat prevention events data for all products or for selected ones.

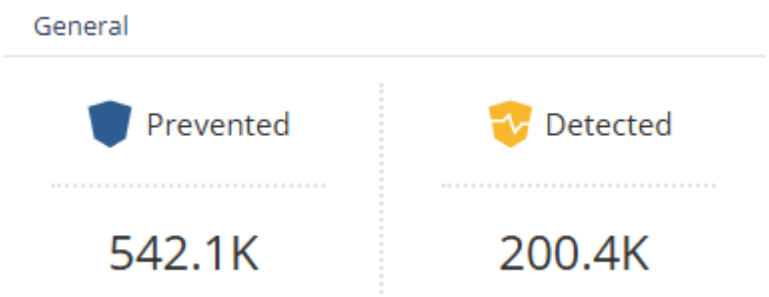


By default, the dashboard displays the overview for the last seven days. You can filter the page for these time periods:

- Last 24 hours
- Last 7 days
- Last 30 days

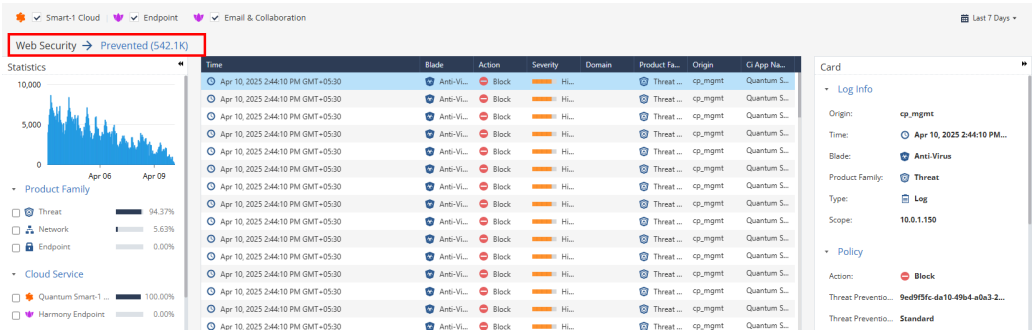
1. Access the Events & AIOps Administrator Portal *(on page 13)*.
2. Go to **Threat Prevention** > **Web Security**.

10.1.1. Web Security - General

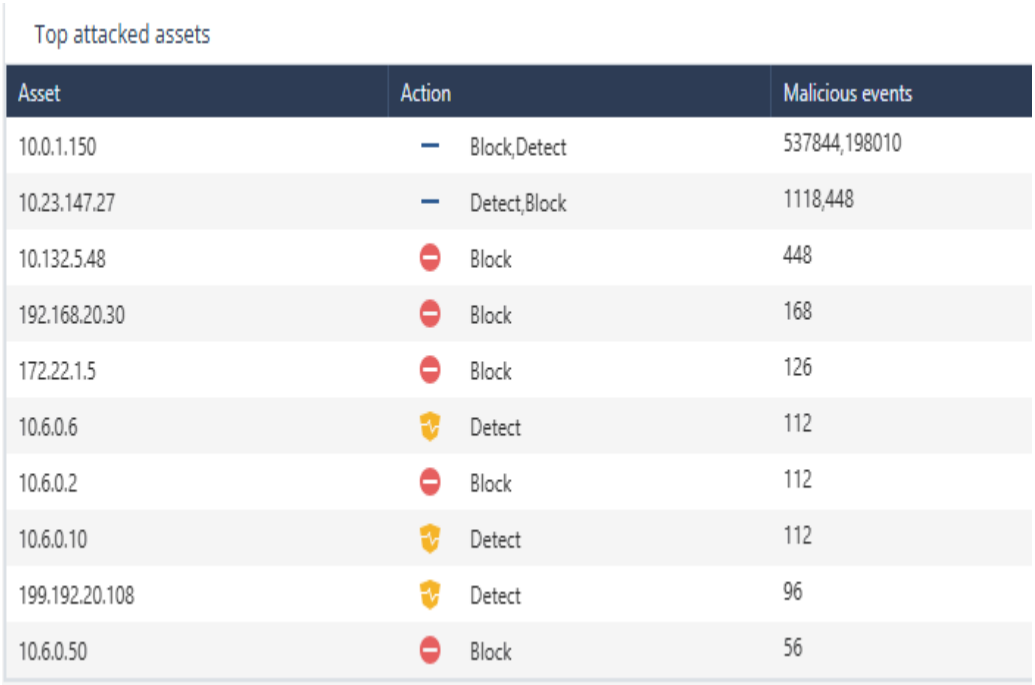


The **General** widget shows the total number of web security threat prevention events in the selected time-range and selected products.

To view logs, click the count in the respective category.



10.1.2. Attacks Timeline

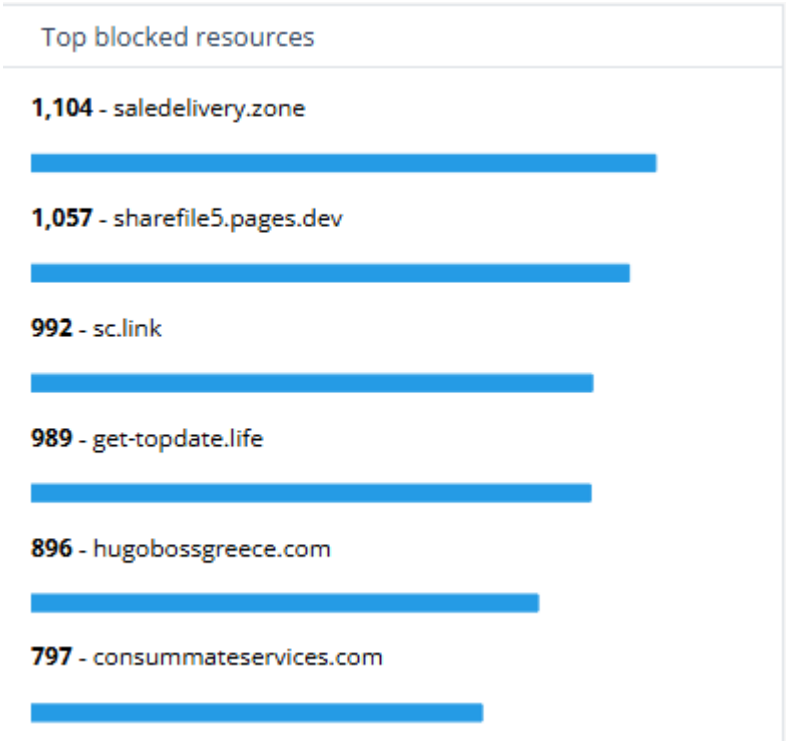


Top attacked assets

Asset	Action	Malicious events
10.0.1.150	Block,Detect	537844,198010
10.23.147.27	Detect,Block	1118,448
10.132.5.48	Block	448
192.168.20.30	Block	168
172.22.1.5	Block	126
10.6.0.6	Detect	112
10.6.0.2	Block	112
10.6.0.10	Detect	112
199.192.20.108	Detect	96
10.6.0.50	Block	56

The **Attacks timeline** widget shows the trend of threat prevention events during the selected time period.

10.1.3. Top Blocked Resources



The **Top blocked resources** widget shows the top 10 blocked web resources (domains or URLs) based on the number of threat prevention events for the resource.

To view event details for a resource, click the blue bar.

10.1.4. Top Attacked Assets

Top attacked assets

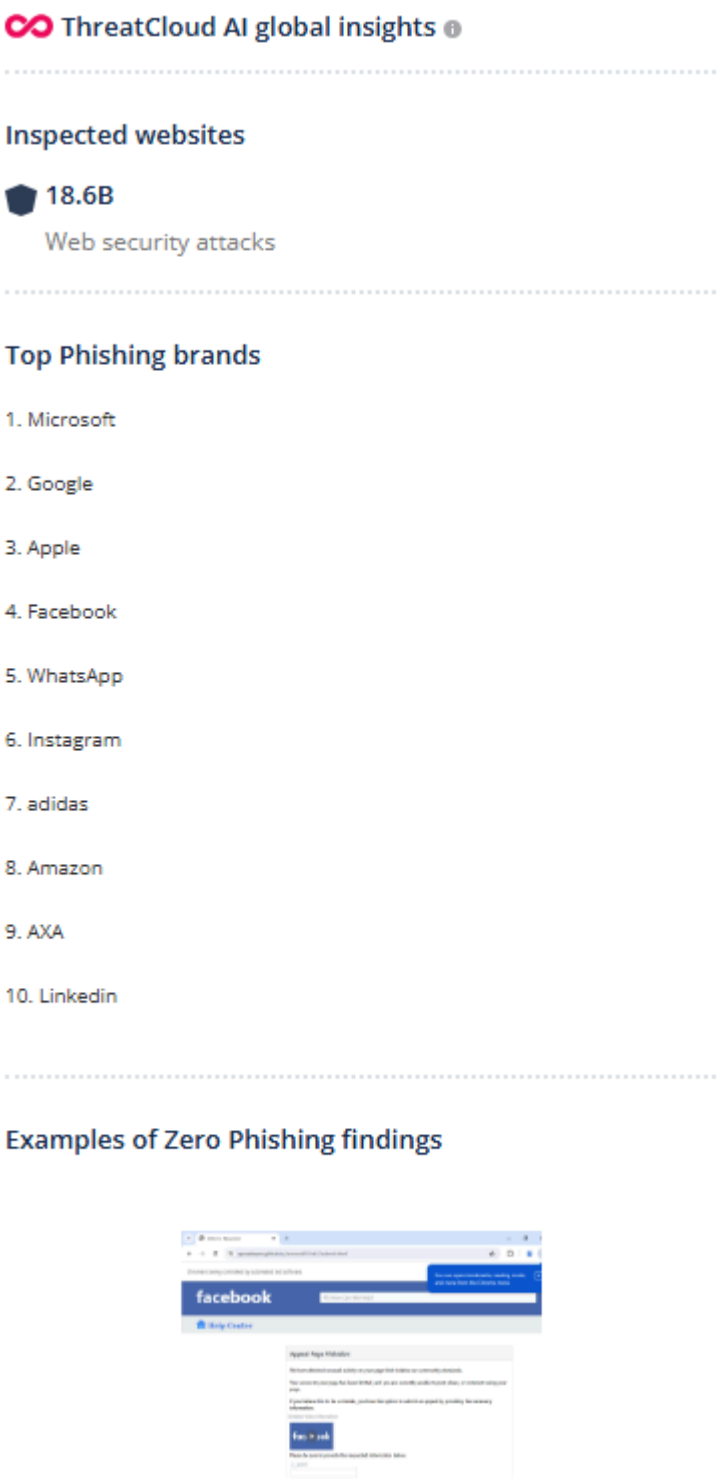
Asset	Action	Malicious events
10.0.1.150	Block,Detect	537844,198010
10.23.147.27	Detect,Block	1118,448
10.132.5.48	Block	448
192.168.20.30	Block	168
172.22.1.5	Block	126
10.6.0.6	Detect	112
10.6.0.2	Block	112
10.6.0.10	Detect	112
199.192.20.108	Detect	96
10.6.0.50	Block	56

The **Top attacked assets** widget shows the top 10 assets based on the number of threat prevention events.

Item	Description
Asset	IP address of the asset.
Action	Action taken for the event: • Detect • Block **Note:** When both **Detect** and **Block** actions are present, the action with the higher number of events is listed first.
Malicious events	Number of detected or blocked events. **Note:** When both **Detect** and **Block** actions are present, their respective counts are displayed in descending order.

To view logs related to an asset, click the asset row.

10.1.5. Web Security - ThreatCloud AI Global Insights



The **ThreatCloud AI global insights** widget shows global insights related to web security from the ThreatCloud AI. It includes:

- Global web attack statistics.
- Top brands impersonated in global phishing attacks.
- Examples of zero phishing findings.

10.2. File Security

The **File Security** dashboard shows an overview of threat prevention events related to file security in the selected products.

Currently, the dashboard displays threat prevention events for:

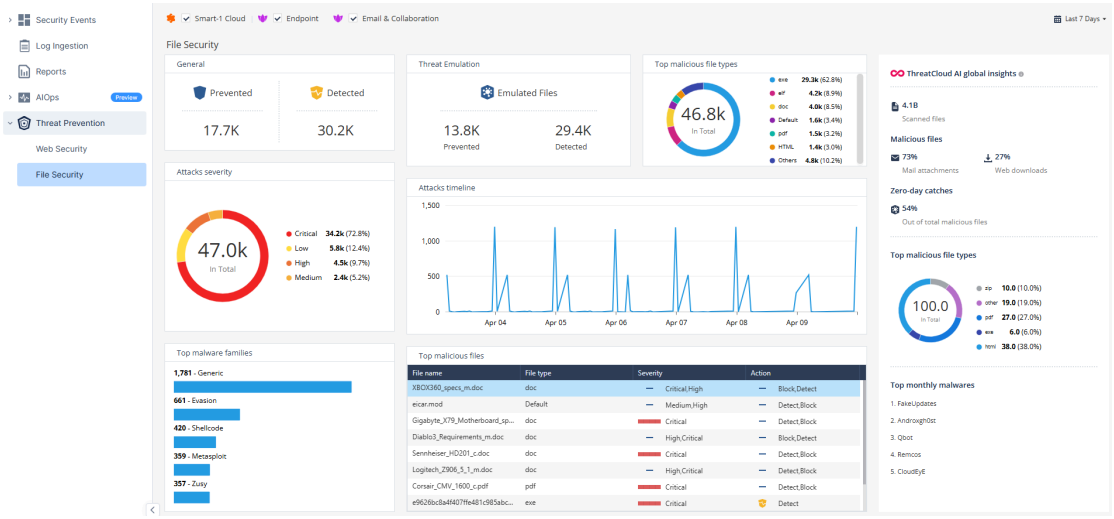
- Smart-1 Cloud
- Endpoint Security
- Email Security

You can view the combined threat prevention events data for all products or for selected ones.

10.2.1. View the File Security dashboard

To view the File Security dashboard:

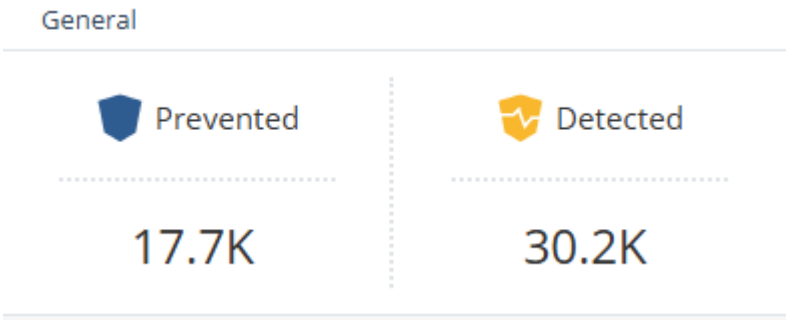
1. Access the Events & AIOpsAdministrator Portal *(on page 13)*.
2. Go to **Threat Prevention** > **File Security**.



By default, the dashboard displays the overview for the last seven days. You can filter the page for these time periods:

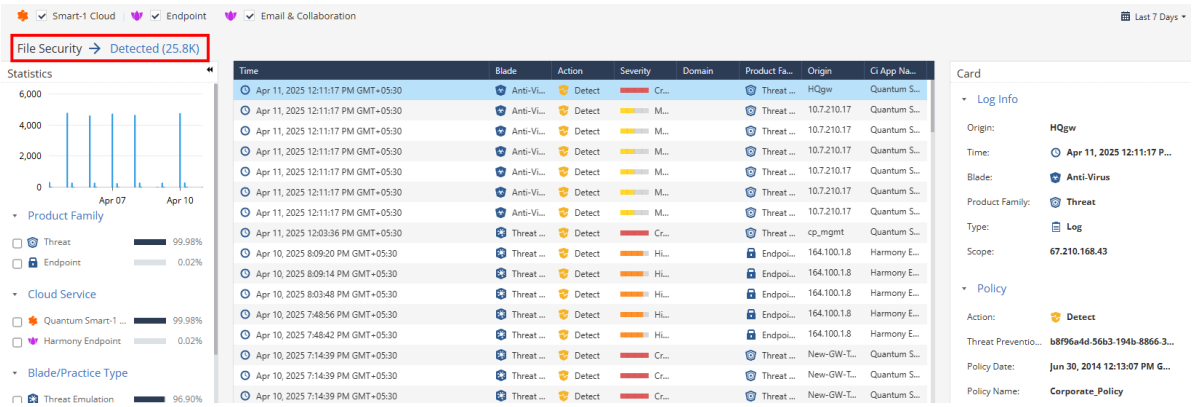
- Last 24 hours
- Last 7 days
- Last 30 days

10.2.2. File Security - General

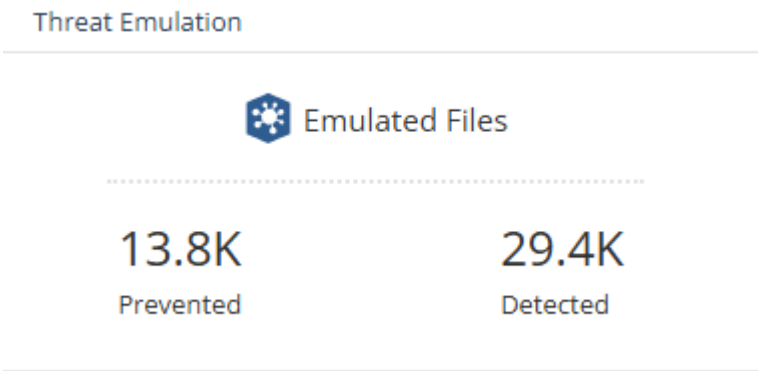


The **General** widget shows the total number of file security threat prevention events in the selected time-range and selected products.

To view logs, click the count in the respective category.



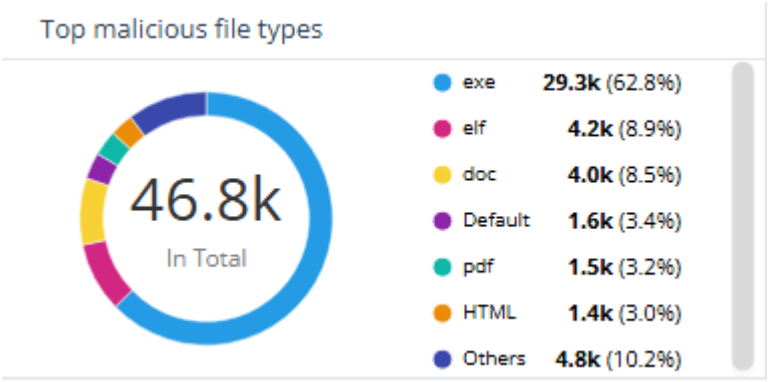
10.2.3. Threat Emulation



The **Threat Emulation** widget shows the total number of threat prevention events processed by the Threat Emulation service.

To view logs, click the count in the respective category.

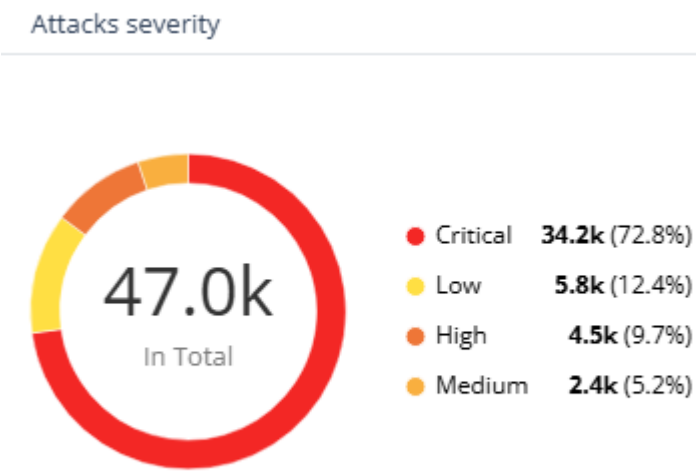
10.2.4. Top Malicious File Types



The **Top malicious file types** widget shows the top six file types base on the number of threat prevention events.

To view logs for each file type, click the respective type on the pie chart.

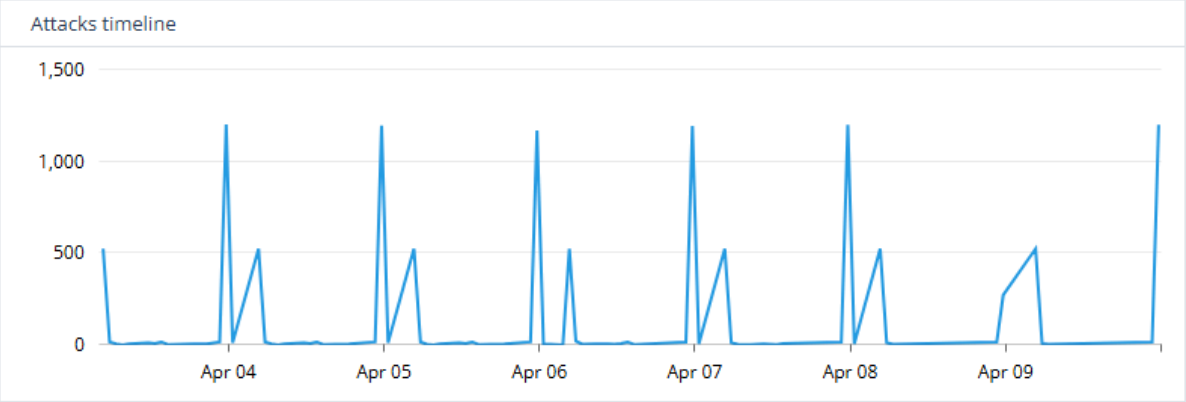
10.2.5. Attacks Severity



The **Attacks severity** widget shows the distribution of threat prevention events based on the severity level.

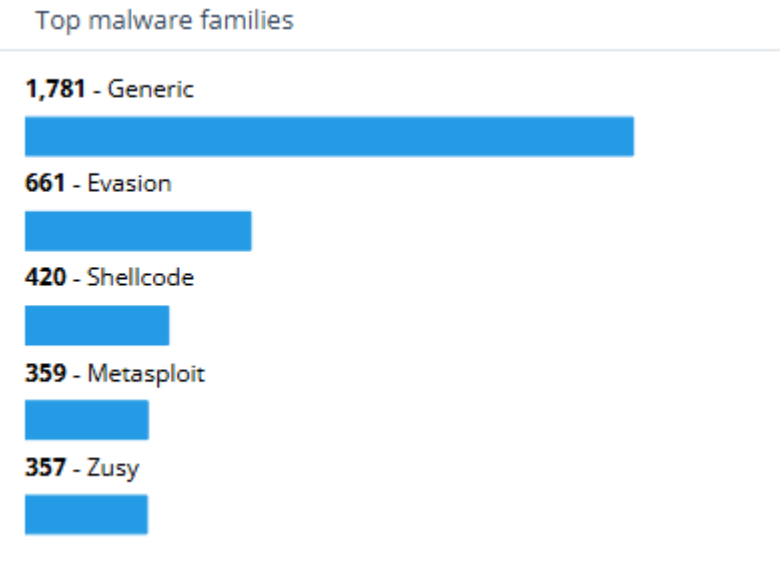
To view logs of each severity, click the respective severity on the pie chart.

10.2.6. Attacks Timeline



The **Attacks Timeline** widget shows the trend of threat prevention events in the selected time period.

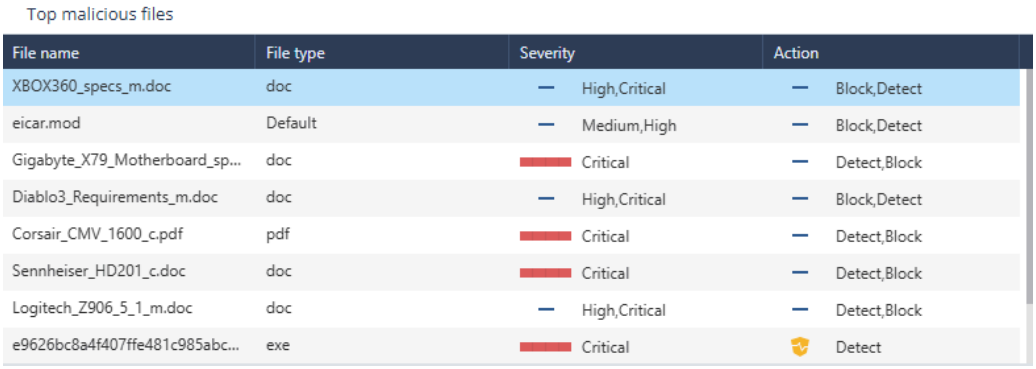
10.2.7. Top Malware Families



The **Top malware families** widget shows the top five malware families based on the number of threat prevention events.

To view logs for a malware family, click the blue bar.

10.2.8. Top Malicious Files


Top malicious files

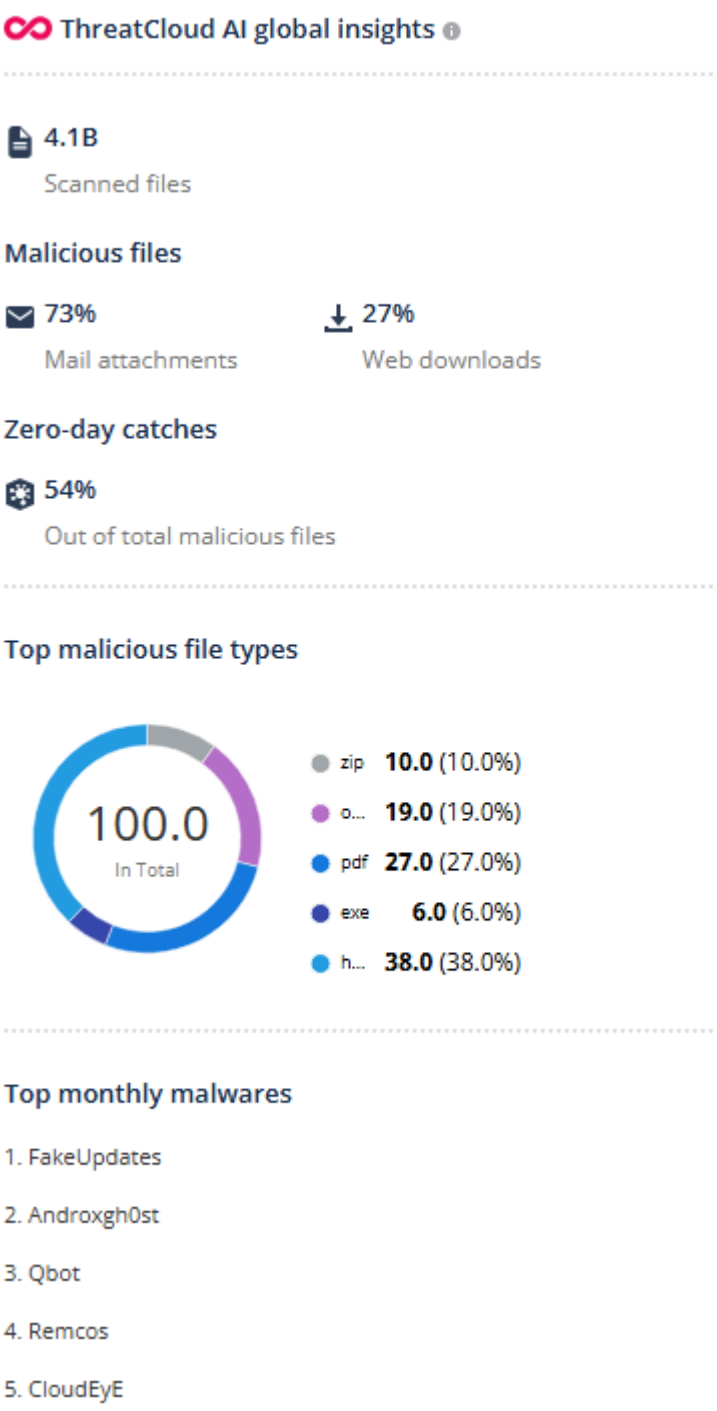
File name	File type	Severity	Action
XBOX360_specs_m.doc	doc	High,Critical	Block,Detect
eicar.mod	Default	Medium,High	Block,Detect
Gigabyte_X79_Motherboard_sp...	doc	Critical	Detect,Block
Diablo3_Requirements_m.doc	doc	High,Critical	Block,Detect
Corsair_CMV_1600_c.pdf	pdf	Critical	Detect,Block
Sennheiser_HD201_c.doc	doc	Critical	Detect,Block
Logitech_Z906_5_1_m.doc	doc	High,Critical	Detect,Block
e9626bc8a4f407ffe481c985abc...	exe	Critical	Detect

The **Top malicious files** widget shows the top 10 malicious files based on the number of prevention events.

Item	Description
File name	Name of the file.
File type	Type of the file.
Severity	Severity level of the file for the action taken (Detect/Block) **Note:** When there are multiple severity levels for a file, the severity level with the higher number of events is listed first.
Action	Action taken for the event: • Detect • Block **Note:** When both **Detect** and **Block** actions are present, the action with the higher number of events is listed first.

To view event details for a file, click the file row.

10.2.9. File Security - ThreatCloud AI Global Insights



The **ThreatCloud AI global insights** widget shows global insights related to file security from the ThreatCloud AI. It includes:

- Global statistics of scanned files.
- Global statistics of malicious files, including email attachments and files downloaded from the web.
- Percentage of zero-day catch for malicious files.

- Global statistics of top malicious file types.
- Monthly rankings of the top malware threats.

10.3. Threat Prevention Report

A **Threat Prevention Summary** report provides an overview of web security and file security Threat Prevention events for the Check Point products you are subscribed to in Check Point Portal.

Currently, the Threat Prevention report shows information on these products:

- Smart-1 Cloud
- Endpoint Security
- Email Security

To generate the report, see Reports *(on page 40)*.

11. Appendix A - AIOps Alerts

Alert Text	Summary/Description
High risk of kernel crashes when the 'ena' interface is in use.	Your machine is at high risk of kernel crashes due to an unsupported ethtool feature when using the `ena` interface.
Possibility of crash when bond interfaces are configured.	The Security Gateway <`machine name`> may crash with a `vmcore` dump file and get into a boot loop due to memory corruption when bond interfaces are configured.
Possibility of high memory utilization when using Site-to-Site VPN with Permanent Tunnels.	The Security Gateway <`machine name`> may experience high memory utilization when using Site-to-Site VPN with Permanent Tunnels.
Possibility of link failure on interfaces with an MTU greater than 1500.	The Security Gateway <`machine name`> may experience intermittent link failures on interfaces configured with an MTU greater than 1500.
License about to expire - License pool may no longer serve CloudGuard Gateways.	Licenses in the license pool will expire soon.
Automatic distribution of Central Licenses failed.	The `vsec_lic_cli` tool on the Management Server failed to distribute licenses to Cloud Firewall Gateways. Traffic through these Security Gateways is at risk.
License expired - License Pool may no longer serve Cloud Firewall Gateways.	Licenses in the license pool expired.

Alert Text	Summary/Description
Failover between Cluster Members failed - Cloud API Errors suspected.	Cluster Members could not fail over. Traffic through this cluster is at risk. Cloud API communication failed during the cluster failover process. When an Active cluster member becomes unavailable, the Standby cluster member must use the cloud provider APIs to reassign IP addresses and update routing tables.
The Cloud Management Extension (CME) service is unable to connect or scan the cloud account <`account name`>	The Cloud Management Extension (CME) service on your Management Server fails to connect to or scan a cloud account. This connection is critical for managing the Cloud Firewall Gateways.
Management API failure: Unable to connect or respond	Alert generated due to one of these reasons: • Management API failed to connect to the Management Server • There was no response from the Management Server • The Management Server command failed
The scale-in failed for the Security Gateway <`gateway name`>	The Cloud Management Extension (CME) automated provisioning failed to remove (scale-in) a Security Gateway.
The scale-out failed for the Security Gateway <`gateway name`>	The Cloud Management Extension (CME) automated provisioning failed to add (scale-out) a Security Gateway.
The Cloud Management Extension (CME) service stopped.	The Cloud Management Extension (CME) service on your Management Server stopped working. CME continuously monitors Cloud Firewall Gateways and synchronizes them with the Management Server. Your ability to manage and scale Security Gateways is at risk.

Alert Text	Summary/Description
Provisioning failure: Unable to complete Virtual WAN setup	Automated provisioning of a Virtual WAN (vWAN) Gateway with the Cloud Management Extension (CME) failed.
CloudGuard Controller scanner failed.	The CloudGuard Controller scanner failed to connect to cloud accounts to retrieve cloud objects. Your ability to create dynamic policy and update existing objects is at risk.
CloudGuard Controller service stopped.	CloudGuard Controller service stopped. This affects dynamic cloud objects management and policy enforcement which can cause policy mismatch failures.
Bond interface does not receive traffic.	Alert triggered by the HCP test about bond interfaces health. Ensure correct bond interface configuration. If required, contact Check Point Support.
Outbound traffic is not balanced in a bond interface.	On the Check Point server <`hostname`>, at least in one bond interface, outbound (TX) traffic is not balanced in between the subordinate interfaces.
Wrong affinity configuration of CoreXL Firewall Instances.	On the Security Gateway <`hostname`>, at least one CoreXL Firewall instance is configured to work on all CPU cores, which is not supported.
CoreXL is enabled on global context(VS0).	CoreXL is enabled on global context (VS0) on the VSX Gateway <`hostname`>
High CPU utilization by the CXLD daemon.	The `cxld` daemon consumes CPU at a high level on the Cluster Member <`hostname`>
Firewall debug is enabled.	Firewall debug is enabled on the Security Gateway <`hostname`>
SecureXL debug is enabled.	SecureXL debug is enabled on the Security Gateway <`hostname`>

Alert Text	Summary/Description
CoreXL Dynamic Balancing is disabled.	CoreXL Dynamic Balancing is disabled on the Security Gateway <hostname>
The Outbound HTTPS Inspection Certificate	The Outbound HTTPS Inspection Certificate has expired on the Security Gateway <hostname>
Critical health issue in an SSD storage device.	There is a critical issue in SMART health of an SSD storage device on the Check Point server <hostname>
Internal Certificate Authority (ICA) Certificate has expired	The Internal Certificate Authority (ICA) Certificate has expired on the Management Server <hostname>
CoreXL utilization issue in the VSX mode.	There is an issue with the number of CoreXL Firewall instances, CoreXL SND instances, and CPU cores on the VSX Gateway <hostname>
The system daemon <process name> is down.	The critical system daemon <process name> is down in the global context <context> on the Security Gateway <hostname>
Fan unit failure	On the Security Gateway <machine name>, the hardware sensor indicates that the fan speed is below the required minimum. Current reading: <Reading> <units>. Valid range: <Minimum>-<Maximum> <units>
Power Supply 12V issue	The device hardware sensor indicates the 12V reading is out of normal bound. Reading: <Voltage> Volts. Valid range: <Minimum voltage> - <Maximum voltage> Volts

Alert Text	Summary/Description
Power Supply 5V issue	The hardware sensor indicates that the power supply VCC 5V output is not within the valid range on the Security Gateway <hostname>. Current reading: <Voltage> Volts. Valid range: <Minimum voltage> - <Maximum voltage> Volts
CPU temperature issue	The device hardware sensor indicates the CPU Temp reading is out of normal bound. Reading: <Current temperature> Celsius. Valid range: <Minimum temperature> - <Maximum temperature> Celsius
System Intake temperature issue	The device hardware sensor indicates the System Intake Temp reading is out of normal bound. Reading: <Current temperature> Celsius. Valid range: <Minimum temperature> - <Maximum temperature> Celsius
Power Supply 1.05V issue.	The device hardware sensor indicates the 1.05V reading is out of normal bound. Reading: <Voltage> Volts. Valid range: <Minimum voltage> - <Maximum voltage> Volts
System temperature issue.	The device hardware sensor indicates the system temperature reading is out of normal bound. Reading: <Current temperature> Celsius. Valid range: <Minimum temperature> - <Maximum temperature> Celsius

Alert Text	Summary/Description
DIMM (RAM) Voltage issue.	On the Security Gateway <hostname>, the hardware sensor indicates that the DIMM Voltage is not within the valid range. Reading: <Current voltage> Volts. Valid range: <Minimum voltage> - <Maximum voltage> Volts
RAID status is degraded.	The RAID status is degraded on the Check Point server <hostname>
Some physical interfaces are not configured with Full Duplex.	Some physical interfaces are not configured with Full Duplex on the Check Point server <hostname>.
Some 10/25/40/100 GbE interfaces are not running the recommended firmware version.	Alert triggered by a firmware version of some interfaces. Check Point recommends installing the latest firmware version on 10/25/40/100 GbE interfaces. See sk141812.
<sensor type> issue	The device hardware sensor indicates the <sensor type> reading is out of normal bound. Reading: <Current voltage> Volts. Valid range: <Minimum voltage> - <Maximum voltage> Volts
IPS update issue	There is an IPS update issue on the Security Gateway <hostname>.
The eMMC flash memory has exceeded 90% of its overall lifespan.	The eMMC flash memory device lifetime used has passed 90% of its overall lifespan. This is critical ware and requires immediate action. See following details: Product: <mac>. Value: 90.0% of device lifetime used.

Alert Text	Summary/Description
Update Required for VPN/Remote Access Security Gateways Using DigiCert/GeoTrust CA by Sep 8, 2025	On September 8, 2025, DigiCert stopped supporting HTTP/1.0 for OCSP and CRL checks. Without upgrading the protocol support, DigiCert certificate validation may fail, and will affect Site-to-Site VPN and Remote Access VPN on Check Point Security Gateways / Quantum Spark Gateways / CloudGuard Network Gateways.
Security Gateway may drop HTTP/2 traffic because the FWK process may terminate.	When HTTPS Inspection is enabled, the Security Gateway <`hostname`> drops HTTP/2 traffic and generates a core dump file for the FWK daemon.
FWK crash on cvpn_expired_session kernel table on `hostname`	During the Multi-Version Cluster (MVC) upgrade, the FWK process may terminate on ClusterXL members with the Mobile Access Software Blade enabled.
Blade `<blade name>` is in <`health template`> state	Received a status update from the Management Server about this blade. Example: `<blade name> is in a degraded state.`
<`asset name`> has <`template`> with entitlement	Received a status update from the Management Server about this asset. Message varies for each machine. Example: `<Asset> has non-critical issues with entitlement`
<`asset name`> has <`healthTemplate`> <`overall status`>	Received a status update from the Management Server about this asset. Message varies for each machine. Example: `<Asset> has critical issues (overall status)`

Alert Text	Summary/Description
Check Point License expired `x` days ago.	Alert triggered by an expired Check Point license. Example: On the Check Point server `<host name>`, the license expired `x` days ago:`<license name>`.
The VPN Certificate is about to expire in `x` days.	Alert triggered by the VPN Certificate expiration. Example: On the Security Gateway <`gateway name`>, the VPN Certificate is about to expire in x days.

12. Appendix B - AIOps Metrics Repository

Data	Description
Blades > Status and Update	
blades.entitlement	Indicates whether the software blade is entitled to download updates. • 0 - Entitled • 1 - Not entitled • 2 - Evaluation • 3 - Expired • 4 - Unavailable • 5 - Unknown status • 6 - Not applicable This metric is available in: • R82 and later • R81.20 Jumbo Hotfix Accumulator, Take 54 and later • R81.10 Jumbo Hotfix Accumulator, Take 135 and later • R81 Jumbo Hotfix Accumulator, Take 99 and later
blades.expiration	Expiration date of software blade entitlement (in seconds) This metric is available in: • R82 and later • R81.20 Jumbo Hotfix Accumulator, Take 54 and later • R81.10 Jumbo Hotfix Accumulator, Take 135 and later • R81 Jumbo Hotfix Accumulator, Take 99 and later

Data	Description
blades.state	Indicates whether the software blade active: • 0 - Enabled • 1 - Disabled • 2 - Unknown This metric is available in: • R82 and later • R81.20 Jumbo Hotfix Accumulator, Take 54 and later • R81.10 Jumbo Hotfix Accumulator, Take 135 and later • R81 Jumbo Hotfix Accumulator, Take 99 and later
blades.update.state	Updated status of software blades.
blades.update.time	Time when software blades were last updated.
CGNS	
cgns.central_license.cpu_cores.allocated	Number of CPU cores allocated by the CGNS central license
cgns.central_license.cpu_cores.total	Total CPU cores available in the CGNS central license
cgns.cme.accounts	Number of accounts managed by CGNS CME
cgns.cme.state	Current state of the CGNS CME service
cgns.cme.take	CGNS CME takeover status
cgns.controller.state	Operational state of the CGNS controller
cgns.controller.take	CGNS controller takeover status
ClusterXL	

Data	Description
cluster_xl.members.state	Current state of the ClusterXL member.
cluster_xl.mode	The ClusterXL mode: • HA - High Availability • LS - Load Sharing • Active-Active.
cluster_xl.pnotes	Names of critical devices that report their state as `problem`.
System > CPU > Top	
connection.top-.cpu.utilization	CPU utilization of the CoreXL Firewall instance, in %. This metric is available in R82 and higher.
connection.top-.cpu.wt.utilization	`PPE_WT` CPU utilization of the CoreXL SND instance, in %. For information about `PPE_WT`, see the **HyperFlow** chapter. This metric is available in: • R82 and later
System > Gaia	
agent.gaia.os.role	The internal role of the Gaia OS agent. This metric identifies the function or role assigned to the Gaia operating system instance (example, Security Gateway, Management Server). Introduced to replace certain CPView metrics.
deployment.package.darwin.info	Information about the deployment package for macOS (Darwin) agents, such as version, status, or package details.
deployment.package.info	Indicates whether it is a recommended software version. **Note:** Marks the relevant software packages as recommended.

Data	Description
env.domain	Domain names on a .
System > Firewall	
firewall.multik.s-tate	The state of CoreXL: • On • Off
firewall.policy-.name	Name of the last installed Access Control policy.
firewall.policy.time	Time of the last Access Control policy installation.
System > Flofiler	
flow_profiler.enti-ties	Number of top CPU consumer entities.
flow_profiler.uti-lization	CPU utilization for each entity, in percentage.
Hardware > BIOS	
hardware.bios	Indicates which BIOS is used: • 1.0 - Primary (default) • 0.0 - Secondary This metric is available in R82 and later.
hardware.bios.s-tate	State of BIOS: • 1.0 - Up • 0.0 - Down
Hardware > Fans	
hardware.fan	The current fan speed.
hardware.fan.max	The maximum supported fan speed.

Data	Description
hardware.fan.min	The minimum supported fan speed.
hardware.fan.s-tate	State of the sensor: • 0 - Works correctly • 1 - Failed
Hardware > Model	
hardware.model	Model name of the Appliance or Open Server. Example: Quantum 6200
Hardware > PSU	
hardware.power_-consumption	Total power consumption of server, in Watts. This metric is available in R82.10 and later.
hardware.power_-supply	State of the PSU: • 0.0 - Down • 1.0 - Up • 2.0 - Empty • 3.0 - Dummy This metric is available in R82 and later.
hardware.power_-supply.state	The PSU used: • 1.0 - Primary (default) • 0.0 - Secondary
Hardware > Temperature	
hardware.temper-ature	Current temperature measurement of the sensor.
hardware.temper-ature.max	Maximum supported temperature

Data	Description
hardware.temperature.min	Minimum supported temperature
hardware.temperature.state	State of the temperature sensor: • 0 - Works correctly • 1 - Failed
Hardware > Voltage	
hardware.voltage	Current voltage measurement of the sensor.
hardware.voltage.max	Maximum supported voltage.
hardware.voltage.min	Minimum supported voltage.
hardware.voltage.state	State of the voltage sensor: • 0 - Works correctly • 1 - Failed
System > CoreXL	
kernel.instances.count	Number of CoreXL Firewall instances
firewall.multik.state	The state of CoreXL: • On • Off
system.cpu.dynamic_balancing.state	The state of CoreXL Dynamic Balancing: • On • Off
Object Management and Database	

Data	Description
management.object.info	Provides metadata or detailed information about objects stored in the Check Point Management .Server.
Network > Heavy Connections	
network.heavy_connection.bytes	Number of bytes transferred in the connection.
network.heavy_connection.packets	Number of packets transferred in the connection. This metric is available in: • R82 and later • R81.20 Jumbo Hotfix Accumulator, Take 54 and later • R81.10 Jumbo Hotfix Accumulator, Take 135 and later • R81 Jumbo Hotfix Accumulator, Take 99 and later
Network > Network Probes (VPN)	
network.probes.last_probe	Time of the last report from the Network probe. This metric is available in R82 and later.
network.probes.last_status_change	Time when Network probe status last changed. This metric is available in R82 and later.
network.probes.mode	Monitoring mode of the Network probe: • ICMP • HTTP This metric is available in R82 and later.
network.probes.state	Current state of the Network probe. This metric is available in R82 and later.
Maestro Orchestrator	

Data	Description
orchestrator.deployment.member_id	Member ID of the Orchestrator on its Maestro Site. This metric is available in R82 and later.
orchestrator.deployment.num_of_mhos_on_site	Number of Orchestrators on the Maestro Site. This metric is available in R82 and later.
orchestrator.deployment.num_of_sites	Number of Maestro Sites. This metric is available in R82 and later.
orchestrator.deployment.orchd	Status of the main daemon `orchd` on this Orchestrator: • 1.0 - Up (default) • 0.0 - Down This metric is available in R82 and later.
orchestrator.deployment.site_id	ID of the Maestro Site. This metric is available in R82 and later.
orchestrator.lag	Current states of Bond (LAG) interfaces for communication with peer Orchestrators, on the same site and on the peer site. This metric is available in R82 and later.
orchestrator.lldp	Information about the LLDP messages received from security appliances. This metric is available in R82 and later.
orchestrator.ports-.admin_state	• 1.0 - Up (default) • 0.0 - Down This metric is available in R82 and later.
orchestrator.ports-.labels	General information about the ports on the Orchestrator. This metric is available in R82 and later.

Data	Description
orchestrator.ports-.link_state	Link state of the ports on the Orchestrator. This metric is available in R82 and later.
orchestrator.ports-.max_rx_power	Maximum received optical power measured on a port (in dBm)
orchestrator.ports-.max_temperature	Highest temperature recorded on a port (in °C)
orchestrator.ports-.max_tx_power	Maximum transmitted optical power measured on a port (in dBm). Indicates the strength of the signal being sent from the port.
orchestrator.ports-.min_rx_power	Minimum received optical power measured on a port. Useful for detecting weak or failing fiber links.
orchestrator.ports-.min_temperature	The minimum temperature (°C) recorded on a port.
orchestrator.ports-.min_tx_power	Minimum transmitted optical power (dBm) measured on the port.
orchestrator.ports-.port_power_class	The power class of the port (example, SFP/SFP+ module class), indicating supported optical power range.
orchestrator.ports-.power_required	The amount of power (W) required by the port/module.
orchestrator.ports-.ports_table.physical_port	Physical port identifier or index in the orchestrator's port table.
orchestrator.ports.rx_bytes_per_second	Traffic received (RX) by the port, in Bytes per second. This metric is available in R82 and later.
orchestrator.ports.rx_frames_per_second	Received (RX) traffic by the port, in packets (frames) per second. This metric is available in R82 and later.
orchestrator.ports-.rx_mbit_per_second	Received (RX) traffic by the port, in Megabits per second. This metric is available in R82 and later.
orchestrator.ports-.temperature	The current temperature of the port in °C.

Data	Description
orchestrator.ports-.transceiver_state	The transceiver state in the port on this Orchestrator: • 1.0 - Plugged (default) • 0.0 - Unplugged This metric is available in R82 and later.
orchestrator.port-s.tx_bytes_per_-second	Transmitted (TX) traffic by the port, in Bytes per second. This metric is available in R82 and later.
orchestrator.port-s.tx_frames_per_-second	Transmitted (TX) traffic by the port, in packets (frames) per second. This metric is available in R82 and later.
orchestrator.ports-.tx_mbit_per_sec-ond	Transmitted (TX) traffic by the port, in Megabits per second. This metric is available in R82 and later.
orchestrator.sg_-lag	The current states of Bond (LAG) interfaces for communication between the Orchestrator and the Security Appliances. This metric is available in R82 and later.
System > CPU	
system.cpu.count	Number of CPU cores.
system.cpu.uti-lization	Utilization of the CPU core as a percentage of the total utilization.
system.cpu.inter-rupts	Number of device interrupts that occurred per CPU core.
System > Filesystem	
system.filesys-tem.limit	Total disk space, in Bytes.
system.filesys-tem.usage	Free disk space currently used, in Bytes.
System > Memory	
system.memory-.limit	Total RAM available for processes, in Bytes.
system.memory-.usage	RAM usage by processes, in Bytes

Data	Description
system.fw.memory.limit	Total RAM available for Firewall processes, in Bytes.
system.fw.memory.usage	RAM usage by Firewall processes, in Bytes.
system.fw.memory.utilization	RAM usage by Firewall processes, in %. This metric is available in R82 and later.
System > Gaia	
system.gaia.os.edition	Operating system distribution if the OS kernel is 32-bit or 64-bit.
system.gaia.os.role	Name of the installed Check Point product configuration.
system.gaia.os.version	Software release version.
System > Input/Output	
system.io.utilization	Percentage of CPU time during which I/O requests were issued to the device (bandwidth utilization for the device). Device saturation occurs when this value is close to 100%.
System > Network	
system.network.connections.rate	Connection rate (connections per second).
System > Network > Packets	
system.network.packets.receive	Total number of received packets by this network interface since the boot.
system.network.packets.transmit	Total number of transmitted packets by this network interface since the boot.
system.network.dropped.receive	Total number of the received packets that were dropped since boot.
system.network.dropped.transmit	Total number of dropped transmitted packets since the boot.
system.network.errors.receive	Total number of received packets that are corrupted since the boot.

Data	Description
system.network-.errors.transmit	Total number of corrupted transmitted packets since the boot.
system.network-.io.receive	Total number of traffic bits received by the network interface since the boot.
system.network-.io.transmit	Total number of traffic bits transmitted by the network interface since the boot.
System > Network > Interfaces	
system.network-.interface.address	IP address of the network interface
system.network-.interface.io.receive.rate	Current rate of successfully received packets over the communication channel (in bits per second).
system.network-.interface.io.receive.rate.peak	Maximal recorded rate of successfully received packets for the network interface (in bits per second).
system.network-.interface.io.transmit.rate	Current rate of successfully transmitted packets over the communication channel (in bits per second).
system.network-.interface.io.transmit.rate.peak	Maximal recorded rate of successfully transmitted packets for this network interface (in bits per second).
system.network-.interface.packets-.receive.rate	Current rate of successfully received packets over the communication channel (in packets per second).
system.network-.interface.packets-.receive.rate.peak	Maximal recorded rate of successfully received packets for this network interface (in packets per second)
system.network-.interface.packets-.transmit.rate	Current rate of successfully transmitted packets over the communication channel (in packets per second).
system.network-.interface.packets.transmit.rate-.peak	Maximal recorded rate of successfully transmitted packets for this network interface (in packets per second).

Data	Description
system.network-.interface.state	The state of the network interface: • 0 - Off • 1 - On
System > Network > NAT	
system.network-.nat.connections-.count	Number of NAT pool concurrent connections.
system.network-.nat.connections-.rate	Number of NAT pool concurrent connections per second.
system.network-.nat.ports	Number of ports used for the NAT pool.
system.network-.nat.ports.limit	Total number of ports that can be used for the NAT pool.
System > Memory Paging	
system.paging-.limit	Total RAM assigned to swap memory, in Bytes.
system.paging.usage	RAM usage for swap, in Bytes.
System > Process > Top	
system.process-.top.cpu.utilization	CPU utilization by a process, in %.
system.process-.top.fd.count	Number of file descriptors by a process.
system.process-.top.memory.usage	Memory utilization by a process, in Bytes.
SD-WAN	
sdwan.modules-.cost	Cost of SD-WAN modules.
sdwan.modules-.jitter	Jitter of SD-WAN modules.

Data	Description
sdwan.modules-.jitter.limit.max	Jitter threshold of SD-WAN modules.
sdwan.modules-.latency	Latency of SD-WAN modules.
sdwan.modules-.latency.limit.max	Latency threshold of SD-WAN modules.
sdwan.modules-.nexthop.nexthop-.jitter	SD-WAN Nexthop Jitter. This metric is available in R81.20 Jumbo Hotfix Accumulator, Take 79 and higher.
sdwan.modules-.nexthop.nexthop-.latency	SD-WAN Nexthop Latency. This metric is available in R81.20 Jumbo Hotfix Accumulator, Take 79 and higher.
sdwan.modules-.nexthop.nexthop-.packetloss	SD-WAN Nexthop Packet Loss. This metric is available in R81.20 Jumbo Hotfix Accumulator, Take 79 and higher.
sdwan.modules-.overlay_vpn.connections.downtime	Indicates how long the Overlay VPN connection was down (in seconds).
sdwan.modules-.overlay_vpn.connections.drops	Indicates how many times the Overlay VPN connection has been dropped.
sdwan.modules-.overlay_vpn.connections.uptime	Indicates how long the Overlay VPN connection was up (in seconds).
sdwan.modules-.packetloss	Packet Loss of SD-WAN modules.
sdwan.modules-.packetloss.count	Packet Loss Counter of SD-WAN modules.
sdwan.modules-.packetloss.limit-.max	Packet Loss threshold of SD-WAN modules.

Data	Description
system.network-.interface.rx_-throughput_bs	Current rate of successfully received packets over the communication channel (in bits per second).
system.network-.interface.tx_-throughput_bs	Current rate of successfully transmitted packets over the communication channel (in bits per second).
sdwan.modules.s-tate	State of SD-WAN modules.
system.sdwan-.overlay_cost	Cost of Overlay VPN
system.sdwan-.overlay_down_to-tal_count	Number of times the Overlay VPN connection has been dropped.
system.sdwan.g-w_data	Data/statistics about SD-WAN gateways (example, status, throughput, or health).
system.sdwan-.overlay_down_-last_time	Timestamp of the last time an SD-WAN overlay tunnel went down.
system.sdwan-.overlay_jitter	Overlay VPN Jitter (in milliseconds).
system.sdwan-.overlay_latency	Overlay VPN Latency (in milliseconds).
system.sdwan-.overlay_packt-loss	Overlay VPN Packet Loss
system.sdwan-.overlay_packt-loss_counter	Packet loss counter
system.sdwan-.overlay_up_last_-time	Overlay VPN Packet Loss Counter.
system.sdwan-.probes.jitter_stat	Jitter statistics (variation in latency) measured by SD-WAN probes.
system.sdwan-.probes.latency_s-tat	Latency statistics (ms) measured by SD-WAN probes.

Data	Description
system.sdwan-.probes.packet-loss_stat	Packet loss statistics (%) measured by SD-WAN probes.
system.sdwan-.rules_steering_-download_speed	Measured download speed (Mbps) for SD-WAN rule-based steering.
system.sdwan-.rules_steer-ing_download_-speed_threshold	The threshold value for download speed in SD-WAN steering rules.
system.sdwan-.rules_steering_is-p_cost	Steering ISP Cost
system.sdwan-.rules_steering_jit-ter_stat	Steering Jitter (in milliseconds).
system.sdwan-.rules_steering_jit-ter_threshold	Steering Jitter Threshold (in milliseconds).
system.sdwan-.rules_steering_-latency_stat	Steering Latency (in milliseconds).
system.sdwan-.rules_steering_-latency_threshold	Steering Latency Threshold (in milliseconds).
system.sdwan-.rules_steering_-packet_lost_per-centage	Steering Packet Loss.
system.sdwan-.rules_steering_-packet_lost_-threshold	Steering Packet Loss Threshold.
system.sdwan-.rules_steering_u-pload_speed	Not available

Data	Description
system.sdwan-.rules_steering_-upload_speed_-threshold	Not available
System > Traffic	
system.traffic.connections	Number of concurrent connections
system.traffic-.dropped	Total number of traffic drops made by Security Gateway Software Blades
system.traffic-.dropped.rate	Rate of traffic drops (number of drops per second) made by Security Gateway Software Blades This metric is available in: • R82 and higher • R81.20 Jumbo Hotfix Accumulator, Take 70 and higher • R81.10 Jumbo Hotfix Accumulator, Take 152 and higher
system.traffic.io-.receive	Inbound throughput (bits per second)
system.traffic.io-.transmit	Outbound throughput (bits per second)
system.traffic-.packets.receive	Inbound packet rate (packets per second)
system.traffic-.packets.transmit	Outbound packet rate (packets per second)
system.traffic.templates	The total number of traffic drops due to the hit rate for Drop Templates exceeding the limit. This metric is available in R81.20 Jumbo Hotfix Accumulator Take 119 and higher.
system.uptime	The total time (in seconds) the system has been running since the last reboot.
VPN > Probes	

Data	Description
vpn.probes.tunnel	The state of the VPN tunnel: • 0 - Down • Any positive integer - Up (this value is the outbound SPI of the VPN tunnel) This metric is available in R82 and higher.
vpn.probes.tunnel_decrypted_bytes	The total number of decrypted bytes. This metric is available in R82 and higher.
vpn.probes.tunnel_decrypt_throughput	VPN tunnel decrypted throughput. This metric is available in R82 and higher.
vpn.probes.tunnel_encrypted_bytes	The total number of encrypted bytes. This metric is available in R82 and higher.
vpn.probes.tunnel_encrypt_throughput	VPN tunnel encrypted throughput. This metric is available in R82 and higher.
vpn.probes.tunnel_expire_time	The time when the VPN Tunnel will expire. This metric is available in R82 and higher.
vpn.probes.tunnel_generated_time	Time when the VPN Tunnel was established. This metric is available in R82 and higher.

Index

F

G

H

I

J

K

L

M

N

O

P

Q

R

S