FORTINET

Release Notes

FortiNDR Cloud 25.4.0

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

November 5, 2025
FortiNDR Cloud 25.4.0 Release Notes
78-254-1113279-20251105

TABLE OF CONTENTS

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
05 November 2025	Version 25.4.0 on page 6
15 September 2025	Version 25.3.c on page 10
03 September 2025	Version 25.3.b on page 16
15 July 2025	Version 25.3.a on page 28
07 July 2025	Version 25.3.0 on page 28
26 June 2025	Version 25.2.c on page 29
21 May 2025	Version 25.2.b on page 39
08 May 2025	Version 25.2.a on page 42
30 April 2025	Version 25.2.0 on page 42
26 March 2025	Version 25.1.e on page 48
12 March 2026	Version 25.1.d on page 55
27 February 2025	Version 25.1.c on page 59
12 February 2025	Version 25.1.b on page 62
29 January 2025	Version 25.1.a on page 64
08 January 2025	Version 25.1.0 on page 69

Version 25.4.0

- Improved functionality
  - Default dashboard
  - Detection device timeline
  - Event fields
- Other improvements
- Resolved issues on page 75

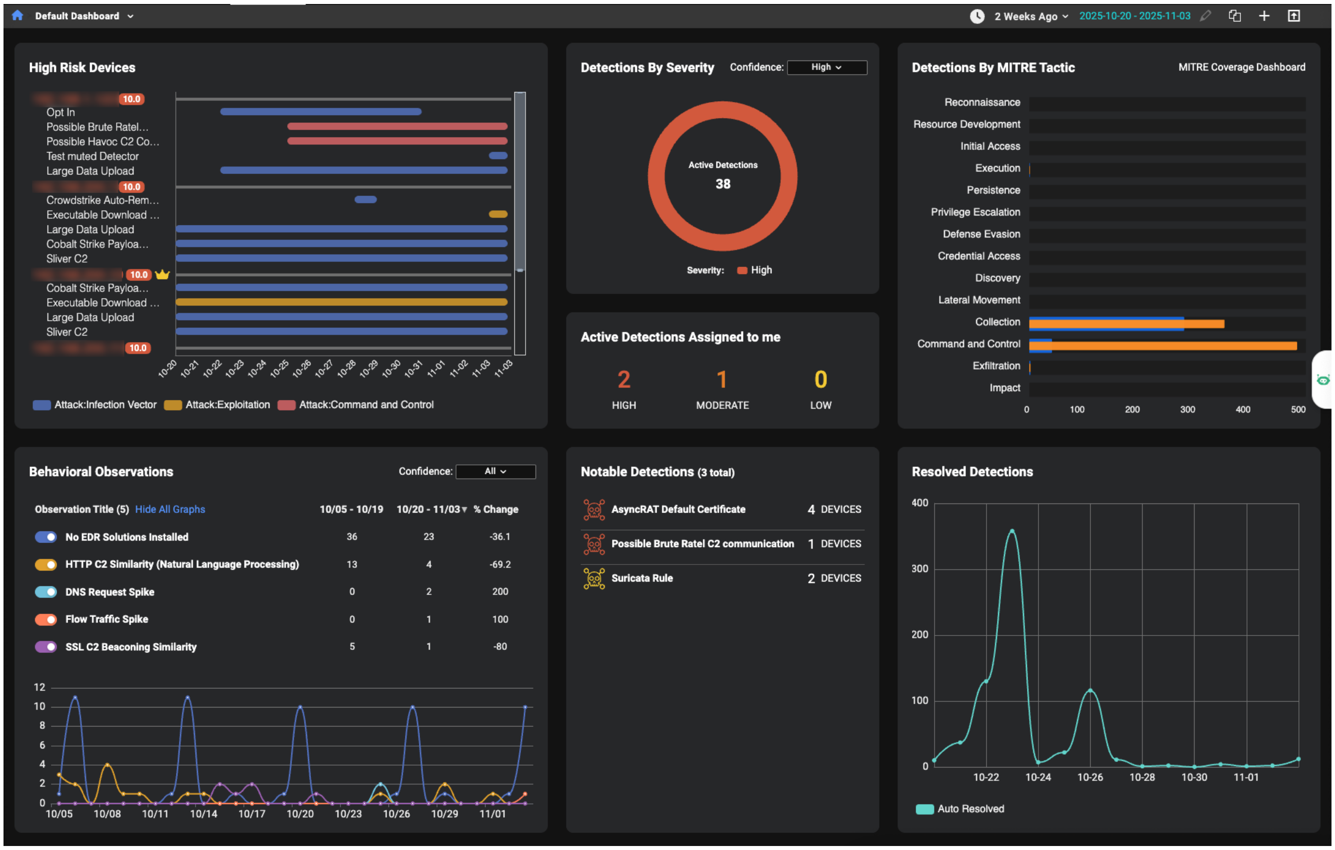
Improved functionality

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.

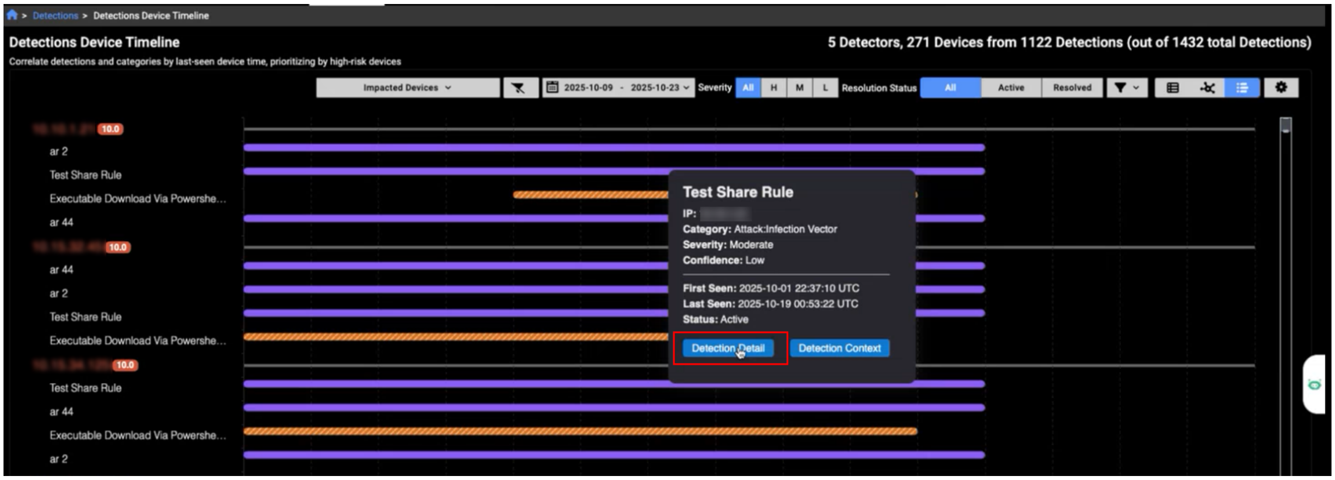


Observation Title (5) Hide All Graphs	10/05 - 10/19	10/20 - 11/03▾	% Change
No EDR Solutions Installed	36	23	-36.1
HTTP C2 Similarity (Natural Language Processing)	13	4	-69.2
DNS Request Spike	0	2	200
Flow Traffic Spike	0	1	100
SSL C2 Beaconing Similarity	5	1	-80

Notable Detections (3 total)	
AsyncRAT Default Certificate	4 DEVICES
Possible Brute Ratel C2 communication	1 DEVICES
Suricata Rule	2 DEVICES

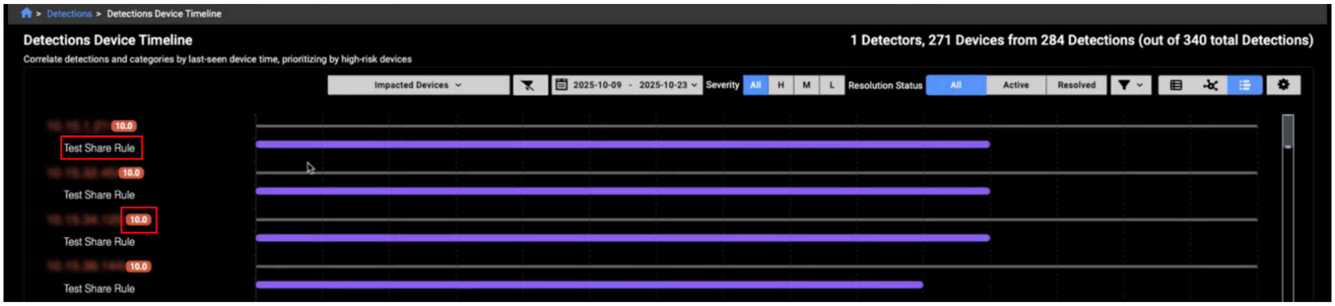
Detection device timeline

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.


Detections > Detections Device Timeline
Detections Device Timeline
Correlate detections and categories by last-seen device time, prioritizing by high-risk devices
5 Detectors, 271 Devices from 1122 Detections (out of 1432 total Detections)
Impacted Devices
2025-10-09 - 2025-10-23
Severity All H M L
Resolution Status All Active Resolved
10.0
ar 2
Test Share Rule
Executable Download Via Powershe...
ar 44
10.0
ar 44
ar 2
Test Share Rule
Executable Download Via Powershe...
10.0
Test Share Rule
ar 44
Executable Download Via Powershe...
ar 2
Detection Detail
Detection Context

Test Share Rule
IP: [redacted]
Category: Attack:Infection Vector
Severity: Moderate
Confidence: Low
First Seen: 2025-10-01 22:37:10 UTC
Last Seen: 2025-10-19 00:53:22 UTC
Status: Active

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.



Detections > Detections Device Timeline

Detections Device Timeline

Correlate detections and categories by last-seen device time, prioritizing by high-risk devices

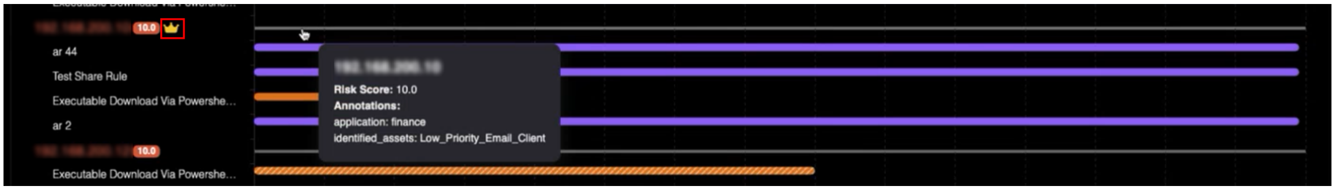
1 Detectors, 271 Devices from 284 Detections (out of 340 total Detections)

2025-10-09 - 2025-10-23

Severity: All

Resolution Status: All

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.



[redacted]

Risk Score: 10.0

Annotations:

application: finance

identified_assets: Low_Priority_Email_Client

Executable Download Via Powershe...
[redacted] 10.0
ar 44
Test Share Rule
Executable Download Via Powershe...
ar 2
[redacted] 10.0
Executable Download Via Powershe...

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 to do not fit a broswer page. We have all also improved the performance of the context menus.

Version 25.3.c

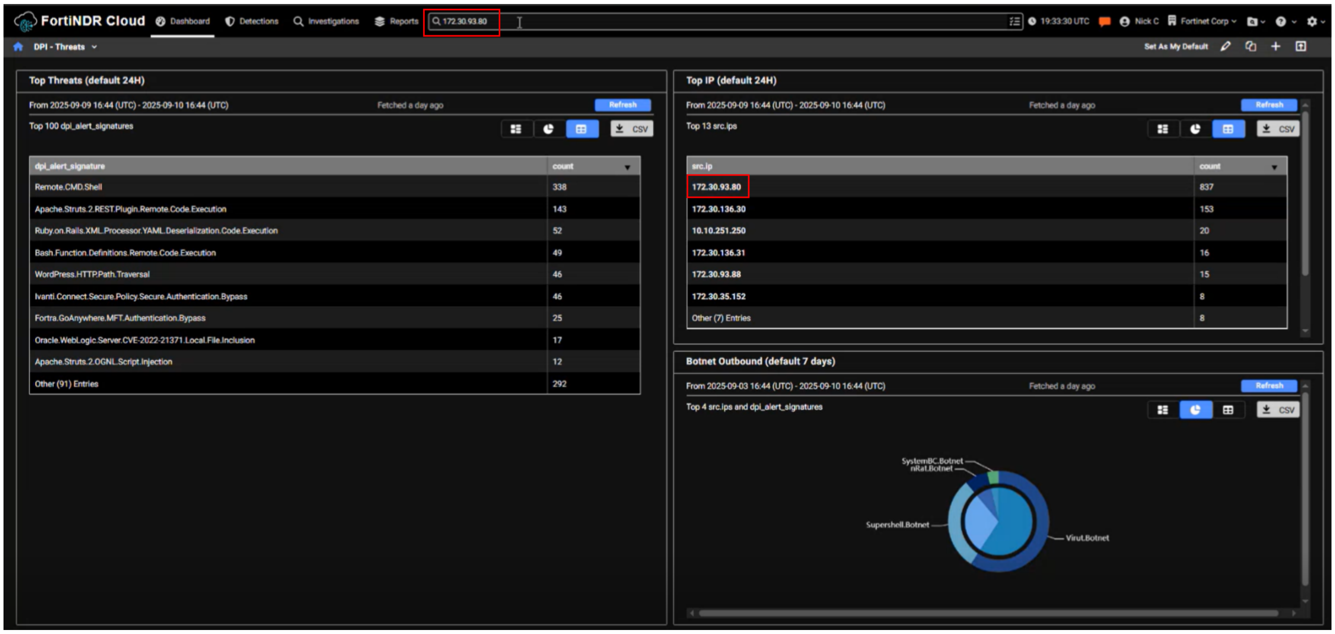
New functionality

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.



Top Threats (default 24H)

From 2025-09-09 16:44 (UTC) - 2025-09-10 16:44 (UTC)   Fetched a day ago   Refresh

Top 100 dpi_alert_signatures   CSV

dpi_alert_signature	count
Remote.CMD.Shell	338
Apache.Struts.2.REST.Plugin.Remote.Code.Execution	143
Ruby.on.Rails.XML.Processor.YAML.Deserialization.Code.Execution	52
Bash.Function.Definitions.Remote.Code.Execution	49
WordPress.HTTP.Path.Traversal	46
Ivanti.Connect.Secure.Policy.Secure.Authentication.Bypass	46
Fortra.GoAnywhere.MFT.Authentication.Bypass	25
Oracle.WebLogic.Server.CVE-2022-21371.Local.File.Inclusion	17
Apache.Struts.2.OGNL.Script.Injection	12
Other (91) Entries	292

Top IP (default 24H)

From 2025-09-09 16:44 (UTC) - 2025-09-10 16:44 (UTC)   Fetched a day ago   Refresh

Top 13 src.ips   CSV

src.ip	count
172.30.93.80	837
172.30.136.30	153
10.10.251.250	20
172.30.136.31	16
172.30.93.88	15
172.30.35.152	8
Other (7) Entries	8

Botnet Outbound (default 7 days)

From 2025-09-03 16:44 (UTC) - 2025-09-10 16:44 (UTC)   Fetched a day ago   Refresh

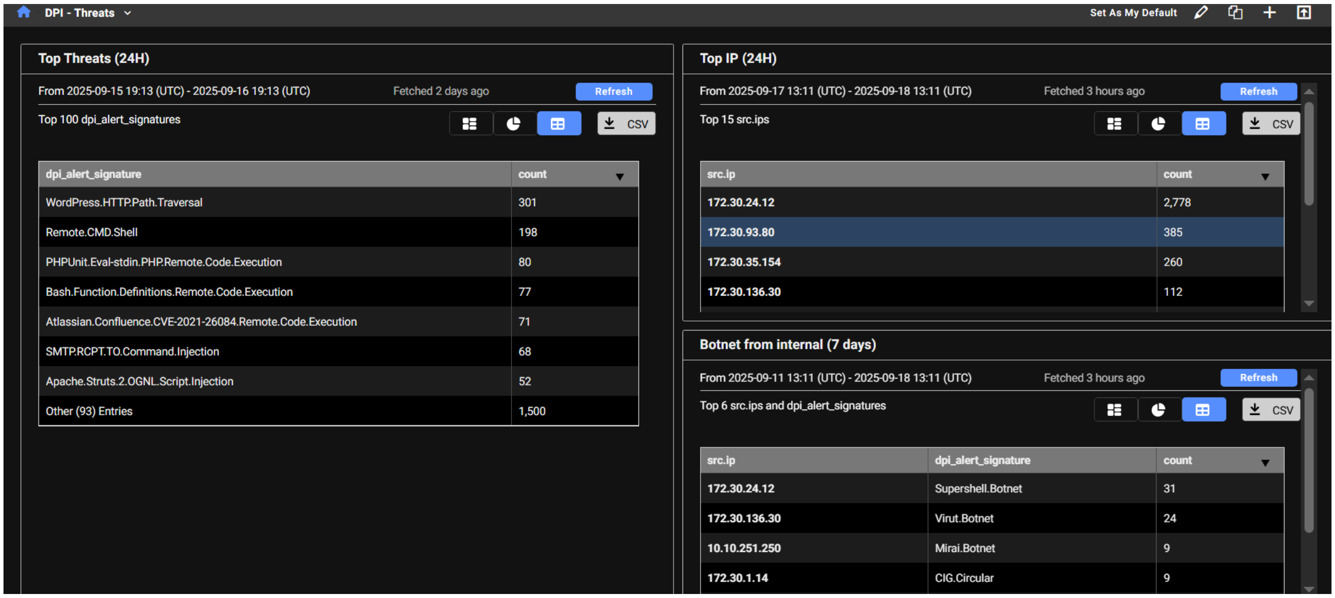
Top 4 src.ips and dpi_alert_signatures   CSV

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.



Top Threats (24H)

From 2025-09-15 19:13 (UTC) - 2025-09-16 19:13 (UTC) Fetched 2 days ago

Top 100 dpi_alert_signatures

dpi_alert_signature	count
WordPress.HTTP.Path.Traversal	301
Remote.CMD.Shell	198
PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	80
Bash.Function.Definitions.Remote.Code.Execution	77
Atlassian.Confluence.CVE-2021-26084.Remote.Code.Execution	71
SMTP.RCPT.TO.Command.Injection	68
Apache.Struts.2.OGNL.Script.Injection	52
Other (93) Entries	1,500

Top IP (24H)

From 2025-09-17 13:11 (UTC) - 2025-09-18 13:11 (UTC) Fetched 3 hours ago

Top 15 src.ips

src.ip	count
172.30.24.12	2,778
172.30.93.80	385
172.30.35.154	260
172.30.136.30	112

Botnet from internal (7 days)

From 2025-09-11 13:11 (UTC) - 2025-09-18 13:11 (UTC) Fetched 3 hours ago

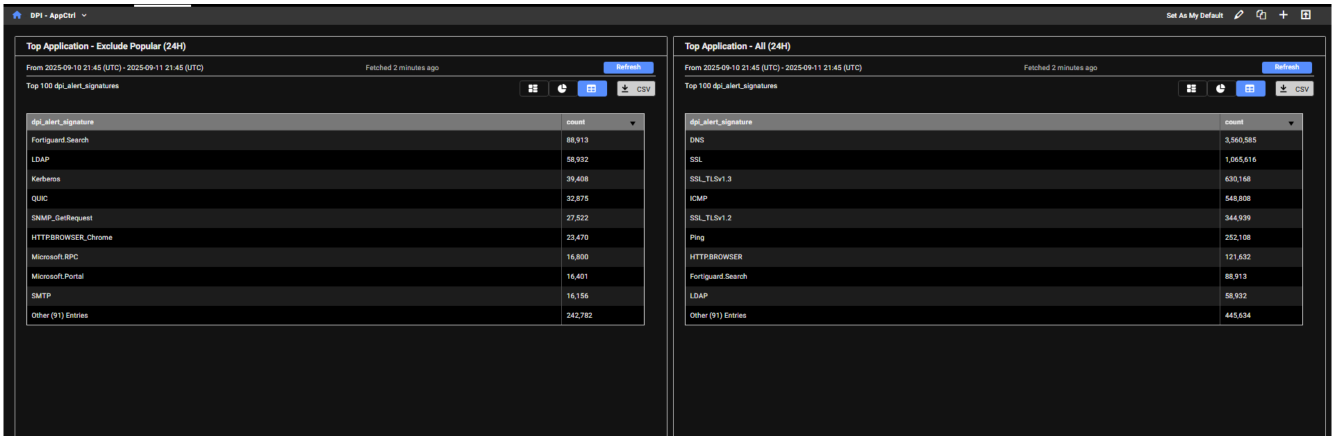
Top 6 src.ips and dpi_alert_signatures

src.ip	dpi_alert_signature	count
172.30.24.12	Supershell.Botnet	31
172.30.136.30	Virut.Botnet	24
10.10.251.250	Mirai.Botnet	9
172.30.1.14	CIG.Circular	9

DPI - AppCtrl

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

Top Application - Exclude Popular (24H)	This monitor filters out common or expected traffic (such as DNS, ICMP, ping, and browser activity) to highlight less typical application usage. The results are grouped by application signature, helping identify less common or potentially suspicious applications being used internally
Top Application - All (24H)	This monitor includes all detected application types, including browser activity, offering a complete view of application traffic. The results are grouped by application signature, allowing you to see which applications are being detected across internal traffic, without the noise from automated scanners. This helps focus on legitimate or potentially suspicious application usage within the network.



Top Application - Exclude Popular (24H)

From 2025-09-10 21:45 (UTC) - 2025-09-11 21:45 (UTC) Fetched 2 minutes ago

Top 100 dpi_alert_signatures

dpi_alert_signature	count
Fortiguard.Search	88,913
LDAP	58,932
Kerberos	39,408
QUIC	32,875
SNMP_GetRequest	27,522
HTTP.BROWSER_Chrome	23,470
Microsoft.RPC	16,800
Microsoft.Portal	16,401
SMTP	16,156
Other (91) Entries	242,782

Top Application - All (24H)

From 2025-09-10 21:45 (UTC) - 2025-09-11 21:45 (UTC) Fetched 2 minutes ago

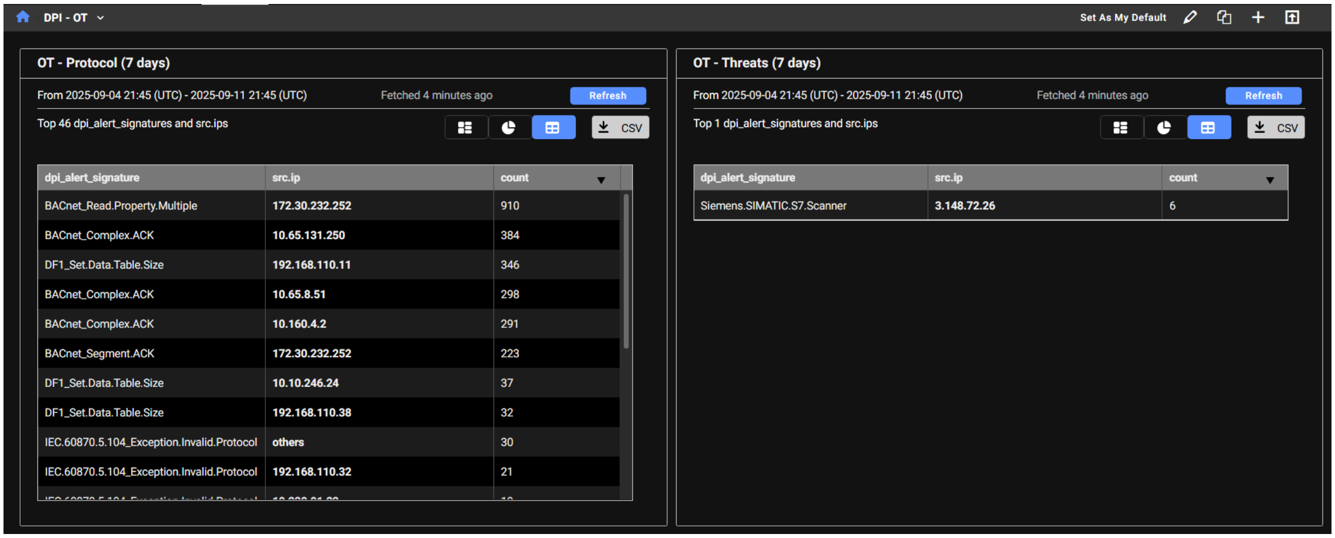
Top 100 dpi_alert_signatures

dpi_alert_signature	count
DNS	3,560,585
SSL	1,065,616
SSL_TLSv1.3	630,168
ICMP	548,808
SSL_TLSv1.2	344,939
Ping	252,108
HTTP.BROWSER	121,632
Fortiguard.Search	88,913
LDAP	58,932
Other (91) Entries	445,634

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.



OT - Protocol (7 days)

From 2025-09-04 21:45 (UTC) - 2025-09-11 21:45 (UTC)

Fetched 4 minutes ago

Top 46 dpi_alert_signatures and src.ips

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

OT - Threats (7 days)

From 2025-09-04 21:45 (UTC) - 2025-09-11 21:45 (UTC)

Fetched 4 minutes ago

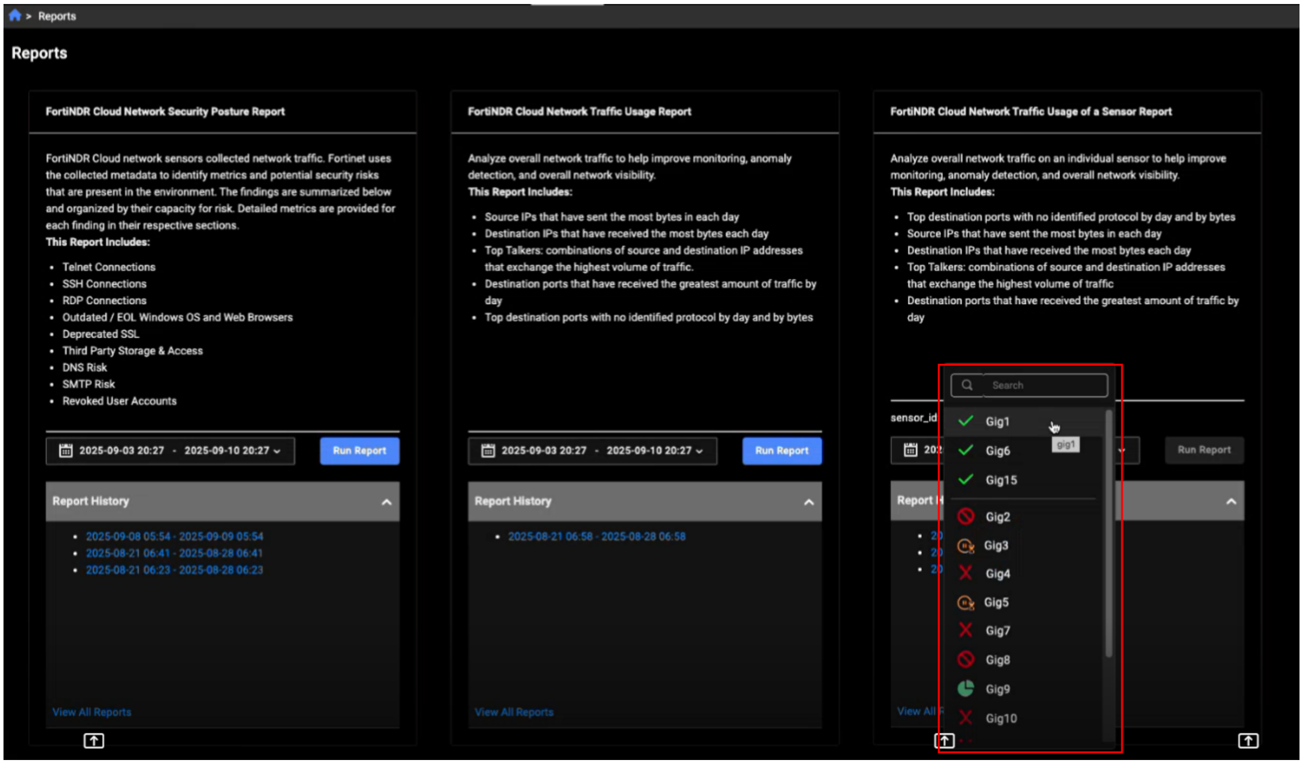
Top 1 dpi_alert_signatures and src.ips

dpi_alert_signature	src.ip	count
Siemens.SIMATIC.S7.Scanner	3.148.72.26	6

Improved functionality

Reports

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



FortiNDR Cloud Network Security Posture Report

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

This Report Includes:

- Telnet Connections
- SSH Connections
- RDP Connections
- Outdated / EOL Windows OS and Web Browsers
- Deprecated SSL
- Third Party Storage & Access
- DNS Risk
- SMTP Risk
- Revoked User Accounts

2025-09-03 20:27 - 2025-09-10 20:27

- 2025-09-08 05:54 - 2025-09-09 05:54
- 2025-08-21 06:41 - 2025-08-28 06:41
- 2025-08-21 06:23 - 2025-08-28 06:23

FortiNDR Cloud Network Traffic Usage Report

Analyze overall network traffic to help improve monitoring, anomaly detection, and overall network visibility.

This Report Includes:

- Source IPs that have sent the most bytes in each day
- Destination IPs that have received the most bytes each day
- Top Talkers: combinations of source and destination IP addresses that exchange the highest volume of traffic.
- Destination ports that have received the greatest amount of traffic by day
- Top destination ports with no identified protocol by day and by bytes

2025-09-03 20:27 - 2025-09-10 20:27

- 2025-08-21 06:58 - 2025-08-28 06:58

FortiNDR Cloud Network Traffic Usage of a Sensor Report

Analyze overall network traffic on an individual sensor to help improve monitoring, anomaly detection, and overall network visibility.

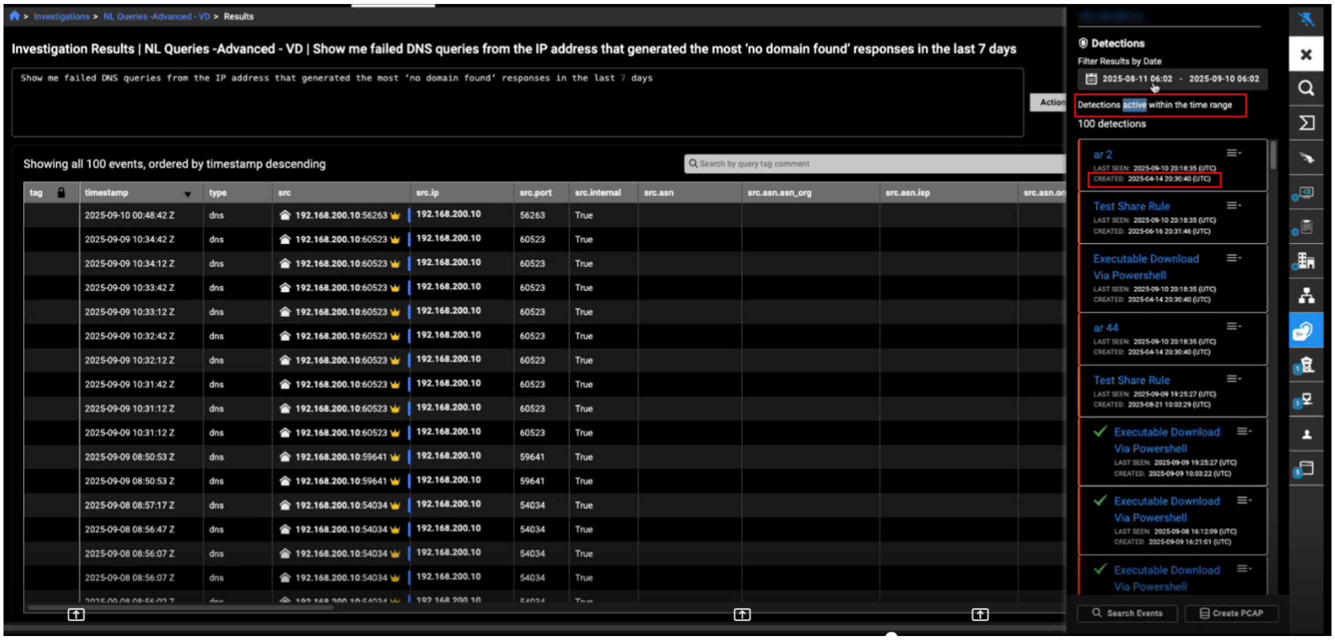
This Report Includes:

- Top destination ports with no identified protocol by day and by bytes
- Source IPs that have sent the most bytes in each day
- Destination IPs that have received the most bytes each day
- Top Talkers: combinations of source and destination IP addresses that exchange the highest volume of traffic
- Destination ports that have received the greatest amount of traffic by day

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.



Investigations > NL Queries -Advanced - VD > Results

Investigation Results | NL Queries -Advanced - VD | Show me failed DNS queries from the IP address that generated the most 'no domain found' responses in the last 7 days

```
Show me failed DNS queries from the IP address that generated the most 'no domain found' responses in the last 7 days
```

Showing all 100 events, ordered by timestamp descending

tag	timestamp	type	src	src.ip	src.port	src.internal	src.asn	src.asn.asn_org	src.asn.isp
	2025-09-10 00:48:42 Z	dns	192.168.200.10:56263	192.168.200.10	56263	True			
	2025-09-09 10:34:42 Z	dns	192.168.200.10:60523	192.168.200.10	60523	True			
	2025-09-09 10:34:12 Z	dns	192.168.200.10:60523	192.168.200.10	60523	True			
	2025-09-09 10:33:42 Z	dns	192.168.200.10:60523	192.168.200.10	60523	True			
	2025-09-09 10:33:12 Z	dns	192.168.200.10:60523	192.168.200.10	60523	True			
	2025-09-09 10:32:42 Z	dns	192.168.200.10:60523	192.168.200.10	60523	True			
	2025-09-09 10:32:12 Z	dns	192.168.200.10:60523	192.168.200.10	60523	True			
	2025-09-09 10:31:42 Z	dns	192.168.200.10:60523	192.168.200.10	60523	True			
	2025-09-09 10:31:12 Z	dns	192.168.200.10:60523	192.168.200.10	60523	True			
	2025-09-09 10:31:12 Z	dns	192.168.200.10:60523	192.168.200.10	60523	True			
	2025-09-09 08:50:53 Z	dns	192.168.200.10:59641	192.168.200.10	59641	True			
	2025-09-09 08:50:53 Z	dns	192.168.200.10:59641	192.168.200.10	59641	True			
	2025-09-08 08:57:17 Z	dns	192.168.200.10:54034	192.168.200.10	54034	True			
	2025-09-08 08:56:47 Z	dns	192.168.200.10:54034	192.168.200.10	54034	True			
	2025-09-08 08:56:07 Z	dns	192.168.200.10:54034	192.168.200.10	54034	True			
	2025-09-08 08:56:07 Z	dns	192.168.200.10:54034	192.168.200.10	54034	True			

Detections

Filter Results by Date

2025-08-11 06:02 - 2025-09-10 06:02

Detections active within the time range

100 detections

ar 2
LAST SEEN: 2025-09-10 20:18:35 (UTC)
CREATED: 2025-04-14 20:30:40 (UTC)

Test Share Rule
LAST SEEN: 2025-09-10 20:18:35 (UTC)
CREATED: 2025-06-16 20:31:46 (UTC)

Executable Download Via Powershell
LAST SEEN: 2025-09-10 20:18:35 (UTC)
CREATED: 2025-04-14 20:30:40 (UTC)

ar 44
LAST SEEN: 2025-09-10 20:18:35 (UTC)
CREATED: 2025-04-14 20:30:40 (UTC)

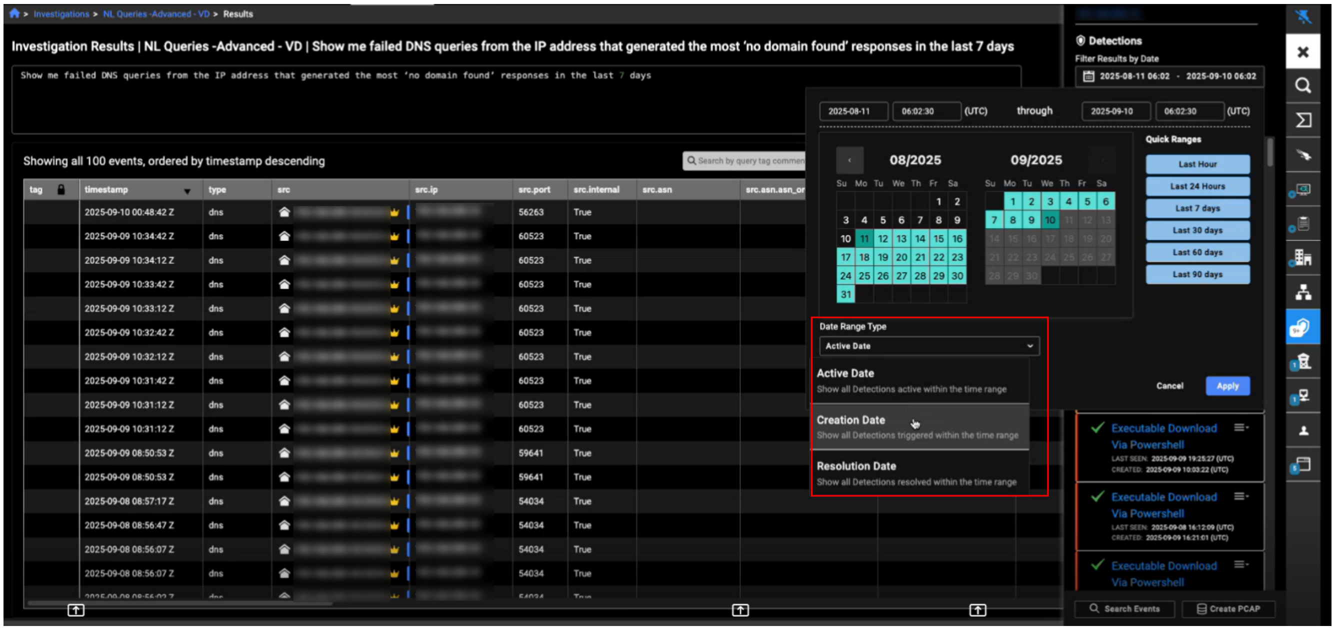
Test Share Rule
LAST SEEN: 2025-09-09 19:25:27 (UTC)
CREATED: 2025-08-21 10:03:29 (UTC)

✓ Executable Download Via Powershell
LAST SEEN: 2025-09-09 19:25:27 (UTC)
CREATED: 2025-09-09 10:03:22 (UTC)

✓ Executable Download Via Powershell
LAST SEEN: 2025-09-08 16:12:09 (UTC)
CREATED: 2025-09-09 16:21:01 (UTC)

✓ Executable Download Via Powershell

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.



Investigations > NL Queries -Advanced - VD > Results

Investigation Results | NL Queries -Advanced - VD | Show me failed DNS queries from the IP address that generated the most 'no domain found' responses in the last 7 days

```
Show me failed DNS queries from the IP address that generated the most 'no domain found' responses in the last 7 days
```

Showing all 100 events, ordered by timestamp descending

tag	timestamp	type	src	src.ip	src.port	src.internal	src.asn	src.asn.asn_or
	2025-09-10 00:48:42 Z	dns	[redacted]	[redacted]	56263	True		
	2025-09-09 10:34:42 Z	dns	[redacted]	[redacted]	60523	True		
	2025-09-09 10:34:12 Z	dns	[redacted]	[redacted]	60523	True		
	2025-09-09 10:33:42 Z	dns	[redacted]	[redacted]	60523	True		
	2025-09-09 10:33:12 Z	dns	[redacted]	[redacted]	60523	True		
	2025-09-09 10:32:42 Z	dns	[redacted]	[redacted]	60523	True		
	2025-09-09 10:32:12 Z	dns	[redacted]	[redacted]	60523	True		
	2025-09-09 10:31:42 Z	dns	[redacted]	[redacted]	60523	True		
	2025-09-09 10:31:12 Z	dns	[redacted]	[redacted]	60523	True		
	2025-09-09 10:31:12 Z	dns	[redacted]	[redacted]	60523	True		
	2025-09-09 08:50:53 Z	dns	[redacted]	[redacted]	59641	True		
	2025-09-09 08:50:53 Z	dns	[redacted]	[redacted]	59641	True		
	2025-09-08 08:57:17 Z	dns	[redacted]	[redacted]	54034	True		
	2025-09-08 08:56:47 Z	dns	[redacted]	[redacted]	54034	True		
	2025-09-08 08:56:07 Z	dns	[redacted]	[redacted]	54034	True		
	2025-09-08 08:56:07 Z	dns	[redacted]	[redacted]	54034	True		

Detections

Filter Results by Date

2025-08-11 06:02 - 2025-09-10 06:02

2025-08-11 06:02:30 (UTC) through 2025-09-10 06:02:30 (UTC)

Date Range Type: Active Date

Active Date
Show all Detections active within the time range

Creation Date
Show all Detections triggered within the time range

Resolution Date
Show all Detections resolved within the time range

✓ Executable Download Via Powershell
LAST SEEN: 2025-09-09 19:25:27 (UTC)
CREATED: 2025-09-09 10:03:22 (UTC)

✓ Executable Download Via Powershell
LAST SEEN: 2025-09-08 16:12:09 (UTC)
CREATED: 2025-09-09 16:21:01 (UTC)

✓ Executable Download Via Powershell

Other improvements

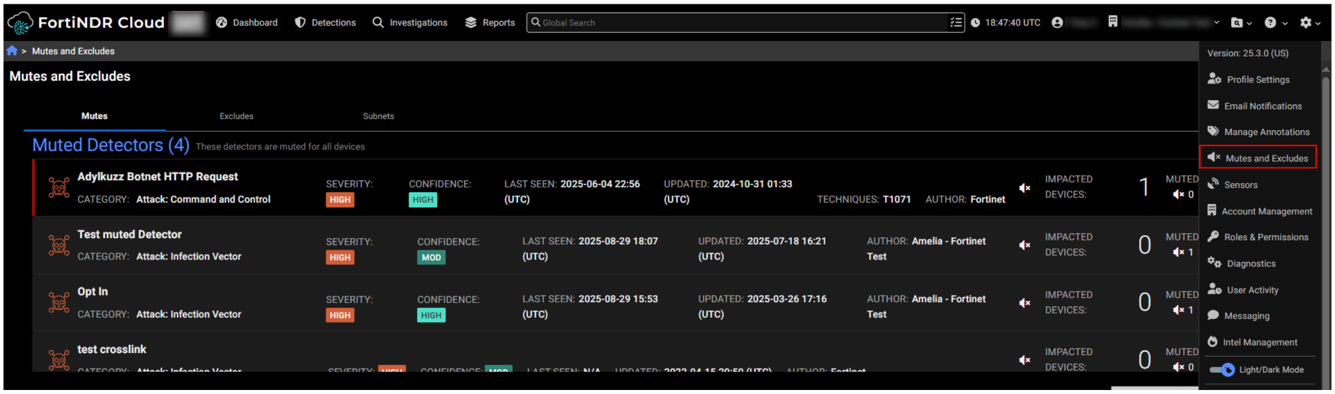
- This release includes internal hardening updates to improve system security and resilience.

Version 25.3.b

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 and Excludes

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

Adylkuzz Botnet HTTP Request
CATEGORY: Attack: Command and Control
SEVERITY: HIGH CONFIDENCE: HIGH LAST SEEN: 2025-06-04 22:56 (UTC) UPDATED: 2024-10-31 01:33 (UTC) TECHNIQUES: T1071 AUTHOR: Fortinet
IMPACTED DEVICES: 1 MUTED 0

Test muted Detector
CATEGORY: Attack: Infection Vector
SEVERITY: HIGH CONFIDENCE: MOD LAST SEEN: 2025-08-29 18:07 (UTC) UPDATED: 2025-07-18 16:21 (UTC) AUTHOR: Amelia - Fortinet Test
IMPACTED DEVICES: 0 MUTED 1

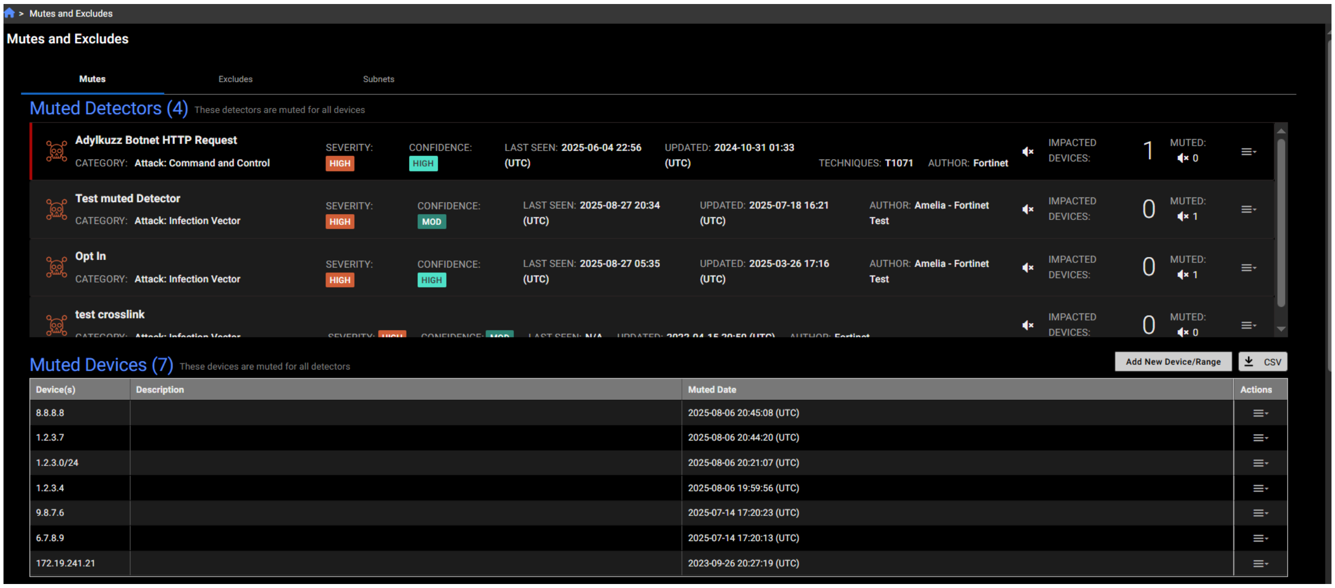
Opt In
CATEGORY: Attack: Infection Vector
SEVERITY: HIGH CONFIDENCE: HIGH LAST SEEN: 2025-08-29 15:53 (UTC) UPDATED: 2025-03-26 17:16 (UTC) AUTHOR: Amelia - Fortinet Test
IMPACTED DEVICES: 0 MUTED 1

test crosslink
CATEGORY: Attack: Infection Vector SEVERITY: HIGH CONFIDENCE: MOD LAST SEEN: N/A UPDATED: 2022-04-15 20:50 (UTC) AUTHOR: Fortinet
IMPACTED DEVICES: 0 MUTED 0

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.



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

Adylkuzz Botnet HTTP Request
CATEGORY: Attack: Command and Control — SEVERITY: HIGH — CONFIDENCE: HIGH — LAST SEEN: 2025-06-04 22:56 (UTC) — UPDATED: 2024-10-31 01:33 (UTC) — TECHNIQUES: T1071 — AUTHOR: Fortinet — IMPACTED DEVICES: 1 — MUTED: 0

Test muted Detector
CATEGORY: Attack: Infection Vector — SEVERITY: HIGH — CONFIDENCE: MOD — LAST SEEN: 2025-08-27 20:34 (UTC) — UPDATED: 2025-07-18 16:21 (UTC) — AUTHOR: Amelia - Fortinet Test — IMPACTED DEVICES: 0 — MUTED: 1

Opt In
CATEGORY: Attack: Infection Vector — SEVERITY: HIGH — CONFIDENCE: HIGH — LAST SEEN: 2025-08-27 05:35 (UTC) — UPDATED: 2025-03-26 17:16 (UTC) — AUTHOR: Amelia - Fortinet Test — IMPACTED DEVICES: 0 — MUTED: 1

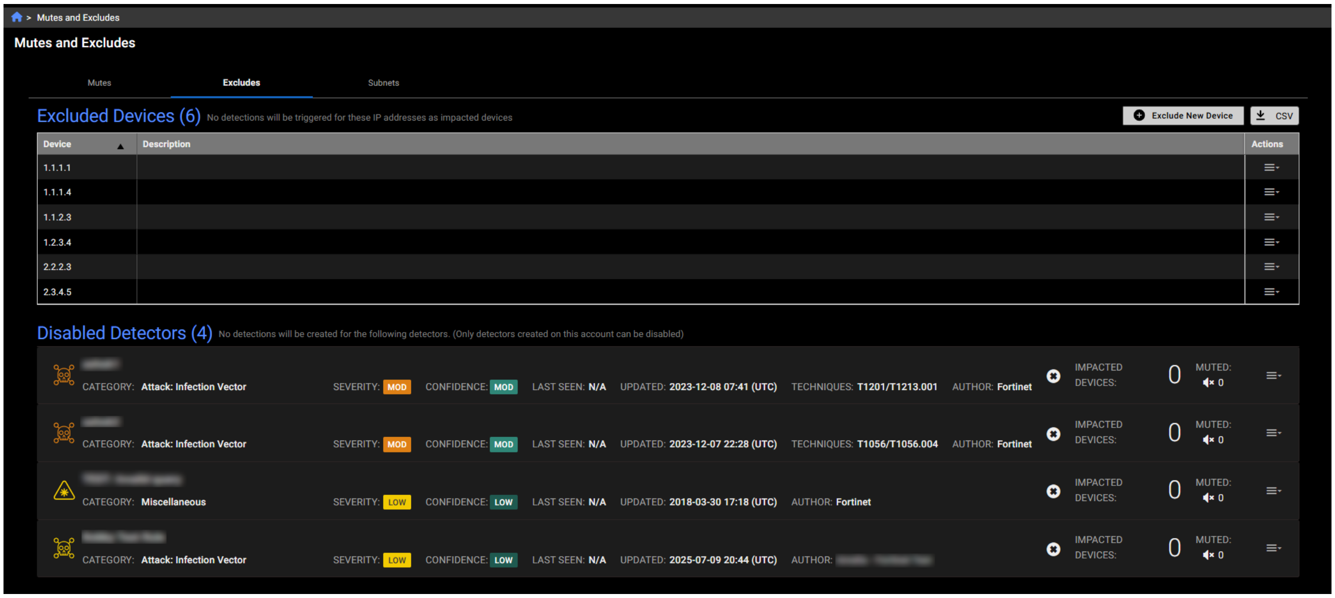
test crosslink
CATEGORY: Attack: Infection Vector — SEVERITY: HIGH — CONFIDENCE: MOD — LAST SEEN: N/A — UPDATED: 2022-04-15 20:50 (UTC) — AUTHOR: Fortinet — IMPACTED DEVICES: 0 — MUTED: 0

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

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

Excludes tab

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



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)

[redacted]
CATEGORY: Attack: Infection Vector — SEVERITY: MOD — CONFIDENCE: MOD — LAST SEEN: N/A — UPDATED: 2023-12-08 07:41 (UTC) — TECHNIQUES: T1201/T1213.001 — AUTHOR: Fortinet — IMPACTED DEVICES: 0 — MUTED: 0

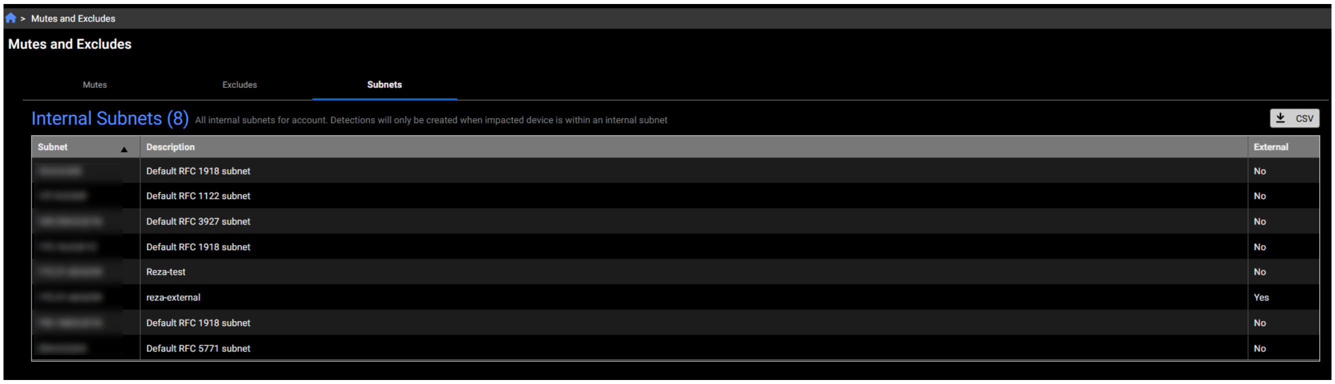
[redacted]
CATEGORY: Attack: Infection Vector — SEVERITY: MOD — CONFIDENCE: MOD — LAST SEEN: N/A — UPDATED: 2023-12-07 22:28 (UTC) — TECHNIQUES: T1056/T1056.004 — AUTHOR: Fortinet — IMPACTED DEVICES: 0 — MUTED: 0

[redacted]
CATEGORY: Miscellaneous — SEVERITY: LOW — CONFIDENCE: LOW — LAST SEEN: N/A — UPDATED: 2018-03-30 17:18 (UTC) — AUTHOR: Fortinet — IMPACTED DEVICES: 0 — MUTED: 0

[redacted]
CATEGORY: Attack: Infection Vector — SEVERITY: LOW — CONFIDENCE: LOW — LAST SEEN: N/A — UPDATED: 2025-07-09 20:44 (UTC) — AUTHOR: [redacted] — IMPACTED DEVICES: 0 — MUTED: 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

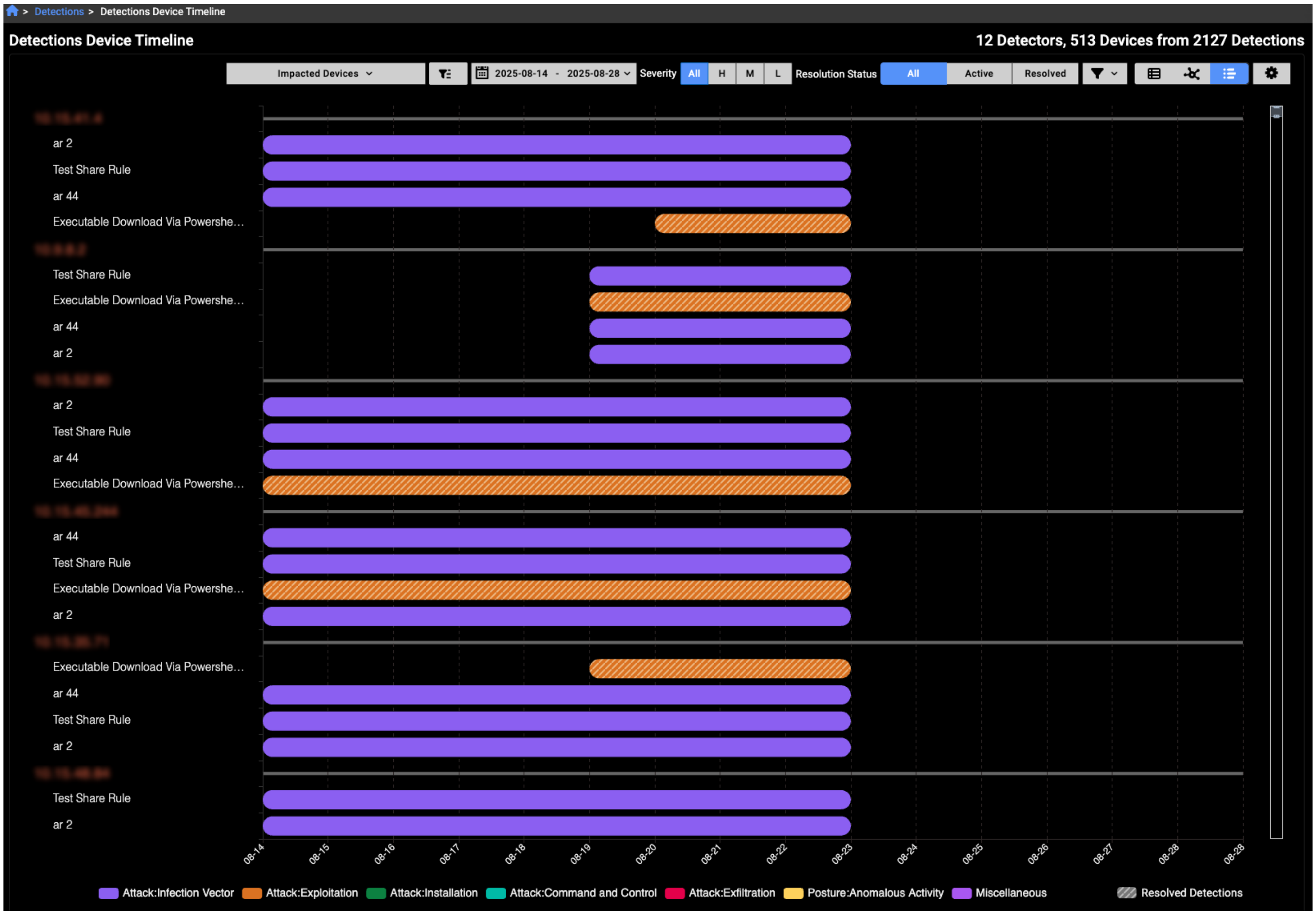


Internal Subnets (8) All internal subnets for account. Detections will only be created when impacted device is within an internal subnet

Subnet	Description	External
[redacted]	Default RFC 1918 subnet	No
[redacted]	Default RFC 1122 subnet	No
[redacted]	Default RFC 3927 subnet	No
[redacted]	Default RFC 1918 subnet	No
[redacted]	Reza-test	No
[redacted]	reza-external	Yes
[redacted]	Default RFC 1918 subnet	No
[redacted]	Default RFC 5771 subnet	No

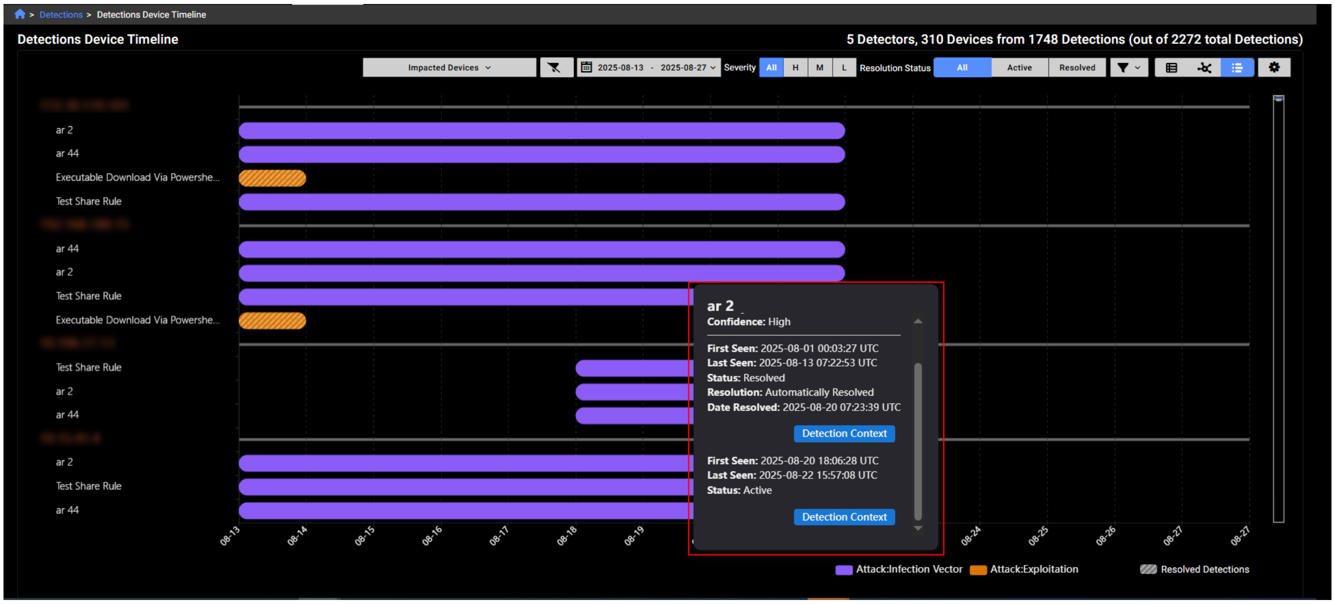
Detections Device Timeline

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.



ar 2
Confidence: High

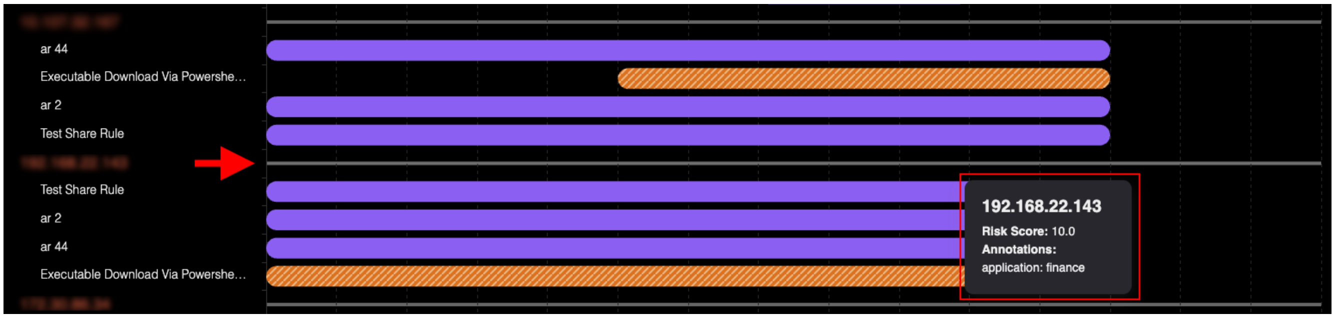
First Seen: 2025-08-01 00:03:27 UTC
Last Seen: 2025-08-13 07:22:53 UTC
Status: Resolved
Resolution: Automatically Resolved
Date Resolved: 2025-08-20 07:23:39 UTC

Detection Context

First Seen: 2025-08-20 18:06:28 UTC
Last Seen: 2025-08-22 15:57:08 UTC
Status: Active

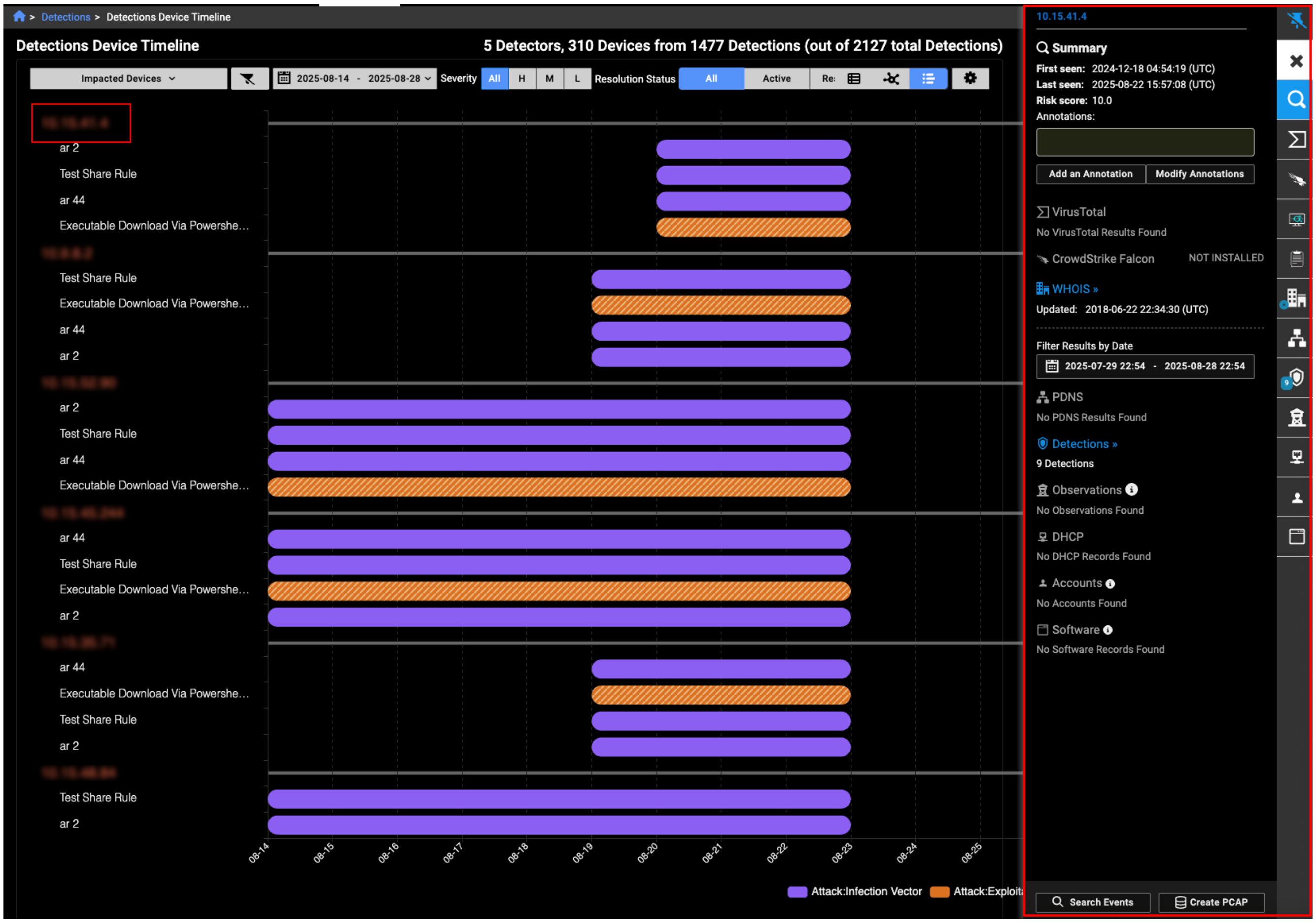
Detection Context

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



192.168.22.143
Risk Score: 10.0
Annotations:
application: finance

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



Detections > Detections Device Timeline

Detections Device Timeline

5 Detectors, 310 Devices from 1477 Detections (out of 2127 total Detections)

10.15.41.4

Summary

First seen: 2024-12-18 04:54:19 (UTC)
Last seen: 2025-08-22 15:57:08 (UTC)
Risk score: 10.0
Annotations:

VirusTotal
No VirusTotal Results Found

CrowdStrike Falcon NOT INSTALLED

WHOIS »
Updated: 2018-06-22 22:34:30 (UTC)

Filter Results by Date
2025-07-29 22:54 - 2025-08-28 22:54

PDNS
No PDNS Results Found

Detections »
9 Detections

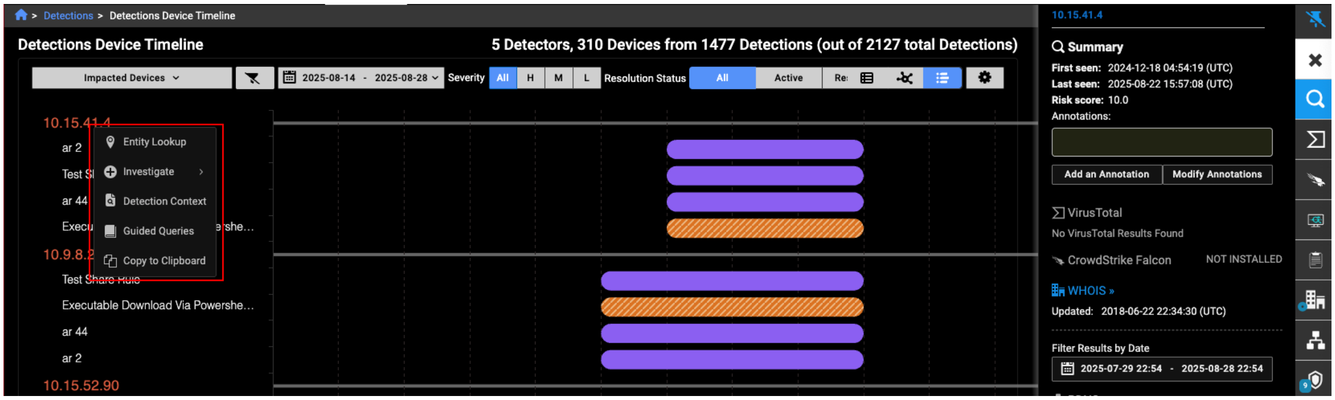
Observations
No Observations Found

DHCP
No DHCP Records Found

Accounts
No Accounts Found

Software
No Software Records Found

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



Detections > Detections Device Timeline

Detections Device Timeline

5 Detectors, 310 Devices from 1477 Detections (out of 2127 total Detections)

10.15.41.4

Summary

First seen: 2024-12-18 04:54:19 (UTC)
Last seen: 2025-08-22 15:57:08 (UTC)
Risk score: 10.0
Annotations:

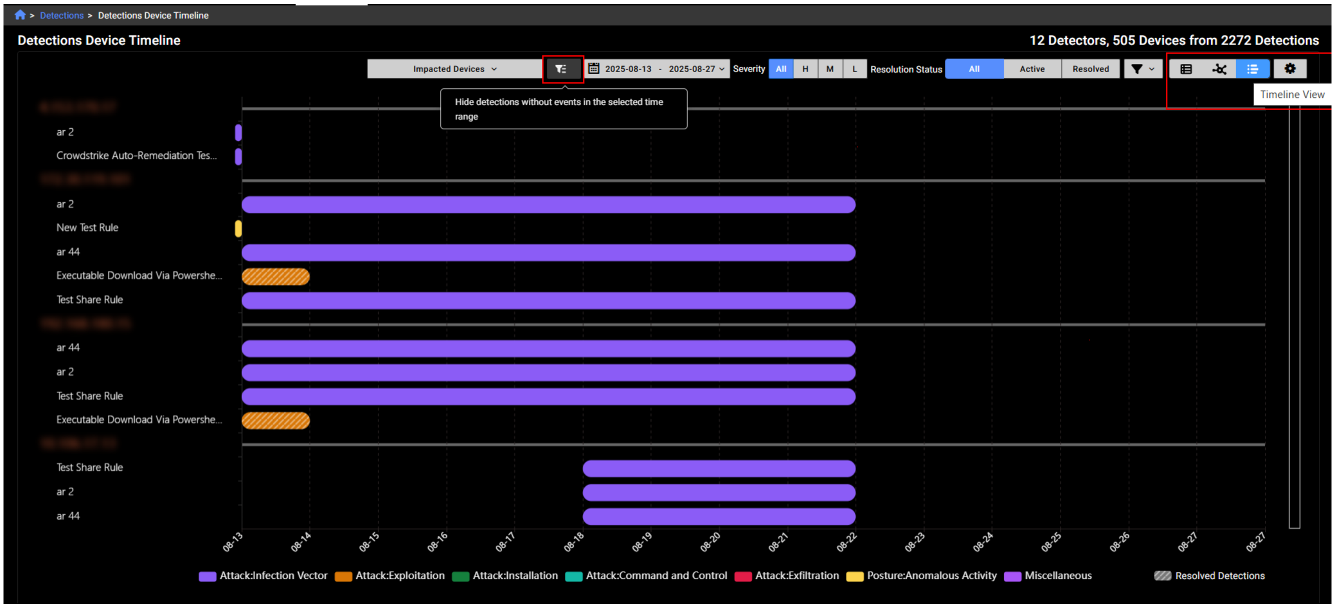
VirusTotal
No VirusTotal Results Found

CrowdStrike Falcon NOT INSTALLED

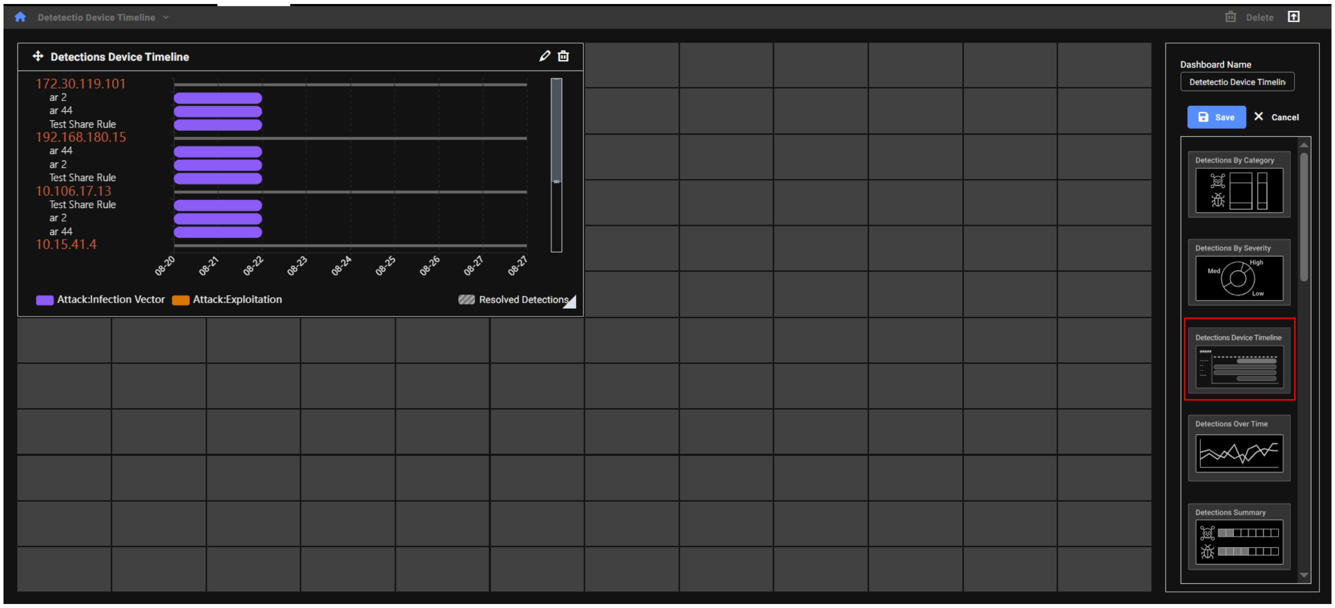
WHOIS »
Updated: 2018-06-22 22:34:30 (UTC)

Filter Results by Date
2025-07-29 22:54 - 2025-08-28 22:54

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.



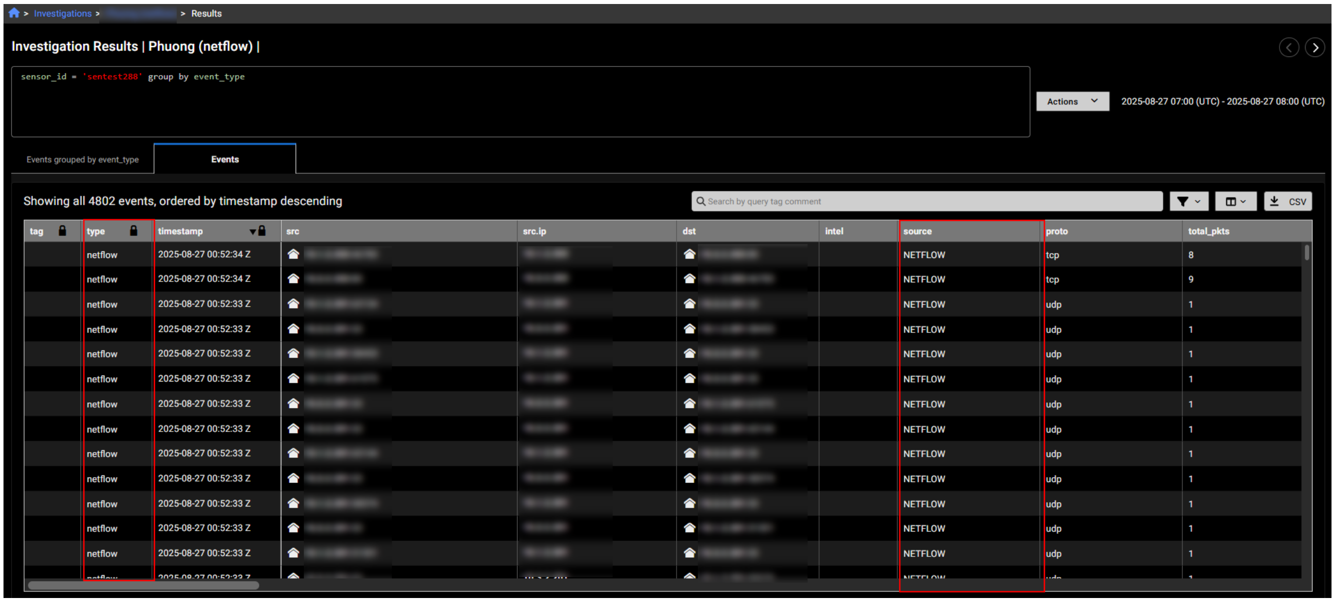
The *Detections Device Timeline* is available as a dedicated dashboard widget. By default, it displays the top five IPs with the highest risk scores from the past seven days. These settings are customizable.



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.


Investigations > [redacted] > Results

Investigation Results | Phuong (netflow) |

```
sensor_id = 'sentest288' group by event_type
```

Actions
2025-08-27 07:00 (UTC) - 2025-08-27 08:00 (UTC)
Events grouped by event_type
Events
Search by query tag comment
CSV

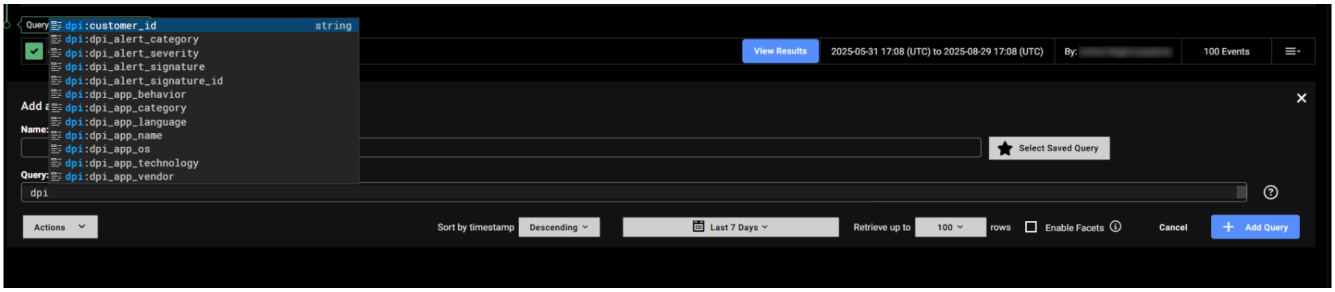
Showing all 4802 events, ordered by timestamp descending

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

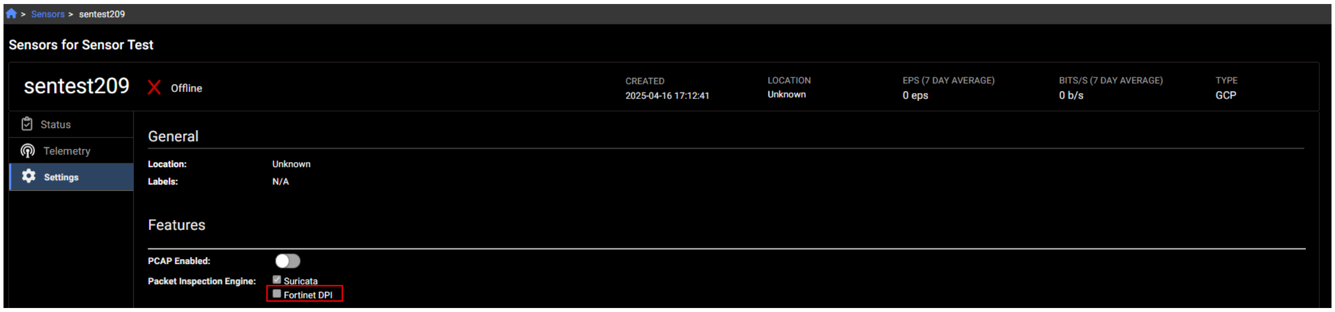
DPI alerts classify network activity and threats into key categories. *AppID* identifies applications like DNS, P2P, and social media. *OT - Protocol* detects operational technology protocols, while *OT - Threats* flags malicious activity in OT environments. *Botnet* alerts track known botnets, and IDS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



```
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

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



Sensors for Sensor Test

sentest209 Offline

CREATED	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE
2025-04-16 17:12:41	Unknown	0 eps	0 b/s	GCP

General

Location: Unknown
Labels: N/A

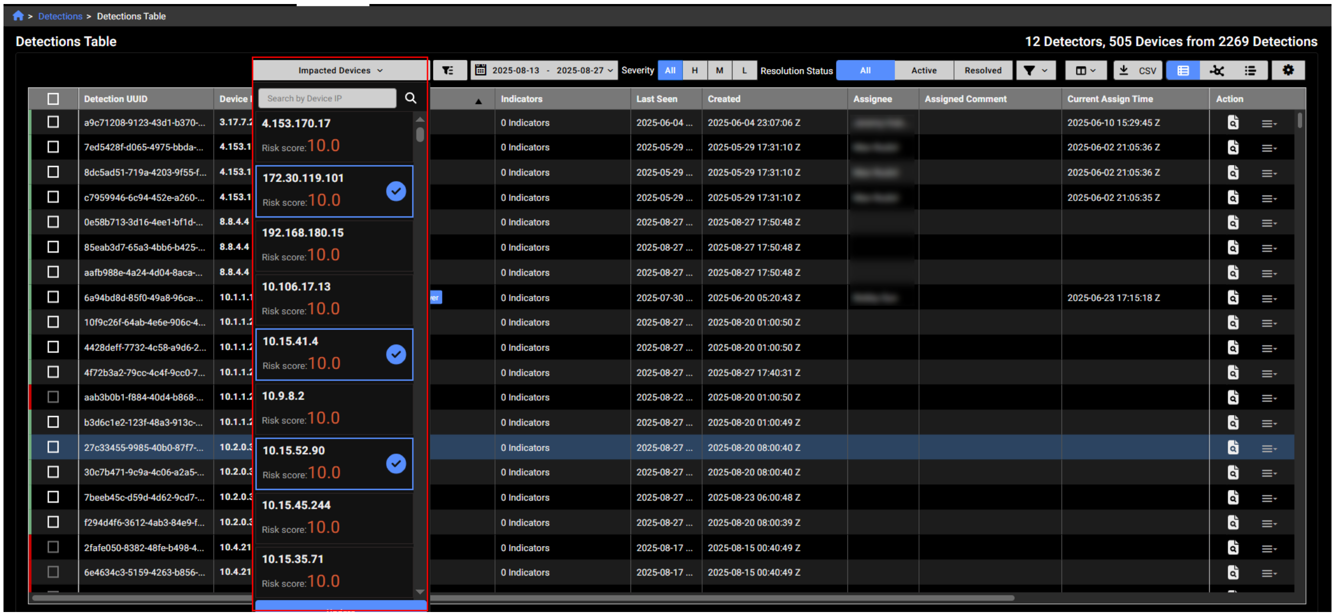
Features

PCAP Enabled:
Packet Inspection Engine: ☑ Suricata ☐ 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.



Detections > Detections Table

Detections Table

12 Detectors, 505 Devices from 2269 Detections

Impacted Devices
2025-08-13 - 2025-08-27
Severity All H M L
Resolution Status All Active Resolved
CSV

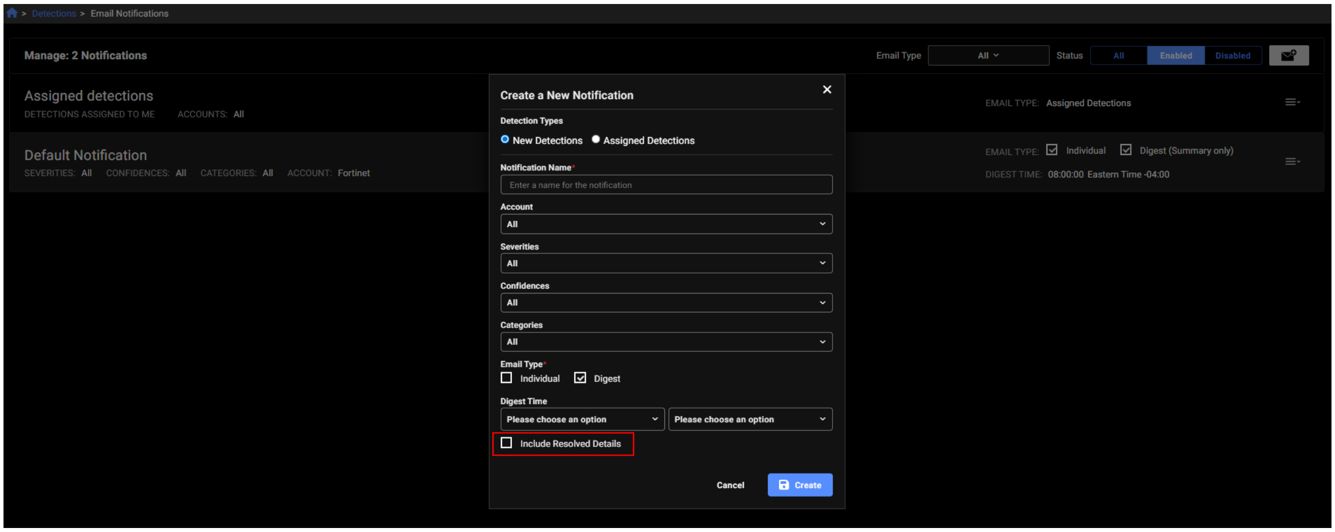
Search by Device IP

- 4.153.170.17 Risk score: 10.0
- 172.30.119.101 Risk score: 10.0 ✓
- 192.168.180.15 Risk score: 10.0
- 10.106.17.13 Risk score: 10.0
- 10.15.41.4 Risk score: 10.0 ✓
- 10.9.8.2 Risk score: 10.0
- 10.15.52.90 Risk score: 10.0 ✓
- 10.15.45.244 Risk score: 10.0
- 10.15.35.71 Risk score: 10.0

☐	Detection UUID	Device I	Indicators	Last Seen	Created	Assignee	Assigned Comment	Current Assign Time
☐	a9c71208-9123-43d1-b370-...	3.17.7.2	0 Indicators	2025-06-04 ...	2025-06-04 23:07:06 Z	[redacted]		2025-06-10 15:29:45 Z
☐	7ed5428f-d065-4975-bbda-...	4.153.1	0 Indicators	2025-05-29 ...	2025-05-29 17:31:10 Z	[redacted]		2025-06-02 21:05:36 Z
☐	8dc5ad51-719a-4203-9f55-f...	4.153.1	0 Indicators	2025-05-29 ...	2025-05-29 17:31:10 Z	[redacted]		2025-06-02 21:05:36 Z
☐	c7959946-6c94-452e-a260-...	4.153.1	0 Indicators	2025-05-29 ...	2025-05-29 17:31:10 Z	[redacted]		2025-06-02 21:05:35 Z
☐	0e58b713-3d16-4ee1-bf1d-...	8.8.4.4	0 Indicators	2025-08-27 ...	2025-08-27 17:50:48 Z			
☐	85eab3d7-65a3-4bb6-b425-...	8.8.4.4	0 Indicators	2025-08-27 ...	2025-08-27 17:50:48 Z			
☐	aafb988e-4a24-4d04-8aca-...	8.8.4.4	0 Indicators	2025-08-27 ...	2025-08-27 17:50:48 Z			
☐	6a94bd8d-85f0-49a8-96ca-...	10.1.1.1	0 Indicators	2025-07-30 ...	2025-06-20 05:20:43 Z	[redacted]		2025-06-23 17:15:18 Z
☐	10f9c26f-64ab-4e6e-906c-4...	10.1.1.2	0 Indicators	2025-08-27 ...	2025-08-20 01:00:50 Z			
☐	4428deff-7732-4c58-a9d6-2...	10.1.1.2	0 Indicators	2025-08-27 ...	2025-08-20 01:00:50 Z			
☐	4f72b3a2-79cc-4c4f-9cc0-7...	10.1.1.2	0 Indicators	2025-08-27 ...	2025-08-27 17:40:31 Z			
☐	aab3b0b1-f884-40d4-b868-...	10.1.1.2	0 Indicators	2025-08-22 ...	2025-08-20 01:00:50 Z			
☐	b3d6c1e2-123f-48a3-913c-...	10.1.1.2	0 Indicators	2025-08-27 ...	2025-08-20 01:00:49 Z			
☐	27c33455-9985-40b0-87f7-...	10.2.0.3	0 Indicators	2025-08-27 ...	2025-08-20 08:00:40 Z			
☐	30c7b471-9c9a-4c06-a2a5-...	10.2.0.3	0 Indicators	2025-08-27 ...	2025-08-20 08:00:40 Z			
☐	7beeb45c-d59d-4d62-9cd7-...	10.2.0.3	0 Indicators	2025-08-27 ...	2025-08-23 06:00:48 Z			
☐	f294d4f6-3612-4ab3-84e9-f...	10.2.0.3	0 Indicators	2025-08-27 ...	2025-08-20 08:00:39 Z			
☐	2fafe050-8382-48fe-b498-4...	10.4.21	0 Indicators	2025-08-17 ...	2025-08-15 00:40:49 Z			
☐	6e4634c3-5159-4263-b856-...	10.4.21	0 Indicators	2025-08-17 ...	2025-08-15 00:40:49 Z			

Notification emails

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



Detections > Email Notifications

Manage: 2 Notifications

Email Type: All | Status: All | Enabled | Disabled

Assigned detections
DETECTIONS ASSIGNED TO ME   ACCOUNTS: All
EMAIL TYPE: Assigned Detections

Default Notification
SEVERITIES: All   CONFIDENCES: All   CATEGORIES: All   ACCOUNT: Fortinet
EMAIL TYPE: ☑ Individual ☑ Digest (Summary only)
DIGEST TIME: 08:00:00 Eastern Time -04:00

Create a New Notification

Detection Types
● New Detections ○ Assigned Detections

Notification Name*
Enter a name for the notification

Account: All

Severities: All

Confidences: All

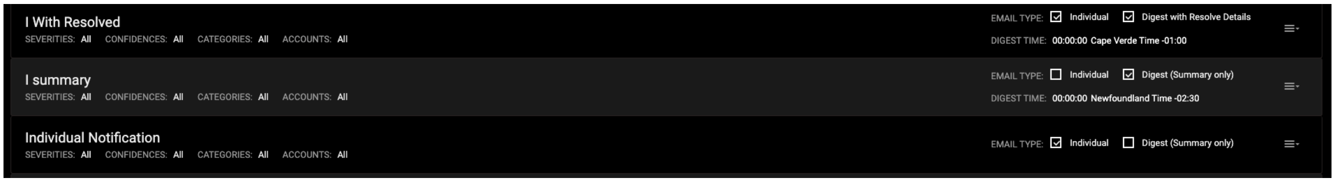
Categories: All

Email Type*
□ Individual ☑ Digest

Digest Time
Please choose an option | Please choose an option

□ Include Resolved Details

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.



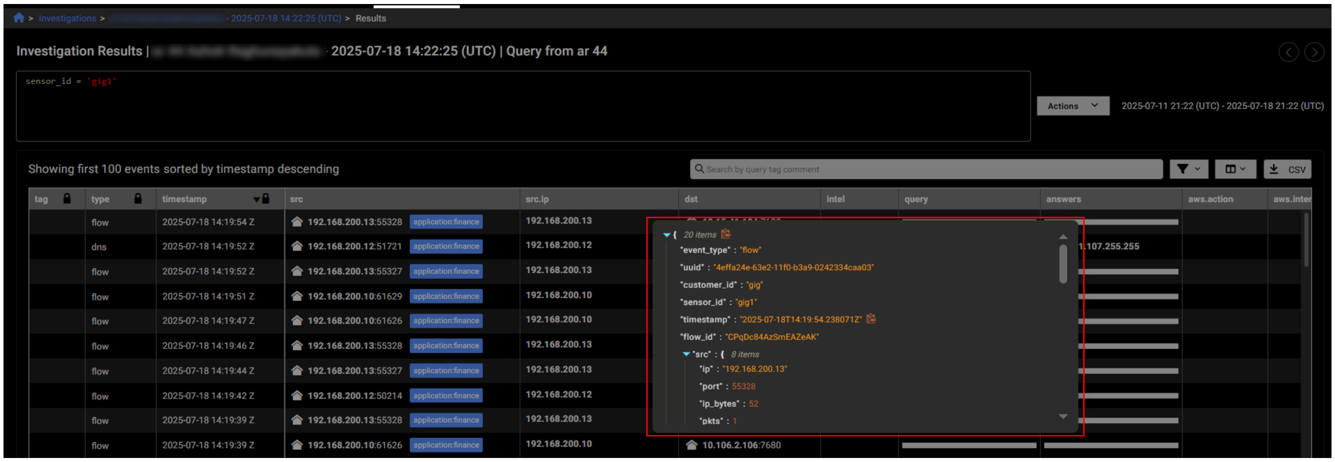
I With Resolved
SEVERITIES: All   CONFIDENCES: All   CATEGORIES: All   ACCOUNTS: All
EMAIL TYPE: ☑ Individual ☑ Digest with Resolve Details
DIGEST TIME: 00:00:00 Cape Verde Time -01:00

I summary
SEVERITIES: All   CONFIDENCES: All   CATEGORIES: All   ACCOUNTS: All
EMAIL TYPE: □ Individual ☑ Digest (Summary only)
DIGEST TIME: 00:00:00 Newfoundland Time -02:30

Individual Notification
SEVERITIES: All   CONFIDENCES: All   CATEGORIES: All   ACCOUNTS: All
EMAIL TYPE: ☑ Individual □ Digest (Summary only)

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.



Investigations > [redacted] - 2025-07-18 14:22:25 (UTC) > Results

Investigation Results | [redacted] 2025-07-18 14:22:25 (UTC) | Query from ar 44

```
sensor_id = 'gig1'
```

Actions   2025-07-11 21:22 (UTC) - 2025-07-18 21:22 (UTC)

Showing first 100 events sorted by timestamp descending

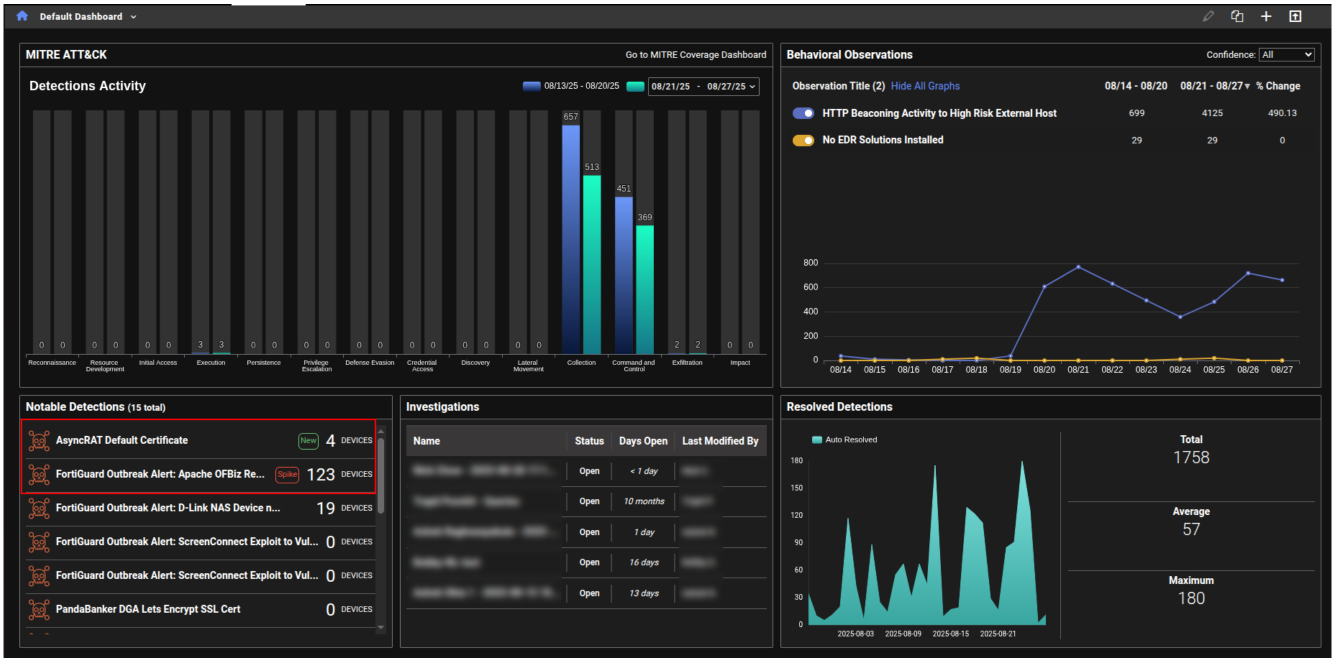
tag	type	timestamp	src	src.ip	dst	intel	query	answers	aws.action	aws.inter
	flow	2025-07-18 14:19:54 Z	192.168.200.13:55328 application:finance	192.168.200.13						
	dns	2025-07-18 14:19:52 Z	192.168.200.12:51721 application:finance	192.168.200.12				1.107.255.255		
	flow	2025-07-18 14:19:52 Z	192.168.200.13:55327 application:finance	192.168.200.13						
	flow	2025-07-18 14:19:51 Z	192.168.200.10:61629 application:finance	192.168.200.10						
	flow	2025-07-18 14:19:47 Z	192.168.200.10:61626 application:finance	192.168.200.10						
	flow	2025-07-18 14:19:46 Z	192.168.200.13:55328 application:finance	192.168.200.13						
	flow	2025-07-18 14:19:44 Z	192.168.200.13:55327 application:finance	192.168.200.13						
	flow	2025-07-18 14:19:42 Z	192.168.200.12:50214 application:finance	192.168.200.12						
	flow	2025-07-18 14:19:39 Z	192.168.200.13:55328 application:finance	192.168.200.13						
	flow	2025-07-18 14:19:39 Z	192.168.200.10:61626 application:finance	192.168.200.10	10.106.2.106:7680					

```
{ 20 items
  "event_type" : "flow"
  "uuid" : "4effa24e-63e2-11f0-b3a9-0242334caa03"
  "customer_id" : "gig"
  "sensor_id" : "gig1"
  "timestamp" : "2025-07-18T14:19:54.238071Z"
  "flow_id" : "CPqDc84AzSmEAZeAK"
  "src" : { 8 items
    "ip" : "192.168.200.13"
    "port" : 55328
    "ip_bytes" : 52
    "pkts" : 1
```

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.



Observation Title (2) Hide All Graphs	08/14 - 08/20	08/21 - 08/27 ▾	% Change
HTTP Beaconing Activity to High Risk External Host	699	4125	490.13
No EDR Solutions Installed	29	29	0

Notable Detections (15 total)

AsyncRAT Default Certificate	New	4	DEVICES
FortiGuard Outbreak Alert: Apache OFBiz Re...	Spike	123	DEVICES
FortiGuard Outbreak Alert: D-Link NAS Device n...		19	DEVICES
FortiGuard Outbreak Alert: ScreenConnect Exploit to Vul...		0	DEVICES
FortiGuard Outbreak Alert: ScreenConnect Exploit to Vul...		0	DEVICES
PandaBanker DGA Lets Encrypt SSL Cert		0	DEVICES

Investigations

Name	Status	Days Open	Last Modified By
[redacted]	Open	*< 1 day*	[redacted]
[redacted]	Open	*10 months*	[redacted]
[redacted]	Open	*1 day*	[redacted]
[redacted]	Open	*16 days*	[redacted]
[redacted]	Open	*13 days*	[redacted]

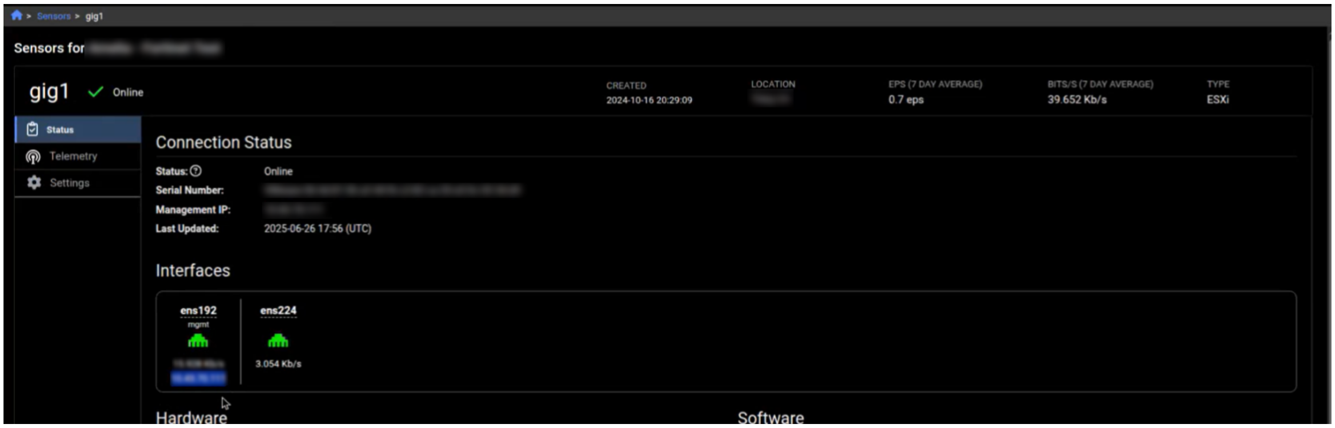
Total
1758

Average
57

Maximum
180

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.



Sensors for [redacted]

gig1 ✓ Online

CREATED	LOCATION	EPS (7 DAY AVERAGE)	BITS/S (7 DAY AVERAGE)	TYPE
2024-10-16 20:29:09	[redacted]	0.7 eps	39.652 Kb/s	ESXi

Connection Status

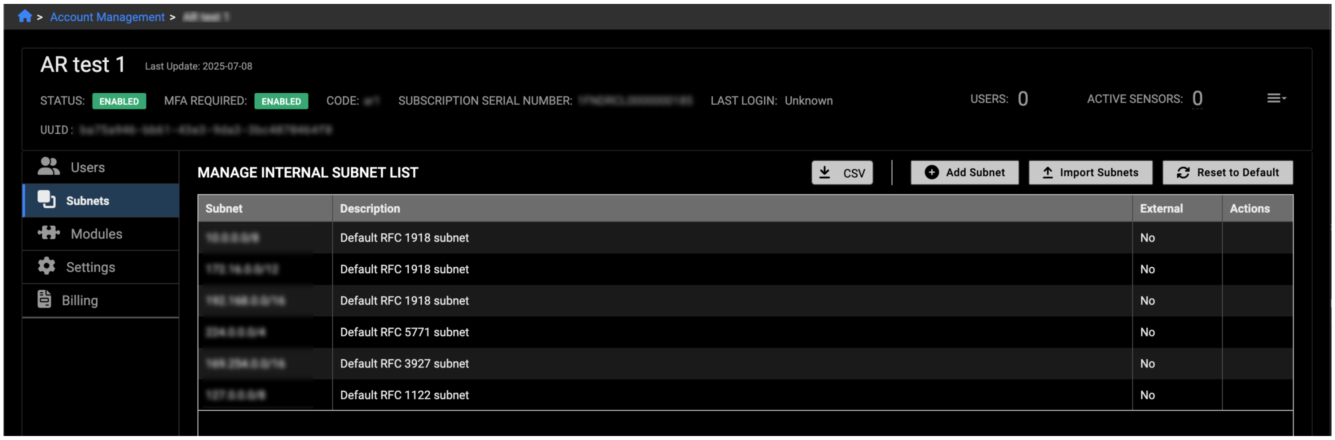
Status: Online
Serial Number: [redacted]
Management IP: [redacted]
Last Updated: 2025-06-26 17:56 (UTC)

Interfaces

ens192 mgmt	ens224
[redacted]	3.054 Kb/s

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.



AR test 1 Last Update: 2025-07-08

STATUS: ENABLED MFA REQUIRED: ENABLED CODE: [redacted] SUBSCRIPTION SERIAL NUMBER: [redacted] LAST LOGIN: Unknown USERS: 0 ACTIVE SENSORS: 0

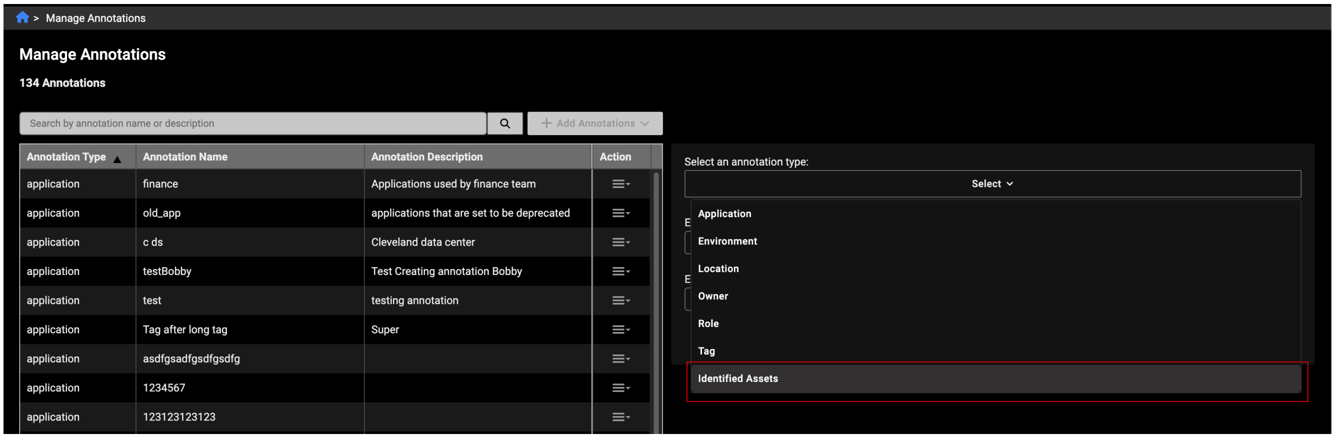
UUID: [redacted]

MANAGE INTERNAL SUBNET LIST

Subnet	Description	External	Actions
[redacted]	Default RFC 1918 subnet	No	
[redacted]	Default RFC 1918 subnet	No	
[redacted]	Default RFC 1918 subnet	No	
[redacted]	Default RFC 5771 subnet	No	
[redacted]	Default RFC 3927 subnet	No	
[redacted]	Default RFC 1122 subnet	No	

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.



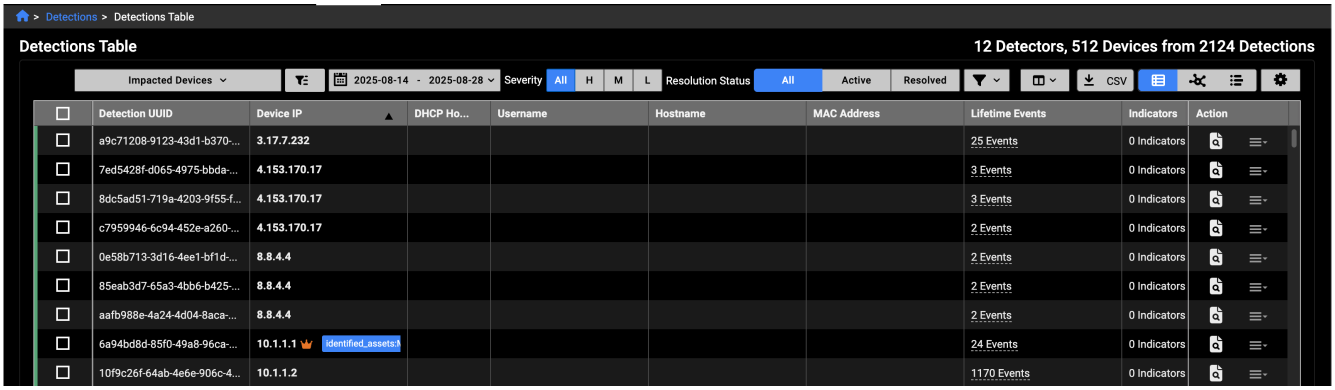
Manage Annotations

134 Annotations

Annotation Type ▲	Annotation Name	Annotation Description	Action
application	finance	Applications used by finance team	☰
application	old_app	applications that are set to be deprecated	☰
application	c ds	Cleveland data center	☰
application	testBobby	Test Creating annotation Bobby	☰
application	test	testing annotation	☰
application	Tag after long tag	Super	☰
application	asdfgsadfgsdfgsdfg		☰
application	1234567		☰
application	123123123123		☰

Select an annotation type:

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



Detections > Detections Table

Detections Table

12 Detectors, 512 Devices from 2124 Detections

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

□	Detection UUID	Device IP	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Indicators	Action
□	a9c71208-9123-43d1-b370-...	3.17.7.232					25 Events	0 Indicators	
□	7ed5428f-d065-4975-bbda-...	4.153.170.17					3 Events	0 Indicators	
□	8dc5ad51-719a-4203-9f55-f...	4.153.170.17					3 Events	0 Indicators	
□	c7959946-6c94-452e-a260-...	4.153.170.17					2 Events	0 Indicators	
□	0e58b713-3d16-4ee1-bf1d-...	8.8.4.4					2 Events	0 Indicators	
□	85eab3d7-65a3-4bb6-b425-...	8.8.4.4					2 Events	0 Indicators	
□	aafb988e-4a24-4d04-8aca-...	8.8.4.4					2 Events	0 Indicators	
□	6a94bd8d-85f0-49a8-96ca-...	10.1.1.1 identified_assets:N					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 75

Version 25.3.0

- Deprecation notice
- Other improvements
- Resolved issues on page 75

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

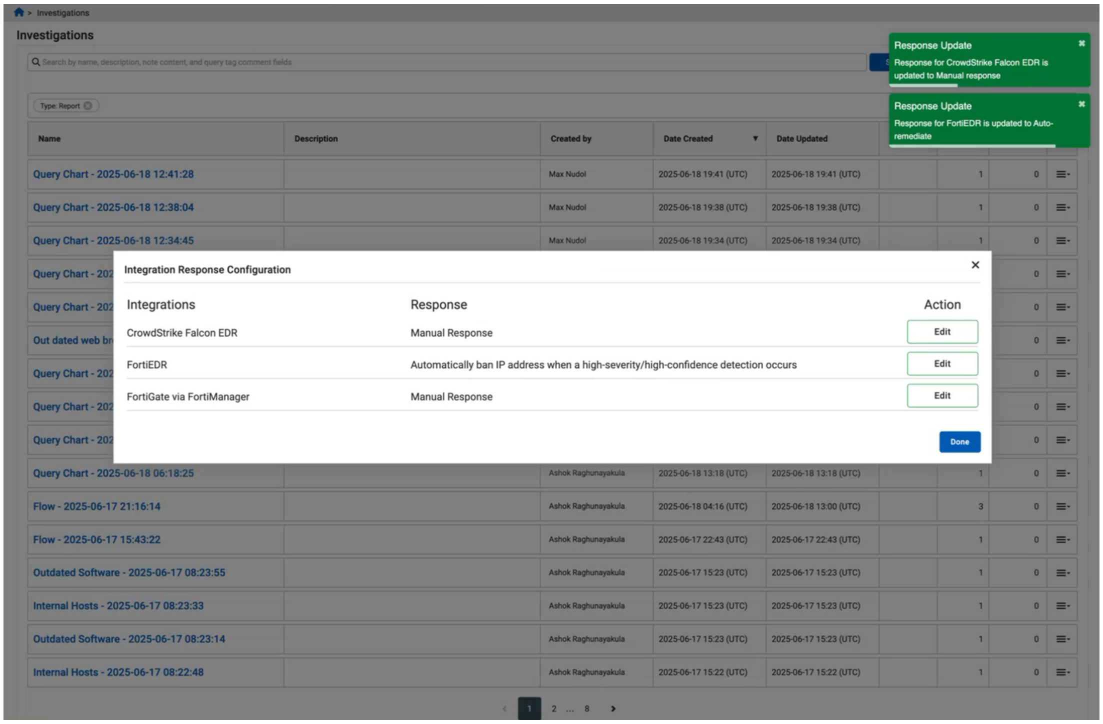
- The sensor filter on the *Triage Detection* page now remains active as you click through the detector rows. This allows you to apply the same filter to different detectors.
- The funnel icon shows when a filter has been changed from its default setting. If the funnel only has one filter, the number 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

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.



Investigations

Search by name, description, note content, and query tag comment fields

Type: Report

Name	Description	Created by	Date Created ▼	Date Updated			
Query Chart - 2025-06-18 12:41:28		Max Nudol	2025-06-18 19:41 (UTC)	2025-06-18 19:41 (UTC)		1	0
Query Chart - 2025-06-18 12:38:04		Max Nudol	2025-06-18 19:38 (UTC)	2025-06-18 19:38 (UTC)		1	0
Query Chart - 2025-06-18 12:34:45		Max Nudol	2025-06-18 19:34 (UTC)	2025-06-18 19:34 (UTC)		1	0
Query Chart - 202							0
Query Chart - 202							0
Out dated web br							0
Query Chart - 202							0
Query Chart - 202							0
Query Chart - 202							0
Query Chart - 2025-06-18 06:18:25		Ashok Raghunayakula	2025-06-18 13:18 (UTC)	2025-06-18 13:18 (UTC)		1	0
Flow - 2025-06-17 21:16:14		Ashok Raghunayakula	2025-06-18 04:16 (UTC)	2025-06-18 13:00 (UTC)		3	0
Flow - 2025-06-17 15:43:22		Ashok Raghunayakula	2025-06-17 22:43 (UTC)	2025-06-17 22:43 (UTC)		1	0
Outdated Software - 2025-06-17 08:23:55		Ashok Raghunayakula	2025-06-17 15:23 (UTC)	2025-06-17 15:23 (UTC)		1	0
Internal Hosts - 2025-06-17 08:23:33		Ashok Raghunayakula	2025-06-17 15:23 (UTC)	2025-06-17 15:23 (UTC)		1	0
Outdated Software - 2025-06-17 08:23:14		Ashok Raghunayakula	2025-06-17 15:23 (UTC)	2025-06-17 15:23 (UTC)		1	0
Internal Hosts - 2025-06-17 08:22:48		Ashok Raghunayakula	2025-06-17 15:22 (UTC)	2025-06-17 15:22 (UTC)		1	0

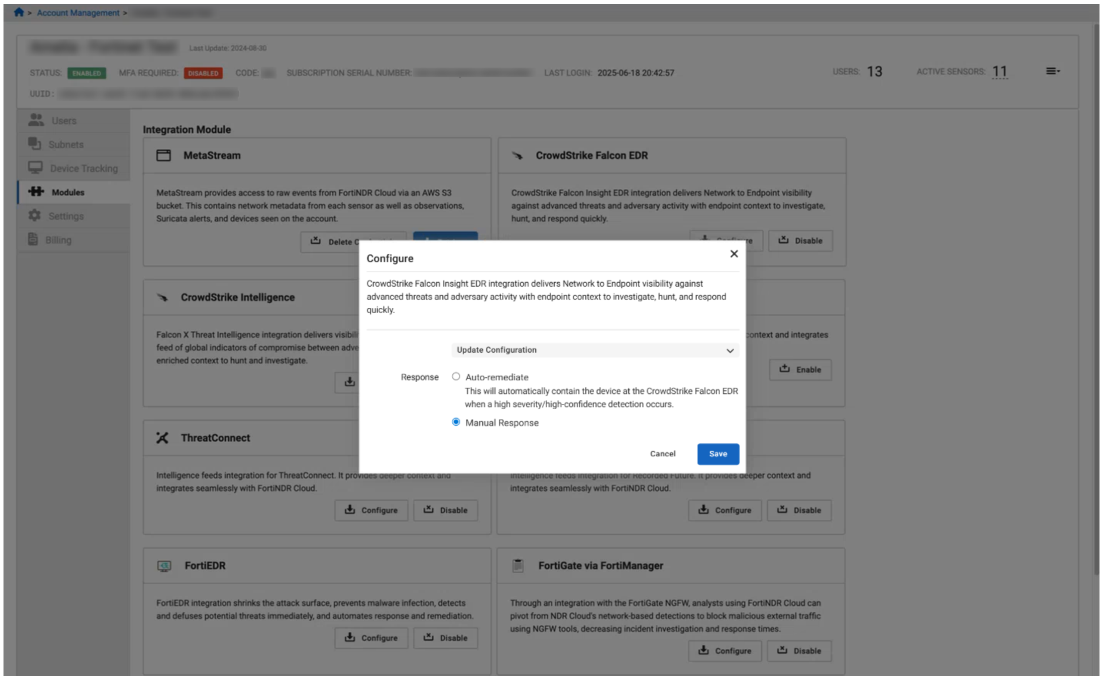
Response Update
Response for CrowdStrike Falcon EDR is updated to Manual response

Response Update
Response for FortiEDR is updated to Auto-remediate

Integration Response Configuration

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

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



Account Management > [redacted]

[redacted] Last Update: 2024-08-30

STATUS: ENABLED MFA REQUIRED: DISABLED CODE: [redacted] SUBSCRIPTION SERIAL NUMBER: [redacted] LAST LOGIN: 2025-06-18 20:42:57 USERS: 13 ACTIVE SENSORS: 11

UUID : [redacted]

Integration Module

MetaStream

MetaStream provides access to raw events from FortiNDR Cloud via an AWS S3 bucket. This contains network metadata from each sensor as well as observations, Suricata alerts, and devices seen on the account.

CrowdStrike Falcon EDR

CrowdStrike Falcon Insight EDR integration delivers Network to Endpoint visibility against advanced threats and adversary activity with endpoint context to investigate, hunt, and respond quickly.

CrowdStrike Intelligence

Falcon X Threat Intelligence integration delivers visibili feed of global indicators of compromise between adve enriched context to hunt and investigate.

ThreatConnect

Intelligence feeds integration for ThreatConnect. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

Intelligence feeds integration for Recorded Future. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

FortiEDR

FortiEDR integration shrinks the attack surface, prevents malware infection, detects and defuses potential threats immediately, and automates response and remediation.

FortiGate via FortiManager

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.

Configure

CrowdStrike Falcon Insight EDR integration delivers Network to Endpoint visibility against advanced threats and adversary activity with endpoint context to investigate, hunt, and respond quickly.

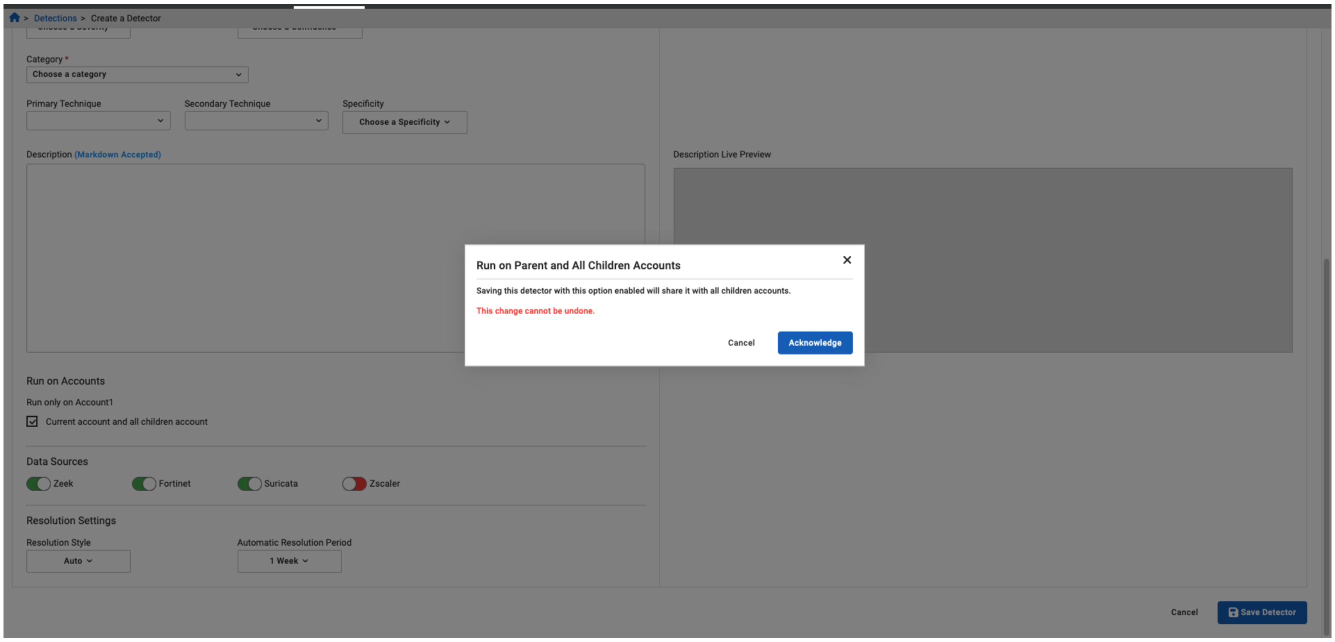
Update Configuration

Response
○ Auto-remediate
This will automatically contain the device at the CrowdStrike Falcon EDR when a high severity/high-confidence detection occurs.
● Manual Response

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.


Detections > Create a Detector
Description (Markdown Accepted)
Description Live Preview
Cancel
Save Detector

Category *: Choose a category

Primary Technique

Secondary Technique

Specificity: Choose a Specificity

Run on Parent and All Children Accounts

Saving this detector with this option enabled will share it with all children accounts.

This change cannot be undone.

Run on Accounts

Run only on Account1

☑ Current account and all children account

Data Sources

Zeek (on) · Fortinet (on) · Suricata (on) · Zscaler (off)

Resolution Settings

Resolution Style: Auto

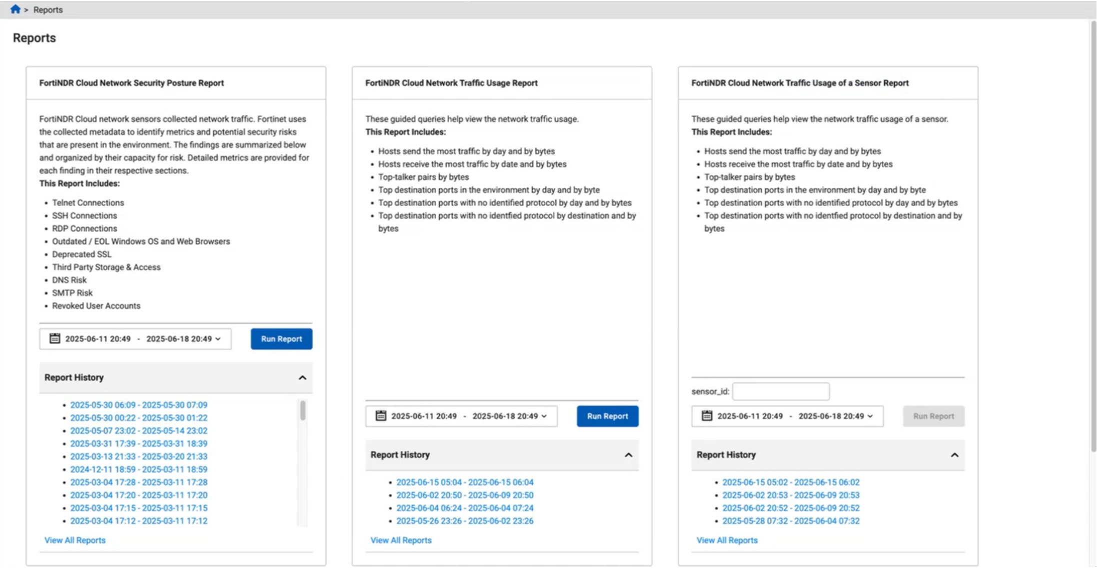
Automatic Resolution Period: 1 Week

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



Reports

FortiNDR Cloud Network Security Posture Report

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

- Telnet Connections
- SSH Connections
- RDP Connections
- Outdated / EOL Windows OS and Web Browsers
- Deprecated SSL
- Third Party Storage & Access
- DNS Risk
- SMTP Risk
- Revoked User Accounts

2025-06-11 20:49 - 2025-06-18 20:49 | Run Report

Report History

- 2025-05-30 06:09 - 2025-05-30 07:09
- 2025-05-30 00:22 - 2025-05-30 01:22
- 2025-05-07 23:02 - 2025-05-14 23:02
- 2025-03-31 17:39 - 2025-03-31 18:39
- 2025-03-13 21:33 - 2025-03-20 21:33
- 2024-12-11 18:59 - 2025-03-11 18:59
- 2025-03-04 17:28 - 2025-03-11 17:28
- 2025-03-04 17:20 - 2025-03-11 17:20
- 2025-03-04 17:15 - 2025-03-11 17:15
- 2025-03-04 17:12 - 2025-03-11 17:12

View All Reports

FortiNDR Cloud Network Traffic Usage Report

These guided queries help view the network traffic usage.
This Report Includes:

- 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 the environment by day and by byte
- Top destination ports with no identified protocol by day and by bytes
- Top destination ports with no identfied protocol by destination and by bytes

2025-06-11 20:49 - 2025-06-18 20:49 | Run Report

Report History

- 2025-06-15 05:04 - 2025-06-15 06:04
- 2025-06-02 20:50 - 2025-06-09 20:50
- 2025-06-04 06:24 - 2025-06-04 07:24
- 2025-05-26 23:26 - 2025-06-02 23:26

View All Reports

FortiNDR Cloud Network Traffic Usage of a Sensor Report

These guided queries help view the network traffic usage of a sensor.
This Report Includes:

- 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 the environment by day and by byte
- Top destination ports with no identified protocol by day and by bytes
- Top destination ports with no identfied protocol by destination and by bytes

sensor_id:

2025-06-11 20:49 - 2025-06-18 20:49 | Run Report

Report History

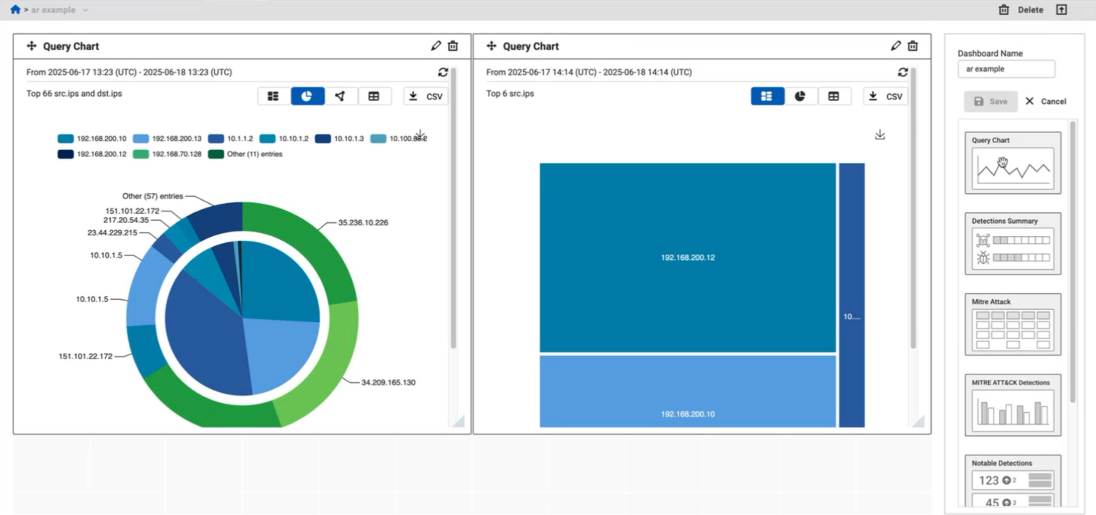
- 2025-06-15 05:02 - 2025-06-15 06:02
- 2025-06-02 20:53 - 2025-06-09 20:53
- 2025-06-02 20:52 - 2025-06-09 20:52
- 2025-05-28 07:32 - 2025-06-04 07:32

View All Reports

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.



Query Chart

From 2025-06-17 13:23 (UTC) - 2025-06-18 13:23 (UTC)

Top 66 src.ips and dst.ips

Query Chart

From 2025-06-17 14:14 (UTC) - 2025-06-18 14:14 (UTC)

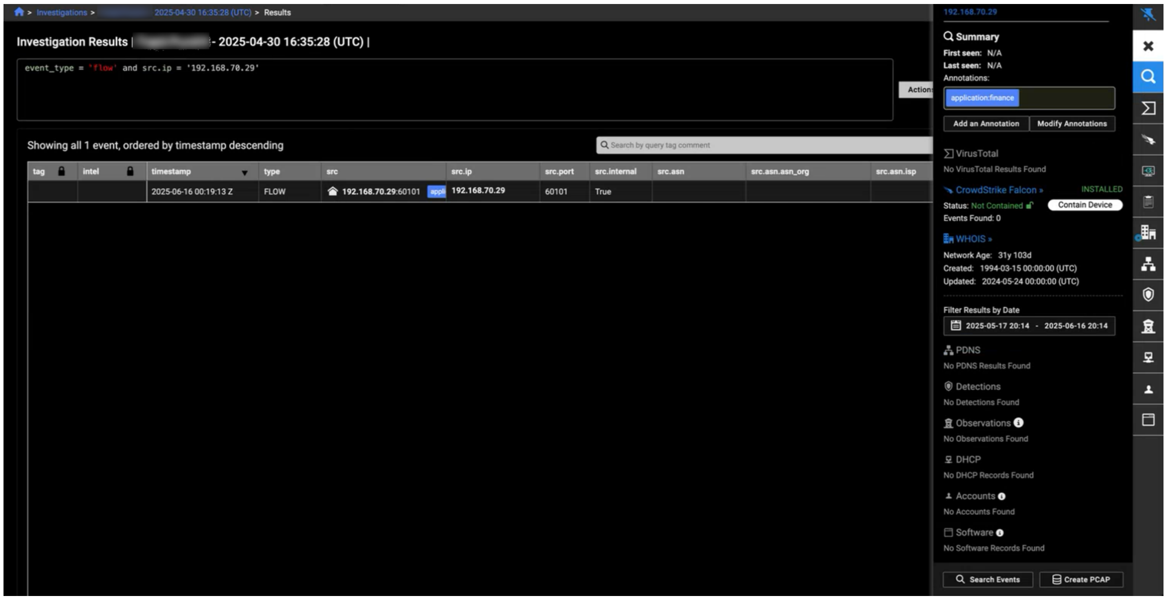
Top 6 src.ips

Dashboard Name: ar example

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.



Investigations > [redacted] 2025-04-30 16:35:28 (UTC) > Results

Investigation Results | [redacted] - 2025-04-30 16:35:28 (UTC) |

```
event_type = 'flow' and src.ip = '192.168.70.29'
```

Showing all 1 event, ordered by timestamp descending

tag	intel	timestamp	type	src	src.ip	src.port	src.internal	src.asn	src.asn.asn_org	src.asn.isp
		2025-06-16 00:19:13 Z	FLOW	192.168.70.29:60101 appl	192.168.70.29	60101	True			

192.168.70.29

Summary

First seen: N/A
Last seen: N/A
Annotations:
application:finance

VirusTotal
No VirusTotal Results Found

CrowdStrike Falcon » INSTALLED
Status: Not Contained
Events Found: 0

WHOIS »
Network Age: 31y 103d
Created: 1994-03-15 00:00:00 (UTC)
Updated: 2024-05-24 00:00:00 (UTC)

Filter Results by Date
2025-05-17 20:14 - 2025-06-16 20:14

PDNS
No PDNS Results Found

Detections
No Detections Found

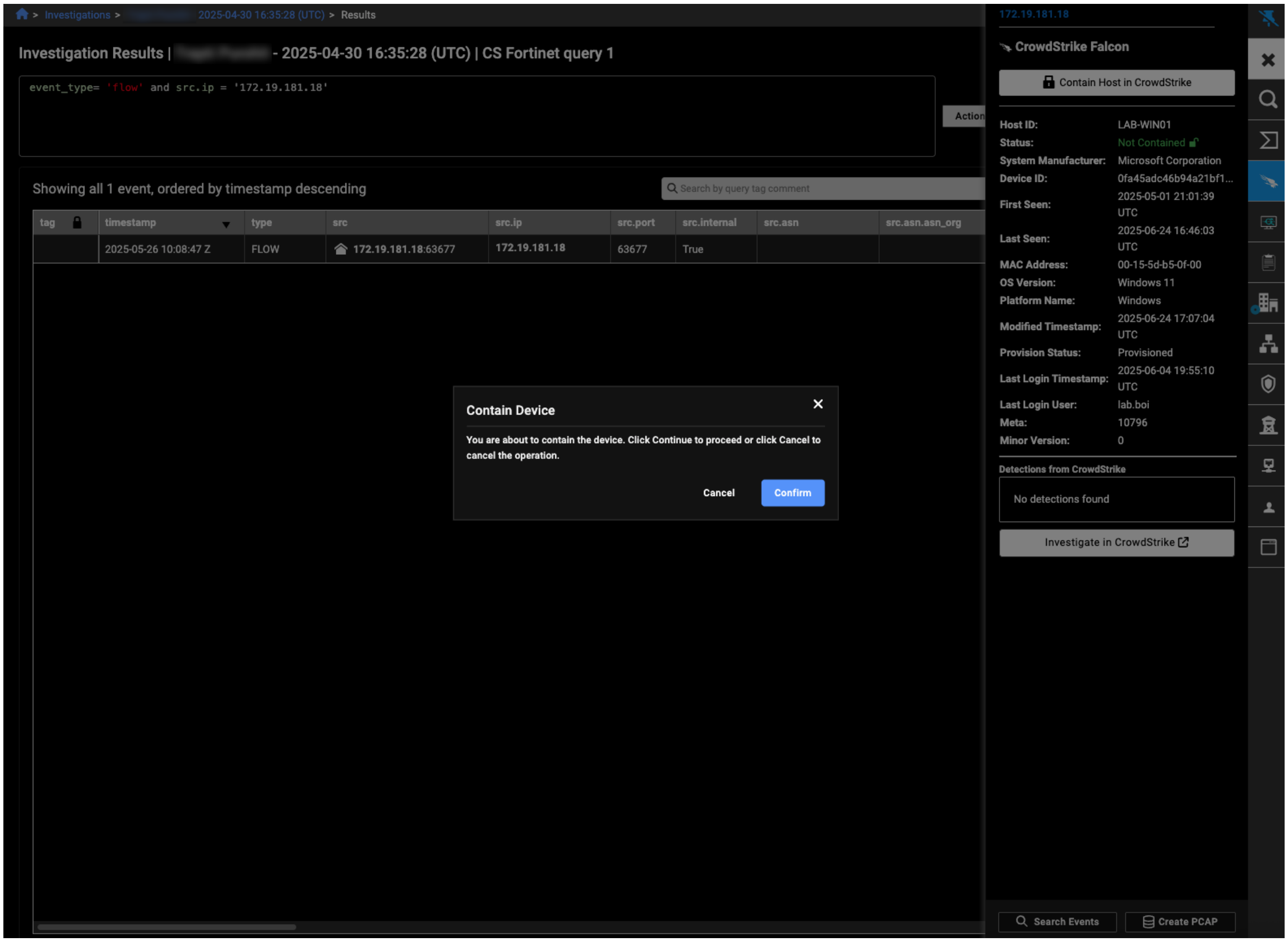
Observations
No Observations Found

DHCP
No DHCP Records Found

Accounts
No Accounts Found

Software
No Software Records Found

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.



Investigations > [redacted] 2025-04-30 16:35:28 (UTC) > Results

Investigation Results | [redacted] - 2025-04-30 16:35:28 (UTC) | CS Fortinet query 1

```
event_type= 'flow' and src.ip = '172.19.181.18'
```

Showing all 1 event, ordered by timestamp descending

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		

Contain Device

You are about to contain the device. Click Continue to proceed or click Cancel to cancel the operation.

172.19.181.18

CrowdStrike Falcon

Host ID:	LAB-WIN01
Status:	Not Contained
System Manufacturer:	Microsoft Corporation
Device ID:	0fa45adc46b94a21bf1...
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

Detections from CrowdStrike

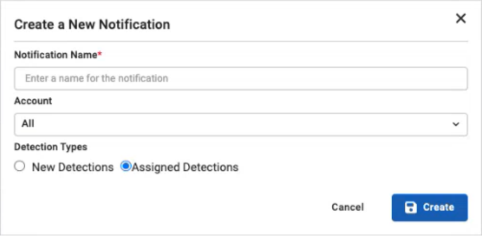
No detections found

Actions
Search by query tag comment
Cancel
Confirm
Contain Host in CrowdStrike
Investigate in CrowdStrike
Search Events
Create PCAP

Assigned detections notifications

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

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



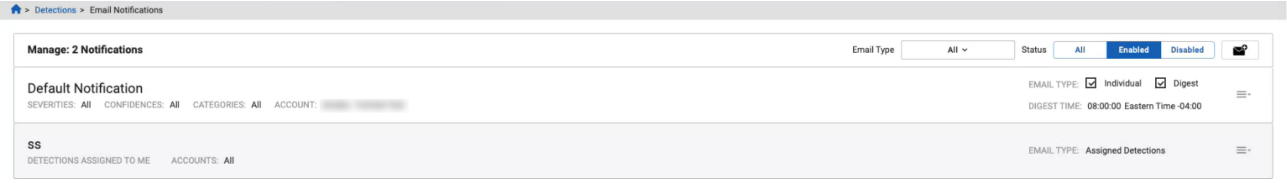
Create a New Notification

Notification Name*: Enter a name for the notification

Account: All

Detection Types: ○ New Detections ● Assigned Detections

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



Manage: 2 Notifications

Email Type: All

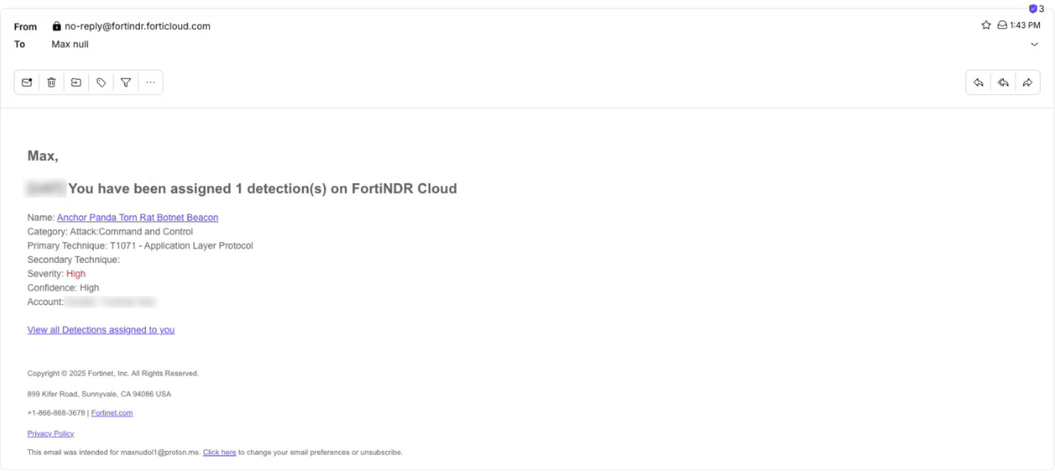
Status: All | Enabled | Disabled

Default Notification
SEVERITIES: All CONFIDENCES: All CATEGORIES: All ACCOUNT: [redacted]
EMAIL TYPE: ☑ Individual ☑ Digest
DIGEST TIME: 08:00:00 Eastern Time -04:00

SS
DETECTIONS ASSIGNED TO ME ACCOUNTS: All
EMAIL TYPE: Assigned Detections

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

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



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

Max,

[redacted] 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.

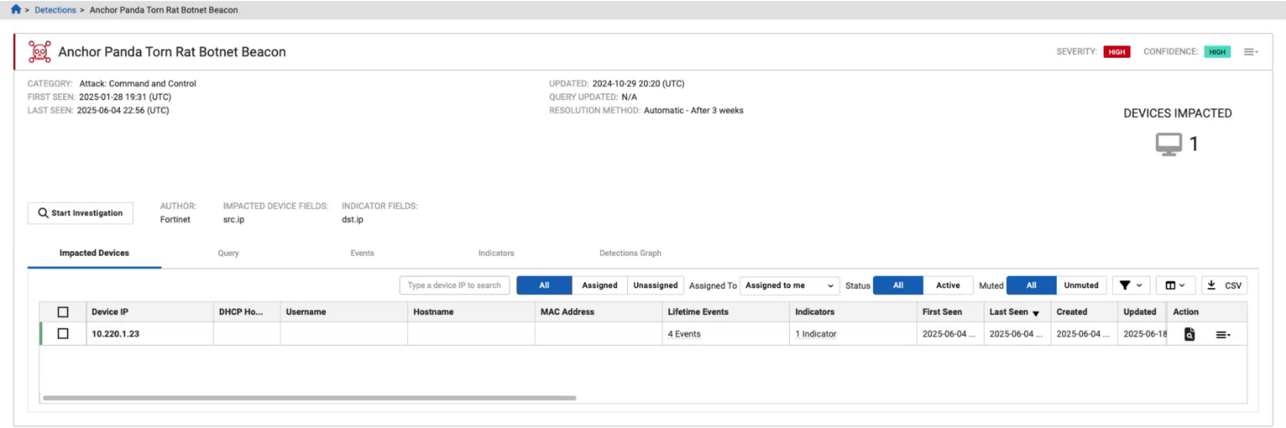
899 Kifer Road, Sunnyvale, CA 94086 USA

+1-866-868-3678 | Fortinet.com

Privacy Policy

This email was intended for maxnudol1@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.



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

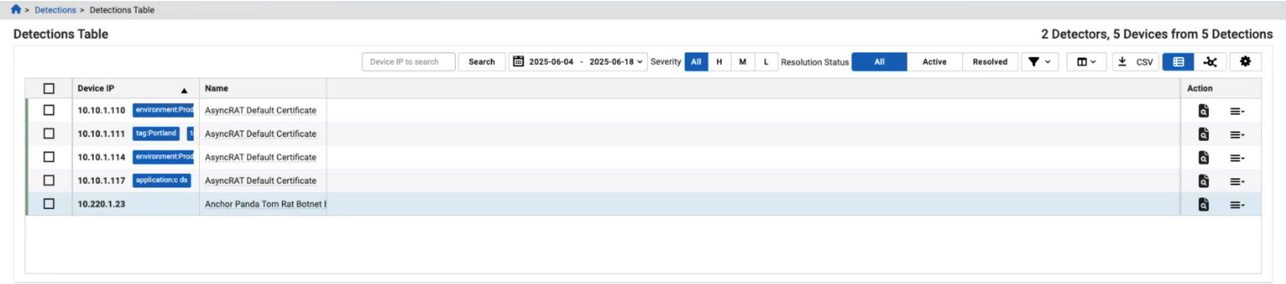
DEVICES IMPACTED 1

Start Investigation

AUTHOR: Fortinet
IMPACTED DEVICE FIELDS: src.ip
INDICATOR FIELDS: dst.ip

□	Device IP	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Indicators	First Seen	Last Seen	Created	Updated	Action
□	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.



Detections > Detections Table

Detections Table

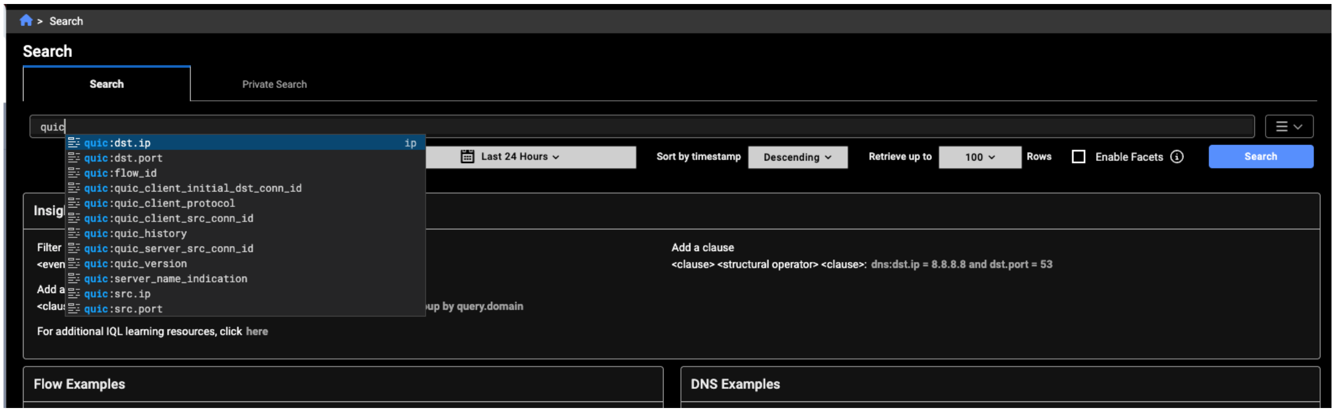
2 Detectors, 5 Devices from 5 Detections

□	Device IP		Name	Action
□	10.10.1.110	environment:Prod	AsyncRAT Default Certificate	
□	10.10.1.111	tag:Portland	AsyncRAT Default Certificate	
□	10.10.1.114	environment:Prod	AsyncRAT Default Certificate	
□	10.10.1.117	application:c ds	AsyncRAT Default Certificate	
□	10.220.1.23		Anchor Panda Torn Rat Botnet E	

Other improvements

Event fields

You can now query *QUIC* events.



Search

Search

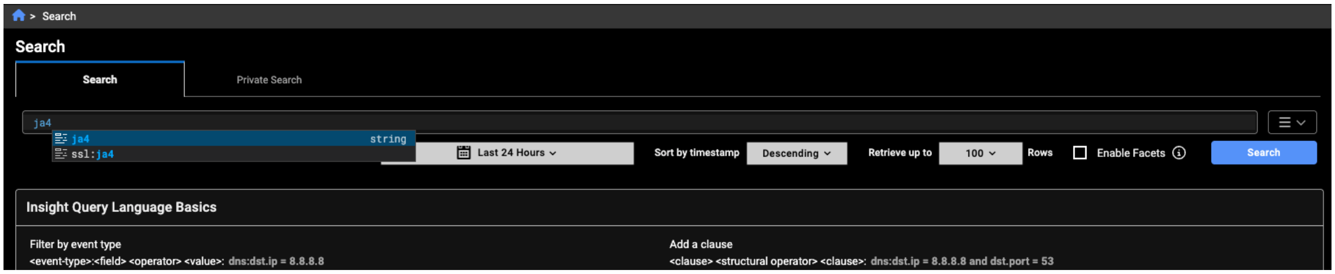
```
quic
quic:dst.ip                                  ip
quic:dst.port
quic:flow_id
quic:quic_client_initial_dst_conn_id
quic:quic_client_protocol
quic:quic_client_src_conn_id
quic:quic_history
quic:quic_server_src_conn_id
quic:quic_version
quic:server_name_indication
quic:src.ip
quic:src.port
```

Filter
<even
Add a
<clau ...up by query.domain

Add a clause
<clause> <structural operator> <clause>: dns:dst.ip = 8.8.8.8 and dst.port = 53

For additional IQL learning resources, click here

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



ja4

ja4 string

ssl:ja4

Last 24 Hours

Sort by timestamp: Descending

Retrieve up to 100 Rows

☐ Enable Facets

Insight Query Language Basics

Filter by event type
<event-type>:<field> <operator> <value>: dns:dst.ip = 8.8.8.8

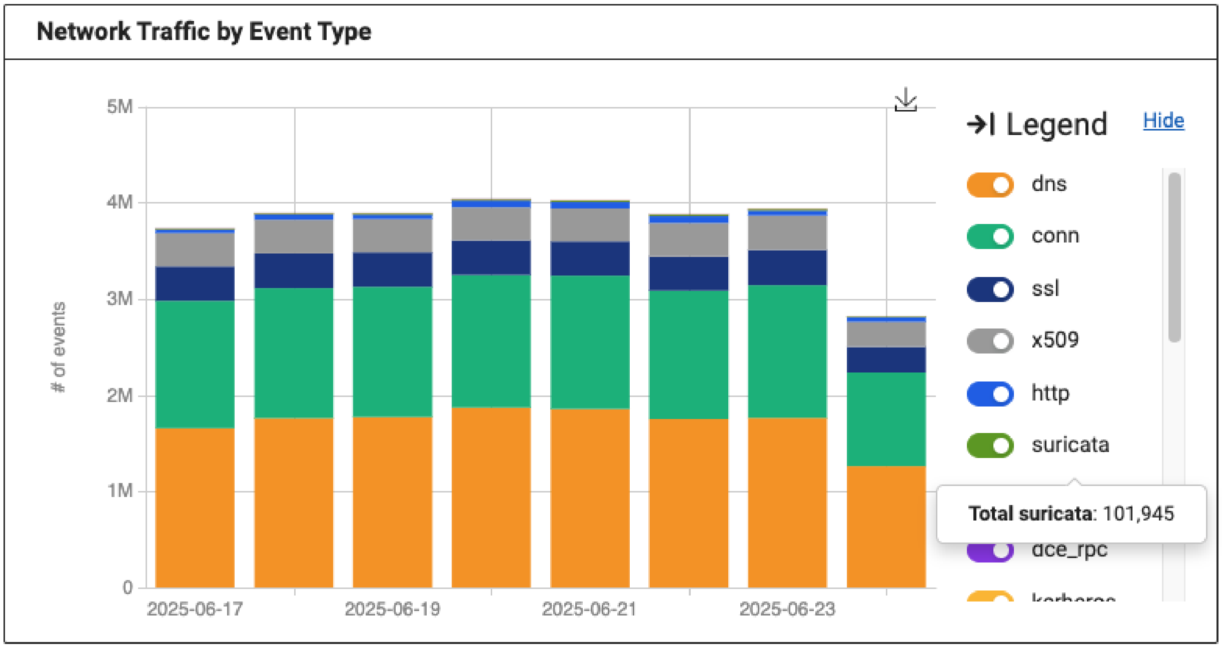
Add a clause
<clause> <structural operator> <clause>: dns:dst.ip = 8.8.8.8 and dst.port = 53

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.

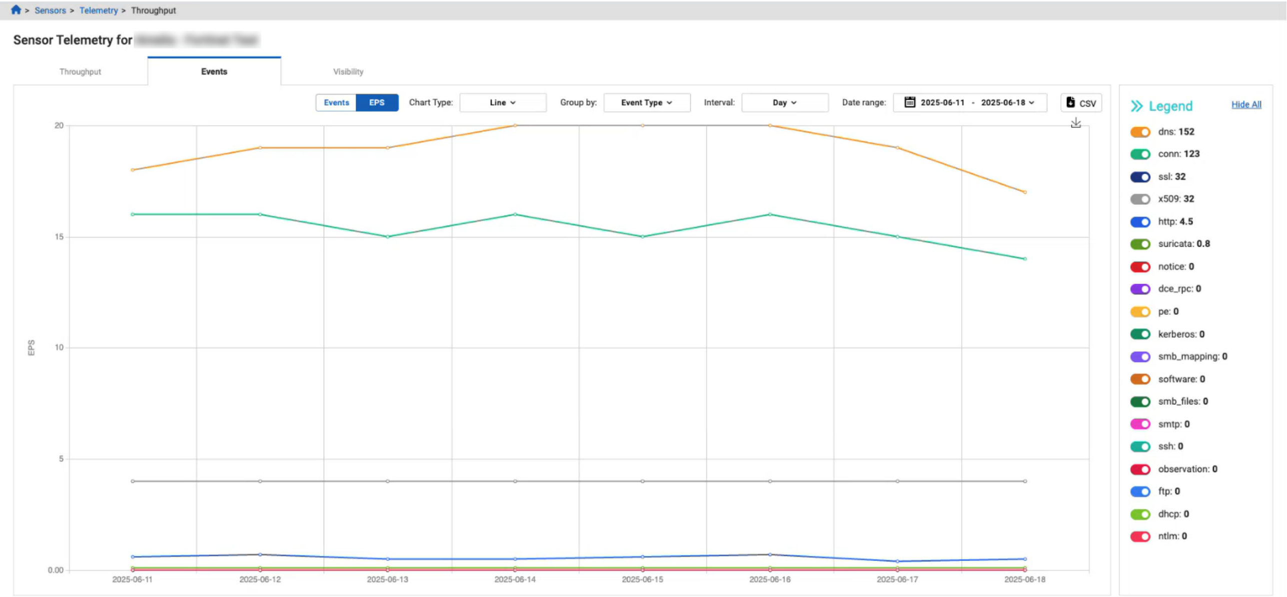
Network Traffic by Event Type widget improvements

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.


Sensors > Telemetry > Throughput

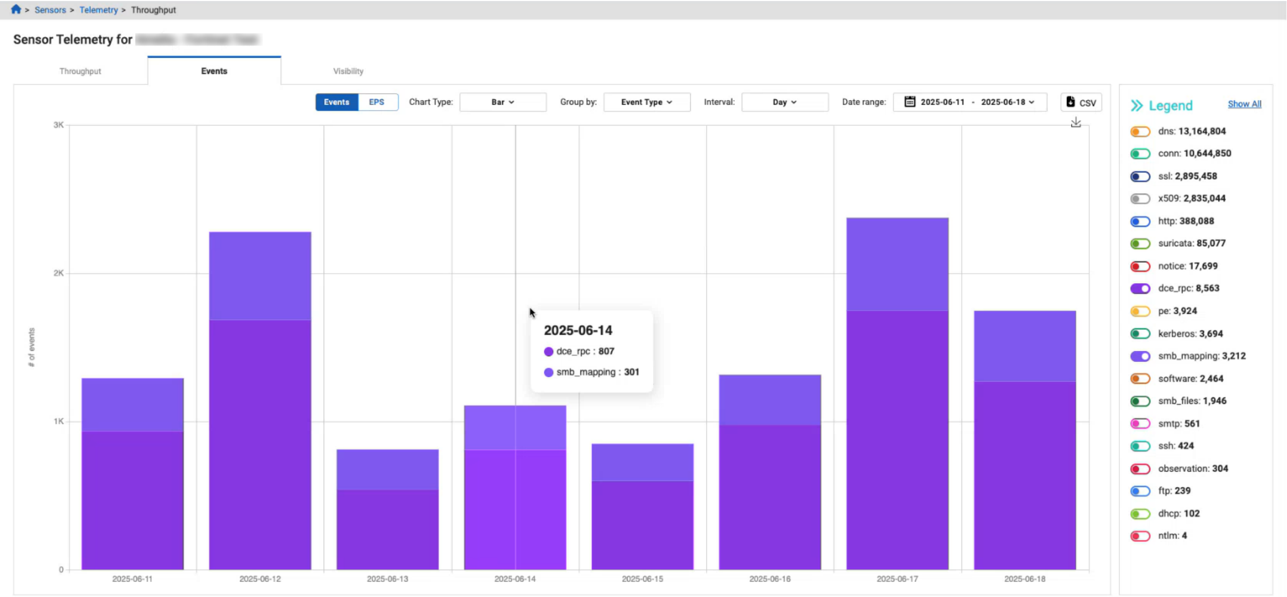
Sensor Telemetry for [redacted]

Chart Type: Line

Group by: Event Type

Interval: Day

Date range: 2025-06-11 - 2025-06-18


Sensors > Telemetry > Throughput

Sensor Telemetry for [redacted]

Chart Type: Bar

Group by: Event Type

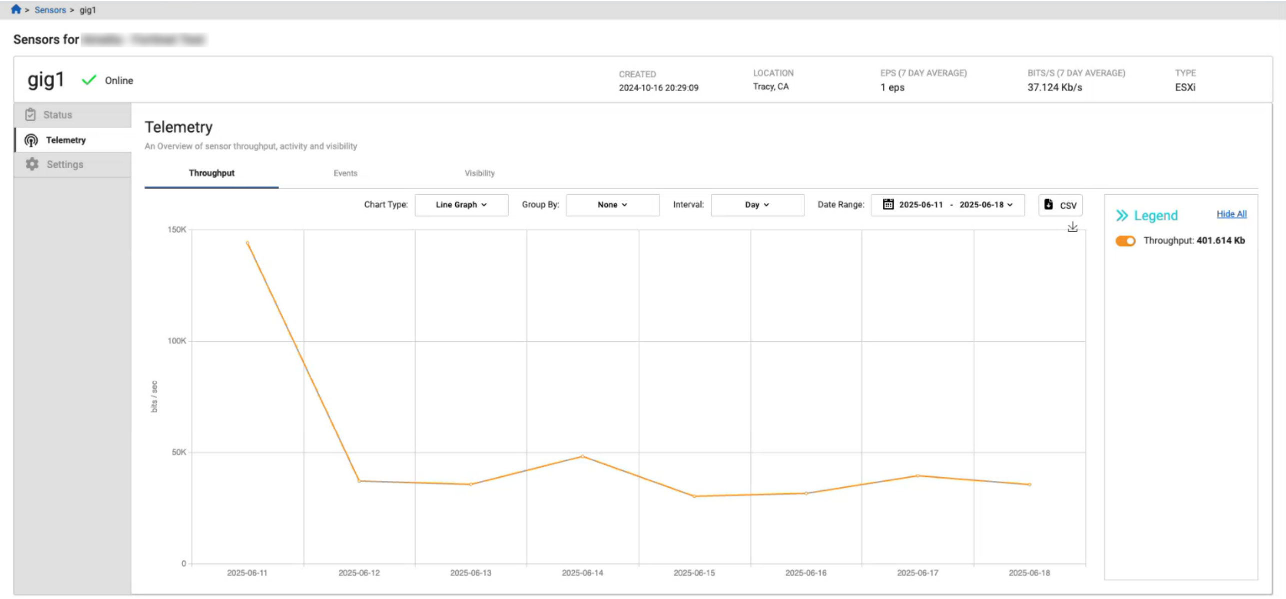
Interval: Day

Date range: 2025-06-11 - 2025-06-18

2025-06-14
dce_rpc : 807
smb_mapping : 301

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.



Sensors > gig1

Sensors for [redacted]

gig1 ✓ Online

CREATED: 2024-10-16 20:29:09

LOCATION: Tracy, CA

EPS (7 DAY AVERAGE): 1 eps

BITS/S (7 DAY AVERAGE): 37.124 Kb/s

TYPE: ESXi

Telemetry

An Overview of sensor throughput, activity and visibility

Chart Type: Line Graph

Group By: None

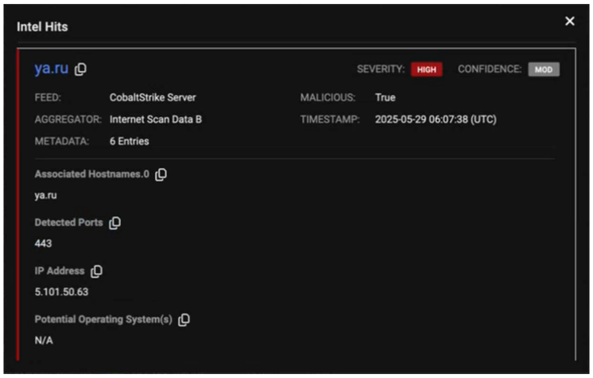
Interval: Day

Date Range: 2025-06-11 - 2025-06-18

Throughput: 401.614 Kb

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*.



Intel Hits

ya.ru

SEVERITY: HIGH

CONFIDENCE: MOD

FEED: CobaltStrike Server

MALICIOUS: True

AGGREGATOR: Internet Scan Data B

TIMESTAMP: 2025-05-29 06:07:38 (UTC)

METADATA: 6 Entries

Associated Hostnames.0

ya.ru

Detected Ports

443

IP Address

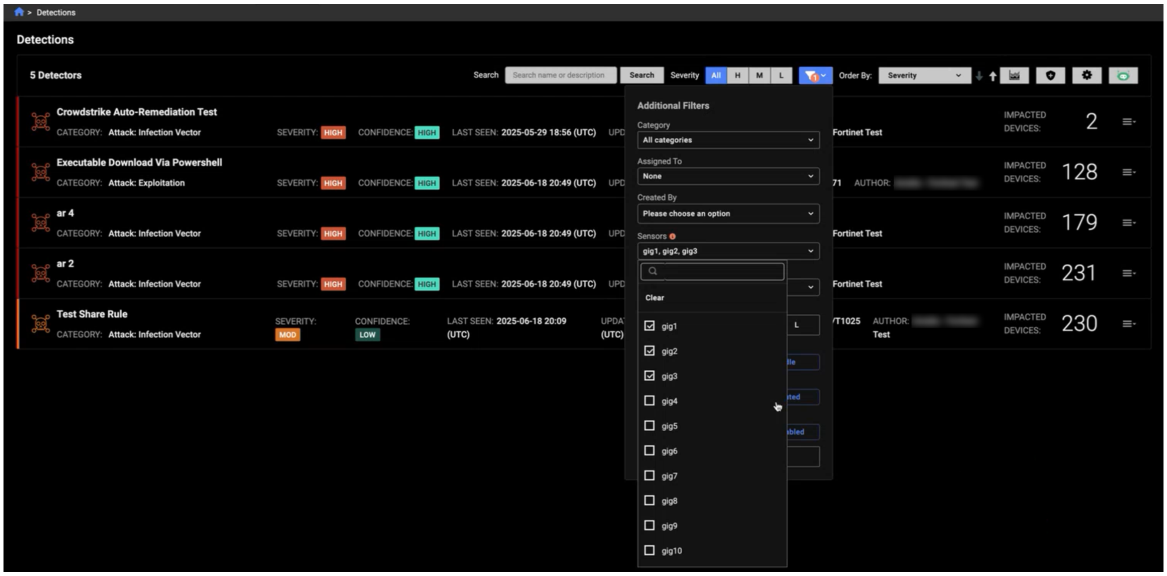
5.101.50.63

Potential Operating System(s)

N/A

Group Detections by sensor

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



Detections

5 Detectors

Order By: Severity

Crowdstrike Auto-Remediation Test
CATEGORY: Attack: Infection Vector SEVERITY: HIGH CONFIDENCE: HIGH LAST SEEN: 2025-05-29 18:56 (UTC) UPD Fortinet Test IMPACTED DEVICES: 2

Executable Download Via Powershell
CATEGORY: Attack: Exploitation SEVERITY: HIGH CONFIDENCE: HIGH LAST SEEN: 2025-06-18 20:49 (UTC) UPD 71 AUTHOR: [redacted] IMPACTED DEVICES: 128

ar 4
CATEGORY: Attack: Infection Vector SEVERITY: HIGH CONFIDENCE: HIGH LAST SEEN: 2025-06-18 20:49 (UTC) UPD Fortinet Test IMPACTED DEVICES: 179

ar 2
CATEGORY: Attack: Infection Vector SEVERITY: HIGH CONFIDENCE: HIGH LAST SEEN: 2025-06-18 20:49 (UTC) UPD Fortinet Test IMPACTED DEVICES: 231

Test Share Rule
CATEGORY: Attack: Infection Vector SEVERITY: MOD CONFIDENCE: LOW LAST SEEN: 2025-06-18 20:09 (UTC) UPDA (UTC) T1025 AUTHOR: [redacted] Test IMPACTED DEVICES: 230

Additional Filters

Category: All categories

Assigned To: None

Created By: Please choose an option

Sensors: gig1, gig2, gig3

Clear

- ☑ gig1
- ☑ gig2
- ☑ gig3
- ☐ gig4
- ☐ gig5
- ☐ gig6
- ☐ gig7
- ☐ gig8
- ☐ gig9
- ☐ gig10

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

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

Version 25.2.b

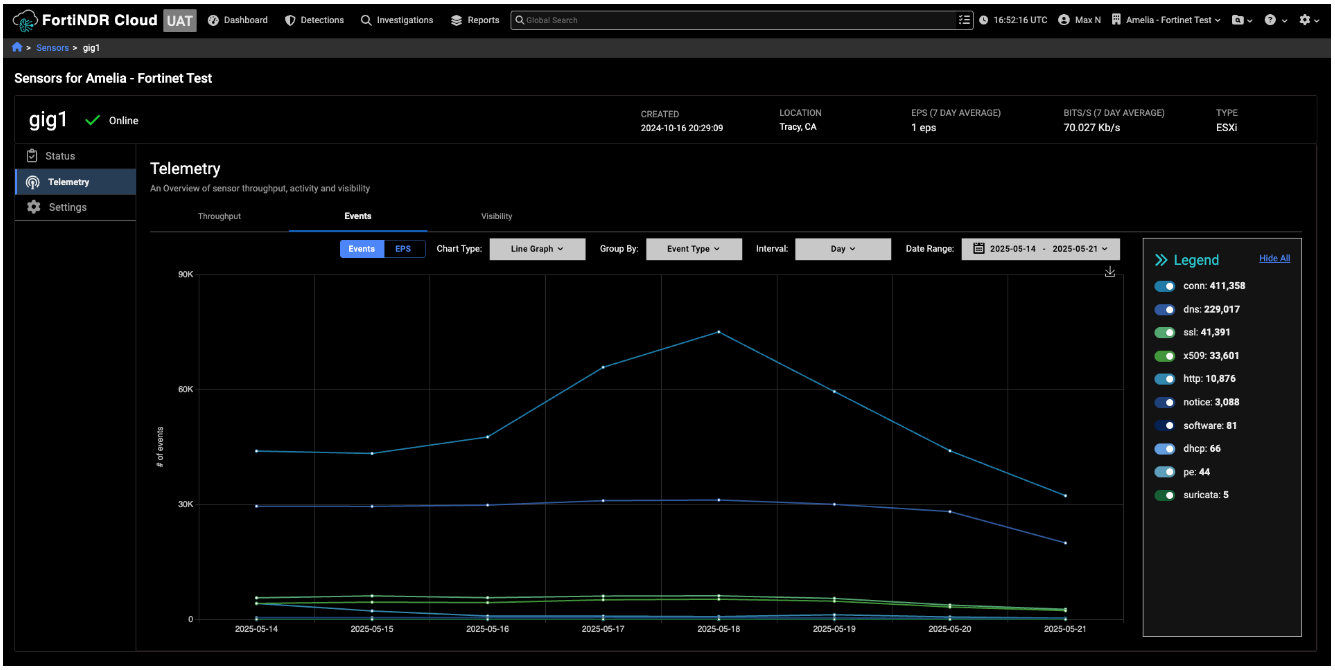
- Improved functionality
  - Sensors
    - Telemetry
    - Throughput
  - Detection context
- Other improvements
- Resolved issues

Improved functionality

Sensors

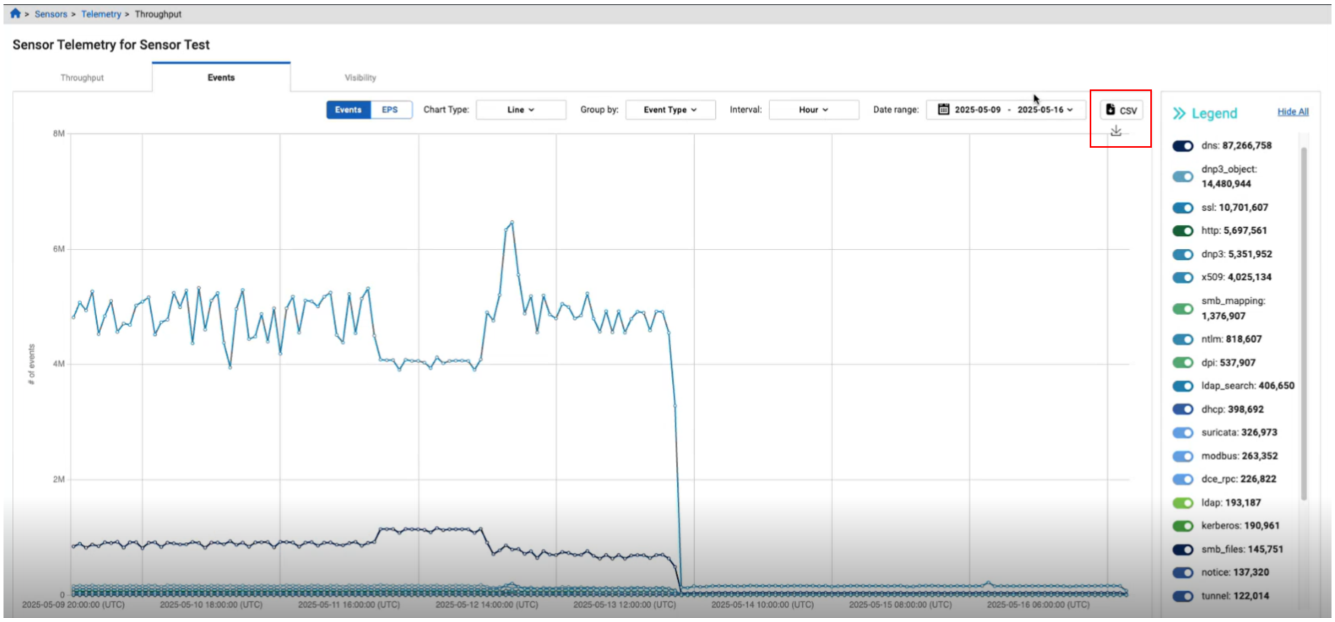
Telemetry

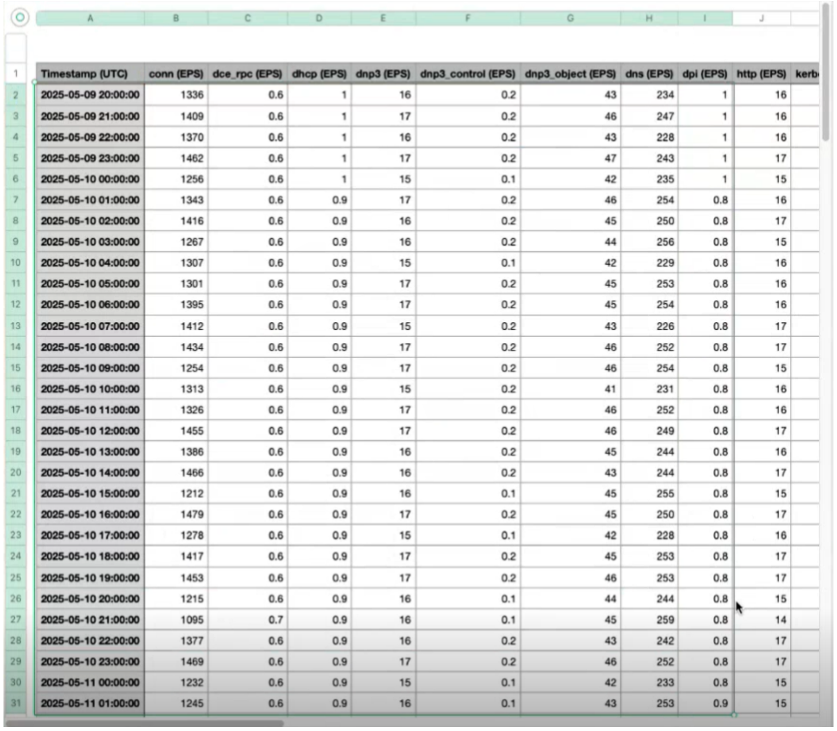
We have improved the performance and responsiveness in the *Telemetry* page. The *Telemetry Details* page now includes a legend that displays the total throughput count for each individual sensor.



Throughput

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





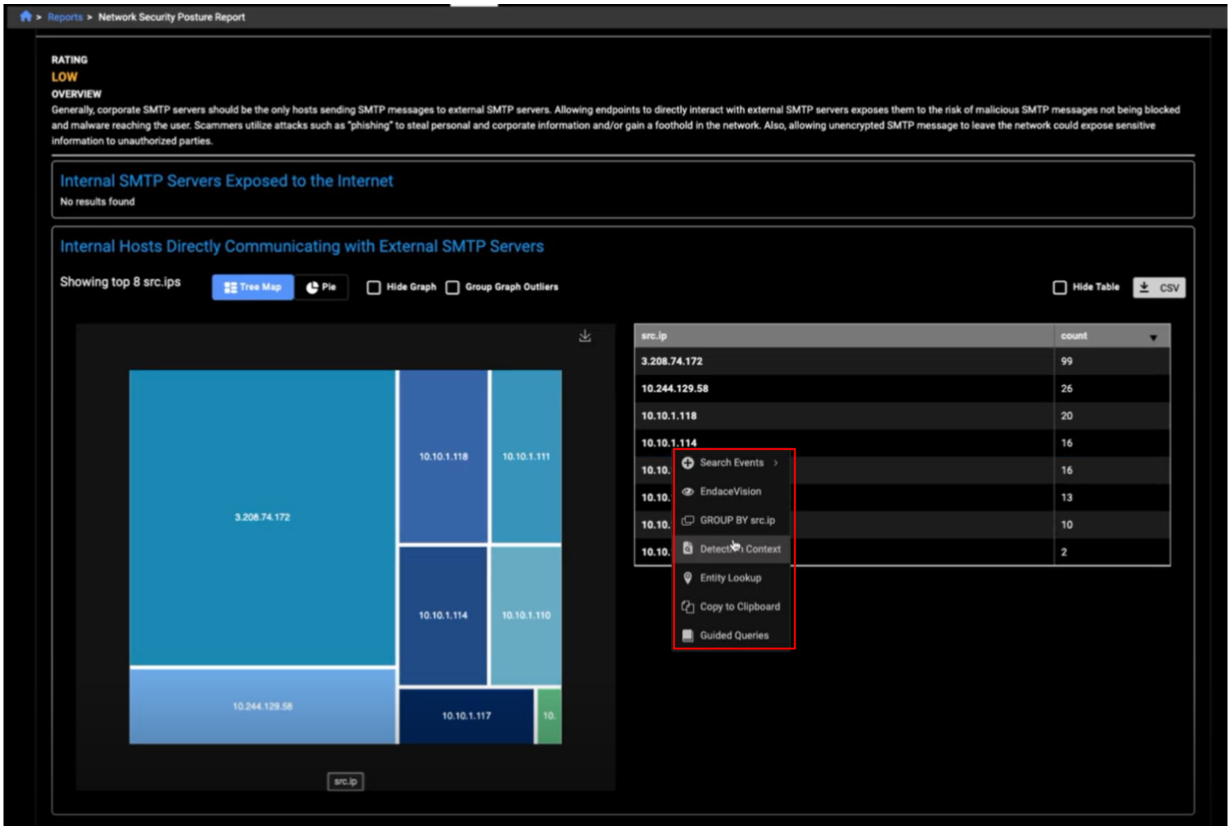
Timestamp (UTC)	conn (EPS)	dce_rpc (EPS)	dhcp (EPS)	dnp3 (EPS)	dnp3_control (EPS)	dnp3_object (EPS)	dns (EPS)	dpi (EPS)	http (EPS)	kerb
2025-05-09 20:00:00	1336	0.6	1	16	0.2	43	234	1	16	
2025-05-09 21:00:00	1409	0.6	1	17	0.2	46	247	1	16	
2025-05-09 22:00:00	1370	0.6	1	16	0.2	43	228	1	16	
2025-05-09 23:00:00	1462	0.6	1	17	0.2	47	243	1	17	
2025-05-10 00:00:00	1256	0.6	1	15	0.1	42	235	1	15	
2025-05-10 01:00:00	1343	0.6	0.9	17	0.2	46	254	0.8	16	
2025-05-10 02:00:00	1416	0.6	0.9	16	0.2	45	250	0.8	17	
2025-05-10 03:00:00	1267	0.6	0.9	16	0.2	44	256	0.8	15	
2025-05-10 04:00:00	1307	0.6	0.9	15	0.1	42	229	0.8	16	
2025-05-10 05:00:00	1301	0.6	0.9	17	0.2	45	253	0.8	16	
2025-05-10 06:00:00	1395	0.6	0.9	17	0.2	45	254	0.8	16	
2025-05-10 07:00:00	1412	0.6	0.9	15	0.2	43	226	0.8	17	
2025-05-10 08:00:00	1434	0.6	0.9	17	0.2	46	252	0.8	17	
2025-05-10 09:00:00	1254	0.6	0.9	17	0.2	46	254	0.8	15	
2025-05-10 10:00:00	1313	0.6	0.9	15	0.2	41	231	0.8	16	
2025-05-10 11:00:00	1326	0.6	0.9	17	0.2	46	252	0.8	16	
2025-05-10 12:00:00	1455	0.6	0.9	17	0.2	46	249	0.8	17	
2025-05-10 13:00:00	1386	0.6	0.9	16	0.2	45	244	0.8	16	
2025-05-10 14:00:00	1466	0.6	0.9	16	0.2	43	244	0.8	17	
2025-05-10 15:00:00	1212	0.6	0.9	16	0.1	45	255	0.8	15	
2025-05-10 16:00:00	1479	0.6	0.9	17	0.2	45	250	0.8	17	
2025-05-10 17:00:00	1278	0.6	0.9	15	0.1	42	228	0.8	16	
2025-05-10 18:00:00	1417	0.6	0.9	17	0.2	45	253	0.8	17	
2025-05-10 19:00:00	1453	0.6	0.9	17	0.2	46	253	0.8	17	
2025-05-10 20:00:00	1215	0.6	0.9	16	0.1	44	244	0.8	15	
2025-05-10 21:00:00	1095	0.7	0.9	16	0.1	45	259	0.8	14	
2025-05-10 22:00:00	1377	0.6	0.9	16	0.2	43	242	0.8	17	
2025-05-10 23:00:00	1469	0.6	0.9	17	0.2	46	252	0.8	17	
2025-05-11 00:00:00	1232	0.6	0.9	15	0.1	42	233	0.8	15	
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.



RATING

LOW

OVERVIEW

Generally, corporate SMTP servers should be the only hosts sending SMTP messages to external SMTP servers. Allowing endpoints to directly interact with external SMTP servers exposes them to the risk of malicious SMTP messages not being blocked and malware reaching the user. Scammers utilize attacks such as "phishing" to steal personal and corporate information and/or gain a foothold in the network. Also, allowing unencrypted SMTP message to leave the network could expose sensitive information to unauthorized parties.

Internal SMTP Servers Exposed to the Internet

No results found

Internal Hosts Directly Communicating with External SMTP Servers

Showing top 8 src.ips

src.ip	count
3.208.74.172	99
10.244.129.58	26
10.10.1.118	20
10.10.1.114	16
10.10.	16
10.10.	13
10.10.	10
10.10.	2

Other improvements

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

Version 25.2.a

FortiNDR Cloud 25.2.a includes bug fixes, but no new features. See Resolved issues on page 75.

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

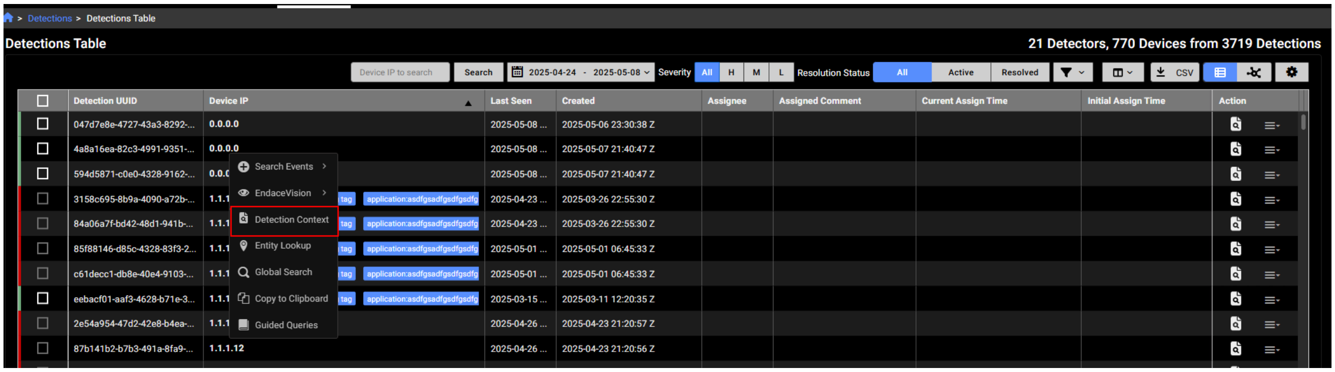
New functionality

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*.



Detections Table

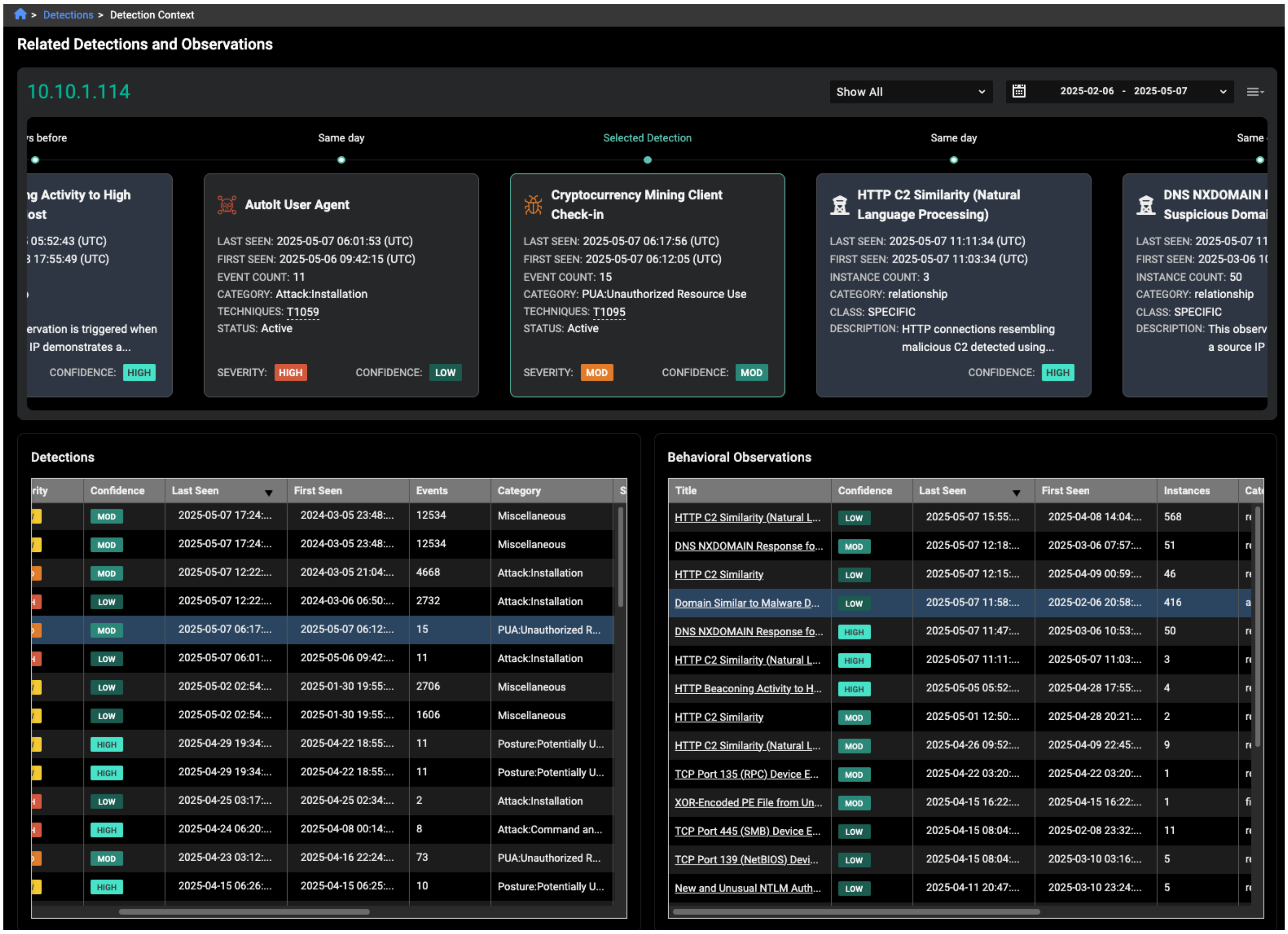
21 Detectors, 770 Devices from 3719 Detections

□	Detection UUID	Device IP	Last Seen	Created	Assignee	Assigned Comment	Current Assign Time	Initial Assign Time	Action
□	047d7e8e-4727-43a3-8292-...	0.0.0.0	2025-05-08 ...	2025-05-06 23:30:38 Z					
□	4a8a16ea-82c3-4991-9351-...	0.0.0.0	2025-05-08 ...	2025-05-07 21:40:47 Z					
□	594d5871-c0e0-4328-9162-...	0.0.0	2025-05-08 ...	2025-05-07 21:40:47 Z					
□	3158c695-8b9a-4090-a72b-...	1.1.1 tag application:asdfgsadfgsdfgsdfg	2025-04-23 ...	2025-03-26 22:55:30 Z					
□	84a06a7f-bd42-48d1-941b-...	1.1.1 tag application:asdfgsadfgsdfgsdfg	2025-04-23 ...	2025-03-26 22:55:30 Z					
□	85f88146-d85c-4328-83f3-2...	1.1.1 tag application:asdfgsadfgsdfgsdfg	2025-05-01 ...	2025-05-01 06:45:33 Z					
□	c61decc1-db8e-40e4-9103-...	1.1.1 tag application:asdfgsadfgsdfgsdfg	2025-05-01 ...	2025-05-01 06:45:33 Z					
□	eebacf01-aaf3-4628-b71e-3...	1.1.1 tag application:asdfgsadfgsdfgsdfg	2025-03-15 ...	2025-03-11 12:20:35 Z					
□	2e54a954-47d2-42e8-b4ea-...	1.1.1	2025-04-26 ...	2025-04-23 21:20:57 Z					
□	87b141b2-b7b3-491a-8fa9-...	1.1.1.12	2025-04-26 ...	2025-04-23 21:20:56 Z					

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

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

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



Detections > Detection Context

Related Detections and Observations

10.10.1.114

Show All

2025-02-06 - 2025-05-07

s before

ng Activity to High
ost
05:52:43 (UTC)
3 17:55:49 (UTC)
ervation is triggered when
IP demonstrates a...
CONFIDENCE: HIGH

Same day

AutoIt 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

Selected Detection

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

Same day

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

Same

DNS NXDOMAIN I
Suspicious Domai
LAST SEEN: 2025-05-07 11
FIRST SEEN: 2025-03-06 1(
INSTANCE COUNT: 50
CATEGORY: relationship
CLASS: SPECIFIC
DESCRIPTION: This observ
a source IP

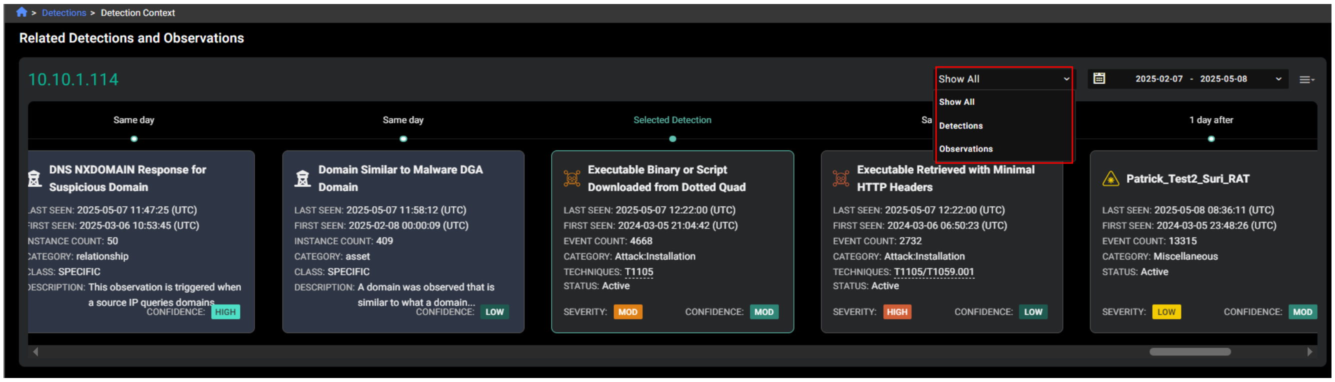
Detections

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

Behavioral Observations

Title	Confidence	Last Seen	First Seen	Instances	Cate
HTTP C2 Similarity (Natural L...	LOW	2025-05-07 15:55:...	2025-04-08 14:04:...	568	re
DNS NXDOMAIN Response fo...	MOD	2025-05-07 12:18:...	2025-03-06 07:57:...	51	re
HTTP C2 Similarity	LOW	2025-05-07 12:15:...	2025-04-09 00:59:...	46	re
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	re
HTTP C2 Similarity (Natural L...	HIGH	2025-05-07 11:11:...	2025-05-07 11:03:...	3	re
HTTP Beaconing Activity to H...	HIGH	2025-05-05 05:52:...	2025-04-28 17:55:...	4	re
HTTP C2 Similarity	MOD	2025-05-01 12:50:...	2025-04-28 20:21:...	2	re
HTTP C2 Similarity (Natural L...	MOD	2025-04-26 09:52:...	2025-04-09 22:45:...	9	re
TCP Port 135 (RPC) Device E...	MOD	2025-04-22 03:20:...	2025-04-22 03:20:...	1	re
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	re
TCP Port 139 (NetBIOS) Devi...	LOW	2025-04-15 08:04:...	2025-03-10 03:16:...	5	re
New and Unusual NTLM Auth...	LOW	2025-04-11 20:47:...	2025-03-10 23:24:...	5	re

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



Detections > Detection Context

Related Detections and Observations

10.10.1.114

Show All

2025-02-07 - 2025-05-08

Same day

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

Same day

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

Selected Detection

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

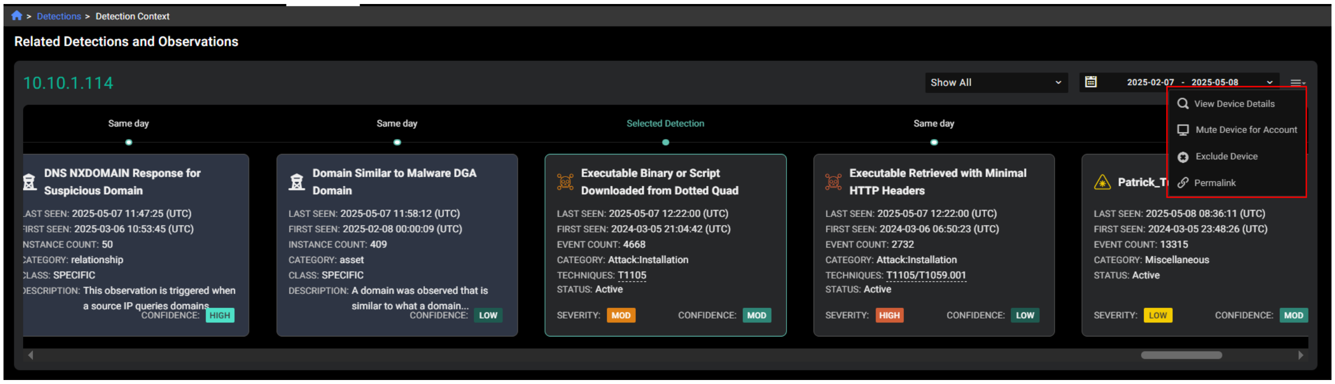
Sa

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

1 day after

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

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



Related Detections and Observations

10.10.1.114

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

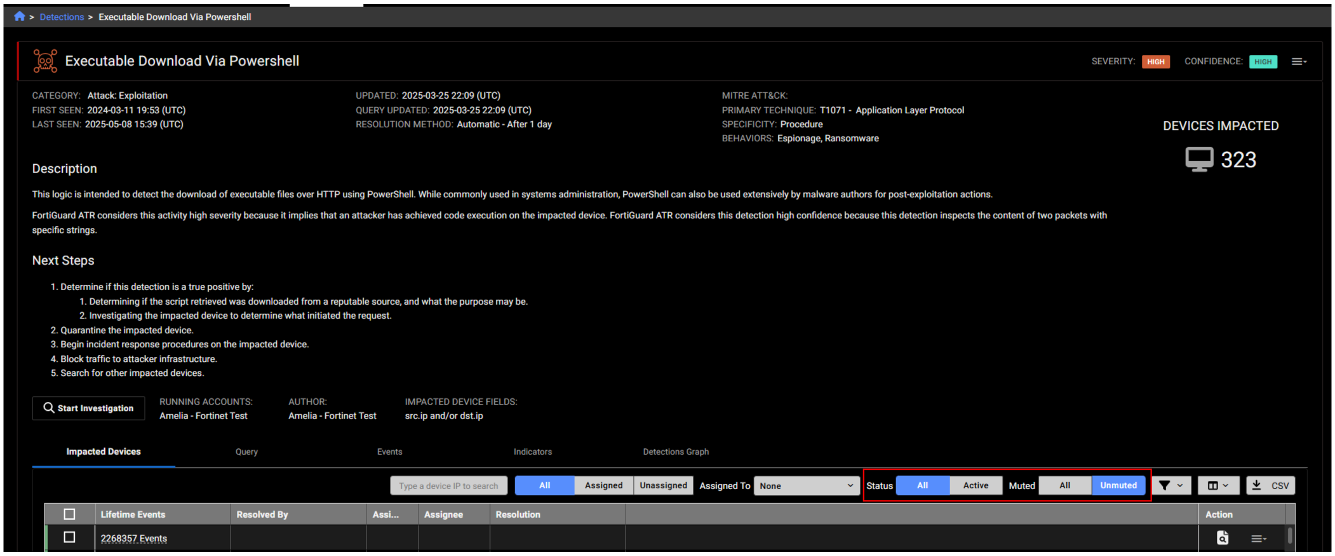
Domain Similar to Malware DGA Domain
LAST SEEN: 2025-05-07 11:58:12 (UTC)
FIRST SEEN: 2025-02-08 00:00:09 (UTC)
INSTANCE COUNT: 409
CATEGORY: asset
CLASS: SPECIFIC
DESCRIPTION: A domain was observed that is similar to what a domain...
CONFIDENCE: LOW

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

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

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

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.



Executable Download Via Powershell

SEVERITY: HIGH CONFIDENCE: HIGH

CATEGORY: Attack: Exploitation
FIRST SEEN: 2024-03-11 19:53 (UTC)
LAST SEEN: 2025-05-08 15:39 (UTC)

UPDATED: 2025-03-25 22:09 (UTC)
QUERY UPDATED: 2025-03-25 22:09 (UTC)
RESOLUTION METHOD: Automatic - After 1 day

MITRE ATT&CK:
PRIMARY TECHNIQUE: T1071 - Application Layer Protocol
SPECIFICITY: Procedure
BEHAVIORS: Espionage, Ransomware

DEVICES IMPACTED
323

Description

This logic is intended to detect the download of executable files over HTTP using PowerShell. While commonly used in systems administration, PowerShell can also be used extensively by malware authors for post-exploitation actions.

FortiGuard ATR considers this activity high severity because it implies that an attacker has achieved code execution on the impacted device. FortiGuard ATR considers this detection high confidence because this detection inspects the content of two packets with specific strings.

Next Steps

1. Determine if this detection is a true positive by:
    1. Determining if the script retrieved was downloaded from a reputable source, and what the purpose may be.
    2. Investigating the impacted device to determine what initiated the request.
2. Quarantine the impacted device.
3. Begin incident response procedures on the impacted device.
4. Block traffic to attacker infrastructure.
5. Search for other impacted devices.

RUNNING ACCOUNTS: Amelia - Fortinet Test
AUTHOR: Amelia - Fortinet Test
IMPACTED DEVICE FIELDS: src.ip and/or dst.ip

Assigned To: None
Status: All | Active
Muted: All | Unmuted

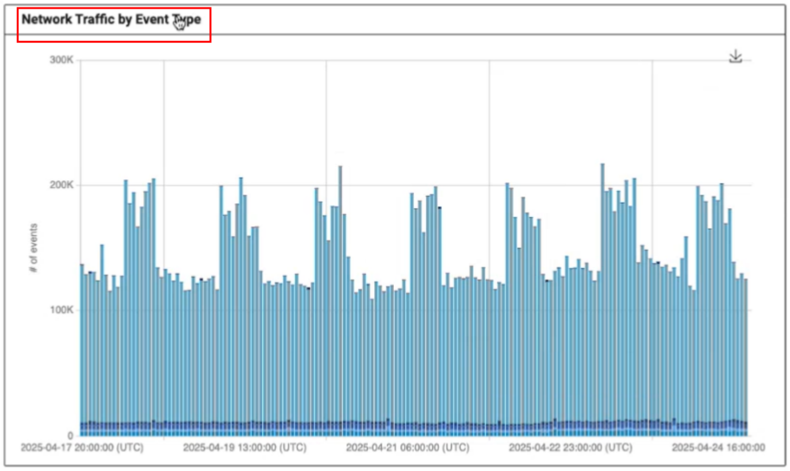
□	Lifetime Events	Resolved By	Assi...	Assignee	Resolution	Action
□	2268357 Events					

Improved functionality

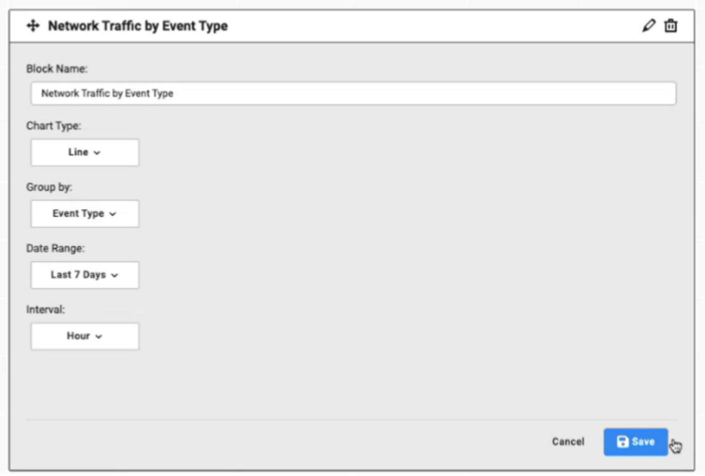
Sensor telemetry

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.


Network Traffic by Event Type
300K
200K
100K
0
# of events
2025-04-17 20:00:00 (UTC)
2025-04-19 13:00:00 (UTC)
2025-04-21 06:00:00 (UTC)
2025-04-22 23:00:00 (UTC)
2025-04-24 16:00:00

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



Network Traffic by Event Type

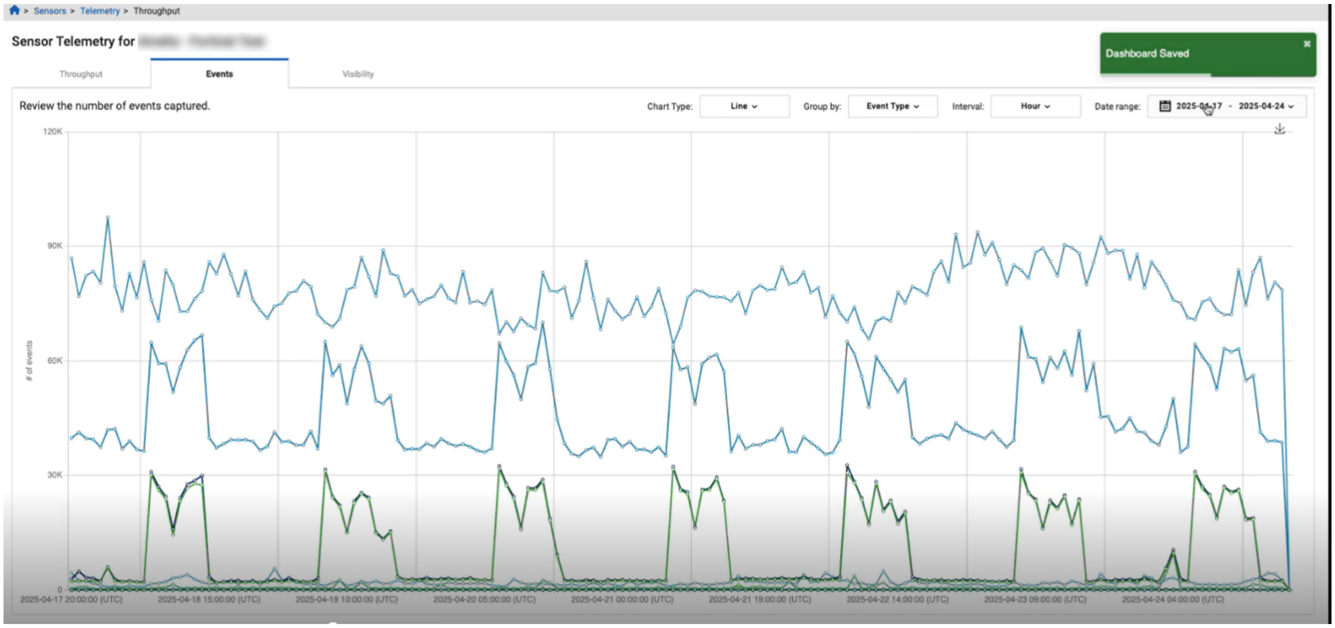
Block Name: Network Traffic by Event Type

Chart Type: Line

Group by: Event Type

Date Range: Last 7 Days

Interval: Hour



> Sensors > Telemetry > Throughput

Sensor Telemetry for [redacted]

Dashboard Saved
Throughput
Events
Visibility

Review the number of events captured.

Chart Type: Line

Group by: Event Type

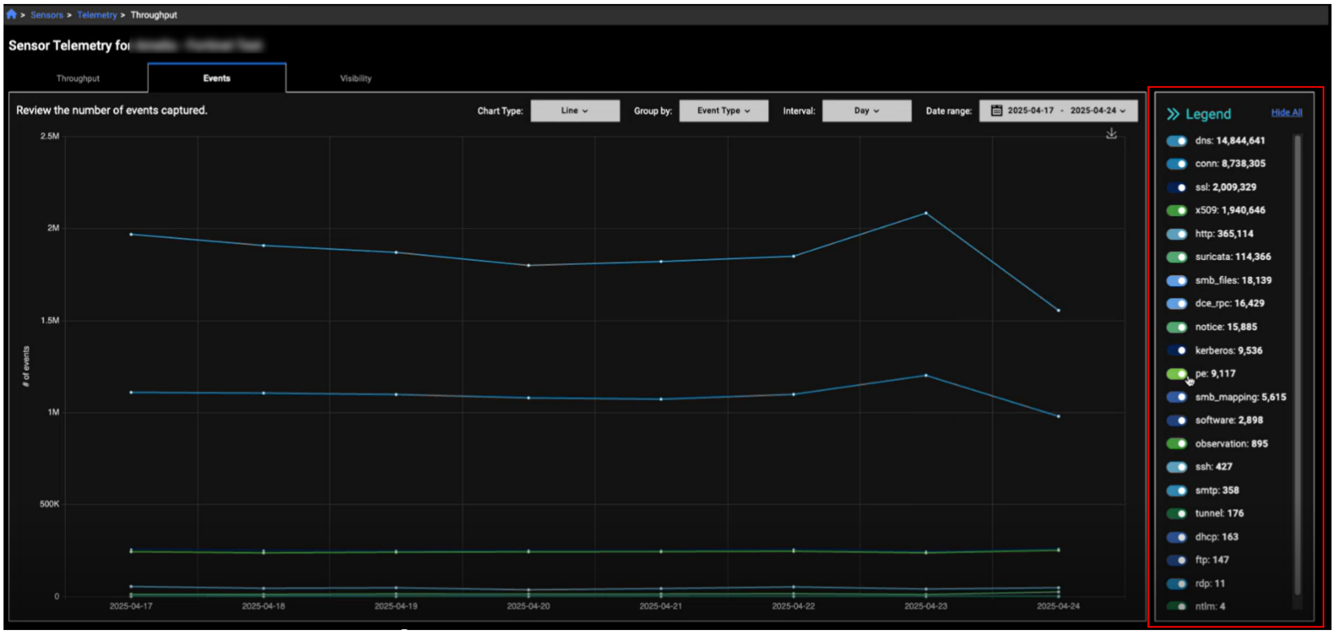
Interval: Hour

Date range: 2025-04-17 - 2025-04-24

120K
90K
60K
30K
0
# of events
2025-04-17 20:00:00 (UTC)
2025-04-18 15:00:00 (UTC)
2025-04-19 10:00:00 (UTC)
2025-04-20 05:00:00 (UTC)
2025-04-21 00:00:00 (UTC)
2025-04-21 19:00:00 (UTC)
2025-04-22 14:00:00 (UTC)
2025-04-23 09:00:00 (UTC)
2025-04-24 04:00:00 (UTC)

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.



Sensor Telemetry for [redacted]

Review the number of events captured.

Chart Type: Line
Group by: Event Type
Interval: Day
Date range: 2025-04-17 - 2025-04-24

dns: 14,844,641
conn: 8,738,305
ssl: 2,009,329
x509: 1,940,646
http: 365,114
suricata: 114,366
smb_files: 18,139
dce_rpc: 16,429
notice: 15,885
kerberos: 9,536
pe: 9,117
smb_mapping: 5,615
software: 2,898
observation: 895
ssh: 427
smtp: 358
tunnel: 176
dhcp: 163
ftp: 147
rdp: 11
ntlm: 4

IQL queries

ldap and ldap_search

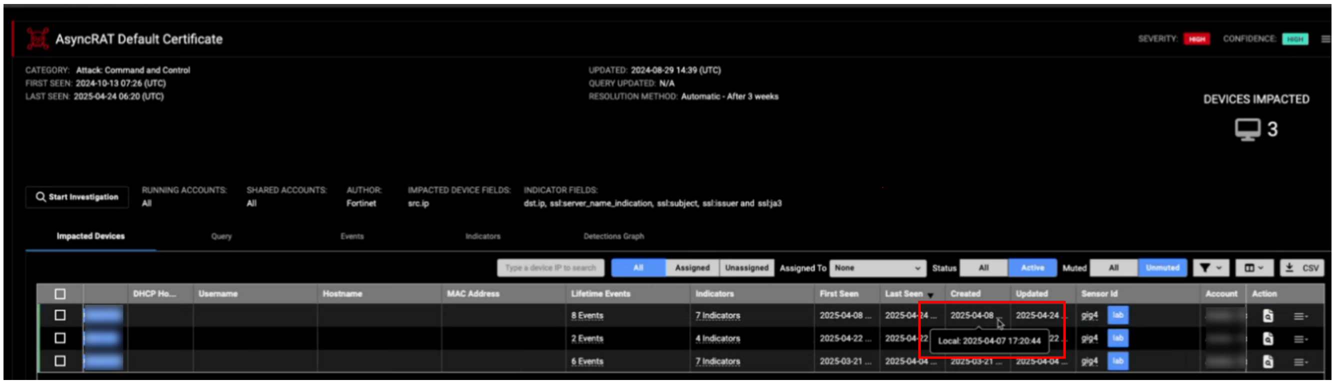
We have added the following event fields to the IQL search:

`ldap`	*argument*, *diagnostic_message*, *message_id*, *object*, *opcode*, *result*, *version*
`ldap_search`	*attributes*, *base_object*, *deref_aliases*, *diagnostic_message*, *filter*, *message_id*, *result*, *result_count*, *scope*

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.



AsyncRAT Default Certificate

SEVERITY: HIGH CONFIDENCE: HIGH

CATEGORY: Attack: Command and Control
FIRST SEEN: 2024-10-13 07:26 (UTC)
LAST SEEN: 2025-04-24 06:20 (UTC)

UPDATED: 2024-08-29 14:39 (UTC)
QUERY UPDATED: N/A
RESOLUTION METHOD: Automatic - After 3 weeks

DEVICES IMPACTED 3

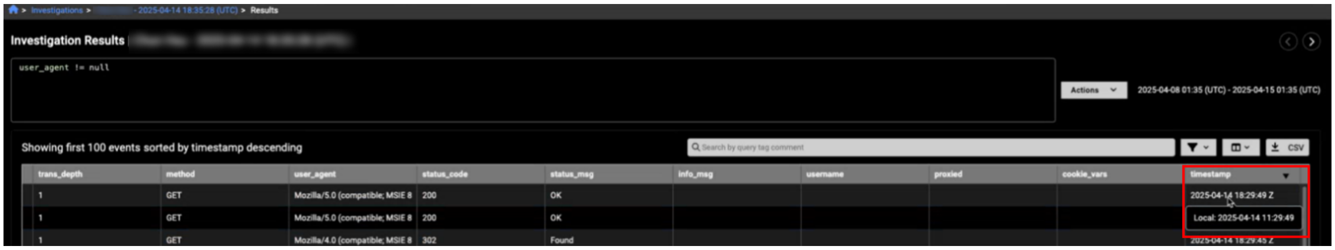
RUNNING ACCOUNTS: All
SHARED ACCOUNTS: All
AUTHOR: Fortinet
IMPACTED DEVICE FIELDS: src.ip
INDICATOR FIELDS: dst.ip, ssl:server_name_indication, ssl:subject, ssl:issuer and ssl:ja3

Assigned To: None
Status: Active
Muted: Unmuted

□		DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Indicators	First Seen	Last Seen	Created	Updated	Sensor Id	Account	Action
□	[redacted]					8 Events	7 Indicators	2025-04-08 ...	2025-04-24 ...	2025-04-08 ...	2025-04-24 ...	gig4 lab	[redacted]	
□	[redacted]					2 Events	4 Indicators	2025-04-22 ...	2025-04-22		22	gig4 lab	[redacted]	
□	[redacted]					6 Events	7 Indicators	2025-03-21 ...	2025-04-04 ...	2025-03-21 ...	2025-04-04 ...	gig4 lab	[redacted]	

Local: 2025-04-07 17:20:44

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



Investigations > [redacted] - 2025-04-14 18:35:28 (UTC) > Results

Investigation Results [redacted]

```
user_agent != null
```

2025-04-08 01:35 (UTC) - 2025-04-15 01:35 (UTC)

Showing first 100 events sorted by timestamp descending

trans_depth	method	user_agent	status_code	status_msg	info_msg	username	proxied	cookie_vars	timestamp
1	GET	Mozilla/5.0 (compatible; MSIE 8	200	OK					2025-04-14 18:29:49 Z
1	GET	Mozilla/5.0 (compatible; MSIE 8	200	OK					
1	GET	Mozilla/4.0 (compatible; MSIE 8	302	Found					2025-04-14 18:29:45 Z

Local: 2025-04-14 11:29:49

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.

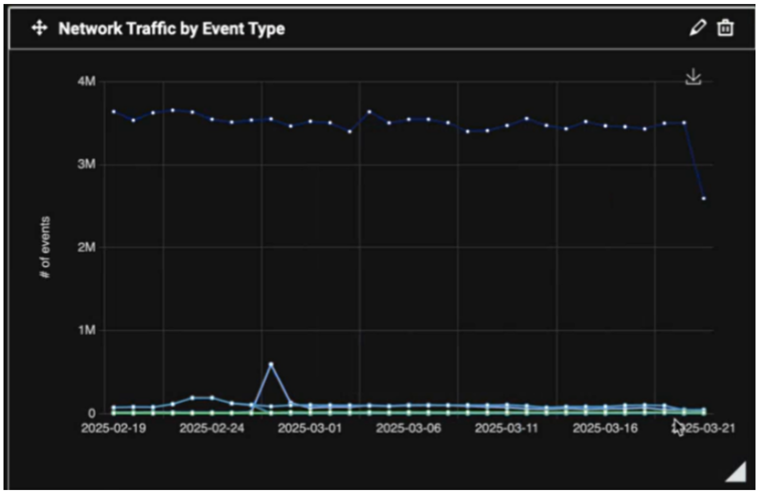
Version 25.1.e

New functionality

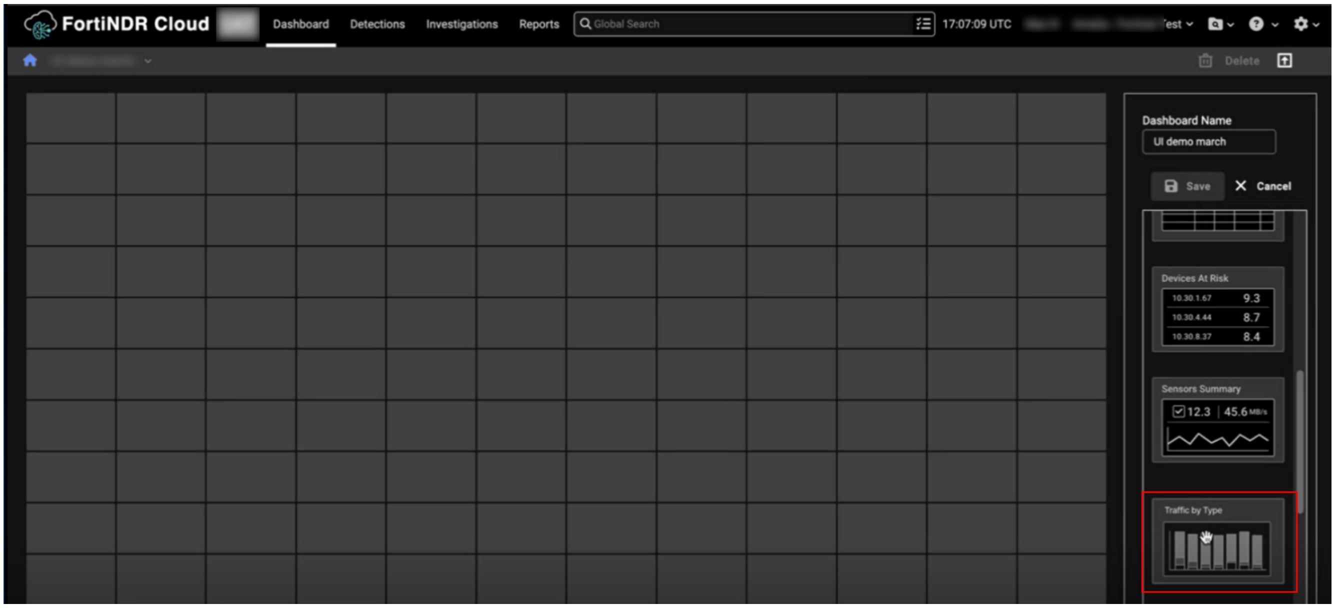
Custom dashboards

Traffic by 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.

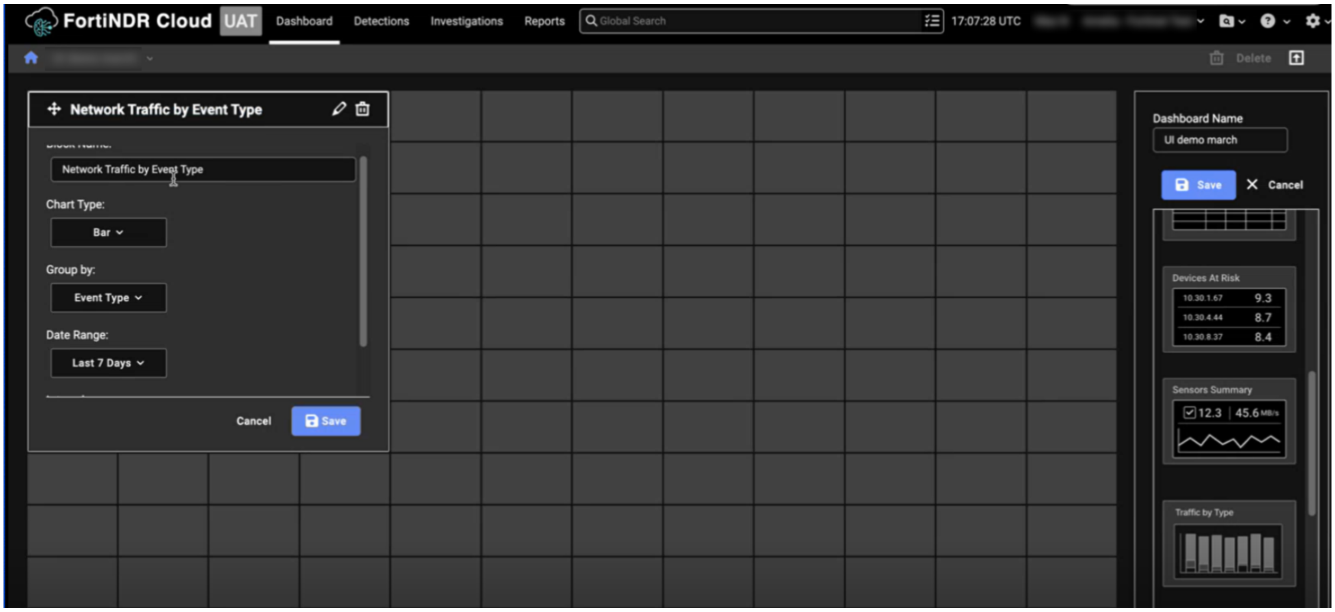


To add the widget, create a new dashboard, and select the *Traffic by type* widget in the menu.



Dashboard Name: UI demo march

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.



Block Name: Network Traffic by Event Type

Chart Type: Bar

Group by: Event Type

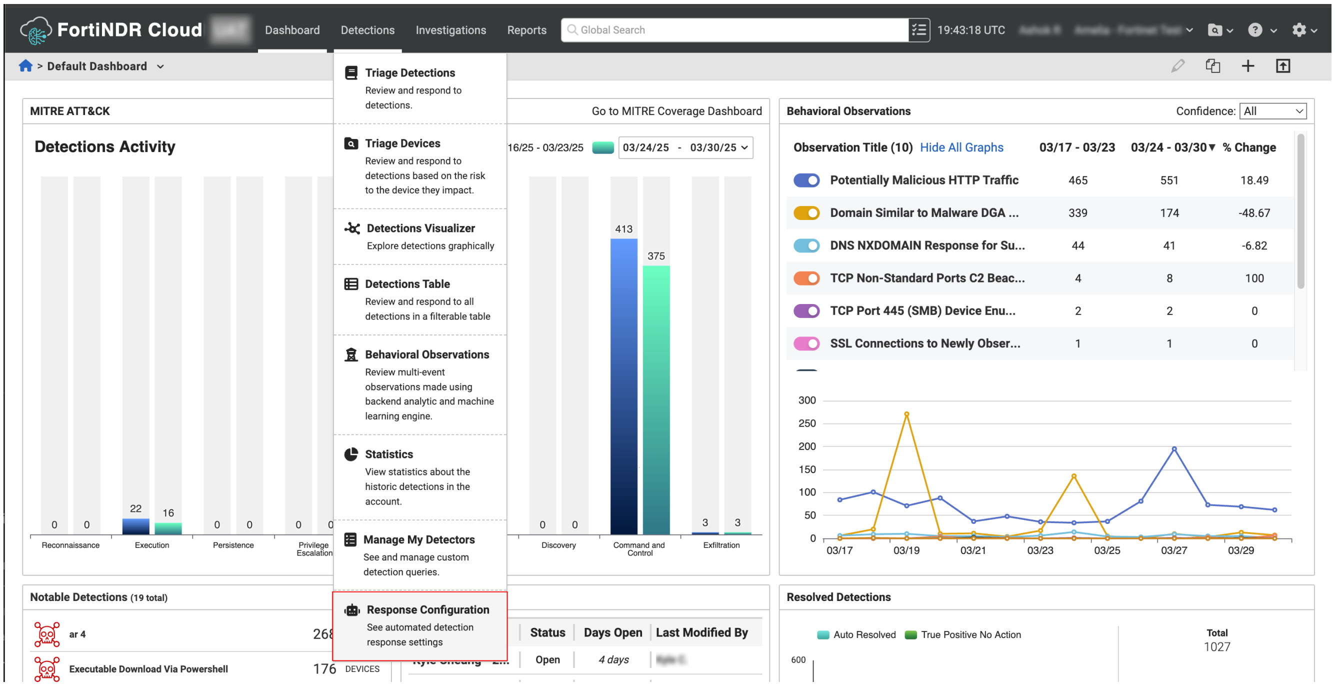
Date Range: Last 7 Days

Dashboard Name: UI demo march

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.



Triage Detections
Review and respond to detections.

Triage Devices
Review and respond to detections based on the risk to the device they impact.

Detections Visualizer
Explore detections graphically

Detections Table
Review and respond to all detections in a filterable table

Behavioral Observations
Review multi-event observations made using backend analytic and machine learning engine.

Statistics
View statistics about the historic detections in the account.

Manage My Detectors
See and manage custom detection queries.

Response Configuration
See automated detection response settings

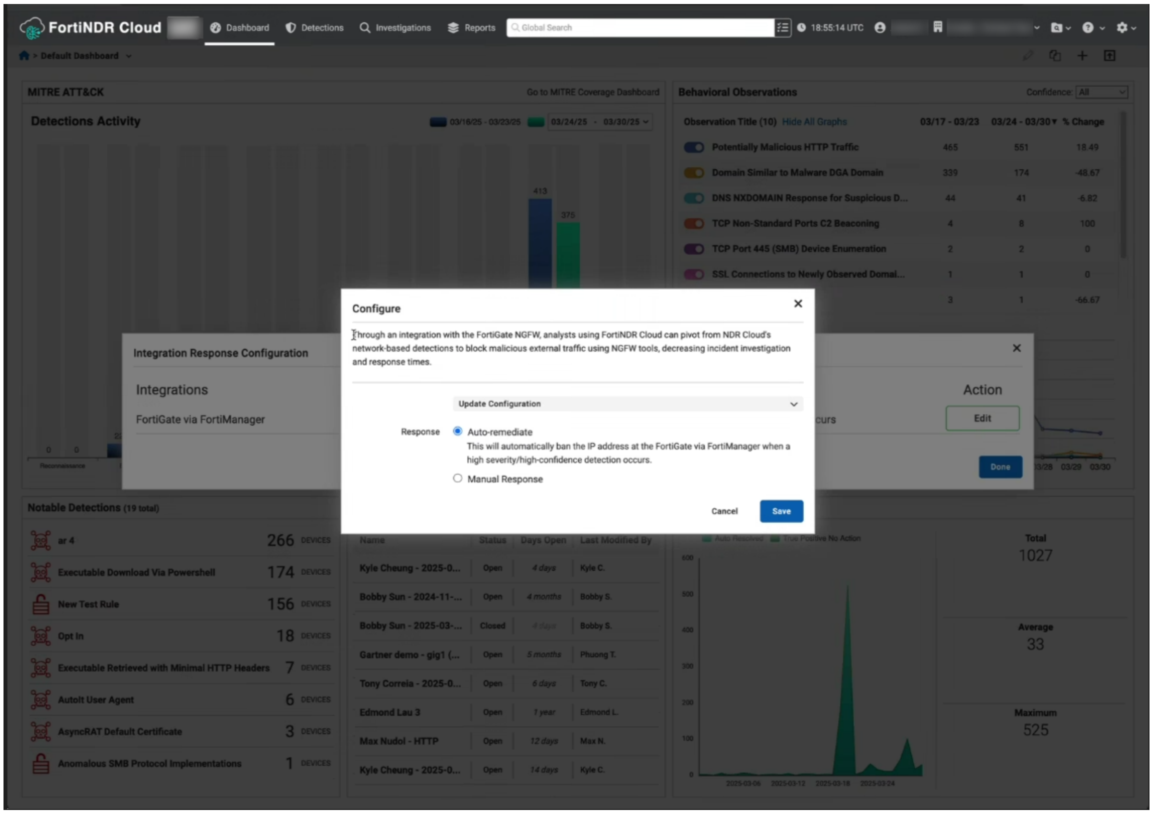
Behavioral Observations — Confidence: All

Observation Title (10) Hide All Graphs	03/17 - 03/23	03/24 - 03/30▾	% Change
Potentially Malicious HTTP Traffic	465	551	18.49
Domain Similar to Malware DGA ...	339	174	-48.67
DNS NXDOMAIN Response for Su...	44	41	-6.82
TCP Non-Standard Ports C2 Beac...	4	8	100
TCP Port 445 (SMB) Device Enu...	2	2	0
SSL Connections to Newly Obser...	1	1	0

Notable Detections (19 total)

			Status	Days Open	Last Modified By
ar 4	268				
Executable Download Via Powershell	176	DEVICES	Open	4 days	

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



Configure

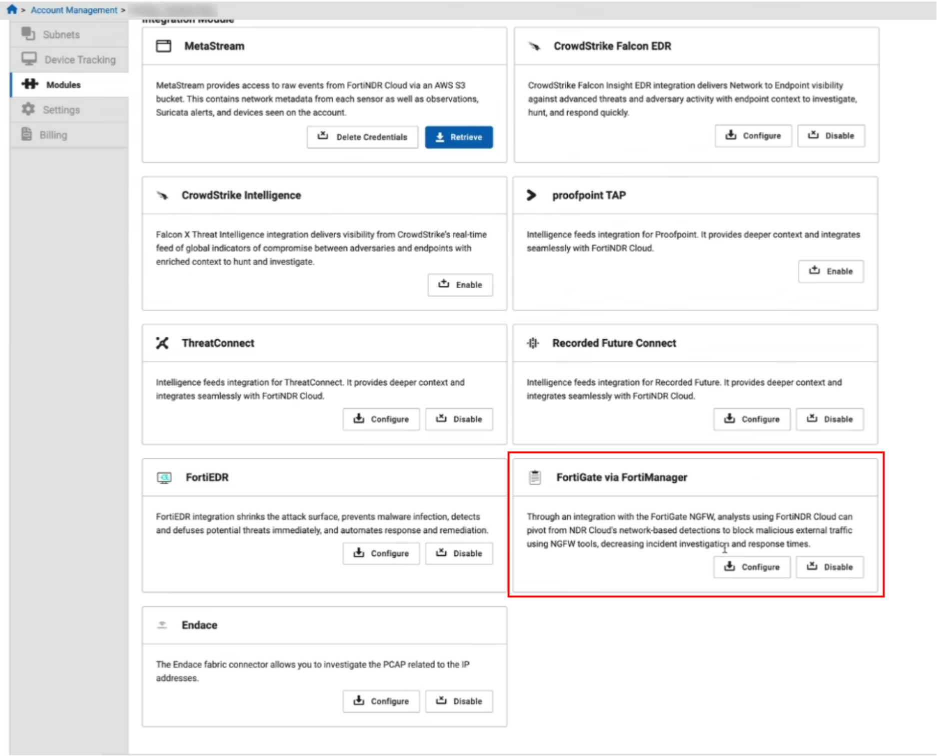
Through an integration with the FortiGate NGFW, analysts using FortiNDR Cloud can pivot from NDR Cloud's network-based detections to block malicious external traffic using NGFW tools, decreasing incident investigation and response times.

Update Configuration

Response ● Auto-remediate
This will automatically ban the IP address at the FortiGate via FortiManager when a high severity/high-confidence detection occurs.
○ Manual Response

Cancel Save

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



MetaStream

MetaStream provides access to raw events from FortiNDR Cloud via an AWS S3 bucket. This contains network metadata from each sensor as well as observations, Suricata alerts, and devices seen on the account.

CrowdStrike Falcon EDR

CrowdStrike Falcon Insight EDR integration delivers Network to Endpoint visibility against advanced threats and adversary activity with endpoint context to investigate, hunt, and respond quickly.

CrowdStrike Intelligence

Falcon X Threat Intelligence integration delivers visibility from CrowdStrike's real-time feed of global indicators of compromise between adversaries and endpoints with enriched context to hunt and investigate.

proofpoint TAP

Intelligence feeds integration for Proofpoint. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

ThreatConnect

Intelligence feeds integration for ThreatConnect. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

Recorded Future Connect

Intelligence feeds integration for Recorded Future. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

FortiEDR

FortiEDR integration shrinks the attack surface, prevents malware infection, detects and defuses potential threats immediately, and automates response and remediation.

FortiGate via FortiManager

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.

Endace

The Endace fabric connector allows you to investigate the PCAP related to the IP addresses.

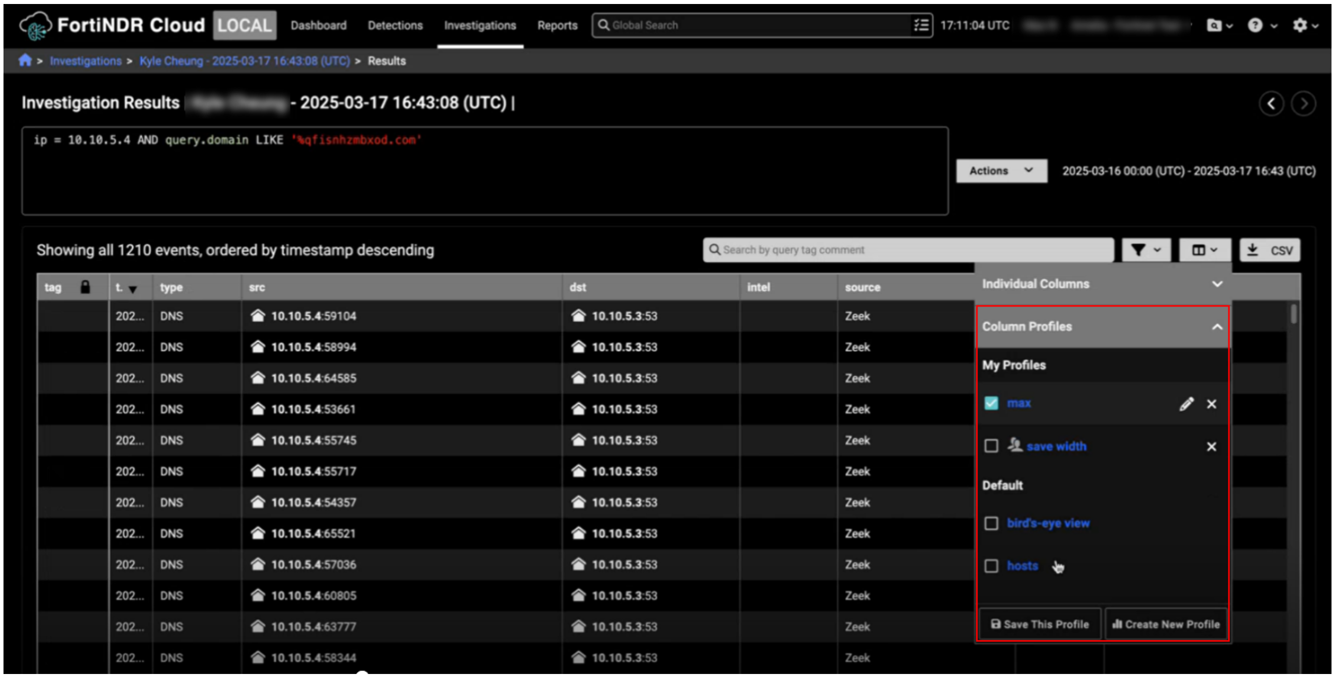
Improved functionality

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.



Investigation Results [redacted] - 2025-03-17 16:43:08 (UTC) |

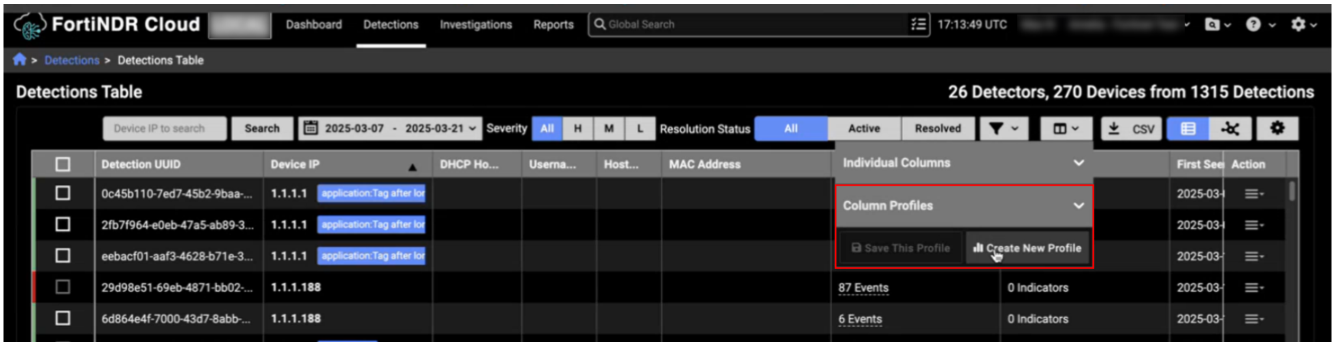
```
ip = 10.10.5.4 AND query.domain LIKE '%qfisnhzmbxod.com'
```

2025-03-16 00:00 (UTC) - 2025-03-17 16:43 (UTC)

Showing all 1210 events, ordered by timestamp descending

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

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.



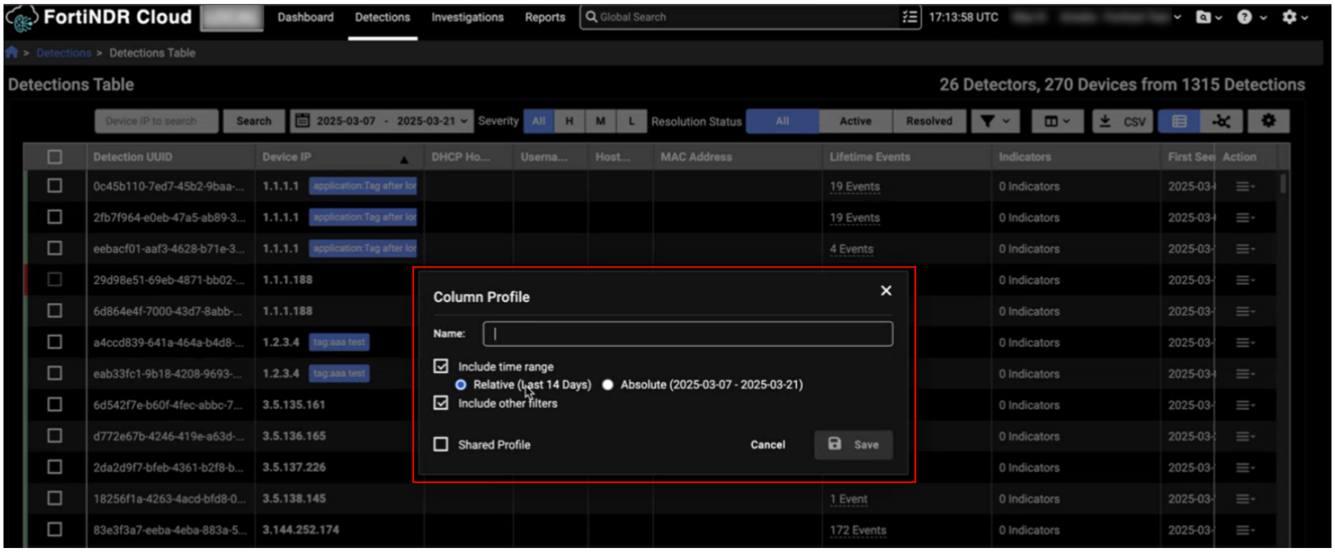
Detections Table

26 Detectors, 270 Devices from 1315 Detections

2025-03-07 - 2025-03-21

☐	Detection UUID	Device IP	DHCP Ho...	Userna...	Host...	MAC Address			First See	Action
☐	0c45b110-7ed7-45b2-9baa-...	1.1.1.1 application:Tag after lor							2025-03-	☰
☐	2fb7f964-e0eb-47a5-ab89-3...	1.1.1.1 application:Tag after lor							2025-03-	☰
☐	eebacf01-aaf3-4628-b71e-3...	1.1.1.1 application:Tag after lor							2025-03-	☰
☐	29d98e51-69eb-4871-bb02-...	1.1.1.188					87 Events	0 Indicators	2025-03-	☰
☐	6d864e4f-7000-43d7-8abb-...	1.1.1.188					6 Events	0 Indicators	2025-03-	☰

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.



Detections Table

26 Detectors, 270 Devices from 1315 Detections

Device IP to search | Search | 2025-03-07 - 2025-03-21 | Severity: All H M L | Resolution Status: All Active Resolved | CSV

□	Detection UUID	Device IP	DHCP Ho...	Userna...	Host...	MAC Address	Lifetime Events	Indicators	First Seen	Action
□	0c45b110-7ed7-45b2-9baa-...	1.1.1.1 application:Tag after lor					19 Events	0 Indicators	2025-03-	≡
□	2fb7f964-e0eb-47a5-ab89-3...	1.1.1.1 application:Tag after lor					19 Events	0 Indicators	2025-03-	≡
□	eebacf01-aaf3-4628-b71e-3...	1.1.1.1 application:Tag after lor					4 Events	0 Indicators	2025-03-	≡
□	29d98e51-69eb-4871-bb02-...	1.1.1.188						0 Indicators	2025-03-	≡
□	6d864e4f-7000-43d7-8abb-...	1.1.1.188						0 Indicators	2025-03-	≡
□	a4ccd839-641a-464a-b4d8-...	1.2.3.4 tag:aaa test						0 Indicators	2025-03-	≡
□	eab33fc1-9b18-4208-9693-...	1.2.3.4 tag:aaa test						0 Indicators	2025-03-	≡
□	6d542f7e-b60f-4fec-abbc-7...	3.5.135.161						0 Indicators	2025-03-	≡
□	d772e67b-4246-419e-a63d-...	3.5.136.165						0 Indicators	2025-03-	≡
□	2da2d9f7-bfeb-4361-b2f8-b...	3.5.137.226						0 Indicators	2025-03-	≡
□	18256f1a-4263-4acd-bfd8-0...	3.5.138.145					1 Event	0 Indicators	2025-03-	≡
□	83e3f3a7-eeba-4eba-883a-5...	3.144.252.174					172 Events	0 Indicators	2025-03-	≡

Column Profile

Name:

☑ Include time range

● Relative (Last 14 Days) ○ Absolute (2025-03-07 - 2025-03-21)

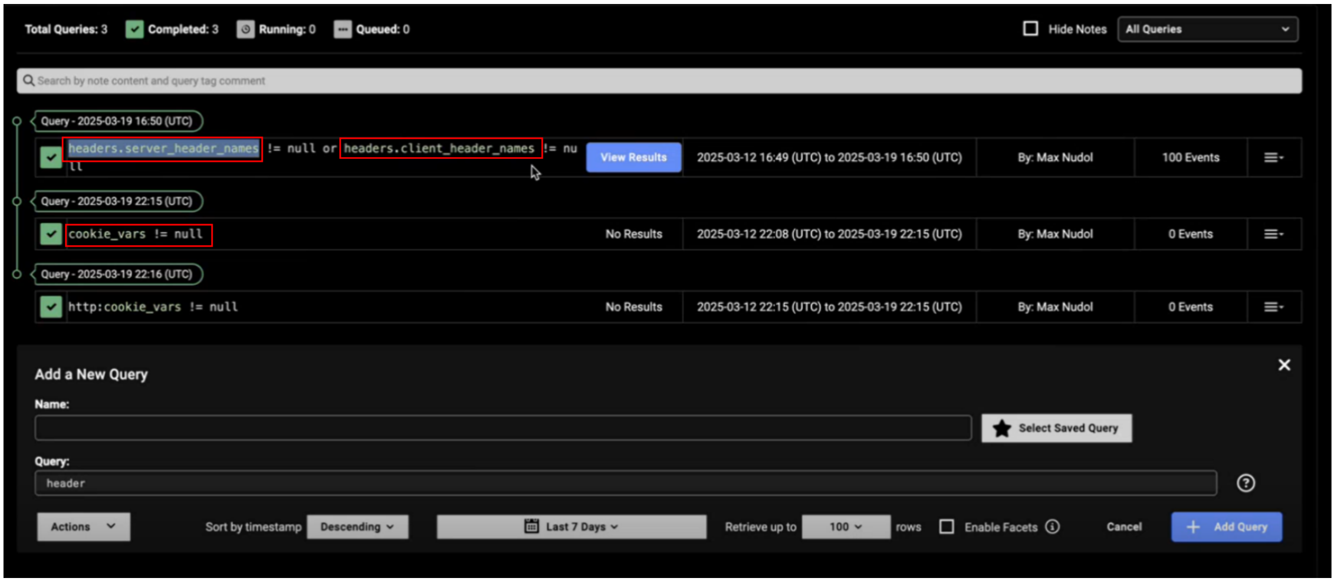
☑ Include other filters

□ Shared Profile

Cancel | Save

IQL queries

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



Total Queries: 3 | ☑ Completed: 3 | Running: 0 | Queued: 0

□ Hide Notes | All Queries

Search by note content and query tag comment

Query - 2025-03-19 16:50 (UTC)

	Query	Results	Time range	By	Events
☑	`headers.server_header_names != null or headers.client_header_names != null`	View Results	2025-03-12 16:49 (UTC) to 2025-03-19 16:50 (UTC)	By: Max Nudol	100 Events

Query - 2025-03-19 22:15 (UTC)

	Query	Results	Time range	By	Events
☑	`cookie_vars != null`	No Results	2025-03-12 22:08 (UTC) to 2025-03-19 22:15 (UTC)	By: Max Nudol	0 Events

Query - 2025-03-19 22:16 (UTC)

	Query	Results	Time range	By	Events
☑	`http:cookie_vars != null`	No Results	2025-03-12 22:15 (UTC) to 2025-03-19 22:15 (UTC)	By: Max Nudol	0 Events

Add a New Query

Name:

Select Saved Query

Query:

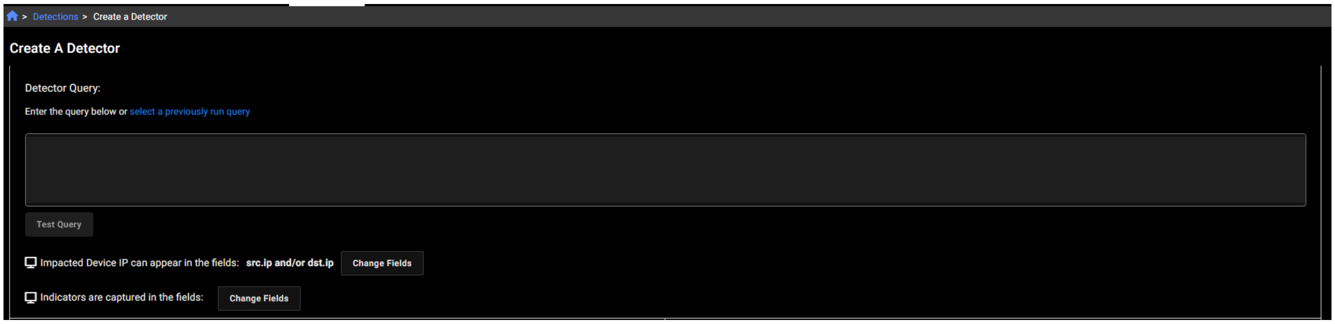
```
header
```

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

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.



Create A Detector

Detector Query:

Enter the query below or select a previously run query

Impacted Device IP can appear in the fields: **src.ip and/or dst.ip**

Indicators are captured in the fields:

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.

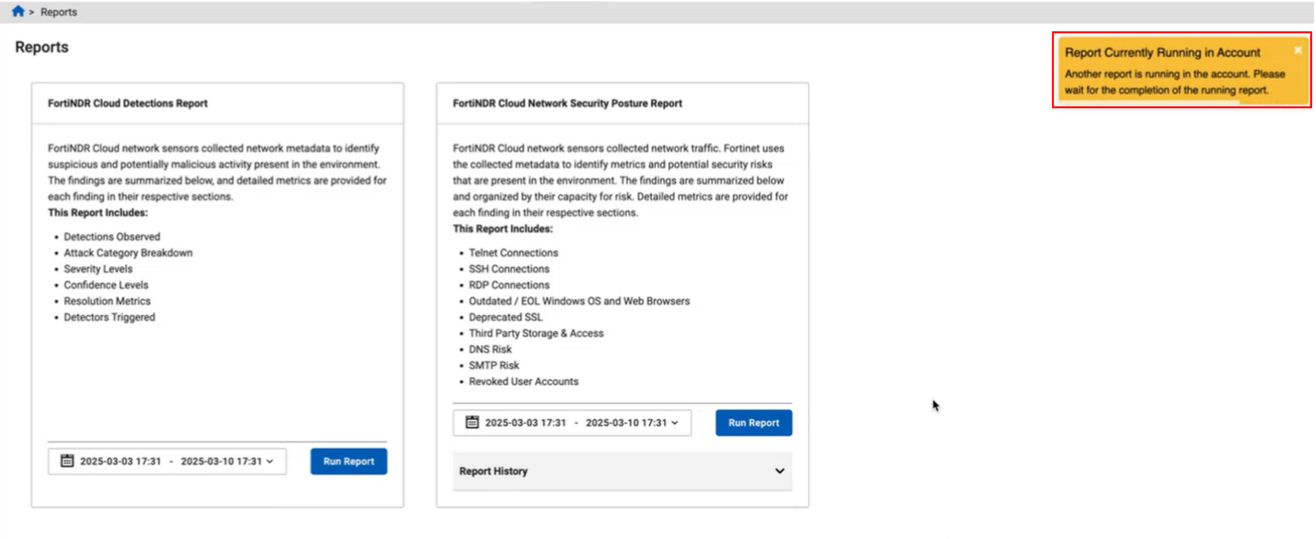
Version 25.1.d

Improved functionality

Reports

Pending queries in reports

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.



Reports

Report Currently Running in Account
Another report is running in the account. Please wait for the completion of the running report.

FortiNDR Cloud Detections Report

FortiNDR Cloud network sensors collected network metadata to identify suspicious and potentially malicious activity present in the environment. The findings are summarized below, and detailed metrics are provided for each finding in their respective sections.
This Report Includes:
- Detections Observed
- Attack Category Breakdown
- Severity Levels
- Confidence Levels
- Resolution Metrics
- Detectors Triggered

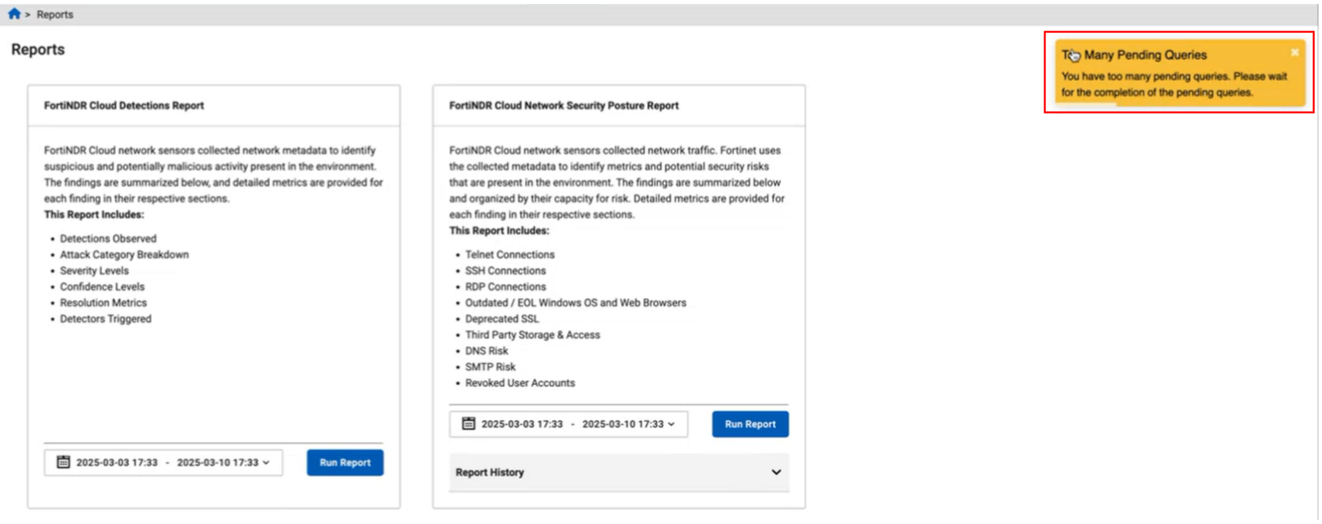
2025-03-03 17:31 - 2025-03-10 17:31

FortiNDR Cloud Network Security Posture Report

FortiNDR Cloud network sensors collected network traffic. Fortinet uses the collected metadata to identify metrics and potential security risks that are present in the environment. The findings are summarized below and organized by their capacity for risk. Detailed metrics are provided for each finding in their respective sections.
This Report Includes:
- Telnet Connections
- SSH Connections
- RDP Connections
- Outdated / EOL Windows OS and Web Browsers
- Deprecated SSL
- Third Party Storage & Access
- DNS Risk
- SMTP Risk
- Revoked User Accounts

2025-03-03 17:31 - 2025-03-10 17:31

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



Reports

Too Many Pending Queries
You have too many pending queries. Please wait for the completion of the pending queries.

FortiNDR Cloud Detections Report

FortiNDR Cloud network sensors collected network metadata to identify suspicious and potentially malicious activity present in the environment. The findings are summarized below, and detailed metrics are provided for each finding in their respective sections.
This Report Includes:
- Detections Observed
- Attack Category Breakdown
- Severity Levels
- Confidence Levels
- Resolution Metrics
- Detectors Triggered

2025-03-03 17:33 - 2025-03-10 17:33

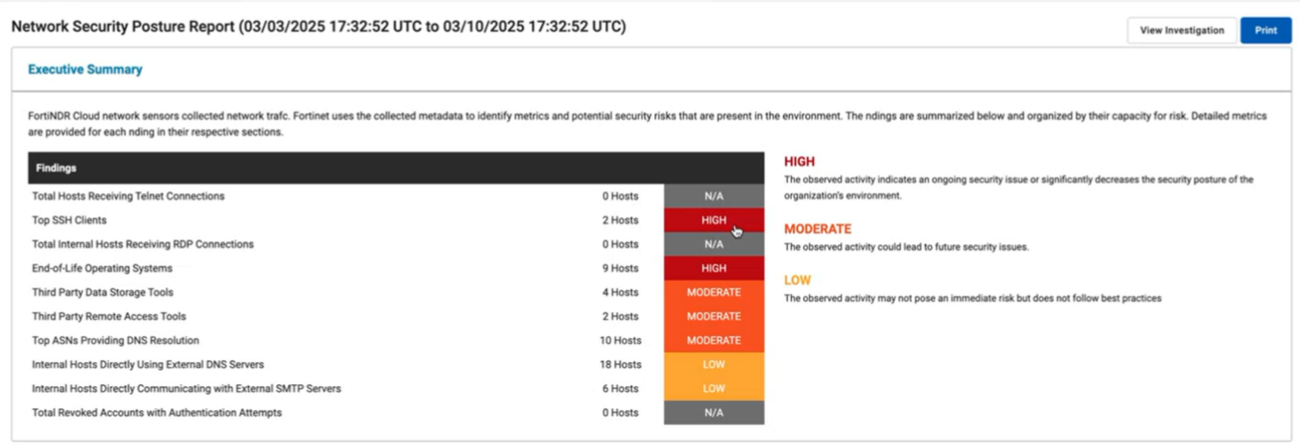
FortiNDR Cloud Network Security Posture Report

FortiNDR Cloud network sensors collected network traffic. Fortinet uses the collected metadata to identify metrics and potential security risks that are present in the environment. The findings are summarized below and organized by their capacity for risk. Detailed metrics are provided for each finding in their respective sections.
This Report Includes:
- Telnet Connections
- SSH Connections
- RDP Connections
- Outdated / EOL Windows OS and Web Browsers
- Deprecated SSL
- Third Party Storage & Access
- DNS Risk
- SMTP Risk
- Revoked User Accounts

2025-03-03 17:33 - 2025-03-10 17:33

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.



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

Executive Summary

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

Findings		
Total Hosts Receiving Telnet Connections	0 Hosts	N/A
Top SSH Clients	2 Hosts	HIGH
Total Internal Hosts Receiving RDP Connections	0 Hosts	N/A
End-of-Life Operating Systems	9 Hosts	HIGH
Third Party Data Storage Tools	4 Hosts	MODERATE
Third Party Remote Access Tools	2 Hosts	MODERATE
Top ASNs Providing DNS Resolution	10 Hosts	MODERATE
Internal Hosts Directly Using External DNS Servers	18 Hosts	LOW
Internal Hosts Directly Communicating with External SMTP Servers	6 Hosts	LOW
Total Revoked Accounts with Authentication Attempts	0 Hosts	N/A

HIGH

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

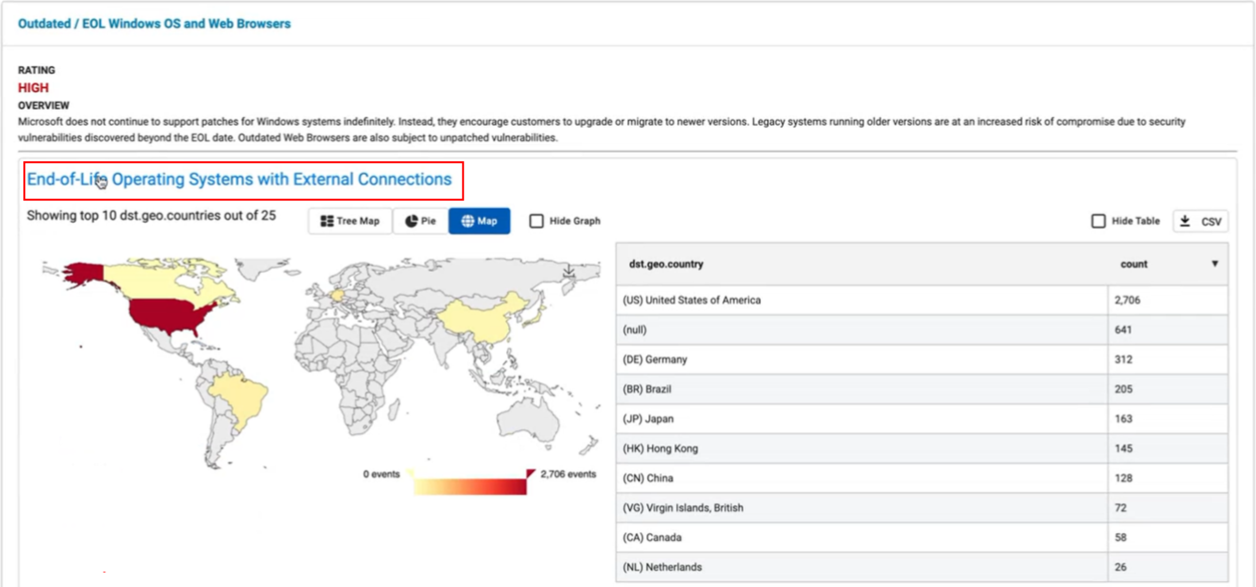
MODERATE

The observed activity could lead to future security issues.

LOW

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

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

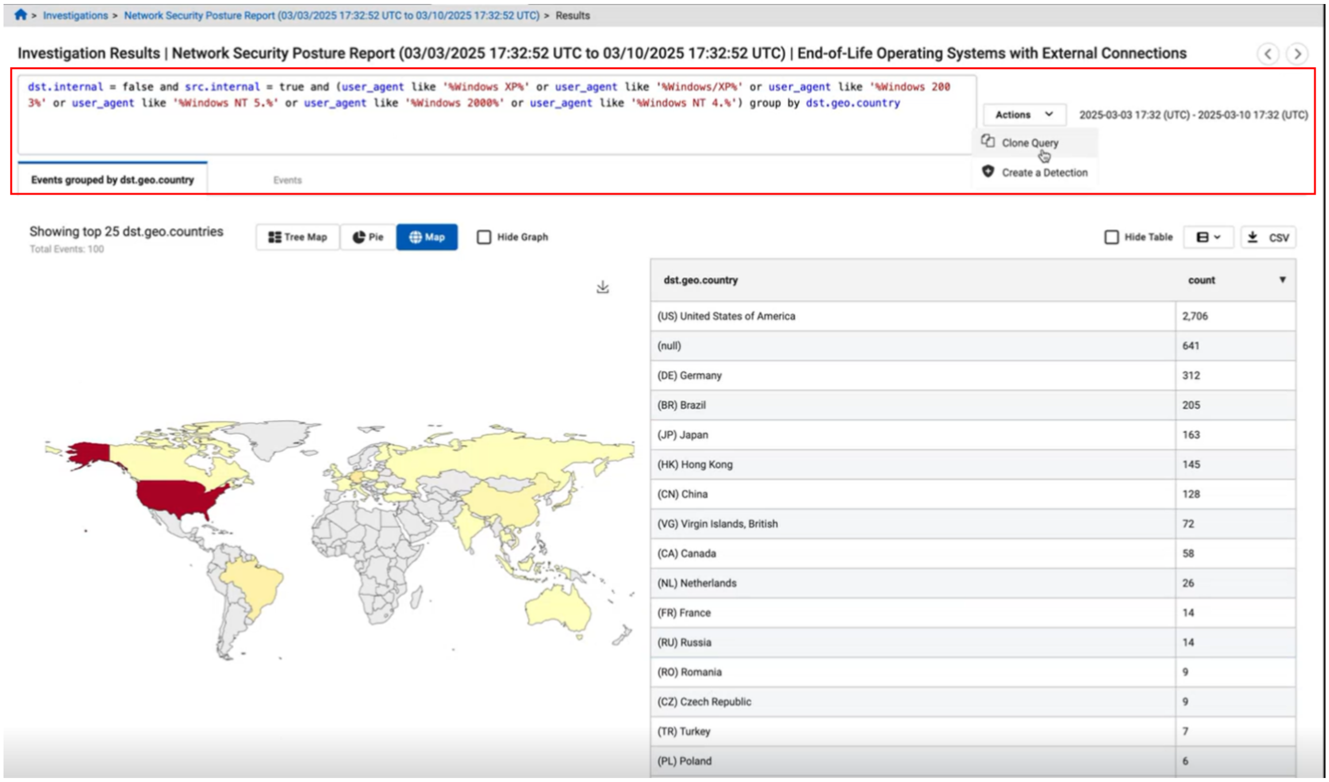
OVERVIEW

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

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 200
3%' or user_agent like '%Windows NT 5.%' or user_agent like '%Windows 2000%' or user_agent like '%Windows NT 4.%') group by dst.geo.country
```

Showing top 25 dst.geo.countries
Total Events: 100

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.

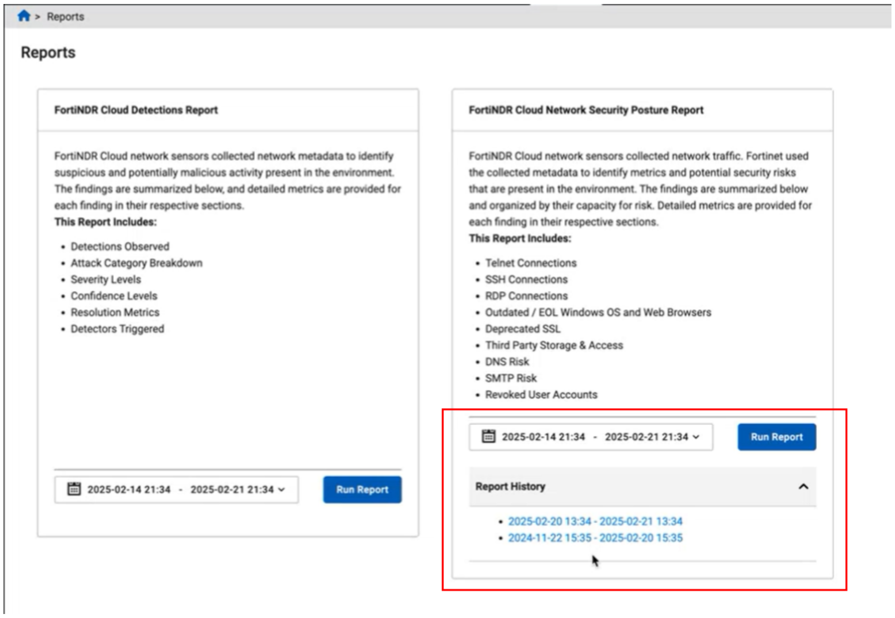
Version 25.1.c

New functionality

Reports

FortiNDR Cloud Network Security Posture Report

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.



FortiNDR Cloud Detections Report

FortiNDR Cloud network sensors collected network metadata to identify suspicious and potentially malicious activity present in the environment. The findings are summarized below, and detailed metrics are provided for each finding in their respective sections.

This Report Includes:

- Detections Observed
- Attack Category Breakdown
- Severity Levels
- Confidence Levels
- Resolution Metrics
- Detectors Triggered

2025-02-14 21:34 - 2025-02-21 21:34

FortiNDR Cloud Network Security Posture Report

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

This Report Includes:

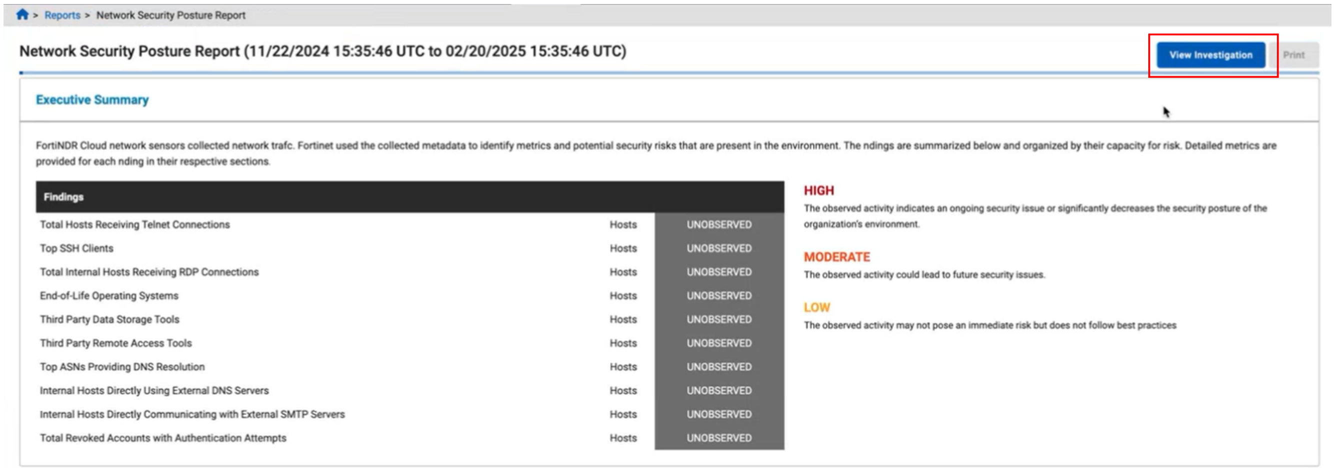
- Telnet Connections
- SSH Connections
- RDP Connections
- Outdated / EOL Windows OS and Web Browsers
- Deprecated SSL
- Third Party Storage & Access
- DNS Risk
- SMTP Risk
- Revoked User Accounts

2025-02-14 21:34 - 2025-02-21 21:34

Report History

- 2025-02-20 13:34 - 2025-02-21 13:34
- 2024-11-22 15:35 - 2025-02-20 15:35

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



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

Executive Summary

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

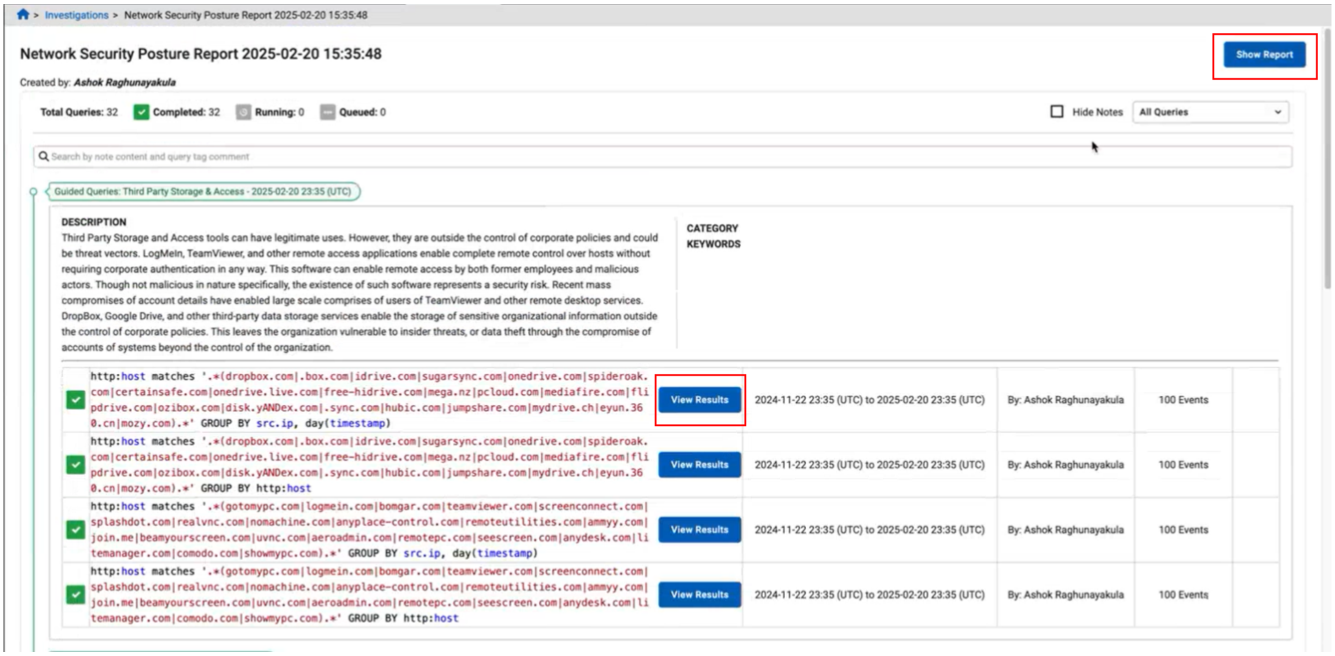
Findings		
Total Hosts Receiving Telnet Connections	Hosts	UNOBSERVED
Top SSH Clients	Hosts	UNOBSERVED
Total Internal Hosts Receiving RDP Connections	Hosts	UNOBSERVED
End-of-Life Operating Systems	Hosts	UNOBSERVED
Third Party Data Storage Tools	Hosts	UNOBSERVED
Third Party Remote Access Tools	Hosts	UNOBSERVED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

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

MODERATE
The observed activity could lead to future security issues.

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

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


Investigations > Network Security Posture Report 2025-02-20 15:35:48
Show Report
Hide Notes
All Queries
Search by note content and query tag comment
View Results

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

Created by: *Ashok Raghunayakula*

Total Queries: 32 ☑ Completed: 32 Running: 0 Queued: 0

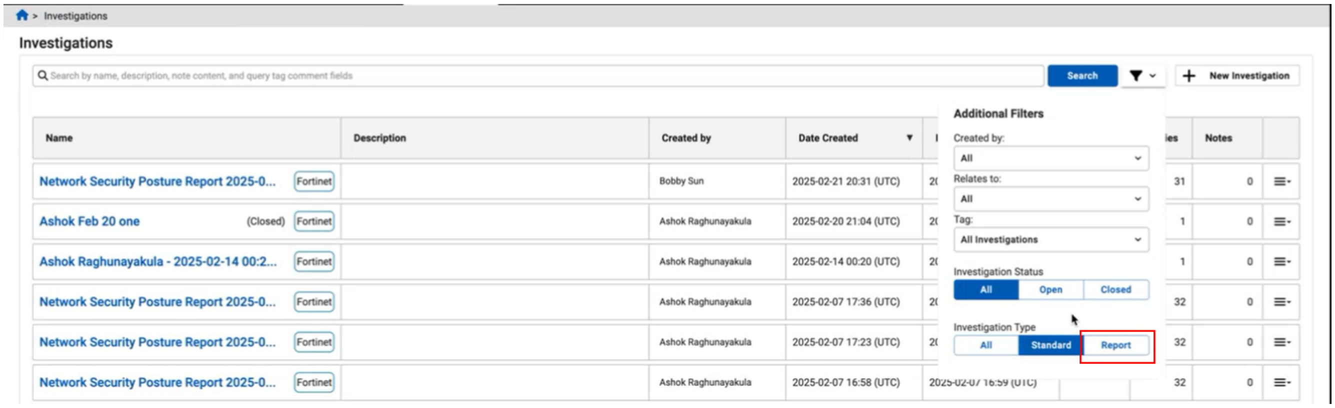
Guided Queries: Third Party Storage & Access - 2025-02-20 23:35 (UTC)

DESCRIPTION
Third Party Storage and Access tools can have legitimate uses. However, they are outside the control of corporate policies and could be threat vectors. LogMeln, TeamViewer, and other remote access applications enable complete remote control over hosts without requiring corporate authentication in any way. This software can enable remote access by both former employees and malicious actors. Though not malicious in nature specifically, the existence of such software represents a security risk. Recent mass compromises of account details have enabled large scale comprises of users of TeamViewer and other remote desktop services. DropBox, Google Drive, and other third-party data storage services enable the storage of sensitive organizational information outside the control of corporate policies. This leaves the organization vulnerable to insider threats, or data theft through the compromise of accounts of systems beyond the control of the organization.

CATEGORY
KEYWORDS

☑	`http:host matches '.*(dropbox.com|.box.com|idrive.com|sugarsync.com|onedrive.com|spideroak.com|certainsafe.com|onedrive.live.com|free-hidrive.com|mega.nz|pcloud.com|mediafire.com|flipdrive.com|ozibox.com|disk.yANDex.com|.sync.com|hubic.com|jumpshare.com|mydrive.ch|eyun.360.cn|mozy.com).*' GROUP BY src.ip, day(timestamp)`	View Results	2024-11-22 23:35 (UTC) to 2025-02-20 23:35 (UTC)	By: Ashok Raghunayakula	100 Events
☑	`http:host matches '.*(dropbox.com|.box.com|idrive.com|sugarsync.com|onedrive.com|spideroak.com|certainsafe.com|onedrive.live.com|free-hidrive.com|mega.nz|pcloud.com|mediafire.com|flipdrive.com|ozibox.com|disk.yANDex.com|.sync.com|hubic.com|jumpshare.com|mydrive.ch|eyun.360.cn|mozy.com).*' GROUP BY http:host`	View Results	2024-11-22 23:35 (UTC) to 2025-02-20 23:35 (UTC)	By: Ashok Raghunayakula	100 Events
☑	`http:host matches '.*(gotomypc.com|logmein.com|bomgar.com|teamviewer.com|screenconnect.com|splashdot.com|realvnc.com|nomachine.com|anyplace-control.com|remoteutilities.com|ammyy.com|join.me|beamyourscreen.com|uvnc.com|aeroadmin.com|remotepc.com|seescreen.com|anydesk.com|litemanager.com|comodo.com|showmypc.com).*' GROUP BY src.ip, day(timestamp)`	View Results	2024-11-22 23:35 (UTC) to 2025-02-20 23:35 (UTC)	By: Ashok Raghunayakula	100 Events
☑	`http:host matches '.*(gotomypc.com|logmein.com|bomgar.com|teamviewer.com|screenconnect.com|splashdot.com|realvnc.com|nomachine.com|anyplace-control.com|remoteutilities.com|ammyy.com|join.me|beamyourscreen.com|uvnc.com|aeroadmin.com|remotepc.com|seescreen.com|anydesk.com|litemanager.com|comodo.com|showmypc.com).*' GROUP BY http:host`	View Results	2024-11-22 23:35 (UTC) to 2025-02-20 23:35 (UTC)	By: Ashok Raghunayakula	100 Events

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



Investigations
Investigations
Search by name, description, note content, and query tag comment fields
Search
New Investigation

Name	Description	Created by	Date Created	I	ies	Notes
Network Security Posture Report 2025-0... Fortinet		Bobby Sun	2025-02-21 20:31 (UTC)	20	31	0
Ashok Feb 20 one (Closed) Fortinet		Ashok Raghunayakula	2025-02-20 21:04 (UTC)	20	1	0
Ashok Raghunayakula - 2025-02-14 00:2... Fortinet		Ashok Raghunayakula	2025-02-14 00:20 (UTC)	20	1	0
Network Security Posture Report 2025-0... Fortinet		Ashok Raghunayakula	2025-02-07 17:36 (UTC)	20	32	0
Network Security Posture Report 2025-0... Fortinet		Ashok Raghunayakula	2025-02-07 17:23 (UTC)	20	32	0
Network Security Posture Report 2025-0... Fortinet		Ashok Raghunayakula	2025-02-07 16:58 (UTC)	2025-02-07 16:59 (UTC)	32	0

Additional Filters

Created by: All

Relates to: All

Tag: All Investigations

Investigation Status: [✓ All] Open Closed

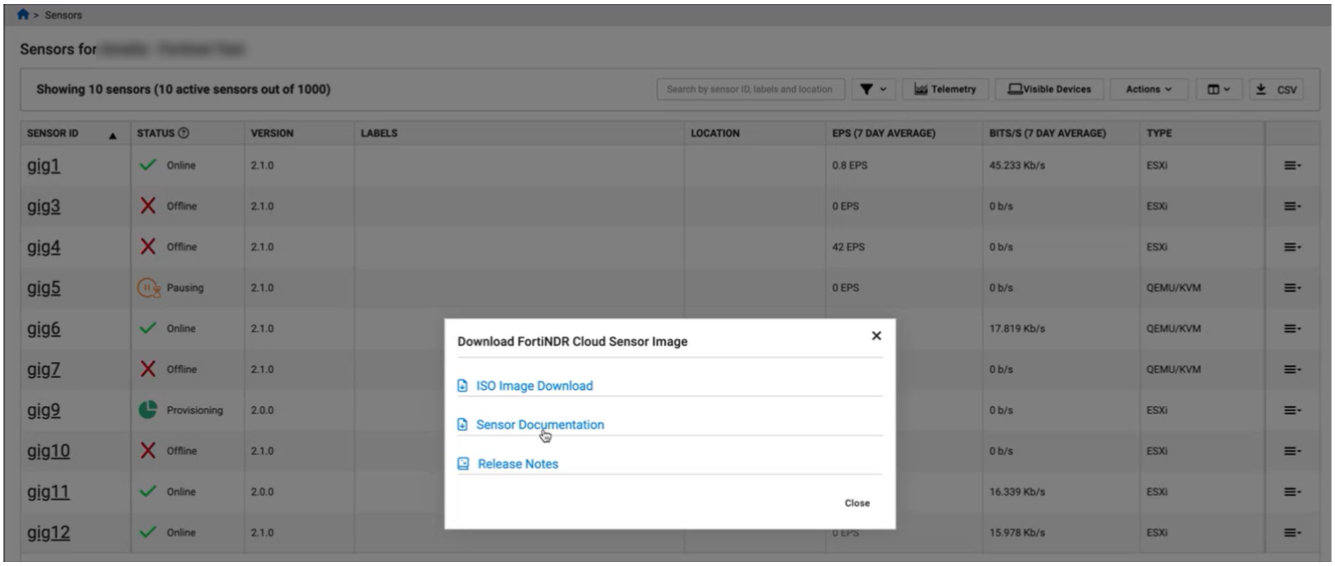
Investigation Type: All [✓ Standard] Report

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*.



Sensors for [redacted]

Showing 10 sensors (10 active sensors out of 1000)

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			0 EPS	15.978 Kb/s	ESXi

Download FortiNDR Cloud Sensor Image

- ISO Image Download
- Sensor Documentation
- Release Notes

Close

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.

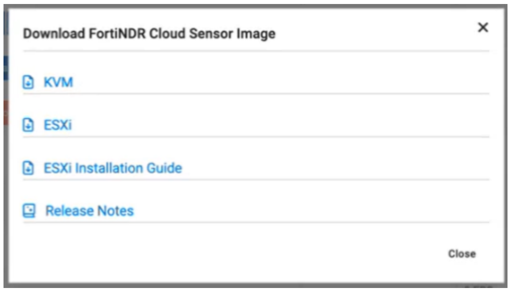
Version 25.1.b

Improved functionality

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.



Download FortiNDR Cloud Sensor Image ×

KVM

ESXi

ESXi Installation Guide

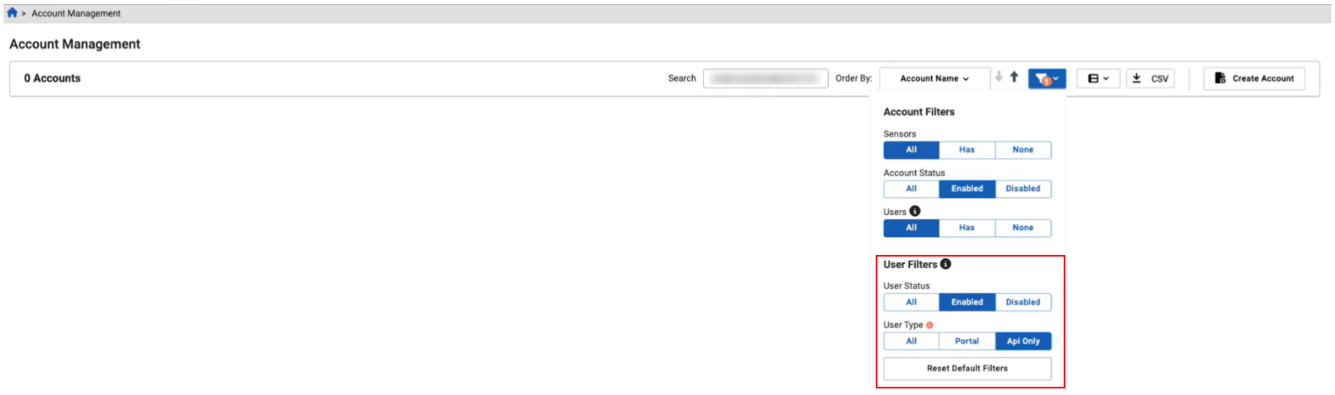
Release Notes

Close

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.



Account Management

Account Management

0 Accounts

Search | Order By: Account Name | CSV | Create Account

Account Filters

Sensors: All | Has | None

Account Status: All | Enabled | Disabled

Users: All | Has | None

User Filters

User Status: All | Enabled | Disabled

User Type: All | Portal | Api Only

Reset Default Filters

Sensors

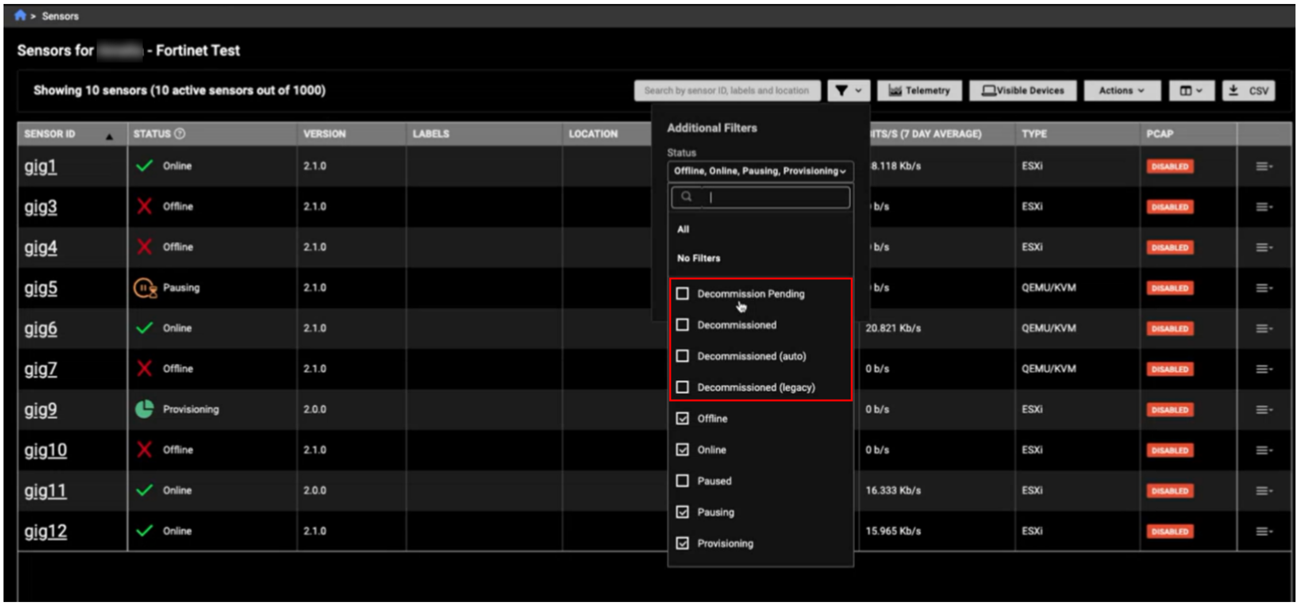
Static filters

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.



Sensors for [redacted] - Fortinet Test

Showing 10 sensors (10 active sensors out of 1000)

SENSOR ID	STATUS	VERSION	LABELS	LOCATION	ITS/S (7 DAY AVERAGE)	TYPE	PCAP
gig1	✓ Online	2.1.0			8.118 Kb/s	ESXi	DISABLED
gig3	✗ Offline	2.1.0			b/s	ESXi	DISABLED
gig4	✗ Offline	2.1.0			b/s	ESXi	DISABLED
gig5	Pausing	2.1.0			b/s	QEMU/KVM	DISABLED
gig6	✓ Online	2.1.0			20.821 Kb/s	QEMU/KVM	DISABLED
gig7	✗ Offline	2.1.0			0 b/s	QEMU/KVM	DISABLED
gig9	Provisioning	2.0.0			0 b/s	ESXi	DISABLED
gig10	✗ Offline	2.1.0			0 b/s	ESXi	DISABLED
gig11	✓ Online	2.0.0			16.333 Kb/s	ESXi	DISABLED
gig12	✓ Online	2.1.0			15.965 Kb/s	ESXi	DISABLED

Additional Filters

Status: Offline, Online, Pausing, Provisioning

All

No Filters

- □ Decommission Pending
- □ Decommissioned
- □ Decommissioned (auto)
- □ Decommissioned (legacy)
- ☑ Offline
- ☑ Online
- □ Paused
- ☑ Pausing
- ☑ Provisioning

Version 25.1.a

- New functionality on page 65
  - Integrations on page 65
    - Endace integration on page 65
  - Investigations on page 67
    - Annotations on page 67
- Improved functionality on page 67
  - Reports on page 67
    - FortiNDR Cloud Network Security Posture Report on page 67
  - Behavioral observations on page 68
    - Time ranges on page 68
  - Integrations on page 69
    - FortiEDR on page 69
  - Other improvements on page 69

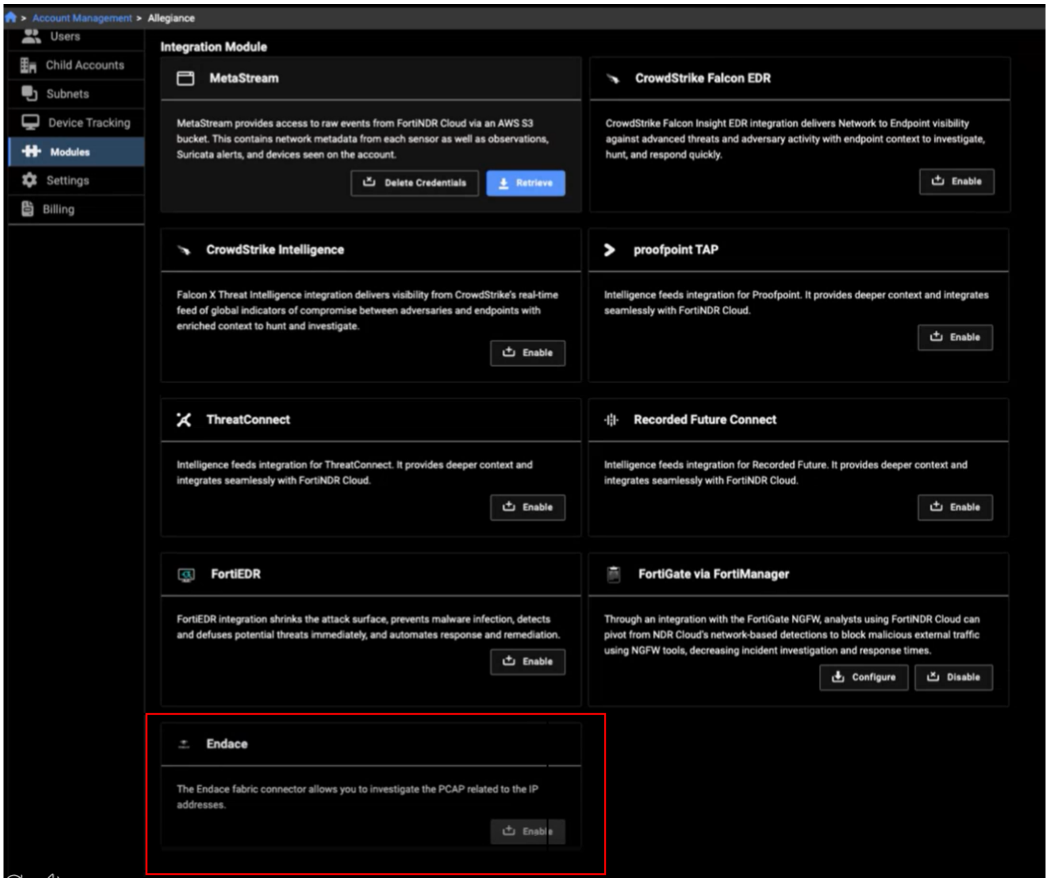
- Tooltips on page 69
- Resolved issues on page 75

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.



MetaStream

MetaStream provides access to raw events from FortiNDR Cloud via an AWS S3 bucket. This contains network metadata from each sensor as well as observations, Suricata alerts, and devices seen on the account.

CrowdStrike Falcon EDR

CrowdStrike Falcon Insight EDR integration delivers Network to Endpoint visibility against advanced threats and adversary activity with endpoint context to investigate, hunt, and respond quickly.

CrowdStrike Intelligence

Falcon X Threat Intelligence integration delivers visibility from CrowdStrike's real-time feed of global indicators of compromise between adversaries and endpoints with enriched context to hunt and investigate.

proofpoint TAP

Intelligence feeds integration for Proofpoint. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

ThreatConnect

Intelligence feeds integration for ThreatConnect. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

Recorded Future Connect

Intelligence feeds integration for Recorded Future. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

FortiEDR

FortiEDR integration shrinks the attack surface, prevents malware infection, detects and defuses potential threats immediately, and automates response and remediation.

FortiGate via FortiManager

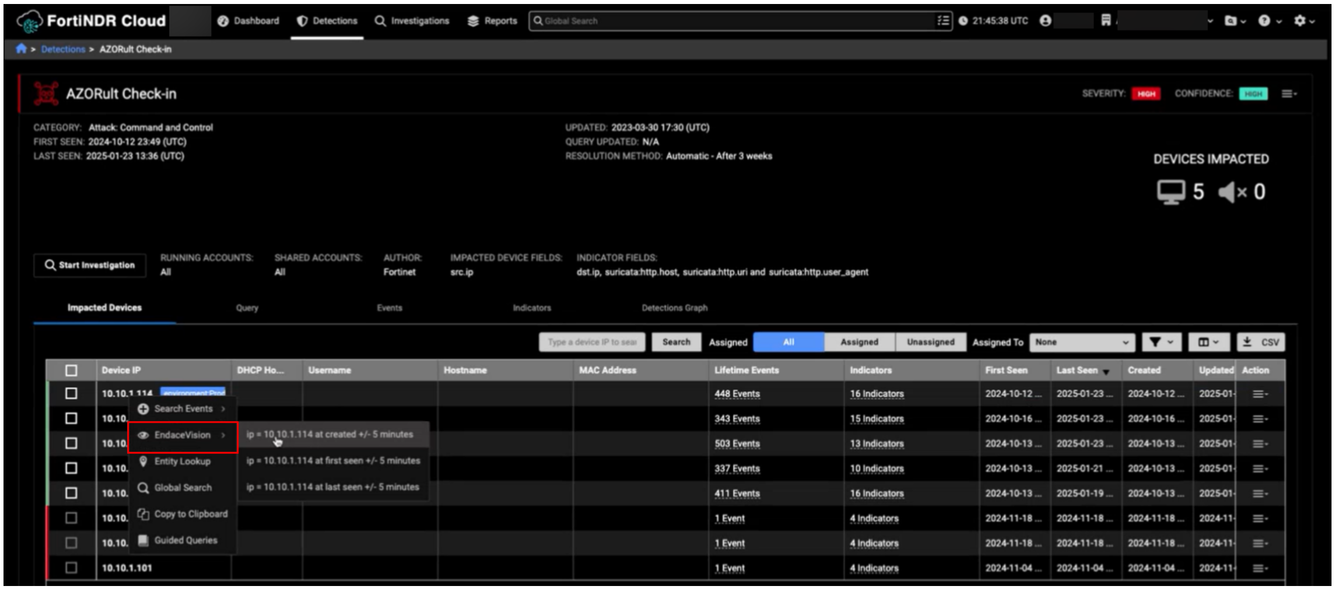
Through an integration with the FortiGate NGFW, analysts using FortiNDR Cloud can pivot from NDR Cloud's network-based detections to block malicious external traffic using NGFW tools, decreasing incident investigation and response times.

Endace

The Endace fabric connector allows you to investigate the PCAP related to the IP addresses.

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.



AZORult Check-in

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

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

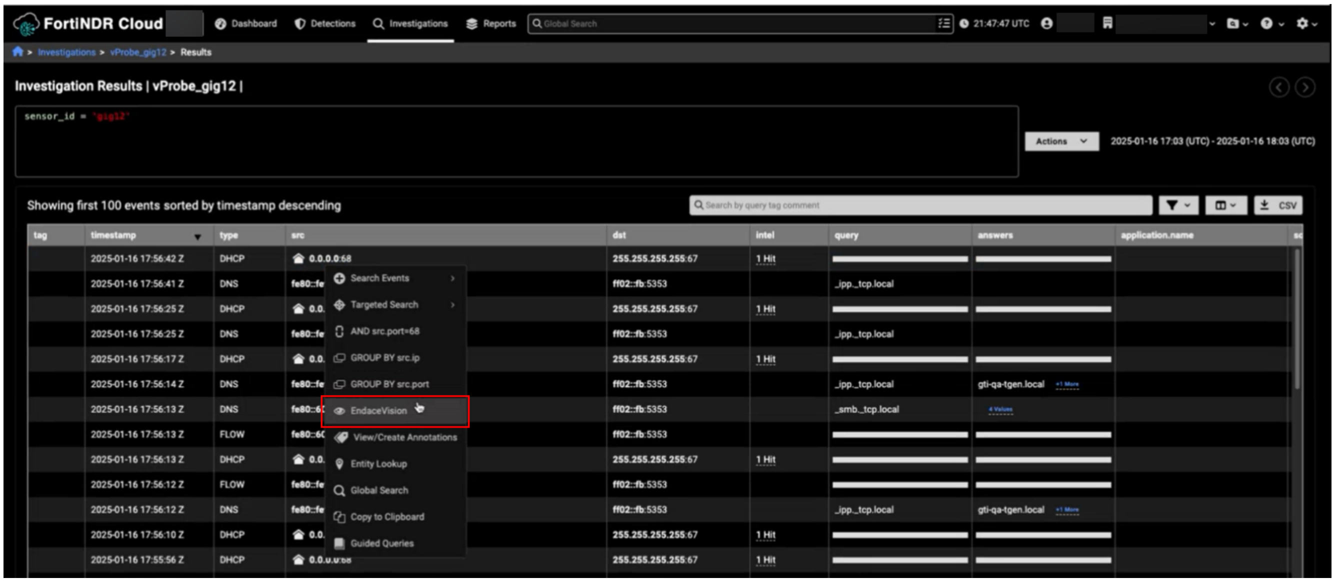
RUNNING ACCOUNTS: All
SHARED ACCOUNTS: All
AUTHOR: Fortinet
IMPACTED DEVICE FIELDS: src.ip
INDICATOR FIELDS: dst.ip, suricata:http.host, suricata:http.uri and suricata:http.user_agent

☐	Device IP	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Indicators	First Seen	Last Seen	Created	Updated	Action
☐	10.10.1.114 environment:Prod					448 Events	16 Indicators	2024-10-12 ...	2025-01-23 ...	2024-10-12 ...	2025-01-	≡
☐	10.10.					343 Events	15 Indicators	2024-10-16 ...	2025-01-23 ...	2024-10-16 ...	2025-01-	≡
☐	10.10.					503 Events	13 Indicators	2024-10-13 ...	2025-01-23 ...	2024-10-13 ...	2025-01-	≡
☐	10.10.					337 Events	10 Indicators	2024-10-13 ...	2025-01-21 ...	2024-10-13 ...	2025-01-	≡
☐	10.10.					411 Events	16 Indicators	2024-10-13 ...	2025-01-19 ...	2024-10-13 ...	2025-01-	≡
☐	10.10.					1 Event	4 Indicators	2024-11-18 ...	2024-11-18 ...	2024-11-18 ...	2024-11-	≡
☐	10.10.					1 Event	4 Indicators	2024-11-18 ...	2024-11-18 ...	2024-11-18 ...	2024-11-	≡
☐	10.10.1.101					1 Event	4 Indicators	2024-11-04 ...	2024-11-04 ...	2024-11-04 ...	2024-11-	≡

ip = 10.10.1.114 at created +/- 5 minutes
ip = 10.10.1.114 at first seen +/- 5 minutes
ip = 10.10.1.114 at last seen +/- 5 minutes

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.



Investigation Results | vProbe_gig12 |

```
sensor_id = 'gig12'
```

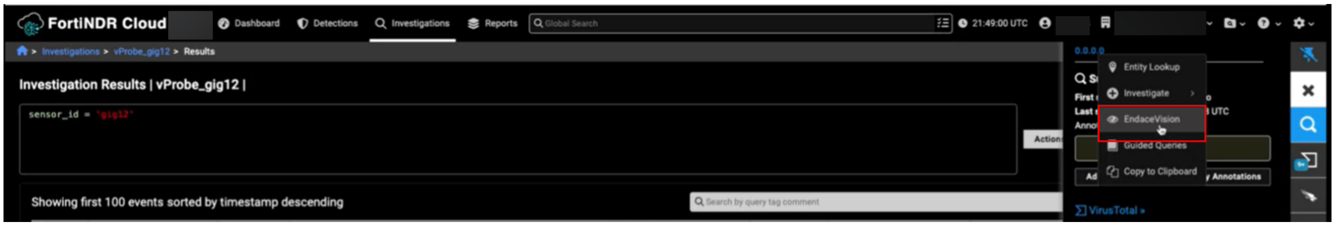
2025-01-16 17:03 (UTC) - 2025-01-16 18:03 (UTC)

Showing first 100 events sorted by timestamp descending

tag	timestamp	type	src	dst	intel	query	answers	application.name	sc
	2025-01-16 17:56:42 Z	DHCP	0.0.0.0:68	255.255.255.255:67	1 Hit				
	2025-01-16 17:56:41 Z	DNS	fe80::fe	ff02::fb:5353		_ipp._tcp.local			
	2025-01-16 17:56:25 Z	DHCP	0.0.	255.255.255.255:67	1 Hit				
	2025-01-16 17:56:25 Z	DNS	fe80::fe	ff02::fb:5353		_ipp._tcp.local			
	2025-01-16 17:56:17 Z	DHCP	0.0.	255.255.255.255:67	1 Hit				
	2025-01-16 17:56:14 Z	DNS	fe80::fe	ff02::fb:5353		_ipp._tcp.local	gti-qa-tgen.local +1 More		
	2025-01-16 17:56:13 Z	DNS	fe80::6	ff02::fb:5353		_smb._tcp.local	4 Values		
	2025-01-16 17:56:13 Z	FLOW	fe80::6	ff02::fb:5353					
	2025-01-16 17:56:13 Z	DHCP	0.0.	255.255.255.255:67	1 Hit				
	2025-01-16 17:56:12 Z	FLOW	fe80::fe	ff02::fb:5353					
	2025-01-16 17:56:12 Z	DNS	fe80::fe	ff02::fb:5353		_ipp._tcp.local	gti-qa-tgen.local +1 More		
	2025-01-16 17:56:10 Z	DHCP	0.0.	255.255.255.255:67	1 Hit				
	2025-01-16 17:55:56 Z	DHCP	0.0.0.0:68	255.255.255.255:67	1 Hit				

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

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



Investigation Results | vProbe_gig12 |

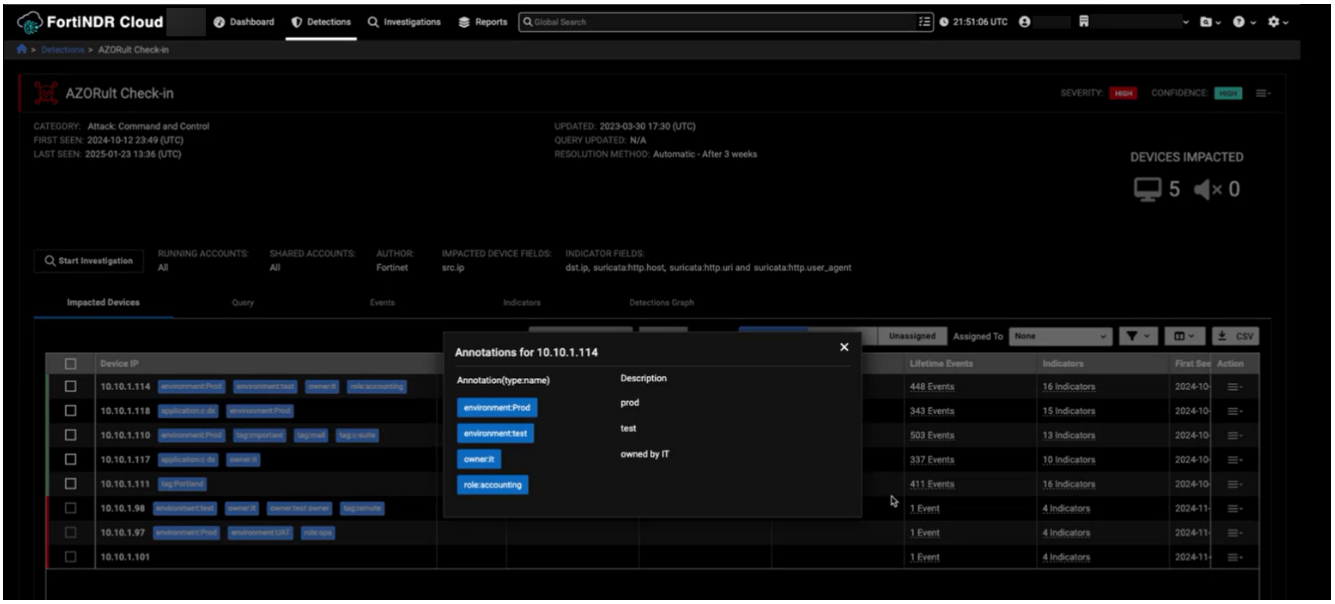
```
sensor_id = 'gig12'
```

Showing first 100 events sorted by timestamp descending

Investigations

Annotations

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



AZORult Check-in

SEVERITY: HIGH CONFIDENCE: HIGH

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

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

DEVICES IMPACTED 5 × 0

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

Annotations for 10.10.1.114

Annotation(type:name)	Description
environment:Prod	prod
environment:test	test
owner:it	owned by IT
role:accounting	

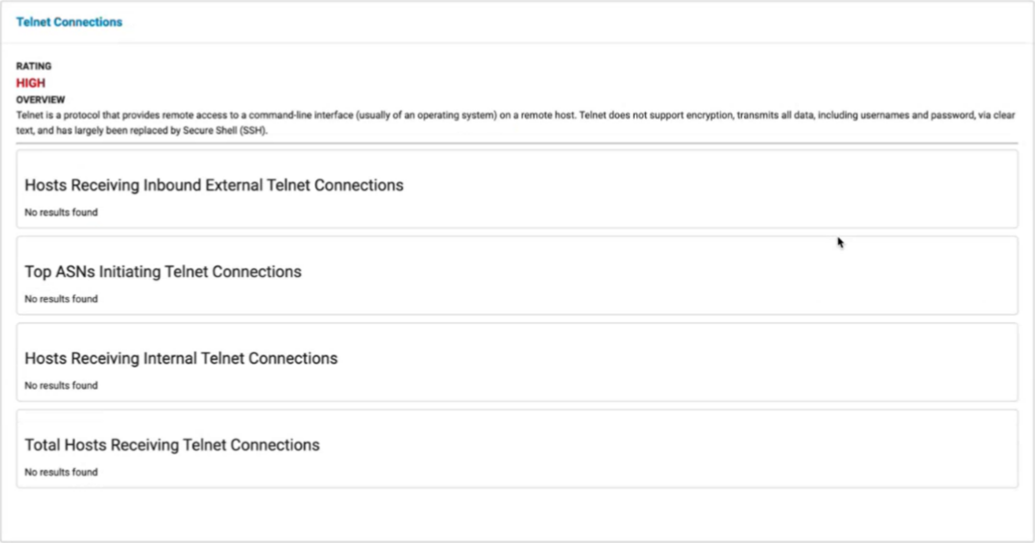
Device IP	Lifetime Events	Indicators	First See	Action
10.10.1.114 environment:Prod environment:test owner:it role:accounting	448 Events	16 Indicators	2024-10-	
10.10.1.118 application:c ds environment:Prod	343 Events	15 Indicators	2024-10-	
10.10.1.110 environment:Prod tag:important tag:mail tag:c-suite	503 Events	13 Indicators	2024-10-	
10.10.1.117 application:c ds owner:it	337 Events	10 Indicators	2024-10-	
10.10.1.111 tag:Portland	411 Events	16 Indicators	2024-10-	
10.10.1.98 environment:test owner:it owner:test owner tag:remote	1 Event	4 Indicators	2024-11-	
10.10.1.97 environment:Prod environment:UAT role:ops	1 Event	4 Indicators	2024-11-	
10.10.1.101	1 Event	4 Indicators	2024-11-	

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.



Telnet Connections

RATING

HIGH

OVERVIEW

Telnet is a protocol that provides remote access to a command-line interface (usually of an operating system) on a remote host. Telnet does not support encryption, transmits all data, including usernames and password, via clear text, and has largely been replaced by Secure Shell (SSH).

Hosts Receiving Inbound External Telnet Connections

No results found

Top ASNs Initiating Telnet Connections

No results found

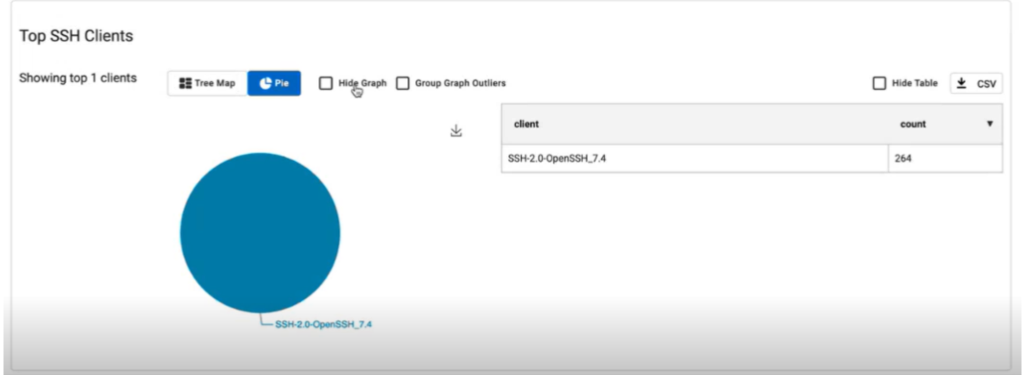
Hosts Receiving Internal Telnet Connections

No results found

Total Hosts Receiving Telnet Connections

No results found

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

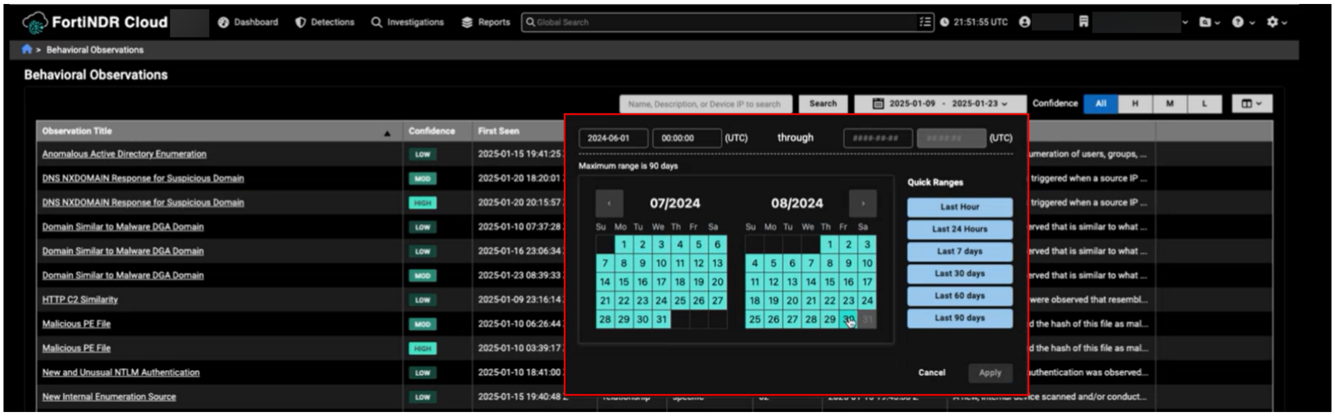


client	count
SSH-2.0-OpenSSH_7.4	264

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 availble in the *Observation Details* page.



Behavioral Observations

2024-06-01 00:00:00 (UTC) through ####-##-## ##:##:## (UTC)

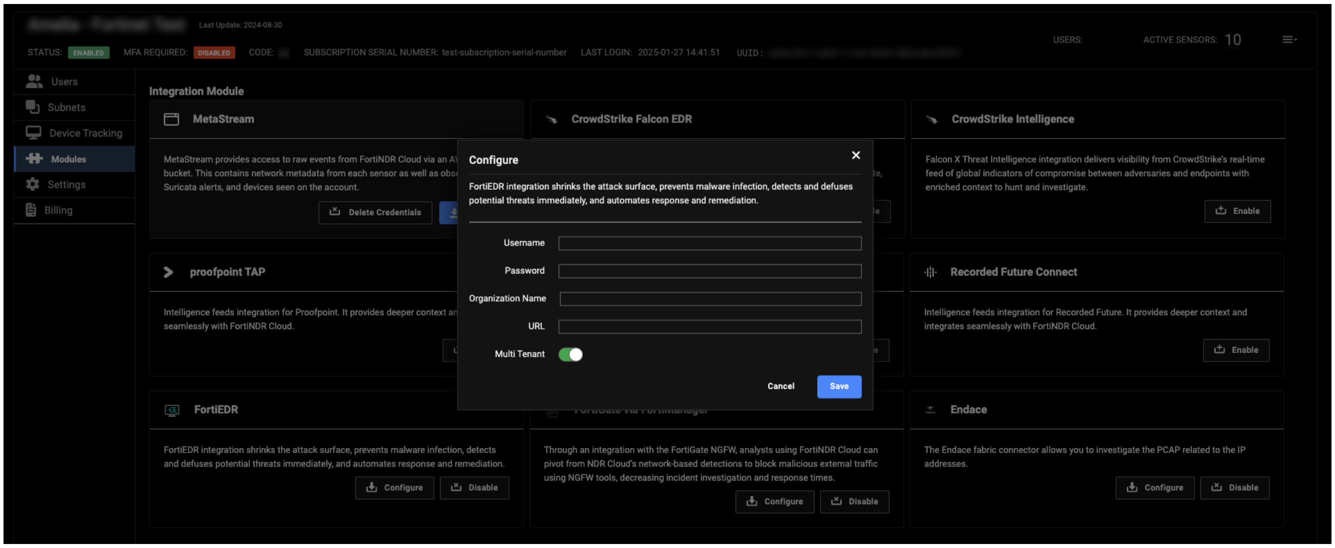
Maximum range is 90 days

Observation Title	Confidence	First Seen	
Anomalous Active Directory Enumeration	LOW	2025-01-15 19:41:25	umeration of users, groups, ...
DNS NXDOMAIN Response for Suspicious Domain	MOD	2025-01-20 18:20:01	triggered when a source IP ...
DNS NXDOMAIN Response for Suspicious Domain	HIGH	2025-01-20 20:15:57	triggered when a source IP ...
Domain Similar to Malware DGA Domain	LOW	2025-01-10 07:37:28	erved that is similar to what ...
Domain Similar to Malware DGA Domain	LOW	2025-01-16 23:06:34	erved that is similar to what ...
Domain Similar to Malware DGA Domain	MOD	2025-01-23 08:39:33	erved that is similar to what ...
HTTP C2 Similarity	LOW	2025-01-09 23:16:14	were observed that resembl...
Malicious PE File	MOD	2025-01-10 06:26:44	d the hash of this file as mal...
Malicious PE File	HIGH	2025-01-10 03:39:17	d the hash of this file as mal...
New and Unusual NTLM Authentication	LOW	2025-01-10 18:41:00	uthentication was observed...
New Internal Enumeration Source	LOW	2025-01-15 19:40:48	ce scanned and/or conduct...

Integrations

FortiEDR

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



MetaStream provides access to raw events from FortiNDR Cloud via an A… bucket. This contains network metadata from each sensor as well as obs… Suricata alerts, and devices seen on the account.

Falcon X Threat Intelligence integration delivers visibility from CrowdStrike's real-time feed of global indicators of compromise between adversaries and endpoints with enriched context to hunt and investigate.

Intelligence feeds integration for Proofpoint. It provides deeper context a… seamlessly with FortiNDR Cloud.

Intelligence feeds integration for Recorded Future. It provides deeper context and integrates seamlessly with FortiNDR Cloud.

FortiEDR integration shrinks the attack surface, prevents malware infection, detects and defuses potential threats immediately, and automates response and remediation.

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.

The Endace fabric connector allows you to investigate the PCAP related to the IP addresses.

Configure ✕

FortiEDR integration shrinks the attack surface, prevents malware infection, detects and defuses potential threats immediately, and automates response and remediation.

Username

Password

Organization Name

URL

Multi Tenant ●

Cancel Save

Other improvements

Tooltips

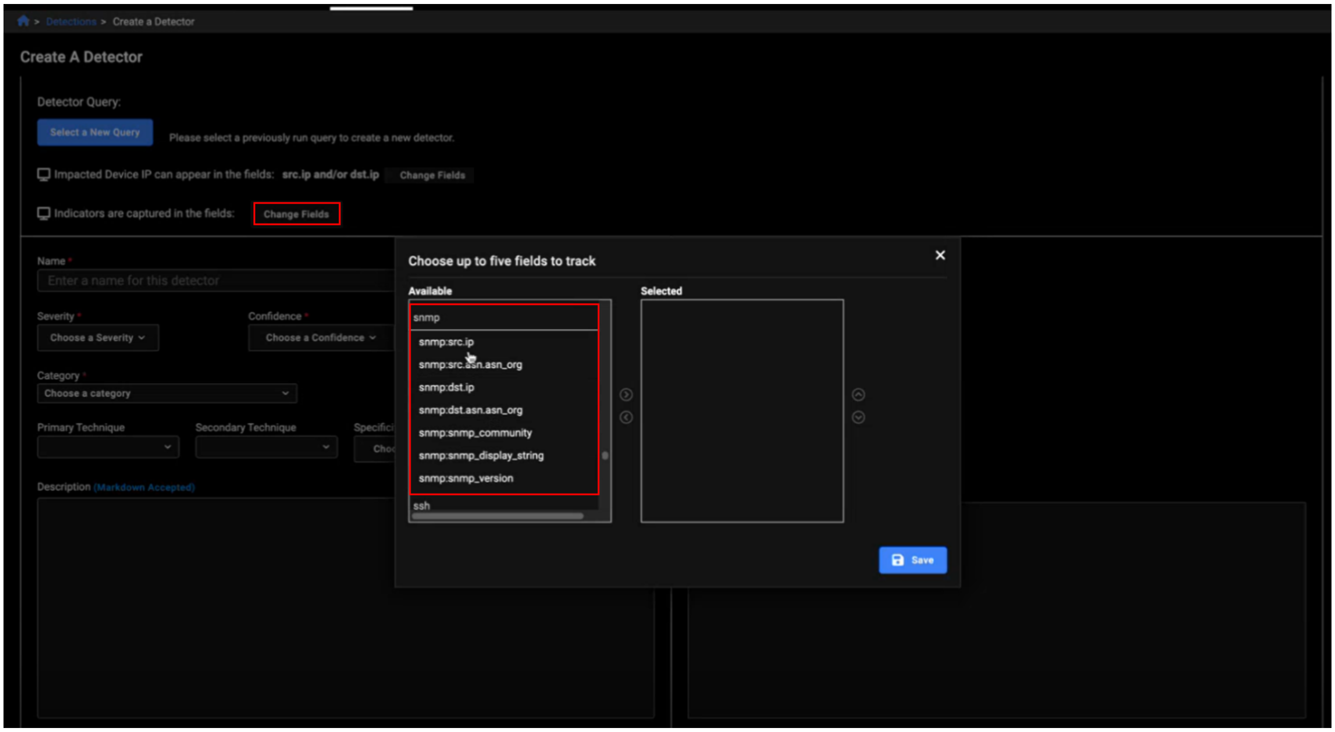
- The chart tooltips have been redesigned to make them easier to read.
- A scroll bar was added to longer tooltips allowing the information to fit the page.
- The *Throughput* tooltip in the *Sensors* widget now shows the time when you hover over a data point.

Version 25.1.0

New functionality

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.



Please select a previously run query to create a new detector.

Impacted Device IP can appear in the fields: src.ip and/or dst.ip

Indicators are captured in the fields:

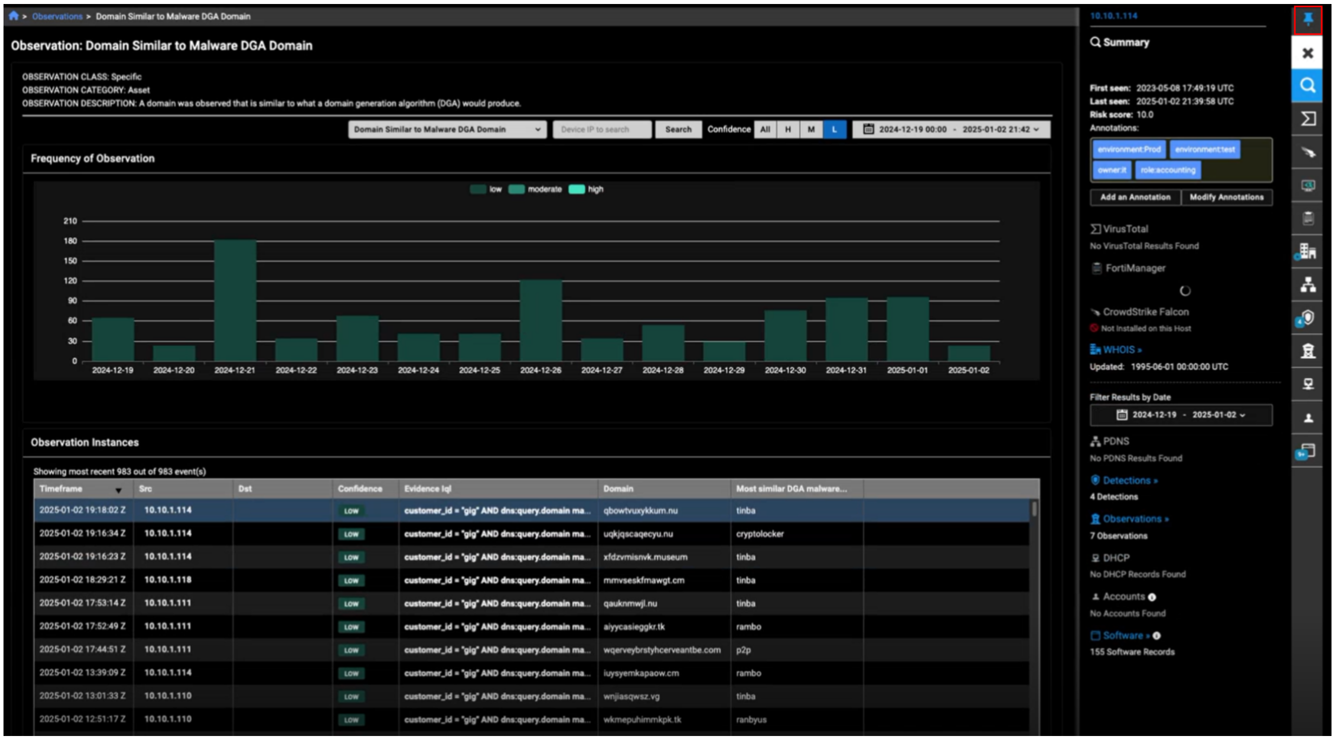
Choose up to five fields to track

snmp

- snmp:src.ip
- snmp:src.asn.asn_org
- snmp:dst.ip
- snmp:dst.asn.asn_org
- snmp:snmp_community
- snmp:snmp_display_string
- snmp:snmp_version
- ssh

Entity Panel

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



Observation: Domain Similar to Malware DGA Domain

OBSERVATION CLASS: Specific
OBSERVATION CATEGORY: Asset
OBSERVATION DESCRIPTION: A domain was observed that is similar to what a domain generation algorithm (DGA) would produce.

Observation Instances

Showing most recent 983 out of 983 event(s)

Timeframe	Src	Dst	Confidence	Evidence Iql	Domain	Most similar DGA malware...
2025-01-02 19:18:02 Z	10.10.1.114		LOW	customer_id = "gig" AND dns:query.domain ma...	qbowtvuxykkum.nu	tinba
2025-01-02 19:16:34 Z	10.10.1.114		LOW	customer_id = "gig" AND dns:query.domain ma...	uqkjqscaqecyu.nu	cryptolocker
2025-01-02 19:16:23 Z	10.10.1.114		LOW	customer_id = "gig" AND dns:query.domain ma...	xfdzvmisnvk.museum	tinba
2025-01-02 18:29:21 Z	10.10.1.118		LOW	customer_id = "gig" AND dns:query.domain ma...	mmvseskfmawgt.cm	tinba
2025-01-02 17:53:14 Z	10.10.1.111		LOW	customer_id = "gig" AND dns:query.domain ma...	qauknmwjl.nu	tinba
2025-01-02 17:52:49 Z	10.10.1.111		LOW	customer_id = "gig" AND dns:query.domain ma...	aiyycasieggkr.tk	rambo
2025-01-02 17:44:51 Z	10.10.1.111		LOW	customer_id = "gig" AND dns:query.domain ma...	wqerveybrstyhcerveantbe.com	p2p
2025-01-02 13:39:09 Z	10.10.1.114		LOW	customer_id = "gig" AND dns:query.domain ma...	iuysyemkapaow.cm	rambo
2025-01-02 13:01:33 Z	10.10.1.110		LOW	customer_id = "gig" AND dns:query.domain ma...	wnjiasqwsz.vg	tinba
2025-01-02 12:51:17 Z	10.10.1.110		LOW	customer_id = "gig" AND dns:query.domain ma...	wkmepuhimmkpk.tk	ranbyus

10.10.1.114

Summary

First seen: 2023-05-08 17:49:19 UTC
Last seen: 2025-01-02 21:39:58 UTC
Risk score: 10.0
Annotations: environment:Prod environment:test owner:it role:accounting

VirusTotal
No VirusTotal Results Found

FortiManager

CrowdStrike Falcon
Not Installed on this Host

WHOIS »
Updated: 1995-06-01 00:00:00 UTC

Filter Results by Date
2024-12-19 - 2025-01-02

PDNS
No PDNS Results Found

Detections »
4 Detections

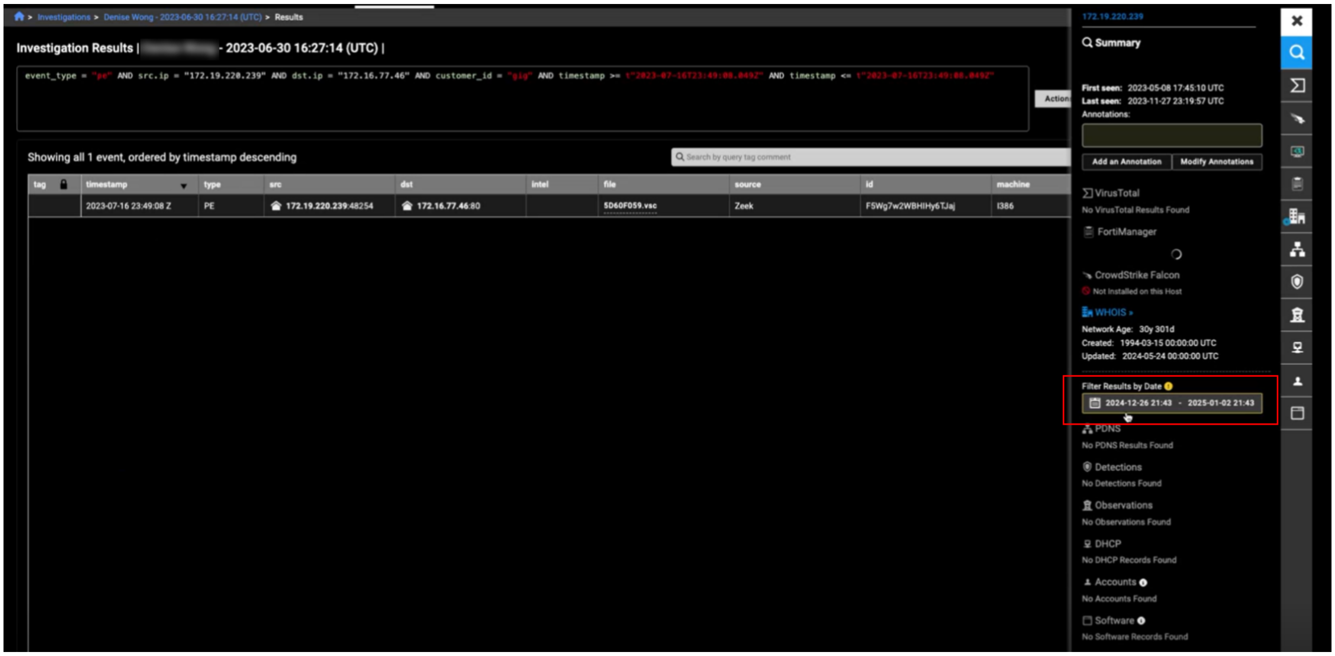
Observations »
7 Observations

DHCP
No DHCP Records Found

Accounts
No Accounts Found

Software »
155 Software Records

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.



Investigations > Denise Wong - 2023-06-30 16:27:14 (UTC) > Results

Investigation Results | [redacted] - 2023-06-30 16:27:14 (UTC) |

```
event_type = "pe" AND src.ip = "172.19.220.239" AND dst.ip = "172.16.77.46" AND customer_id = "gig" AND timestamp >= t"[illegible]" AND timestamp <= t"[illegible]"
```

Action
Search by query tag comment

Showing all 1 event, ordered by timestamp descending

tag	timestamp	type	src	dst	intel	file	source	id	machine
	2023-07-16 23:49:08 Z	PE	172.19.220.239:48254	172.16.77.46:80		5D60F059.vsc	Zeek	F5Wg7w2WBHIHy6TJaj	I386

172.19.220.239

Summary

First seen: 2023-05-08 17:45:10 UTC
Last seen: 2023-11-27 23:19:57 UTC
Annotations:

VirusTotal
No VirusTotal Results Found

FortiManager

CrowdStrike Falcon
Not Installed on this Host

WHOIS »
Network Age: 30y 301d
Created: 1994-03-15 00:00:00 UTC
Updated: 2024-05-24 00:00:00 UTC

Filter Results by Date
2024-12-26 21:43 - 2025-01-02 21:43

PDNS
No PDNS Results Found

Detections
No Detections Found

Observations
No Observations Found

DHCP
No DHCP Records Found

Accounts
No Accounts Found

Software
No Software Records Found

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.

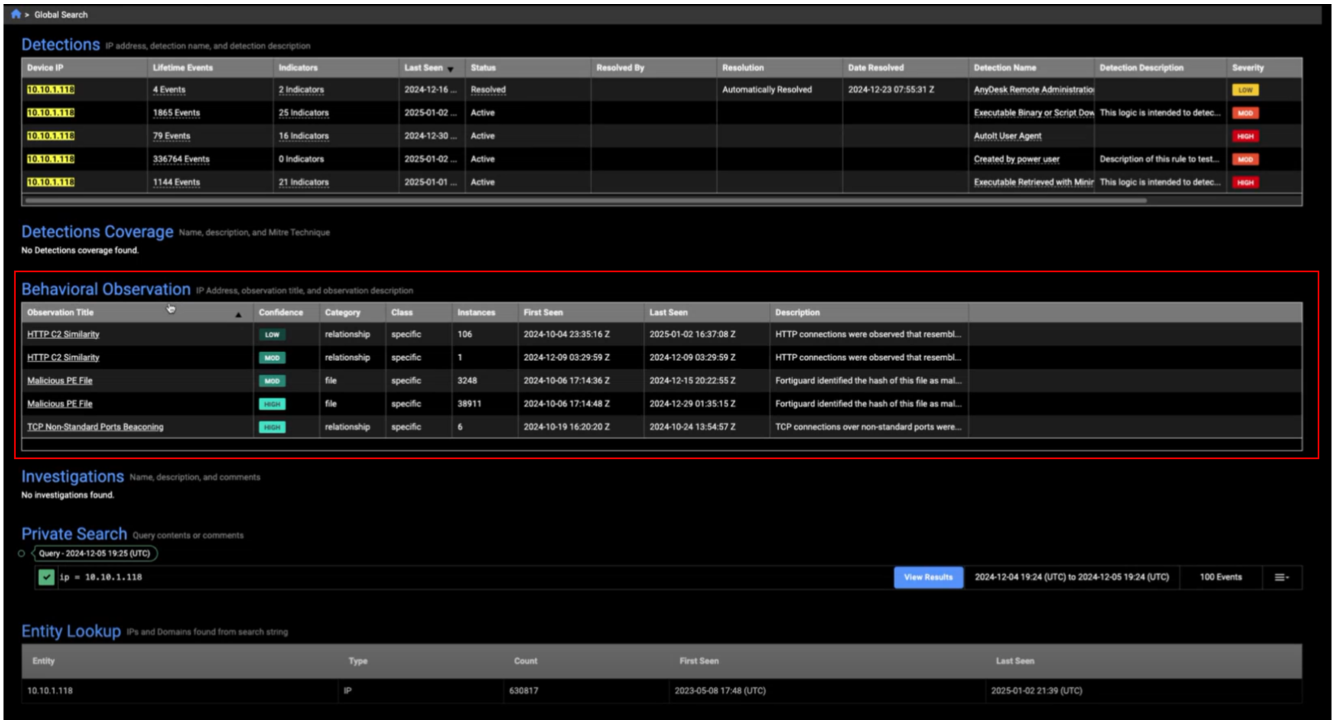
A timestamp is displayed for detections within the current year in the *Entity Panel*. Detections that are more than a year old, appear as *More than a year ago*.

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.



Detections IP address, detection name, and detection description

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

Detections Coverage Name, description, and Mitre Technique

No Detections coverage found.

Behavioral Observation IP Address, observation title, and observation description

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

Investigations Name, description, and comments

No investigations found.

Private Search Query contents or comments

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

```
ip = 10.10.1.118
```

2024-12-04 19:24 (UTC) to 2024-12-05 19:24 (UTC) 100 Events

Entity Lookup IPs and Domains found from search string

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

Other improvements

- We have a 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.

25.4.0

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.

Description
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.

Description
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 e in the *Entity Panel*
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*.

FORTINET®

www.fortinet.com