



Release Notes

FortiNDR Cloud 25.4.a



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



December 16, 2025

FortiNDR Cloud 25.4.a Release Notes

78-254-1113279-20251216

TABLE OF CONTENTS

FortiNDR Cloud release notes	5
Version history	6
Version 25.4.a	6
New functionality	7
Improved functionality	13
Other improvements	18
Version 25.4.0	18
New functionality	18
Improved functionality	19
Other improvements	22
Version 25.3.c	22
New functionality	22
Improved functionality	26
Other improvements	27
Version 25.3.b	28
New functionality	28
Improved functionality	35
Other improvements	39
Deprecated features	40
Version 25.3.a	40
Version 25.3.0	40
Deprecation notice	40
Other improvements	41
Version 25.2.c	41
New functionality	41
Improved functionality	44
Other improvements	47
Version 25.2.b	51
Improved functionality	51
Other improvements	54
Version 25.2.a	54
Version 25.2.0	54
New functionality	55
Improved functionality	57
Other improvements	59
Version 25.1.e	60
New functionality	61
Improved functionality	64
IQL queries	66
Other improvements	67
Version 25.1.d	67
Improved functionality	68
Other improvements	70
Version 25.1.c	71
New functionality	71

Improved functionality	73
Other improvements	74
Deprecated functionality	74
Version 25.1.b	74
Improved functionality	75
Version 25.1.a	76
New functionality	77
Improved functionality	79
Integrations	81
Other improvements	81
Version 25.1.0	81
New functionality	82
Improved functionality	84
Other improvements	84
Product integration and support	85
Resolved issues	87
25.4.a	87
25.4.0	87
25.3.c	88
25.3.b	88
25.3.a	88
25.3.0	89
25.2.c	89
25.2.b	89
25.2.a	90
25.2.0	90
25.1.e	90
25.1.d	90
25.1.c	91
25.1.b	91
25.1.a	91
25.1.0	92
Known issues	93
25.4.a	93

FortiNDR Cloud release notes

This document provides information about FortiNDR Cloud releases.

FortiNDR Cloud is a SaaS network security monitoring platform designed to facilitate rapid detection, investigations, and threat hunting within your environment. FortiNDR Cloud is designed to be scalable and to remove the responsibilities of maintaining tooling from security analysts. For more information, see the [FortiNDR Cloud User Guide](#).

Version history

Date	Version
10 December 2025	Version 25.4.a on page 6
05 November 2025	Version 25.4.0 on page 18
15 September 2025	Version 25.3.c on page 22
03 September 2025	Version 25.3.b on page 28
15 July 2025	Version 25.3.a on page 40
07 July 2025	Version 25.3.0 on page 40
26 June 2025	Version 25.2.c on page 41
21 May 2025	Version 25.2.b on page 51
08 May 2025	Version 25.2.a on page 54
30 April 2025	Version 25.2.0 on page 54
26 March 2025	Version 25.1.e on page 60
12 March 2026	Version 25.1.d on page 67
27 February 2025	Version 25.1.c on page 71
12 February 2025	Version 25.1.b on page 74
29 January 2025	Version 25.1.a on page 76
08 January 2025	Version 25.1.0 on page 81

Version 25.4.a

- [New functionality](#)
 - [Natural Language Queries](#)
 - [FortiAI](#)
 - [Device enrichment](#)
 - [Gen AI Dashboard](#)
- [Improved functionality](#)
 - [Entity panel](#)
 - [Sensor metrics](#)
 - [Sensors page](#)
 - [Detections table](#)

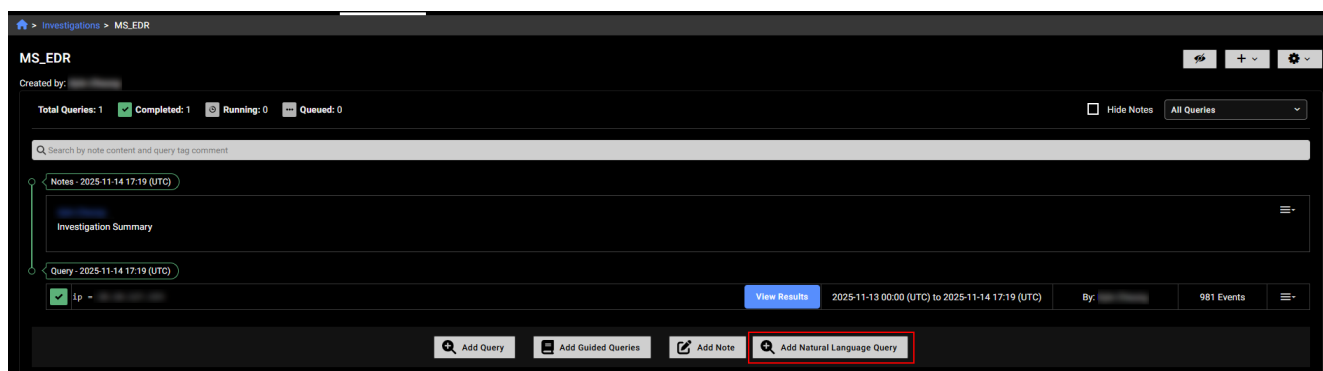
- [Detection resolution comments](#)
- [Investigation results](#)
- [FortiNDR Essentials Solution Pack v1.0.1](#)
- [Other improvements](#)
- [Resolved issues on page 87](#)

New functionality

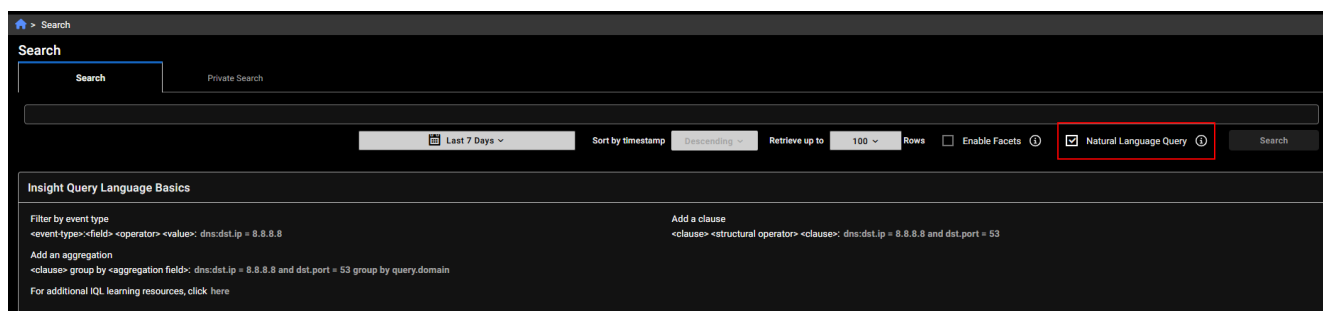
Natural Language Queries

Natural Language (NL) Queries allow you to use simple statements for investigations and private searches as an alternative to the Internal Query Language (IQL). You can start an NL query from the *Investigations* or *Private Search* pages. **Note:** NL queries currently do not support all event types. For more information, see [Natural Language Queries](#).

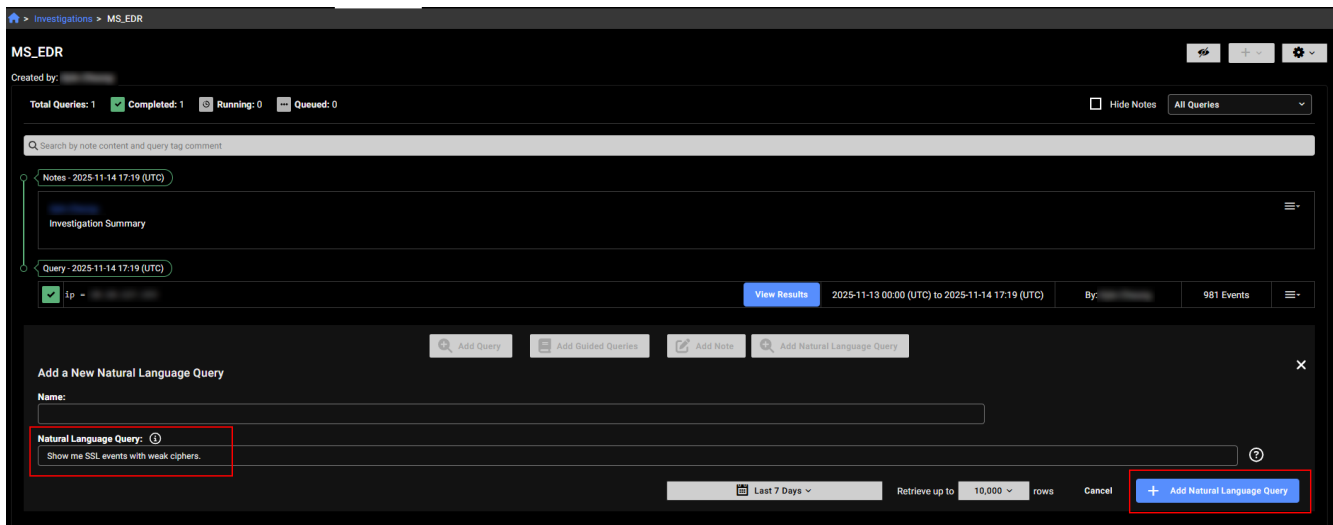
To use an NL query in an investigation, click the *Add Natural language Query* button the investigations details page.



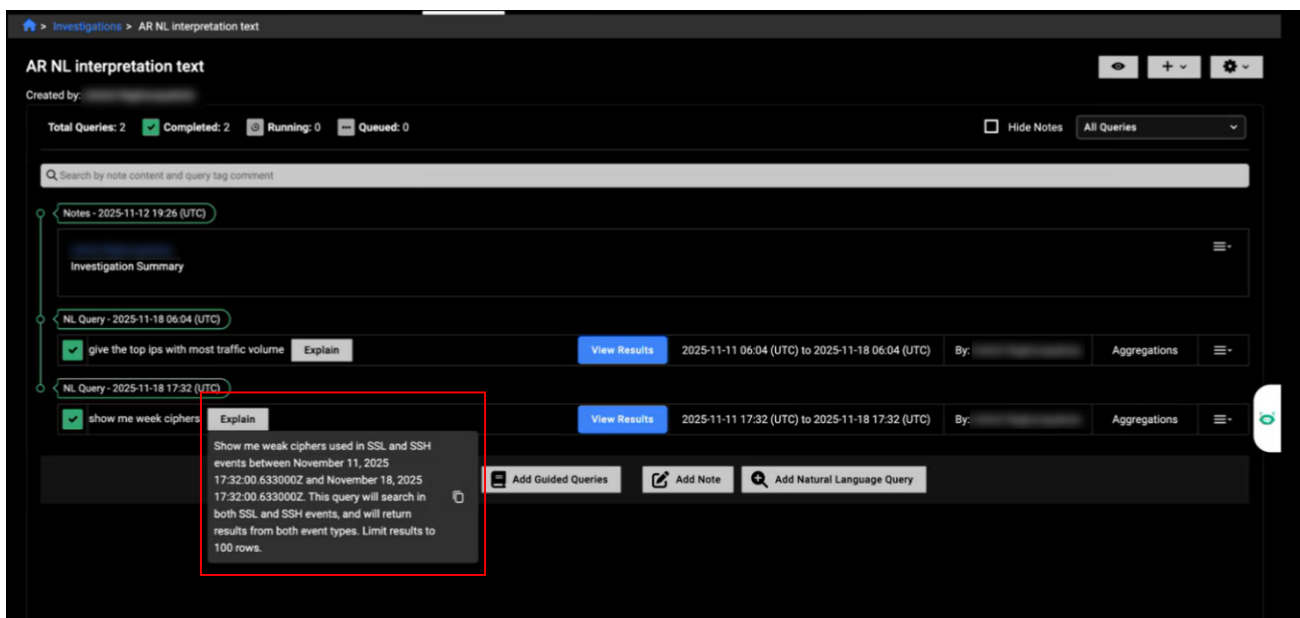
To use an NL query in *Private Search*, enable *Natural Language Query* at the top of the page.



Enter a query string such as *Show me SSL events with weak ciphers* in the search field and click *Search* or *Add Natural language Query* depending on the page you are in.



The *Explain* button next to the query results displays how the system interpreted your request and the queries it executed. You can copy this explanation and edit it to refine your queries. The Explain button is also available in *Private Search*.



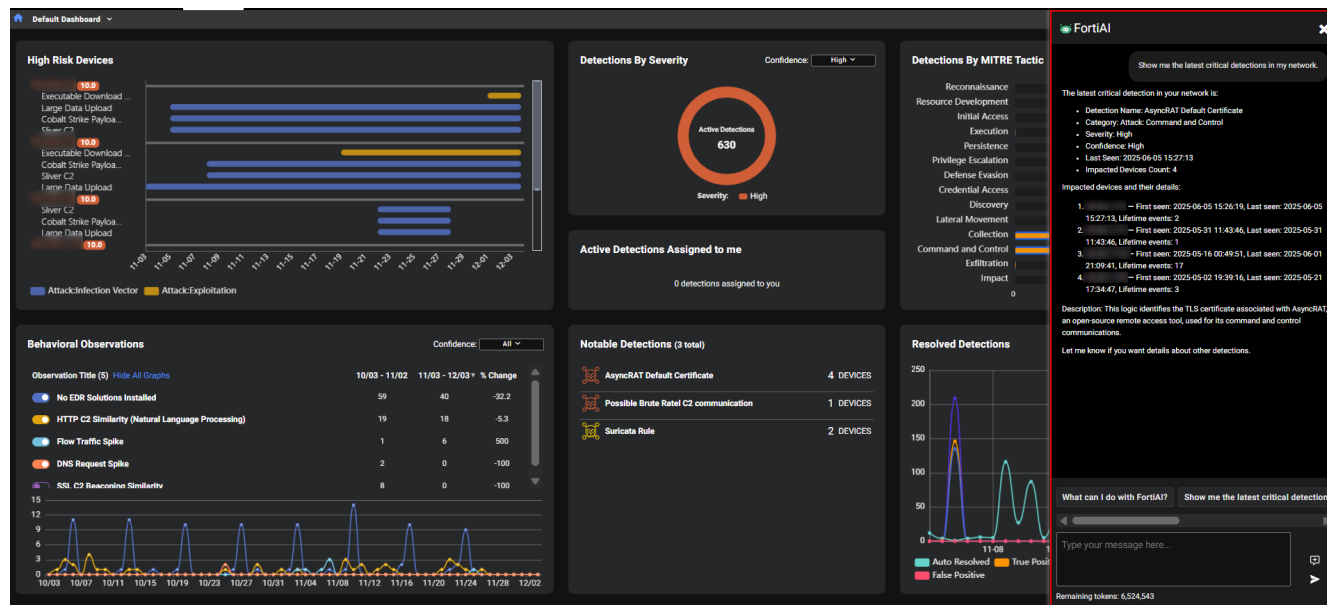
FortiAI

FortiAI in FortiNDR Cloud is Fortinet's generative AI assistant designed to accelerate threat investigation and improve visibility into network activity. Integrated into the FortiNDR portal, FortiAI allows administrators to interact in natural language and receive precise, context-aware insights about detections, understand which threats and behaviors are being monitored, and generate detailed entity reports with historical context through intuitive, conversational queries.

FortiAI requires a valid license and operates on a token-based entitlement system, where each query consumes tokens based on complexity and response length.

Fortinet requires customers to opt in to use FortAI features. Once enabled, administrators must assign roles to specific users who need access to FortAI. If the organization has child accounts, FortAI must be enabled individually for each child account.

For more information, see [FortAI](#).



Device enrichment

You can now enhance device identification using *Device Enrichment*. When configured, it retrieves hostname information from Windows Active Directory (AD) and DNS servers in the target network. Once enabled, the enrichment process runs on the schedule defined in the enrichment settings.

After a cycle completes, the process schedules the next cycle based on the profile settings. If the current cycle is still running when the next scheduled cycle is due, the system skips that cycle.

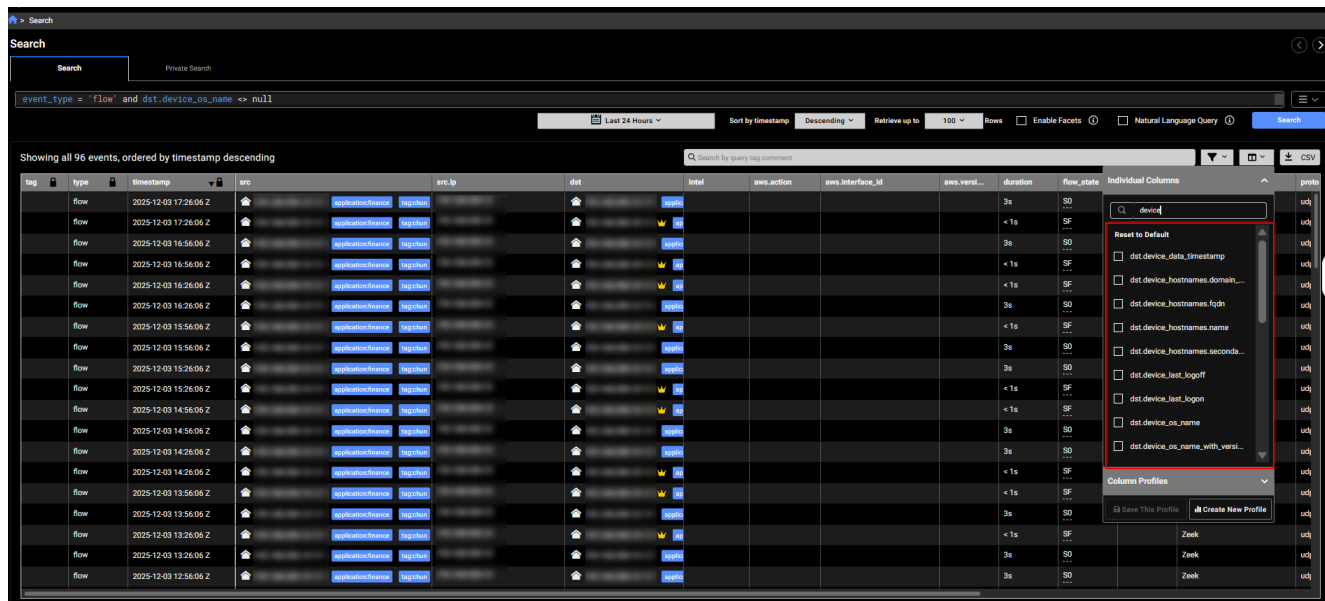
Only one sensor can be used for Device Enrichment per account. Device Enrichment requires sensors running 2.4.0 or higher.

The screenshot shows the configuration page for FortiNDR Cloud 25.4.a, specifically the 'DEVICE ENRICHMENT CONFIGURATION' section.

- USER ACTIVITY TIMEOUT:** A section with a text input field set to 480 and an 'Update' button.
- DEVICE ENRICHMENT CONFIGURATION:** A section with a 'Configure' button and a description: 'Configure Active Directory and DNS settings for device enrichment.'
- CONTRACTED BANDWIDTH:** A section with a table for bandwidth configuration. The table has columns for 'Start Month', 'End Month', and 'Bandwidth'. The current state shows 'No licenses configured'.

Once the profile is configured, it retrieves a list of devices and their names, performs DNS queries to resolve corresponding IP addresses, and sends detailed information for each device, including its name, IP address, operating system, and other attributes.

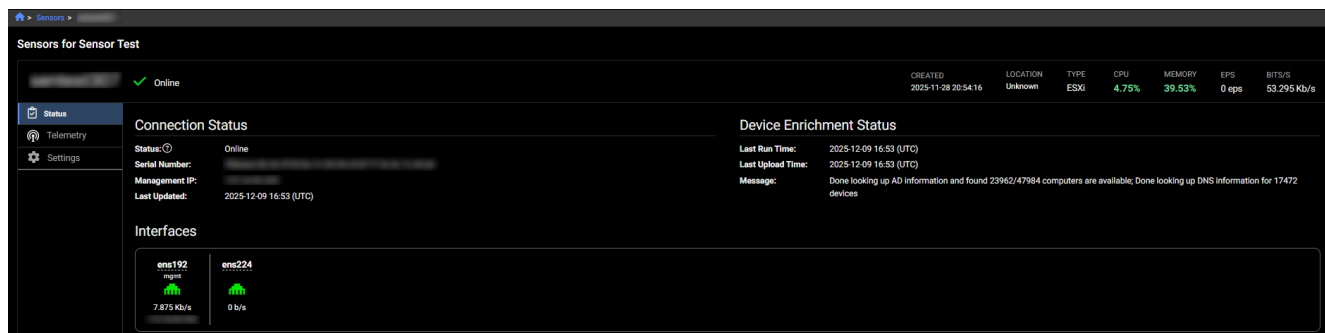
The fields related to the new newly added by Active Directory injection enrichment start with *device* underscore.



The screenshot shows the FortiNDR Cloud search interface. The main table displays a list of events, sorted by timestamp descending. The table columns include log, type, timestamp, src, dst, intel, aws.action, aws.interface_id, aws.verd..., duration, flow_state, and proto. The sidebar on the right shows the 'Individual Columns' section with a search bar and a list of filters, including 'device' and 'dst.device_data.timestamp'.

log	type	timestamp	src	dst	intel	aws.action	aws.interface_id	aws.verd...	duration	flow_state	proto
flow	flow	2025-12-03 17:26:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 17:26:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 16:56:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 16:56:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 16:26:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 15:56:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 15:26:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 15:26:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 14:56:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 14:56:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 14:26:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 13:56:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 13:26:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 13:26:06 Z	...	...	...	...	...	...	< 1s	SF	udp
flow	flow	2025-12-03 12:56:06 Z	...	...	...	...	...	...	< 1s	SF	udp

The sensor's details page displays the *Device Enrichment Status*.



The screenshot shows the FortiNDR Cloud sensor details page. The page displays the sensor's status as 'Online' and provides a summary of its connection status and device enrichment status. The 'Device Enrichment Status' section shows the last run time, last upload time, and a message indicating that AD information was found and DNS information was looked up.

Connection Status	Device Enrichment Status
Status: Online Serial Number: ... Management IP: ... Last Updated: 2025-12-09 16:53 (UTC)	Last Run Time: 2025-12-09 16:53 (UTC) Last Upload Time: 2025-12-09 16:53 (UTC) Message: Done looking up AD information and found 23962/47984 computers are available; Done looking up DNS information for 17472 devices

Gen AI Dashboard

The *Gen AI Dashboard* provides a centralized view of generative AI usage within your organization, helping analysts identify unauthorized activity, detect potential data exfiltration, investigate anomalies with full device and detection context, and align AI activity with the organization's security policies.

The widgets consolidate all observation details from FortiNDR Cloud into a single view, giving analysts visibility into AI usage across the organization. This unified perspective is useful for identifying patterns and anomalies by turning raw observations into actionable insights, enabling faster, more informed investigations.

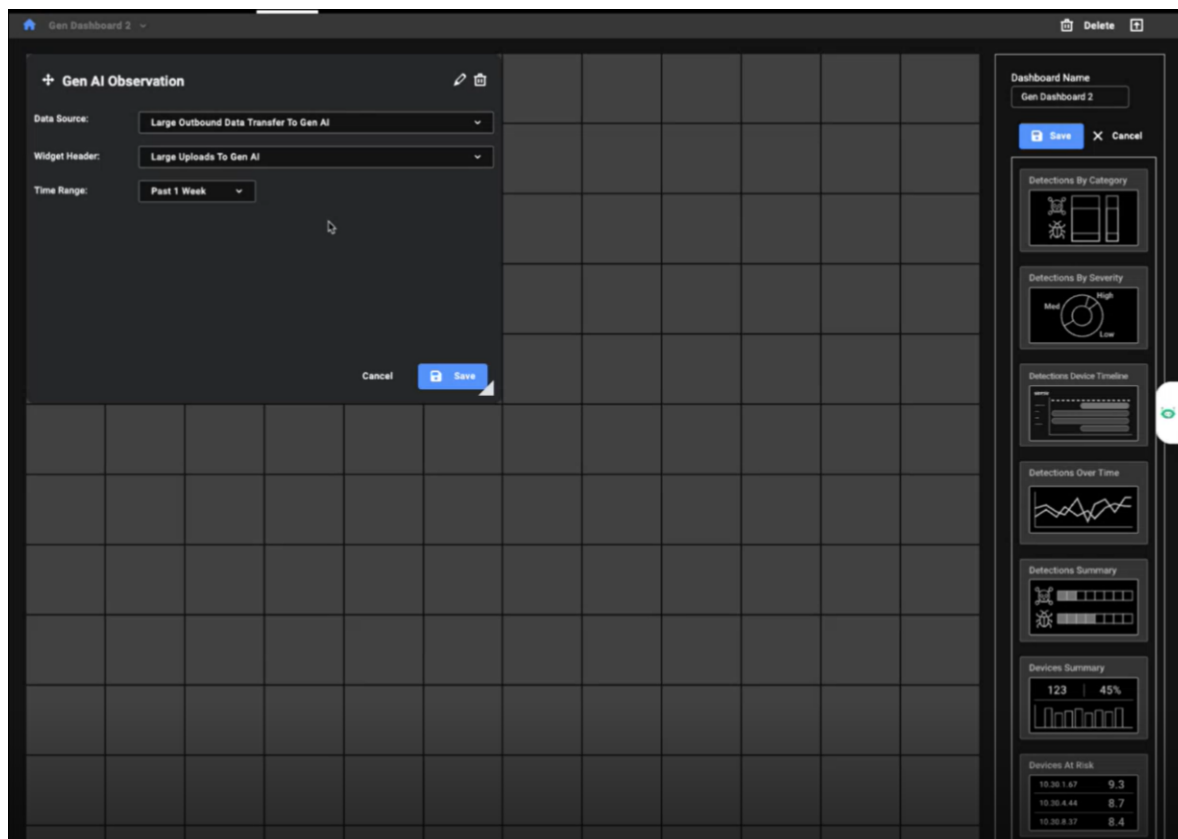
You can use the widgets in this dashboard to track which AI providers are accessed and by which devices and identify large uploads and frequent connections that may indicate risky behavior.

The dashboard contains the following widgets:

Widget	Description
No. of Connections to Gen AI Providers	Tracks the number of connections and provider type for the last 14 days. The widget also identifies which generative AI is a General Assistant and a Coding Assistant.
No. of Connections from Source	Shows which IPs connect to which providers and the number of connections to AI providers for the last 14 days. Click on the IP address to open the Entity Panel. Hovering over the bar opens a tooltip that connects to the <i>Observation Details</i> and <i>Detection Context</i> .
Large outbound traffic to Gen AI	Displays size of large outbound transfers for the last 14 days. Click the IP to open the Entity Panel. Hover over the lines in the chart to see details about the upload.
Sum of Bytes Sent to Gen AI	Aggregates data volume per IP and provider for the last 14 days. The data is sorted highest to lowest to identify top uploader IP address. Hovering over the bar opens a tooltip that connects to the <i>Observation Details</i> and <i>Detection Context</i> .
No. of Files Uploaded by Source	Counts files sent to AI services for the last 14 days.
Large outbound traffic sessions	Monitors connection frequency of large outbound connections. Hovering over the bar opens a tooltip that connects to the <i>Observation Details</i> and <i>Detection Context</i> .



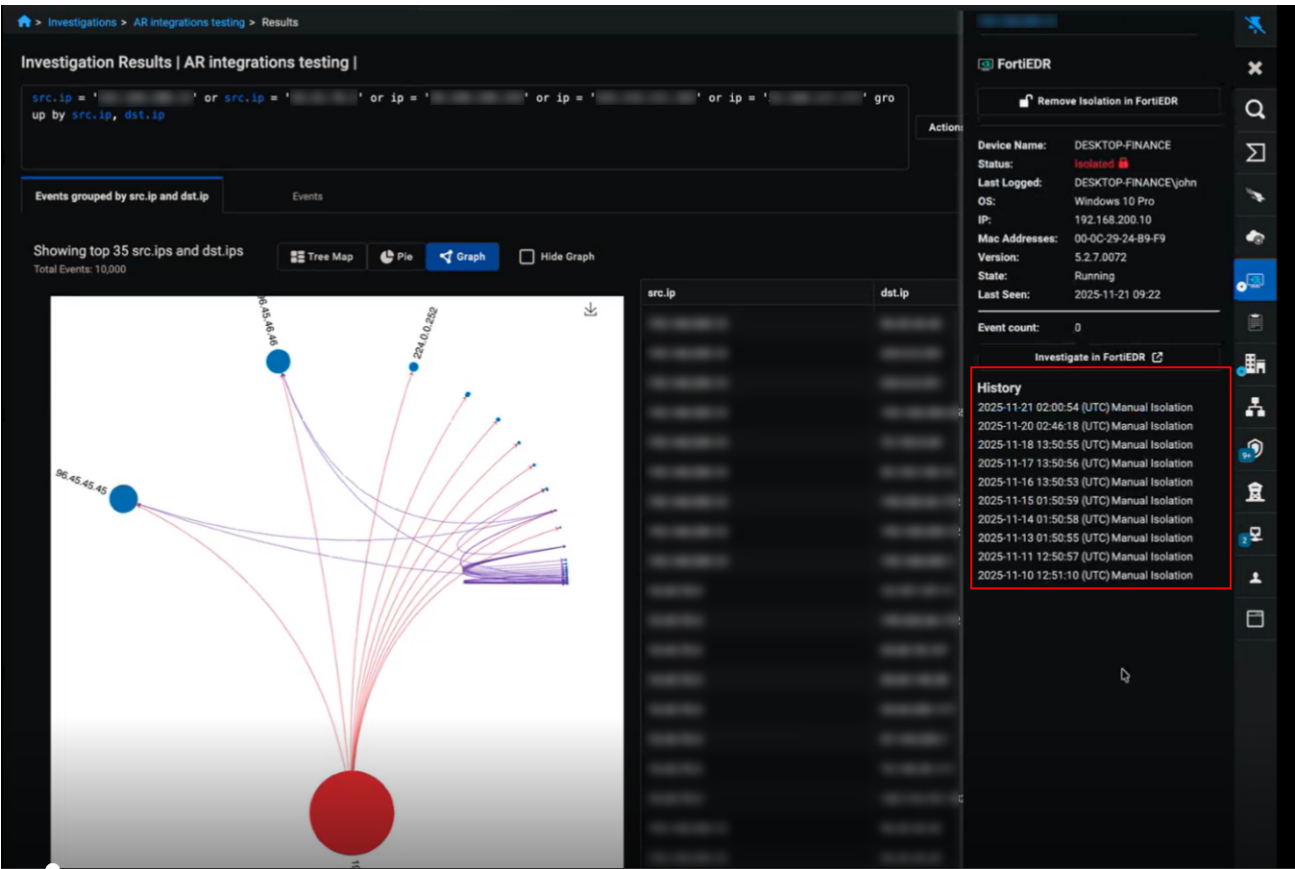
You can also create a custom dashboard based on the Gen AI widgets.



Improved functionality

Entity panel

The *Entity Panel* now displays the history of actions performed on a device for CrowdStrike, EDR, and FortiManager integrations. These actions include manual isolation, automatic isolation, and removal of isolation. The list shows up to 50 of the most recent actions. Actions triggered by the Fortinet Automation Service appear in the *Fortinet Automation Service* tab.



Sensors page

The *Sensors* page now includes a *Features* column that lists the enabled tools used to analyze network traffic and detect anomalies, such as Suricata, PCAP or DPI.

Sensors for [selected sensor]

Showing 15 sensors (15 active sensors)

Search by sensor ID, status and location

Telemetry Visible Devices Actions CSV

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	EPS (7 DAYS AVERAGE)	BITS/s (7 DAYS AVERAGE)	TYPE	Features
gig1	Online	2.1.0	top	Spain	0.8 EPS	60.464 kb/s	ESXI	PCAP, SURICATA
gig3	Pausing	2.1.0	internal, updated	Spain	0 EPS	0 b/s	ESXI	SURICATA
gig4	Offline	2.1.0	lab		42 EPS	0 b/s	ESXI	SURICATA
gig5	Pausing	2.1.0			0 EPS	0 b/s	QEMU/KVM	SURICATA

A corresponding *Features* filter was also added to the page.

Sensors for **FortiNDR Cloud**

Showing 15 sensors (15 active sensors)

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	EPS (7 DAYS AVERAGE)	BITS/S (7 DAYS AVERAGE)	TYPE
gig1	Online	2.1.0	Internal		0.8 EPS	60.464 Kb/s	ESXi
gig3	Pausing	2.1.0	Internal		0 EPS	0 b/s	ESXi
gig4	Offline	2.1.0	Internal		42 EPS	0 b/s	ESXi
gig5	Pausing	2.1.0			0 EPS	0 b/s	QEMU
gig6	Online	2.1.0			0.3 EPS	8.724 Kb/s	QEMU
gig7	Offline	2.1.0			0 EPS	0 b/s	QEMU
gig9	Provisioning	2.0.0			0 EPS	0 b/s	ESXi
gig10	Offline	2.1.0			0 EPS	0 b/s	ESXi
gig11	Offline	2.0.0	Internal		0 EPS	0 b/s	ESXi

Additional Filters

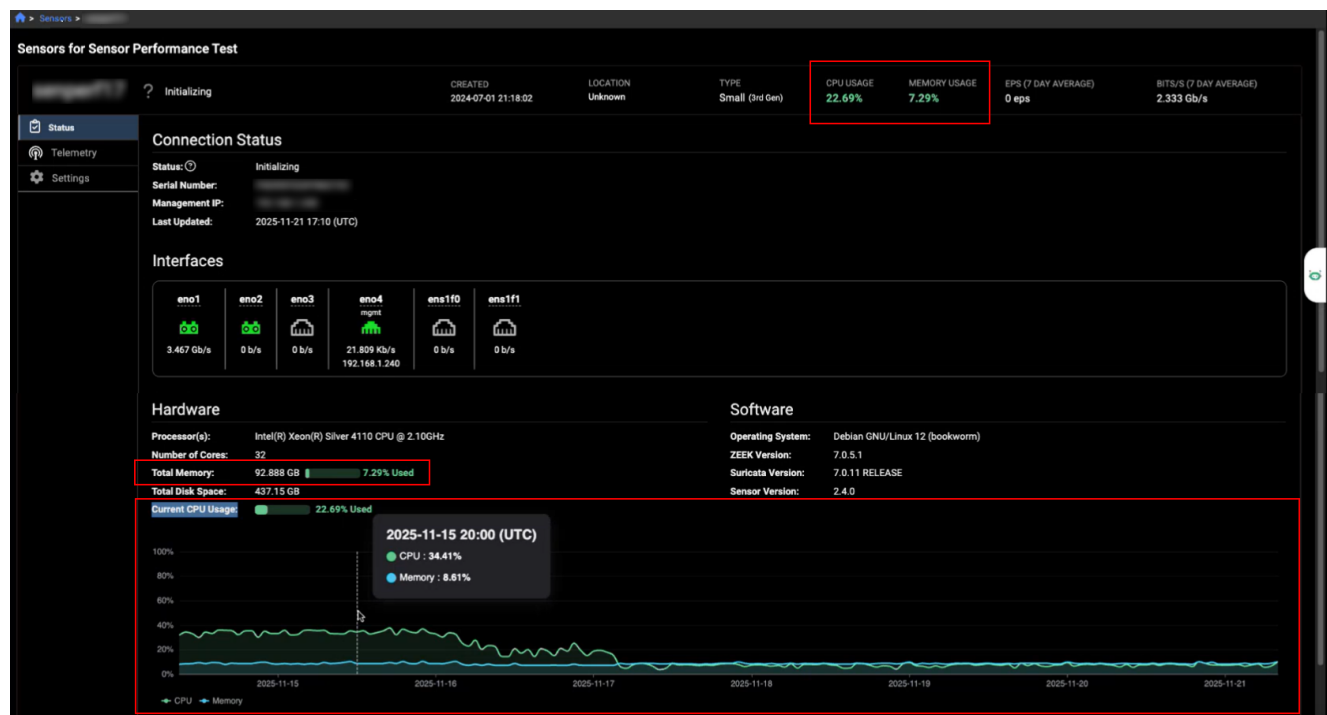
- Status: Offline, Online, Pausing, Provisioning
- Type: All
- Version: No Filters
- Features: No Filters
- DPI: ☐
- PCAP: ☐
- Suricata: ☐

Sensor metrics

The *Sensor Details* page now displays the current CPU and memory usage for the sensor at the top of the page and as a bar charts in the *Hardware* section. The usage values are color-coded:

- Green if usage is 0-59%
- Yellow if usage exceeds 60%
- Red if usage exceeds 90%

A graph has been added to the *Hardware* section to track CPU and memory usage over the last 24 hours. You can hover over the graph to view usage at a specific point in time. This graph was also added to a to the *Telemetry* tab; to view it click *CPU & Memory Usage*.



Detections table

The filters in the *Detections Table* have been redesigned as a collapsible pane on the left side of the page. This allows you to select all filters at once before applying them, reducing the number of page refreshes. To remove all filters, simply click *Clear All*. This update was also applied to graph and timeline views of the table.

The screenshot shows the 'Detections Table' interface. On the left, there is a new 'Filters' pane with a 'Clear Filter' button and an 'Apply' button. The main table displays 13 detectors and 265 devices from 5000 detections (out of 6922 total). The table columns include Detection UUID, Device IP, DHCP Hostname, Username, Hostname, MAC Address, Lifetime Events, Indicators, First Seen, Last Seen, and Action. The filters pane on the left includes sections for Impacted Devices, Date (2025-11-24 to 2025-12-08), Category (None), Created By (All), MITRE ATTACK (None), Assigned To (None), Resolved By (None), Resolution (None), Sensor (None), Detection Name (Detection Name), Remediation Status (None), and Severity.

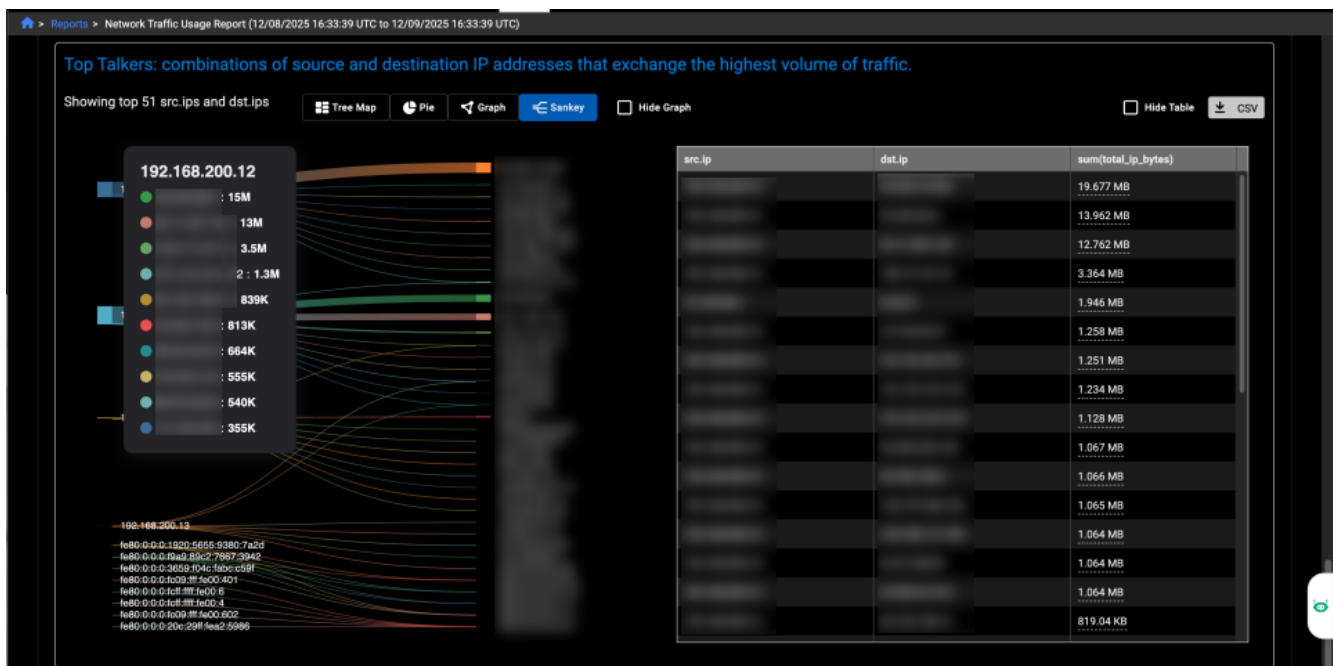
Detection resolution comments

We have also added the ability to update the resolution comment directly from the *Actions* menu.

The screenshot shows the 'Detections Table' interface with 14 detectors and 272 devices from 5000 detections (out of 6856 total). The table columns include Muted By, Date Muted, Mute Co..., Resolved Comment, Assigned Comment, Assignee, and Action. The 'Actions' menu is open for a specific detection, showing options like 'Unresolve Detection', 'Update Resolution Comment', 'Mute Device for Detection', 'Mute Device for Detector', and 'Mute Device for Account'.

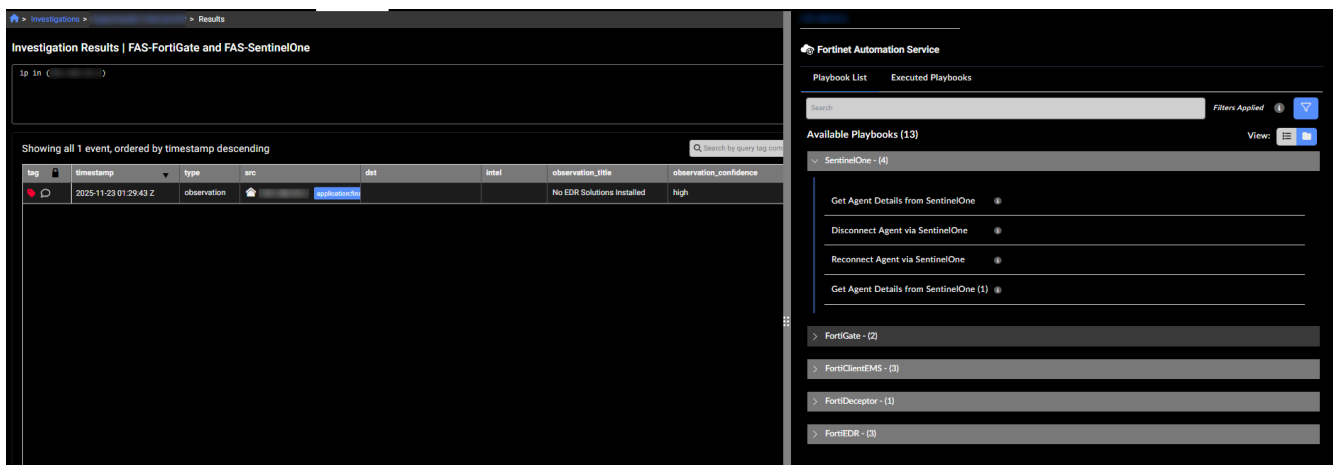
Investigation results

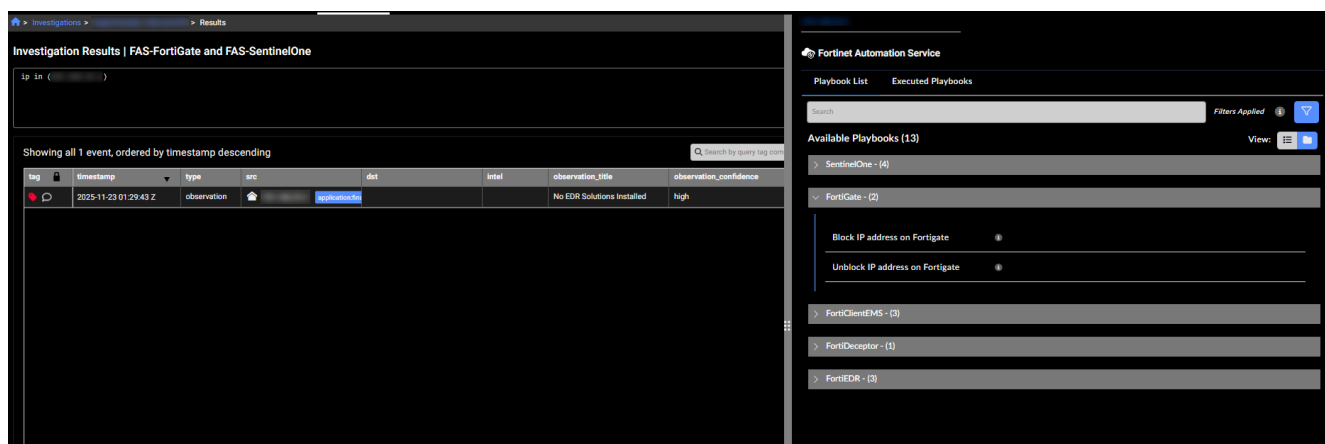
A new *Sankey* chart has been added to the investigation results and the *Network Traffic Usage* report. It is available for aggregations where *Group By* includes two IP fields or when there are two dimensions and a measure. The Sankey chart type appears only when there are 50 or fewer dimensions.



FortiNDR Essentials Solution Pack v1.0.1

The *FortiNDR Essentials Solution Pack* version 1.0.1 contains connectors and playbooks for FortiGate and Sentinel One.





Other improvements

- You can now download the data in the *Behavioral Observations* page as a CSV file.
- The Client Secret is masked when you configure an integration.
- Updated *Security Posture* queries to include checks for outdated web browsers and end-of-life operating systems.

Version 25.4.0

- New functionality
 - Fortinet Automation Service
- Improved functionality
 - Default dashboard
 - Detection device timeline
 - Event fields
- Other improvements
- Resolved issues on page 87

New functionality

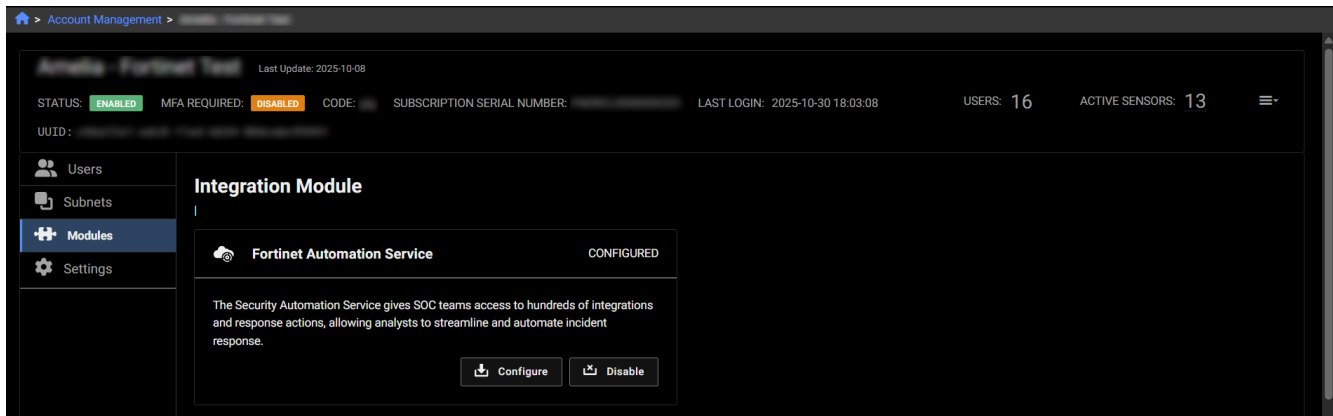
Fortinet Automation Service

The Fortinet Automation Service integration streamlines and automates security operations within FortiNDR Cloud. This service enables security teams to execute predefined playbooks that perform specific actions based on connector configurations and conditional logic. A playbook can range from a simple API call to a complex, multi-step process involving several queries. Users can trigger playbooks without needing to

understand the underlying logic, allowing them to focus on the intended outcome rather than the implementation details. This service enhances operational efficiency by simplifying tasks such as isolating devices, retrieving deployment network details, and executing other automated actions.

When the Fortinet Automation Service is provisioned, the *FNDR Essentials Solution Pack* is installed automatically. This service pack contains both connectors and playbooks. To configure and install the related connectors and agents go to *Account Management > Modules* and click *Configure*.

For more information, see [Fortinet Automation Service](#).



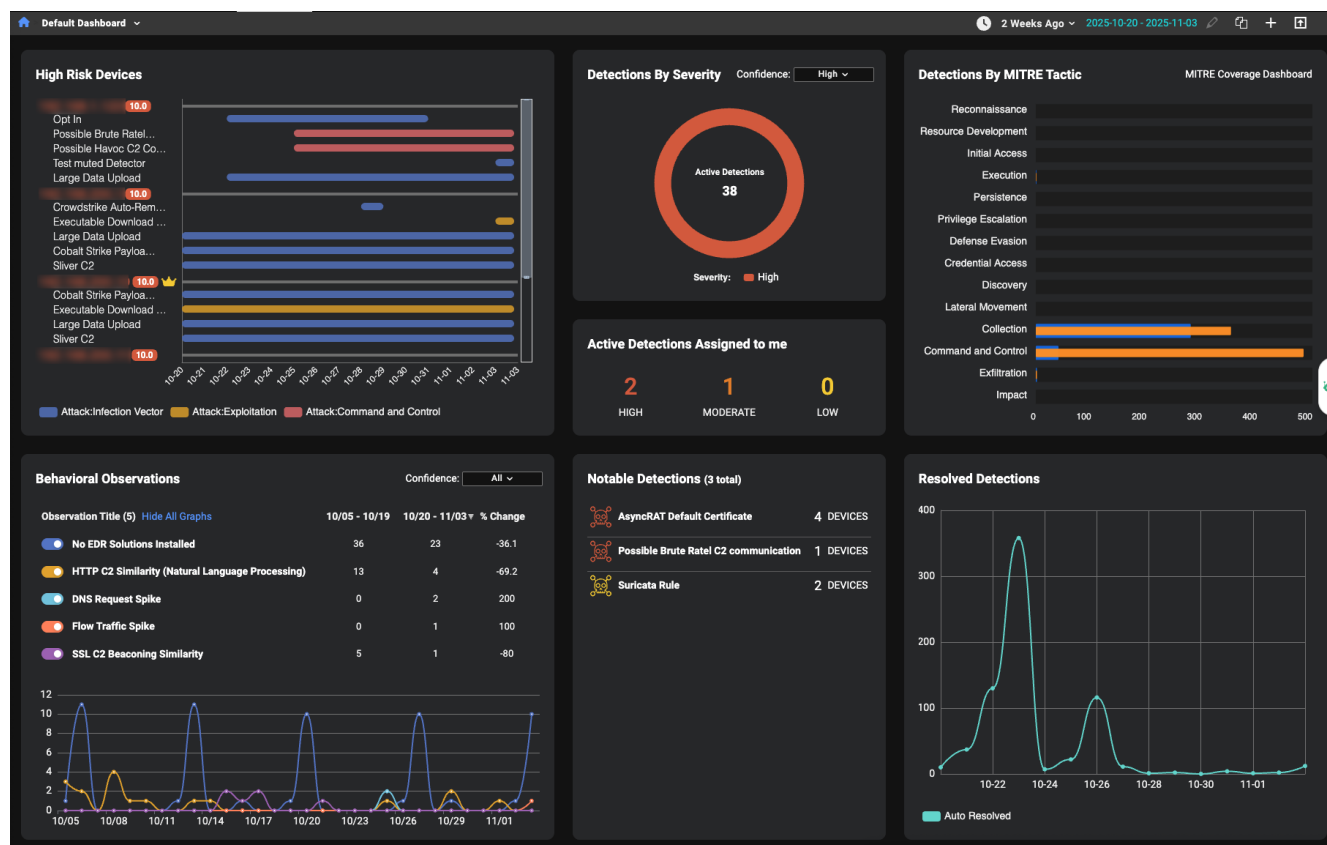
Improved functionality

Default dashboard

The default dashboard has been redesigned with a cleaner, more modern layout. The new design introduces enhanced functionality and richer visualizations. This redesign is driven by a focus on analyst workflows and risk-based prioritization. All dashboard widgets (both default and custom) now feature a refreshed look with simplified styling for a more streamlined appearance. Widgets also load in a structured sequence, improving visual consistency during page load.

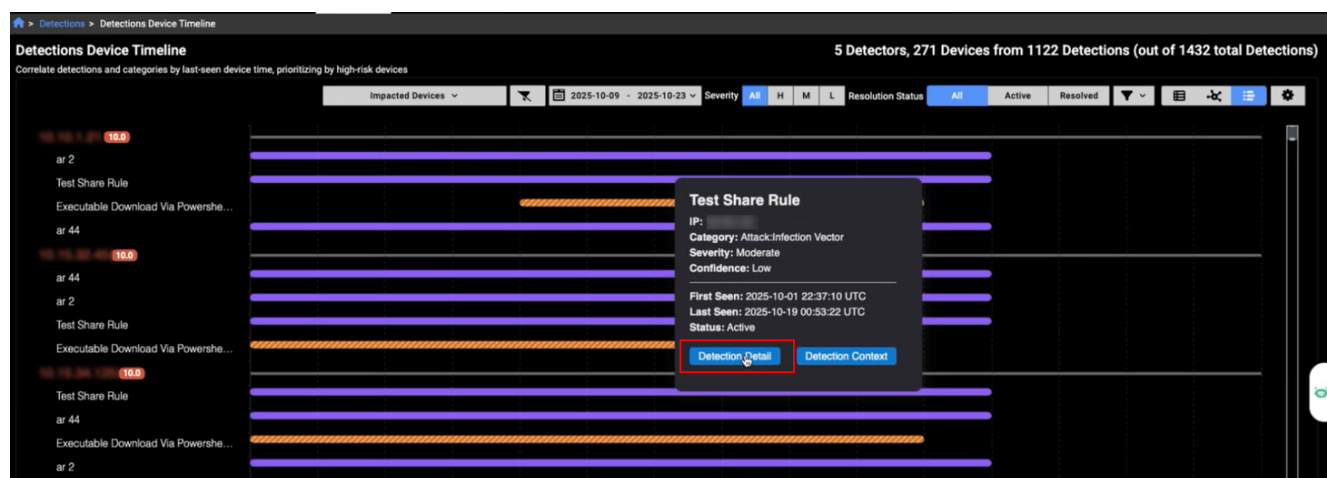
Key improvements:

- The *Global Date Picker* (located above the *Detections by MITRE Tactic* widget) applies a selected date range to all dashboard widgets with a time range, updating them simultaneously regardless of their individual time settings.
- The new *High-Risk Devices* widget helps you quickly identify high-risk assets by displaying risk scores next to device IPs and using color-coded crown icons for identified assets. Click a device IP to open the *Entity Panel*.
- The *Detections by Severity* widget helps you identify high-severity detections by grouping them by confidence level on initial load, with an added dropdown menu to switch between severity levels or view all.
- The *Notable Detections* widget highlights detectors with tags such as *New* or *Spike* to help quickly identify emerging or unusual activity.
- The *Detections by MITRE Tactic* and *Resolved Detections* widgets now features redesigned visualizations for improved clarity.



Detection device timeline

The *Detection Device Timeline* now features a cleaner design for improved readability. A new *Detection Detail* button has been added to the tooltip, allowing you to quickly navigate to the detection details page for a selected detector.



You can now filter the timeline to show detections from a specific detector by clicking its name. Risk scores are displayed next to the IP addresses, providing quick insight into the risk level of the detection.



A crown icon appears next to an IP to indicate *Identified Assets* within the timeline view. The crown's color is determined by the priority level: High, Moderate, or Low.



Event fields

IQL queries have been expanded to include the following events and fields:

- **BACnet events:**
 - *BACnet Device control* :A BACnet device control event occurs when BACnet messages like Reinitialize-Device or Device-Communication-Control are detected. These events log administrative actions that affect device availability and behavior.
 - *BACnet Discovery*: A BACnet discovery event is created when Who-Is/I-Am/Who-Has/I-Have messages are observed, recording device/object identifiers and vendor information for rapid inventory. This log focuses on unconfirmed services used for discovery.
 - *BACnet Property*: A BACnet property event is created when Read-Property-Request, Read-Property-ACK, or Write-Property-Request messages are observed, capturing object type, instance number, property identifier, array index, and value. This log focuses on confirmed services used for reading and writing properties.
 - *BACnet header*: A BACnet header event is created when any BACnet/IP packet is seen; the log captures header information for both APDU and NPDU messages. BACnet is a building automation/control protocol used for device discovery, property access, and supervisory functions.
- **Profinet**: A profinet event is created by the use of PROFINET an Ethernet protocol for communication between devices in industrial automation systems.
- **SSH**: SSH events now support the following fields:
 - *ssf_hassh*: Adds support for identifying SSH clients and servers using network fingerprinting, helping to detect and classify SSH traffic more accurately.
 - *ssh_hassh_server*: Adds network fingerprinting to help detect and classify specific SSH server implementations based on their behavior.
- **community_id**: This field was added to Suricata and Flow events. This field makes it easier to match network connections across different tools to help streamline investigations and improve event correlation.

Other improvements

Improved Entity Panel performance:

- We have improved the responsiveness of the *Entity Panel*. Individual sections now appear sooner, providing faster visibility and a smoother user experience.

MITRE techniques:

- The following techniques were added: *Compromise Infrastructure - Network Devices, Wi-Fi Networks, Remote Access Tools - Remote Desktop Software, Modify Registry, Account Manipulation - Additional Local or Domain Groups, Application Layer Protocol - Publish/Subscribe Protocols, Software Extensions - IDE Extensions, Exfiltration Over Web Service - Exfiltration Over Webhook, Resource Hijacking - Compute Hijacking, Resource Hijacking - Bandwidth Hijacking, and Hide Infrastructure.*

Improved visual styling:

- We have refined the appearance of the *Investigation Details* page by applying distinct colors and italic styling to improve clarity and visibility.
- Dropdown menus have been improved to accommodate sub-menus that do not fit a browser page. We have also improved the performance of the context menus.

Version 25.3.c

- [New functionality](#)
 - [DPI Dashboards](#)
 - [Improved functionality](#)
- [Reports](#)
 - [Entity Panel](#)
- [Other improvements](#)
- [Resolved issues on page 87](#)

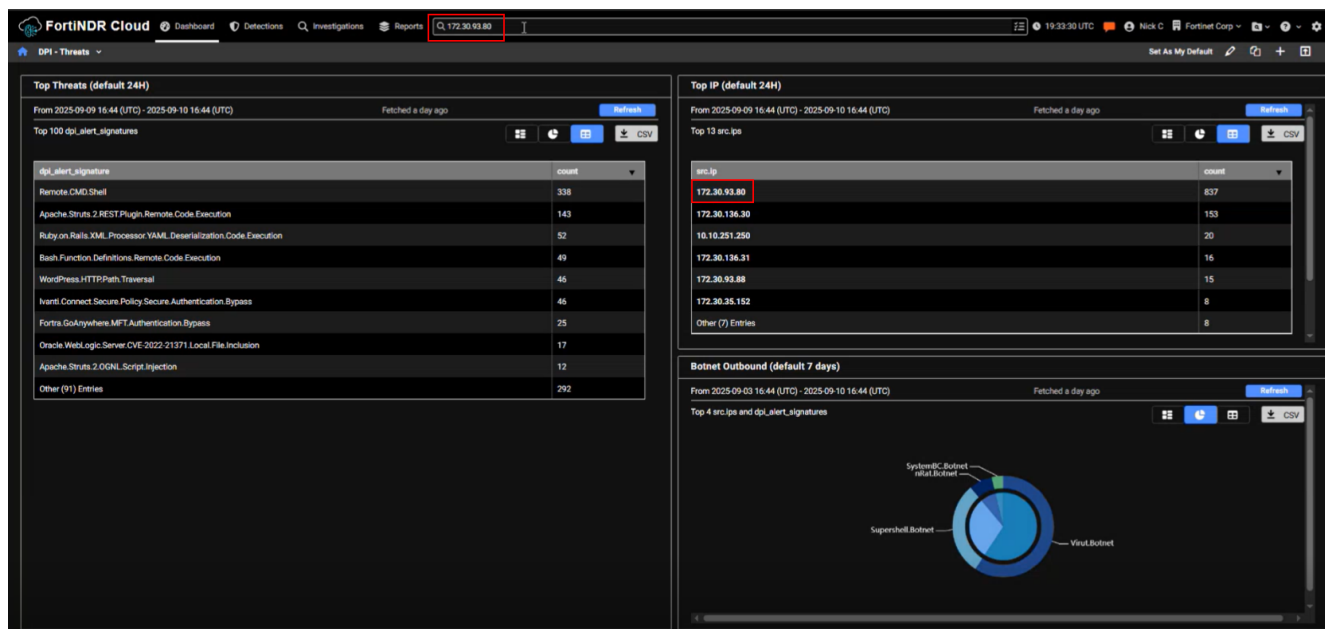
New functionality

DPI Dashboards

Three new dashboards have been added for Fortinet DPI:

- DPI - Threats
- DPI - AppCtrl
- DPI - OT

These dashboards are available from the *Dashboard* menu but will only display data when *Fortinet DPI* is enabled on the *Sensor Settings* page. The dashboards display DPI events from either the past 24 hours or the past 7 days, depending on the dashboard. The data can be refreshed at any time. You can view the dashboards as a chart, pie chart, or table, and export the data as a CSV file. DPI dashboards are useful when starting an investigation. For example, if an IP address is flagged in one of the dashboards, you can enter it in the Global Search field or use it to create a query in Private Search.



DPI - Threats

The DPI - Threats dashboard displays detected threats and their corresponding counts. The dashboard provides a summary of the most frequently detected threats and highlights the IP addresses that are triggering the highest number of signatures. When an IP address triggers a large number of IPS signatures, it's a strong indicator that the IP should be investigated further.

This dashboard contains three monitors:

Top Threats

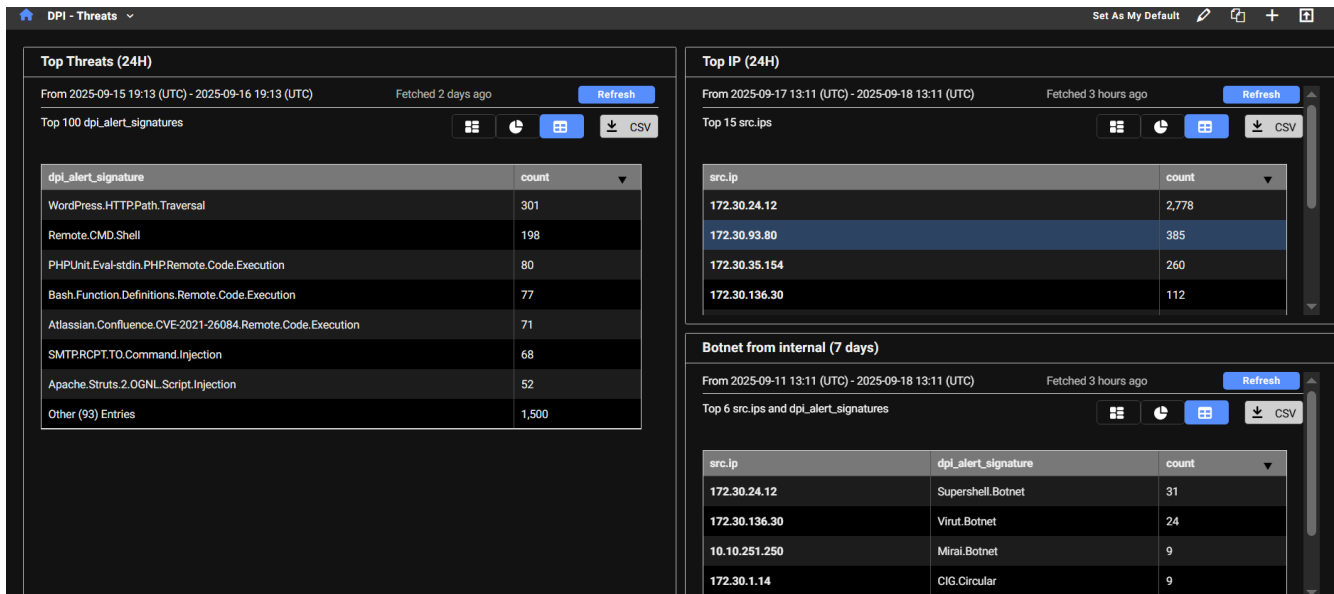
This monitor queries high-severity IDS alerts (severity level 4) detected by DPI, where either the source or destination is internal. It excludes alerts triggered by device tagged as *Scan* and *Nessus* and filters out two noisy Apache-related signatures. The results are grouped by alert signature, helping identify which threat signatures are most frequently triggered.

Top IP

This monitor retrieves high-severity IDS alerts (severity level 4) detected by DPI, where either the source or destination is internal. It excludes alerts triggered by devices tagged as *Scan* or *Nessus* and filters out two noisy Apache-related signatures. The results are grouped by source IP, helping identify which internal hosts are generating the most IDS alerts.

Botnet from internal

This monitor identifies outbound botnet-related DPI alerts where the source IP is internal. It groups the results by both the internal source IP and the specific botnet signature that was triggered, helping pinpoint which internal hosts are attempting to communicate with known botnets.



DPI - AppCtrl

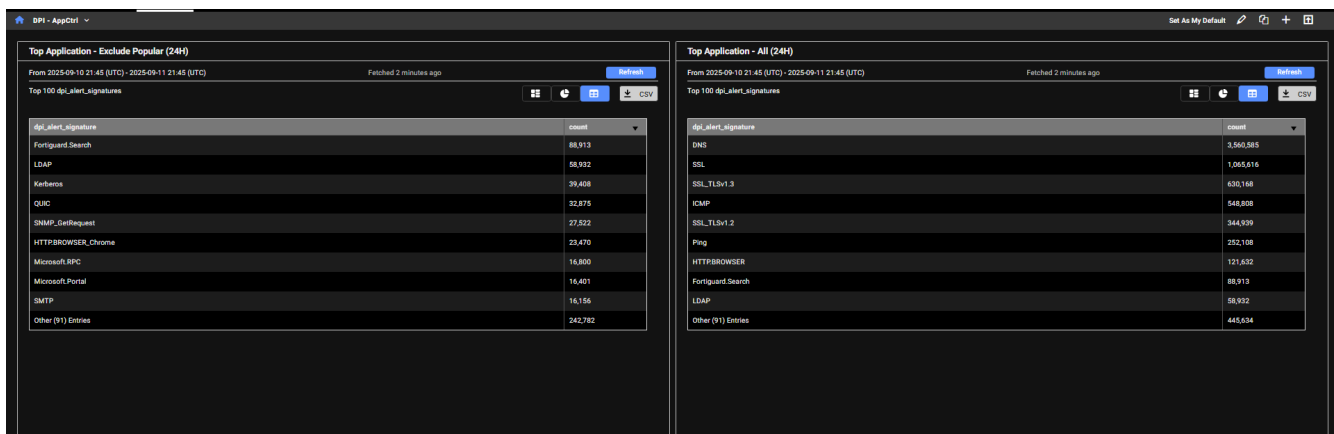
The *DPI - AppCtrl* dashboard displays detections of applications and protocols used by IP addresses, such as DNS, HTTP, and other common services. This provides insight into the types and volume of traffic an IP address is generating.

Top Application - Exclude Popular (24H)

This monitor filters out common or expected traffic (such as DNS, ICMP, ping, and browser activity) to highlight less typical application usage. The results are grouped by application signature, helping identify less common or potentially suspicious applications being used internally

Top Application - All (24H)

This monitor includes all detected application types, including browser activity, offering a complete view of application traffic. The results are grouped by application signature, allowing you to see which applications are being detected across internal traffic, without the noise from automated scanners. This helps focus on legitimate or potentially suspicious application usage within the network.



DPI - OT

The *DPI - OT* dashboard provides visibility into OT (Operational Technology) protocols used in industrial control systems. Any OT-related activity detected on the network will be tracked and displayed here. The dashboard highlights specific OT protocols (such as Bacnet, Profinet, and DNP3) with MP3 being one of the more commonly observed.

OT Protocol

This monitor displays DPI alerts categorized as *OT - Protocol*, which relate to industrial control system protocols, where either the source or destination IP is internal. It excludes alerts triggered by device tagged as *Scan* and *Nessus*.

The results are grouped by both the OT protocol signature and the source IP, allowing you to:

- See which internal IPs are generating OT protocol traffic.
- Identify which specific OT protocols are being used or triggered by each IP.

This helps in monitoring legitimate OT activity and detecting unusual or unauthorized use of industrial protocols.

OT Threats

This monitor displays DPI alerts categorized as *OT - Threats*, which indicate suspicious or malicious activity targeting Operational Technology (OT) systems. It filters for alerts where either the source or destination IP is internal and excludes alerts triggered by device tagged as *Scan* and *Nessus*.

The results are grouped by both the OT threat signature and the source IP, allowing you to:

- Identify which internal IPs are involved in OT-related threat activity.
- See which specific OT threat types are being detected per IP.

This helps in monitoring and investigating potential compromises or unauthorized access attempts within industrial environments.

The screenshot displays the FortiNDR Cloud DPI - OT dashboard. It features two main panels: 'OT - Protocol (7 days)' and 'OT - Threats (7 days)'. Both panels show data from 2025-09-04 21:45 (UTC) to 2025-09-11 21:45 (UTC), fetched 4 minutes ago. The 'OT - Protocol' panel lists the top 46 dpl_alert_signatures and src_ips, with a table showing details for the top 10. The 'OT - Threats' panel lists the top 1 dpl_alert_signatures and src_ips, with a table showing details for the top 1.

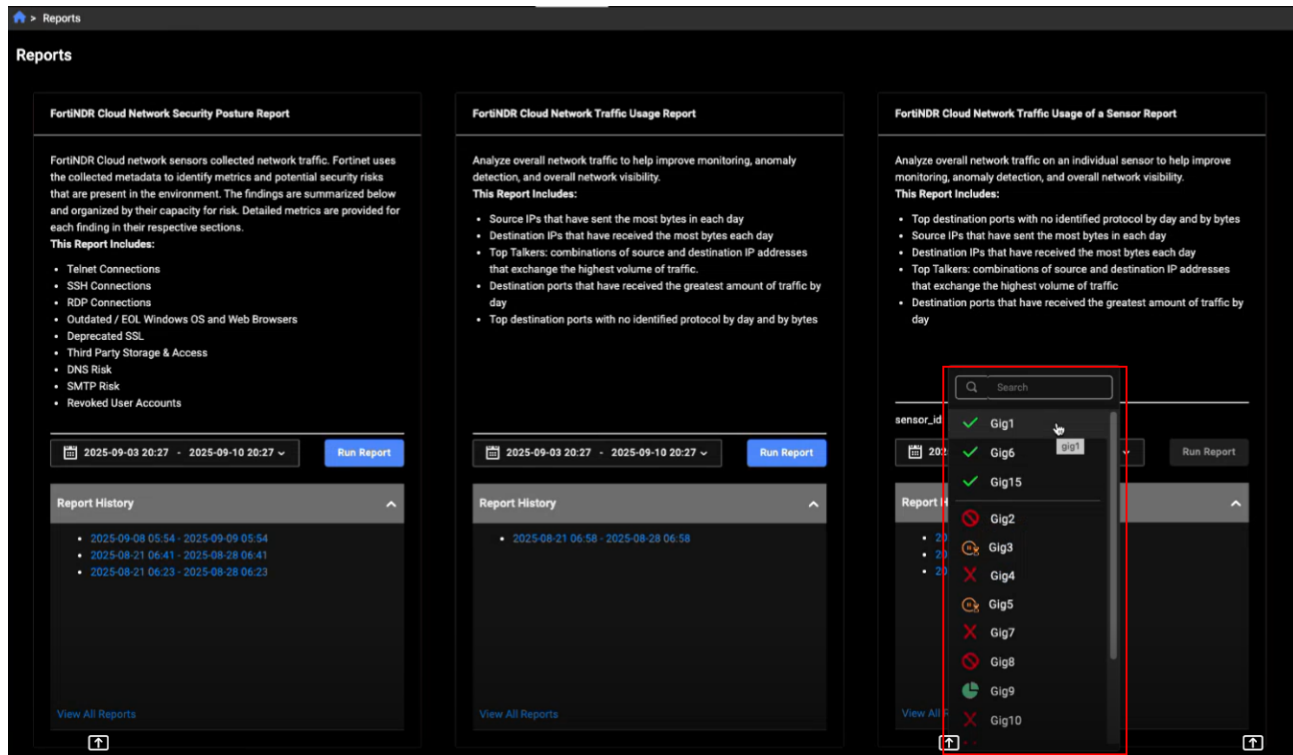
dpl_alert_signature	src_ip	count
BACnet_Read.Property.Multiple	172.30.232.252	910
BACnet_Complex.ACK	10.65.131.250	384
DF1_Set.Data.Table.Size	192.168.110.11	346
BACnet_Complex.ACK	10.65.8.51	298
BACnet_Complex.ACK	10.160.4.2	291
BACnet_Segment.ACK	172.30.232.252	223
DF1_Set.Data.Table.Size	10.10.246.24	37
DF1_Set.Data.Table.Size	192.168.110.38	32
IEC.60870.5.104_Exception.Invalid.Protocol	others	30
IEC.60870.5.104_Exception.Invalid.Protocol	192.168.110.32	21

dpl_alert_signature	src_ip	count
Siemens.SIMATIC.S7.Scanner	3.148.72.26	6

Improved functionality

Reports

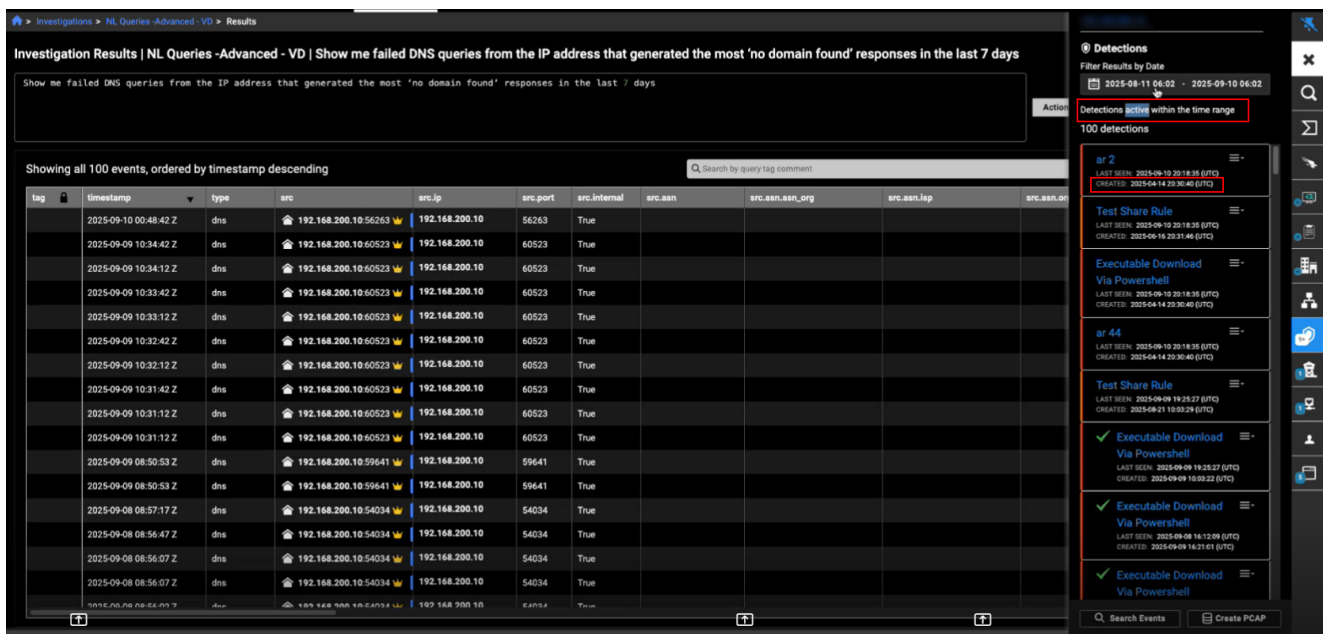
We've updated the *sensor_id* filter in the *FortiNDR Cloud Network Traffic Usage of a Sensor Report* and *Detections* list page to a dropdown menu that displays all sensors in the account. The dropdown is divided into two groups: online sensors appear at the top, while other statuses are listed below. Retrieving the list of sensors may take a few moments. During this time, a spinner will appear to indicate that the request is in progress.



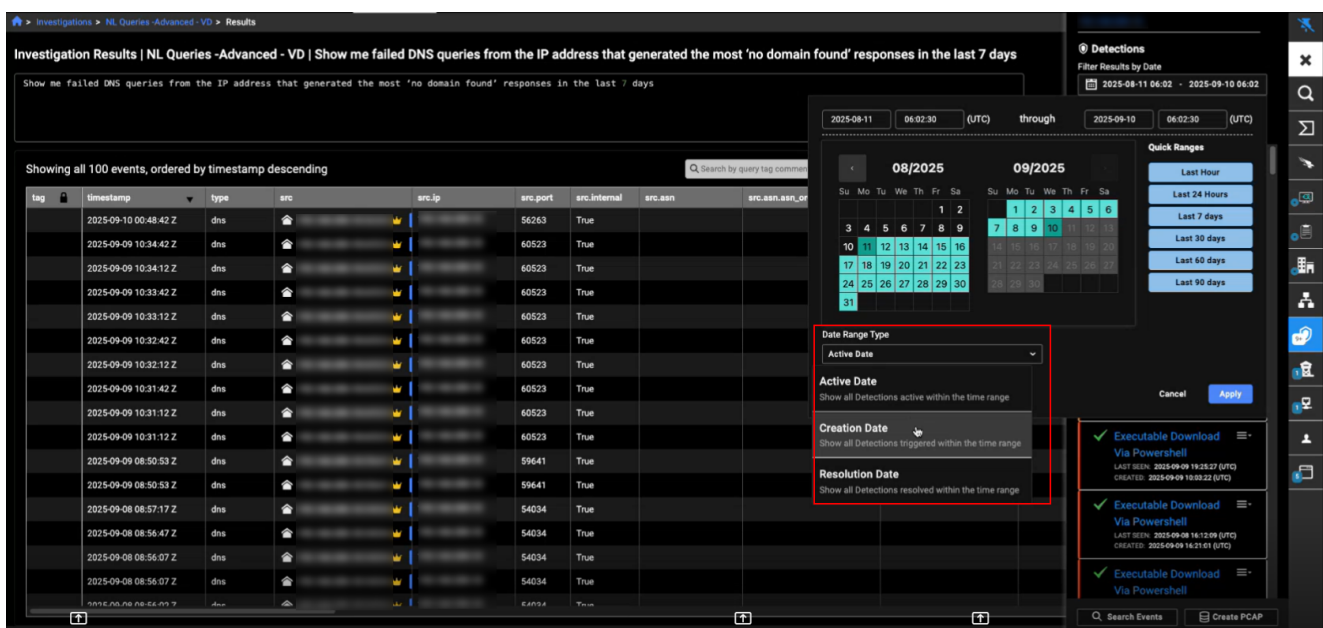
Entity panel

The *Detections* tab in the Entity Panel now displays the *Active* detections within the time range. In previous versions, it displayed detections triggered within the time range. In the detection details, we have replaced *Account* with the *Created* date.

Note that this update does not apply to the *Detections Table* page.



You can also choose the *Date Range Type* (Active Date, Creation Date, or Resolution Date) when selecting the time range in the date picker. This update is applied to *Entity Panel* throughout the portal.



Other improvements

- This release includes internal hardening updates to improve system security and resilience.

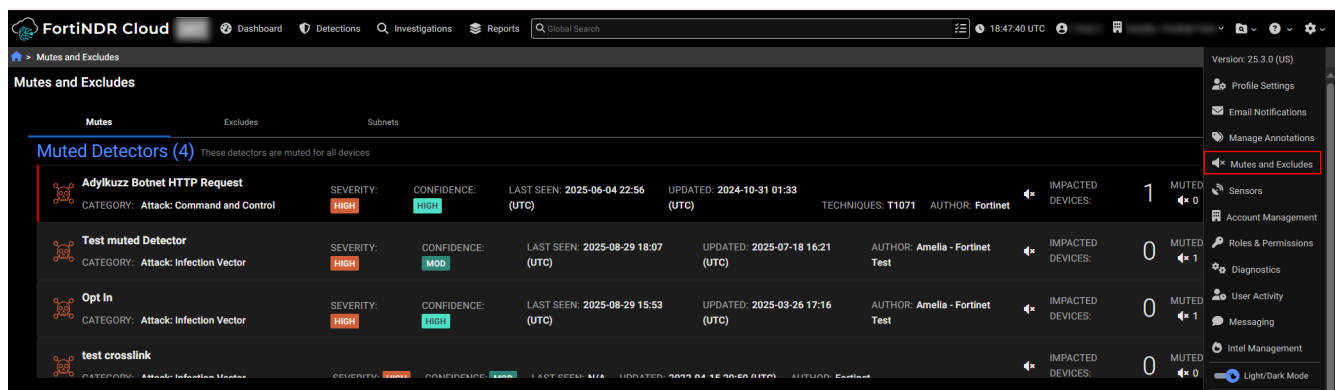
Version 25.3.b

- New functionality on page 28
 - Mutes and Excludes page on page 28
 - Detections Device Timeline on page 30
 - NetFlow events on page 33
 - DPI events on page 34
- Improved functionality on page 35
 - Impacted device filter on page 35
 - Notification emails on page 35
 - Single Event View on page 36
 - Notable detections on page 37
 - Sensor details on page 37
 - Bulk subnet imports on page 38
 - Annotations on page 38
 - Shared dashboards on page 39
- Other improvements on page 39
 - Investigation Summary field on page 39
 - Data sources on page 39
 - Network Security Posture Report on page 40
- Deprecated features
- Resolved issues on page 87

New functionality

Mutes and Excludes page

A new *Mutes and Excludes* page has been added to the main settings menu. This page summarizes all muted and excluded devices, including device-level mutes for detectors. It contains three tabs: *Mutes*, *Excludes* and *Subnets*.



Mutes tab

The *Mutes* tab shows *Muted Detectors* (detectors that are muted); *Muted Devices* (Devices that have muted all detectors); *Muted Devices for Detectors* (Devices that are muted for specific detectors); and *Muted Detections* (The detection is muted or impacted device is muted for the whole account or for a specific detector).

You can use this table to add a muted device for the whole account, unmute or edit existing muted devices, add or update a muted device for a specific detector.

Mutes and Excludes

Muted Detectors (4) These detectors are muted for all devices

Detector	Category	Severity	Confidence	Last Seen	Updated	Techniques	Author	Impacted Devices	Muted	Actions
Adylkuzz Botnet HTTP Request	Attack: Command and Control	HIGH	HIGH	2025-06-04 22:56 (UTC)	2024-10-31 01:33 (UTC)	T1071	Fortinet	1	0	⋮
Test muted Detector	Attack: Infection Vector	HIGH	MOD	2025-08-27 20:34 (UTC)	2025-07-18 16:21 (UTC)		Amelia - Fortinet Test	0	1	⋮
Opt In	Attack: Infection Vector	HIGH	HIGH	2025-08-27 05:35 (UTC)	2025-03-26 17:16 (UTC)		Amelia - Fortinet Test	0	1	⋮
test crosslink	Attack: Infection Vector	HIGH	MOD	2025-08-27 05:35 (UTC)	2025-03-26 17:16 (UTC)		Amelia - Fortinet Test	0	0	⋮

Muted Devices (7) These devices are muted for all detectors

Add New Device/Range CSV

Device(s)	Description	Muted Date	Actions
8.8.8.8		2025-08-06 20:45:08 (UTC)	⋮
1.2.3.7		2025-08-06 20:44:20 (UTC)	⋮
1.2.3.0/24		2025-08-06 20:21:07 (UTC)	⋮
1.2.3.4		2025-08-06 19:59:56 (UTC)	⋮
9.8.7.6		2025-07-14 17:20:23 (UTC)	⋮
6.7.8.9		2025-07-14 17:20:13 (UTC)	⋮
172.19.241.21		2023-09-26 20:27:19 (UTC)	⋮

Excludes tab

This tab shows devices that are excluded at the account level, meaning no detections will be triggered for them. It also includes disabled detectors.

Mutes and Excludes

Excluded Devices (6) No detections will be triggered for these IP addresses as impacted devices

Exclude New Device CSV

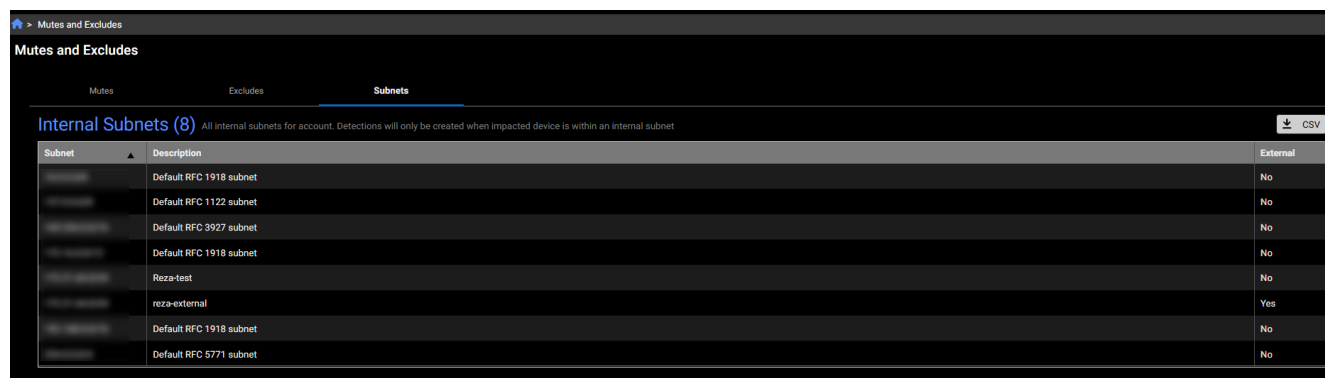
Device	Description	Actions
1.1.1.1		⋮
1.1.1.4		⋮
1.1.2.3		⋮
1.2.3.4		⋮
2.2.2.3		⋮
2.3.4.5		⋮

Disabled Detectors (4) No detections will be created for the following detectors. (Only detectors created on this account can be disabled)

Detector	Category	Severity	Confidence	Last Seen	Updated	Techniques	Author	Impacted Devices	Muted	Actions
	Attack: Infection Vector	MOD	MOD	N/A	2023-12-08 07:41 (UTC)	T1201/T1213.001	Fortinet	0	0	⋮
	Attack: Infection Vector	MOD	MOD	N/A	2023-12-07 22:28 (UTC)	T1056/T1056.004	Fortinet	0	0	⋮
	Miscellaneous	LOW	LOW	N/A	2018-03-30 17:18 (UTC)		Fortinet	0	0	⋮
	Attack: Infection Vector	LOW	LOW	N/A	2025-07-09 20:44 (UTC)			0	0	⋮

Subnets tab

This tab displays all internal subnets for the account. Detections will only be created when the impacted device is within an internal subnet



Subnet	Description	External
10.10.10.0/24	Default RFC 1918 subnet	No
10.10.10.0/24	Default RFC 1122 subnet	No
10.10.10.0/24	Default RFC 3927 subnet	No
10.10.10.0/24	Default RFC 1918 subnet	No
10.10.10.0/24	Reza-test	No
10.10.10.0/24	reza-external	Yes
10.10.10.0/24	Default RFC 1918 subnet	No
10.10.10.0/24	Default RFC 5771 subnet	No

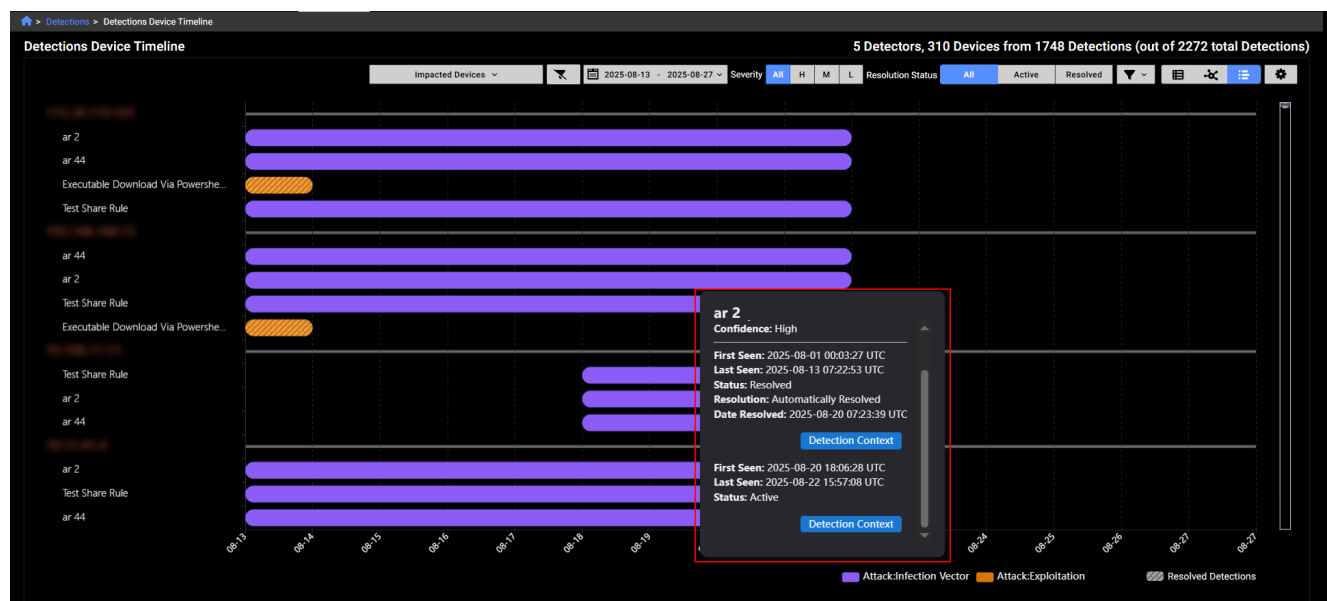
Detections Device Timeline

We have added a new view called *Detections Device Timeline* to *Detections*. This view shows all detections sorted by the device risk score.

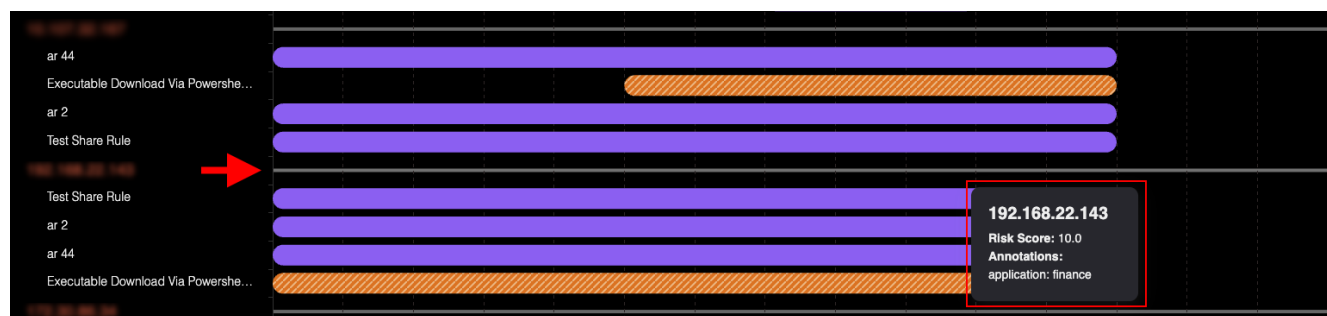


A solid background color in each bar on the chart represents a detection category, as indicated in the legend at the bottom of the page. If a bar is striped, it means all detections within that range have been resolved. Note that a single bar does not correspond to one detection; instead, it may represent multiple detections that occurred within the same time range.

Hover over a bar in the chart to view details about the detection. You can also click the *Detection Context* button to view the detections and observations related to this IP on the *Detection Context* page.



Hover over the line next to the IP label to view its risk score. Any annotations related to the IP will be displayed here



Left-click the IP label to open the *Entity Panel*.



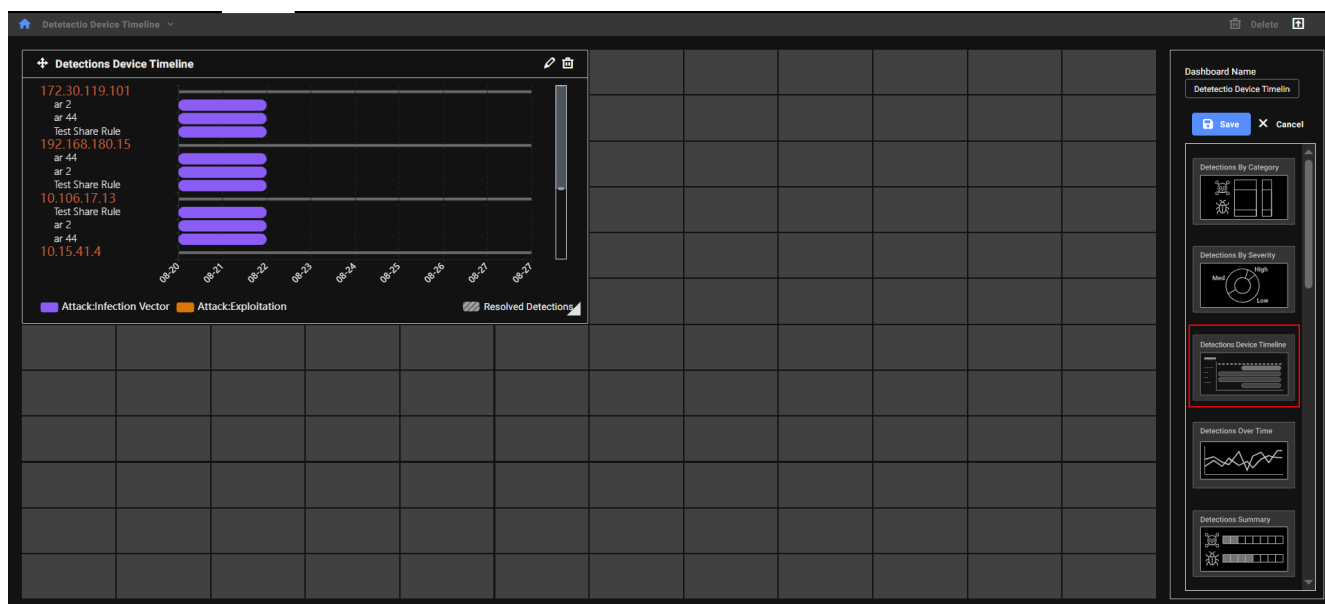
Right-click the IP label to open the context menu.



You can filter the view to hide detections that have no associated events during the selected time range. Use the toggles on the right side of the page to switch between the *Detections Table* and *Detections Visualizer* views. Both views also support the *Detections Device Timeline* toggle.



The *Detections Device Timeline* is available as a dedicated dashboard widget. By default, it displays the top five IPs with the highest risk scores from the past seven days. These settings are customizable.



NetFlow events

NetFlow event types are now supported in investigations. NetFlow traffic is processed using source and destination objects. The Entity Panel continues to treat this traffic as sensor data. If incoming NetFlow matches your sensor's configuration, it will be displayed accordingly.



- A NetFlow annual subscription license is required for FortiNDR Cloud to ingest third-party logs for anomaly detection.
- Only NetFlow-based botnet detections are currently displayed. Detections for spam, phishing, Tor, and proxy traffic are not available at this time. Additionally, an IOC (Indicator of Compromise) risk score may not be shown for every IP address.

Investigation Results | Phung (netflow) |

sensor_id = 'sctest288' group by event_type

Events grouped by event_type

Showing all 4802 events, ordered by timestamp descending

tag	type	timestamp	src	src_ip	dst	intel	source	proto	total_pkts
	netflow	2025-08-27 00:52:34 Z					NETFLOW	tcp	8
	netflow	2025-08-27 00:52:34 Z					NETFLOW	tcp	9
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1
	netflow	2025-08-27 00:52:33 Z					NETFLOW	udp	1

DPI events

Deep Packet Inspection (DPI) is now a supported event type. Unlike traditional stateful packet inspection, which only analyzes packet headers (e.g., source/destination IP and port), DPI examines both the header and the payload of each packet. This allows for deeper visibility into network traffic by inspecting a broader range of metadata and content. DPI events provide enhanced context for threat detection and investigation by capturing detailed packet-level data as it passes through network checkpoints.

DPI alerts classify network activity and threats into key categories. *AppID* identifies applications like DNS, P2P, and social media. *OT - Protocol* detects operational technology protocols, while *OT - Threats* flags malicious activity in OT environments. *Botnet* alerts track known botnets, and *IDS* covers intrusion detection signatures. Information includes general alerts such as insecure SSL configurations.

Query: `dpi:customer_id` string

☒ `dpi:dpi_alert_category`

☒ `dpi:dpi_alert_severity`

☒ `dpi:dpi_alert_signature`

☒ `dpi:dpi_alert_signature_id`

☒ `dpi:dpi_app_behavior`

☒ `dpi:dpi_app_category`

☒ `dpi:dpi_app_language`

☒ `dpi:dpi_app_name`

☒ `dpi:dpi_app_os`

☒ `dpi:dpi_app_technology`

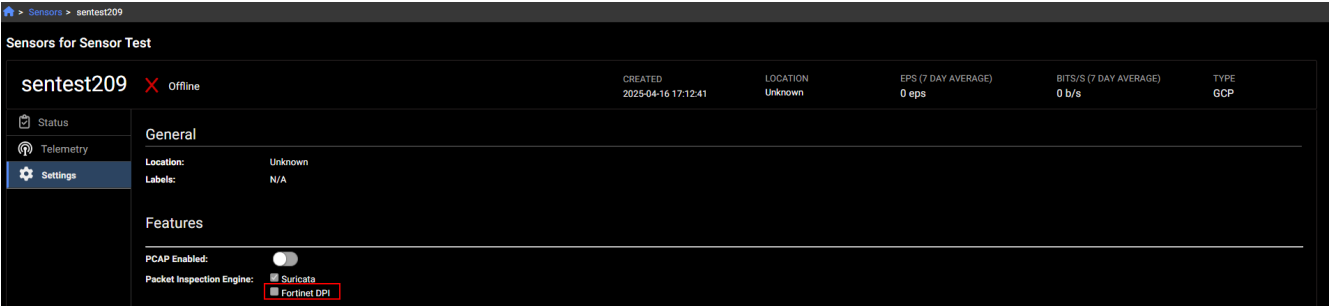
☒ `dpi:dpi_app_vendor`

Query: `dpi`

View Results 2025-05-31 17:08 (UTC) to 2025-08-29 17:08 (UTC) By: 100 Events

Sort by timestamp Descending Last 7 Days Retrieve up to 100 rows Enable Facets Cancel Add Query

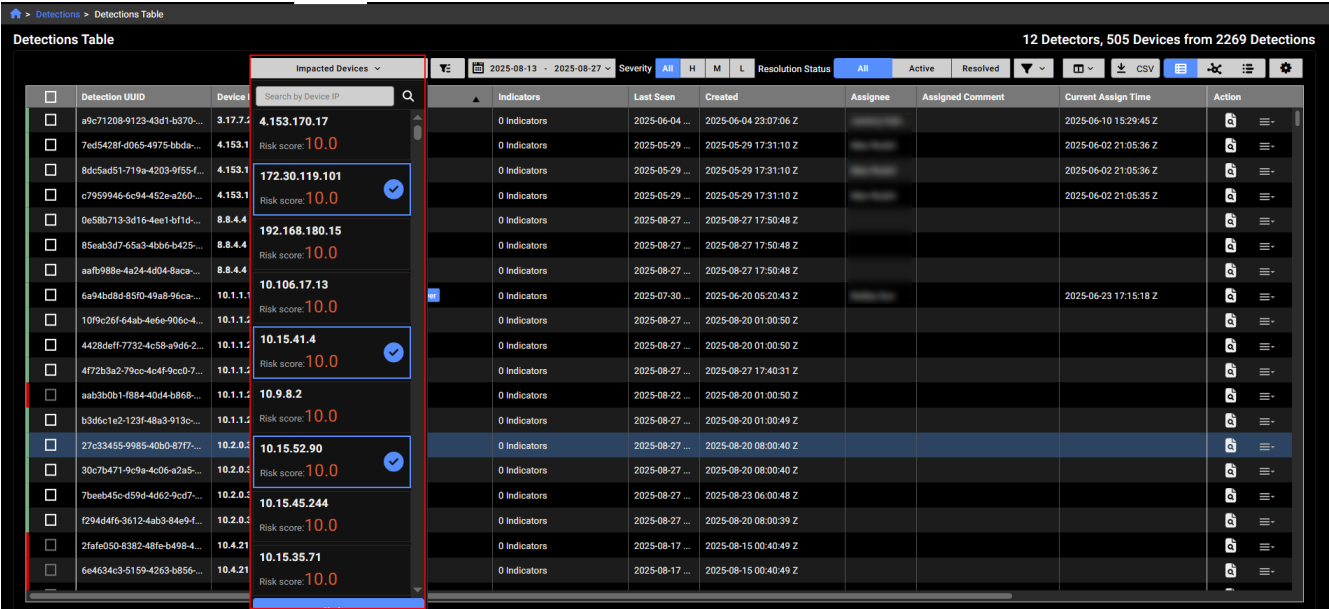
To enable DPI events, go to the sensor's *Settings* and select *Fortinet DPI*.



Improved functionality

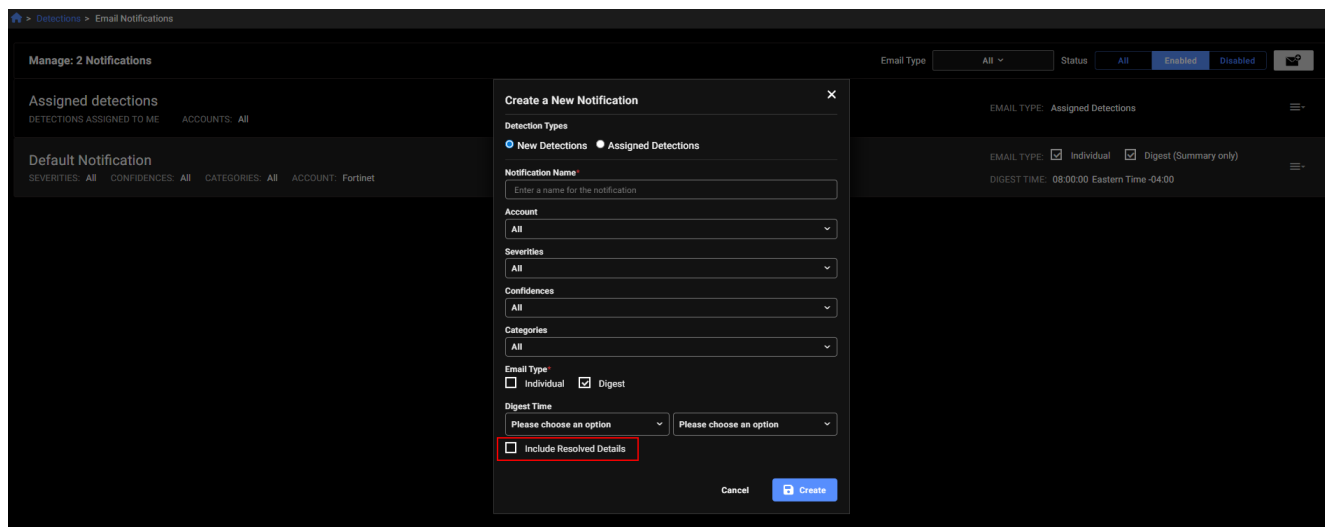
Impacted device filter

We have replaced the *Device IP* search box with a new filter called *Impacted Devices* in the *Detections Table*, *Detections Visualizer* and *Detection Device Timeline*. The IPs in the list are sorted by Risk Score. You can filter IPs with the search box and select the devices you want to include in the view.



Notification emails

The email notifications settings and page have been updated include resolved details in *Digest* emails.

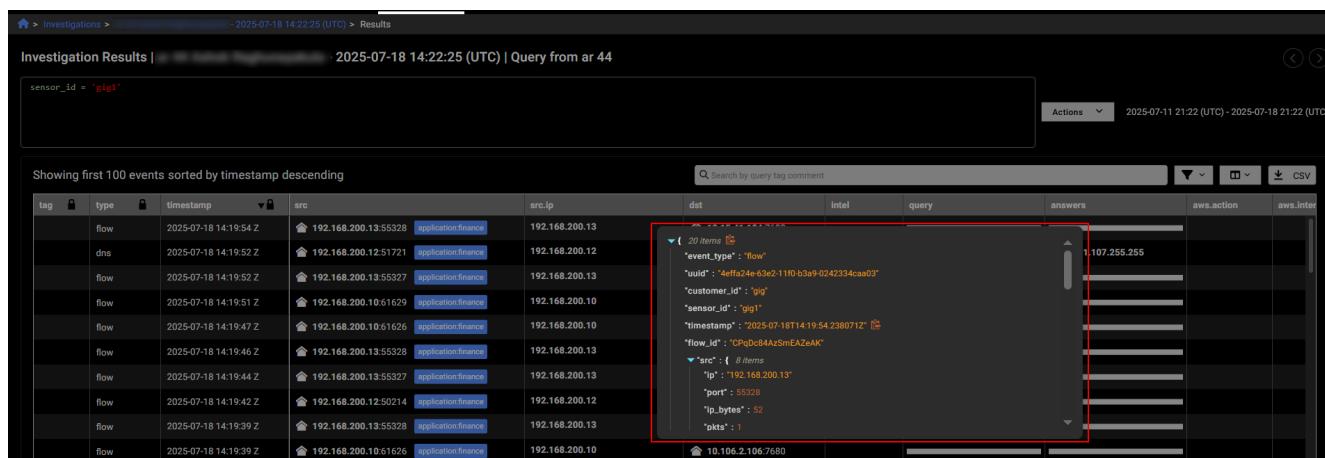


The *Email Notifications* page will display *Digest with Resolve Details* next to the email when this feature is enabled. This feature is in limited availability. If you would like it enabled please contact your TSM.



Single Event View

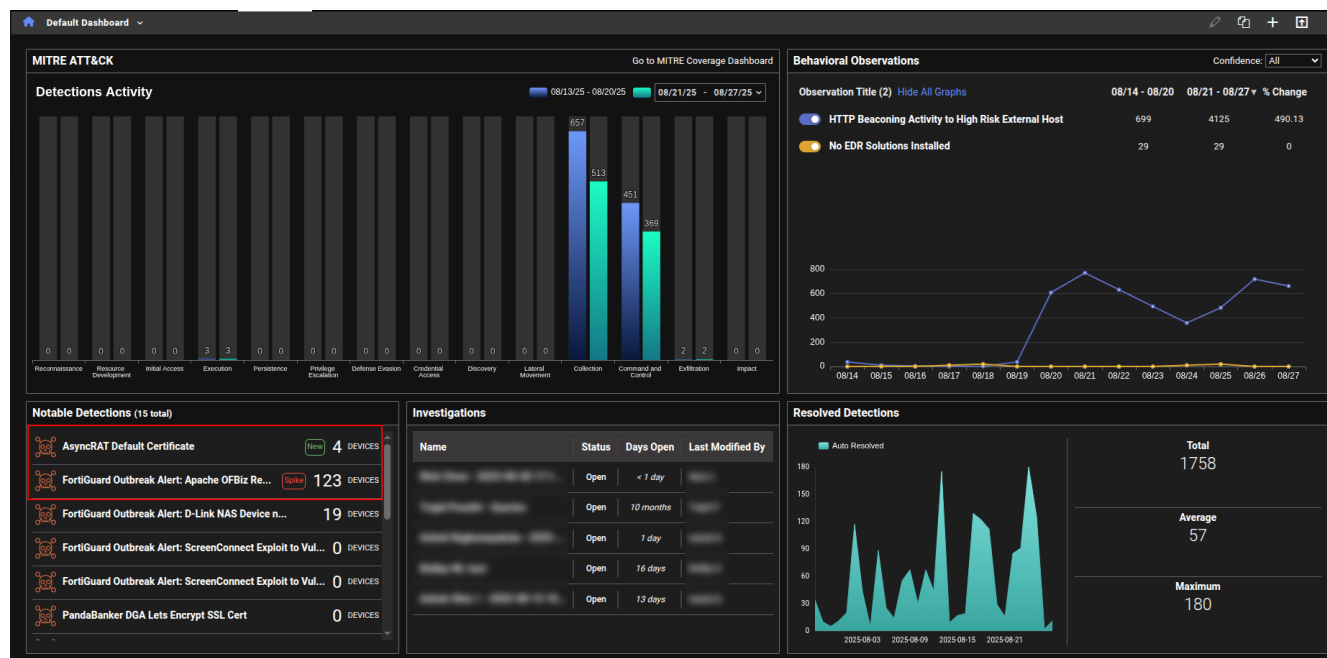
You can now view all details for a single event by double-clicking a blank area within the event row. This opens a pop-up displaying the full row data in JSON format. To copy the JSON, click the copy icon next to the first line. This feature saves time by eliminating the need to scroll through individual cells in the investigation results table.



Notable detections

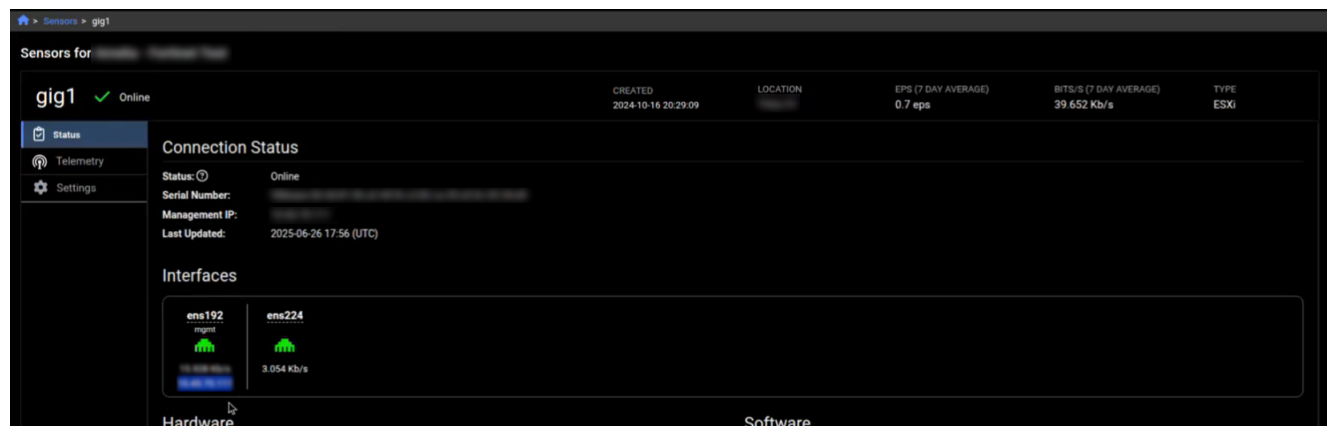
We have added labels to the *Notable Detections* table in the *Dashboard* to highlight new detections and spikes in detection activity.

- New* indicates that there were no active detections during the baseline period (defined as 30 to 7 days ago), but at least one detection has occurred in the past 7 days.
- Spike* indicates that the number of active detections in the past 7 days is more than three times higher than the baseline count.



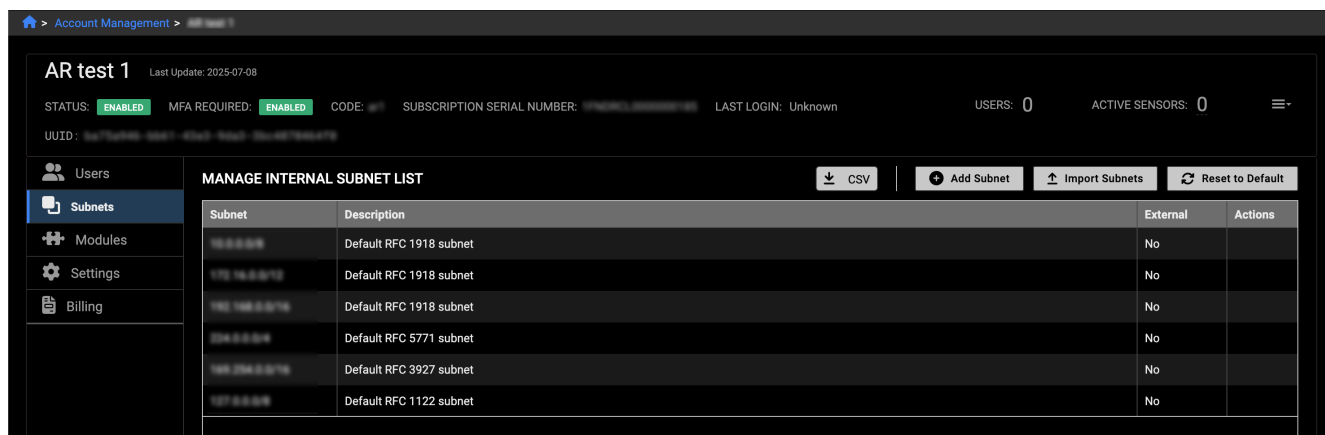
Sensor details

On the *Sensors* details page, each interface now displays its IP address—if that information is included in the API response. This is especially useful when the interface is configured as a NetFlow collector.



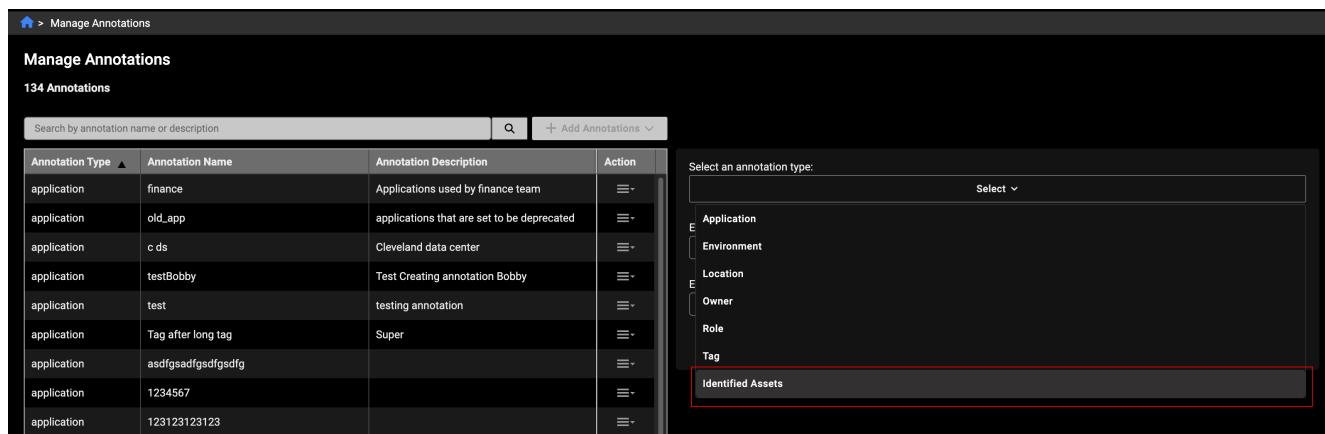
Bulk subnet imports

We have added a new *Import Subnets* button to the *Account Management > Subnets* tab. This allows you to upload thousands of subnets at once and delete them in bulk. Click the *CSV* button to download the current subnets, then add or remove entries and re-upload the file. You can also click the *Reset to Default* button to delete all subnets except the default.



Annotations

A new annotation type, *Identified Assets*, has been added for FortiGuard ATR. This allows assets to be tagged with priority levels—high, moderate, or low risk—which are then visible in the events and detections tables.



Assets marked as *identified* will display a crown icon, color-coded by priority: red for high, orange for moderate, and yellow for low.

Home > Detections > Detections Table

Detections Table 12 Detectors, 512 Devices from 2124 Detections

Impacted Devices 25 2025-08-14 - 2025-08-28 Severity All H M L Resolution Status All Active Resolved CSV

☐	Detection UUID	Device IP	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Indicators	Action
☐	a9c71208-9123-43d1-b370-...	3.17.7.232					25 Events	0 Indicators	
☐	7ed5428f-d065-4975-bbda-...	4.153.170.17					3 Events	0 Indicators	
☐	8dc5ad51-719a-4203-9f55-f...	4.153.170.17					3 Events	0 Indicators	
☐	c7959946-6c94-452e-a260-...	4.153.170.17					2 Events	0 Indicators	
☐	0e58b713-3d16-4ee1-bf1d-...	8.8.4.4					2 Events	0 Indicators	
☐	85eab3d7-65a3-4bb6-b425-...	8.8.4.4					2 Events	0 Indicators	
☐	aafb988e-4a24-4d04-8aca-...	8.8.4.4					2 Events	0 Indicators	
☐	6a94bd8d-85fd-49a8-96ca-...	10.1.1.1 Identified assets					24 Events	0 Indicators	
☐	10f9c26f-64ab-4e6e-906c-4...	10.1.1.2					1170 Events	0 Indicators	

Shared dashboards

In previous versions for FortiNDR Cloud when a user opened a shared dashboard containing query charts, the associated investigations and results were tied to the account that originally created the dashboard. In version 25.3.b, when a user opens a shared dashboard with query charts, a new investigation is now created in their own account. This ensures that:

- The query results shown are based on the current account's data, not the dashboard creator's.
- Clicking the chart title also opens the query inside the investigation specific to the current account.

When a user clones a dashboard that contains query charts, a new investigation is automatically created in the user's account for each query chart widget. This ensures that the cloned dashboard runs fresh queries and displays results based on the current account data. The investigation is independent of the original dashboard and tailored to the account.

Users with only the *Admin* role (and no additional roles like *User*) will not see dashboards that contain query charts. This ensures that only users with the appropriate permissions can access dashboards with query-based data.

Other improvements

Investigation Summary field

When a new investigation is created, the system now automatically adds a summary note at the top. This ensures the summary remains visible above any subsequent query entries, unlike regular notes which follow the timeline order.

Data sources

Previously, users could only view included and excluded data sources by going to the *Edit Detector* page. Now, this information is also visible in *View* mode under the *Query* tab, making it easier to access without needing to edit the detector.

Network Security Posture Report

A new query named *DNS over HTTPS(DoH) Usage* was added the *Network Security Posture Report*.

Deprecated features

The following dashboards, features and view have been deprecated in version 25.3.b

- Dashboards:
 - Example Hunt Dashboard 2
 - Security Posture - Deprecated SSL
 - Security Posture -DNS
 - Security Posture - Outdated / EOL software
 - Security Posture - SSH Connections
- Device tracking
- Triage devices

Version 25.3.a

FortiNDR Cloud 25.3.a includes bug fixes, but no new features. See [Resolved issues on page 87](#)

Version 25.3.0

- [Deprecation notice](#)
- [Other improvements](#)
- [Resolved issues on page 87](#)

Deprecation notice

Enriched object field types

The `asn.isp` and `asn.org` fields are no longer supported. Please use `asn.asn_org` or `asn.asn` fields instead. This change applies to all IP-related fields.

Other improvements

- The sensor filter on the *Triage Detection* page now remains active as you click through the detector rows. This allows you to apply the same filter to different detectors.
- The funnel icon shows when a filter has been changed from its default setting. If the funnel only has one filter, the number next to it will either show 1 (if the filter is changed) or nothing (if it's still set to default).
- The *Query Chart* widget has been re-sized to allow the graph to fit within the widget's view.

Version 25.2.c

- New functionality on page 41
 - [Automated integration response modules on page 41](#)
 - [Share detectors with other accounts on page 42](#)
 - [Network Traffic Usage reports on page 43](#)
 - [Query chart widget on page 44](#)
- Improved functionality on page 44
 - [Manage endpoints in the Entity Panel on page 44](#)
 - [Assigned detections notifications on page 46](#)
 - [Version 25.2.c on page 41](#)
 - [Sensor telemetry on page 49](#)
- Other improvements on page 47
 - [Event fields on page 47](#)
 - [Scrollable Account list on page 48](#)
 - [Network Traffic by Event Type widget improvements on page 48](#)
 - [Sensor telemetry legend on page 48](#)
 - [Intel hits dialog on page 50](#)
 - [Group Detections by sensor on page 50](#)
- Resolved issues

New functionality

Automated integration response modules

Automated integration response modules are added for FortiEDR and CrowdStrike Falcon EDR. Only a single integration can be set to *Auto-Remediate* at a time; others may be configured, but must be set up to respond manually.

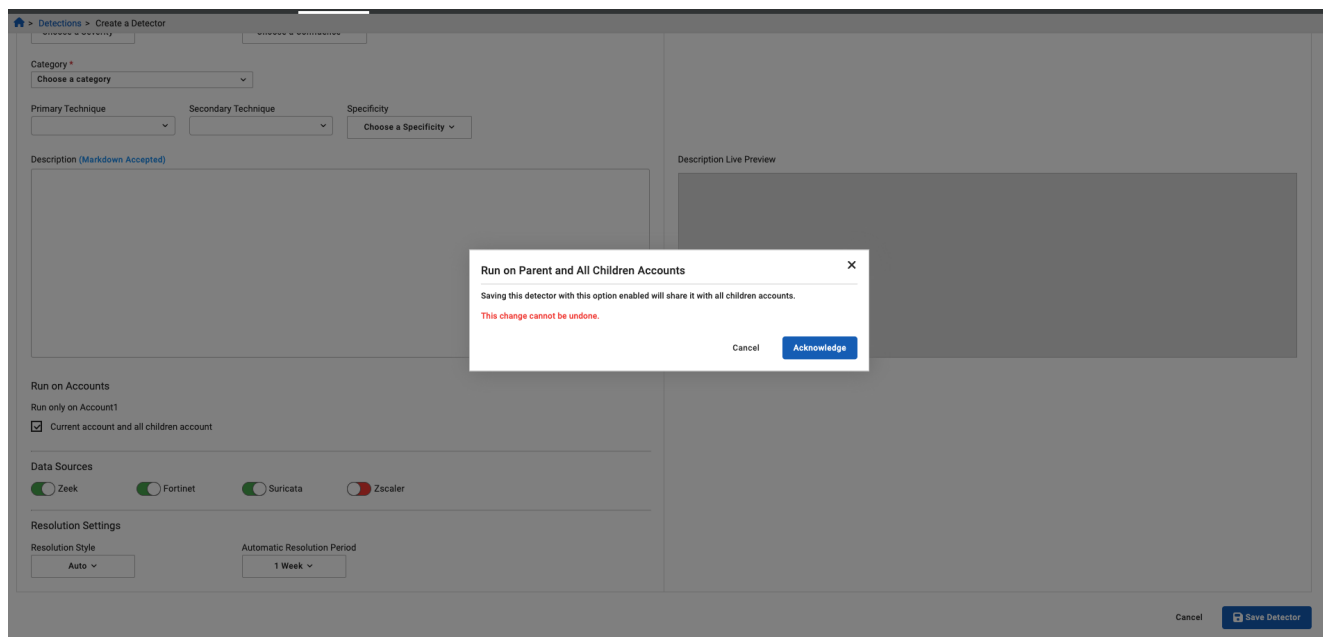
Integration Response Configuration			X
Integrations	Response		Action
CrowdStrike Falcon EDR	Manual Response		<button>Edit</button>
FortiEDR	Automatically ban IP address when a high-severity/high-confidence detection occurs		<button>Edit</button>
FortiGate via FortiManager	Manual Response		<button>Edit</button>
			<button>Done</button>

Integrations can also be configured from the *Account Management > <account> > Modules* page.

Share detectors with other accounts

When creating a detector on a parent account, you have the option to run the detector on the current account and child accounts by enabling the *Current account and all children account* option. Note that this cannot be undone.

On a child account, when you create a detector, it can run on the current account or it can be moved to the parent account and run on the parent and all children accounts. Note that this selection also cannot be undone.

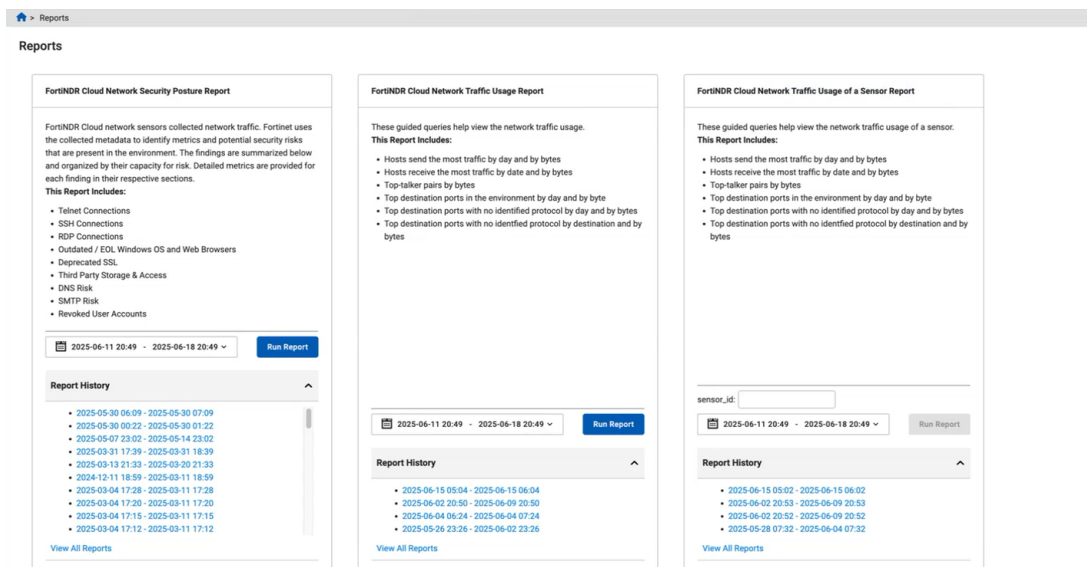


Network Traffic Usage reports

Two new reports are added for network traffic usage of an account and network traffic usage of a specific sensor over the past billing cycle (by default).

The reports include:

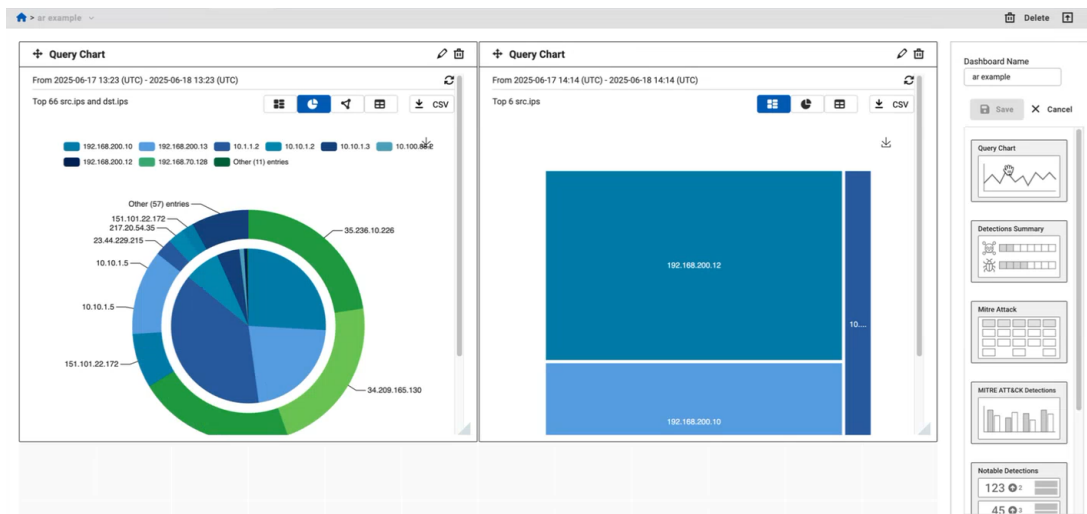
- Hosts send the most traffic by day and by bytes
- Hosts receive the most traffic by date and by bytes
- Top-talker pairs by bytes
- Top destination ports in my environment by day and by bytes
- Top destination ports with no identified protocol by day and by bytes



Query chart widget

A *Query Chart* widget can be added to the dashboard. Saved group by queries from the investigations can be added to the widget, the time range can be selected, and the widget can be given a custom *Name*. Different types of charts or a table can be selected to display the data, and a CSV file can be downloaded. The refresh button must be clicked to refresh the data.

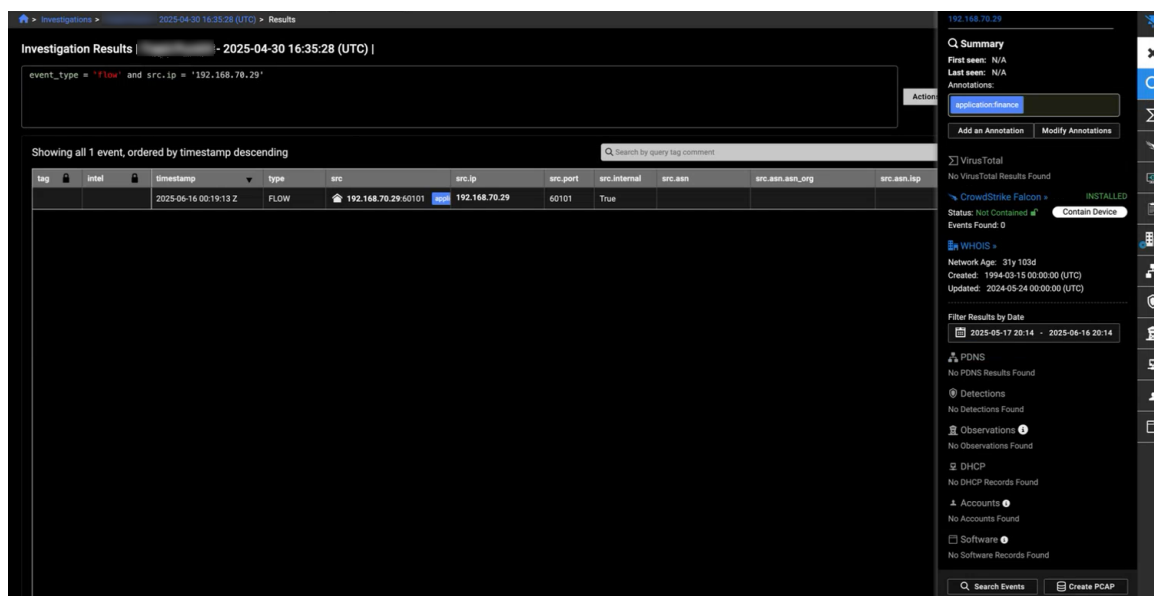
Click on the widget title to go the underlying query object and view the particular events for that investigation.



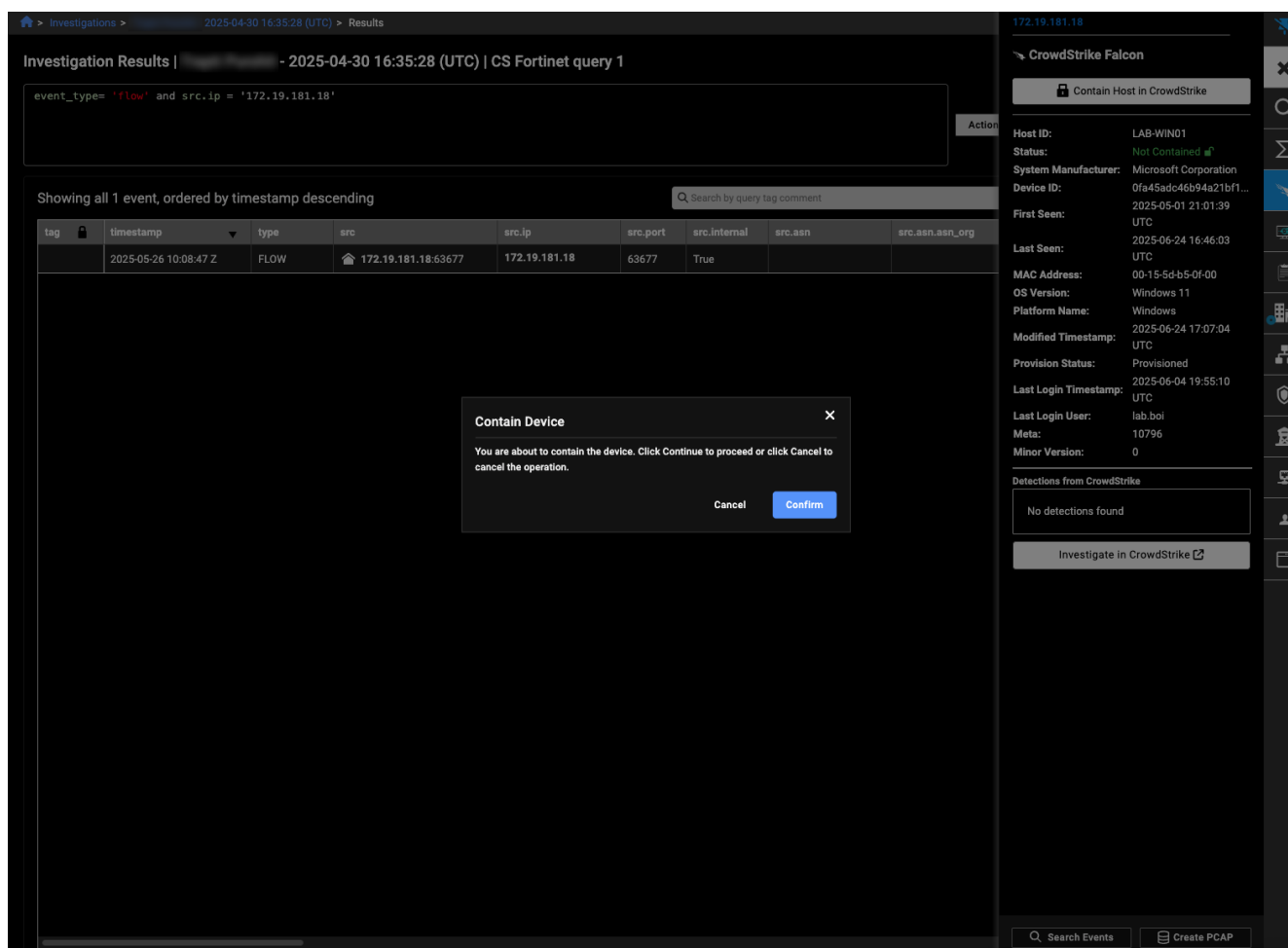
Improved functionality

Manage endpoints in the Entity Panel

The entity panel shows the current status of the device, and includes a button to contain, isolate, or ban the endpoint.



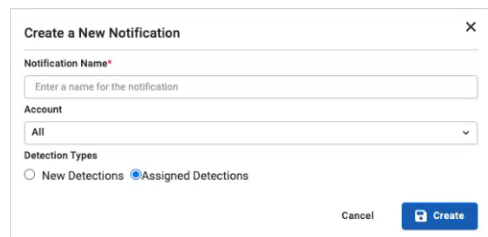
The button on the device panel is also moved to the top of the panel, and a confirmation box is shown when containing, isolating, or banning the endpoint.



Assigned detections notifications

The *Detections > Email Notifications* page is a single, scrollable list, without the need to select how many rows are shown.

When adding a new notification, you can choose to add a *New Detections* or *Assigned Detections*.



Create a New Notification [X]

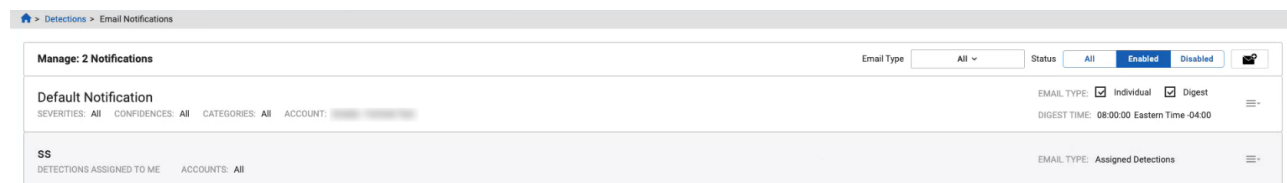
Notification Name*
Enter a name for the notification

Account
All

Detection Types
☐ New Detections
 ☒ Assigned Detections

Cancel **Create**

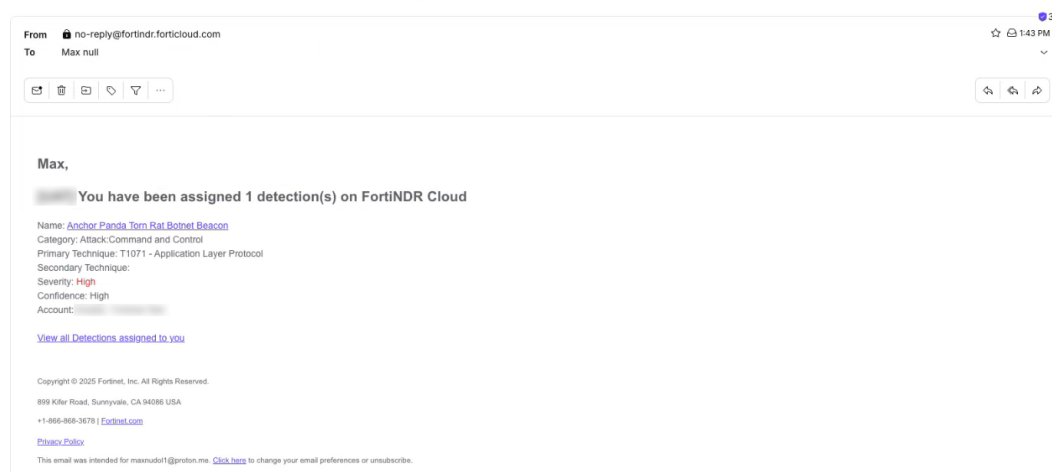
New Detections is the current functionality. When *Assigned Detections* is selected, an email notification will be sent to the user that it is assigned to and they will see the detection as *Assigned to me*.



Manage: 2 Notifications		Email Type	All	Status	All	Enabled	Disabled	
Default Notification SEVERITIES: All CONFIDENCES: All CATEGORIES: All ACCOUNT: [redacted] EMAIL TYPE: ☒ Individual ☒ Digest DIGEST TIME: 08:00:00 Eastern Time -04:00								
SS DETECTIONS ASSIGNED TO ME ACCOUNTS: All EMAIL TYPE: Assigned Detections								

When a detection is assigned to you, or you assign one to yourself, you receive an email to let you know that the detection has been assigned.

Detection Anchor Panda Torn Rat Botnet Beacon has been assigned at 2025-06-18T20:43:36.605688Z



Clicking the detector name link in the email takes you to that detector's page.

Version history

The screenshot shows the 'Anchor Panda Torn Rat Botnet Beacon' detection page. It includes a breadcrumb trail 'Detections > Anchor Panda Torn Rat Botnet Beacon'. The page header shows 'SEVERITY: HIGH' and 'CONFIDENCE: HIGH'. The main content area displays the category 'Attack Command and Control', first seen '2025-01-29 19:31 (UTC)', last seen '2025-06-04 22:56 (UTC)', updated '2024-10-29 20:20 (UTC)', query updated 'N/A', and resolution method 'Automatic - After 3 weeks'. A 'DEVICES IMPACTED' section shows a count of 1. Below this is a 'Start Investigation' button and a table of impacted devices. The table has columns for Device IP, DHCP Hostname, Username, Hostname, MAC Address, Lifetime Events, Indicators, First Seen, Last Seen, Created, Updated, and Action. One device is listed: 10.220.1.23 with 4 events and 1 indicator.

Clicking the *View all Detections assigned to you* link in the email will take you to the *Detections Table* page, showing all of the detections that you have been assigned.

The screenshot shows the 'Detections Table' page. It includes a breadcrumb trail 'Detections > Detections Table'. The page header shows '2 Detectors, 5 Devices from 5 Detections'. The main content area is a table with columns for Device IP, Name, and Action. The table lists five detections, all of which are 'AsymRAT Default Certificate' events. The first four are associated with the device 10.10.1.110, and the fifth is associated with 10.220.1.23. The table also includes a 'Device IP to search' field and a 'Search' button.

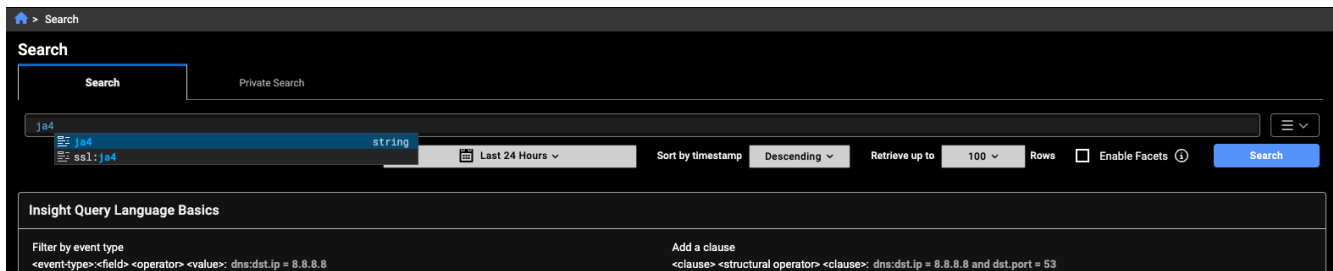
Other improvements

Event fields

You can now query *QUIC* events.

The screenshot shows the 'Search' page in the FortiNDR Cloud interface. It includes a breadcrumb trail 'Search'. The page has a 'Search' button and a 'Private Search' button. A search bar contains the query 'quic'. Below the search bar is a dropdown menu with suggestions for 'quic:dst.ip', 'quic:dst.port', 'quic:flow_id', 'quic:quic_client_initial_dst_conn_id', 'quic:quic_client_protocol', 'quic:quic_client_src_conn_id', 'quic:quic_history', 'quic:quic_server_src_conn_id', 'quic:quic_version', 'quic:server_name_indication', 'quic:src.ip', and 'quic:src.port'. The 'quic:src.ip' field is highlighted. The page also includes a 'Filter' section with a 'Filter by query.domain' button. The 'Add a clause' section shows a clause: '<clause> <structural operator> <clause>: dns:dst.ip = 8.8.8.8 and dst.port = 53'. The page has a 'Flow Examples' button and a 'DNS Examples' button.

The *ja4* field has been added to *SSL* events.

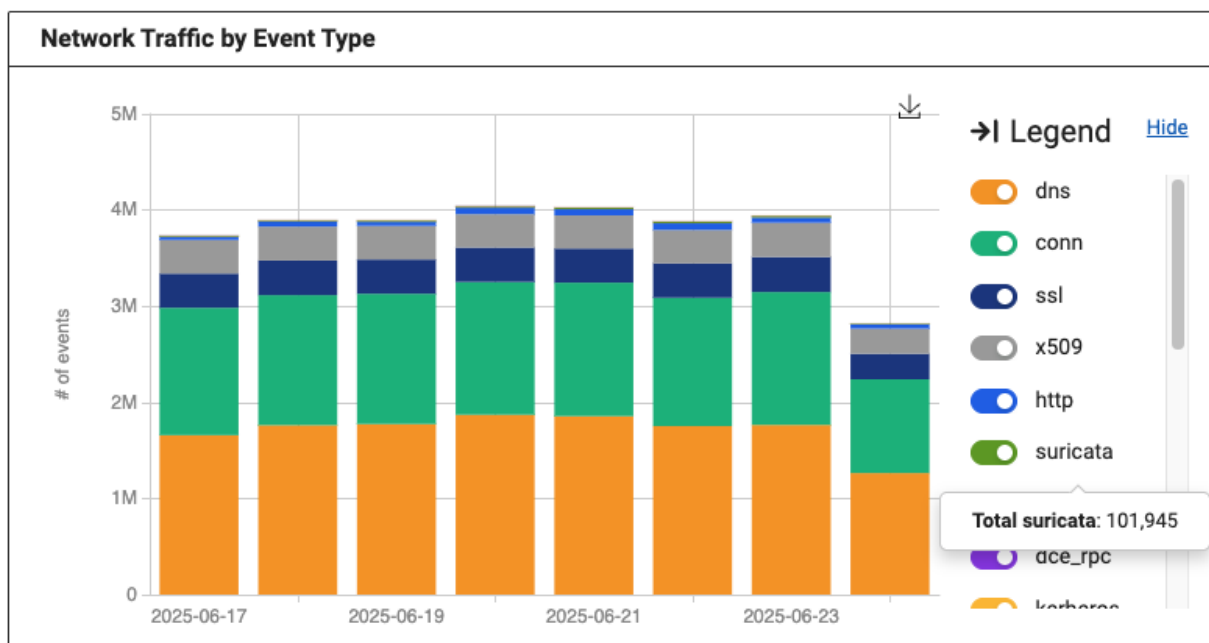


Scrollable Account list

On the *Account Management* page, the account list is shown as a single, scrollable list, without the need to select how many rows that are shown.

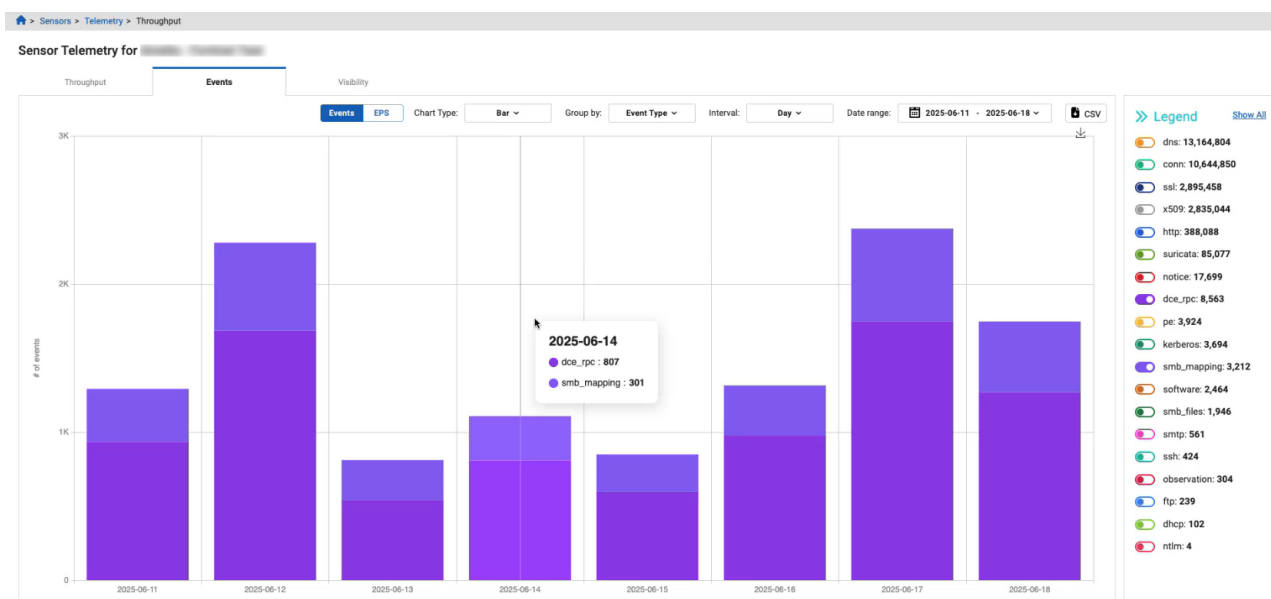
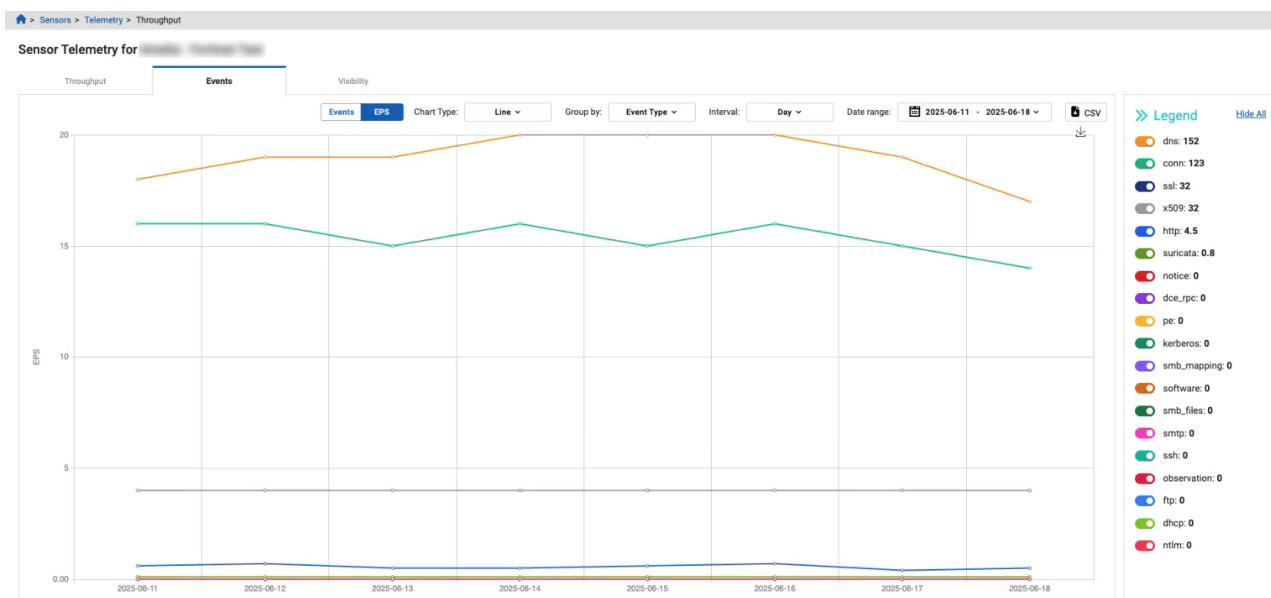
Network Traffic by Event Type widget improvements

The *Network Traffic by Event Type* widget includes a selectable legend with multiple colors to make it easy to differentiate between the event types.



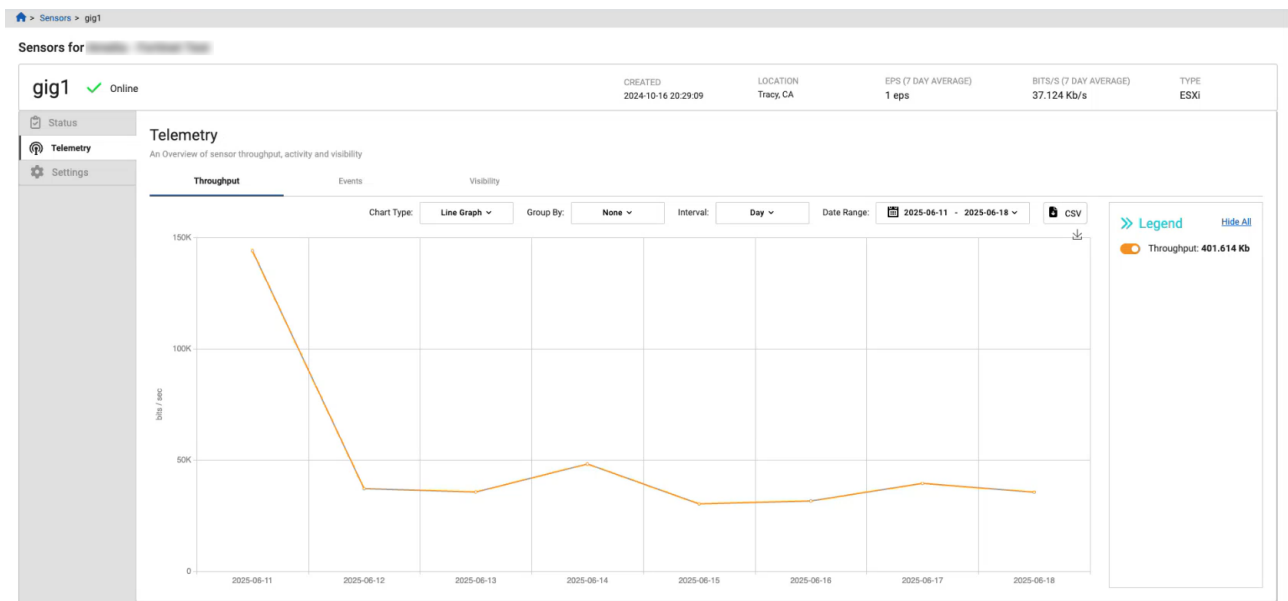
Sensor telemetry legend

The legend has multiple colors to make it easy to differentiate between the event types, and the event types stay in the same order when switching between *Events* and *EPS* views.



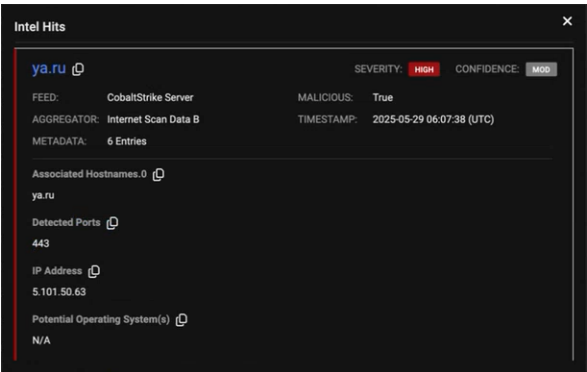
Sensor telemetry

You can now download the data in the *Sensors* detail page as a CSV file. The CSV file will download everything in the graph. You can use the legend to select the sensor data that you want to download.



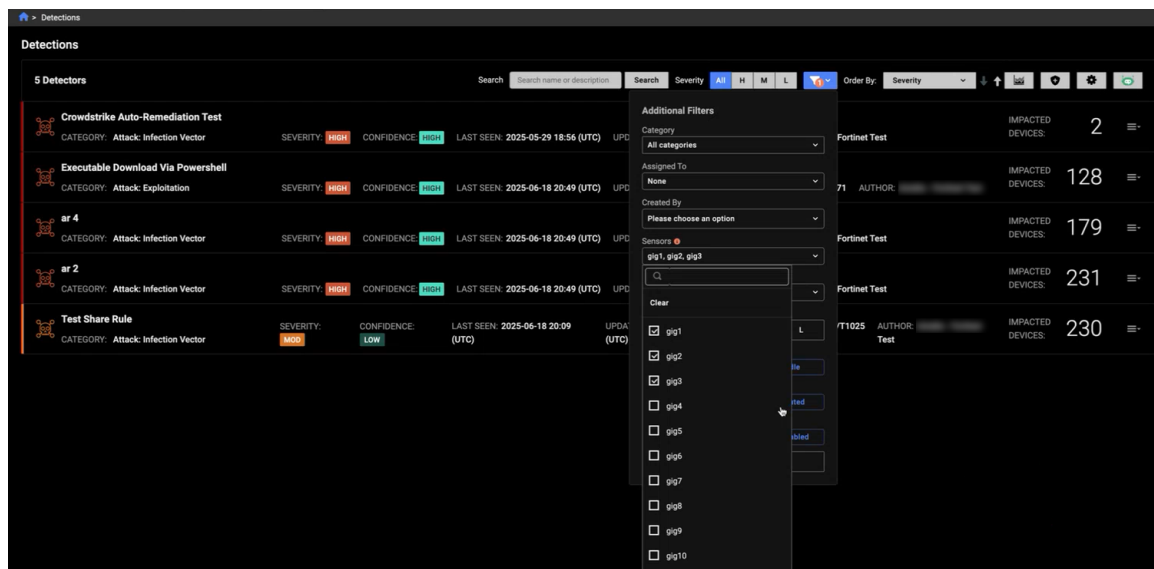
Intel hits dialog

The general fields and additional information are separated into two sections. Clicking the indicator in the title will open the *Entity Panel*.



Group Detections by sensor

A new filter is added to the *Detections* page, allowing multiple sensors to be selected.



The new filter is also added to the *Triage Detections* and *Detections Table* pages.

Note that observations will only identify a single sensor even if activity from multiple sensors was taken into account in producing the observation.

Version 25.2.b

- Improved functionality
 - Sensors
 - Telemetry
 - Throughput
 - Detection context
- Other improvements
- Resolved issues

Improved functionality

Sensors

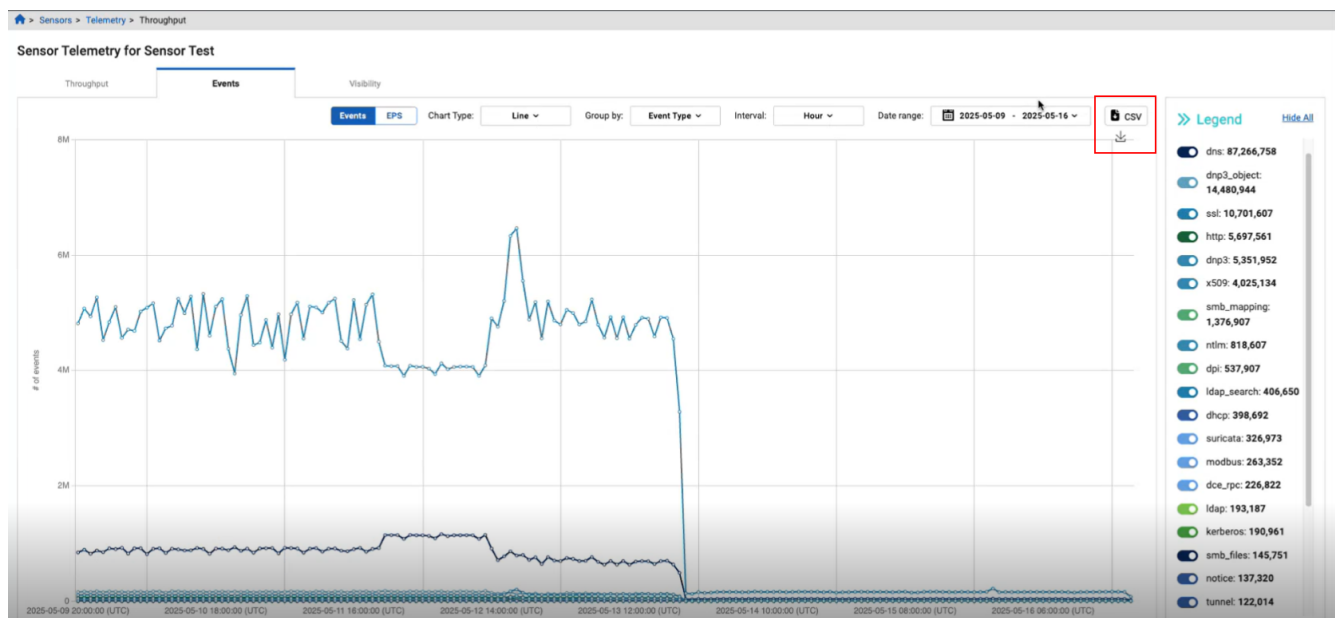
Telemetry

We have improved the performance and responsiveness in the *Telemetry* page. The *Telemetry Details* page now includes a legend that displays the total throughput count for each individual sensor.



Throughput

You can now download the data in the *Sensors > Telemetry > Throughput* page as a CSV file. The CSV file will download everything in the graph. You can use the legend to select the sensor data you want to download.



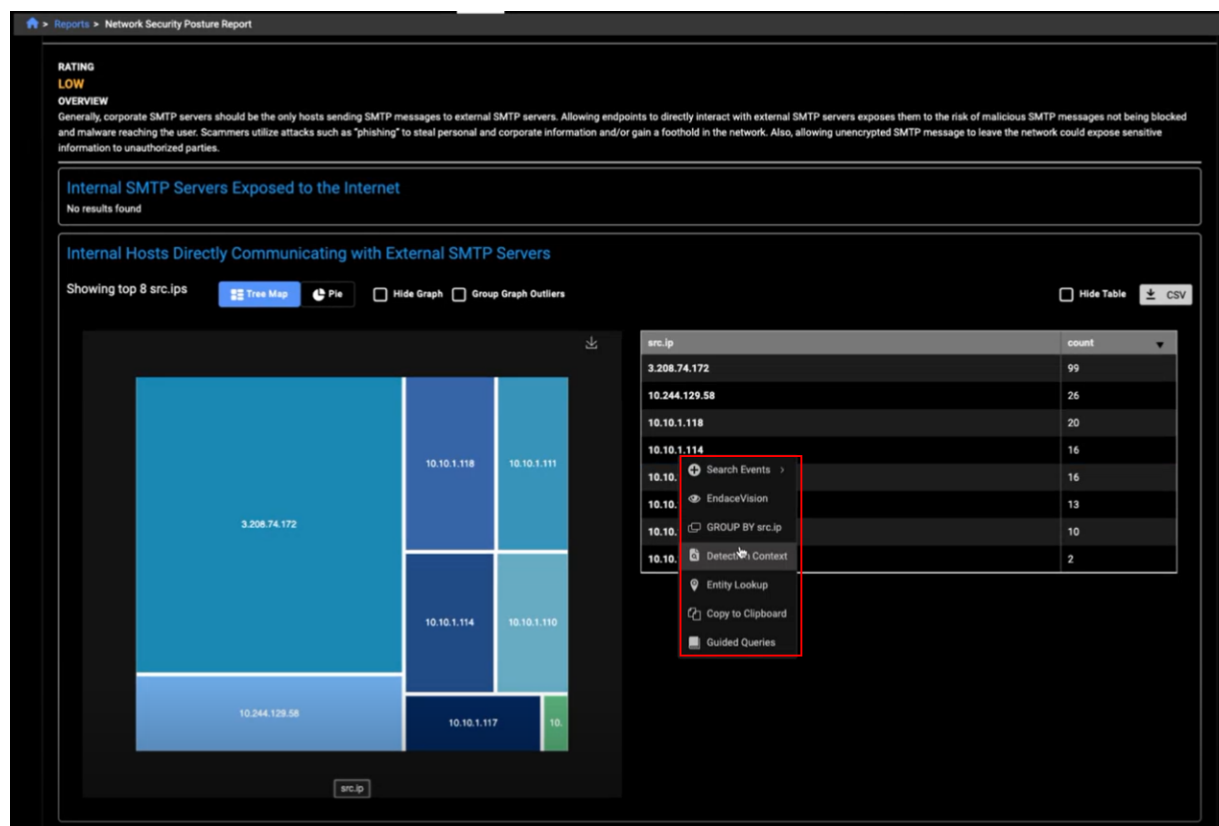
	A	B	C	D	E	F	G	H	I	J	
1	Timestamp (UTC)	conn (EPS)	dce_rpc (EPS)	dhcp (EPS)	dnp3 (EPS)	dnp3_control (EPS)	dnp3_object (EPS)	dns (EPS)	dpi (EPS)	http (EPS)	kerb
2	2025-05-09 20:00:00	1336	0.6	1	16	0.2	43	234	1	16	
3	2025-05-09 21:00:00	1409	0.6	1	17	0.2	46	247	1	16	
4	2025-05-09 22:00:00	1370	0.6	1	16	0.2	43	228	1	16	
5	2025-05-09 23:00:00	1462	0.6	1	17	0.2	47	243	1	17	
6	2025-05-10 00:00:00	1256	0.6	1	15	0.1	42	235	1	15	
7	2025-05-10 01:00:00	1343	0.6	0.9	17	0.2	46	254	0.8	16	
8	2025-05-10 02:00:00	1416	0.6	0.9	16	0.2	45	250	0.8	17	
9	2025-05-10 03:00:00	1267	0.6	0.9	16	0.2	44	256	0.8	15	
10	2025-05-10 04:00:00	1307	0.6	0.9	15	0.1	42	229	0.8	16	
11	2025-05-10 05:00:00	1301	0.6	0.9	17	0.2	45	253	0.8	16	
12	2025-05-10 06:00:00	1395	0.6	0.9	17	0.2	45	254	0.8	16	
13	2025-05-10 07:00:00	1412	0.6	0.9	15	0.2	43	226	0.8	17	
14	2025-05-10 08:00:00	1434	0.6	0.9	17	0.2	46	252	0.8	17	
15	2025-05-10 09:00:00	1254	0.6	0.9	17	0.2	46	254	0.8	15	
16	2025-05-10 10:00:00	1313	0.6	0.9	15	0.2	41	231	0.8	16	
17	2025-05-10 11:00:00	1326	0.6	0.9	17	0.2	46	252	0.8	16	
18	2025-05-10 12:00:00	1455	0.6	0.9	17	0.2	46	249	0.8	17	
19	2025-05-10 13:00:00	1386	0.6	0.9	16	0.2	45	244	0.8	16	
20	2025-05-10 14:00:00	1466	0.6	0.9	16	0.2	43	244	0.8	17	
21	2025-05-10 15:00:00	1212	0.6	0.9	16	0.1	45	255	0.8	15	
22	2025-05-10 16:00:00	1479	0.6	0.9	17	0.2	45	250	0.8	17	
23	2025-05-10 17:00:00	1278	0.6	0.9	15	0.1	42	228	0.8	16	
24	2025-05-10 18:00:00	1417	0.6	0.9	17	0.2	45	253	0.8	17	
25	2025-05-10 19:00:00	1453	0.6	0.9	17	0.2	46	253	0.8	17	
26	2025-05-10 20:00:00	1215	0.6	0.9	16	0.1	44	244	0.8	15	
27	2025-05-10 21:00:00	1095	0.7	0.9	16	0.1	45	259	0.8	14	
28	2025-05-10 22:00:00	1377	0.6	0.9	16	0.2	43	242	0.8	17	
29	2025-05-10 23:00:00	1469	0.6	0.9	17	0.2	46	252	0.8	17	
30	2025-05-11 00:00:00	1232	0.6	0.9	15	0.1	42	233	0.8	15	
31	2025-05-11 01:00:00	1245	0.6	0.9	16	0.1	43	253	0.9	15	

Detection context

You can now pivot to the *Detection Context* page from any page that displays an IP address, this includes:

- The *Events table > Investigation* results page. Note that the page will not display a selected detection because you are pivoting from an event.
- The *Private Search* page.
- The *Triage Detection* page > *Events* tab.
- *Detections* details > *Lifetime Events* column.
- The *Behavioral Observations* details page
- The *Aggregation* table including the table in a report. Note that when you pivot from the Aggregation table in a report, the *Detection Context* page will always show the last 90 days.
- The *Entity lookup* table. This includes the *Entity Lookup* table in *Global Search* results.
- The *Manage Annotations* page. This is limited to valid IPs for the last 90 days.
- The *Entity Panel*. You can pivot to the *Detection Context* page when the Entity Panel title is an IP address.
- *Detections Table > Indicators* column.

Note that the *Detection Context* page will display a message indicating that there are no detections or observations when none are present.



Other improvements

- We have updated some of the names of the event fields in `ldap` and `ldap_search`.

Version 25.2.a

FortiNDR Cloud 25.2.a includes bug fixes, but no new features. See [Resolved issues on page 87](#).

Version 25.2.0

- New functionality
 - Detections table
 - Detection context

- Improved functionality
 - Sensor telemetry
 - Traffic by event type widget
 - Sensor telemetry page
 - IQL queries
 - Idap and Idap_search
- Other improvements
 - Local time
 - Performance improvements
- Resolved issues

New functionality

Detections table

Detection context

You can now view all the device detections that fall within a time range. In the *Detections* table, do one of the following:

- Right-click an IP that was last seen is within the last year and select *Detections Context*.
- Click the *Detections Context* icon in the *Actions* column.
- Click the *Actions* menu in the *Entity Panel* and select *Detections Context*.

Detection UUID	Device IP	Last Seen	Created	Assignee	Assigned Comment	Current Assign Time	Initial Assign Time	Action
04707e8e-4727-43a3-8292...	0.0.0.0	2025-05-08 ...	2025-05-06 23:30:38 Z					
4a8a16ea-82c3-4991-9351...	0.0.0.0	2025-05-08 ...	2025-05-07 21:40:47 Z					
594d5871-c0e0-4328-9162...	0.0.0.0	2025-05-08 ...	2025-05-07 21:40:47 Z					
3158c995-8b9a-4090-a72b...	1.1.1	2025-04-23 ...	2025-03-26 22:55:30 Z					
84a06a7f-bd42-48d1-941b...	1.1.1	2025-04-23 ...	2025-03-26 22:55:30 Z					
85f88146-d85c-4328-83f9-2...	1.1.1	2025-05-01 ...	2025-05-01 06:45:33 Z					
c61decc1-d88e-40e4-9103...	1.1.1	2025-05-01 ...	2025-05-01 06:45:33 Z					
eebacf01-eaf9-4628-b71e-3...	1.1.1	2025-03-15 ...	2025-03-11 12:20:35 Z					
2e54a954-47d2-42e8-b4ea...	1.1.1	2025-04-26 ...	2025-04-23 21:20:57 Z					
87b141b2-b7b3-491e-8fa9...	1.1.1.12	2025-04-26 ...	2025-04-23 21:20:56 Z					

The *Detection Context* page displays the detections and observations timeline, as well as *Detections* and *Behavioral Observations* tables. The tables are sorted by *Last Seen* in descending order.

The detection you pivoted from in the *Detections* table will appear as the *Selected Detection* in the center of the timeline and display details about the detection. The timeline is sorted by *Last Seen* in ascending order. To change the *Selected Detection*, click a row in the *Detections* table. To change the selection to an observation, click a row in the *Behavioral Observations* table. You can also use the scroll bar below the timeline to move back and forth.

To pivot to the *Detections* or *Behavioral Observations* pages, click the *Detection Name* or observation *Title* in the table, or click a tile in the timeline.

Fortinet FortiNDR Cloud 25.4.a Release Notes

Version history

Related Detections and Observations

10.10.1.114

Show All 2025-02-06 2025-05-07

1 day before Same day Selected Detection Same day 1 day after

DNS NXDOMAIN Response for Suspicious Domain
LAST SEEN: 2025-05-07 11:47:25 (UTC)
FIRST SEEN: 2025-03-06 10:53:45 (UTC)
INSTANCE COUNT: 50
CATEGORY: relationship
CLASS: SPECIFIC
DESCRIPTION: This observation is triggered when a source IP queries domains similar to what a domain...
CONFIDENCE: HIGH

Autolt User Agent
LAST SEEN: 2025-05-07 06:01:53 (UTC)
FIRST SEEN: 2025-05-06 09:42:15 (UTC)
EVENT COUNT: 11
CATEGORY: Attack:Installation
TECHNIQUES: T1059
STATUS: Active
SEVERITY: HIGH CONFIDENCE: LOW

Cryptocurrency Mining Client Check-in
LAST SEEN: 2025-05-07 06:17:56 (UTC)
FIRST SEEN: 2025-05-07 06:12:05 (UTC)
EVENT COUNT: 15
CATEGORY: PUA:Unauthorized Resource Use
TECHNIQUES: T1095
STATUS: Active
SEVERITY: MOD CONFIDENCE: MOD

HTTP C2 Similarity (Natural Language Processing)
LAST SEEN: 2025-05-07 11:11:34 (UTC)
FIRST SEEN: 2025-05-07 11:03:34 (UTC)
INSTANCE COUNT: 3
CATEGORY: relationship
CLASS: SPECIFIC
DESCRIPTION: HTTP connections resembling malicious C2 detected using...
CONFIDENCE: HIGH

DNS NXDOMAIN Response for Suspicious Domain
LAST SEEN: 2025-05-07 11:47:25 (UTC)
FIRST SEEN: 2025-03-06 10:53:45 (UTC)
INSTANCE COUNT: 50
CATEGORY: relationship
CLASS: SPECIFIC
DESCRIPTION: This observation is triggered when a source IP queries domains similar to what a domain...
CONFIDENCE: HIGH

Detections

Priority	Confidence	Last Seen	First Seen	Events	Category
MOD	MOD	2025-05-07 17:24:...	2024-03-05 23:48:...	12534	Miscellaneous
MOD	MOD	2025-05-07 17:24:...	2024-03-05 23:48:...	12534	Miscellaneous
MOD	MOD	2025-05-07 12:22:...	2024-03-05 21:04:...	4668	Attack:Installation
LOW	LOW	2025-05-07 12:22:...	2024-03-06 06:50:...	2732	Attack:Installation
MOD	MOD	2025-05-07 06:17:...	2025-05-07 06:12:...	15	PUA:Unauthorized Resource Use
LOW	LOW	2025-05-07 06:01:...	2025-05-06 09:42:...	11	Attack:Installation
LOW	LOW	2025-05-02 02:54:...	2025-01-30 19:55:...	2706	Miscellaneous
LOW	LOW	2025-05-02 02:54:...	2025-01-30 19:55:...	1606	Miscellaneous
HIGH	HIGH	2025-04-29 19:34:...	2025-04-22 18:55:...	11	Posture:Potentially Unwanted
HIGH	HIGH	2025-04-29 19:34:...	2025-04-22 18:55:...	11	Posture:Potentially Unwanted
LOW	LOW	2025-04-26 03:17:...	2025-04-25 02:34:...	2	Attack:Installation
HIGH	HIGH	2025-04-24 06:20:...	2025-04-08 00:14:...	8	Attack:Command and Control
MOD	MOD	2025-04-23 03:12:...	2025-04-16 22:24:...	73	PUA:Unauthorized Resource Use
HIGH	HIGH	2025-04-15 06:26:...	2025-04-15 06:25:...	10	Posture:Potentially Unwanted

Behavioral Observations

Title	Confidence	Last Seen	First Seen	Instances	Category
HTTP C2 Similarity (Natural Language Processing)	LOW	2025-05-07 15:55:...	2025-04-08 14:04:...	568	relationship
DNS NXDOMAIN Response for Suspicious Domain	MOD	2025-05-07 12:18:...	2025-03-06 07:57:...	51	relationship
HTTP C2 Similarity	LOW	2025-05-07 12:15:...	2025-04-09 00:59:...	46	relationship
Domain Similar to Malware Domain	LOW	2025-05-07 11:58:...	2025-02-06 20:58:...	416	relationship
DNS NXDOMAIN Response for Suspicious Domain	HIGH	2025-05-07 11:47:...	2025-03-06 10:53:...	50	relationship
HTTP C2 Similarity (Natural Language Processing)	HIGH	2025-05-07 11:11:...	2025-05-07 11:03:...	3	relationship
HTTP Beaconsing Activity to Host	HIGH	2025-05-05 05:52:...	2025-04-28 17:55:...	4	relationship
HTTP C2 Similarity	MOD	2025-05-01 12:50:...	2025-04-28 20:21:...	2	relationship
HTTP C2 Similarity (Natural Language Processing)	MOD	2025-04-26 09:52:...	2025-04-09 22:45:...	9	relationship
TCP Port 135 (RPC) Device Enumeration	MOD	2025-04-22 03:20:...	2025-04-22 03:20:...	1	relationship
XOR-Encoded PE File from Untrusted Source	MOD	2025-04-15 16:22:...	2025-04-15 16:22:...	1	file
TCP Port 445 (SMB) Device Enumeration	LOW	2025-04-15 08:04:...	2025-02-08 23:32:...	11	relationship
TCP Port 139 (NetBIOS) Device Enumeration	LOW	2025-04-15 08:04:...	2025-03-10 03:16:...	5	relationship
New and Unusual NTLM Authentication	LOW	2025-04-11 20:47:...	2025-03-10 23:24:...	5	relationship

You can filter the *Detection Context* page by *Detections* and *Observations*.

Fortinet FortiNDR Cloud 25.4.a Release Notes

Version history

Related Detections and Observations

10.10.1.114

Show All 2025-02-07 2025-05-08

1 day before Same day Selected Detection Same day 1 day after

DNS NXDOMAIN Response for Suspicious Domain
LAST SEEN: 2025-05-07 11:47:25 (UTC)
FIRST SEEN: 2025-03-06 10:53:45 (UTC)
INSTANCE COUNT: 50
CATEGORY: relationship
CLASS: SPECIFIC
DESCRIPTION: This observation is triggered when a source IP queries domains similar to what a domain...
CONFIDENCE: HIGH

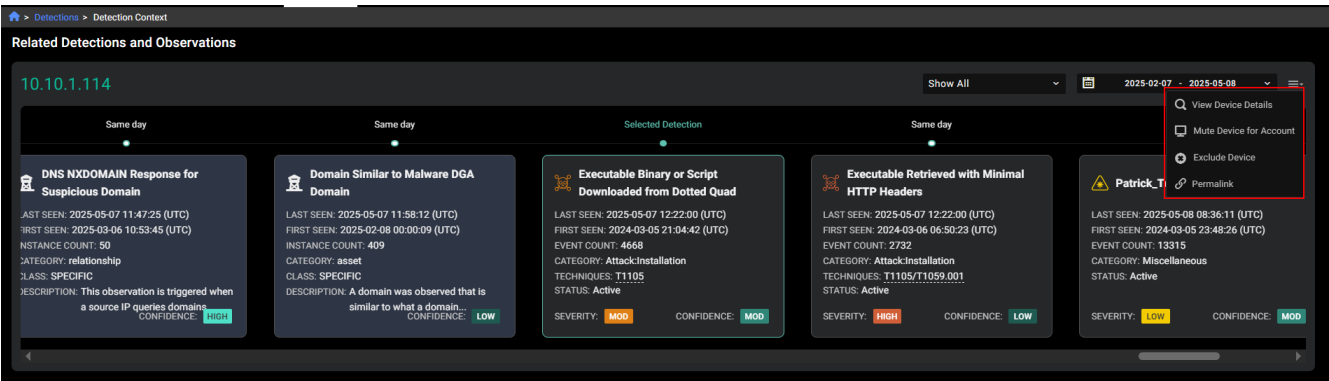
Domain Similar to Malware DGA Domain
LAST SEEN: 2025-05-07 11:58:12 (UTC)
FIRST SEEN: 2025-02-08 00:00:09 (UTC)
INSTANCE COUNT: 409
CATEGORY: asset
CLASS: SPECIFIC
DESCRIPTION: A domain was observed that is similar to what a domain...
CONFIDENCE: LOW

Executable Binary or Script Downloaded from Dotted Quad
LAST SEEN: 2025-05-07 12:22:00 (UTC)
FIRST SEEN: 2024-03-05 21:04:42 (UTC)
EVENT COUNT: 4668
CATEGORY: Attack:Installation
TECHNIQUES: T1105
STATUS: Active
SEVERITY: MOD CONFIDENCE: MOD

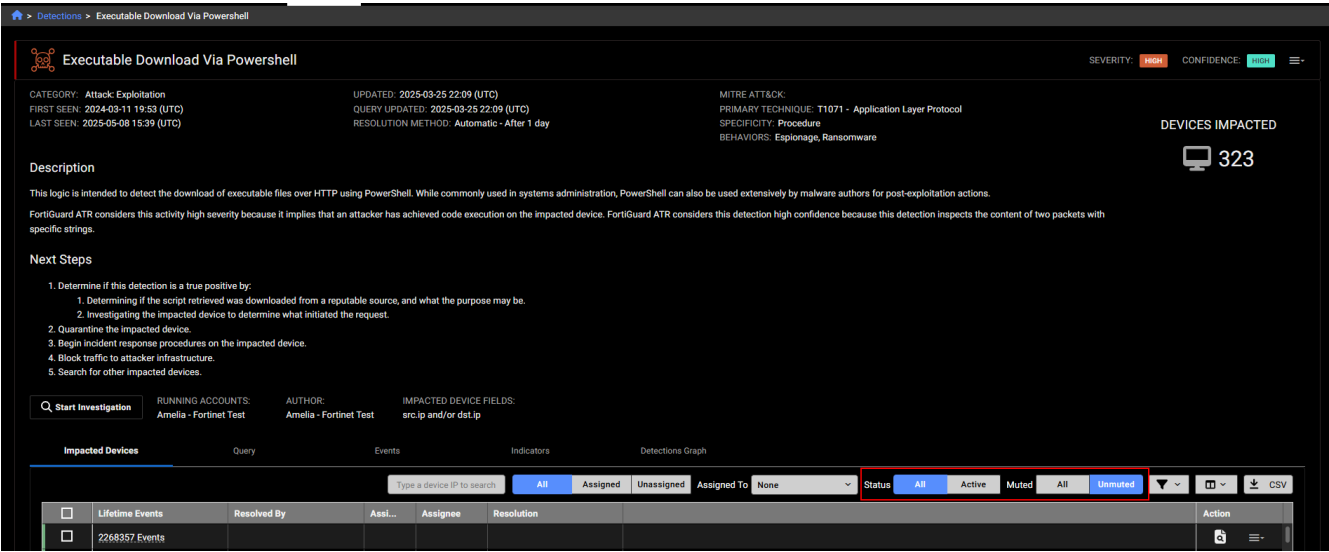
Executable Retrieved with Minimal HTTP Headers
LAST SEEN: 2025-05-07 12:22:00 (UTC)
FIRST SEEN: 2024-03-06 06:50:23 (UTC)
EVENT COUNT: 2732
CATEGORY: Attack:Installation
TECHNIQUES: T1105/T1059.001
STATUS: Active
SEVERITY: HIGH CONFIDENCE: LOW

Patrick_Test2_Suri_RAT
LAST SEEN: 2025-05-08 08:36:11 (UTC)
FIRST SEEN: 2024-03-05 23:48:26 (UTC)
EVENT COUNT: 13315
CATEGORY: Miscellaneous
STATUS: Active
SEVERITY: LOW CONFIDENCE: MOD

You can use the *Detection Context* page to view the device details, mute or exclude the device.



When you click a detection in the timeline, you are pivoted the *Triage Detections* details page. This page has been updated to include the *Status* and *Muted* filters. By default, the page shows *All* detections and *Unmuted* detections.

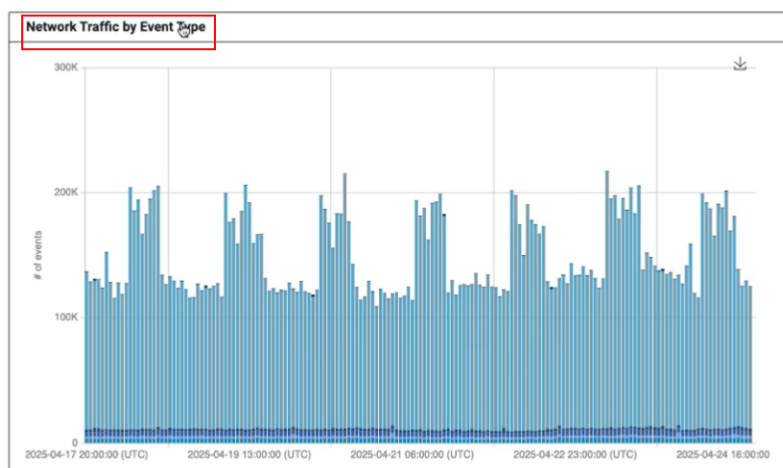


Improved functionality

Sensor telemetry

Traffic by event type widget

You can now click the header in the *Traffic by Event Type* dashboard widget to pivot to the *Sensor Telemetry* page.

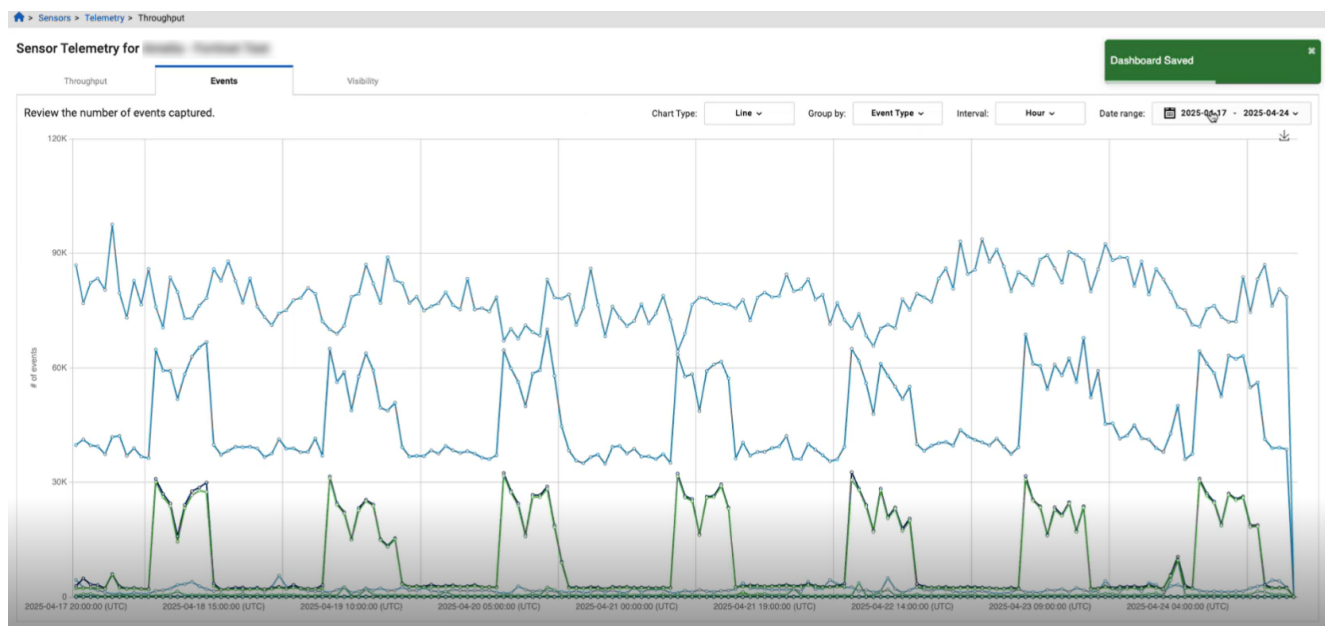


All the filters applied to the widget will be transferred to the *Sensor Telemetry* page.

Configuration panel for the "Network Traffic by Event Type" widget. The panel includes the following settings:

- Block Name: Network Traffic by Event Type
- Chart Type: Line
- Group by: Event Type
- Date Range: Last 7 Days
- Interval: Hour

Buttons: Cancel, Save



Sensor telemetry page

We have added a legend to the Sensor Telemetry page. This is useful when you want to isolate entries on the page. The legend displays the entries in descending order from highest to lowest. You can use the toggles in the legend to show or hide a line in the graph. You also have the option of showing or hiding all entries.



IQL queries

Idap and Idap_search

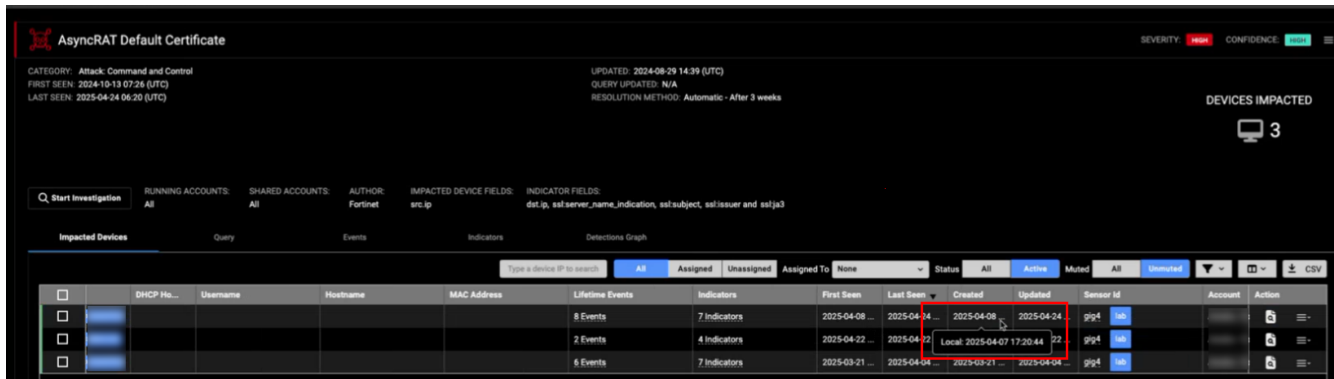
We have added the following event fields to the IQL search:

ldap	<i>argument, diagnostic_message, message_id, object, opcode, result, version</i>
ldap_search	<i>attributes, base_object, deref_aliases, diagnostic_message, filter, message_id, result, result_count, scope</i>

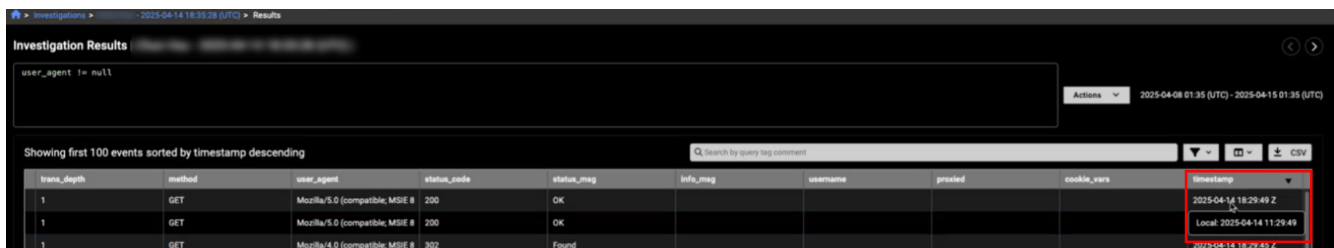
Other improvements

Local time

We have added the local time to the timestamps throughout the portal. To view the local time, hover over the UTC timestamp.



Note that in the *Events Table*, you need to click the timestamp to view the local time.



Performance improvements

- The CrowdStrike integration has been updated to ensure continued functionality after the deprecation of the old API.
- Email alerts for individual detections now include the detection name in the subject field.
- The API now allows you to retrieve all detections that have been updated after a specified date.

Version 25.1.e

- New functionality
 - Custom dashboards
 - Traffic by type widget
 - Detections
 - Automated response configuration
- Improved functionality
 - Investigations
 - Column profiles
 - IQL queries
 - Detections
 - Create new detectors

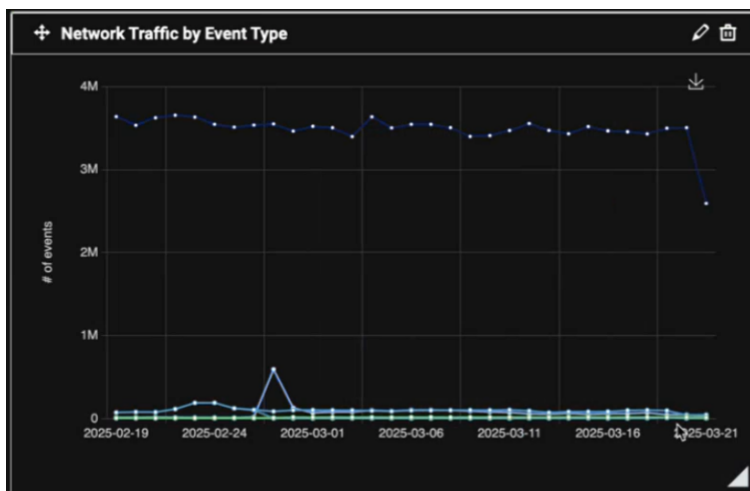
- Other improvements
 - Sensors
 - Encryption keys
- Resolved issues

New functionality

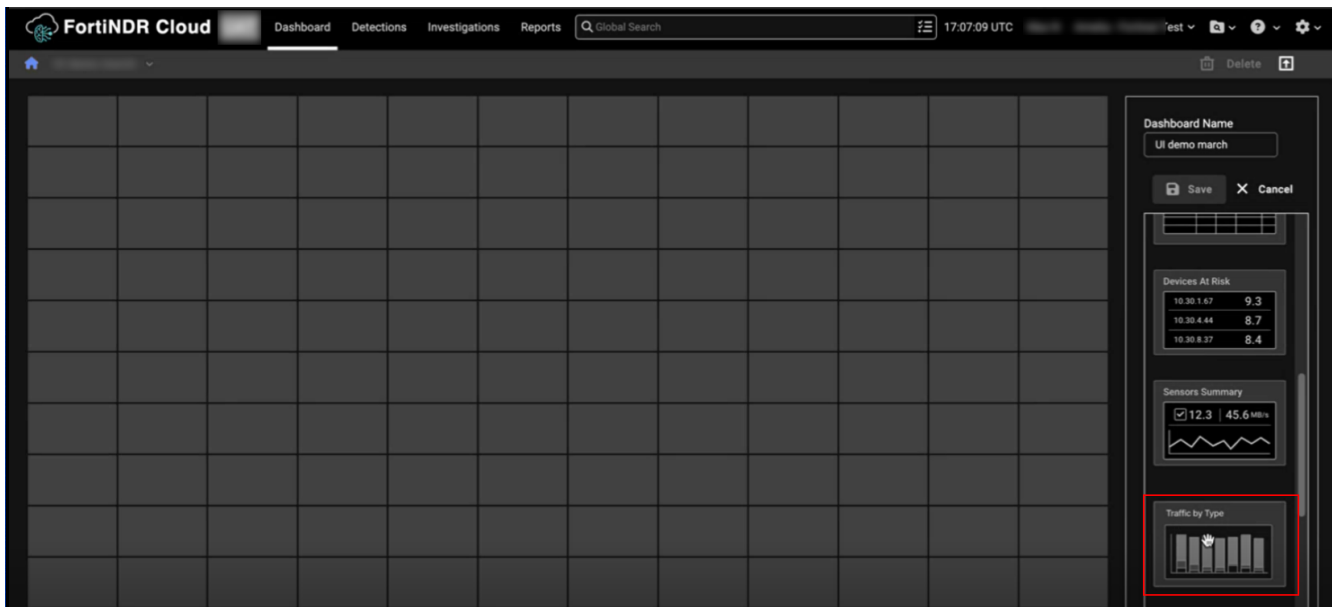
Custom dashboards

Traffic by Event Type widget

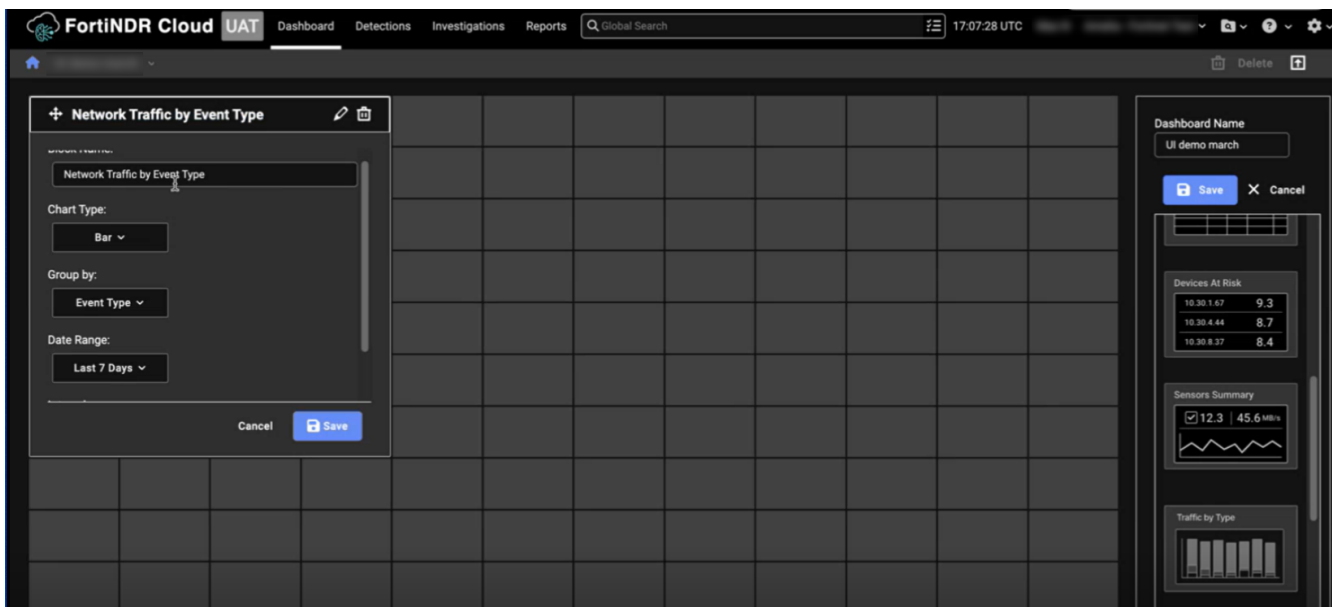
We have added a new *Network traffic by Event Type* widget to the custom dashboard menu. The data in the widget mirrors the *Events* tab in the *Sensor telemetry* page.



To add the widget, create a new dashboard, and select the *Traffic by type* widget in the menu.



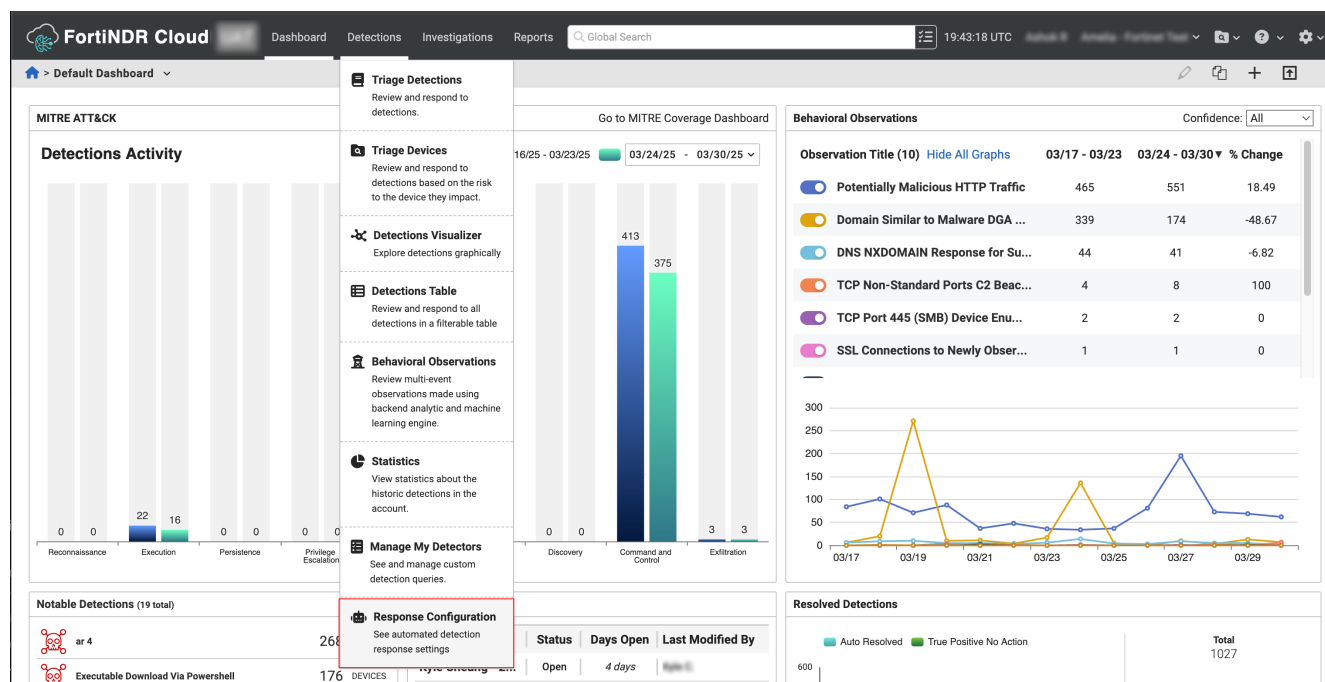
The widget's default name is *Network Traffic by Event*. You can change the name of the widget as well as the default chart type and data filters.



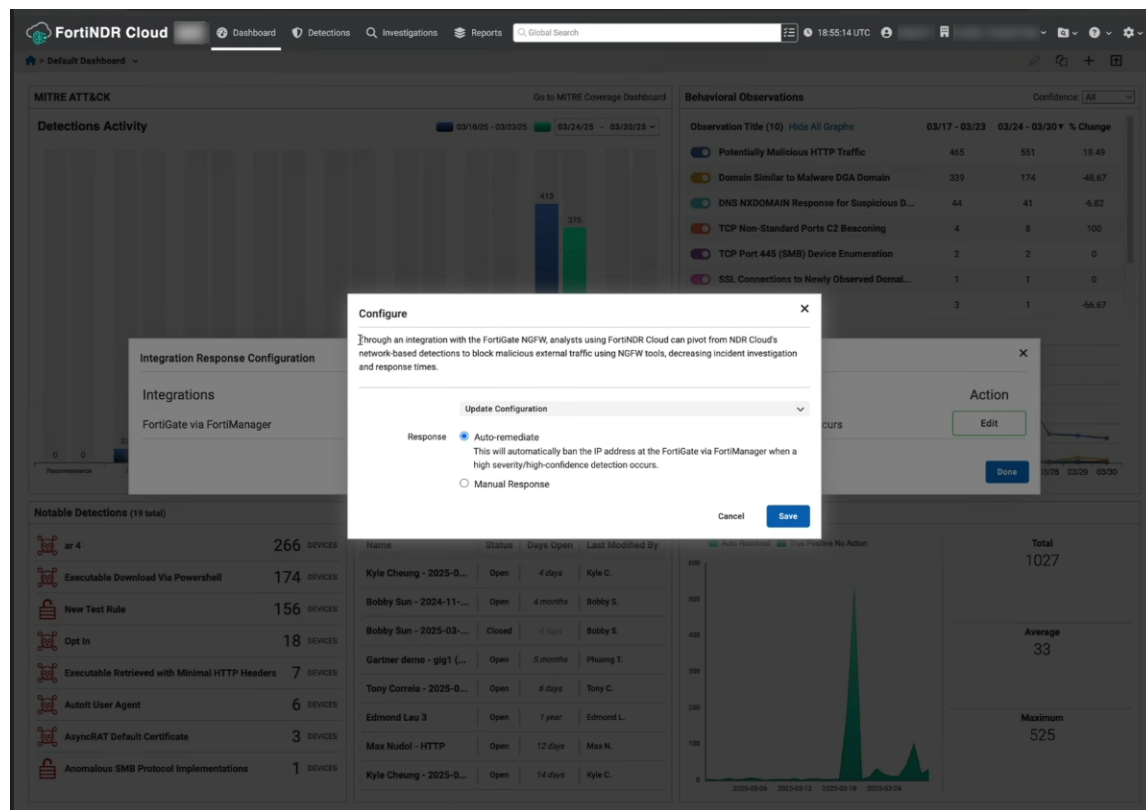
Detections

Automated response configuration

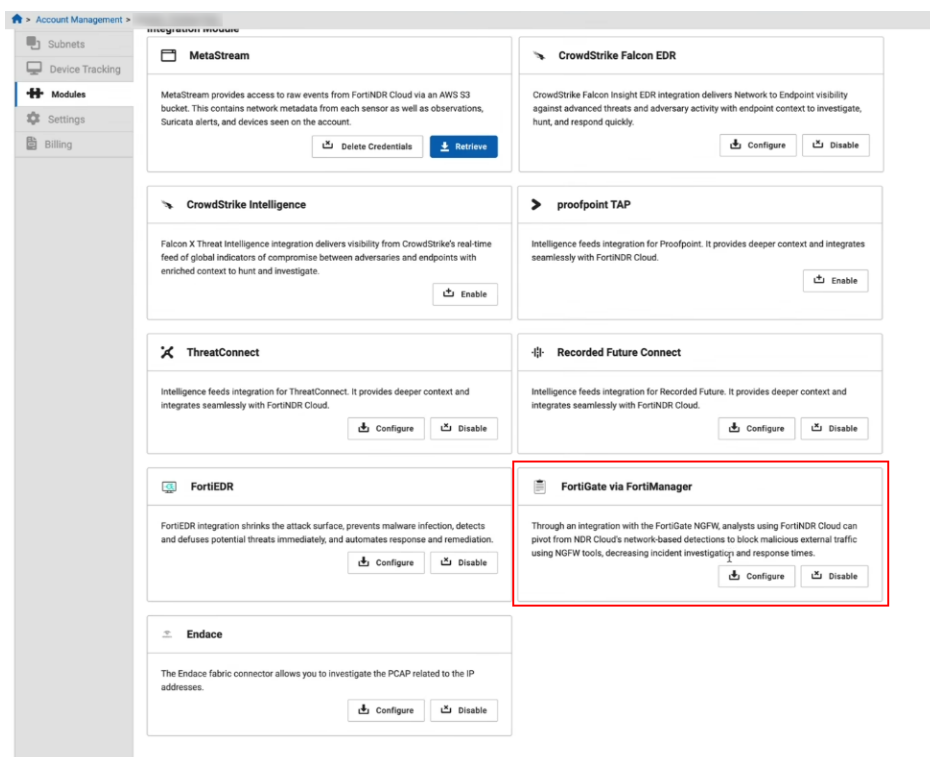
The new *Response Configuration* feature allows you to automatically ban an IP address when a high-severity and high-confidence detection occurs. This feature is only available for FortiGate via FortiManager integrations at this time.



To enable and configure the Response Configuration, go to *Detections > Response Configuration*. In the *Configure* dialog, select *Auto-remediate* or *Manual Response*.



You can also enable *Response Configuration* in the *Account Management > Modules* page by clicking *Configure* in the *FortiGate via FortiManager* tile.



Improved functionality

Investigations

Column profiles

We have improved the usability of the *Column Profiles* feature. For example, you no longer need to refresh the page when you create a new profile for it to appear in the profile list. We have also added a radio button to select the profile you want to edit or delete.

To create a new profile, simply add or remove columns to the current view and adjust the column width, then click *Create New Profile*. Everything in the table will be saved to the profile including the column width. To update changes to an existing profile, simply click *Save this Profile*. After you have finished creating or editing a profile, the page refreshes automatically and applies your changes.

FortiNDR Cloud LOCAL Dashboard Detections Investigations Reports Global Search 17:11:04 UTC

Investigation Results **Kyle Cheung - 2025-03-17 16:43:08 (UTC)**

ip = 10.10.5.4 AND query.domain LIKE '%qfishnhzbxod.com'

Showing all 1210 events, ordered by timestamp descending

tag	t	type	src	dst	intel	source
	202...	DNS	10.10.5.4:59104	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:58994	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:64585	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:53661	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:55745	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:55717	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:54357	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:65521	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:57036	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:60805	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:63777	10.10.5.3:53		Zeek
	202...	DNS	10.10.5.4:58344	10.10.5.3:53		Zeek

Individual Columns

- Column Profiles
- My Profiles
 - max
 - save width
- Default
 - bird's-eye view
 - hosts
- Save This Profile
- Create New Profile

You can also create a new column profile from the *Individual Columns* menu in the *Detections Table* that will include the filters you applied to the page.

FortiNDR Cloud LOCAL Dashboard Detections Investigations Reports Global Search 17:13:49 UTC

Detections Table

26 Detectors, 270 Devices from 1315 Detections

Detection UUID	Device IP	DHCP Ho...	Usena...	Host...	MAC Address	First See	Action
0c45b110-7ed7-45b2-9baa...	1.1.1.1	application:Tag after for				2025-03-	
2fb7f964-e0eb-47a5-ab89-3...	1.1.1.1	application:Tag after for				2025-03-	
eebacf01-aaf3-4628-b71e-3...	1.1.1.1	application:Tag after for				2025-03-	
29d98e51-69eb-4871-bb02...	1.1.1.188					2025-03-	
6d864e4f-7000-43d7-8abb...	1.1.1.188					2025-03-	

Individual Columns

- Column Profiles
- Save This Profile
- Create New Profile

You can configure the profile to include a date range as well as the filters you have applied to the current view of the table.

The screenshot shows the FortiNDR Cloud interface with the 'Detections Table' view. The table lists 26 detectors and 270 devices from 1315 detections. A 'Column Profile' dialog is open, allowing users to configure the table columns. The dialog includes a 'Name' field, a 'Include time range' checkbox (checked), a 'Relative (last 14 Days)' radio button (selected), an 'Absolute (2025-03-07 - 2025-03-21)' radio button, an 'Include other filters' checkbox (checked), and a 'Shared Profile' checkbox (unchecked). The 'Save' button is highlighted.

IQL queries

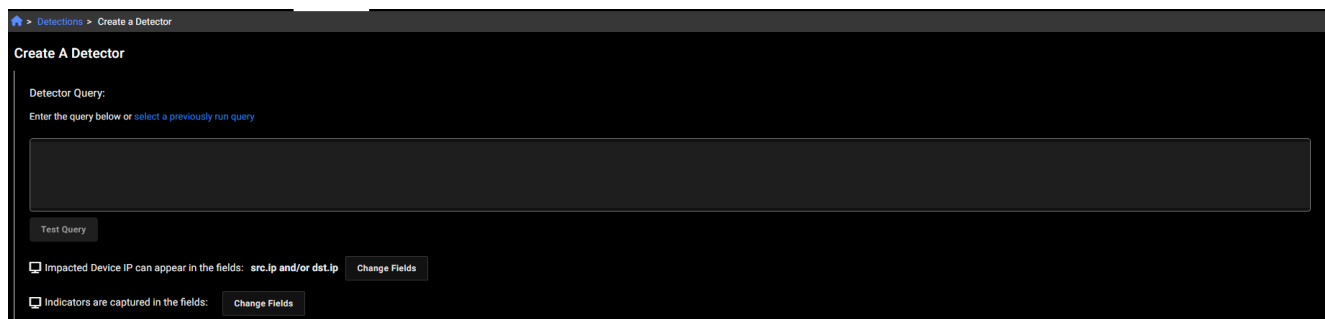
IQL queries now support HTTP server header names, client server names, and cookie variables.

The screenshot shows the FortiNDR Cloud interface with the 'IQL queries' view. The interface displays a list of queries, including 'headers.server_header_names != null or headers.client_header_names != null', 'cookie_vars != null', and 'http:cookie_vars != null'. The 'Add a New Query' dialog is open, showing a 'Name' field, a 'Query' field with the text 'header', and a 'Select Saved Query' button. The 'Add Query' button is highlighted.

Detections

Create new detectors

You can now create a new detector with a new query. In the *Create Detector* page, either enter a new query in the text field or click *select a previously run query*, to use a saved or existing query. If you enter a new query or edit an existing one, you are required to click *Test Query* and resolve any errors before you can save it.



Other improvements

Sensors

- We have improved the tooltip in the *Events* tab of the *Sensors telemetry* page.
- We have added the *Serial Number* column to the *Sensor list* page.

Encryption keys

- We have added the *Uploaded by* and *Uploaded date* values to the *Account management > Settings* page. Going forward the *Settings* page will display the full name and UUID of the user who uploaded the key, as well as the date. If the user does not belong to the account, *Unknown User* is displayed.

Version 25.1.d

- Improved functionality
 - Reports
 - Pending queries in reports
 - Executive summary
- Other improvements
 - Detectors
 - Edit detector
 - Entity lookup
 - GUI
- Resolved Issues

Improved functionality

Reports

Pending queries in reports

FortiNDR Cloud can support up to 35 pending queries simultaneously. To prevent system overload, we have added a tooltip advising users to wait before running another report.

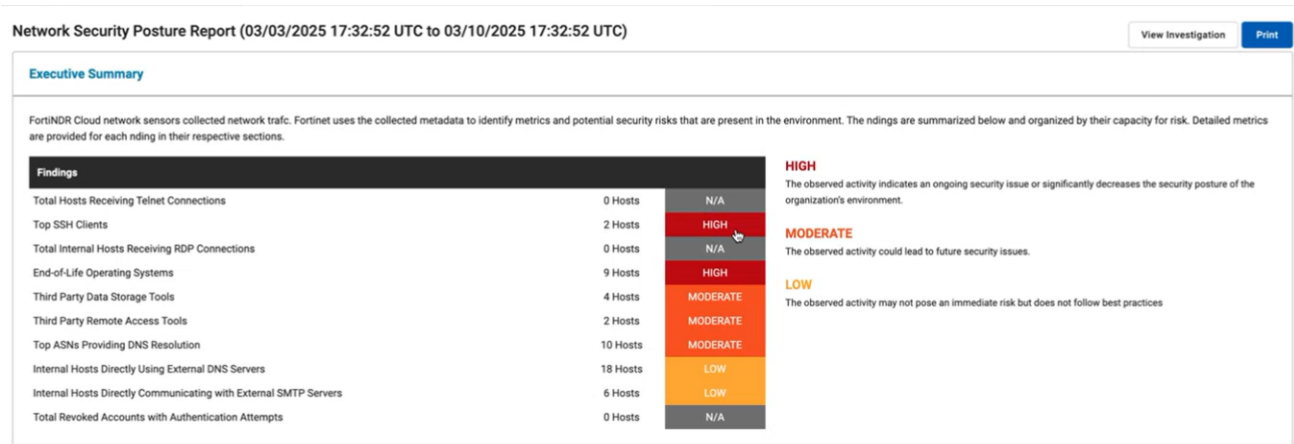
The screenshot shows the 'Reports' section of the FortiNDR Cloud interface. It contains two report cards: 'FortiNDR Cloud Detections Report' and 'FortiNDR Cloud Network Security Posture Report'. Each card has a description, a list of included findings, a date range selector, and a 'Run Report' button. A yellow tooltip with a red border is displayed in the top right corner, stating: 'Report Currently Running in Account. Another report is running in the account. Please wait for the completion of the running report.'

For customers with multiple accounts, users in another account will see the following message:

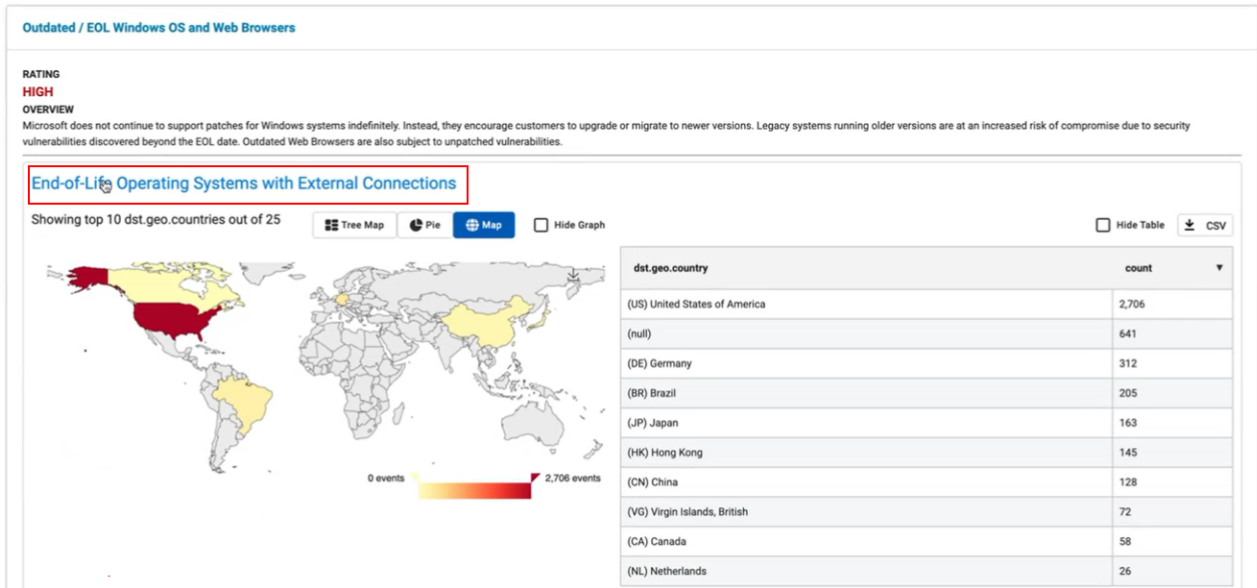
This screenshot shows the same 'Reports' interface as the previous one, but with a different warning. A yellow tooltip with a red border is displayed in the top right corner, stating: 'Too Many Pending Queries. You have too many pending queries. Please wait for the completion of the pending queries.'

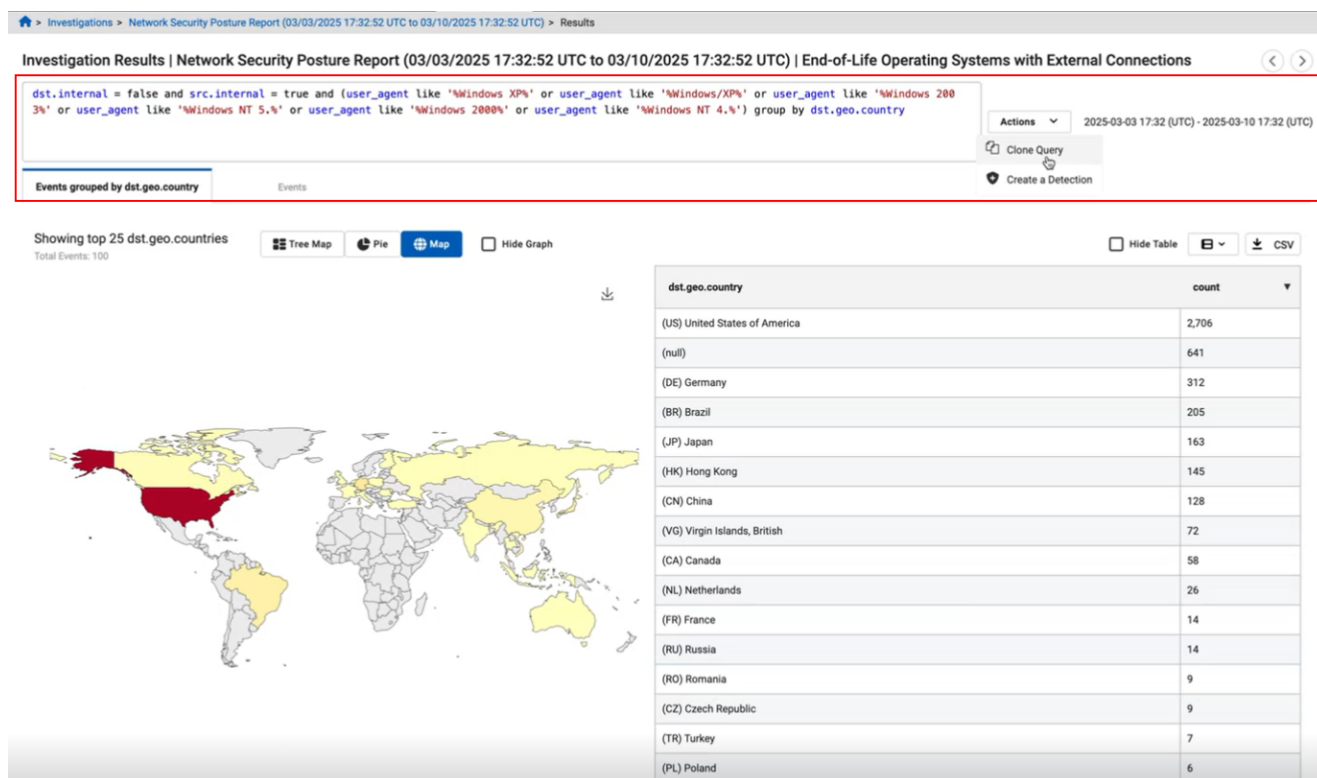
Executive summary

If there are zero hosts for a finding, the Execute Summary will display No Answer (N/A) instead of *High*. You can also click a heading in the *Findings* column to navigate to the corresponding section in the report.



You can click the query title in the report to view the query in the investigations results where you can view the query, clone the query, and create a new detection.





Other improvements

Detectors

Edit detector

- The Resolution Settings longer displays an *Automatic Resolution Period* when *Resolution Style* is set to *Manual*.

Entity lookup

GUI

- The cursor no long appears as a pointer to prevent users from clicking on a table or chart.
- We have added the time range to the *Entity information* field at the top of the page.

Search and Private Search

Group Graph Outliers

- We have updated the *Group Outliers* view to match the contents shown in the graph.

Version 25.1.c

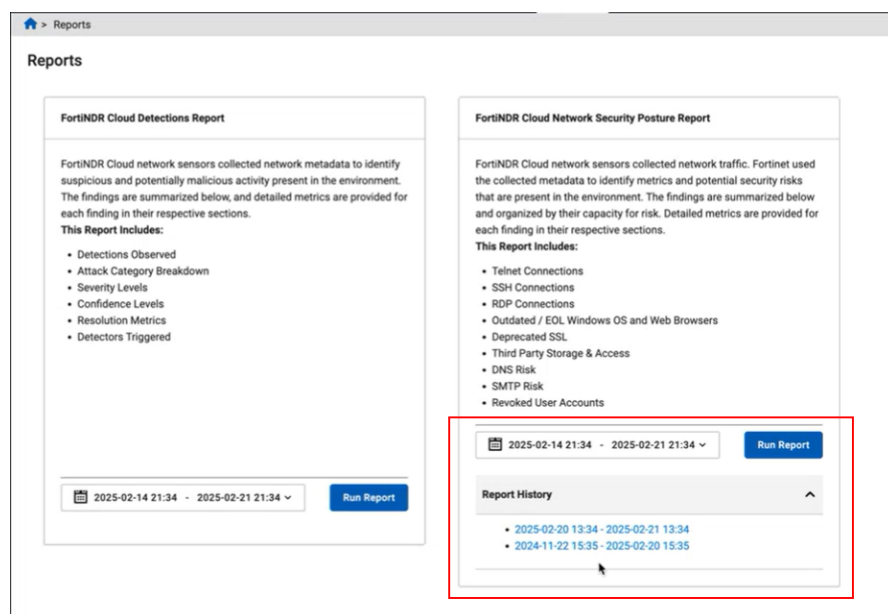
- New functionality
 - Reports
 - FortiNDR Cloud Network Security Posture Report
- Improved functionality
 - Sensors
 - Download sensor images
- Other improvements
 - Portal
- Deprecated functionality
 - Dashboard
- Resolved issues on page 87

New functionality

Reports

FortiNDR Cloud Network Security Posture Report

We have added a Report History panel to the *FortiNDR Cloud Network Security Posture Report* in the *Reports* page. When you click the *Run Report* button, the *Report History* panel displays a log of previously generated reports. To view the report, click the date in the report history.



The *FortiNDR Cloud Network Security Posture Report* also contains a *View Investigation* button to view the investigation in *Read-Only* mode.

Network Security Posture Report (11/22/2024 15:35:46 UTC to 02/20/2025 15:35:46 UTC)

View Investigation Print

Executive Summary

FortiNDR Cloud network sensors collected network traffic. Fortinet used the collected metadata to identify metrics and potential security risks that are present in the environment. The findings are summarized below and organized by their capacity for risk. Detailed metrics are provided for each finding in their respective sections.

Findings	Hosts	UNOBSERVED
Total Hosts Receiving Telnet Connections	Hosts	UNOBSERVED
Top SSH Clients	Hosts	UNOBSERVED
Total Internal Hosts Receiving RDP Connections	Hosts	UNOBSERVED
End-of-Life Operating Systems	Hosts	UNOBSERVED
Third Party Data Storage Tools	Hosts	UNOBSERVED
Third Party Remote Access Tools	Hosts	UNOBSERVED
Top ASNs Providing DNS Resolution	Hosts	UNOBSERVED
Internal Hosts Directly Using External DNS Servers	Hosts	UNOBSERVED
Internal Hosts Directly Communicating with External SMTP Servers	Hosts	UNOBSERVED
Total Revoked Accounts with Authentication Attempts	Hosts	UNOBSERVED

HIGH
The observed activity indicates an ongoing security issue or significantly decreases the security posture of the organization's environment.

MODERATE
The observed activity could lead to future security issues.

LOW
The observed activity may not pose an immediate risk but does not follow best practices

The investigation cannot be altered, however, you can view individual results or go back to the report.

Network Security Posture Report 2025-02-20 15:35:48

Show Report

Created by: Ashok Raghunayakula

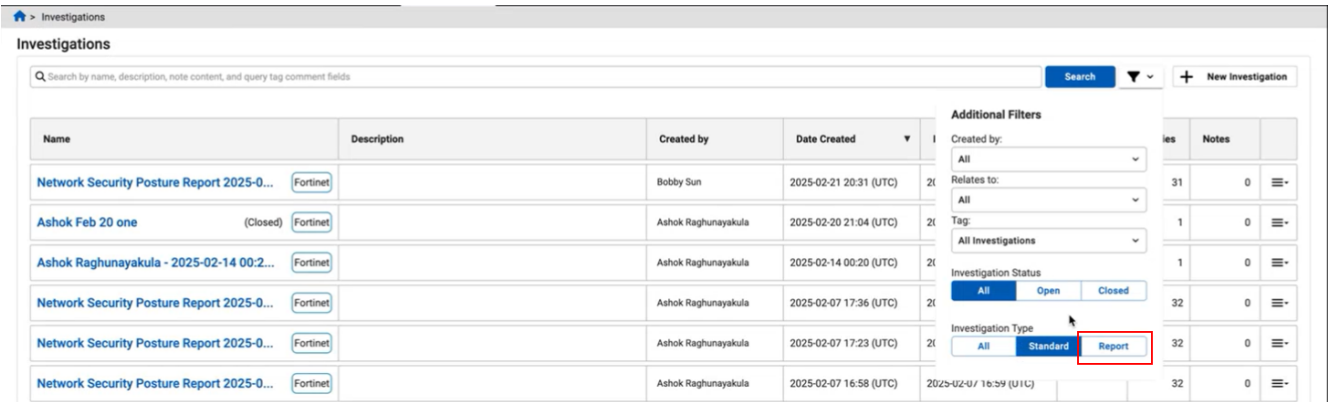
Total Queries: 32 ☒ Completed: 32 ☐ Running: 0 ☐ Queued: 0 ☐ Hide Notes

Search by note content and query tag comment

Guided Queries: Third Party Storage & Access - 2025-02-20 23:35 (UTC)

DESCRIPTION	CATEGORY KEYWORDS
Third Party Storage and Access tools can have legitimate uses. However, they are outside the control of corporate policies and could be threat vectors. LogMeIn, TeamViewer, and other remote access applications enable complete remote control over hosts without requiring corporate authentication in any way. This software can enable remote access by both former employees and malicious actors. Though not malicious in nature specifically, the existence of such software represents a security risk. Recent mass compromises of account details have enabled large scale compromises of users of TeamViewer and other remote desktop services. DropBox, Google Drive, and other third-party data storage services enable the storage of sensitive organizational information outside the control of corporate policies. This leaves the organization vulnerable to insider threats, or data theft through the compromise of accounts of systems beyond the control of the organization.	
☒ http:host matches ".*(dropbox.com .box.com .idrive.com .sugarsync.com .onedrive.com .spideroak.com .certainsafe.com .onedrive.live.com .free-hidrive.com .mega.nz .pcloud.com .mediafire.com .fli.pdrive.com .ozibox.com .disk.yaNDex.com .sync.com .hubic.com .jumpshare.com .mydrive.ch .eyun.360 .cn .mozy.com).*" GROUP BY src.ip, day(timestamp)	☒ View Results 2024-11-22 23:35 (UTC) to 2025-02-20 23:35 (UTC) By: Ashok Raghunayakula 100 Events
☒ http:host matches ".*(dropbox.com .box.com .idrive.com .sugarsync.com .onedrive.com .spideroak.com .certainsafe.com .onedrive.live.com .free-hidrive.com .mega.nz .pcloud.com .mediafire.com .fli.pdrive.com .ozibox.com .disk.yaNDex.com .sync.com .hubic.com .jumpshare.com .mydrive.ch .eyun.360 .cn .mozy.com).*" GROUP BY http:host	☒ View Results 2024-11-22 23:35 (UTC) to 2025-02-20 23:35 (UTC) By: Ashok Raghunayakula 100 Events
☒ http:host matches ".*(gotomypc.com .logmein.com .bongar.com .teamviewer.com .screenconnect.com .splashdot.com .realvnc.com .nonachine.com .anyplace-control.com .remoteteilities.com .amyy.com .join.me .beamyourscreen.com .uvnc.com .aerodmin.com .remotepc.com .seescreen.com .anydesk.com .li.tenanager.com .comodo.com .showmypc.com).*" GROUP BY src.ip, day(timestamp)	☒ View Results 2024-11-22 23:35 (UTC) to 2025-02-20 23:35 (UTC) By: Ashok Raghunayakula 100 Events
☒ http:host matches ".*(gotomypc.com .logmein.com .bongar.com .teamviewer.com .screenconnect.com .splashdot.com .realvnc.com .nonachine.com .anyplace-control.com .remoteteilities.com .amyy.com .join.me .beamyourscreen.com .uvnc.com .aerodmin.com .remotepc.com .seescreen.com .anydesk.com .li.tenanager.com .comodo.com .showmypc.com).*" GROUP BY http:host	☒ View Results 2024-11-22 23:35 (UTC) to 2025-02-20 23:35 (UTC) By: Ashok Raghunayakula 100 Events

We have also added a *Report* option to the *Investigation Type* filter in the *Investigations* page to view report investigations.

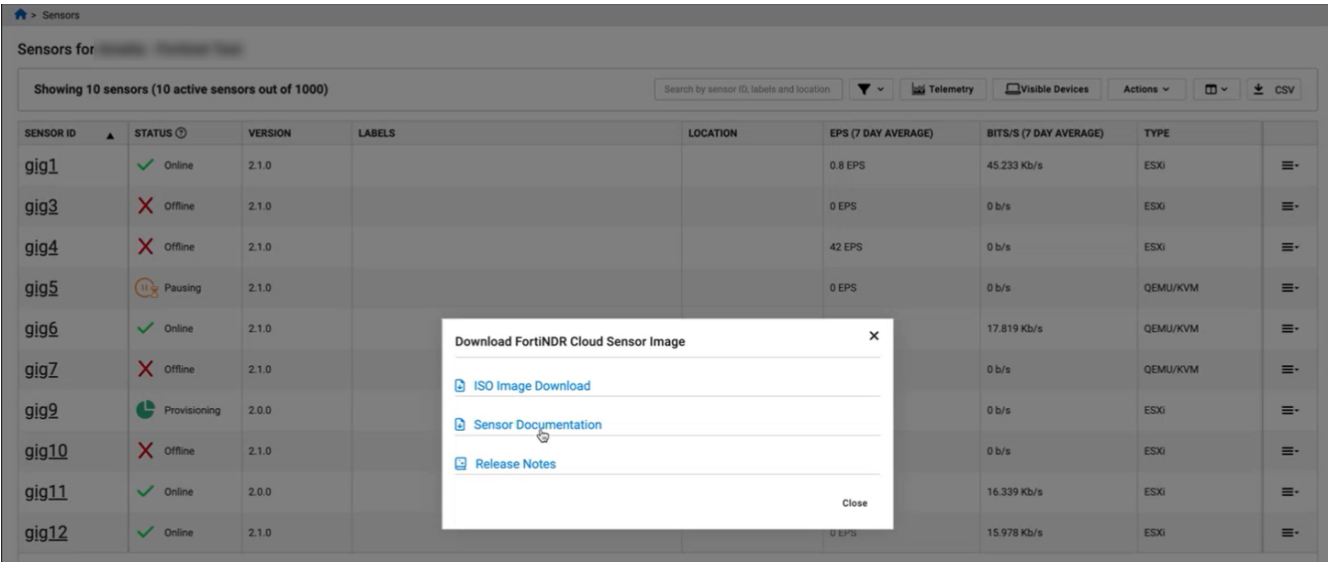


Improved functionality

Sensors

Download sensor images

The *Download FortiNDR Cloud Sensor Image* dialog has been updated to include all the sensor images, as well as links to sensor documentation and release notes. To download the KVM and ESXi sensor images, click *ISO Image Download*.



Other improvements

Portal

When a user logs into the portal for first time, or when a user logs in using a private or incognito browser, the portal defaults to the account the user was created in.

Deprecated functionality

Dashboard

Support for the following dashboards has been deprecated:

- Example Hunt Dashboard 2
- Security Posture - Deprecated SSL
- Security Posture - DNS
- Security Posture - Outdated / EOL Software
- Security Posture - SSH Connections
- Security Posture - Third Party Storage & Access

Please use *Guided Queries* instead.

Version 25.1.b

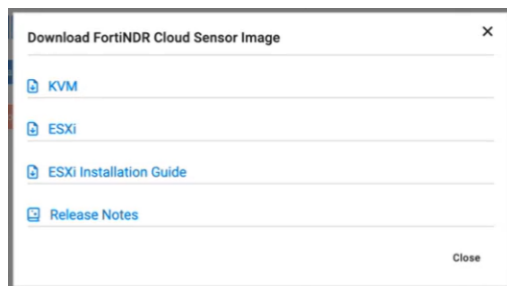
- Improved functionality on page 75
 - Integrations on page 75
 - Sensor images on page 75
 - Account management on page 75
 - User filters on page 75
 - Sensors on page 75
 - Static filters on page 75
- Resolved issues on page 87

Improved functionality

Integrations

Sensor images

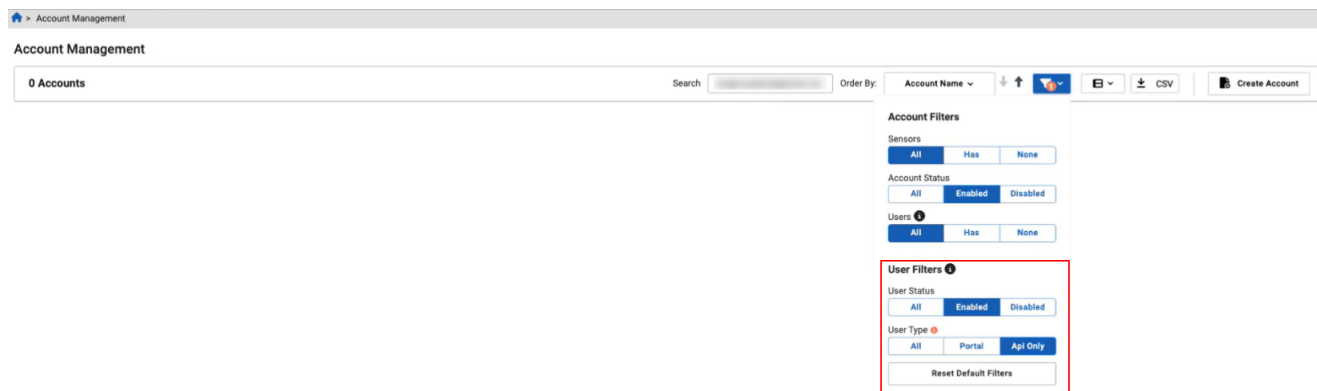
The KVM and ESXi sensor images have been updated. For more information, see the [KVM Sensor Installation Guide](#) and the [ESXi Sensor Installation Guide](#).



Account management

User filters

We have added two new user filters to the *Account Management* page: *User Status* and *User Type*. These filters make it easier to find *API Only* users.



Sensors

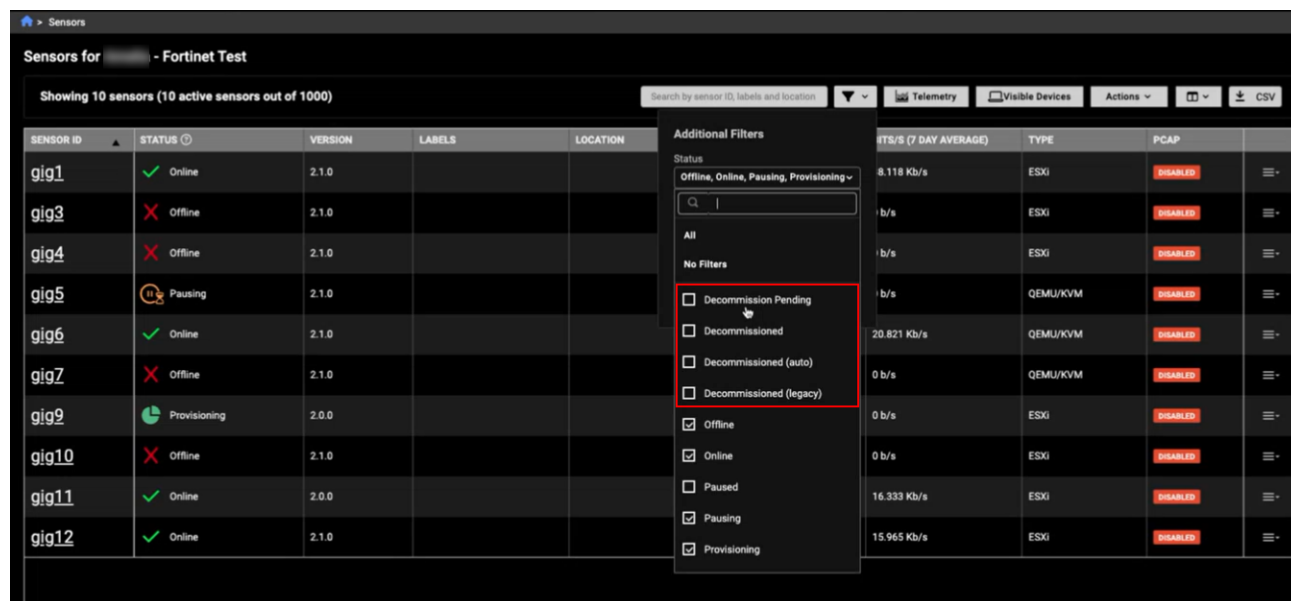
Static filters

Many of the status filters in the *Sensors* page are now static. These include:

- Provisioning
- Online

- Pausing
- Paused
- Resuming
- Decommissioning
- Decommissioned
- Offline

If none of the sensors in your account match the filter, a *No sensors to display* message appears. Other statuses, such as *Unknown*, are displayed in the list dynamically.



Version 25.1.a

- New functionality on page 77
 - Integrations on page 77
 - Endace integration on page 77
 - Investigations on page 79
 - Annotations on page 79
- Improved functionality on page 79
 - Reports on page 79
 - FortiNDR Cloud Network Security Posture Report on page 79
 - Behavioral observations on page 80
 - Time ranges on page 80
 - Integrations on page 81
 - FortiEDR on page 81
 - Other improvements on page 81

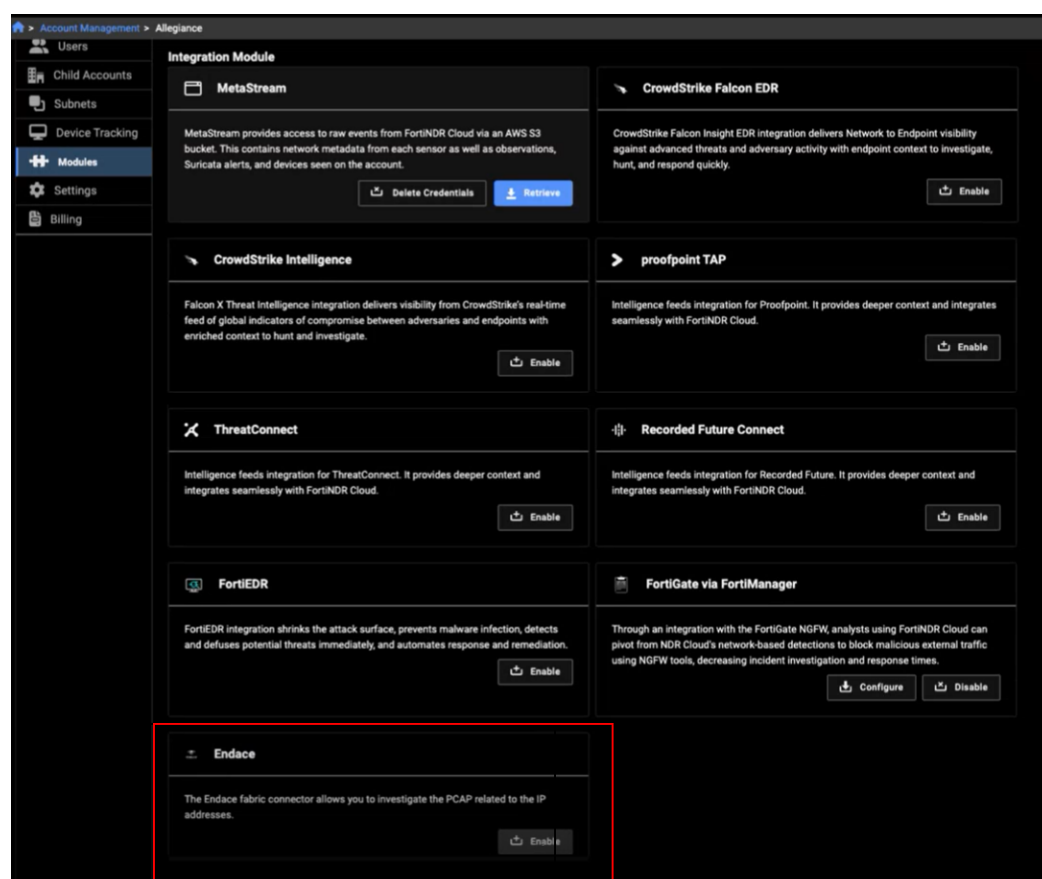
- Tooltips on page 81
- Resolved issues on page 87

New functionality

Integrations

Endace integration

FortiNDR Cloud now supports integration with Endace. Endace probes packet capture data from on-premise, public, and private cloud environments. To enable the integration, go to *Account Management > Modules* and click *Enable* in the Endace module.



You can pivot to Endace by right-clicking an IP address in the Detections table or the Events table. After you pivot from FortiNDR Cloud, Endace will automatically create a new investigation.

In the *Detections* table, right-click the IP address and select the timestamp you want to use (*At created*, *First seen* and *Last seen*) to pivot to Endace.

FortiNDR Cloud | Dashboard | Detections | Investigations | Reports | Global Search

AZORult Check-in | SEVERITY: High | CONFIDENCE: Medium

CATEGORY: Attack: Command and Control
 FIRST SEEN: 2024-10-12 23:49 (UTC)
 LAST SEEN: 2025-01-23 13:36 (UTC)

UPDATED: 2023-03-30 17:30 (UTC)
 QUERY UPDATED: N/A
 RESOLUTION METHOD: Automatic - After 3 weeks

DEVICES IMPACTED: 5 × 0

Start Investigation | RUNNING ACCOUNTS: All | SHARED ACCOUNTS: All | AUTHOR: Fortinet | IMPACTED DEVICE FIELDS: src.ip | INDICATOR FIELDS: dst.ip, suricata.http.host, suricata.http.uri and suricata.http.user_agent

Device IP	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Indicators	First Seen	Last Seen	Created	Updated	Action
10.10.1.114					448 Events	16 Indicators	2024-10-12 ...	2025-01-23 ...	2024-10-12 ...	2025-01-23 ...	
10.10.1.114					343 Events	15 Indicators	2024-10-16 ...	2025-01-23 ...	2024-10-16 ...	2025-01-23 ...	
10.10.1.114					503 Events	13 Indicators	2024-10-13 ...	2025-01-23 ...	2024-10-13 ...	2025-01-23 ...	
10.10.1.114					337 Events	10 Indicators	2024-10-13 ...	2025-01-21 ...	2024-10-13 ...	2025-01-21 ...	
10.10.1.114					411 Events	16 Indicators	2024-10-13 ...	2025-01-19 ...	2024-10-13 ...	2025-01-19 ...	
10.10.1.114					1 Event	4 Indicators	2024-11-18 ...	2024-11-18 ...	2024-11-18 ...	2024-11-18 ...	
10.10.1.114					1 Event	4 Indicators	2024-11-18 ...	2024-11-18 ...	2024-11-18 ...	2024-11-18 ...	
10.10.1.101					1 Event	4 Indicators	2024-11-04 ...	2024-11-04 ...	2024-11-04 ...	2024-11-04 ...	

In the *Events* table, right-click the IP address and select the *EndaceVision* to pivot to Endace.

The time range used is generated from the value in the timestamp column +/- 5 minutes.

FortiNDR Cloud | Dashboard | Detections | Investigations | Reports | Global Search

Investigation Results | vProbe_gig12 |

sensor_id = "gig12"

Showing first 100 events sorted by timestamp descending

tag	timestamp	type	src	dst	intel	query	answers	application_name
	2025-01-16 17:56:42 Z	DHCP	0.0.0.0:68	255.255.255.255:67	1 Hit			
	2025-01-16 17:56:41 Z	DNS	fe80::fe	ff02::fb:5353		_jpp._tcp.local		
	2025-01-16 17:56:25 Z	DHCP	0.0.0.0	255.255.255.255:67	1 Hit			
	2025-01-16 17:56:25 Z	DNS	fe80::fe	ff02::fb:5353		_jpp._tcp.local		
	2025-01-16 17:56:17 Z	DHCP	0.0.0.0	255.255.255.255:67	1 Hit			
	2025-01-16 17:56:14 Z	DNS	fe80::fe	ff02::fb:5353		_jpp._tcp.local	gfi-ga-tgen.local	
	2025-01-16 17:56:13 Z	DNS	fe80::fe	ff02::fb:5353		_smb._tcp.local		
	2025-01-16 17:56:13 Z	FLOW	fe80::fe	ff02::fb:5353				
	2025-01-16 17:56:13 Z	DHCP	0.0.0.0	255.255.255.255:67	1 Hit			
	2025-01-16 17:56:12 Z	FLOW	fe80::fe	ff02::fb:5353				
	2025-01-16 17:56:12 Z	DNS	fe80::fe	ff02::fb:5353		_jpp._tcp.local	gfi-ga-tgen.local	
	2025-01-16 17:56:10 Z	DHCP	0.0.0.0	255.255.255.255:67	1 Hit			
	2025-01-16 17:55:56 Z	DHCP	0.0.0.0:68	255.255.255.255:67	1 Hit			

In the *Entity Panel* you can also pivot to Endace by right-clicking the IP address at the top of the panel.

The time range used will be the same as the Entity Panel.

FortiNDR Cloud | Dashboard | Detections | Investigations | Reports | Global Search

Investigation Results | vProbe_gig12 |

sensor_id = "gig12"

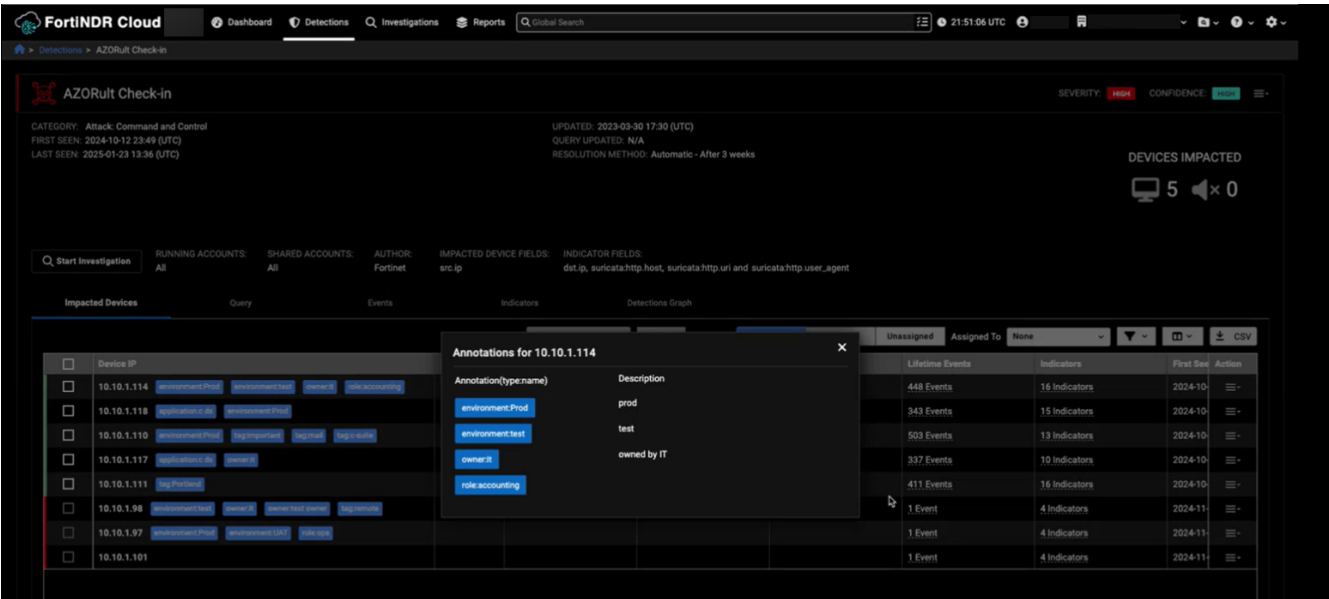
Showing first 100 events sorted by timestamp descending

tag	timestamp	type	src	dst	intel	query	answers	application_name
	2025-01-16 17:56:42 Z	DHCP	0.0.0.0:68	255.255.255.255:67	1 Hit			
	2025-01-16 17:56:41 Z	DNS	fe80::fe	ff02::fb:5353		_jpp._tcp.local		
	2025-01-16 17:56:25 Z	DHCP	0.0.0.0	255.255.255.255:67	1 Hit			
	2025-01-16 17:56:25 Z	DNS	fe80::fe	ff02::fb:5353		_jpp._tcp.local		
	2025-01-16 17:56:17 Z	DHCP	0.0.0.0	255.255.255.255:67	1 Hit			
	2025-01-16 17:56:14 Z	DNS	fe80::fe	ff02::fb:5353		_jpp._tcp.local	gfi-ga-tgen.local	
	2025-01-16 17:56:13 Z	DNS	fe80::fe	ff02::fb:5353		_smb._tcp.local		
	2025-01-16 17:56:13 Z	FLOW	fe80::fe	ff02::fb:5353				
	2025-01-16 17:56:13 Z	DHCP	0.0.0.0	255.255.255.255:67	1 Hit			
	2025-01-16 17:56:12 Z	FLOW	fe80::fe	ff02::fb:5353				
	2025-01-16 17:56:12 Z	DNS	fe80::fe	ff02::fb:5353		_jpp._tcp.local	gfi-ga-tgen.local	
	2025-01-16 17:56:10 Z	DHCP	0.0.0.0	255.255.255.255:67	1 Hit			
	2025-01-16 17:55:56 Z	DHCP	0.0.0.0:68	255.255.255.255:67	1 Hit			

Investigations

Annotations

We have added annotations to the impacted *Device IPs* in all of the *Detection* tables.

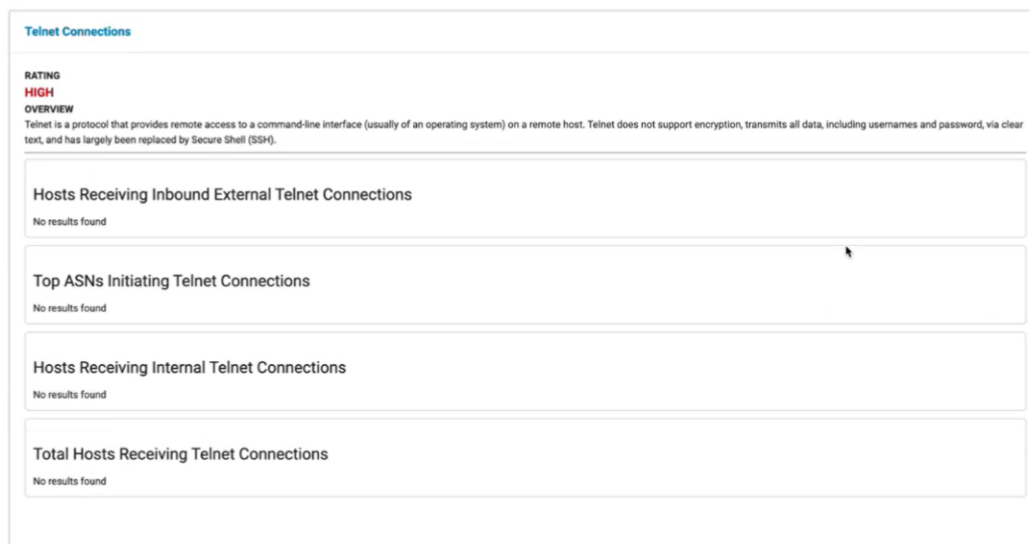


Improved functionality

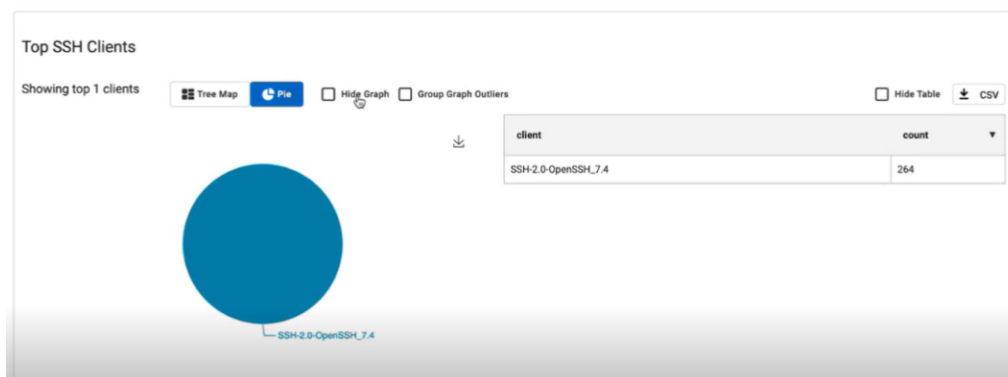
Reports

FortiNDR Cloud Network Security Posture Report

The *FortiNDR Cloud Network Security Posture Report* has been redesigned to include images and more sections with more information. This feature is available upon request.



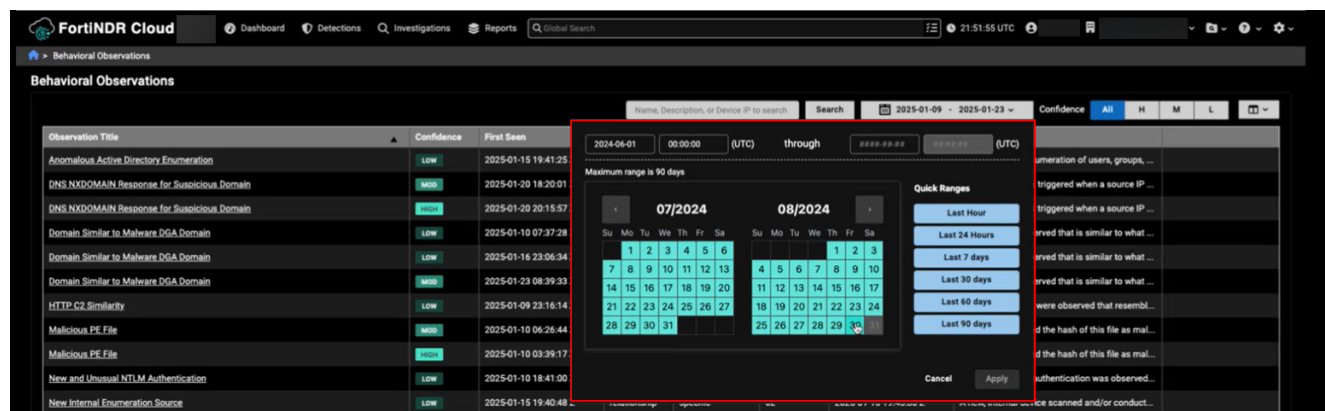
You can switch between charts, hide graphs and tables as well as group graph outliers.



Behavioral observations

Time ranges

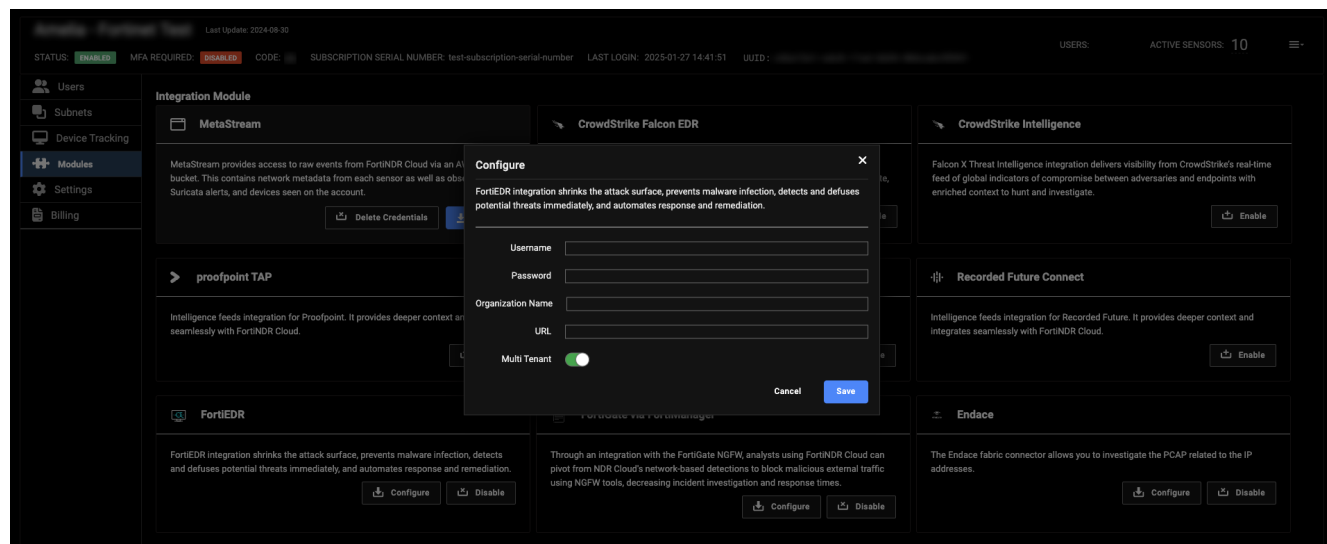
You can view behavioral observations for any 90 days within the last year. In previous versions you could only view the previous 90 days. This functionality is also available in the *Observation Details* page.



Integrations

FortiEDR

Admin users can now make changes to a multi-tenant flag the FortiEDR integration.



Other improvements

Tooltips

- The chart tooltips have been redesigned to make them easier to read.
- A scroll bar was added to longer tooltips allowing the information to fit the page.
- The *Throughput* tooltip in the *Sensors* widget now shows the time when you hover over a data point.

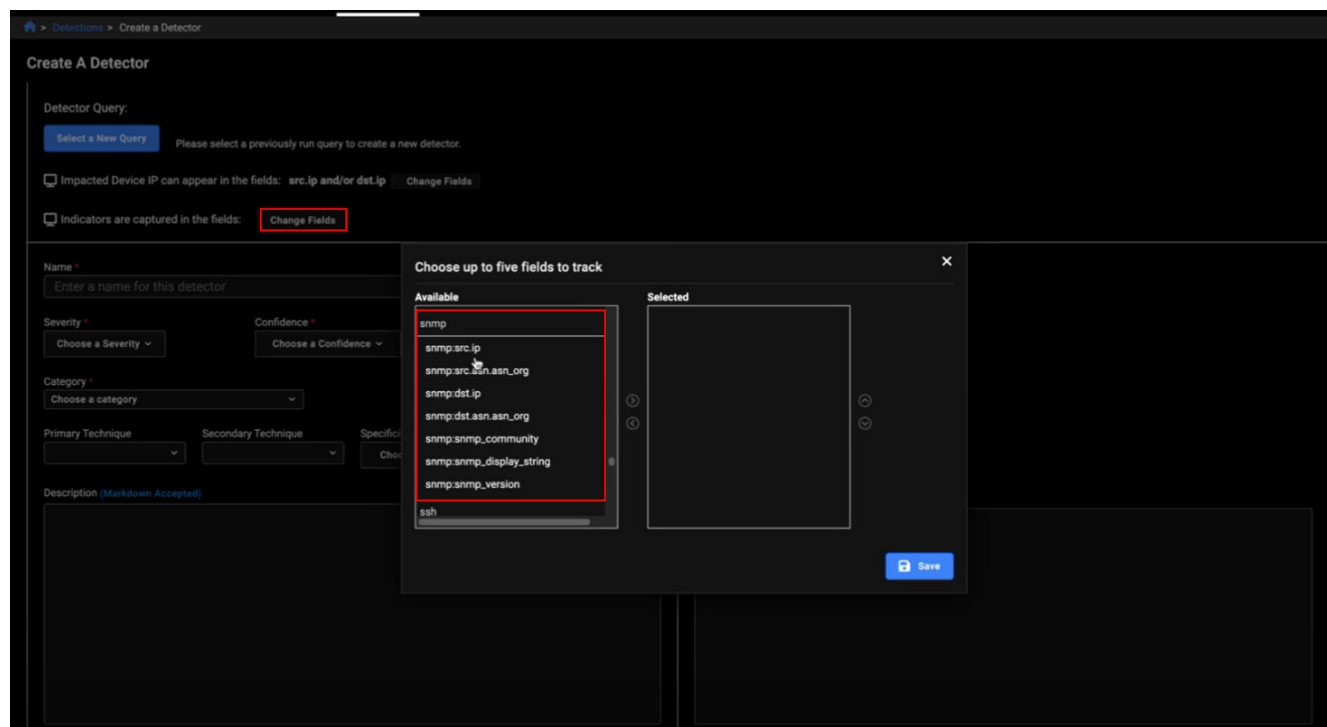
Version 25.1.0

- New functionality on page 82
 - SNMP event fields on page 82
 - Entity Panel on page 82
- Improved functionality on page 84
 - Global Search on page 84
- Other improvements on page 84
- Resolved issues on page 87

New functionality

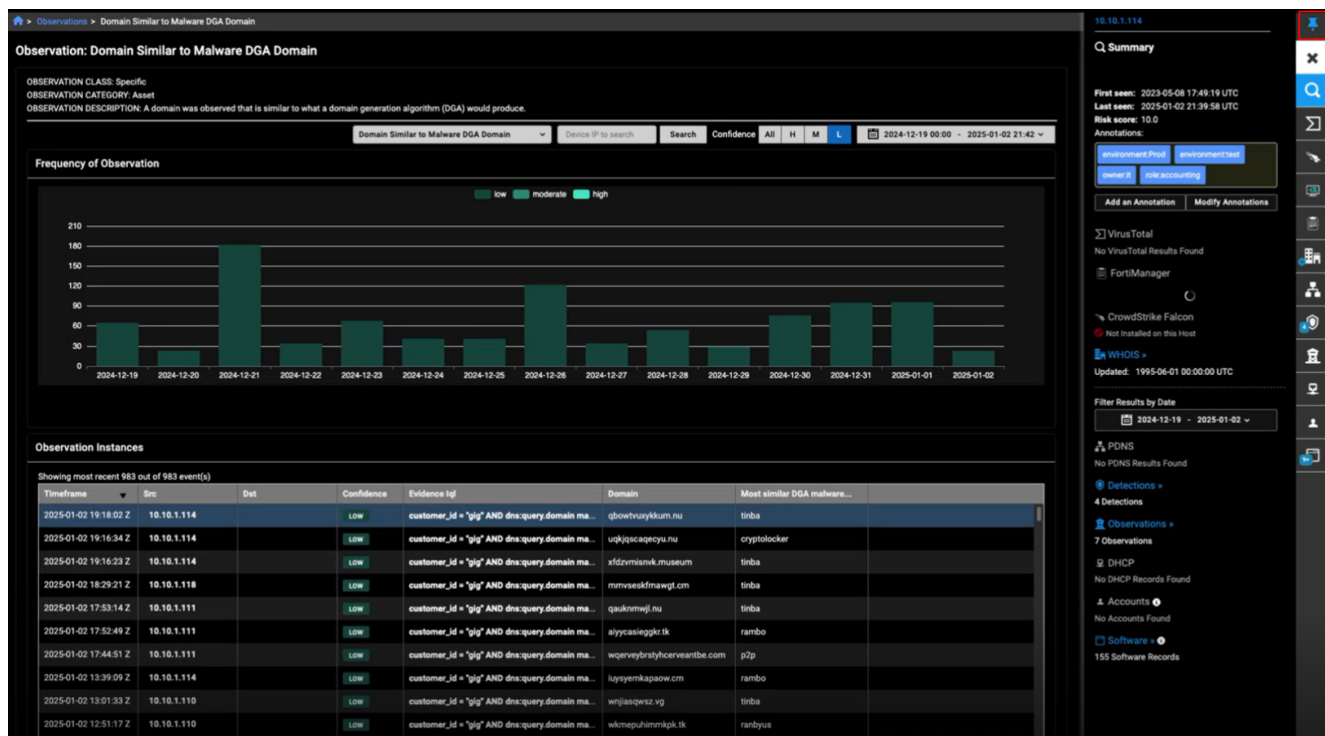
SNMP event fields

SNMP event fields were added to the *Change Fields* option when creating and editing a *Detector*. Any SNMP detections will appear in its own column in the Detector's *Indicators* tab.

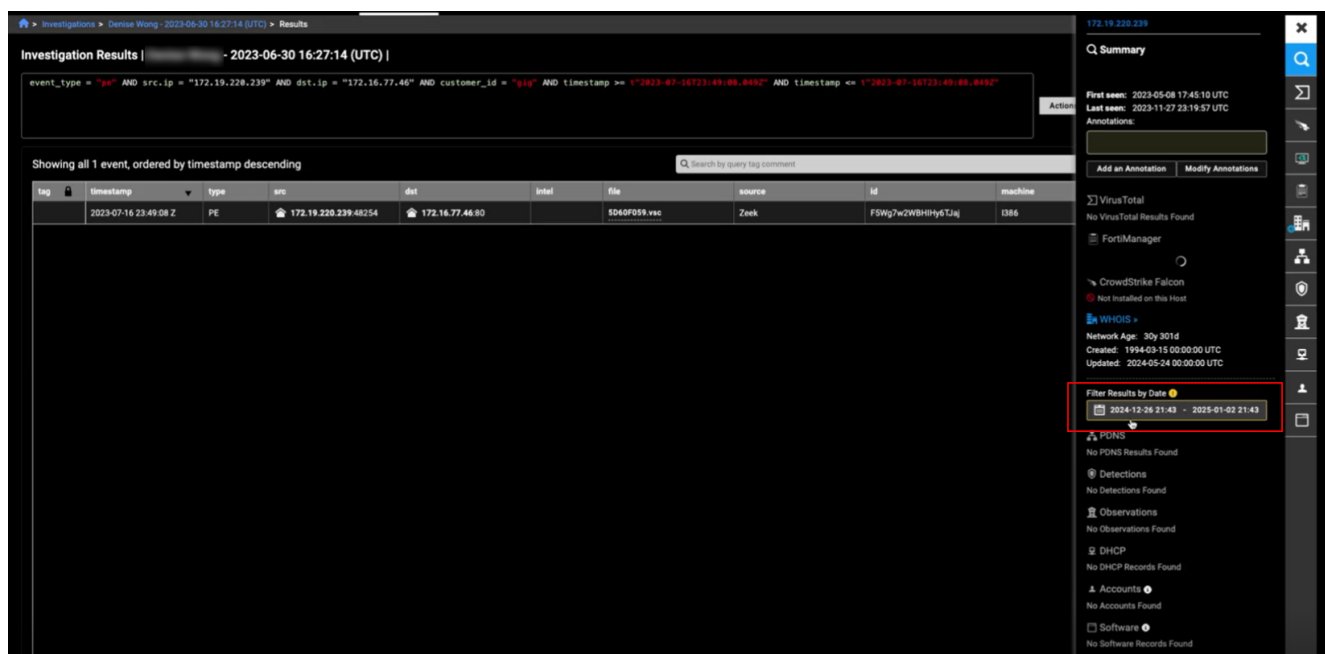


Entity Panel

You can now pin the *Entity Panel* to keep it open and visible when you switch between pages that support it.



We have also limited the date picker in the Entity Panel to one year. If you attempt to enter a date that is more than one year, the picker defaults to the last seven days and a yellow border appears around the date.



The summary *First seen* and *Last seen* fields will display a timestamp for the last year. If the summary is more than a year old, *More than a year ago* is displayed.

A timestamp is displayed for detections within the current year in the *Entity Panel*. Detections that are more than a year old, appear as *More than a year ago*.

NOTE: The *Number of connections from internal devices yesterday* section has been deprecated.

Improved functionality

Global Search

Behavioral Observations have been added to the *Global Search* results.

Global Search

Detections

IP address, detection name, and detection description

Device IP	Lifetime Events	Indicators	Last Seen	Status	Resolved By	Resolution	Date Resolved	Detection Name	Detection Description	Severity
10.10.1.118	4 Events	2 Indicators	2024-12-16 ...	Resolved		Automatically Resolved	2024-12-23 07:55:31 Z	AnyDesk Remote Administration		Low
10.10.1.118	1865 Events	25 Indicators	2025-01-02 ...	Active				Executable Binary or Script Down	This logic is intended to detect...	High
10.10.1.118	79 Events	16 Indicators	2024-12-30 ...	Active				AutoIt User Agent		High
10.10.1.118	336764 Events	0 Indicators	2025-01-02 ...	Active				Created by power user	Description of this rule to test...	High
10.10.1.118	1144 Events	21 Indicators	2025-01-01 ...	Active				Executable Retrieved with Mmr	This logic is intended to detect...	High

Detections Coverage

Name, description, and Mitre Technique

No Detections coverage found.

Behavioral Observation

IP Address, observation title, and observation description

Observation Title	Confidence	Category	Class	Instances	First Seen	Last Seen	Description
HTTP.C2 Similarity	Low	relationship	specific	106	2024-10-04 23:35:16 Z	2025-01-02 16:37:08 Z	HTTP connections were observed that resembl...
HTTP.C2 Similarity	Low	relationship	specific	1	2024-12-09 03:29:59 Z	2024-12-09 03:29:59 Z	HTTP connections were observed that resembl...
Malicious PE File	Medium	file	specific	3248	2024-10-06 17:14:36 Z	2024-12-15 20:22:55 Z	Fortiguard identified the hash of this file as mal...
Malicious PE File	Medium	file	specific	38911	2024-10-06 17:14:48 Z	2024-12-29 01:35:15 Z	Fortiguard identified the hash of this file as mal...
TCP Non-Standard Ports Beaconing	Medium	relationship	specific	6	2024-10-19 16:20:20 Z	2024-10-24 13:54:57 Z	TCP connections over non-standard ports were...

Investigations

Name, description, and comments

No investigations found.

Private Search

Query contents or comments

Query - 2024-12-05 19:25 (UTC)

ip = 10.10.1.118

View Results

2024-12-04 19:24 (UTC) to 2024-12-05 19:24 (UTC)

100 Events

Entity Lookup

IPs and Domains found from search string

Entity	Type	Count	First Seen	Last Seen
10.10.1.118	IP	630817	2023-05-08 17:48 (UTC)	2025-01-02 21:39 (UTC)

Other improvements

- We have added a *Back to Login Page* button to the login error page.
- A *Collapse* button was added to the *Triage Devices* page to hide the *Impacted Devices* column.
- When you pivot to the *Entity Lookup* from a page that supports a time range of one year, the time range picker will default to the *Last Seven Days* and a yellow border appears around the date field.

Product integration and support

The following table lists FortiNDR Cloud product integration and support information.

SIEM	CrowdStrike	Tested with Parser 1.0.2
	FortiSIEM	7.1.0 or higher
	Microsoft Sentinel	Not applicable
	QRadar	IBM QRadar SIEM version 7.3.3 or higher
	Splunk	Splunk Cloud versions: 9.3, 9.2, 9.1
SOAR	Cortex-XSOAR	Tested on: 6.6
	FortiSOAR	Tested on: 7.3.2-2150
	Splunk SOAR	7.3.2-2150 or higher
EDR / Firewall	CrowdStrike EDR	Latest Falcon EDR APIs
	FortiEDR	Not applicable
	FortiEDR Manager	6.2.0 or higher
	FortiEDR Collector	5.2.0 or higher
	FortiManager	7.4.2 or higher
	FortiGate	7.4.2 or higher
Intelligence Feeds	CrowdStrike Falcon Intel	Available as Integration
	Fortinet Botnet IP List	Available to all customers.
	Internet Scan Data B (Shodan)	Available to all customers.
	Known Sinkholes	Available to all customers.
	PhishTank	Available to all customers.
	Proofpoint TAP	Available to all customers.
	Recorded Future connect	Available as Integration.

Other	ThreatConnect	Available as Integration.
	Tor Nodes	Available to all customers.
	URLHaus	Available to all customers.
	Endace	7.2.2 or higher
	Netskope	Not applicable
	Zscaler	Not applicable

Resolved issues

The following issues have been fixed in version 25.4. To inquire about a particular bug, please contact [Customer Service & Support](#).

25.4.a

Resolved an issue where error code 586 occurred when switching from an investigation with a graph chart to one without a graph chart.

Fixed an issue where Automated IR configuration did not work as expected.

Resolved an issue where users could not navigate back to the Dashboard.

Fixed an issue where the scroll bar flashed in the column picker when using Firefox.

Fixed an issue where the parent name was displayed for MITRE sub-techniques.

Resolved an issue where password fields were not masked in the integration modules.

Resolved an error handling issue in FortiAI.

25.4.0

Fixed an issue where the *Add Query* button remained disabled even after correcting IQL syntax errors.

The *Submit* button on both the Reset and Change Password pages now functions correctly and no longer appears disabled.

Removed duplicate drop-downs in the *Email Notification* page.

Resolved an issue where an incorrect dialog appeared when unmuting a detection.

Fixed an issue in the *Detection Device Timeline* where the legend for resolved detections was not displayed.

Corrected the placement of *Info* icons in the *Private Search* page.

Resolved an issue with Multi-Factor Authentication (MFA) on EU portals.

Addressed a bug where *src.mac* and *dst.mac* fields were missing from *NetFlow* event data.

25.3.c

Fixed the date range in the *Investigation Result* page.

Resolved the errors being thrown in the *Excludes* tab in the *Mutes and Excludes* page

Fixed a display issue in the account subnets list table.

Fixed the training indicators in the *Indicators* tab.

25.3.b

Description

Fixed an issue with title case for event types in the results table.

Resolved an issue where invalid IQL queries behaved inconsistently depending on how the search was initiated

Resolved an issue where using *Fit Width* on the *Timeframe* column in the Behavioral Observations page caused the column to resize only one pixel at a time.

Fixed a spelling error on the *Entity Lookup* page

25.3.a

Description

Fixed an error when pivoting to the *Detection Context* page from *Triage Detection* page.

Resolved a styling issue in the *Entity Panel* that caused the bottom of the panel to be cut off in the CrowdStrike tab.

Fixed an issue with displaying muted devices by supporting three mute options: *Mute Device for Detection*, *Mute Device for Detector*, and *Mute Device for Account*.

25.3.0

Description

Fixed the styling in the *Reports* page to align the *Report History* link and *Date* selection.

Fixed the CrowdStrike redirect URL.

Corrected the text in the CrowdStrike EDR configuration dialog.

Fixed the button styles.

25.2.c

Description

When editing a rule, the test query is skipped if no changes have been made to the query.

Resolved an issue with the filters on the *Telemetry* page.

Fixed an issue with user role assignment on account creation.

Fixed an issue with muted devices not being displayed for a detector.

The search submit button is disabled after a query is submitted until there are changes to the query.

When pivoting from a detection table, the detection timeline now scrolls to the selected detection.

Editing a detector no longer requires running the test query unless the query has been modified.

The *Sensor Telemetry* page's *Throughput* tab now shows average values (bits/sec or EPS) in the legend instead of sums, providing a more accurate view of rate-based metrics.

25.2.b

Description

Resolved an error in the *Entity Panel*.

Fixed an issue with the widgets in the *Security Posture* report.

Resolved an issue with the *Telemetry* page where the *Throughput* tab was not displaying all the sensors.

Resolved an issue with the default filters in the *Detections Table*.

The *Mute* and *Unmute* buttons in the *Triage Device* and *Detections Table* pages have been fixed.

25.2.a

Description

Fixed an issue where the *Bandwidth* chart title was getting cut off.

Resolved errors that occurred in the *Event Aggregation* table.

Corrected the sensor legend on the *Sensor Telemetry* page to display all sensors as intended.

Fixed sorting issue for timeline view in *Detection Context* page.

Fixed observation pivot from *Detection Context* when *First Seen* and *Last Seen* are the same.

25.2.0

Description

The column order in the *Column Profile* is now saved correctly.

An issue with custom widget error handling has been resolved.

25.1.e

Description

Fixed the date picker in *Sensor Telemetry* to match the date range in the graph.

An issue with creating and deleting custom filters on the *Triage Detections* page has been fixed.

The entity validation now works as designed when selecting the entity type as *Domain*.

Resolved an issue where event data with fields that have null values did not match against IQL queries using the NOT operator. This issue also affected the EXCLUDE operator.

25.1.d

Description

Fixed inconsistent date selection behavior in the *Entity Panel*

Description

Fixed broken links in the *Security Posture Report*.

The *Resolution Style* no longer displays an invalid resolution period when set to *Auto*.

25.1.c

Description

Resolved an issue with the *Column Profiles* feature.

Fixed the account picker so it does not show *All* accounts when it is not supposed to.

Resolved an issue in the *Sensor Telemetry > Visibility chart* where clicking a subnet did not do anything.

25.1.b

Description

The *Observation* tab in the *Entity Panel* no longer displays an error when selecting more than 90 days.

Fixed the *Entity Panel* so that it no longer changes the date range.

Fixed the behavior of the portal *Login* button to prevent users from clicking it more than once.

Fixed an issue with the *Resolved* filter in the *Detections Table*.

Fixed a styling issue in the *Entity Lookup* page.

25.1.a

Description

Resolved an issue where the *Visualizer* was not updating after searching for an IP.

Fixed the tool tip content in the *Sensor* widget.

Fixed the tool tip for the context fields in the *Observations* instance table.

Fixed the tooltip message in the *Accounts* and *Software* tabs.

25.1.0

Description
Resolved an issue with the <i>API Only</i> filter in the <i>Account Management</i> page.
The <i>Detections Table</i> no longer displays a timestamp in the <i>Mute Comment</i> column.
Resolved an issue with role assignment during account creation for EU portals.
Events that are older than 90 days no longer generate an error in the <i>Entity Panel</i> .

Known issues

The following issues have been identified in version 25.4. To inquire about a particular bug or report a bug, please contact [Customer Service & Support](#).

25.4.a

Description
Natural Language queries • Fields with <i>null</i> values are not included in aggregation results. • In certain cases, Event searches are incorrectly converted into aggregations. • Queries on array fields such as <code>intel</code> or <code>dns.answers</code> return inconsistent or no results.



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.