

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	7
Version history	8
Version 25.4.a	9
New functionality	9
Natural Language Queries	9
FortiAI	11
Device enrichment	12
Gen AI Dashboard	13
Improved functionality	16
Entity panel	16
Sensors page	17
Sensor metrics	18
Detections table	19
Detection resolution comments	19
Investigation results	19
FortiNDR Essentials Solution Pack v1.0.1	20
Other improvements	21
Version 25.4.0	22
New functionality	22
Fortinet Automation Service	22
Improved functionality	23
Default dashboard	23
Detection device timeline	24
Event fields	25
Other improvements	26
Version 25.3.c	27
New functionality	27
DPI Dashboards	27
Improved functionality	31
Reports	31
Entity panel	31
Other improvements	32
Version 25.3.b	33
New functionality	33
Mutes and Excludes page	33
Detections Device Timeline	35
NetFlow events	39
DPI events	40
Improved functionality	41
Impacted device filter	41
Notification emails	41
Single Event View	42
Notable detections	43
Sensor details	43

Bulk subnet imports	44
Annotations	44
Shared dashboards	45
Other improvements	45
Investigation Summary field	45
Data sources	45
Network Security Posture Report	46
Deprecated features	46
Version 25.3.a	47
Version 25.3.0	48
Deprecation notice	48
Other improvements	48
Version 25.2.c	49
New functionality	49
Improved functionality	53
Other improvements	56
Version 25.2.b	60
Improved functionality	60
Sensors	60
Detection context	62
Other improvements	63
Version 25.2.a	64
Version 25.2.0	65
New functionality	65
Detections table	65
Improved functionality	68
Sensor telemetry	68
IQL queries	70
Other improvements	70
Version 25.1.e	72
New functionality	72
Custom dashboards	72
Detections	74
Improved functionality	76
Investigations	76
IQL queries	78
Detections	79
Other improvements	79
Sensors	79
Encryption keys	79
Version 25.1.d	80
Improved functionality	80
Reports	80
Other improvements	83
Detectors	83

Entity lookup	83
Search and Private Search	83
Version 25.1.c	84
New functionality	84
Reports	84
Improved functionality	86
Sensors	86
Other improvements	87
Portal	87
Deprecated functionality	87
Dashboard	87
Version 25.1.b	88
Improved functionality	88
Integrations	88
Account management	88
Sensors	89
Version 25.1.a	91
New functionality	91
Integrations	91
Investigations	93
Improved functionality	94
Reports	94
Behavioral observations	95
Integrations	95
Other improvements	96
Version 25.1.0	97
New functionality	97
SNMP event fields	97
Entity Panel	98
Improved functionality	99
Global Search	99
Other improvements	99
Product integration and support	100
Resolved issues	102
25.4.a	102
25.4.0	102
25.3.c	103
25.3.b	103
25.3.a	103
25.3.0	104
25.2.c	104
25.2.b	104
25.2.a	105
25.2.0	105
25.1.e	105

25.1.d	105
25.1.c	106
25.1.b	106
25.1.a	106
25.1.0	107
Known issues	108
25.4.a	108

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 9
05 November 2025	Version 25.4.0 on page 22
15 September 2025	Version 25.3.c on page 27
03 September 2025	Version 25.3.b on page 33
15 July 2025	Version 25.3.a on page 47
07 July 2025	Version 25.3.0 on page 48
26 June 2025	Version 25.2.c on page 49
21 May 2025	Version 25.2.b on page 60
08 May 2025	Version 25.2.a on page 64
30 April 2025	Version 25.2.0 on page 65
26 March 2025	Version 25.1.e on page 72
12 March 2026	Version 25.1.d on page 80
27 February 2025	Version 25.1.c on page 84
12 February 2025	Version 25.1.b on page 88
29 January 2025	Version 25.1.a on page 91
08 January 2025	Version 25.1.0 on page 97

Version 25.4.a

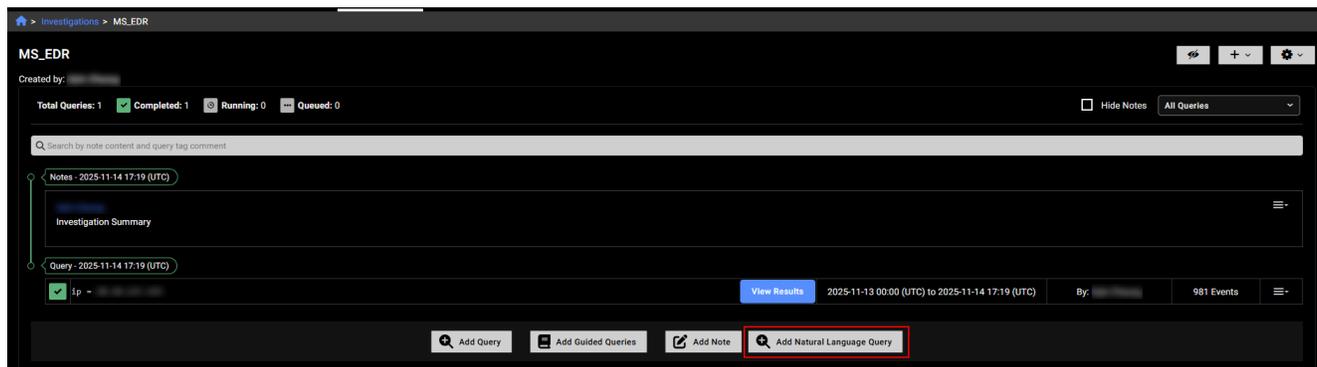
- New functionality
 - Natural Language Queries
 - FortiAI
 - Device enrichment
 - Gen AI Dashboard
- Improved functionality
 - Entity panel
 - Sensor metrics
 - Sensors page
 - Detections table
 - Detection resolution comments
 - Investigation results
 - FortiNDR Essentials Solution Pack v1.0.1
- Other improvements
- Resolved issues on page 102

New functionality

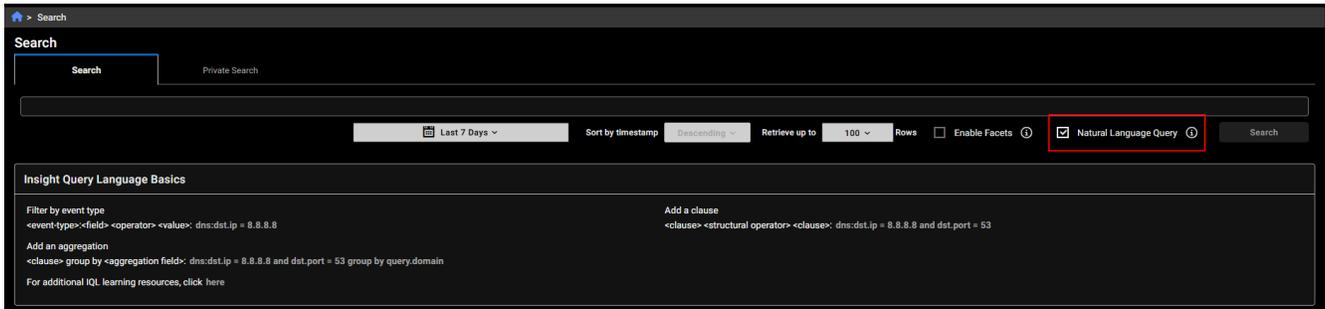
Natural Language Queries

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](#).

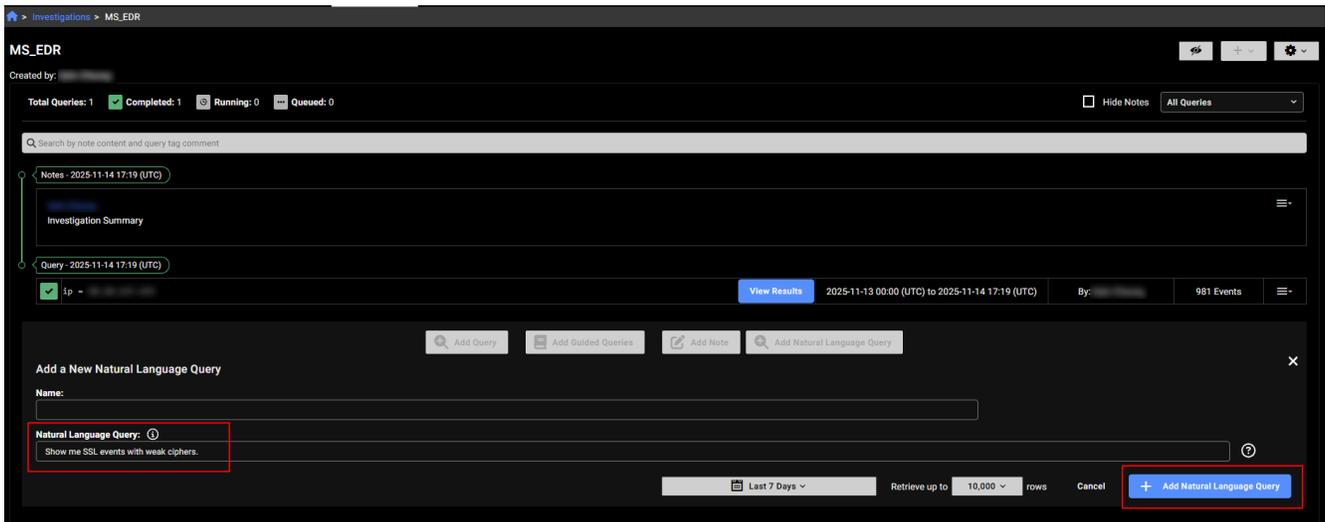
To use an NL query in an investigation, click the *Add Natural language Query* button the investigations details page.



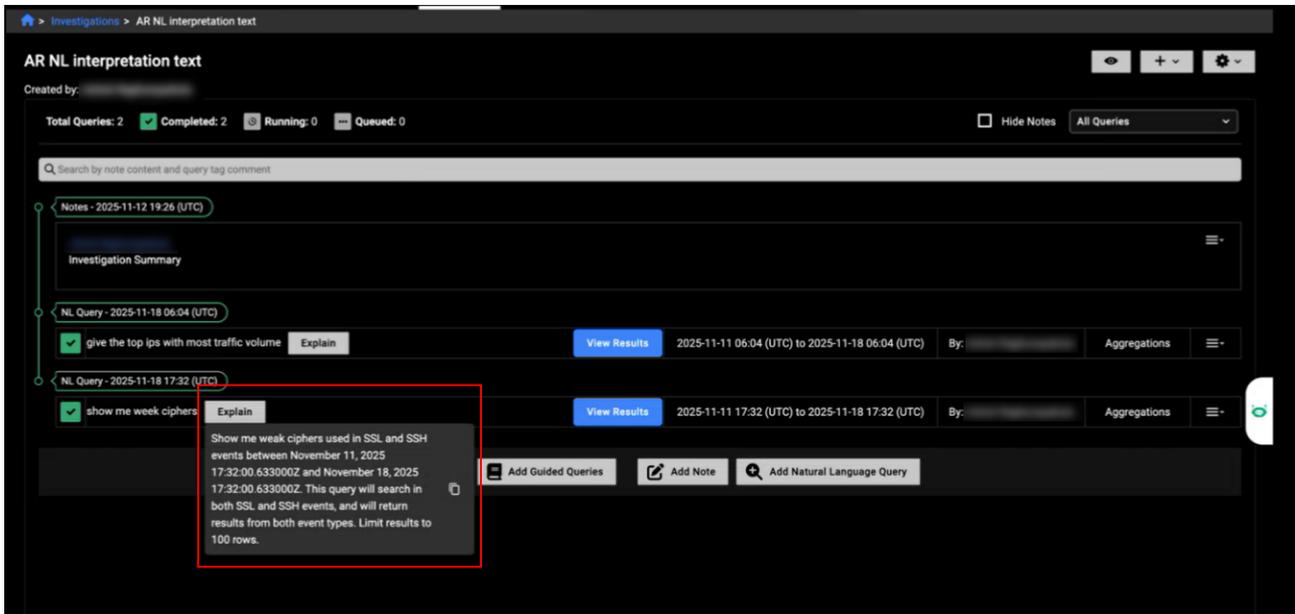
To use an NL query in *Private Search*, enable *Natural Language Query* at the top of the page.



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*.



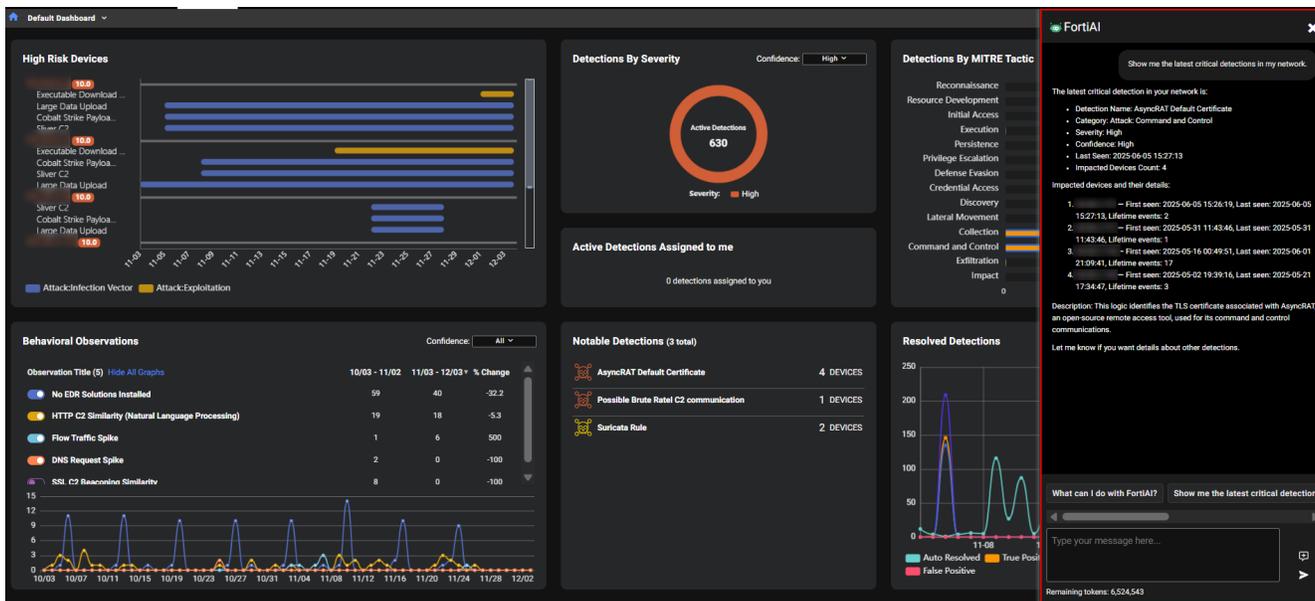
FortiAI

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.



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 search query is `event_type = 'flow' and dst_device_os_name <=> null`. The results are sorted by timestamp descending, showing 96 events. The table columns include: tag, type, timestamp, src, src_ip, dst, intel, exe_action, exe_interface_id, exe_verst..., duration, flow_state, and proto. A column configuration panel is open on the right, showing a search for 'device' and a list of columns to be added, including `dst.device_data.timestamp`, `dst.device_hostnames.domain...`, `dst.device_hostnames.fqdn`, `dst.device_hostnames.name`, `dst.device_hostnames.seconds...`, `dst.device_last_logoff`, `dst.device_last_logon`, `dst.device_os_name`, and `dst.device_os_name_with_verst...`.

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

The screenshot shows the sensor details page for 'Sensor Test'. The sensor is online. The connection status is 'Online'. The device enrichment status is 'Unknown'. The page displays various metrics including CPU (4.75%), MEMORY (39.53%), EPS (0 eps), and BITS/S (53.295 Kb/s). The last run time is 2025-12-09 16:53 (UTC) and the last upload time is 2025-12-09 16:53 (UTC). The message indicates: 'Done looking up AD information and found 23962/47984 computers are available; Done looking up DNS information for 17472 devices'. The interfaces section shows two interfaces: ens192 (7.875 Kb/s) and ens224 (0 b/s).

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.

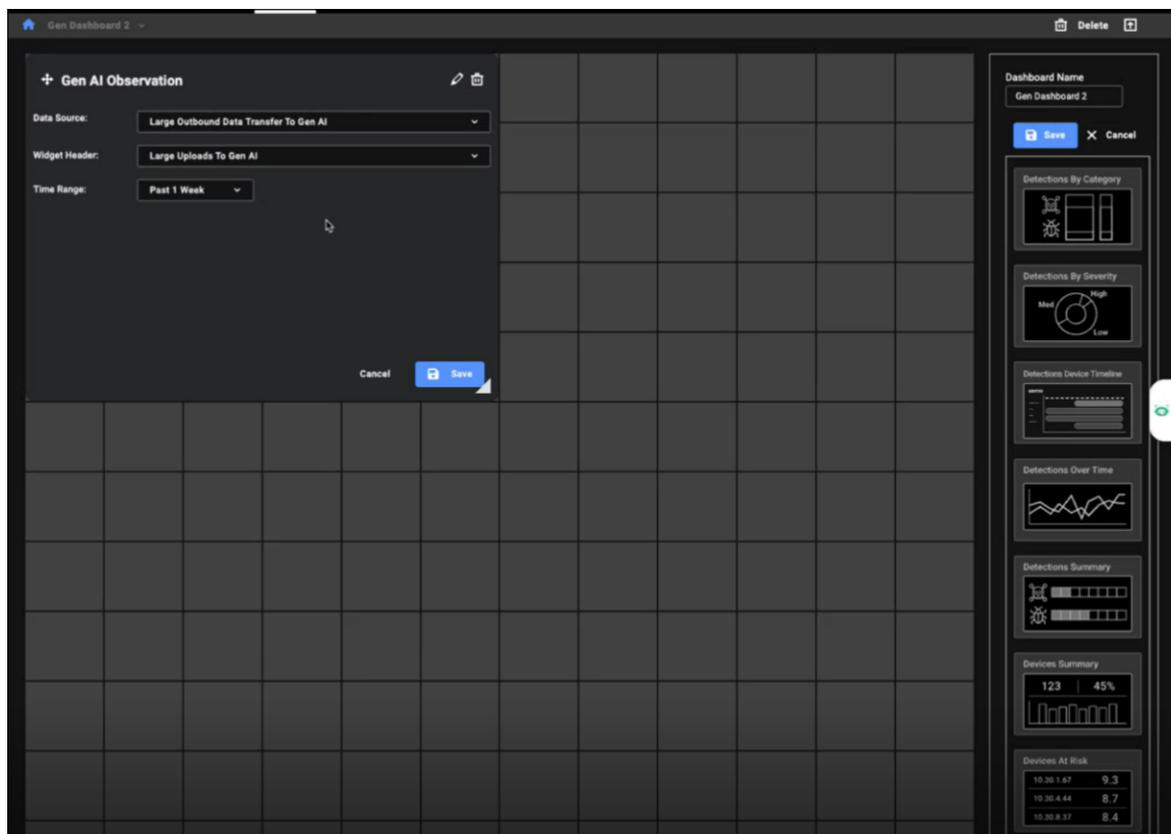
You can use the widgets in this dashboard to track which AI providers are accessed and by which devices and identify large uploads and frequent connections that may indicate risky behavior.

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> .



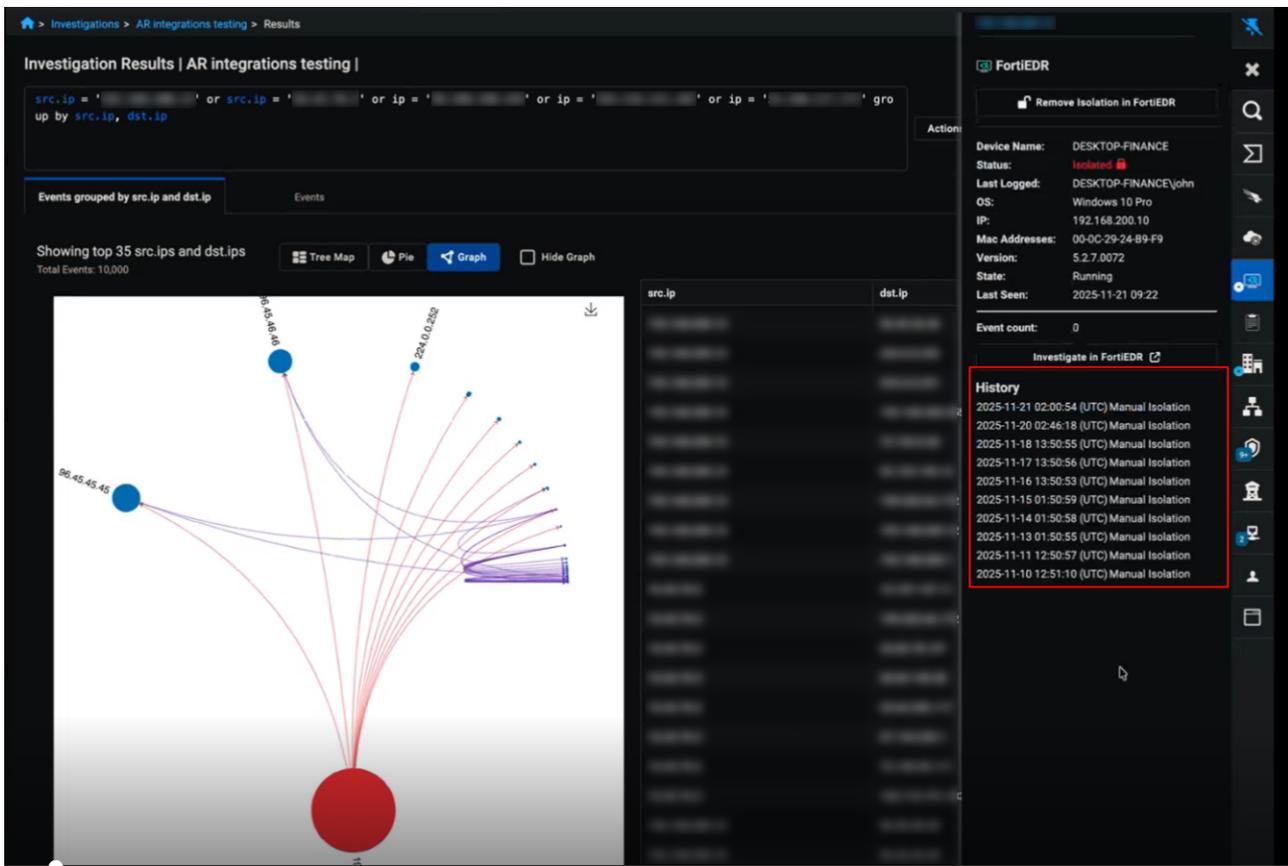
You can also create a custom dashboard based on the Gen AI widgets.



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.

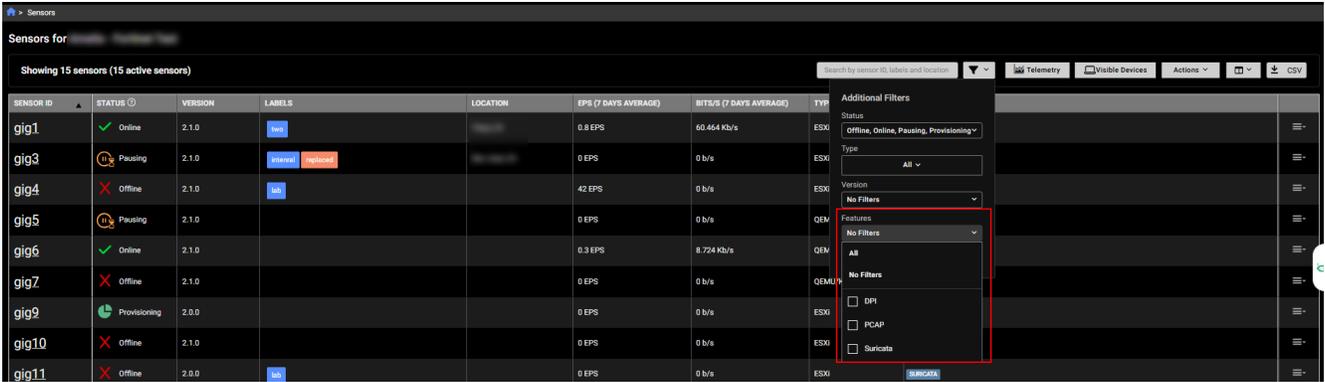


Sensors page

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.

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	EPS (7 DAYS AVERAGE)	BITS/S (7 DAYS AVERAGE)	TYPE	Features
gig1	Online	2.1.0	net		0.8 EPS	60.464 Kb/s	ESXI	PCAP, SURICATA
gig3	Pausing	2.1.0	internal, external		0 EPS	0 b/s	ESXI	SURICATA
gig4	Offline	2.1.0	net		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.



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:

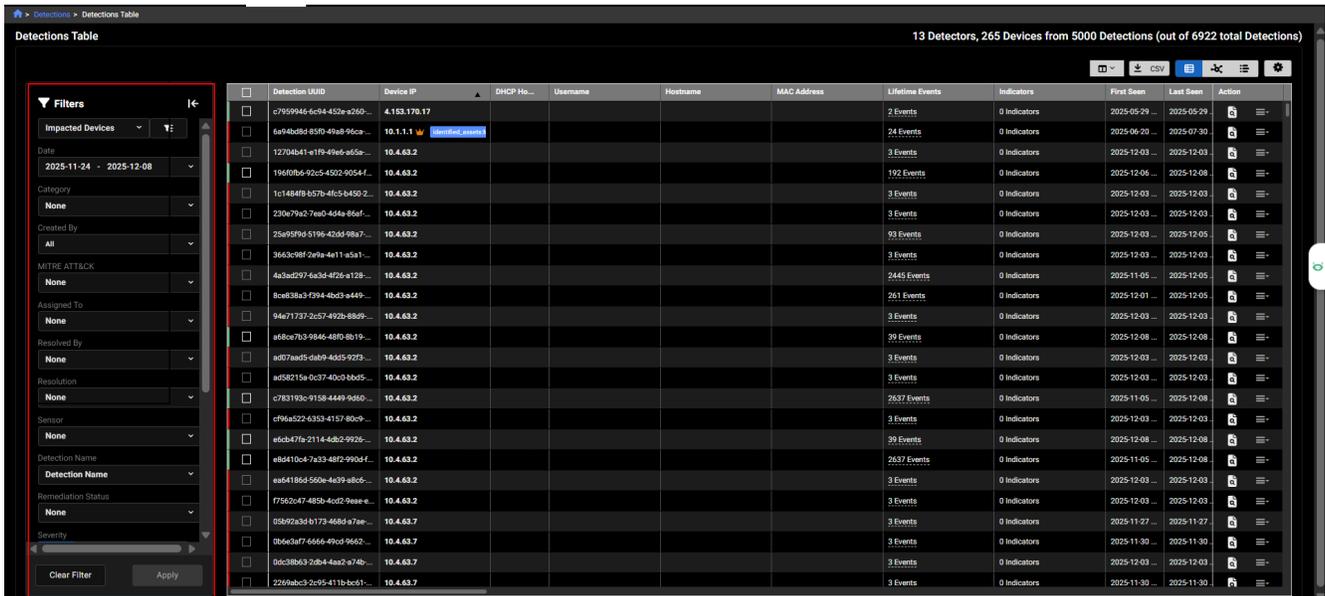
- Green if usage is 0-59%
- Yellow if usage exceeds 60%
- Red if usage exceeds 90%

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

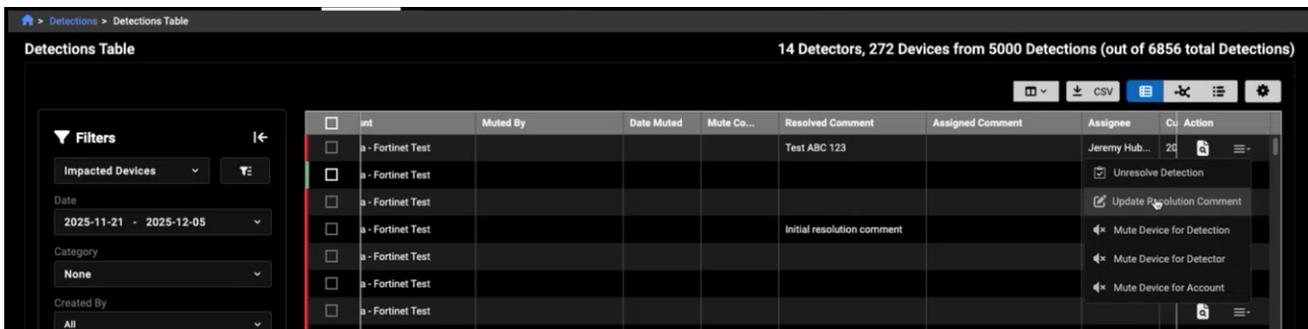
The filters in the *Detections Table* have been redesigned as a collapsible pane on the left side of the page. This allows you to select all filters at once before applying them, reducing the number of page refreshes. To remove all filters, simply click *Clear All*. This update was also applied to graph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



The screenshot shows the 'Detections Table' interface. On the left, there is a 'Filters' pane with various dropdown menus for filtering detections, including 'Impacted Devices', 'Date', 'Category', 'Created By', 'MITRE ATTACK', 'Assigned To', 'Resolved By', 'Resolution', 'Sensor', 'Detection Name', 'Remediation Status', and 'Severity'. The main table displays columns for Detection UUID, Device IP, DHCP No., Username, Hostname, MAC Address, Lifetime Events, Indicators, First Seen, Last Seen, and Action. The table shows 13 detectors and 265 devices from 5000 detections.

Detection resolution comments

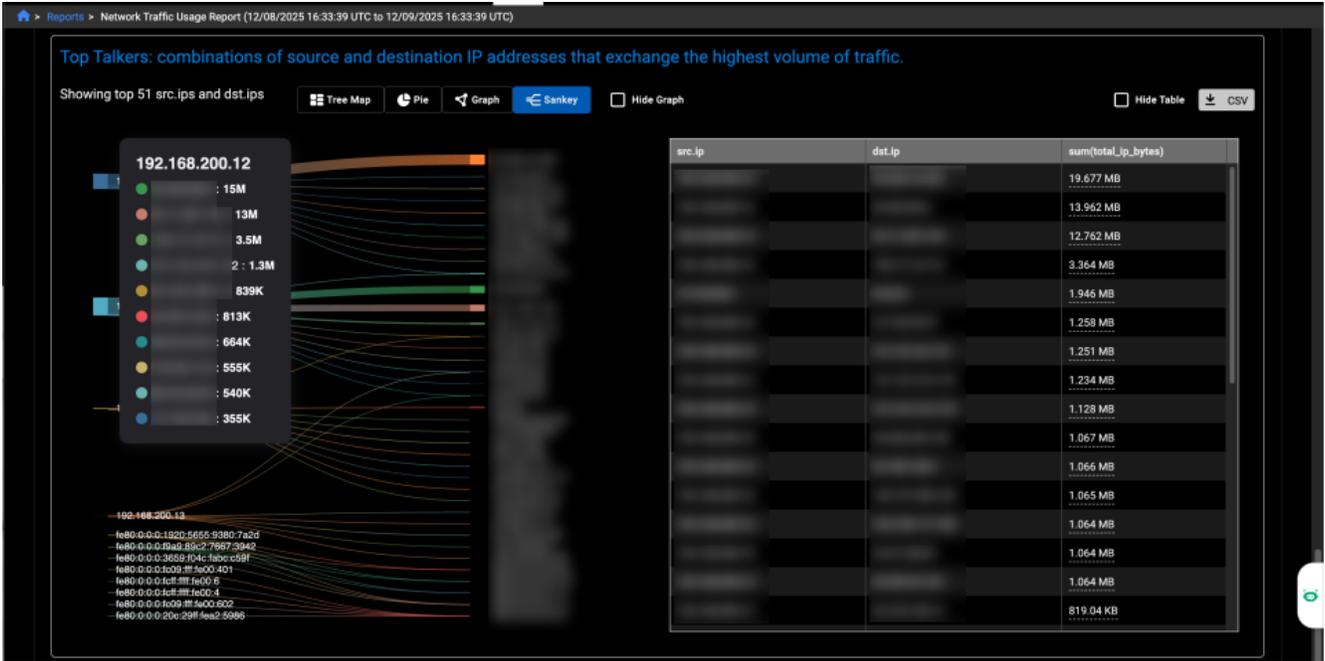
We have also added the ability to update the resolution comment directly from the *Actions* menu.



The screenshot shows the 'Detections Table' interface with a table of detection records. The table has columns for 'Muted By', 'Date Muted', 'Mute Co...', 'Resolved Comment', 'Assigned Comment', 'Assignee', and 'Cu'. The 'Resolved Comment' column contains text like 'Test ABC 123' and 'Initial resolution comment'. The 'Actions' column shows a menu with options like 'Unresolve Detection', 'Update Resolution Comment', 'Mute Device for Detection', and 'Mute Device for Account'.

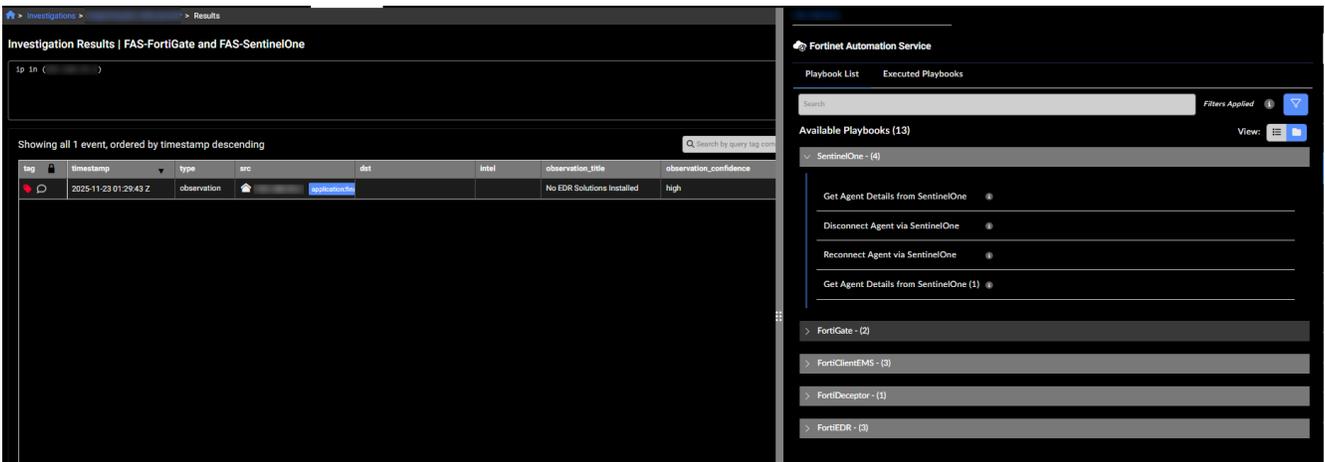
Investigation results

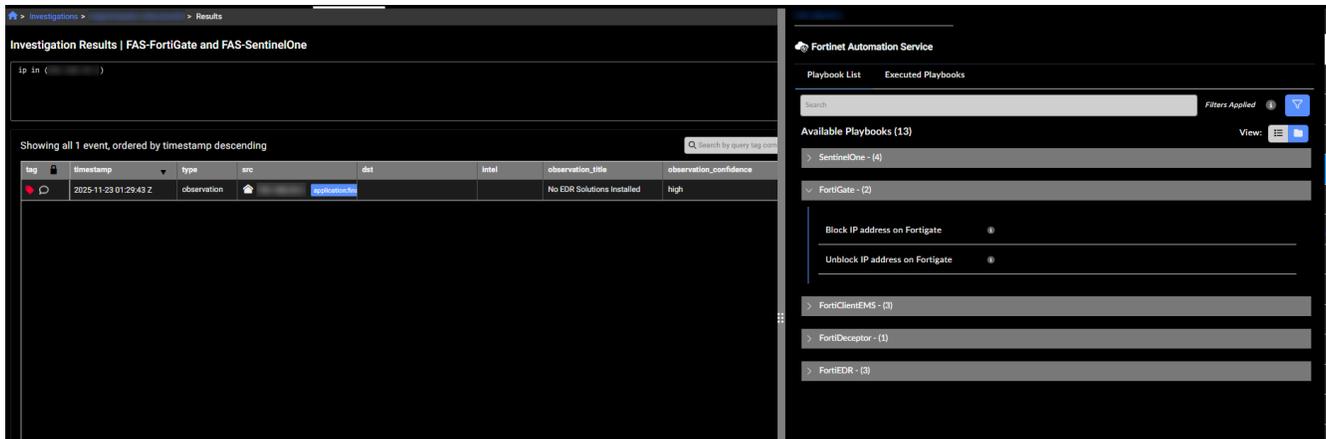
A new *Sankey* chart has been added to the investigation results and the *Network Traffic Usage* report. It is available for aggregations where *Group By* includes two IP fields or when there are two dimensions and a measure. The Sankey chart type appears only when there are 50 or fewer dimensions.



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 102

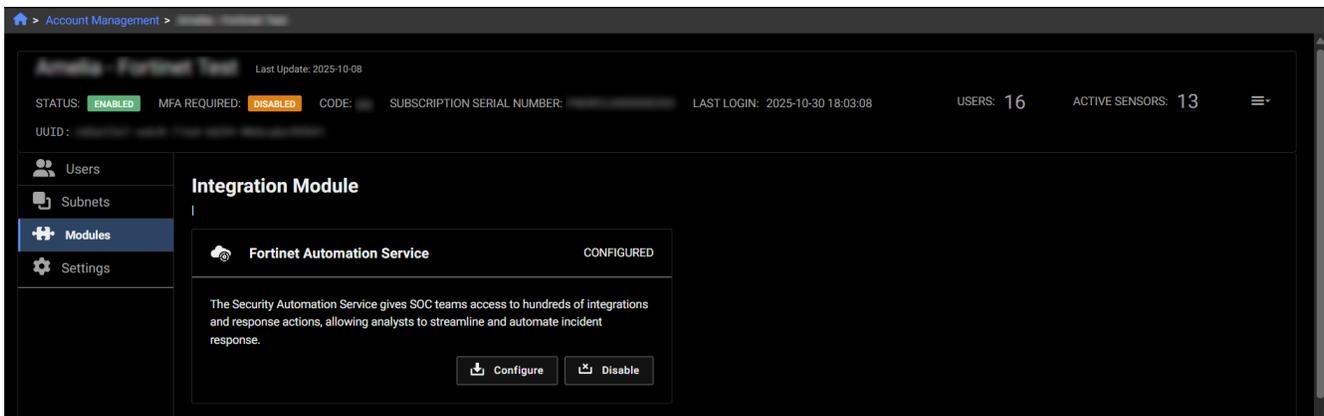
New functionality

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.

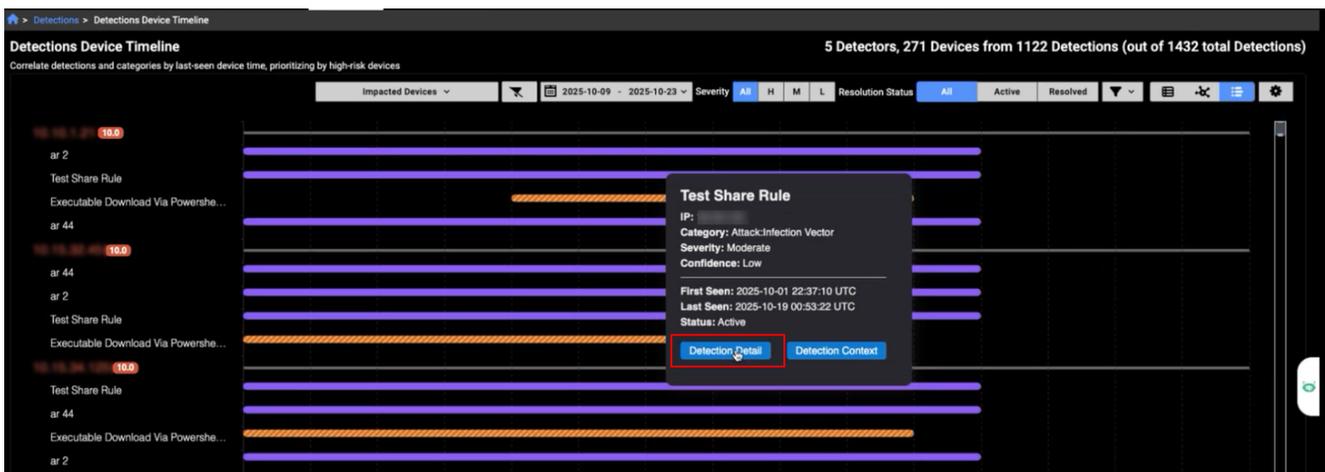
Key improvements:

- 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 102

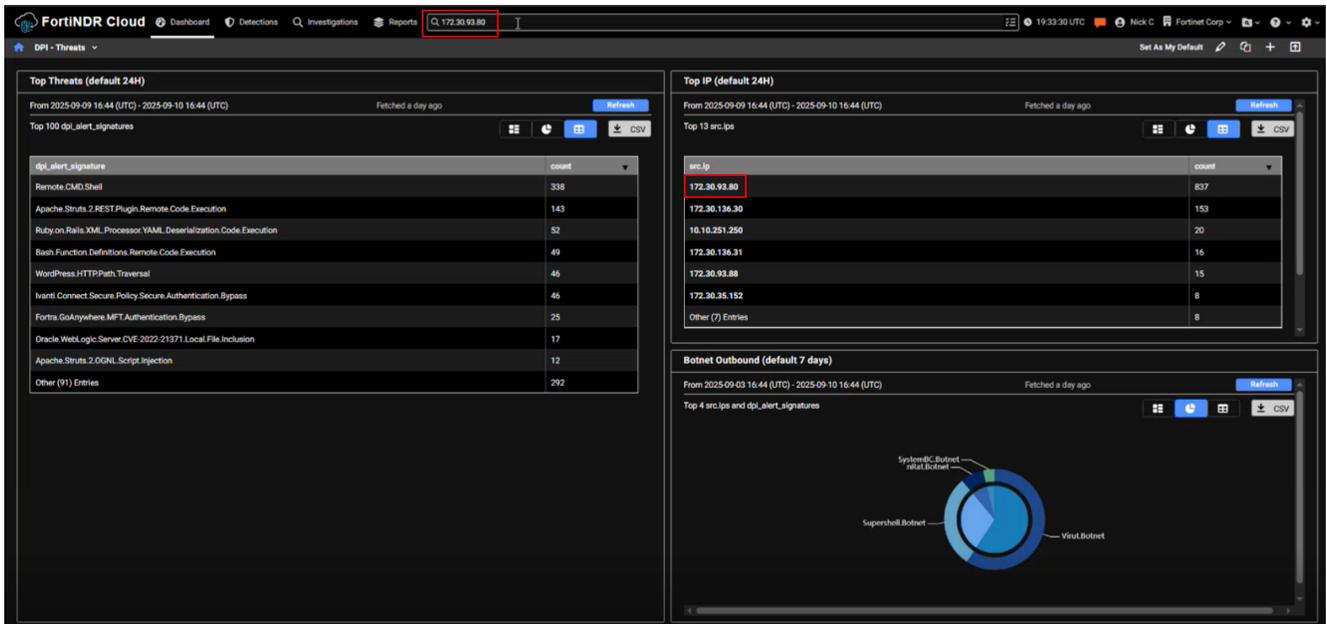
New functionality

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

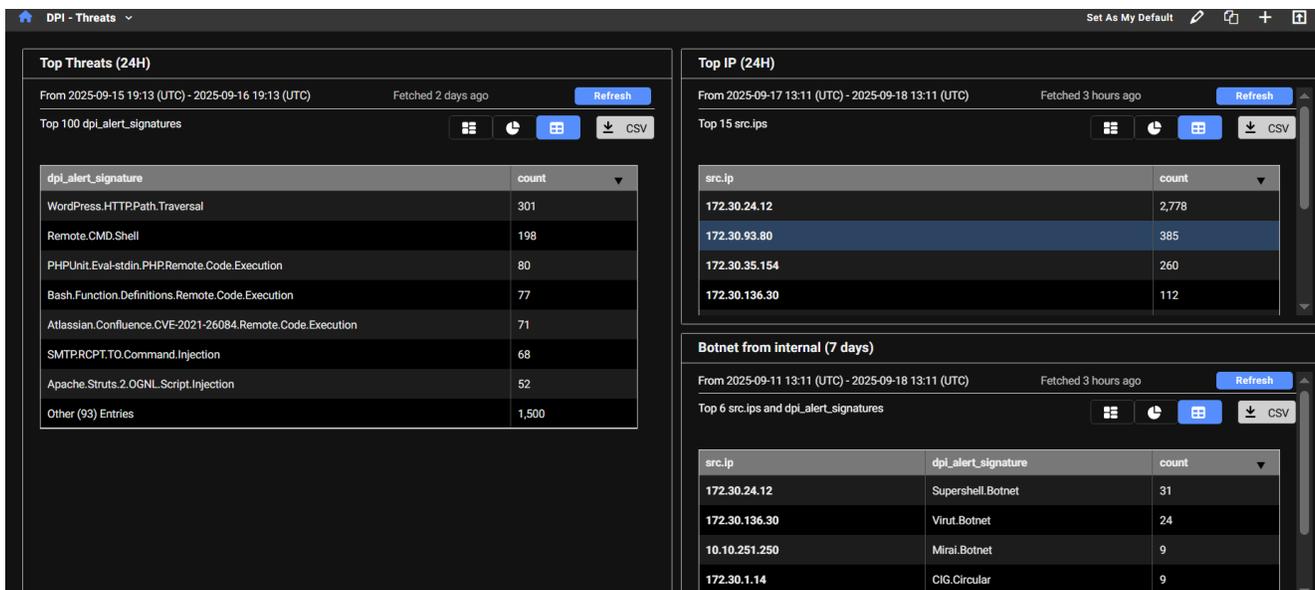
This monitor queries high-severity IDS alerts (severity level 4) detected by DPI, where either the source or destination is internal. It excludes alerts triggered by device tagged as *Scan* and *Nessus* and filters out two noisy Apache-related signatures. The results are grouped by alert signature, helping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

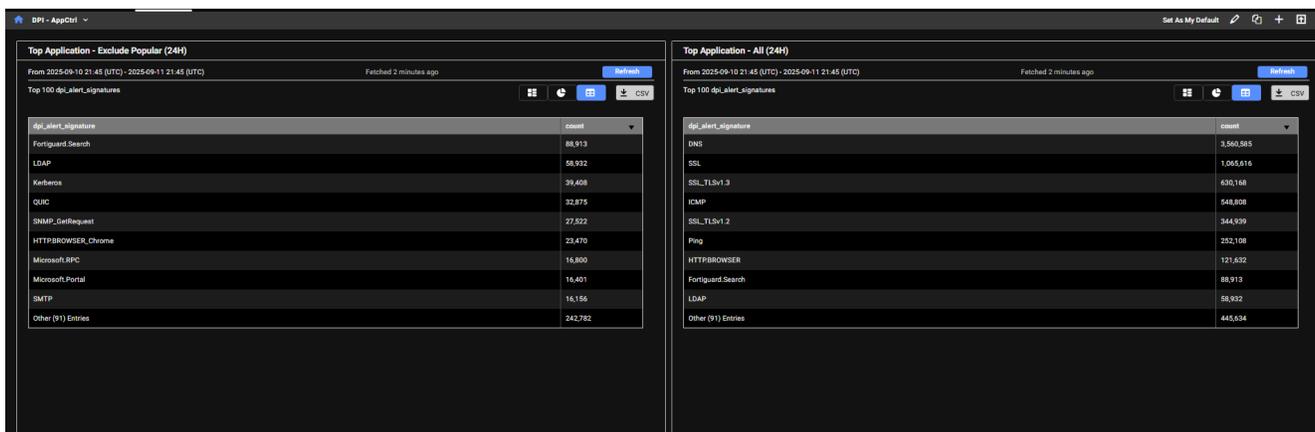
This monitor identifies outbound botnet-related DPI alerts where the source IP is internal. It groups the results by both the internal source IP and the specific botnet signature that was triggered, helping pinpoint which internal hosts are attempting to communicate with known botnets.



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.

<p>Top Application - Exclude Popular (24H)</p>	<p>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</p>
<p>Top Application - All (24H)</p>	<p>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.</p>



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.

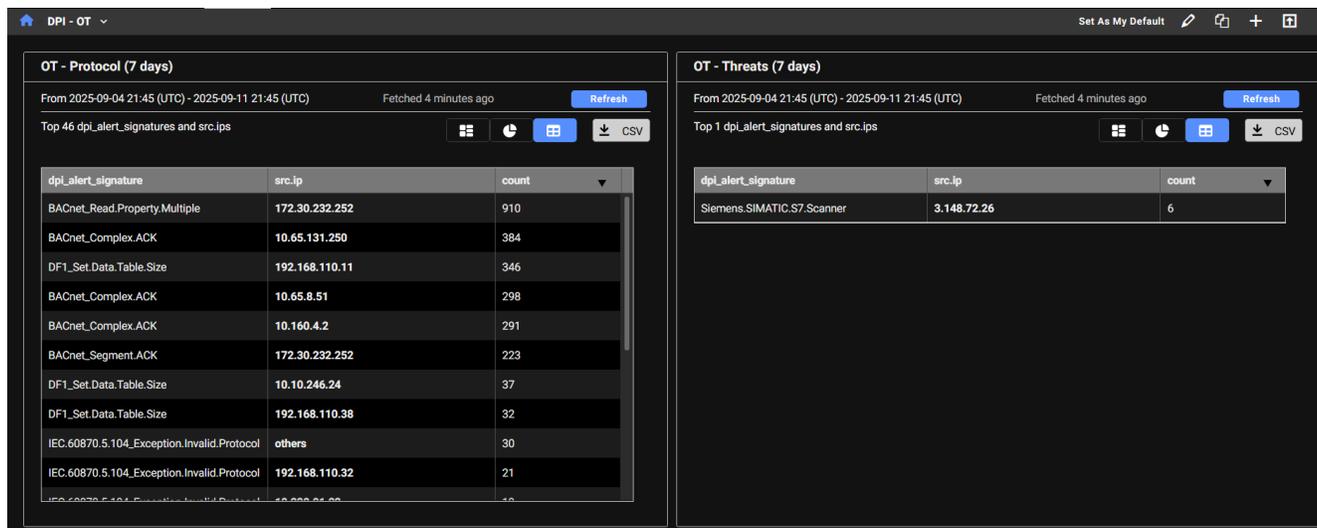
OT Threats

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.

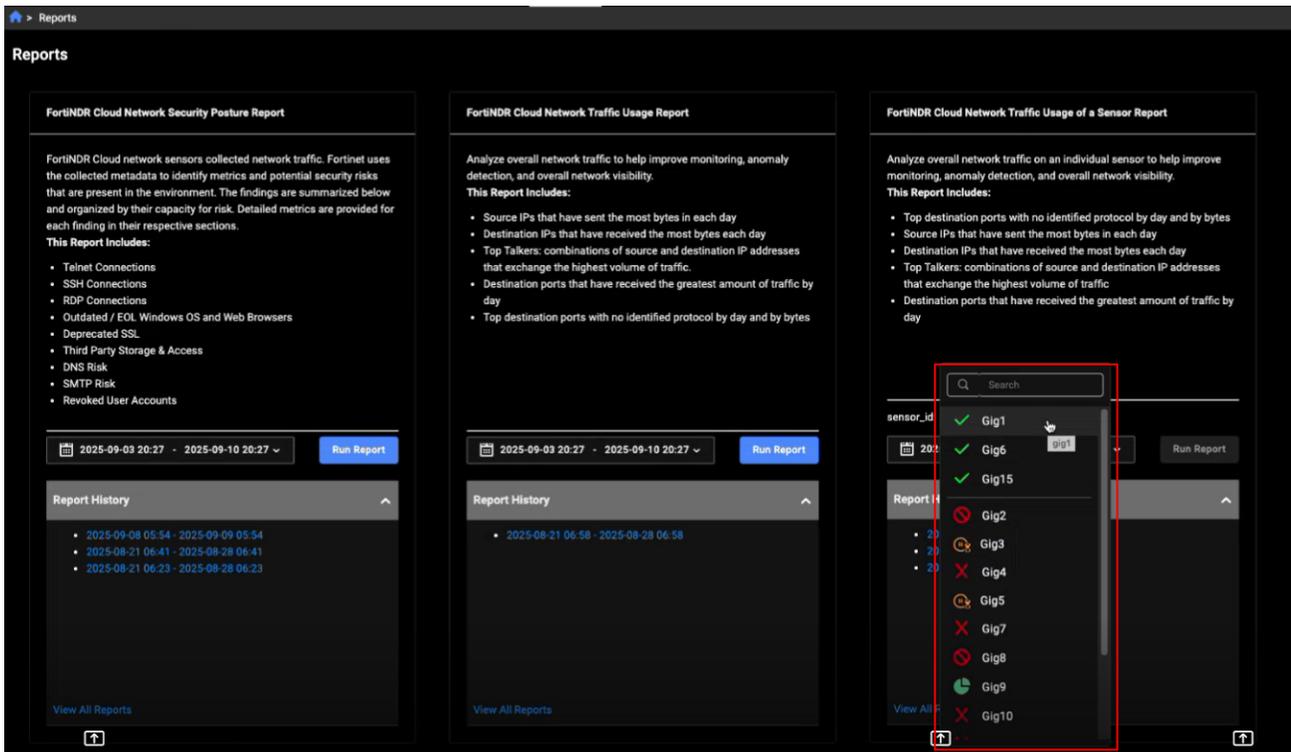
This helps in monitoring and investigating potential compromises or unauthorized access attempts within industrial environments.



Improved functionality

Reports

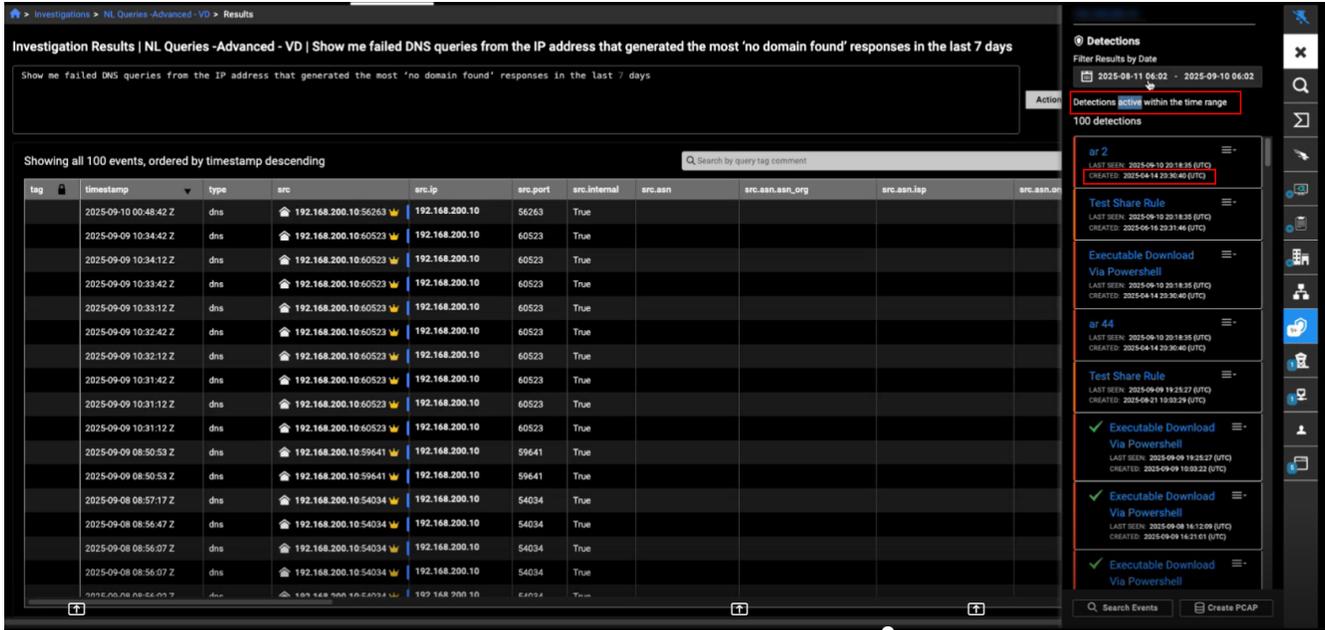
We've updated the *sensor_id* filter in the *FortiNDR Cloud Network Traffic Usage of a Sensor Report* and *Detections* list page to a dropdown menu that displays all sensors in the account. The dropdown is divided into two groups: online sensors appear at the top, while other statuses are listed below. 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.



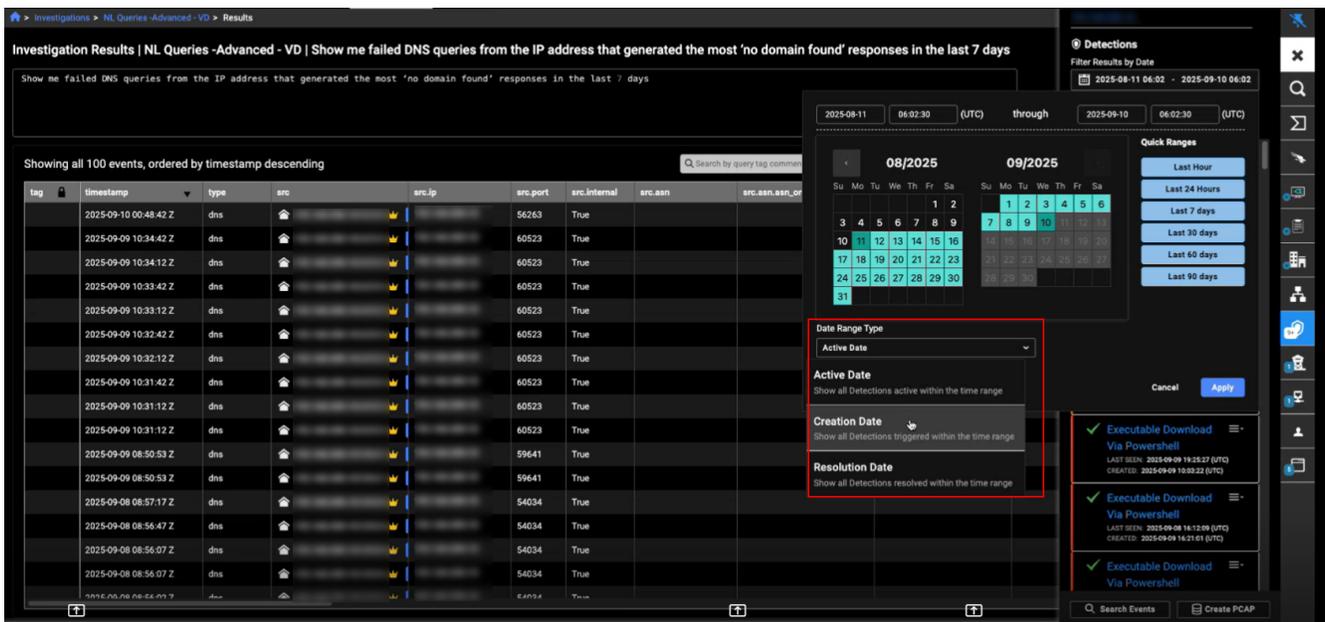
Entity panel

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.

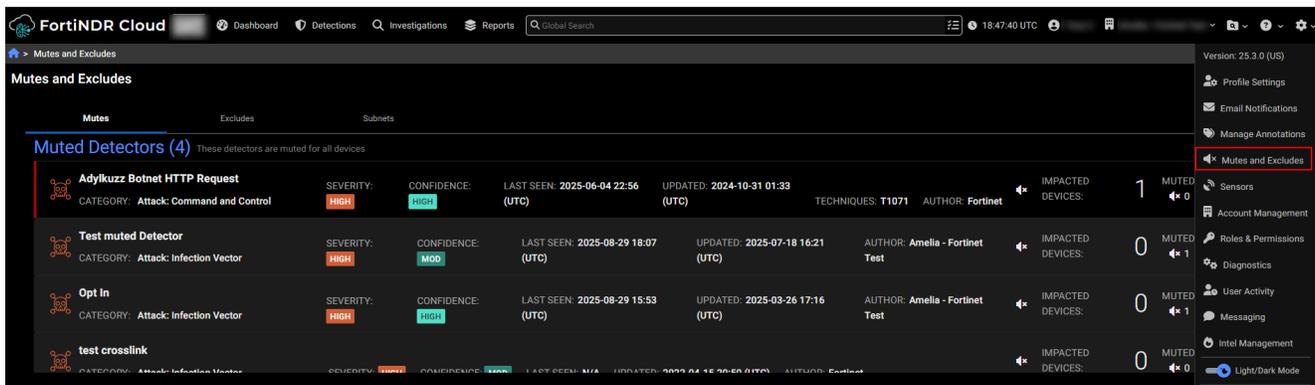
Version 25.3.b

- New functionality on page 33
 - Mutes and Excludes page on page 33
 - Detections Device Timeline on page 35
 - NetFlow events on page 39
 - DPI events on page 40
- Improved functionality on page 41
 - Impacted device filter on page 41
 - Notification emails on page 41
 - Single Event View on page 42
 - Notable detections on page 43
 - Sensor details on page 43
 - Bulk subnet imports on page 44
 - Annotations on page 44
 - Shared dashboards on page 45
- Other improvements on page 45
 - Investigation Summary field on page 45
 - Data sources on page 45
 - Network Security Posture Report on page 46
- Deprecated features
- Resolved issues on page 102

New functionality

Mutes and Excludes page

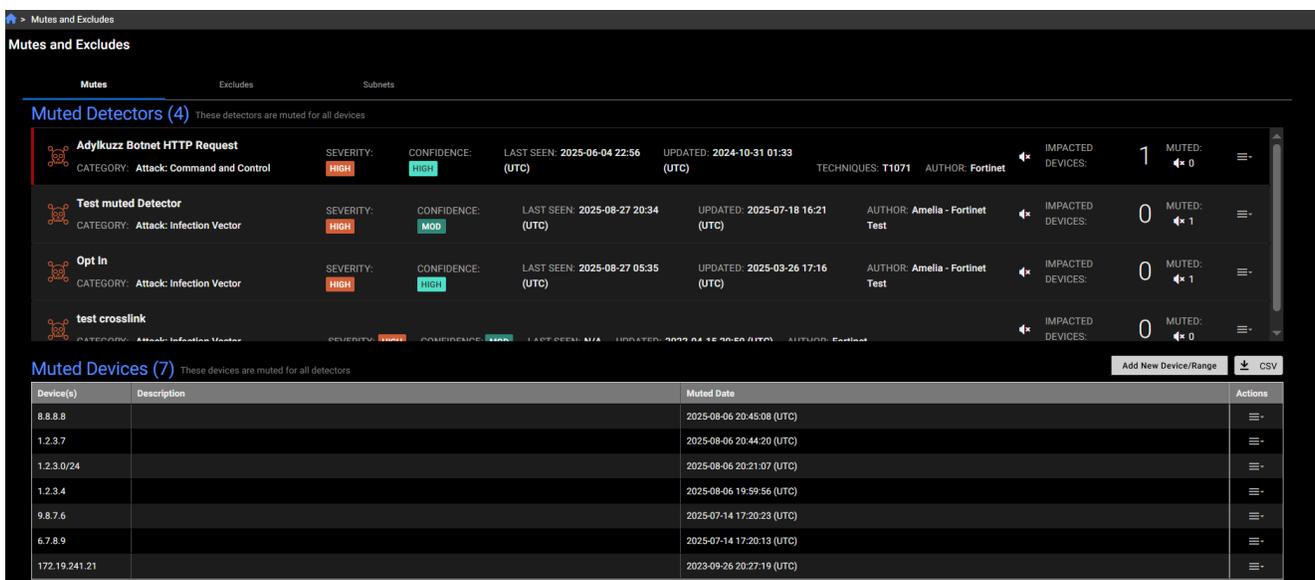
A new *Mutes and Excludes* page has been added to the main settings menu. This page summarizes all muted and excluded devices, including device-level mutes for detectors. It contains three tabs: *Mutes*, *Excludes* and *Subnets*.



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.



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

Mutes **Excludes** Subnets

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

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)

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

Mutes and Excludes

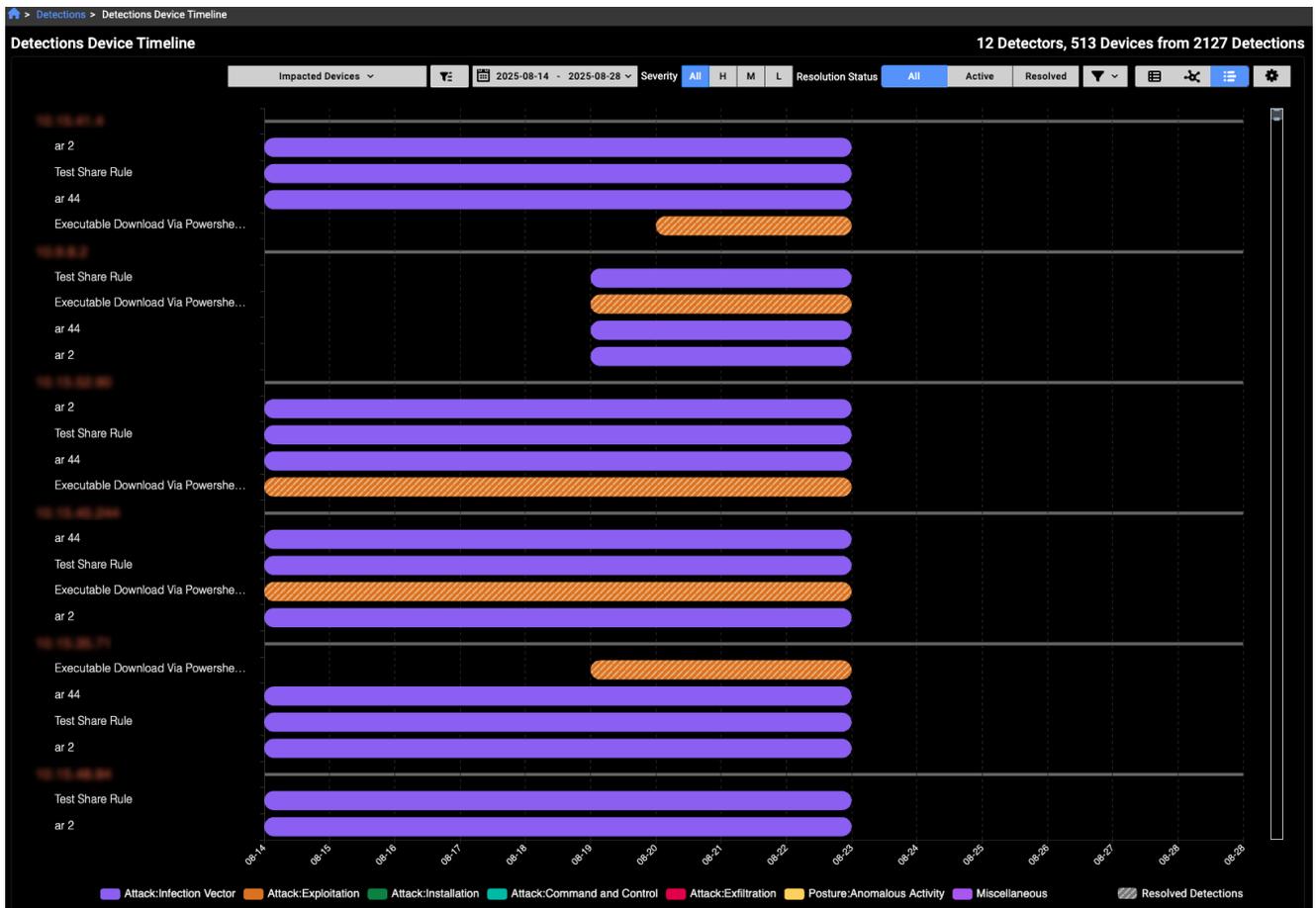
Mutes Excludes **Subnets**

Internal Subnets (8) All internal subnets for account. Detections will only be created when impacted device is within an internal subnet

Subnet	Description	External
	Default RFC 1918 subnet	No
	Default RFC 1122 subnet	No
	Default RFC 3927 subnet	No
	Default RFC 1918 subnet	No
	Reza-test	No
	roza-external	Yes
	Default RFC 1918 subnet	No
	Default RFC 5771 subnet	No

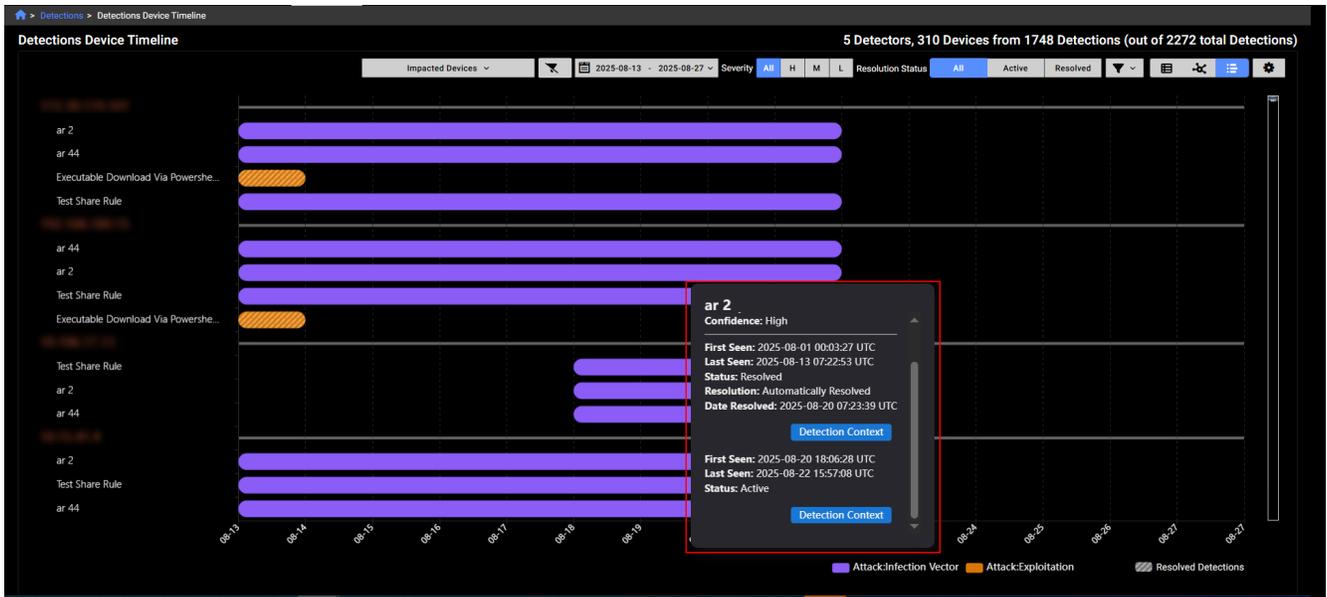
Detections Device Timeline

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

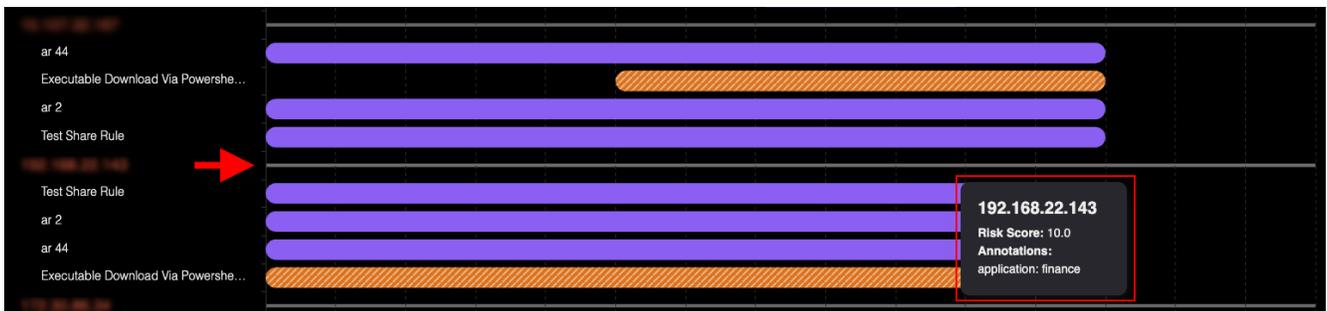


A solid background color in each bar on the chart represents a detection category, as indicated in the legend at the bottom of the page. If a bar is striped, it means all detections within that range have been resolved. Note that a single bar does not correspond to one detection; instead, it may represent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



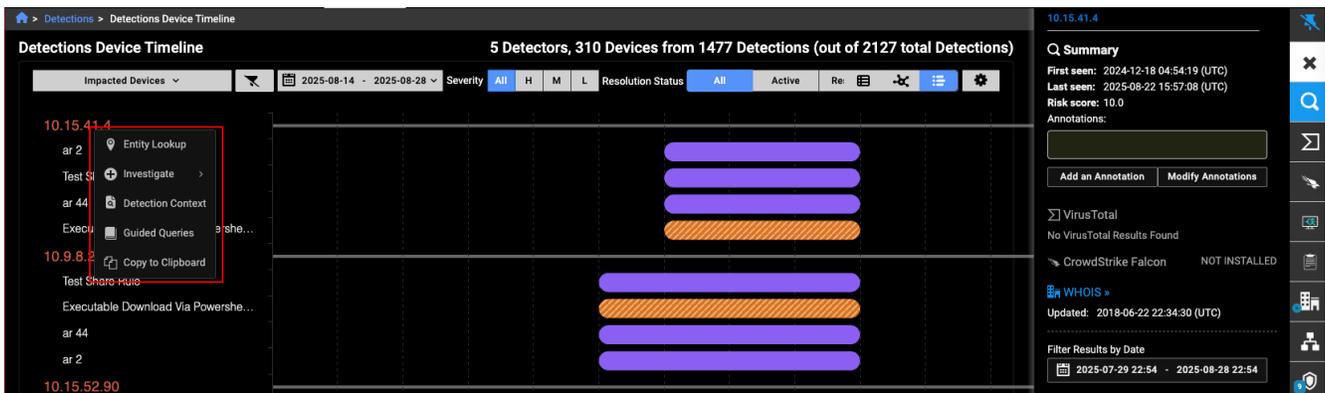
Hover over the line next to the IP label to view its risk score. Any annotations related to the IP will be displayed here



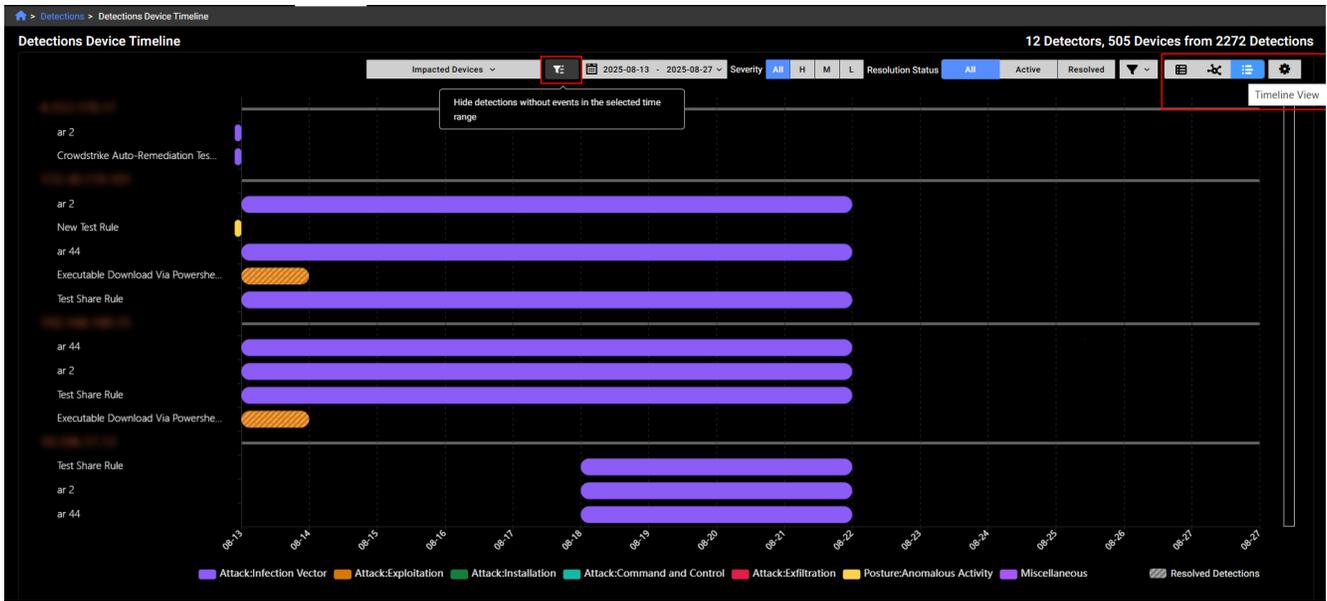
Left-click the IP label to open the *Entity Panel*.



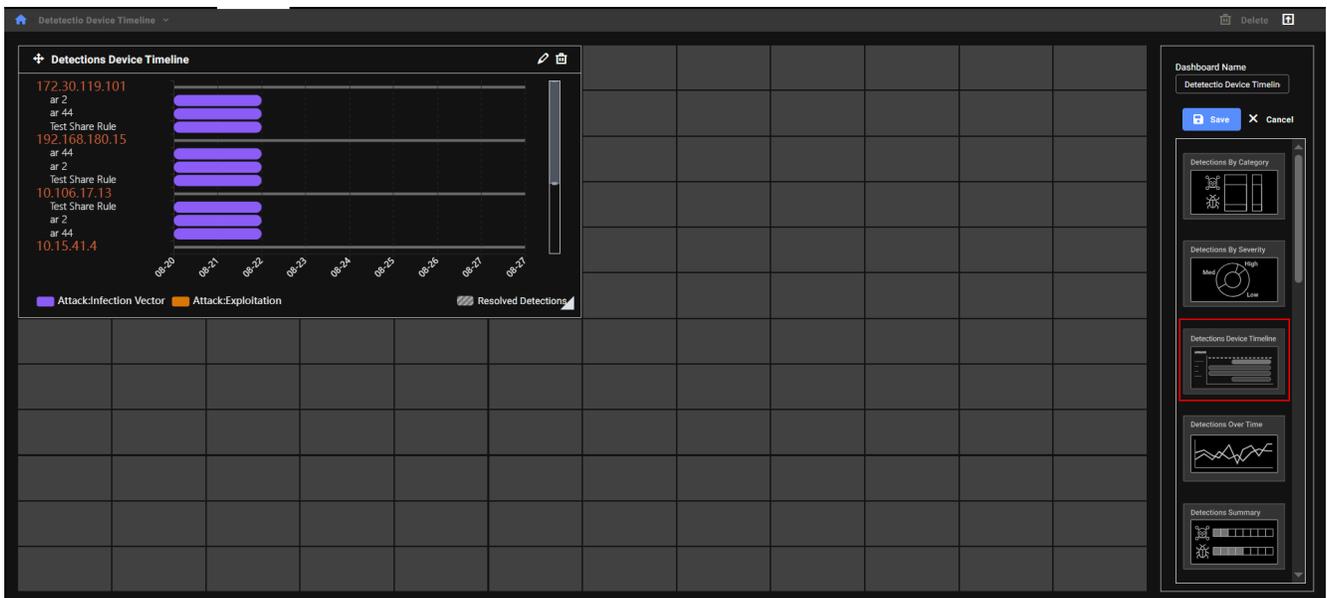
Right-click the IP label to open the context menu.



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 | Phuong (netflow) |

sensor_id = 'sentest288' 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

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`

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

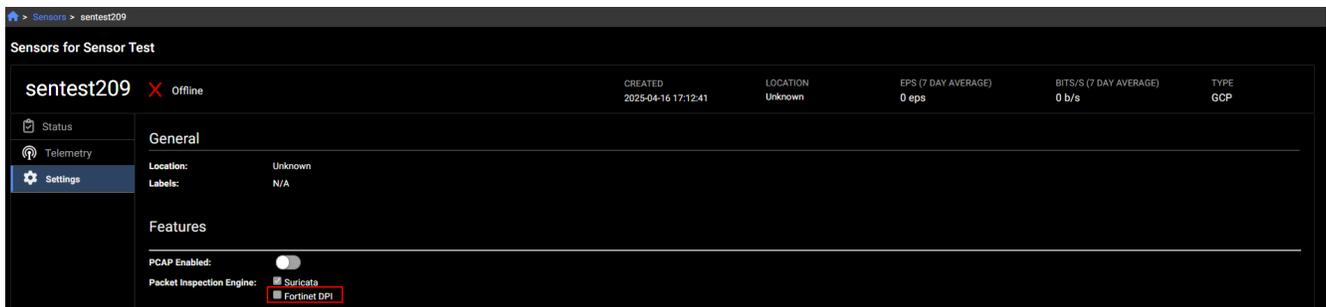
Add:

- `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`

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

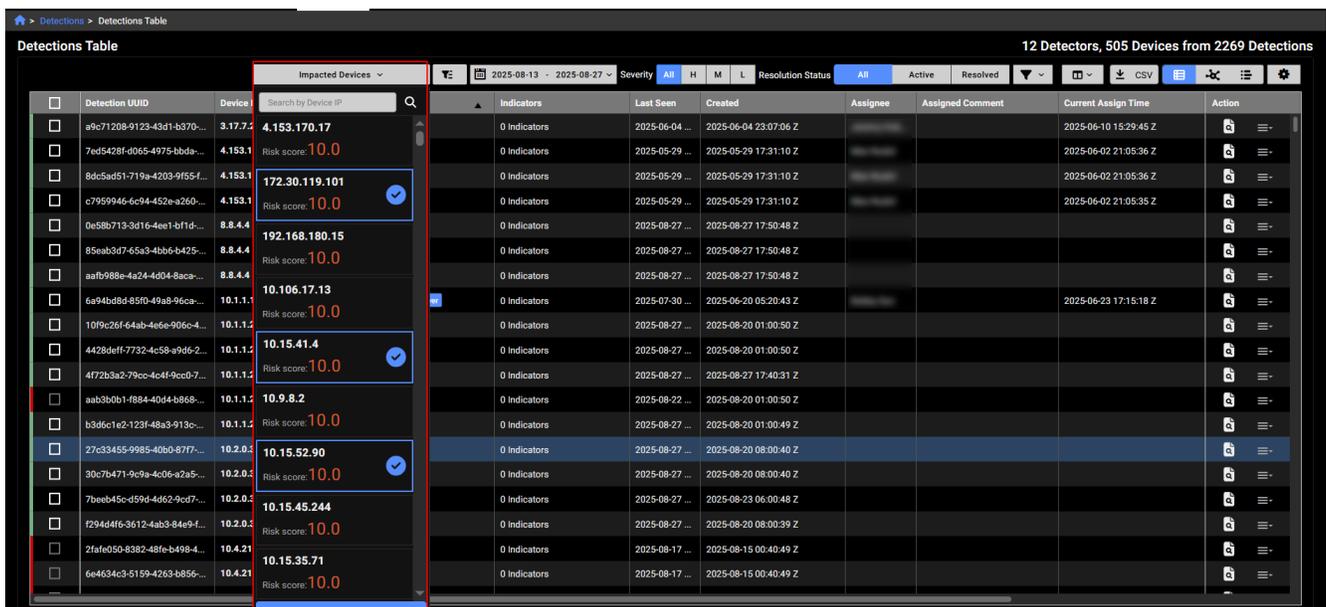
To enable DPI events, go to the sensor's *Settings* and select *Fortinet DPI*.



Improved functionality

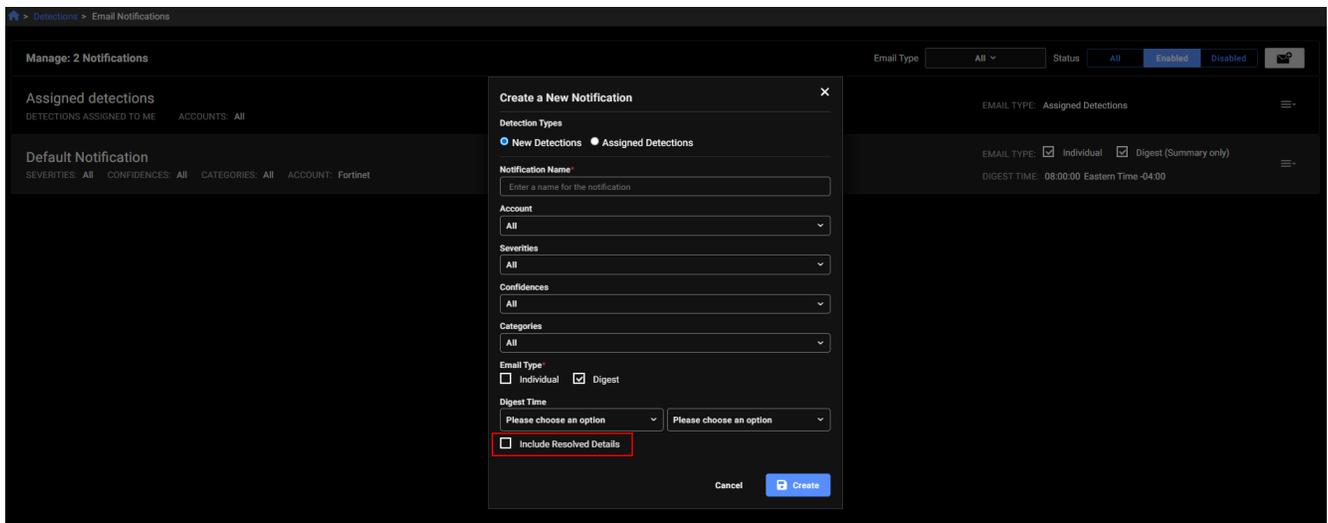
Impacted device filter

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.

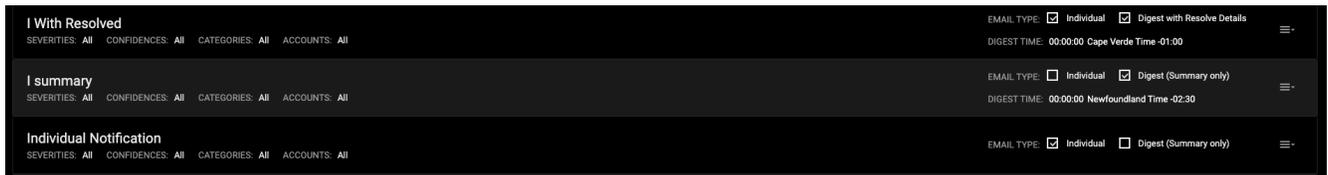


Notification emails

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

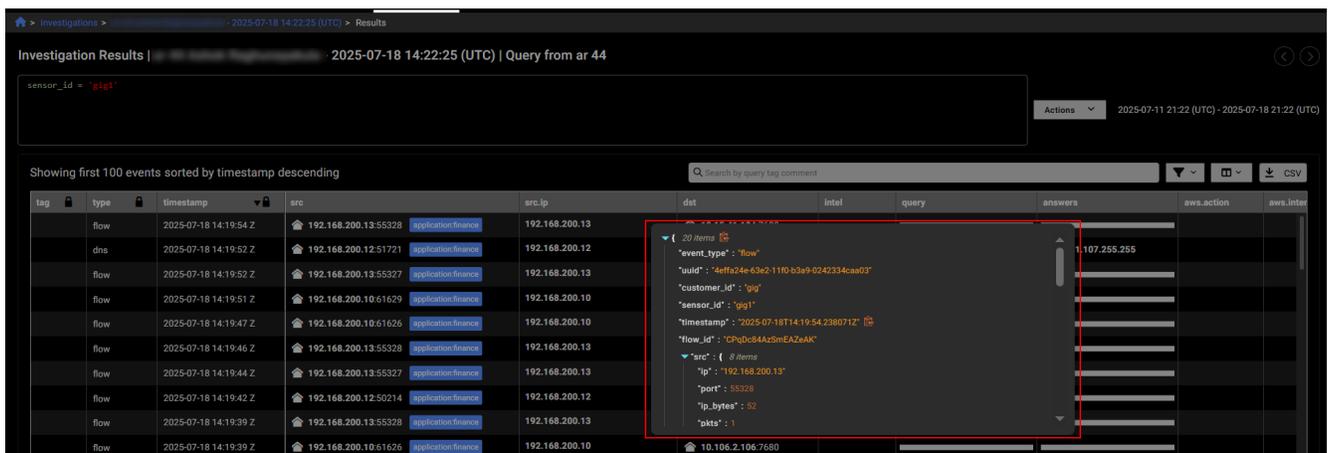


The *Email Notifications* page will display *Digest with Resolve Details* next to the email when this feature is enabled. This feature is in limited availability. If you would like it enabled please contact your TSM.



Single Event View

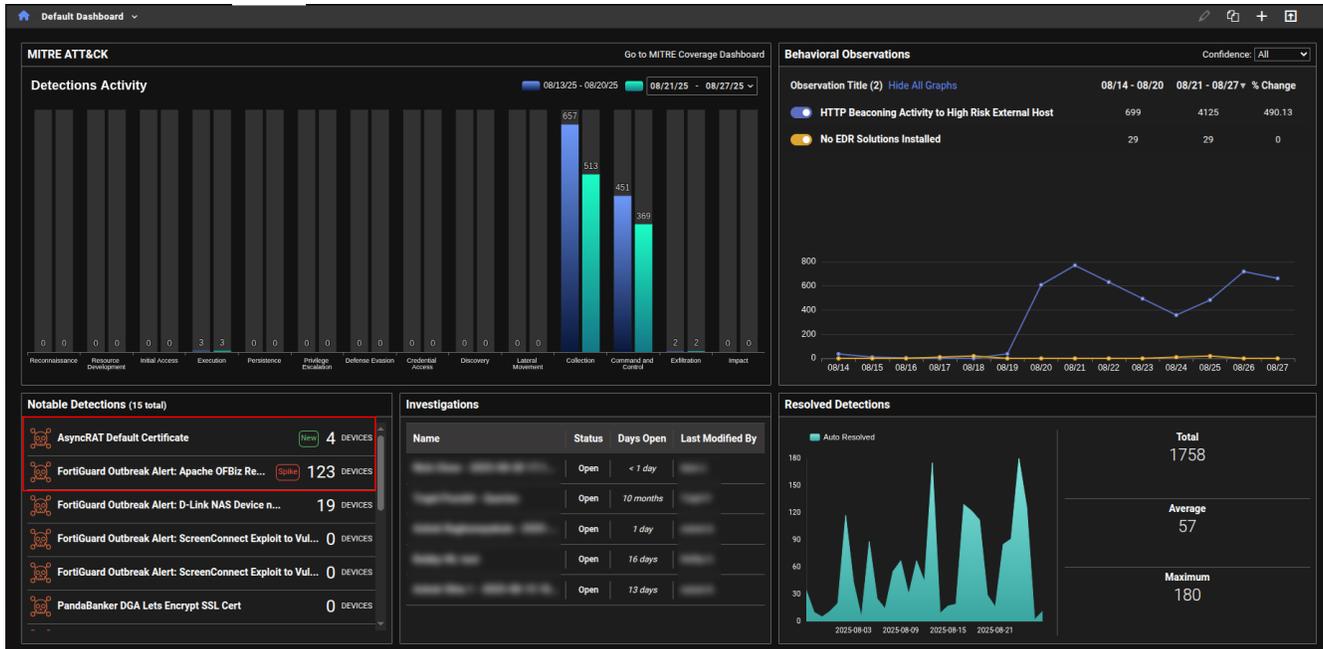
You can now view all details for a single event by double-clicking a blank area within the event row. This opens a pop-up displaying the full row data in JSON format. To copy the JSON, click the copy icon next to the first line. This feature saves time by eliminating the need to scroll through individual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



Notable detections

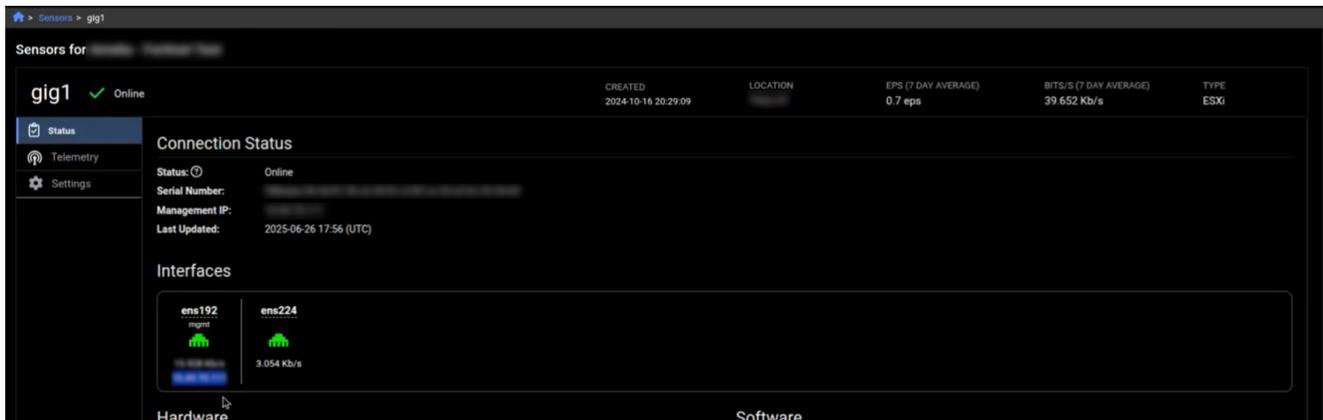
We have added labels to the *Notable Detections* table in the *Dashboard* to highlight new detections and spikes in detection activity.

- *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.



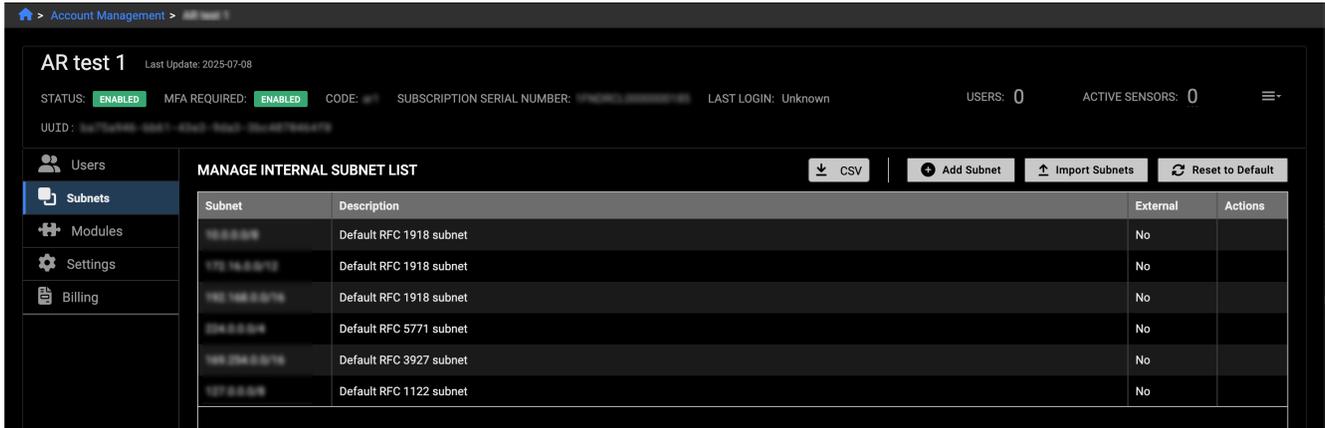
Sensor details

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.



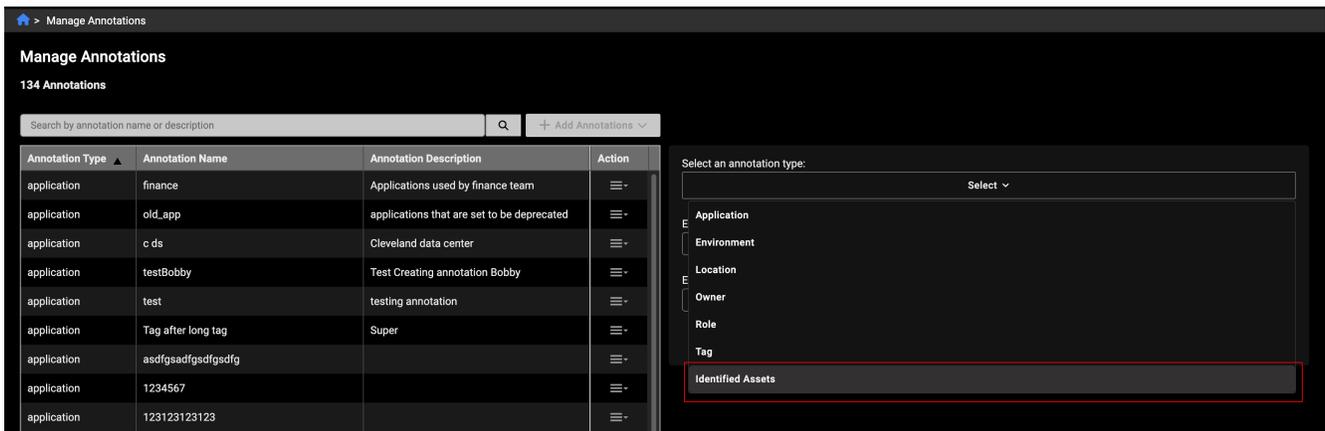
Bulk subnet imports

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.

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 102](#).

Version 25.3.0

- [Deprecation notice](#)
- [Other improvements](#)
- [Resolved issues on page 102](#)

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 49
 - Automated integration response modules on page 49
 - Share detectors with other accounts on page 50
 - Network Traffic Usage reports on page 51
 - Query chart widget on page 52
- Improved functionality on page 53
 - Manage endpoints in the Entity Panel on page 53
 - Assigned detections notifications on page 54
 - Version 25.2.c on page 49
 - Sensor telemetry on page 58
- Other improvements on page 56
 - Event fields on page 56
 - Scrollable Account list on page 56
 - Network Traffic by Event Type widget improvements on page 56
 - Sensor telemetry legend on page 57
 - Intel hits dialog on page 58
 - Group Detections by sensor on page 59
- Resolved issues on page 102

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.

The screenshot shows the 'Investigations' page in FortiNDR Cloud. A table lists various investigations with columns for Name, Description, Created by, Date Created, Date Updated, and a status column. A modal dialog titled 'Integration Response Configuration' is open, displaying a table of integration responses:

Integrations	Response	Action
CrowdStrike Falcon EDR	Manual Response	Edit
FortiEDR	Automatically ban IP address when a high-severity/high-confidence detection occurs	Edit
FortiGate via FortiManager	Manual Response	Edit

Additional notification banners at the top right indicate response updates for CrowdStrike Falcon EDR and FortiEDR.

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

The screenshot shows the 'Account Management > Modules' page. It displays several integration modules with their descriptions and configuration options. A 'Configure' dialog box is open for the 'CrowdStrike Falcon EDR' module, showing the following configuration options:

- Update Configuration:** A dropdown menu.
- Response:**
 - Auto-remediate: This will automatically contain the device at the CrowdStrike Falcon EDR when a high severity/high-confidence detection occurs.
 - Manual Response

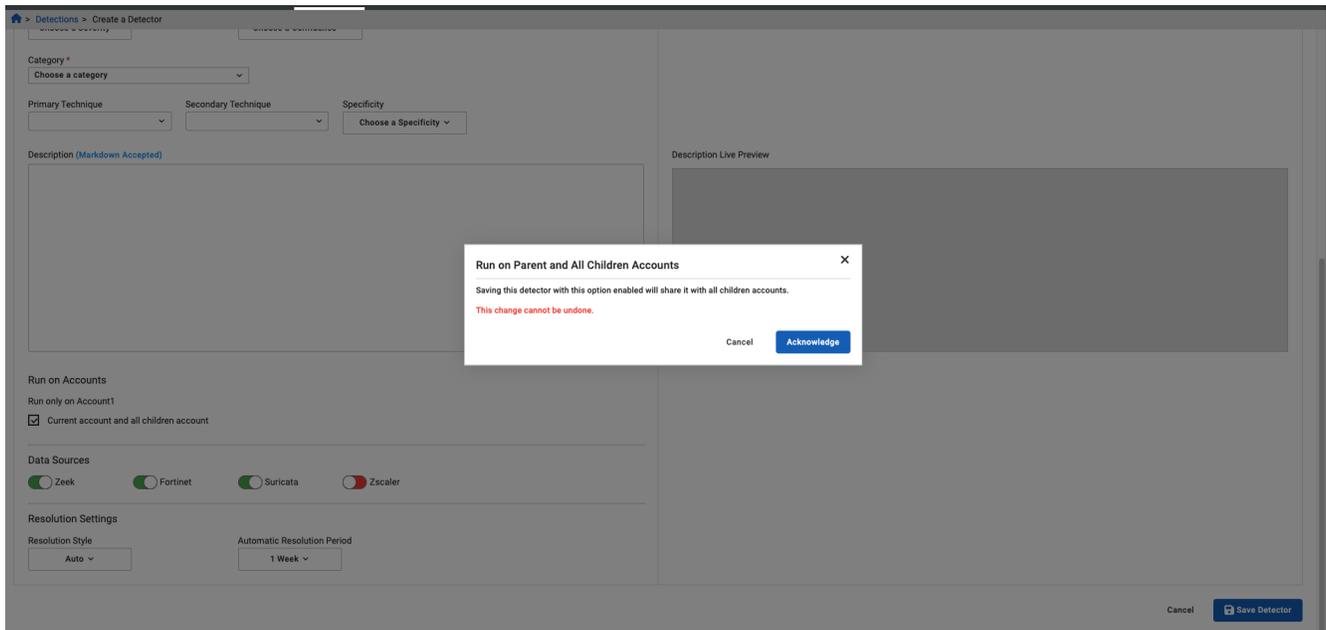
Buttons for 'Cancel' and 'Save' are visible at the bottom of the dialog.

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.

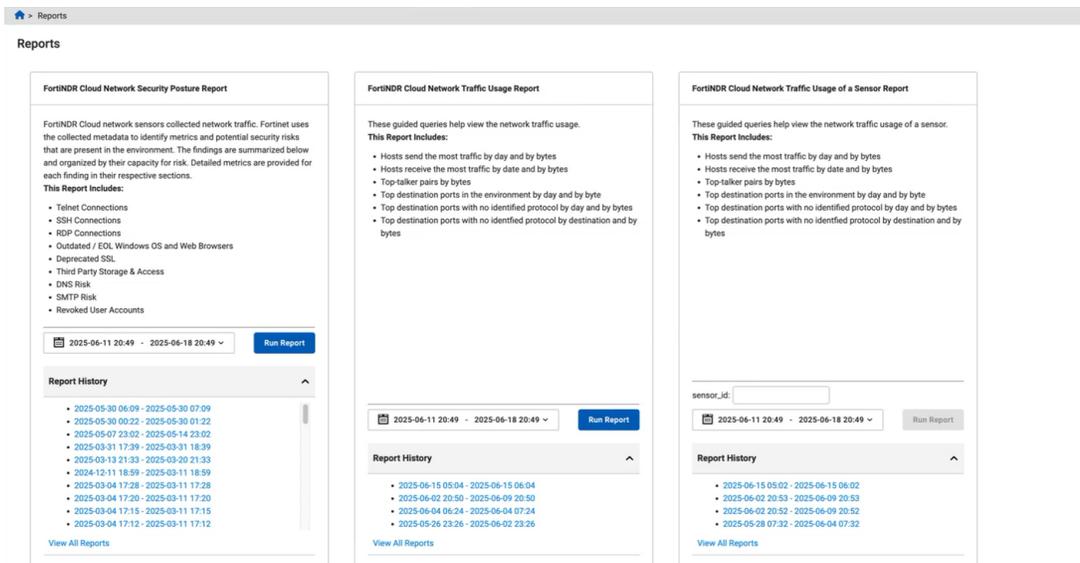


Network Traffic Usage reports

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:

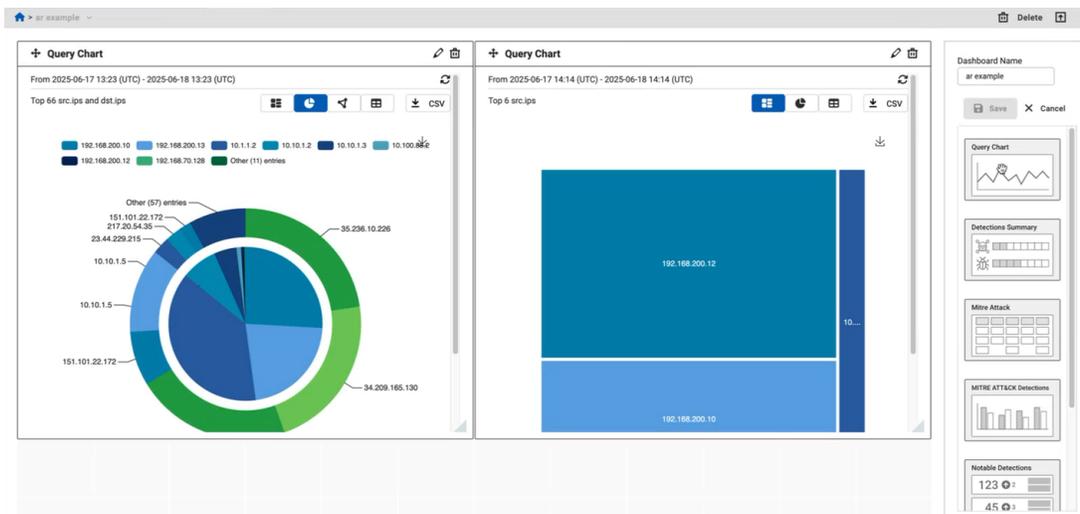
- Hosts send the most traffic by day and by bytes
- Hosts receive the most traffic by date and by bytes
- Top-talker pairs by bytes
- Top destination ports in my environment by day and by bytes
- Top destination ports with no identified protocol by day and by bytes



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.

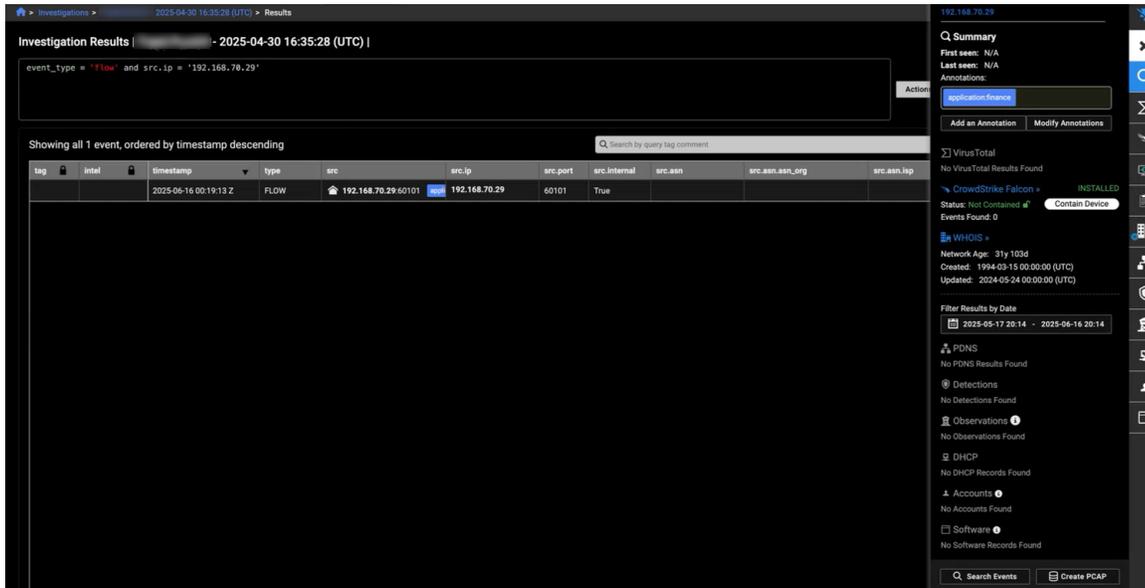
Click on the widget title to go the underlying query object and view the particular events for that investigation.



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.

The screenshot displays the FortiNDR Cloud interface. At the top, it shows the breadcrumb path: Investigations > 2025-04-30 16:35:28 (UTC) > Results. The main heading is 'Investigation Results | [redacted] - 2025-04-30 16:35:28 (UTC) | CS Fortinet query 1'. Below this, a search bar contains the query: 'event_type= 'flow' and src_ip = '172.19.181.18''. An 'Action' button is visible to the right of the search bar.

The main content area shows 'Showing all 1 event, ordered by timestamp descending'. Below this is a table with the following data:

tag	timestamp	type	src	src.ip	src.port	src.internal	src.asn	src.asn.asn_org
	2025-05-26 10:08:47 Z	FLOW	🏠 172.19.181.18.63677	172.19.181.18	63677	True		

A 'Contain Device' dialog box is overlaid on the table. The dialog contains the text: 'You are about to contain the device. Click Continue to proceed or click Cancel to cancel the operation.' There are 'Cancel' and 'Confirm' buttons at the bottom of the dialog.

On the right side of the interface, there is a 'CrowdStrike Falcon' panel. It includes a 'Contain Host in CrowdStrike' button and a list of host details:

- Host ID: LAB-WIN01
- Status: Not Contained
- System Manufacturer: Microsoft Corporation
- Device ID: 0fa45ad046b94a21bf1...
- First Seen: 2025-05-01 21:01:39 UTC
- Last Seen: 2025-06-24 16:46:03 UTC
- MAC Address: 00-15-5d-b5-0f-00
- OS Version: Windows 11
- Platform Name: Windows
- Modified Timestamp: 2025-06-24 17:07:04 UTC
- Provision Status: Provisioned
- Last Login Timestamp: 2025-06-04 19:55:10 UTC
- Last Login User: lab.boi
- Meta: 10796
- Minor Version: 0

Below the host details, there is a 'Detections from CrowdStrike' section showing 'No detections found' and an 'Investigate in CrowdStrike' button. At the bottom of the interface, there are 'Search Events' and 'Create PCAP' buttons.

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*.

The 'Create a New Notification' dialog box contains the following fields and options:

- Notification Name***: A text input field with the placeholder 'Enter a name for the notification'.
- Account**: A dropdown menu currently set to 'All'.
- Detection Types**: Two radio buttons, 'New Detections' and 'Assigned Detections'. The 'Assigned Detections' option is selected.
- Buttons: 'Cancel' and 'Create' (with a lock icon).

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*.

Home > Detections > Email Notifications

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

From: no-reply@fortindr.forticloud.com
 To: Max null

Max,

You have been assigned 1 detection(s) on FortiNDR Cloud

Name: [Anchor Panda Torn Rat Botnet Beacon](#)
 Category: Attack:Command and Control
 Primary Technique: T1071 - Application Layer Protocol
 Secondary Technique:
 Severity: High
 Confidence: High
 Account: [redacted]

[View all Detections assigned to you](#)

Copyright © 2025 Fortinet, Inc. All Rights Reserved.
 899 Kifer Road, Sunnyvale, CA 94088 USA
 +1-866-868-3679 | [Fortinet.com](#)
[Privacy Policy](#)

This email was intended for maxnull1@proton.me. [Click here](#) to change your email preferences or unsubscribe.

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

Home > Detections > Anchor Panda Torn Rat Botnet Beacon

Anchor Panda Torn Rat Botnet Beacon SEVERITY: HIGH | CONFIDENCE: HIGH

CATEGORY: Attack: Command and Control
 FIRST SEEN: 2025-01-28 19:31 (UTC)
 LAST SEEN: 2025-06-04 22:56 (UTC)

UPDATED: 2024-10-29 20:20 (UTC)
 QUERY UPDATED: N/A
 RESOLUTION METHOD: Automatic - After 3 weeks

DEVICES IMPACTED: 1

[Start Investigation](#) | AUTHOR: Fortinet | IMPACTED DEVICE FIELDS: src.ip | INDICATOR FIELDS: dst.ip

Impacted Devices

Device IP	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Indicators	First Seen	Last Seen	Created	Updated	Action
<input type="checkbox"/> 10.220.1.23					4 Events	1 Indicator	2025-06-04 ...	2025-06-04 ...	2025-06-04 ...	2025-06-18	

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

Home > Detections > Detections Table

Detections Table 2 Detectors, 5 Devices from 5 Detections

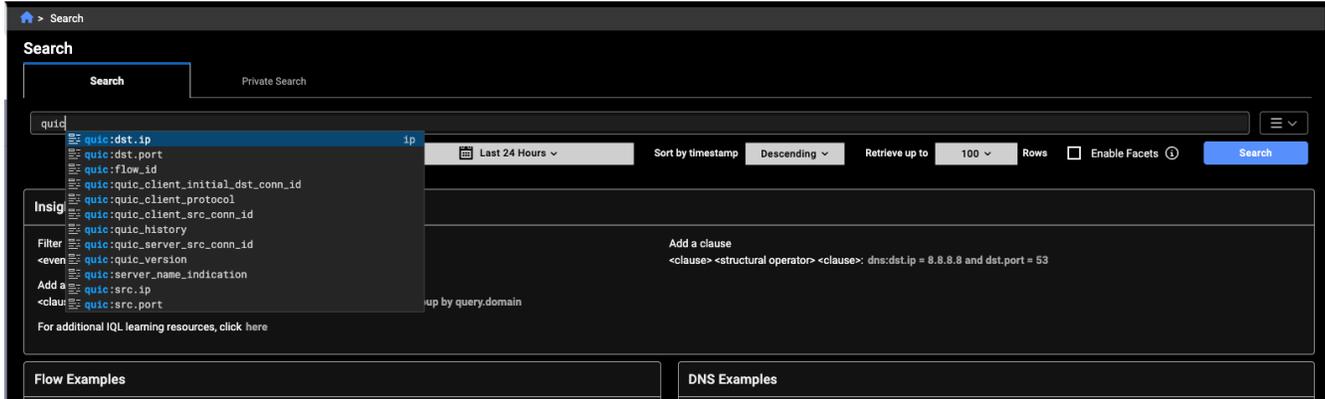
Device IP to search: Search | 2025-06-04 - 2025-06-18 | Severity: All | H | M | L | Resolution Status: All | Active | Resolved

Device IP	Name	Action
<input type="checkbox"/> 10.10.1.110	AsyncRAT Default Certificate	
<input type="checkbox"/> 10.10.1.111	AsyncRAT Default Certificate	
<input type="checkbox"/> 10.10.1.114	AsyncRAT Default Certificate	
<input type="checkbox"/> 10.10.1.117	AsyncRAT Default Certificate	
<input type="checkbox"/> 10.220.1.23	Anchor Panda Torn Rat Botnet Beacon	

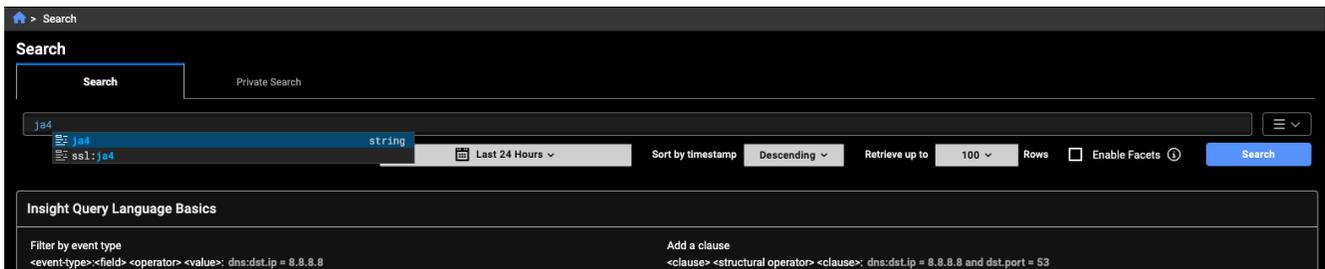
Other improvements

Event fields

You can now query *QUIC* events.



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

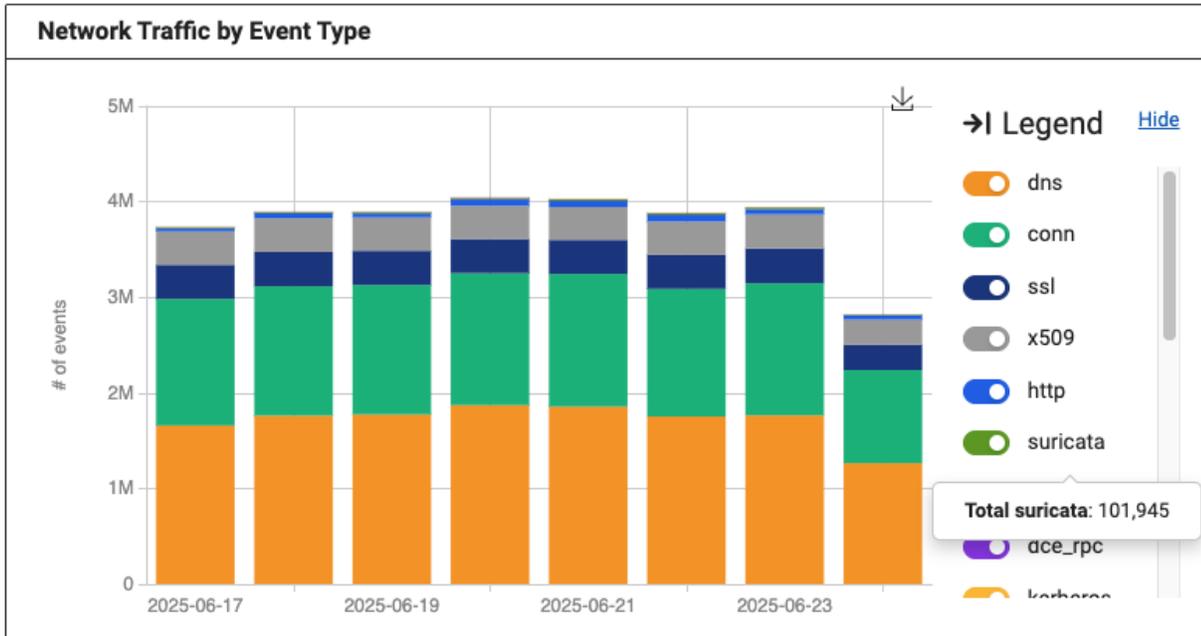


Scrollable Account list

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.

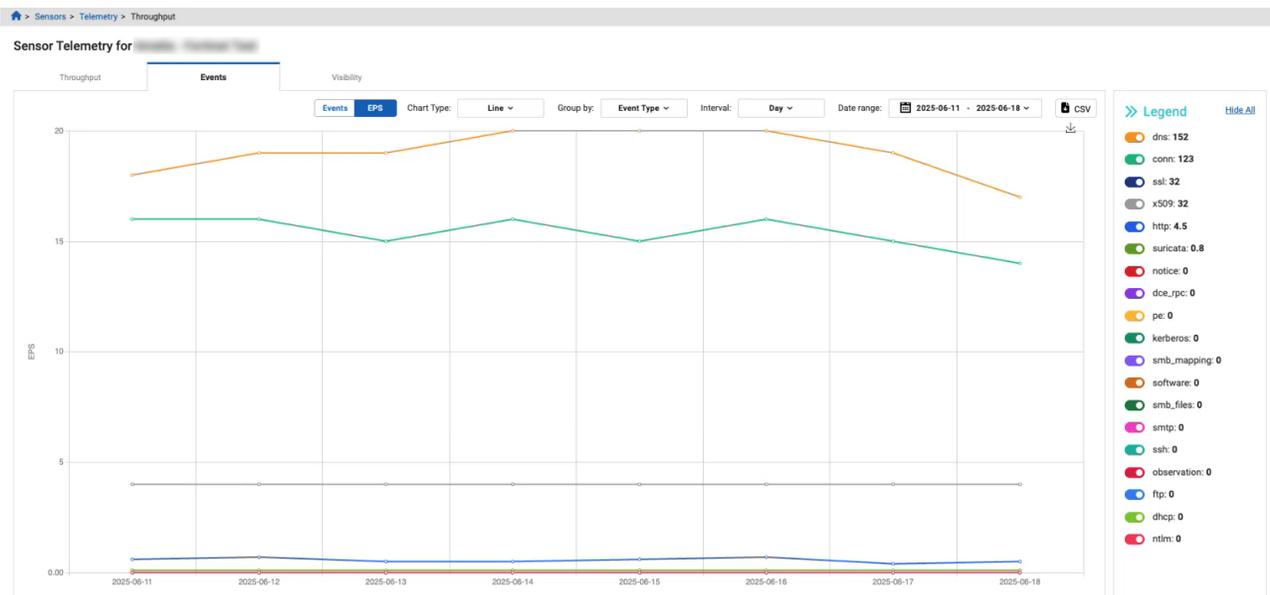
Network Traffic by Event Type widget improvements

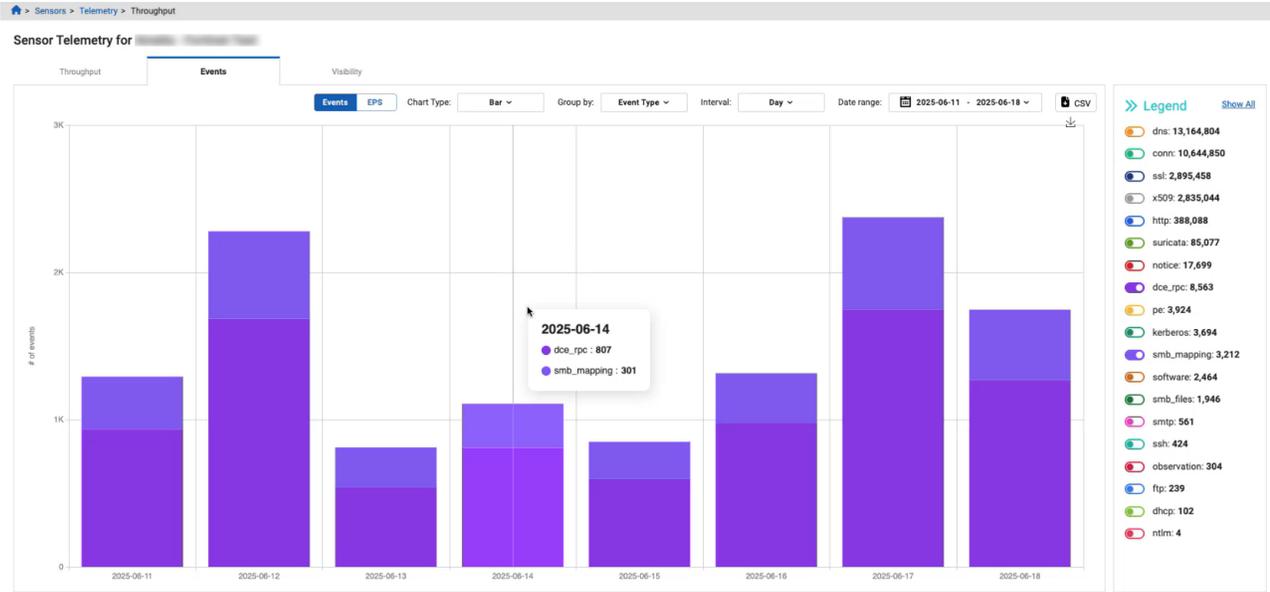
The *Network Traffic by Event Type* widget includes a selectable legend with multiple colors to make it easy to differentiate between the event types.



Sensor telemetry legend

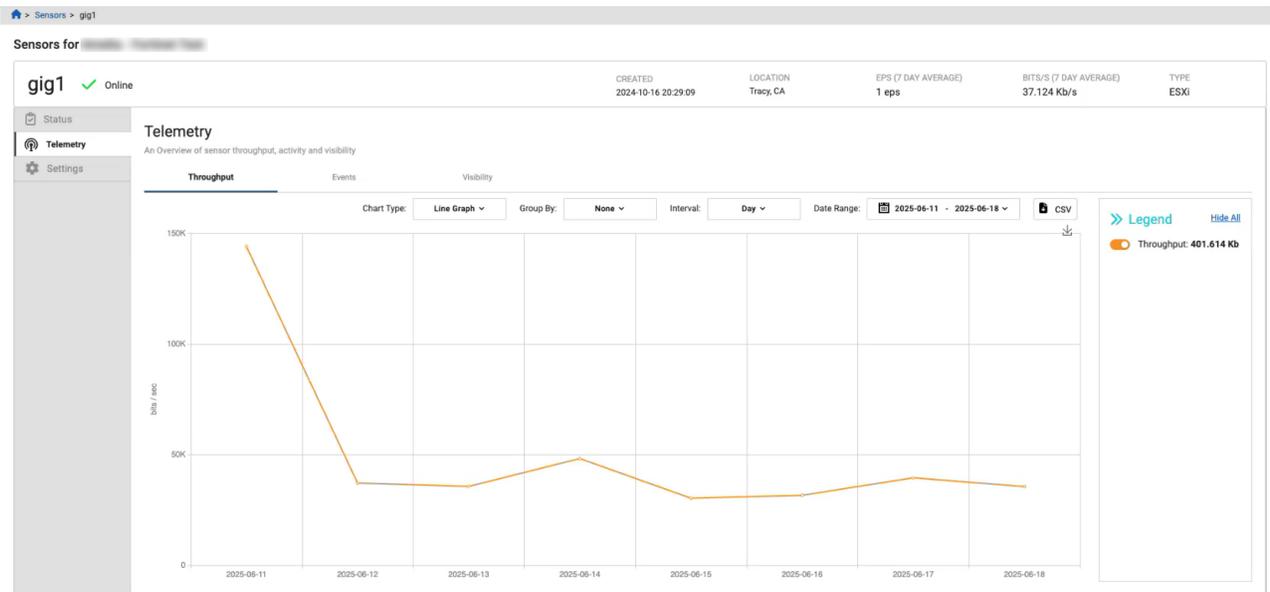
The legend has multiple colors to make it easy to differentiate between the event types, and the event types stay in the same order when switching between *Events* and *EPS* views.





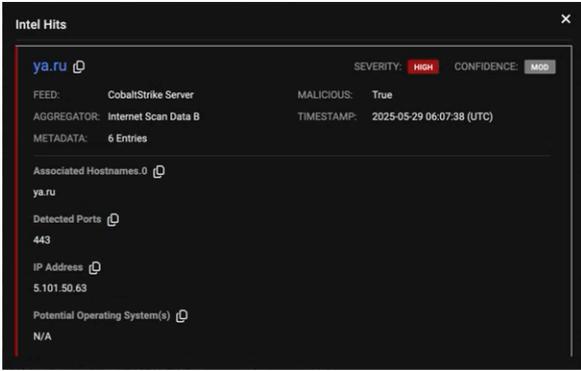
Sensor telemetry

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.



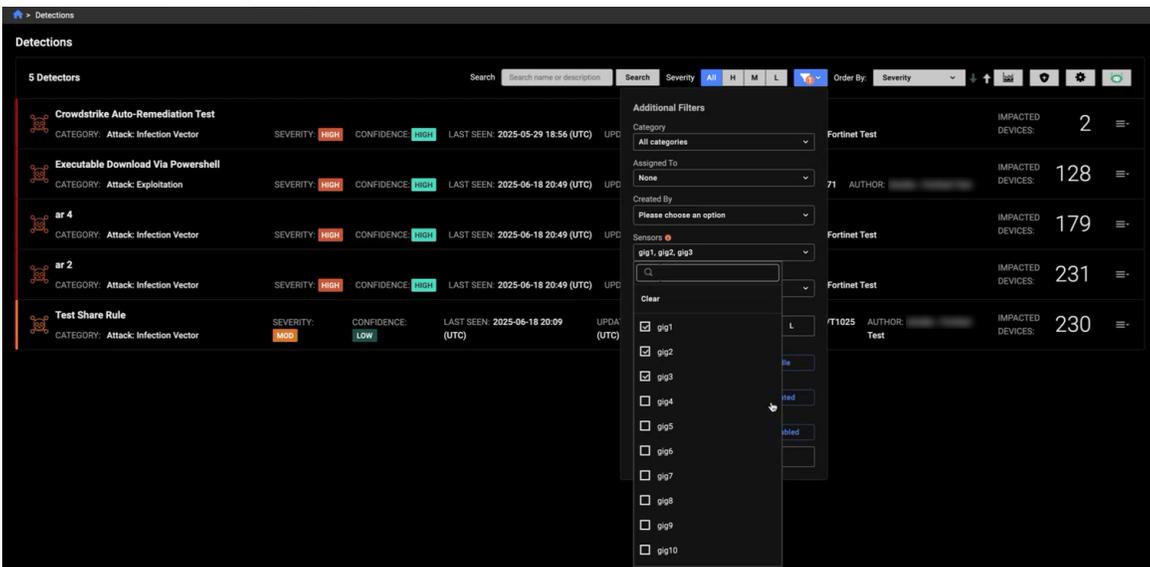
Intel hits dialog

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

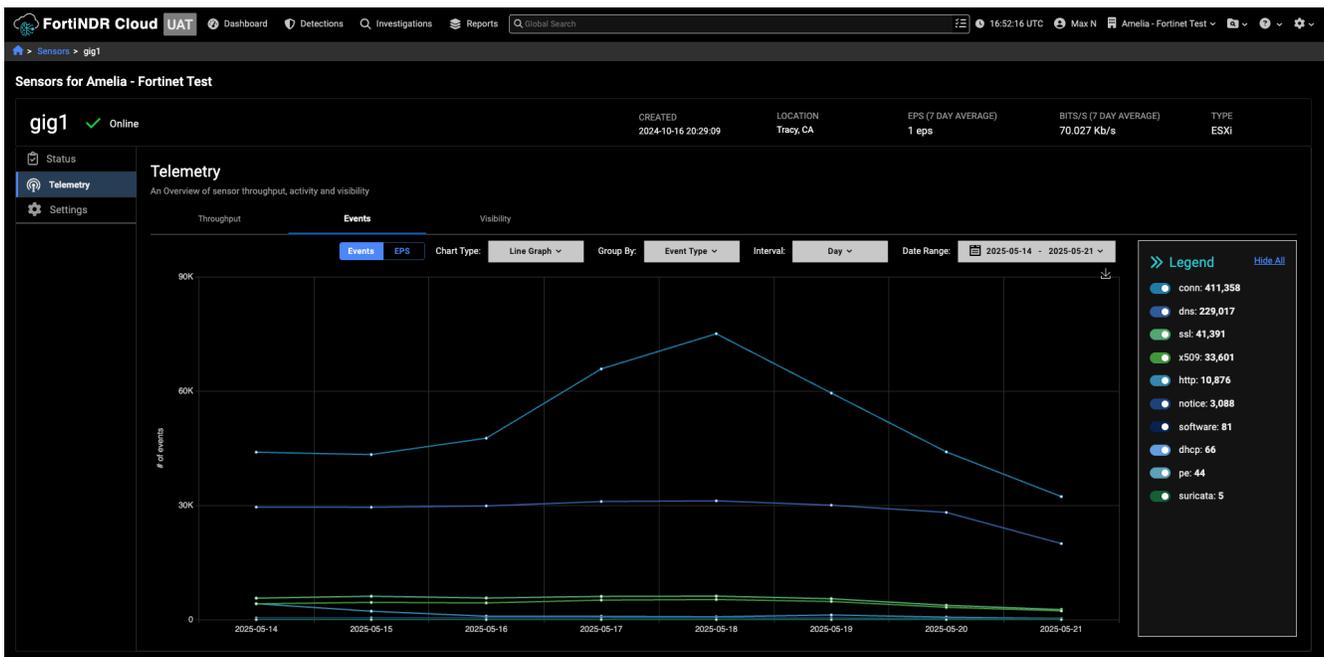
- Improved functionality
 - Sensors
 - Telemetry
 - Throughput
 - Detection context
- Other improvements
- Resolved issues on page 102

Improved functionality

Sensors

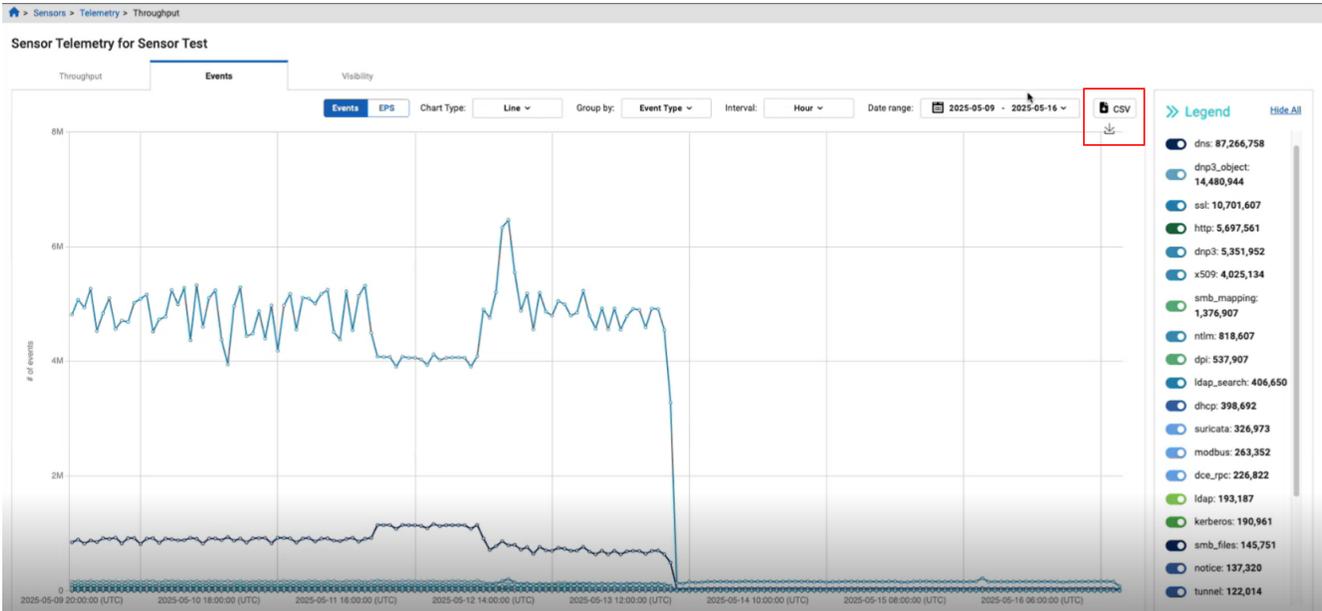
Telemetry

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.



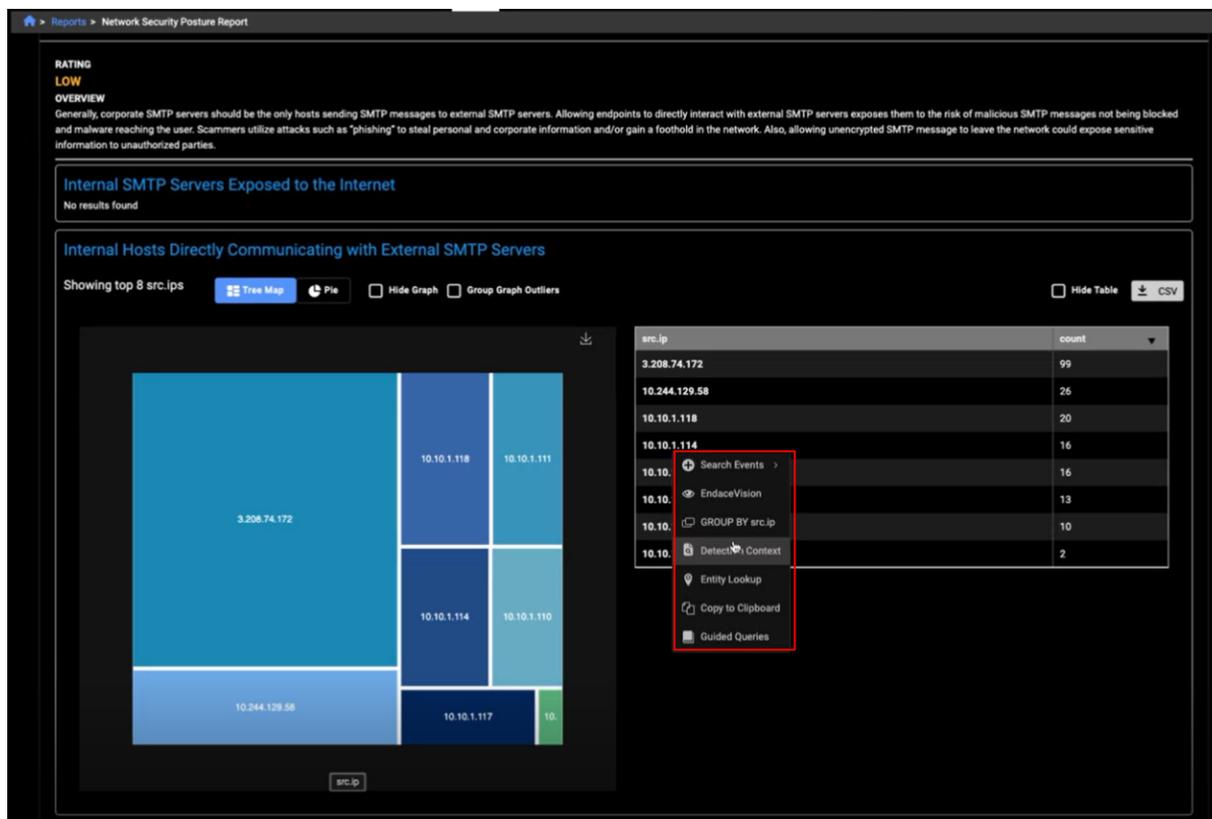
	A	B	C	D	E	F	G	H	I	J	
1	Timestamp (UTC)	conn (EPS)	dce_rpc (EPS)	dhcp (EPS)	dnp3 (EPS)	dnp3_control (EPS)	dnp3_object (EPS)	dns (EPS)	dpi (EPS)	http (EPS)	kerb
2	2025-05-09 20:00:00	1336	0.6	1	16	0.2	43	234	1	16	
3	2025-05-09 21:00:00	1409	0.6	1	17	0.2	46	247	1	16	
4	2025-05-09 22:00:00	1370	0.6	1	16	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 `1dap` and `1dap_search`.

Version 25.2.a

FortiNDR Cloud 25.2.a includes bug fixes, but no new features. See [Resolved issues on page 102](#).

Version 25.2.0

- New functionality
 - Detections table
 - Detection context
- Improved functionality
 - Sensor telemetry
 - Traffic by event type widget
 - Sensor telemetry page
 - IQL queries
 - ldap and ldap_search
- Other improvements
 - Local time
 - Performance improvements
- Resolved issues on page 102

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
04747e8e-4727-43a3-8292...	0.0.0.0	2025-05-08 ...	2025-05-06 23:30:38 Z					[Icon] [Menu]
4a8a16ea-82c3-4991-9351...	0.0.0.0	2025-05-08 ...	2025-05-07 21:40:47 Z					[Icon] [Menu]
594d5871-c0e0-4328-9162...	0.0.0.0	2025-05-08 ...	2025-05-07 21:40:47 Z					[Icon] [Menu]
3158e695-8b9a-4090-a72b...	1.1.1	2025-04-23 ...	2025-03-26 22:55:30 Z					[Icon] [Menu]
84e06a7f-bd42-48d1-941b...	1.1.1	2025-04-23 ...	2025-03-26 22:55:30 Z					[Icon] [Menu]
85f8814e-d85c-4328-83f3-2...	1.1.1	2025-05-01 ...	2025-05-01 06:45:33 Z					[Icon] [Menu]
c51decc1-d08e-40e4-9103...	1.1.1	2025-05-01 ...	2025-05-01 06:45:33 Z					[Icon] [Menu]
eebacf01-aaf3-4628-b71e-3...	1.1.1	2025-03-15 ...	2025-03-11 12:20:35 Z					[Icon] [Menu]
2e54a954-47d2-42e8-b4ea...	1.1.1	2025-04-26 ...	2025-04-23 21:20:57 Z					[Icon] [Menu]
87b141b2-b7b3-491e-8fa9...	1.1.1.12	2025-04-26 ...	2025-04-23 21:20:56 Z					[Icon] [Menu]

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.

The screenshot shows the 'Detection Context' page for IP 10.10.1.114. At the top, there's a header with 'Related Detections and Observations' and a date range of 2025-02-06 to 2025-05-07. Below this is a timeline with a 'Selected Detection' highlighted. Two summary cards are visible:

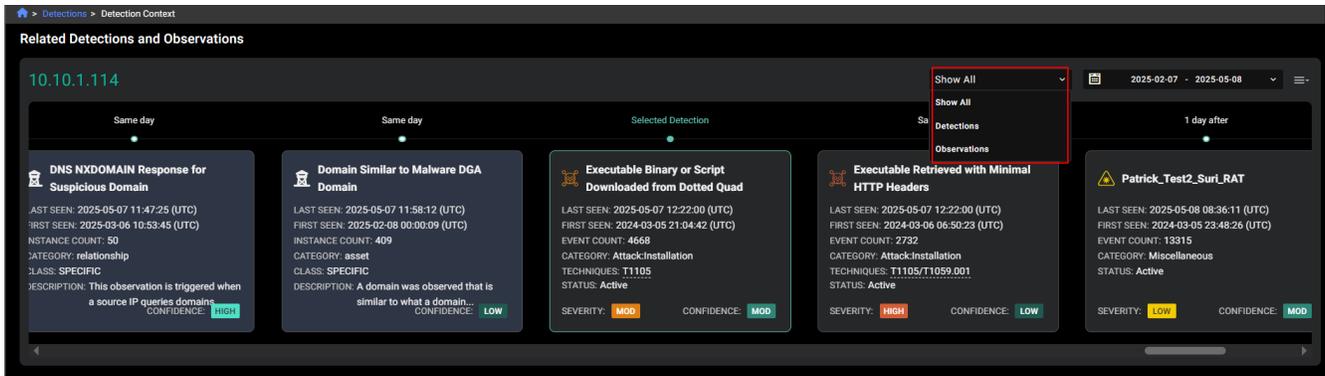
- Autolt User Agent:** LAST SEEN: 2025-05-07 06:01:53 (UTC), FIRST SEEN: 2025-05-06 09:42:15 (UTC), EVENT COUNT: 11, CATEGORY: Attack:Installation, TECHNIQUES: T1059, STATUS: Active, SEVERITY: HIGH, CONFIDENCE: LOW.
- Cryptocurrency Mining Client Check-in:** LAST SEEN: 2025-05-07 06:17:56 (UTC), FIRST SEEN: 2025-05-07 06:12:05 (UTC), EVENT COUNT: 15, CATEGORY: PUA:Unauthorized Resource Use, TECHNIQUES: T1095, STATUS: Active, SEVERITY: MOD, CONFIDENCE: MOD.

Below the timeline are two tables:

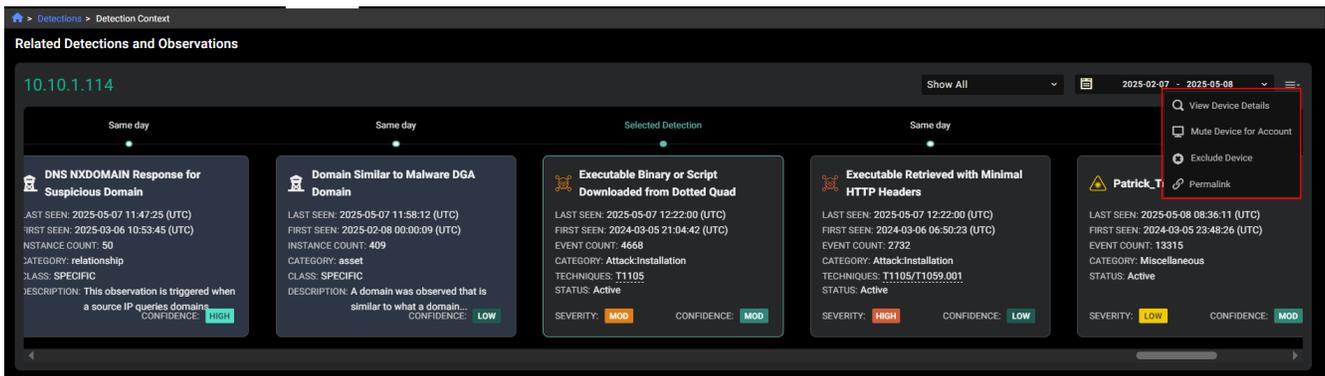
Priority	Confidence	Last Seen	First Seen	Events	Category
MOD	MOD	2025-05-07 17:24:...	2024-03-05 23:48:...	12534	Miscellaneous
MOD	MOD	2025-05-07 17:24:...	2024-03-05 23:48:...	12534	Miscellaneous
MOD	MOD	2025-05-07 12:22:...	2024-03-05 21:04:...	4668	Attack:Installation
LOW	LOW	2025-05-07 12:22:...	2024-03-06 06:50:...	2732	Attack:Installation
MOD	MOD	2025-05-07 06:17:...	2025-05-07 06:12:...	15	PUA:Unauthorized R...
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 U...
HIGH	HIGH	2025-04-29 19:34:...	2025-04-22 18:55:...	11	Posture:Potentially U...
LOW	LOW	2025-04-25 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 an...
MOD	MOD	2025-04-23 03:12:...	2025-04-16 22:24:...	73	PUA:Unauthorized R...
HIGH	HIGH	2025-04-15 06:26:...	2025-04-15 06:25:...	10	Posture:Potentially U...

Title	Confidence	Last Seen	First Seen	Instances	Cat
HTTP C2 Similarity (Natural L...	LOW	2025-05-07 15:55:...	2025-04-08 14:04:...	568	ri
DNS NXDOMAIN Response fo...	MOD	2025-05-07 12:18:...	2025-03-06 07:57:...	51	ri
HTTP C2 Similarity	LOW	2025-05-07 12:15:...	2025-04-09 00:59:...	46	ri
Domain Similar to Malware D...	LOW	2025-05-07 11:58:...	2025-02-06 20:58:...	416	a
DNS NXDOMAIN Response fo...	HIGH	2025-05-07 11:47:...	2025-03-06 10:53:...	50	ri
HTTP C2 Similarity (Natural L...	HIGH	2025-05-07 11:11:...	2025-05-07 11:03:...	3	ri
HTTP Beaconing Activity to H...	HIGH	2025-05-05 05:52:...	2025-04-28 17:55:...	4	ri
HTTP C2 Similarity	MOD	2025-05-01 12:50:...	2025-04-28 20:21:...	2	ri
HTTP C2 Similarity (Natural L...	MOD	2025-04-26 09:52:...	2025-04-09 22:45:...	9	ri
TCP Port 135 (RPC) Device E...	MOD	2025-04-22 03:20:...	2025-04-22 03:20:...	1	ri
XOR-Encoded PE File from Un...	MOD	2025-04-15 16:22:...	2025-04-15 16:22:...	1	fi
TCP Port 445 (SMB) Device E...	LOW	2025-04-15 08:04:...	2025-02-08 23:32:...	11	ri
TCP Port 139 (NetBIOS) Devi...	LOW	2025-04-15 08:04:...	2025-03-10 03:16:...	5	ri
New and Unusual NTLM Auth...	LOW	2025-04-11 20:47:...	2025-03-10 23:24:...	5	ri

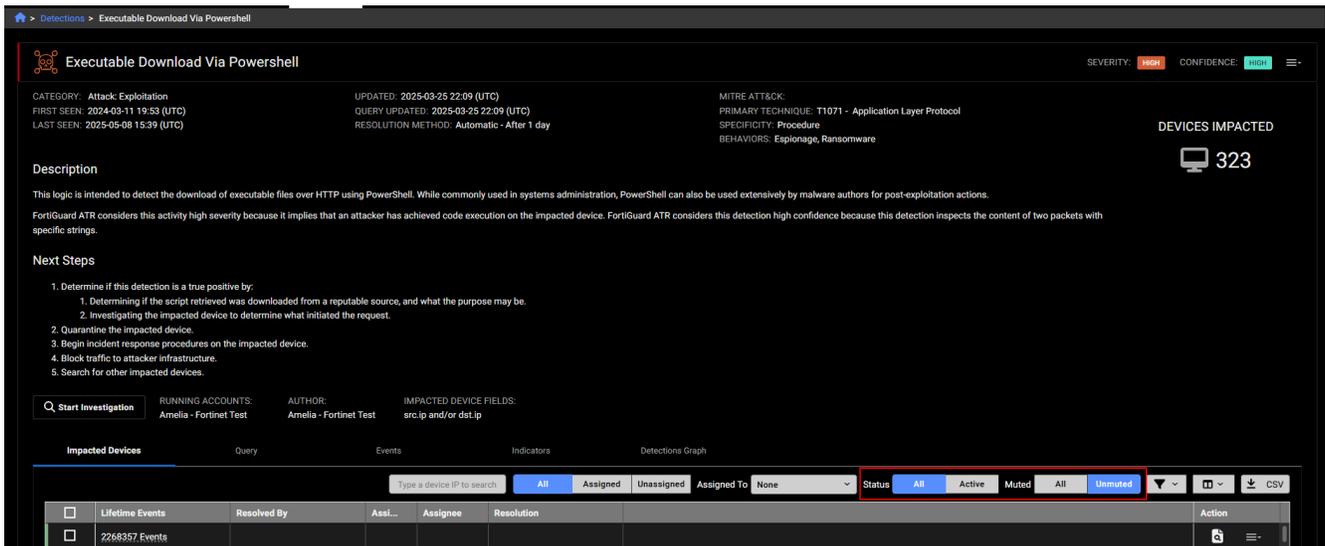
You can filter the *Detection Context* page by *Detections* and *Observations*.



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.

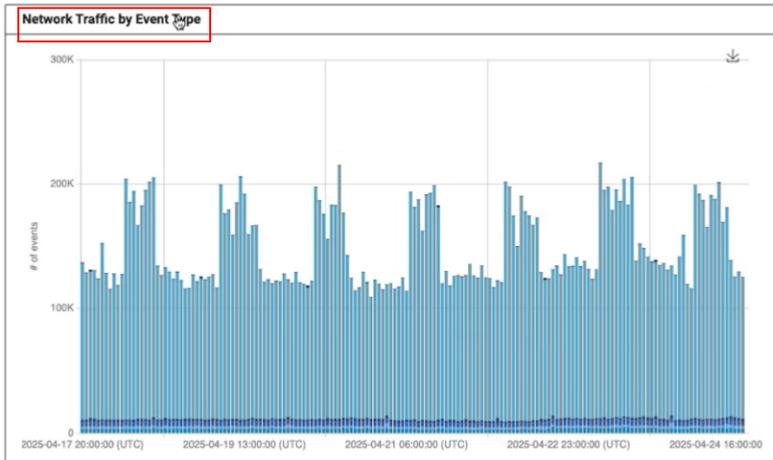


Improved functionality

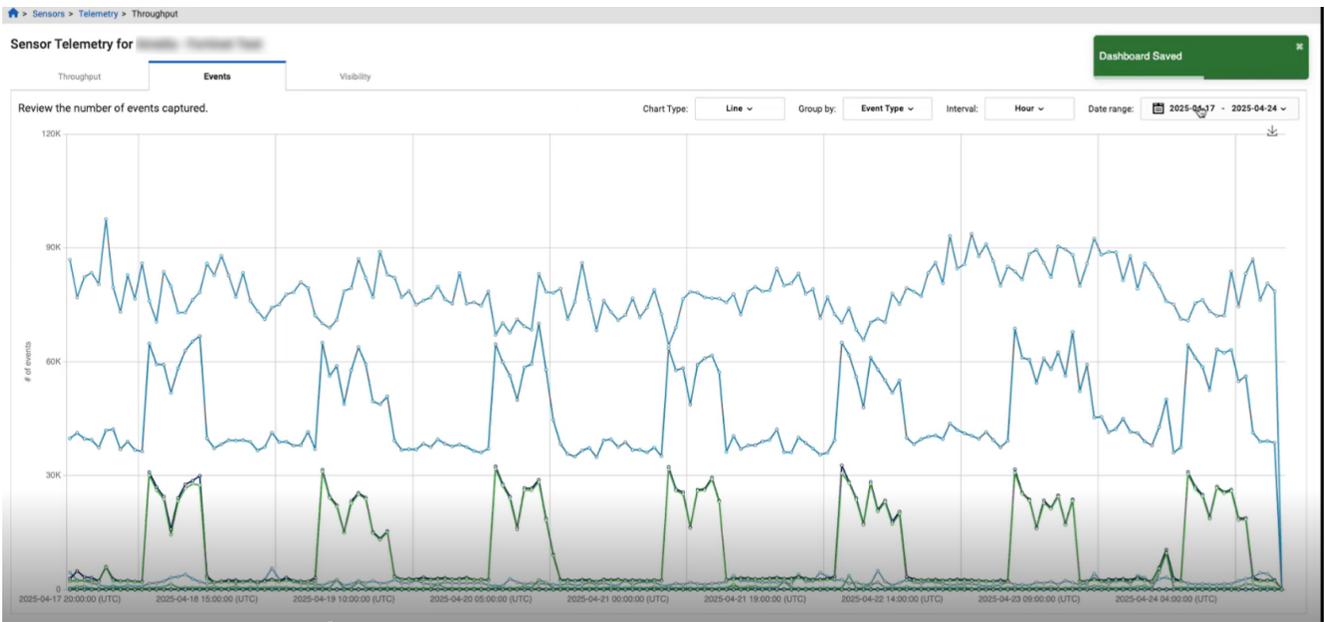
Sensor telemetry

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.

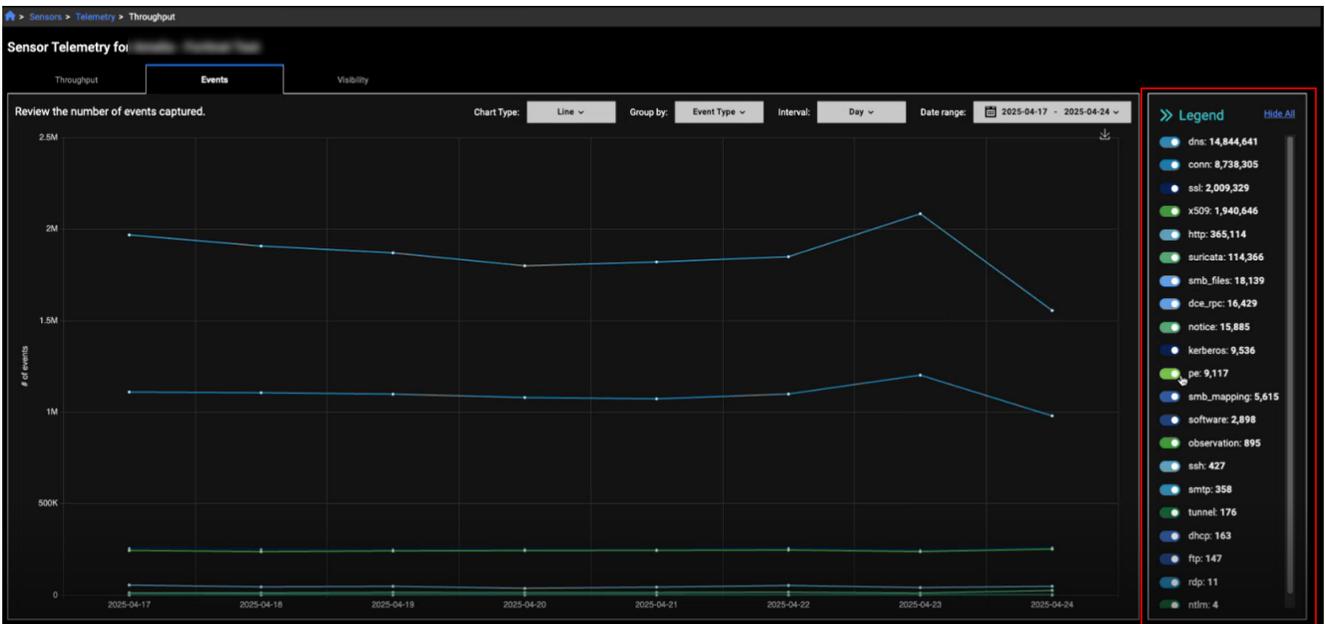


All the filters applied to the widget will be transferred to the *Sensor Telemetry* page.



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

ldap and ldap_search

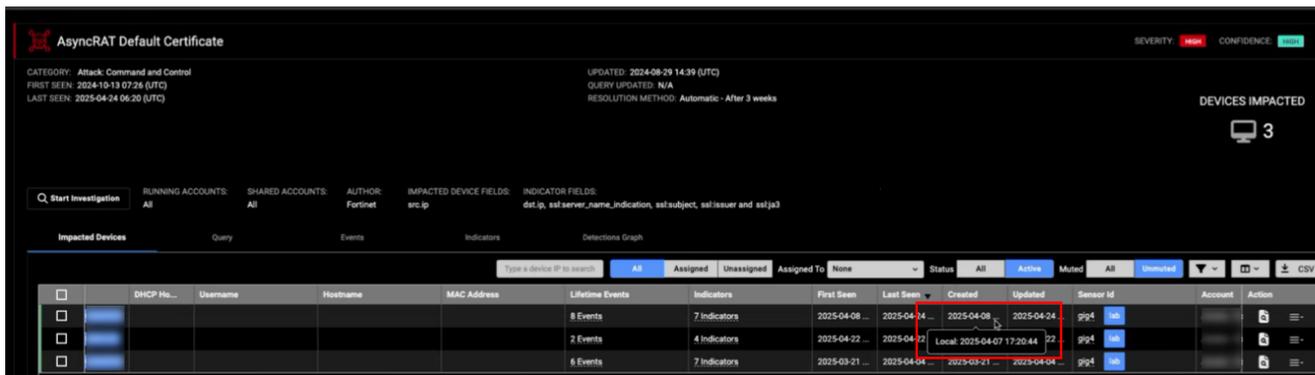
We have added the following event fields to the IQL search:

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>

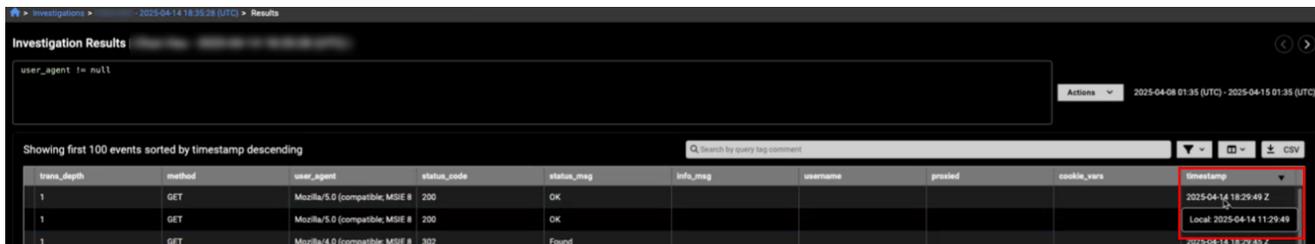
Other improvements

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

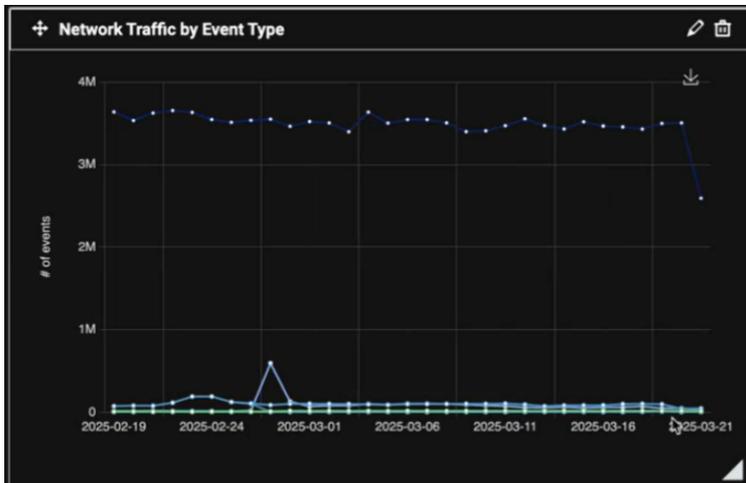
- New functionality
 - Custom dashboards
 - Traffic by type widget
 - Detections
 - Automated response configuration
- Improved functionality
 - Investigations
 - Column profiles
 - IQL queries
 - Detections
 - Create new detectors
- Other improvements
 - Sensors
 - Encryption keys
- Resolved issues on page 102

New functionality

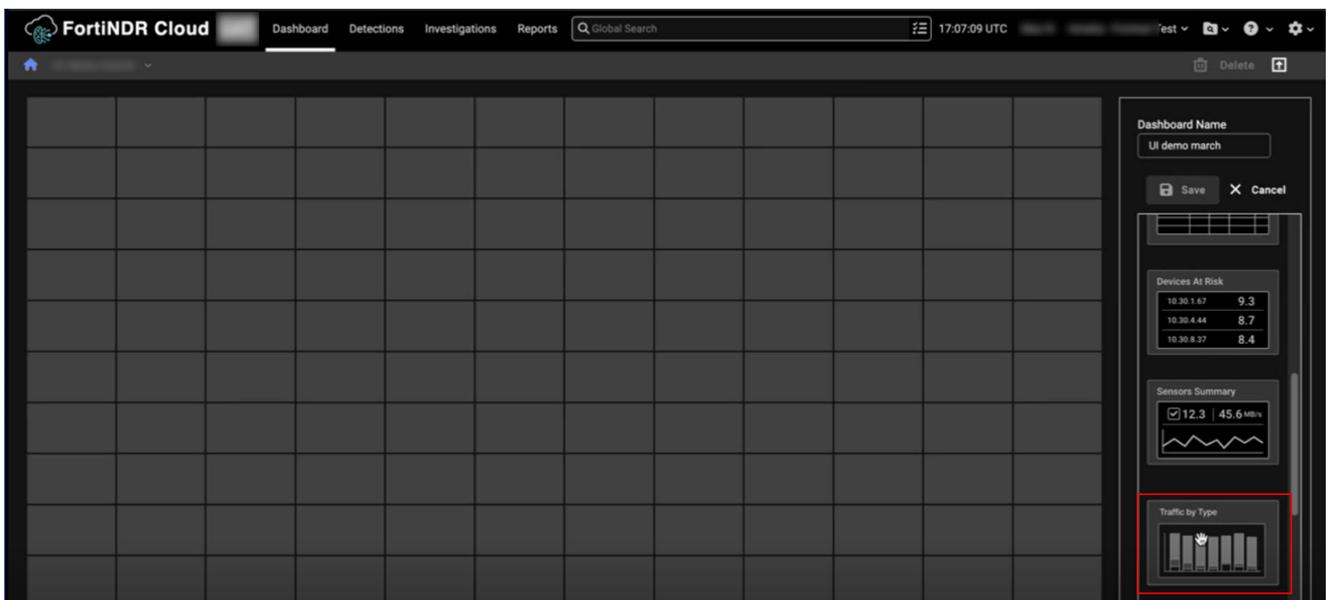
Custom dashboards

Traffic by Event Type widget

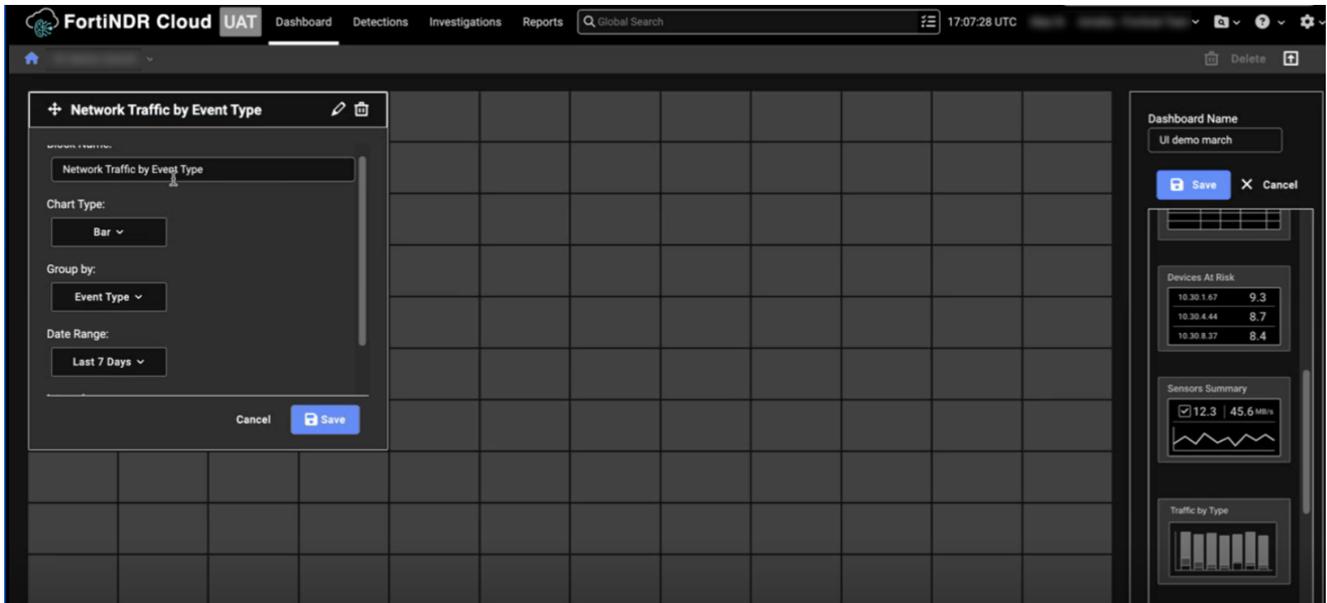
We have added a new *Network traffic by Event Type* widget to the custom dashboard menu. The data in the widget mirrors the *Events* tab in the *Sensor telemetry* page.



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



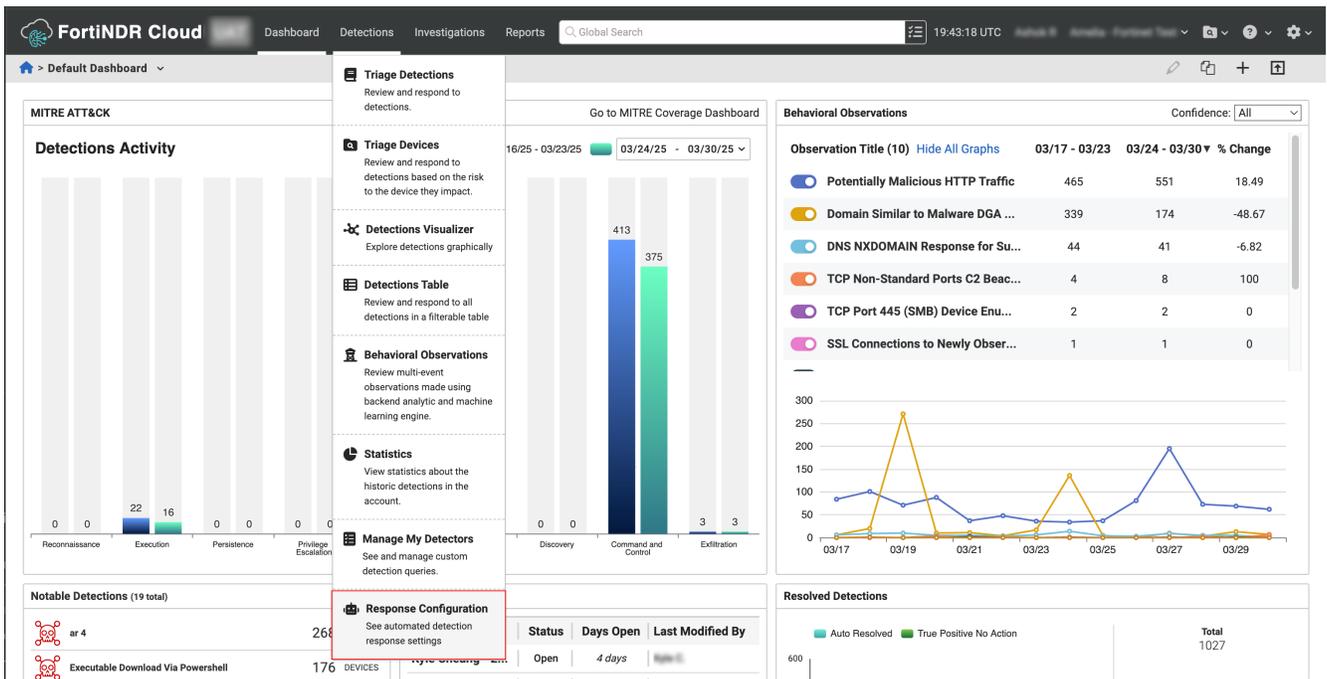
The widget's default name is *Network Traffic by Event*. You can change the name of the widget as well as the default chart type and data filters.



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.

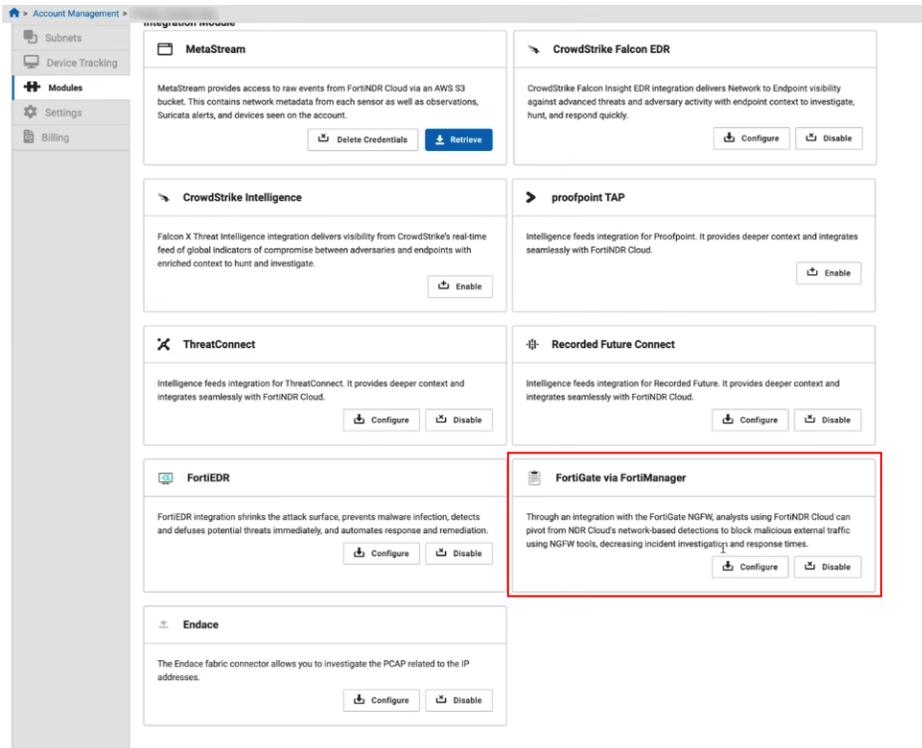


To enable and configure the Response Configuration, go to *Detections > Response Configuration*. In the *Configure* dialog, select *Auto-remediate* or *Manual Response*.

The screenshot displays the FortiNDR Cloud interface. A 'Configure' dialog box is centered, titled 'Configure'. It contains the following text: 'Through an integration with the FortiGate NGFW, analysts using FortiNDR Cloud can pivot from NDR Cloud's network-based detections to block malicious external traffic using NGFW tools, decreasing incident investigation and response times.' Below this is a dropdown menu set to 'Update Configuration'. Under the 'Response' section, there are two radio button options: 'Auto-remediate' (which is selected) and 'Manual Response'. The 'Auto-remediate' option has a sub-description: 'This will automatically ban the IP address at the FortiGate via FortiManager when a high severity/high-confidence detection occurs.' At the bottom of the dialog are 'Cancel' and 'Save' buttons. In the background, the 'Integrations' section is visible, showing 'FortiGate via FortiManager' with an 'Action' menu containing 'Edit' and 'Done' options. Other background elements include a 'Notable Detections' table and a line graph.

Category	Count	Devices
or 4	266	DEVICES
Executable Download Via Powershell	174	DEVICES
New Test Rule	156	DEVICES
Opt In	18	DEVICES
Executable Retrieved with Minimal HTTP Headers	7	DEVICES
Autolt User Agent	6	DEVICES
AsyncRAT Default Certificate	3	DEVICES
Anomalous SMB Protocol Implementations	1	DEVICES

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



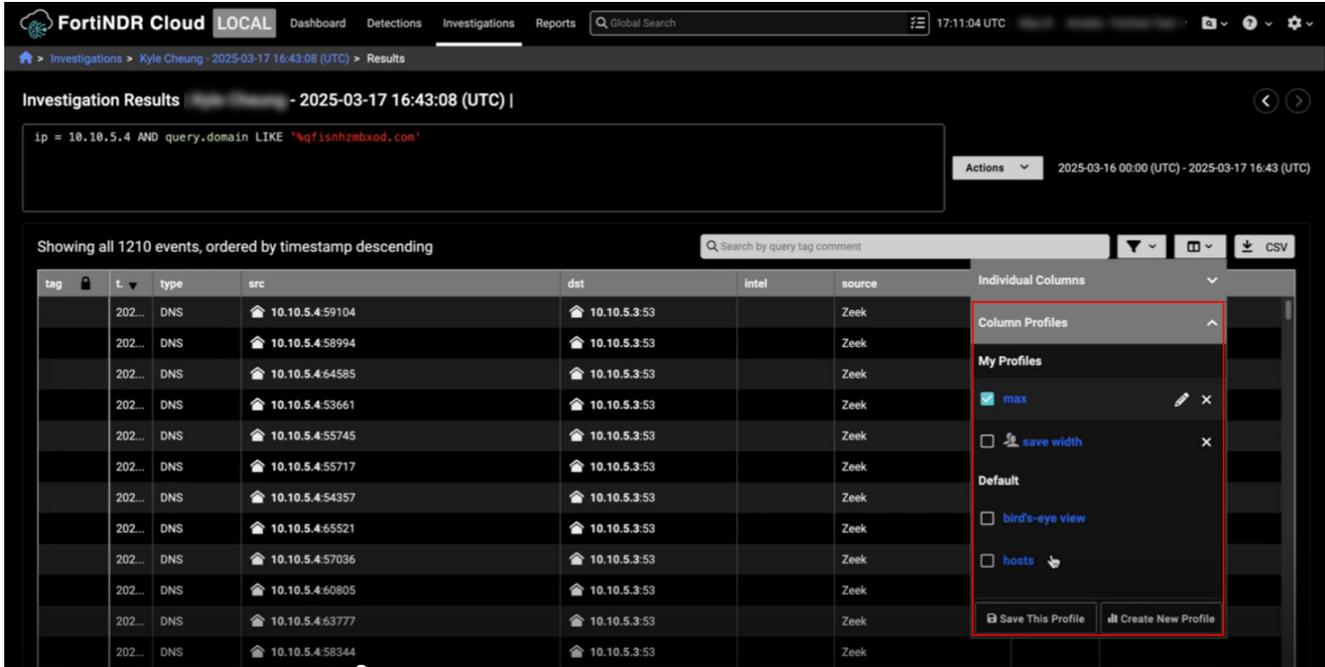
Improved functionality

Investigations

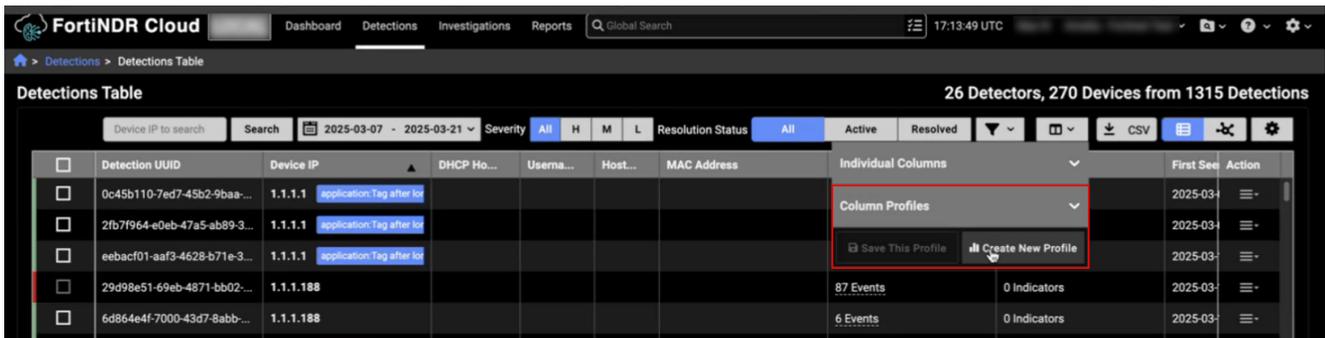
Column profiles

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.

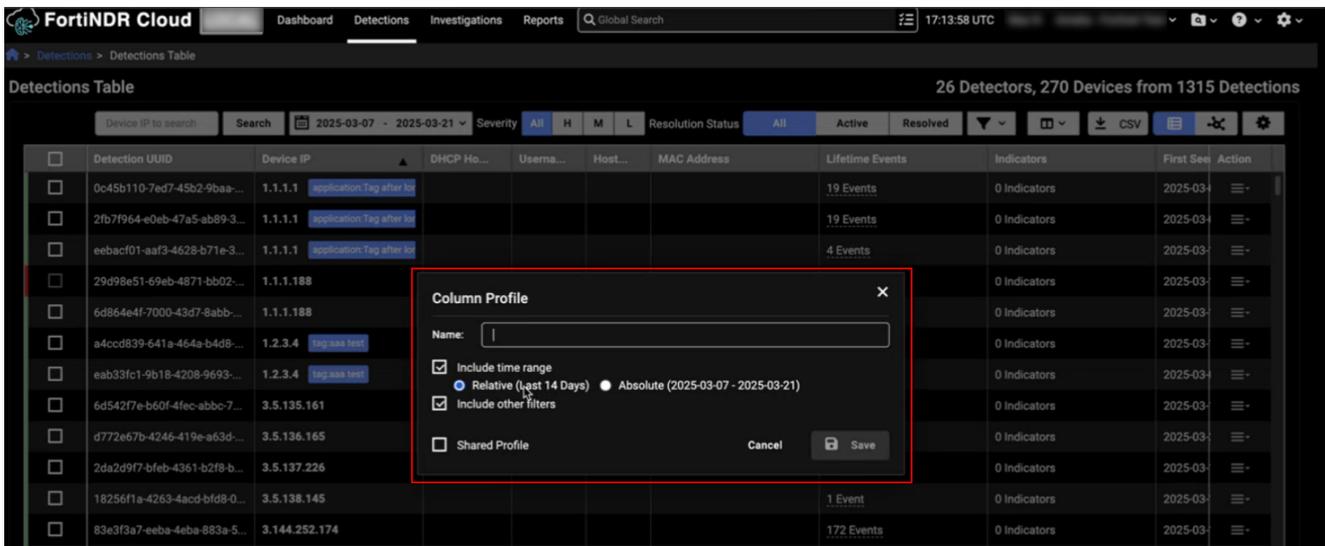
To create a new profile, simply add or remove columns to the current view and adjust the column width, then click *Create New Profile*. Everything in the table will be saved to the profile including the column width. To update changes to an existing profile, simply click *Save this Profile*. After you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



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.

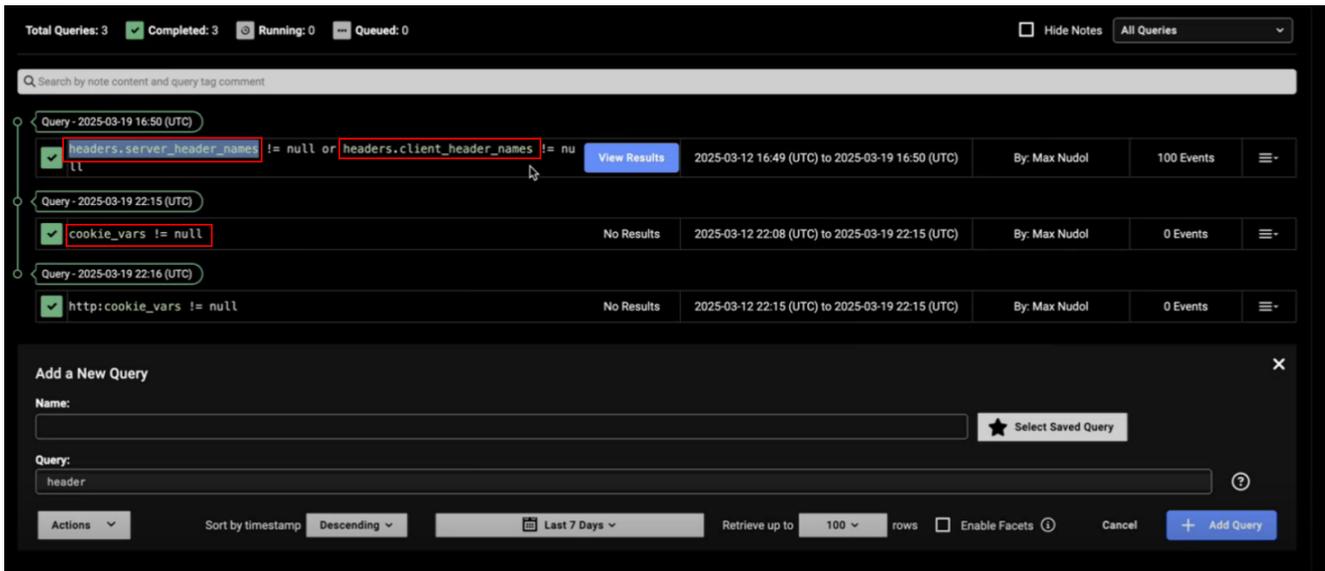


You can configure the profile to include a date range as well as the filters you have applied to the current view of the table.



IQL queries

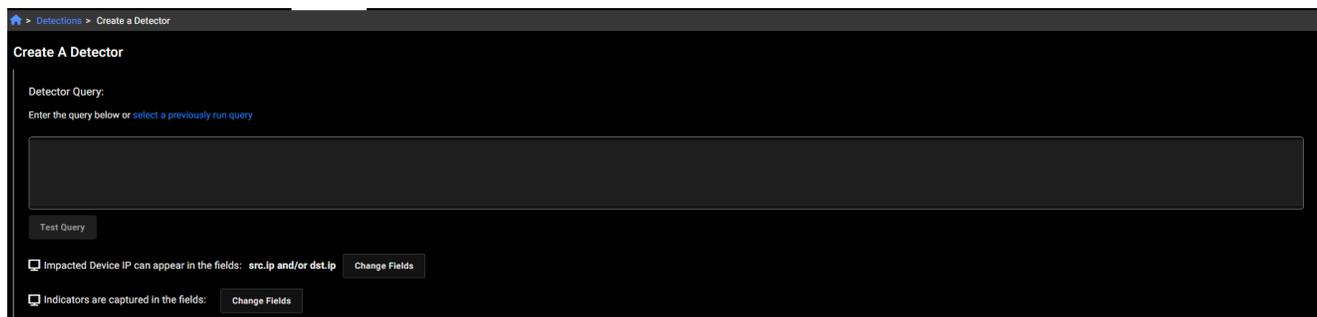
IQL queries now support HTTP server header names, client server names, and cookie variables.



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

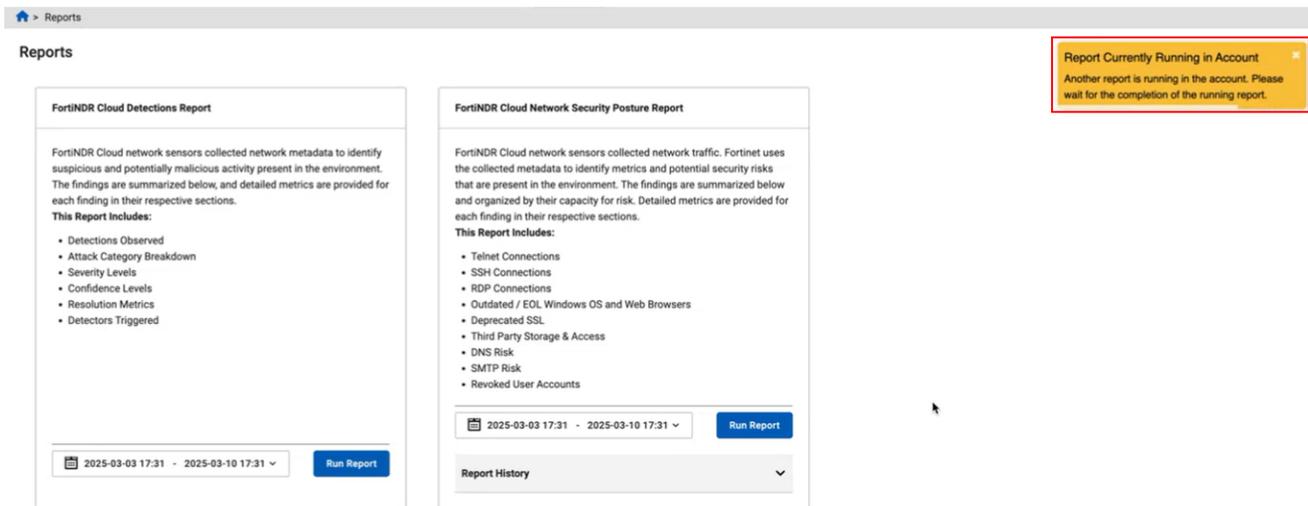
- Improved functionality
 - Reports
 - Pending queries in reports
 - Executive summary
- Other improvements
 - Detectors
 - Edit detector
 - Entity lookup
 - GUI
- Resolved issues on page 102

Improved functionality

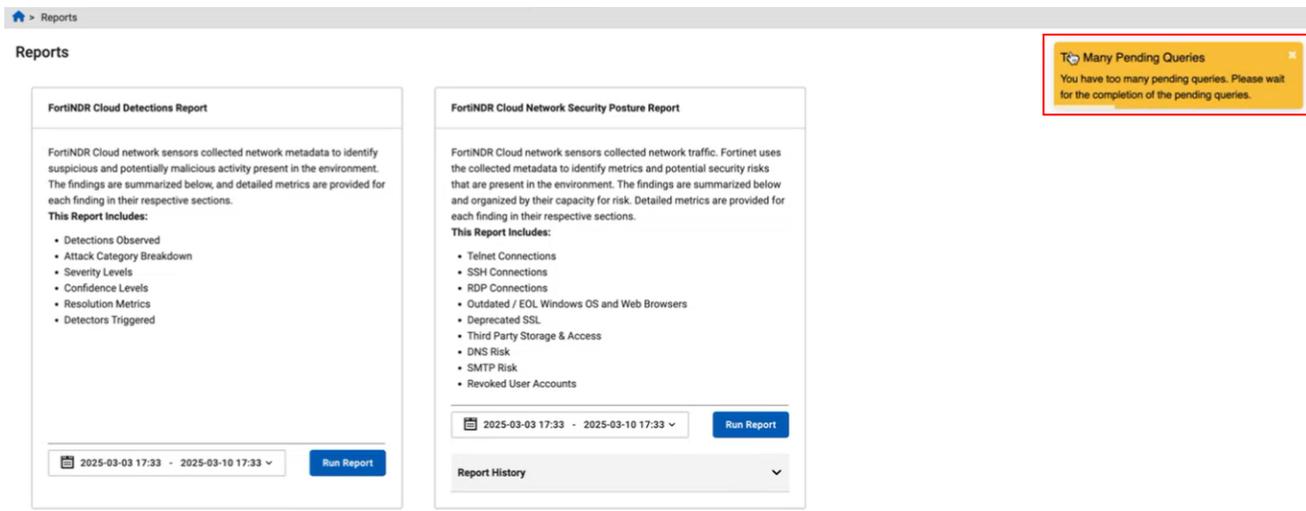
Reports

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.

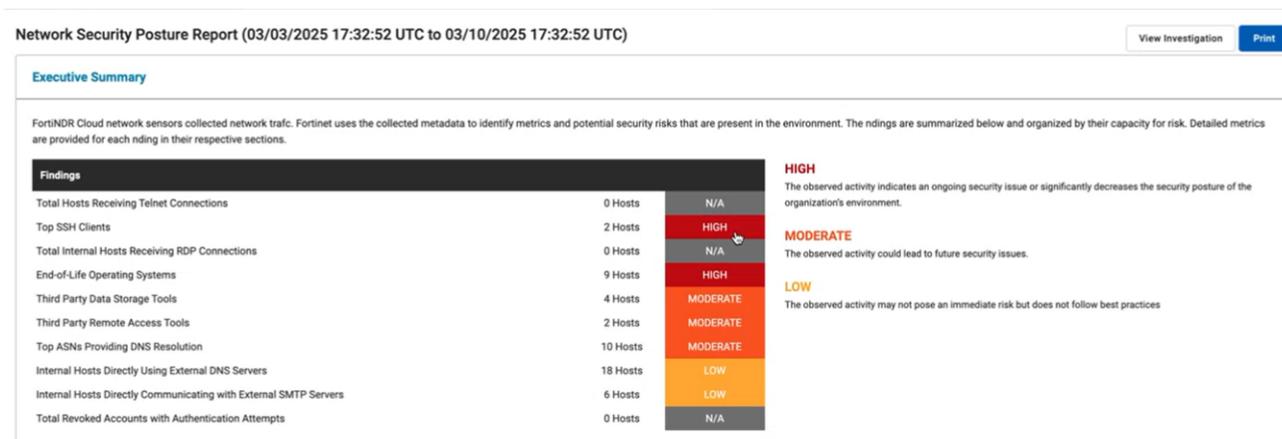


For customers with multiple accounts, users in another account will see the following message:



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.

Outdated / EOL Windows OS and Web Browsers

RATING
HIGH

OVERVIEW
 Microsoft does not continue to support patches for Windows systems indefinitely. Instead, they encourage customers to upgrade or migrate to newer versions. Legacy systems running older versions are at an increased risk of compromise due to security vulnerabilities discovered beyond the EOL date. Outdated Web Browsers are also subject to unpatched vulnerabilities.

End-of-Life Operating Systems with External Connections

Showing top 10 dst.geo.countries out of 25 Tree Map Pie Map Hide Graph Hide Table CSV

dst.geo.country	count
(US) United States of America	2,706
(null)	641
(DE) Germany	312
(BR) Brazil	205
(JP) Japan	163
(HK) Hong Kong	145
(CN) China	128
(VG) Virgin Islands, British	72
(CA) Canada	58
(NL) Netherlands	26

Investigations > Network Security Posture Report (03/03/2025 17:32:52 UTC to 03/10/2025 17:32:52 UTC) > Results

Investigation Results | Network Security Posture Report (03/03/2025 17:32:52 UTC to 03/10/2025 17:32:52 UTC) | End-of-Life Operating Systems with External Connections

`dst.internal = false and src.internal = true and (user_agent like '%Windows XP%' or user_agent like '%Windows/XP%' or user_agent like '%Windows 2003%' or user_agent like '%Windows NT 5.0%' or user_agent like '%Windows 2000%' or user_agent like '%Windows NT 4.0%') group by dst.geo.country`

2025-03-03 17:32 (UTC) - 2025-03-10 17:32 (UTC)

Actions
 Clone Query
 Create a Detection

Events grouped by dst.geo.country

Showing top 25 dst.geo.countries
 Total Events: 100 Tree Map Pie Map Hide Graph Hide Table CSV

dst.geo.country	count
(US) United States of America	2,706
(null)	641
(DE) Germany	312
(BR) Brazil	205
(JP) Japan	163
(HK) Hong Kong	145
(CN) China	128
(VG) Virgin Islands, British	72
(CA) Canada	58
(NL) Netherlands	26
(FR) France	14
(RU) Russia	14
(RO) Romania	9
(CZ) Czech Republic	9
(TR) Turkey	7
(PL) Poland	6

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

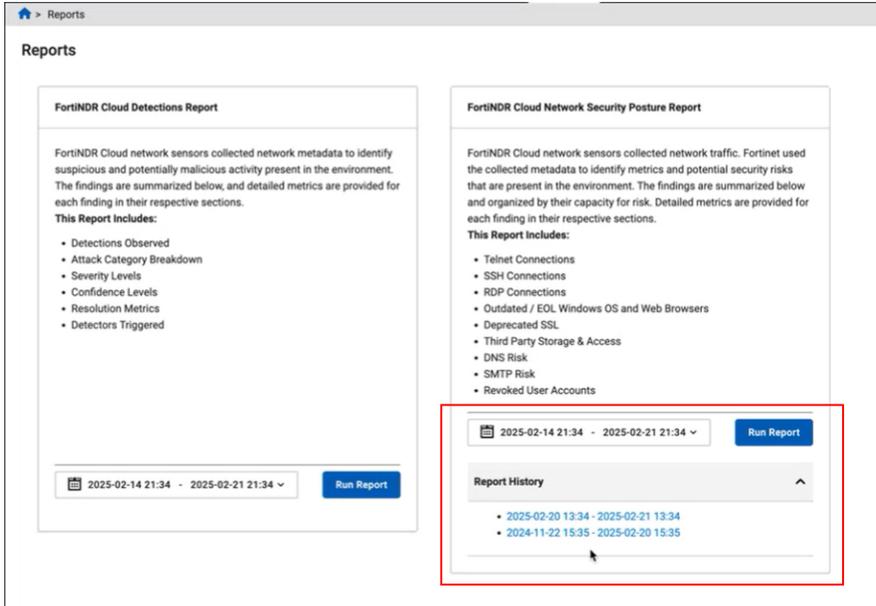
- New functionality
 - Reports
 - FortiNDR Cloud Network Security Posture Report
- Improved functionality
 - Sensors
 - Download sensor images
- Other improvements
 - Portal
- Deprecated functionality
 - Dashboard
- Resolved issues on page 102

New functionality

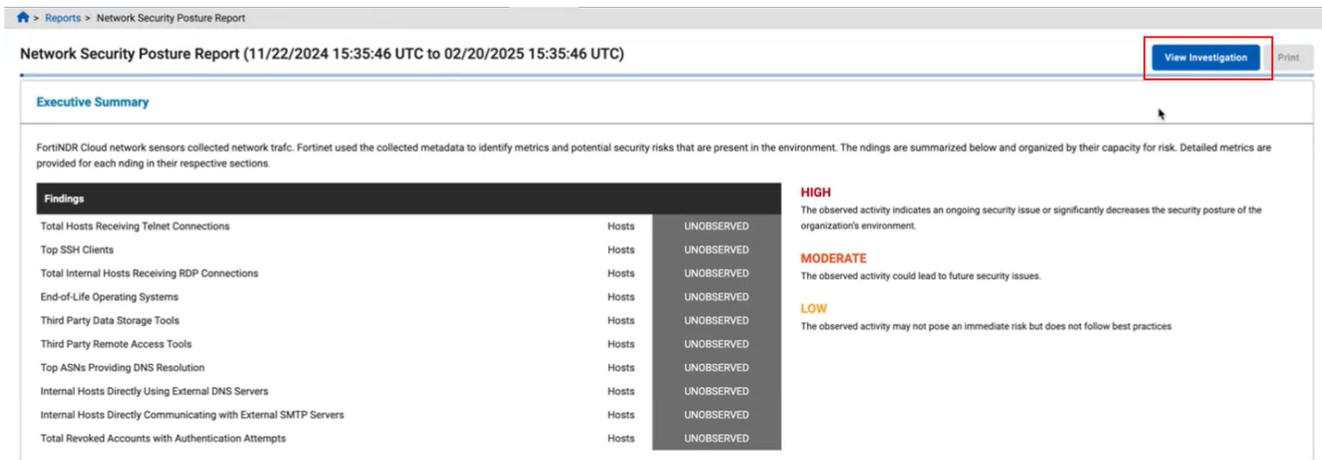
Reports

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.



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

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*.

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE
gig1	Online	2.1.0			0.8 EPS	45.233 Kb/s	ESXI
gig3	Offline	2.1.0			0 EPS	0 b/s	ESXI
gig4	Offline	2.1.0			42 EPS	0 b/s	ESXI
gig5	Pausing	2.1.0			0 EPS	0 b/s	QEMU/KVM
gig6	Online	2.1.0				17.819 Kb/s	QEMU/KVM
gig7	Offline	2.1.0				0 b/s	QEMU/KVM
gig9	Provisioning	2.0.0				0 b/s	ESXI
gig10	Offline	2.1.0				0 b/s	ESXI
gig11	Online	2.0.0				16.339 Kb/s	ESXI
gig12	Online	2.1.0				15.978 Kb/s	ESXI

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

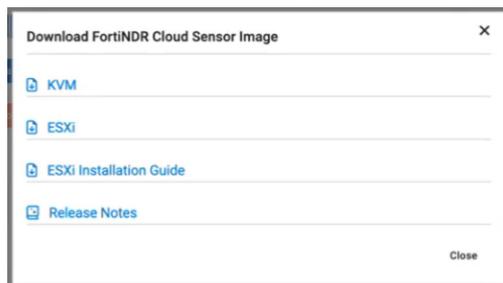
- Improved functionality on page 88
 - Integrations on page 88
 - Sensor images on page 88
 - Account management on page 88
 - User filters on page 88
 - Sensors on page 89
 - Static filters on page 89
- Resolved issues on page 102

Improved functionality

Integrations

Sensor images

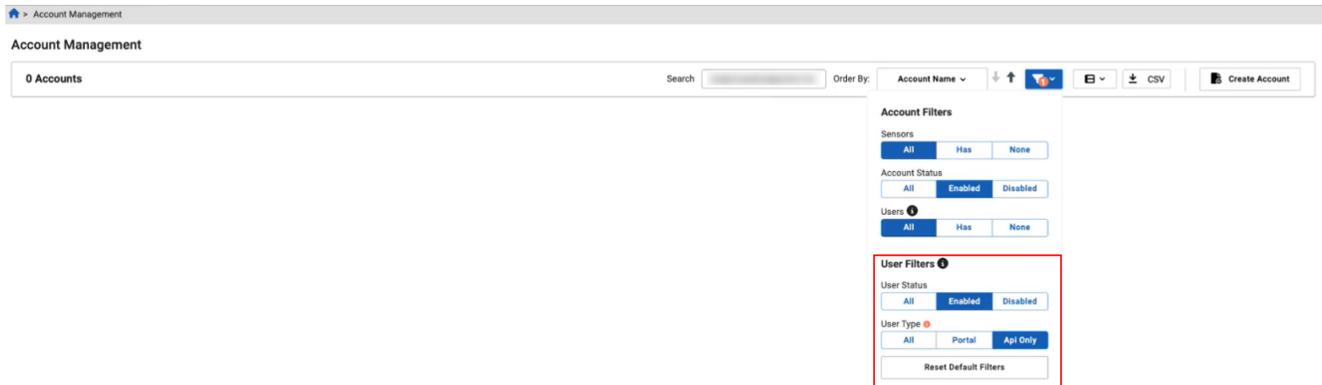
The KVM and ESXi sensor images have been updated. For more information, see the [KVM Sensor Installation Guide](#) and the [ESXi Sensor Installation Guide](#).



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.

The screenshot shows the Fortinet Sensors management interface. At the top, it displays 'Sensors for [redacted] - Fortinet Test' and 'Showing 10 sensors (10 active sensors out of 1000)'. A search bar and several action buttons (Telemetry, Visible Devices, Actions, CSV) are visible. The main area contains a table of sensors with columns for Sensor ID, Status, Version, Labels, Location, and PCAP. A dropdown menu titled 'Additional Filters' is open, showing a search box and a list of filter options. The 'Decommission Pending' option is highlighted with a red box. Other filter options include 'Offline, Online, Pausing, Provisioning', 'All', 'No Filters', 'Decommissioned', 'Decommissioned (auto)', 'Decommissioned (legacy)', 'Offline', 'Online', 'Paused', 'Pausing', and 'Provisioning'.

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	BYTES (7 DAY AVERAGE)	TYPE	PCAP
gjq1	Online	2.1.0			8.118 Kb/s	ESXI	DISABLED
gjq3	Offline	2.1.0			b/s	ESXI	DISABLED
gjq4	Offline	2.1.0			b/s	ESXI	DISABLED
gjq5	Pausing	2.1.0			b/s	QEMU/KVM	DISABLED
gjq6	Online	2.1.0			20.821 Kb/s	QEMU/KVM	DISABLED
gjq7	Offline	2.1.0			0 b/s	QEMU/KVM	DISABLED
gjq9	Provisioning	2.0.0			0 b/s	ESXI	DISABLED
gjq10	Offline	2.1.0			0 b/s	ESXI	DISABLED
gjq11	Online	2.0.0			16.333 Kb/s	ESXI	DISABLED
gjq12	Online	2.1.0			15.965 Kb/s	ESXI	DISABLED

Version 25.1.a

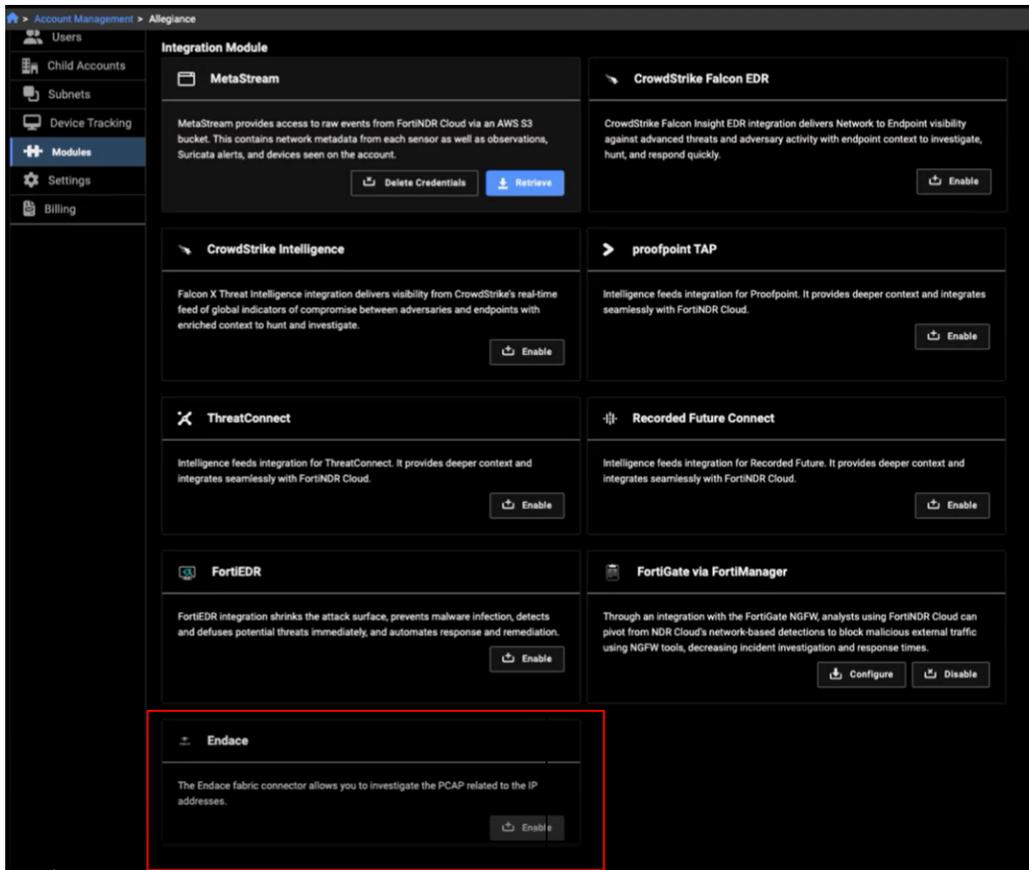
- New functionality on page 91
 - Integrations on page 91
 - Endace integration on page 91
 - Investigations on page 93
 - Annotations on page 93
- Improved functionality on page 94
 - Reports on page 94
 - FortiNDR Cloud Network Security Posture Report on page 94
 - Behavioral observations on page 95
 - Time ranges on page 95
 - Integrations on page 95
 - FortiEDR on page 95
 - Other improvements on page 96
 - Tooltips on page 96
- Resolved issues on page 102

New functionality

Integrations

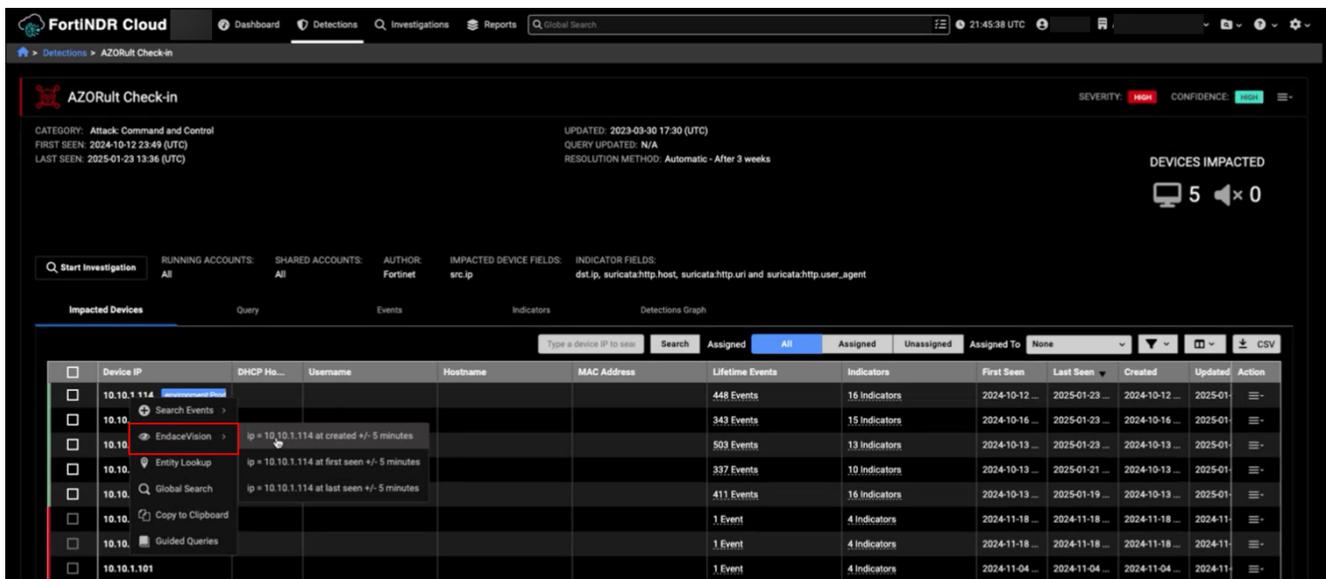
Endace integration

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.



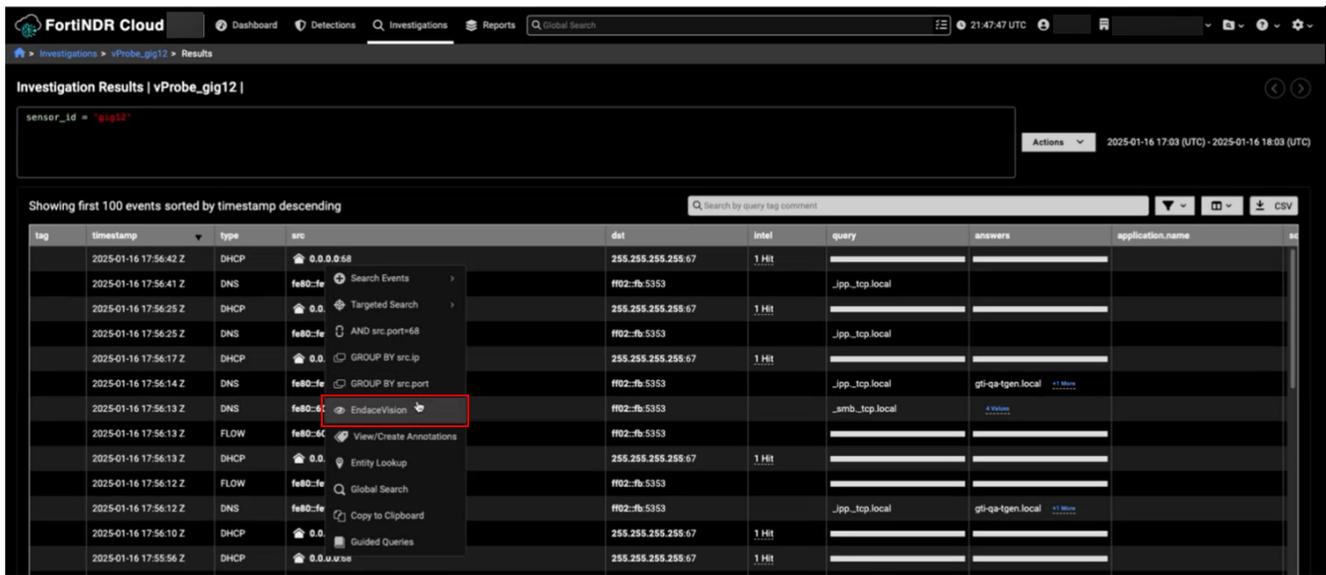
You can pivot to Endace by right-clicking an IP address in the Detections table or the Events table. After you pivot from FortiNDR Cloud, Endace will automatically create a new investigation.

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.

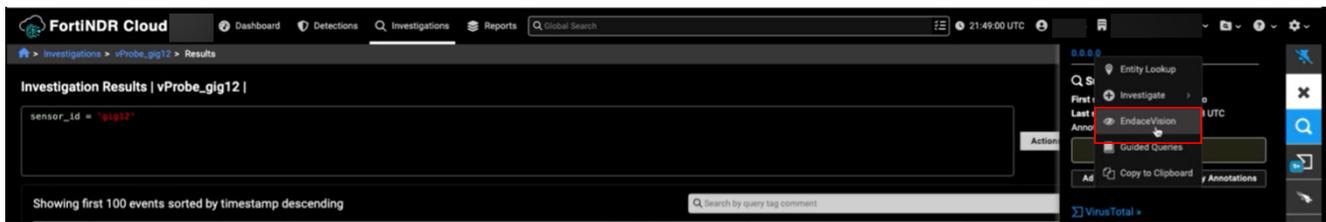


In the *Events* table, right-click the IP address and select the *EndaceVision* to pivot to Endace.

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



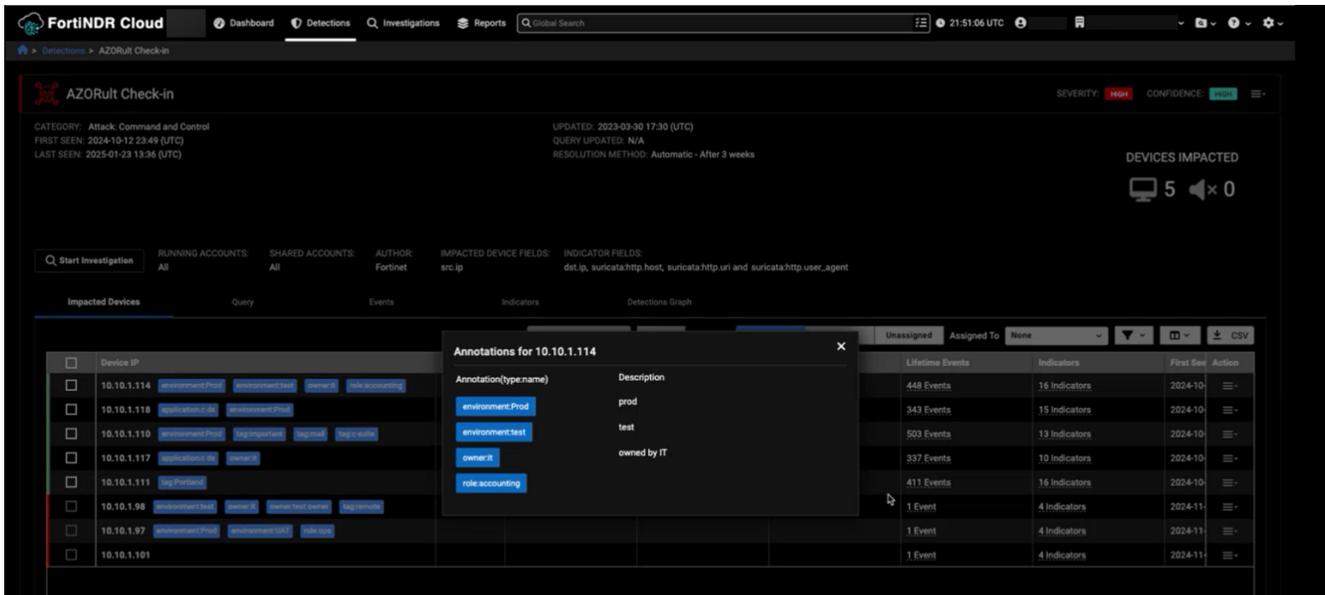
In the *Entity Panel* you can also pivot to Endace by right-clicking the IP address at the top of the panel. The time range used will be the same as the Entity Panel.



Investigations

Annotations

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

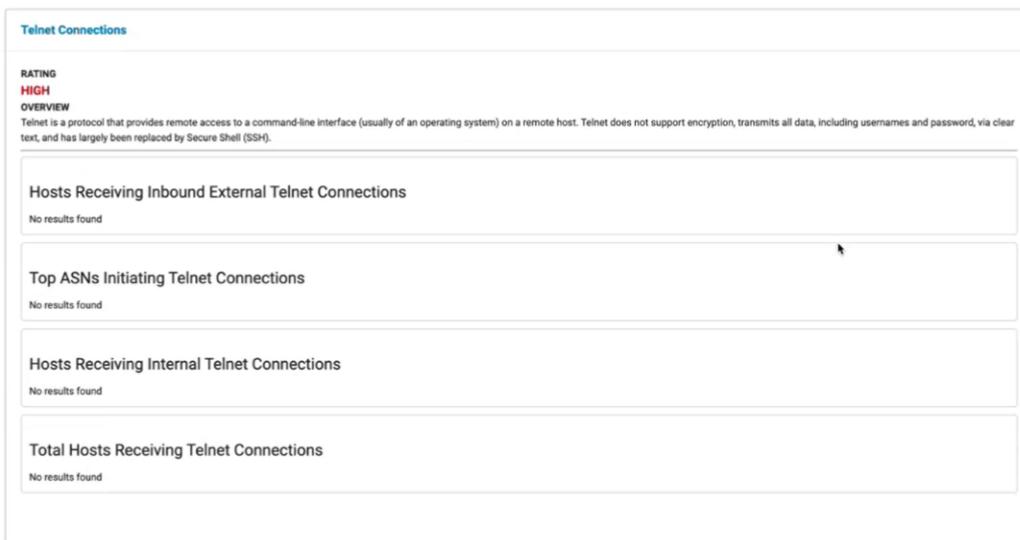


Improved functionality

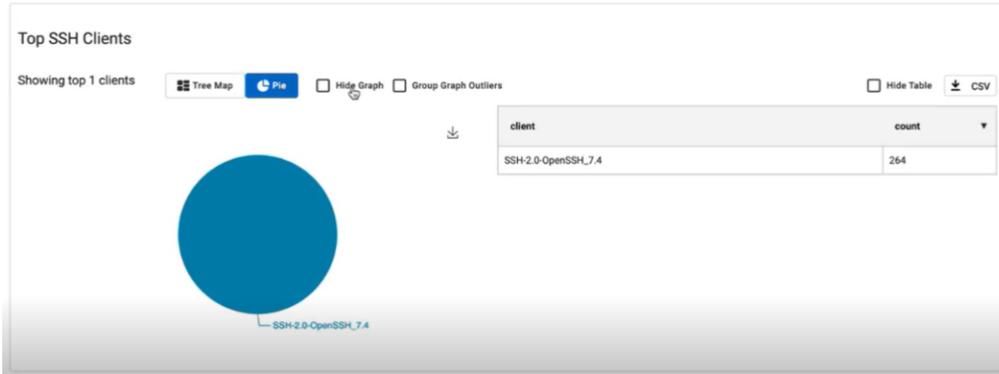
Reports

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.

FortiNDR Cloud

Behavioral Observations

Observation Title	Confidence	First Seen
Anomalous Active Directory Enumeration	LOW	2025-01-15 19:41:25
DNS NXDOMAIN Response for Suspicious Domain	MED	2025-01-20 18:20:01
DNS NXDOMAIN Response for Suspicious Domain	MED	2025-01-20 20:15:57
Domain Similar to Malware DGA Domain	LOW	2025-01-10 07:37:29
Domain Similar to Malware DGA Domain	LOW	2025-01-16 23:06:34
Domain Similar to Malware DGA Domain	MED	2025-01-23 08:39:33
HTTP C2 Similarity	LOW	2025-01-09 23:16:14
Malicious PE File	MED	2025-01-10 06:26:44
Malicious PE File	MED	2025-01-10 03:39:17
New and Unusual NTLM Authentication	LOW	2025-01-10 18:41:00
New Internal Enumeration Source	LOW	2025-01-15 19:40:48

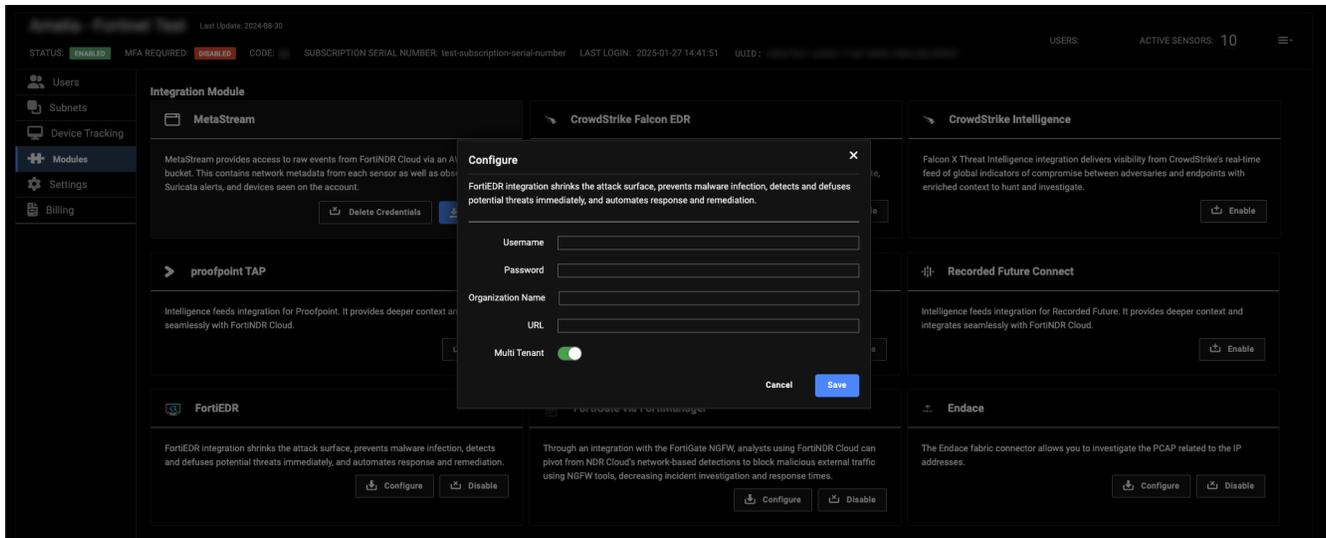
2024-08-01 00:00:00 (UTC) through 2024-08-31 23:59:59 (UTC)

Quick Ranges: Last Hour, Last 24 Hours, Last 7 days, Last 30 days, Last 60 days, Last 90 days

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.

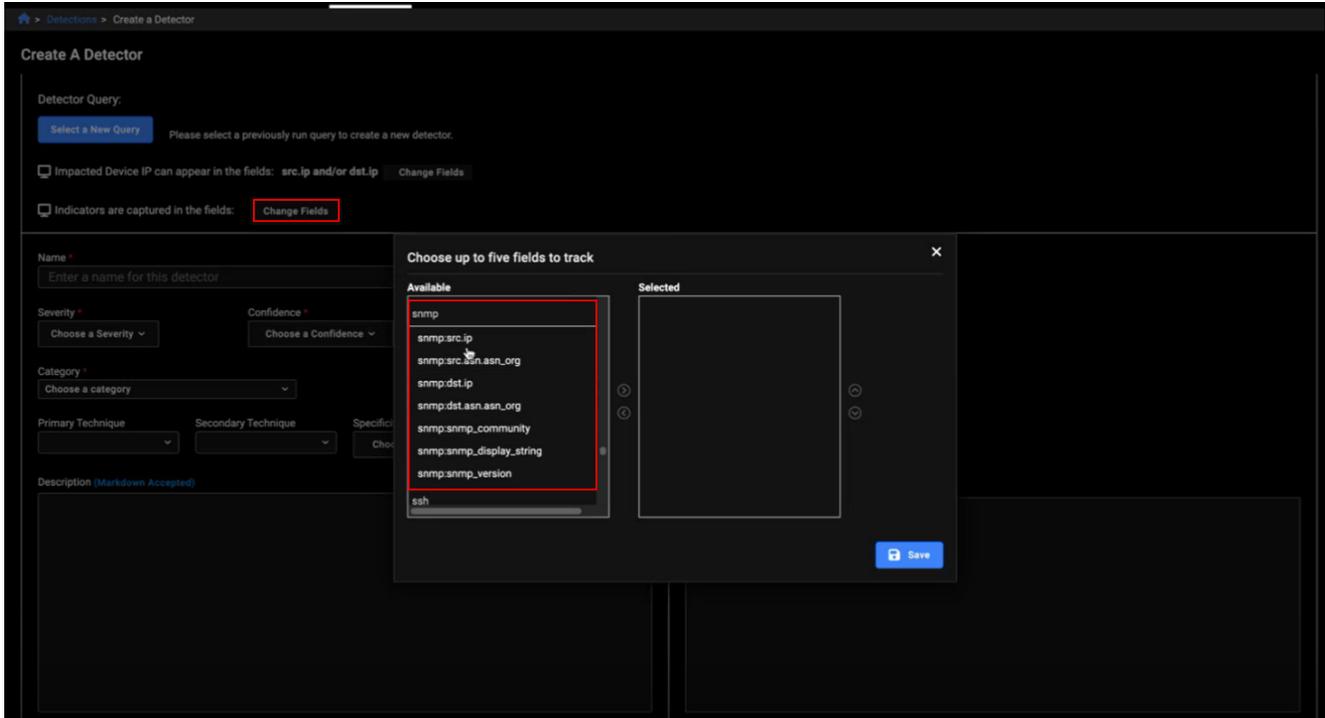
Version 25.1.0

- New functionality on page 97
 - SNMP event fields on page 97
 - Entity Panel on page 98
- Improved functionality on page 99
 - Global Search on page 99
- Other improvements on page 99
- Resolved issues on page 102

New functionality

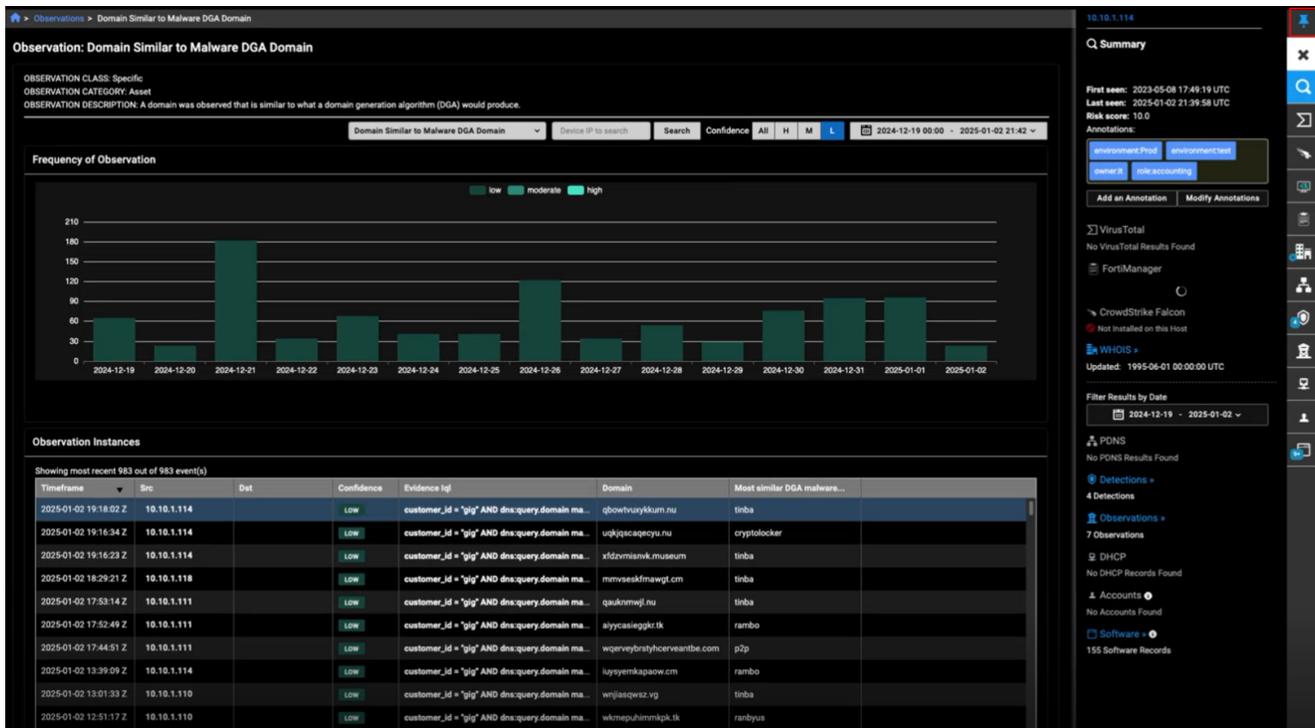
SNMP event fields

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.

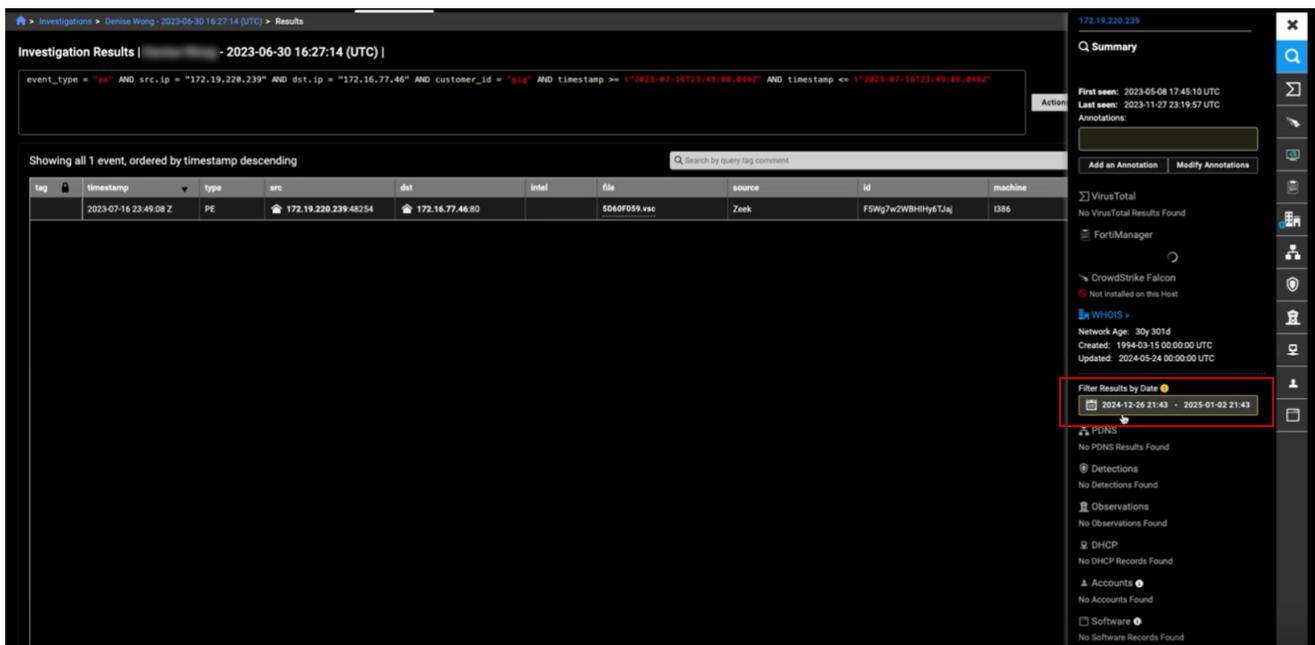


Entity Panel

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.

The screenshot displays the Global Search interface with the following sections:

- Detections:** A table listing various detection events for IP 10.10.1.118, including event counts, indicators, status, and resolution details.
- Detections Coverage:** A section indicating that no detections coverage was found.
- Behavioral Observation:** A table listing behavioral observations such as HTTP.C2 Similarity, Malicious PE File, and TCP Non-Standard Ports Beaconsing, with columns for confidence, category, class, instances, and timestamps.
- Investigations:** A section indicating that no investigations were found.
- Private Search:** A search bar with a query for IP 10.10.1.118 and a 'View Results' button.
- Entity Lookup:** A table showing the entity 10.10.1.118 as an IP address with a count of 630817 and specific first and last seen timestamps.

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.

	ThreatConnect	Available as Integration.
	Tor Nodes	Available to all customers.
	URLHaus	Available to all customers.
Other	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 *API Only* filter in the *Account Management* page.

The *Detections Table* no longer displays a timestamp in the *Mute Comment* 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 *Entity Panel*.

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 *null* values are not included in aggregation results.
- In certain cases, Event searches are incorrectly converted into aggregations.
- Queries on array fields such as `intel` or `dns.answers` return inconsistent or no results.



www.fortinet.com

Copyright © 2026 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.