FORTINET

Release Notes

FortiNDR Cloud 26.1.b

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

March 25, 2026
FortiNDR Cloud 26.1.b Release Notes
78-261-1243236-20260325

TABLE OF CONTENTS

FortiNDR Cloud release notes **4**
Version history **5**
Version 26.1.b 5
New functionality 5
Improved functionality 8
Other improvements 11
Deprecated features 11
Version 26.1.a 12
New functionality 12
Improved functionality 18
Other improvements 20
Version 26.1.0 21
Improved functionality 21
Other improvements 22
Product integration and support **23**
Integrations 23
Fortinet Automation Service 24
Resolved issues **25**
26.1.b 25
26.1.a 25
26.1.0 26
Known issues **27**
25.4.a 27

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
25 March 2026	Version 26.1.b on page 5
11 February 2026	Version 26.1.a on page 12
12 January 2026	Version 26.1.0 on page 21

Version 26.1.b

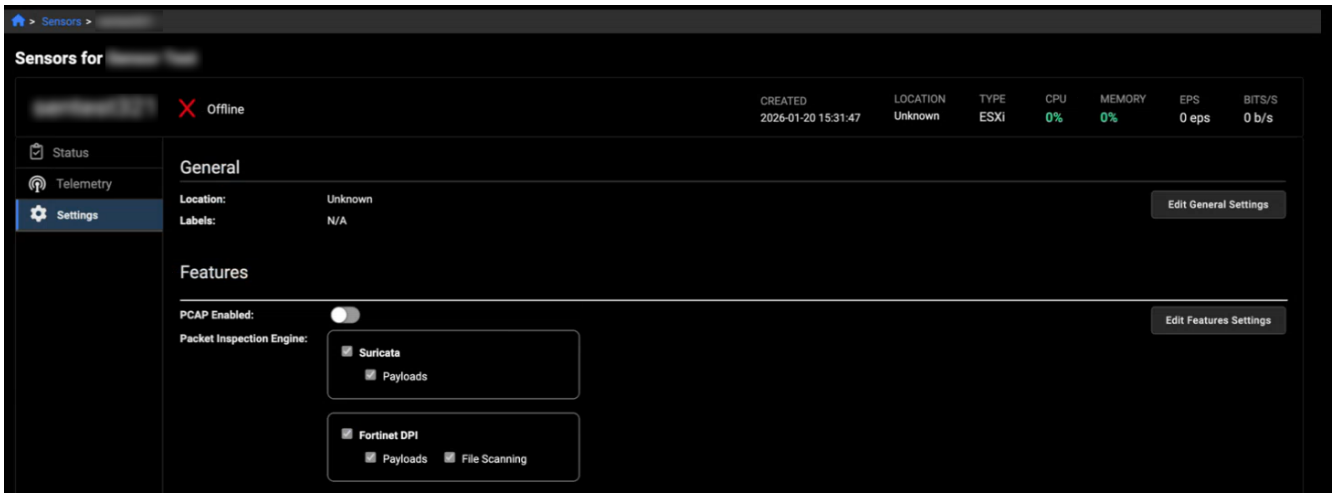
- New functionality
  - DPI Payload
  - Detections details page
- Improved functionality
  - Manage annotations
  - Entity panel
  - Detections
- Other improvements
- Deprecated features
- Resolved issues on page 25

Left navigation is now the default layout in the FortiNDR Cloud portal.

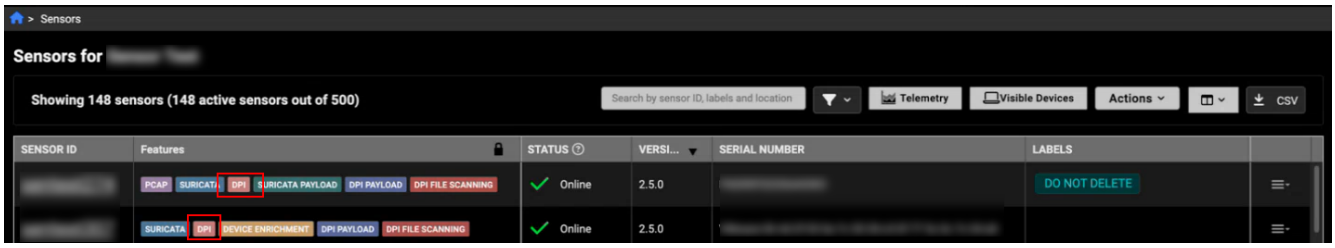
New functionality

DPI Payload

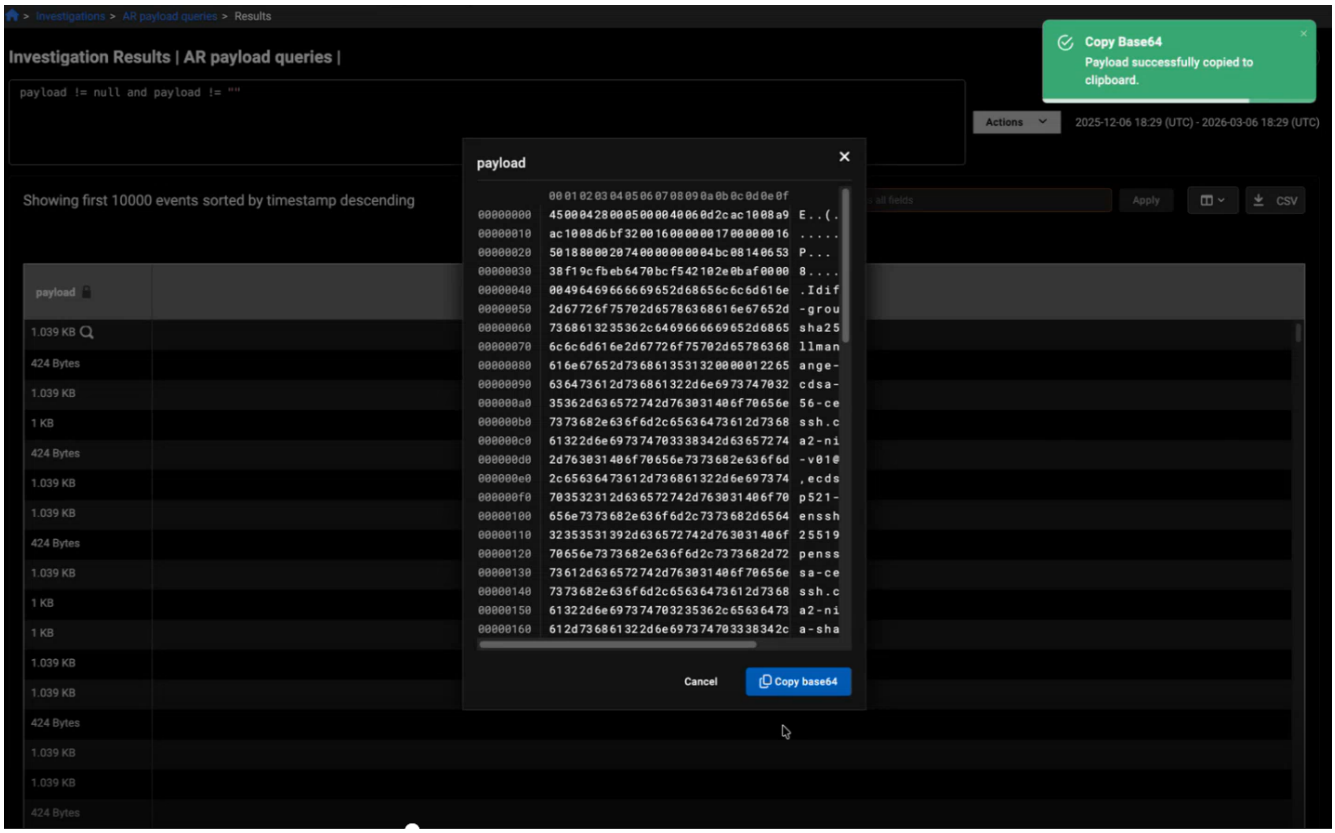
DPI payload capability is now available for sensors running version 2.5.0 or later. This ASCII representation helps determine whether traffic is malicious or benign. In the *Sensor Details* page, the *Packet Inspection Engine* settings now include additional options for *DPI Payloads* and *DPI File Scanning*.



When these features are enabled, they appear in the *Features* column of the sensor list, allowing you to quickly see whether payload inspection or file scanning is active without opening the full sensor configuration.



A new *Payload* field has also been added to the investigation results.

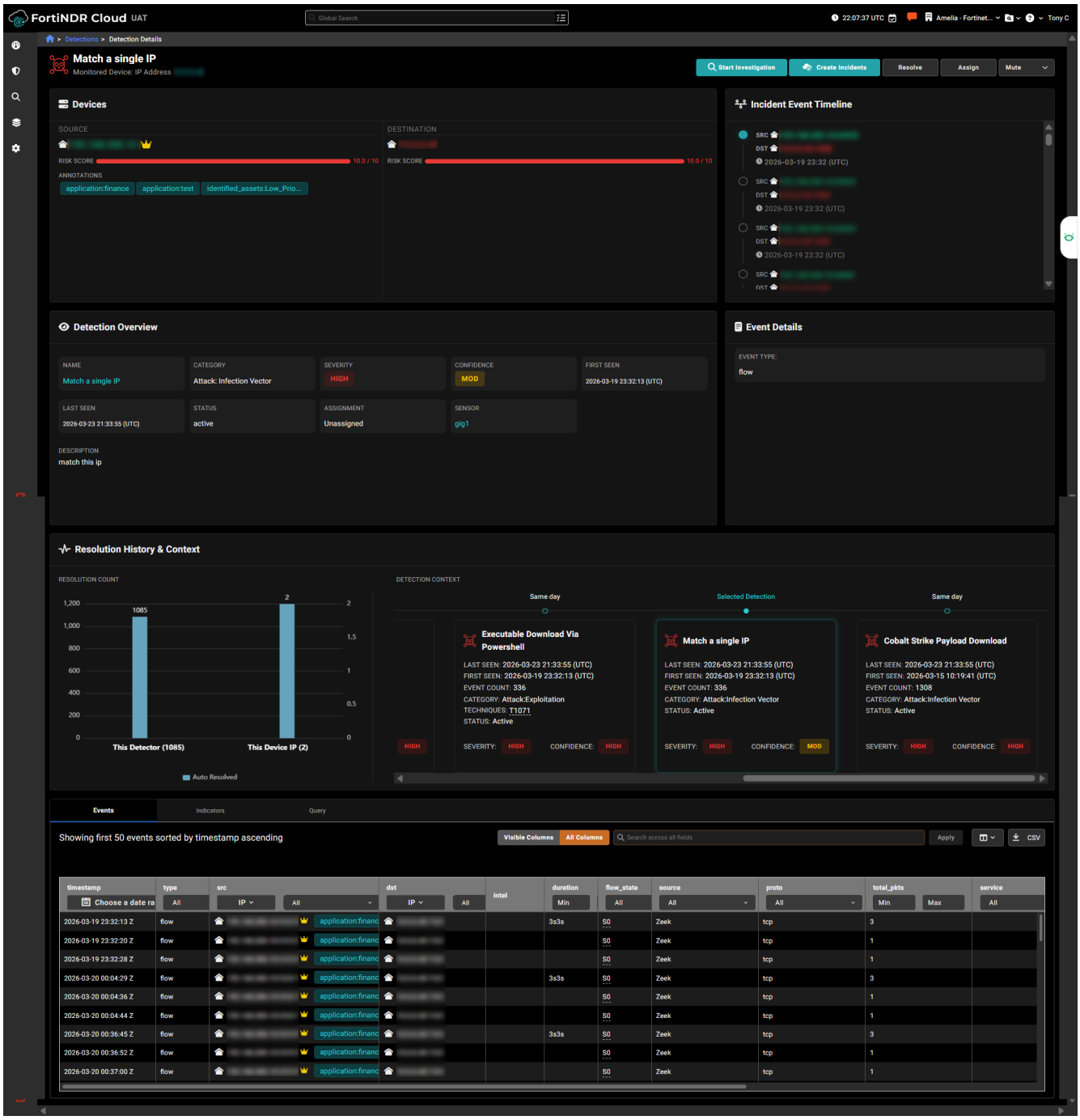


Detections details

The new *Detection Details* page now provides a consolidated, in-depth overview of an individual detection. To access the page from the *Detections table*, click a row or select the *See Detection Details* icon. This updated view brings together all essential information, including source and destination IPs, event timelines, resolution history, detection context, and related events.

The improved layout also highlights related detections to help you quickly identify recurring issues, while clearly presenting event information for observation-based detections. This unified view eliminates the need to navigate across multiple pages.

A new Create Incidents feature is available in the Detection Details page and related views starting in version 26.1.b. This feature requires an active Fortinet Automation Service subscription. Customers with an active subscription can access the feature in the forthcoming Service Pack 1.0.3 release, which will include support for ServiceNow and Jira connectors and their associated playbooks.

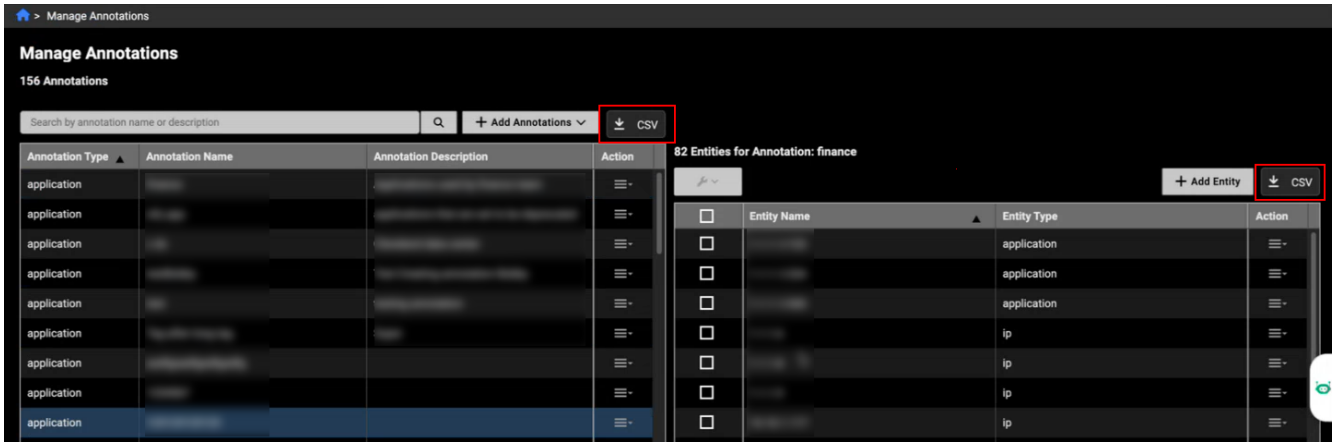


Improved functionality

Manage annotations

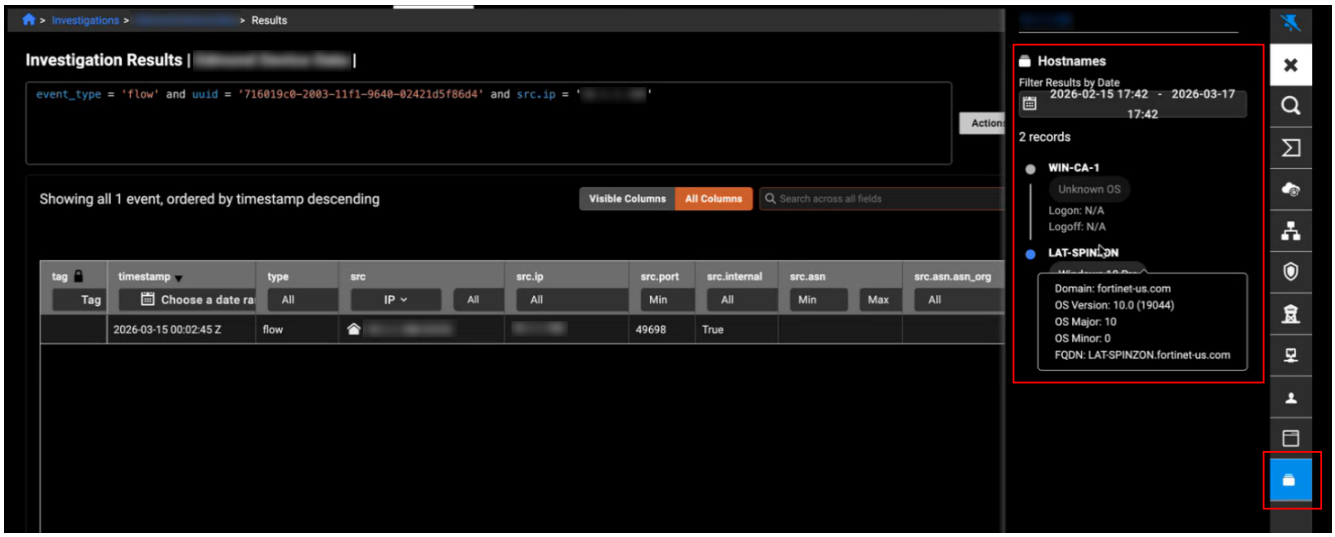
A new CSV download option has been added to the *Manage Annotations* page, providing download buttons for both the Annotations and Entities table. The downloaded file uses the same structure required for uploads,

allowing users to make changes directly in the CSV and then re-upload it without needing to adjust the format. This enhancement streamlines the edit-and-upload workflow and ensures the exported data is immediately ready for reuse.



Entity panel

A new *Hostnames* tab has been added to the *Entity Panel* to display device enrichment data. This tab shows enrichment fields received from event records, including details such as OS name, OS major and minor versions, and any available login or logout timestamps. Where applicable, the data is presented in chronological order, providing clearer visibility into host-level enrichment information directly within the entity view.



Detections

We have introduced a new *gallery* view and a *table* view to the *Detections Triage* page. The updated view includes additional fields to provide more information at a glance. All standard table operations remain available, and selecting a detector still takes you to the detector details page.

Gallery View is the default layout for displaying detections. It presents each detection as a card in a grid, showing key information such as the detection name, severity, category, last-seen time, and impacted devices. This view makes it easy to scan multiple detections quickly and identify the most important items at a glance.

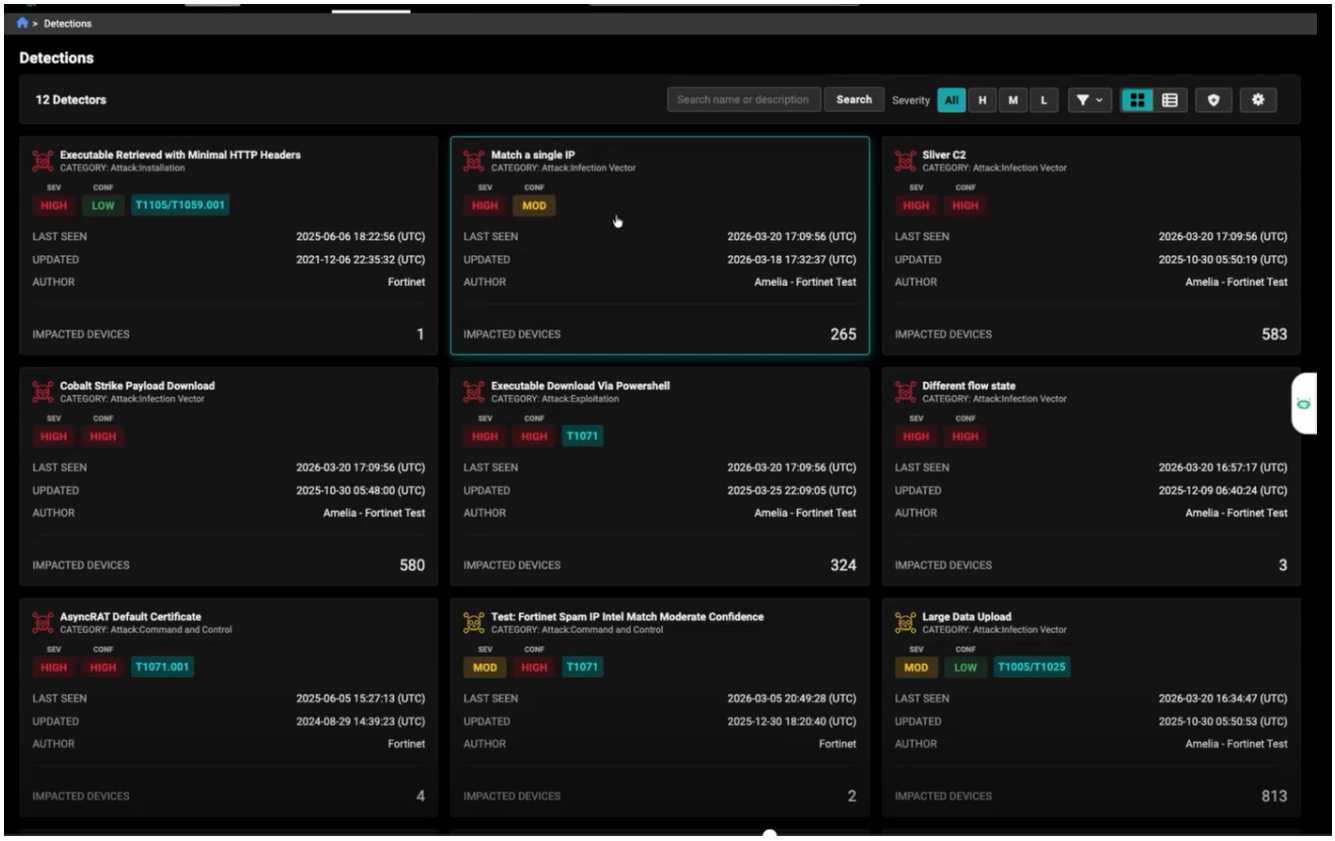
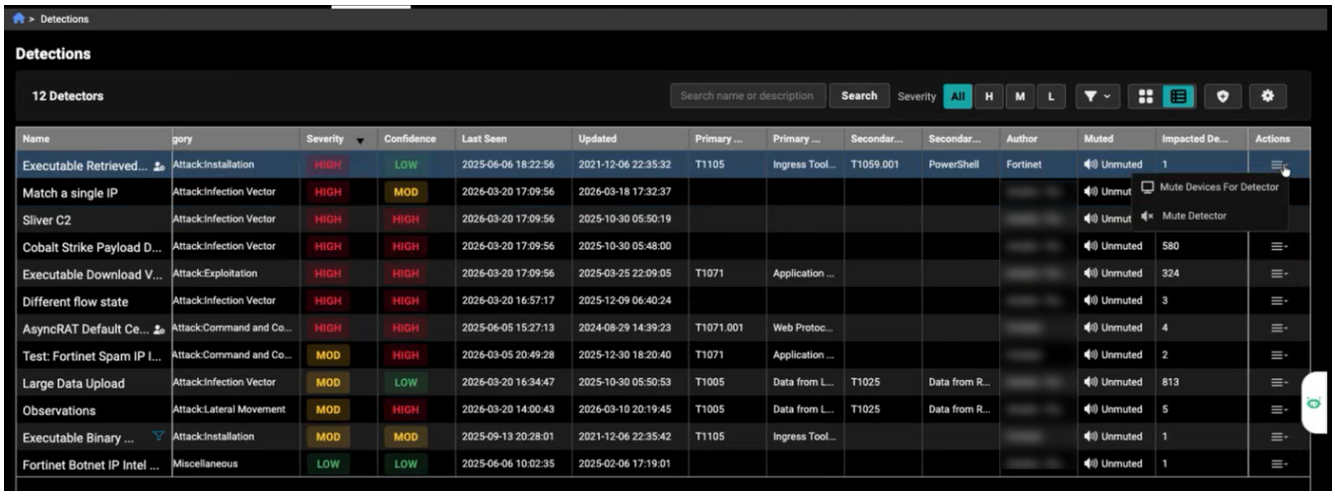
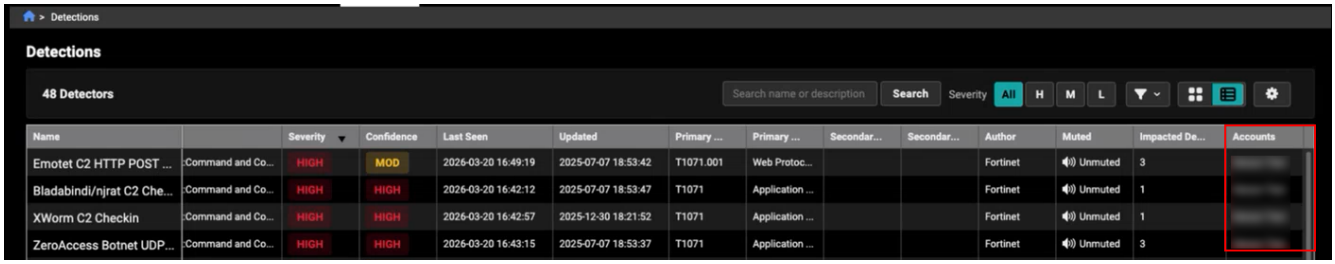


Table View presents detections in a compact, row-and-column format for easier sorting and comparison. Each detection appears as a single row with detailed fields such as name, category, severity, confidence, timestamps, author, mute status, and impacted devices. This view is useful when you need to quickly scan large amounts of data, sort by specific columns, or perform detailed analysis across multiple detections.



The new *Accounts* column displays all the accounts a detector is running on whenever you are viewing detectors in the *All Accounts* view. For detectors that run on a single account, the column shows that account

name. When a detector runs across multiple accounts, hovering over the value opens a tooltip listing all associated accounts. This provides quick visibility into detector coverage without leaving the table. A new *Exclude Accounts* filter has also been added.



Other improvements

- Enhanced *Critical Assets Identification* by adding support for detecting internal proxy servers. The system now automatically identifies and groups internal proxy server assets for easier tracking and investigation. Priority levels are assigned based on activity, with High Priority given when a proxy server is contacted by many distinct source IPs and Moderate Priority otherwise.
- The *Subnets* tab in the *Mutes and Excludes* has been updated to include a sorting option on this field.
- The *Detections*, *Detections Table*, and *Investigations* pages now support the *This Quarter* and *Last Quarter* time range filters.
- The Sensor *Telemetry* graph has been updated for clarity. Days with no data now appear in the legend and are plotted as zero, resulting in the graph line dropping before continuing to the next data point.
- The aggregation table in the query results now supports CSV download regardless of the number of columns included in an NL-based query.
- NL query results now display the correct count of aggregation results. When an NL query returns only aggregated data, the GUI shows the total number of aggregated records instead of a generic placeholder. For example, if the query produces 16 aggregated entries, the interface now displays *16 results* and lists all 16 records in the results table.
- The *Observation Context* in the *Events* table has been redesigned from a list into a set of compact cards, making each key–value pair easier to read.
- The license page now supports entries with Month/Day/Year start and end dates.

Deprecated features

- The *Detections Graph* has been removed from the *Detection Details* page.

Version 26.1.a

- New functionality
  - Advanced filtering for Investigation and Detection Event Tables
  - Device Count Deviation Alert
  - Left navigation
  - Customizable detection resolution methods
  - VPC Flow fields
- Improved functionality
  - Report filtering
  - Natural language query enhancements
  - Device enrichment configuration
  - Netflow event fields
  - FortiAI updates and improvements
- Other improvements
- Resolved issues on page 25

New functionality

Advanced filtering for Investigation and Detection Event Tables

We have enhanced the overall filtering experience across investigation and detection tables by adding column-level filters, keyword search options, clearer visibility into active filters, and automatic row-count updates.

This enhancement improves the analyst experience by enabling fast, interactive filtering directly within result tables across the portal. Previously, analysts had limited options for narrowing large result sets and often needed to run additional queries (for example, filtering again by source IP, server name, or event type such as flow events). This led to repeated follow-up queries, slowed investigations, and made it more difficult to quickly focus on relevant data.

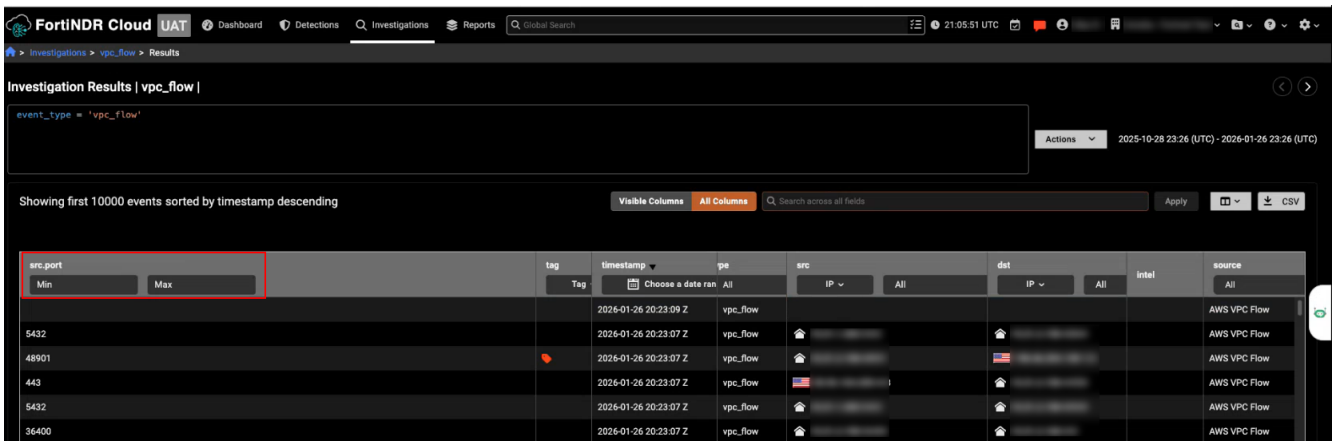
Column-level filters

We have added column-level filtering to Investigation Events tables, providing more precise and flexible ways to explore and narrow down event data directly within the table. This update makes it easier to quickly isolate relevant events and combine multiple criteria without leaving the table.

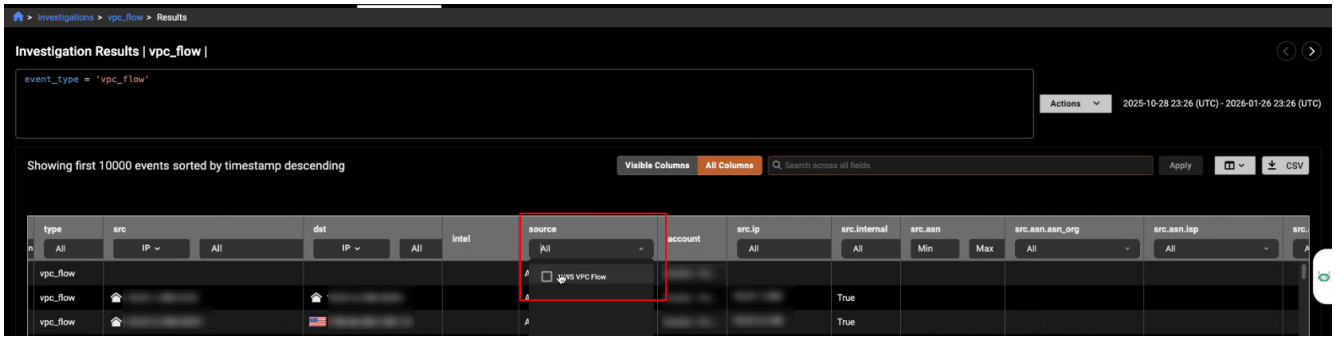
This enhancement is available anywhere the investigation *Events* table is used, including support for granular filters by column type, with filtering enabled for approximately 90% of columns based on their data type.

You can apply multiple column filters at the same time to progressively narrow the results. As filters change, the table automatically updates its row count to show how many rows are currently displayed compared to the total number of available events.

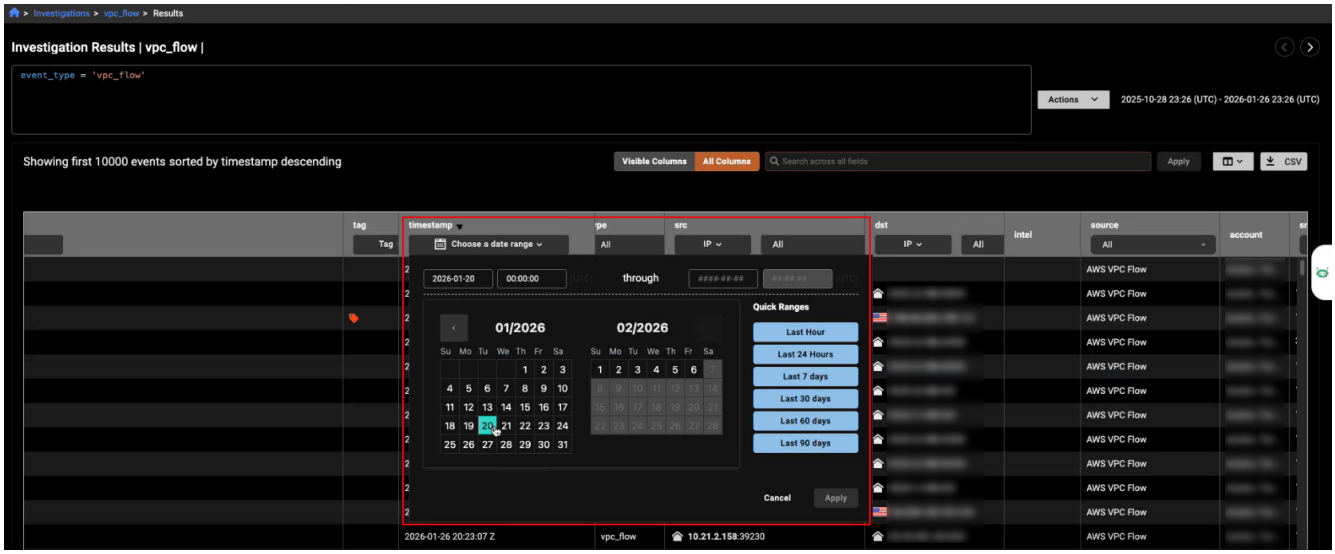
Numeric columns support filtering by minimum and or maximum values, making it easy to narrow results for fields such as ports or other numeric attributes.



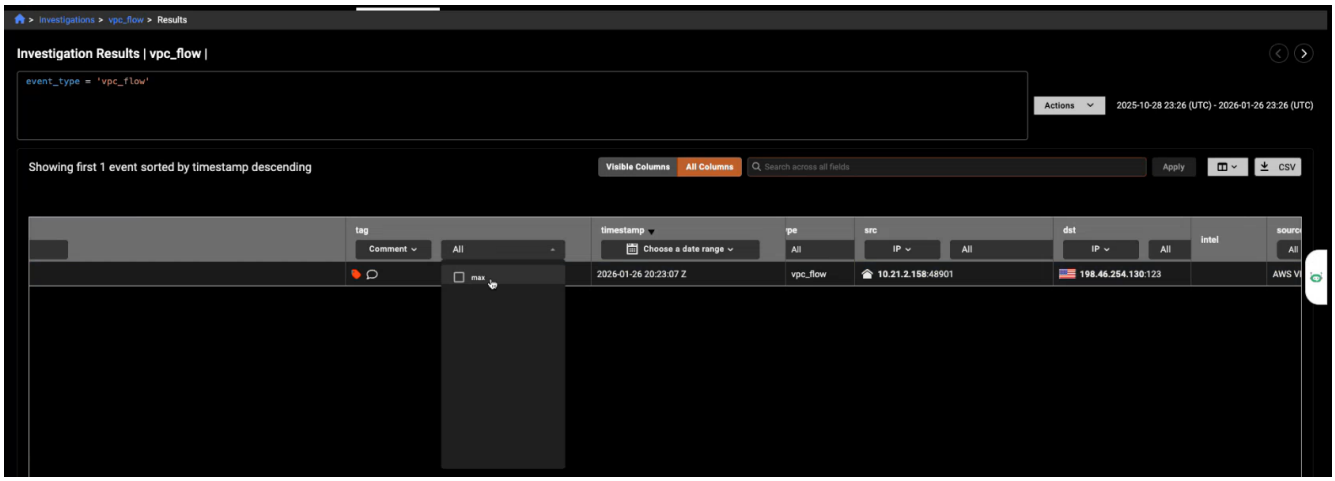
Text and string columns support filtering through a multi-select dropdown that lists all available values in the column, allowing you to select one or more values to refine the results.



Date and time columns can be filtered using a date range picker, where you select a start and end time to display only events that fall within the specified range.

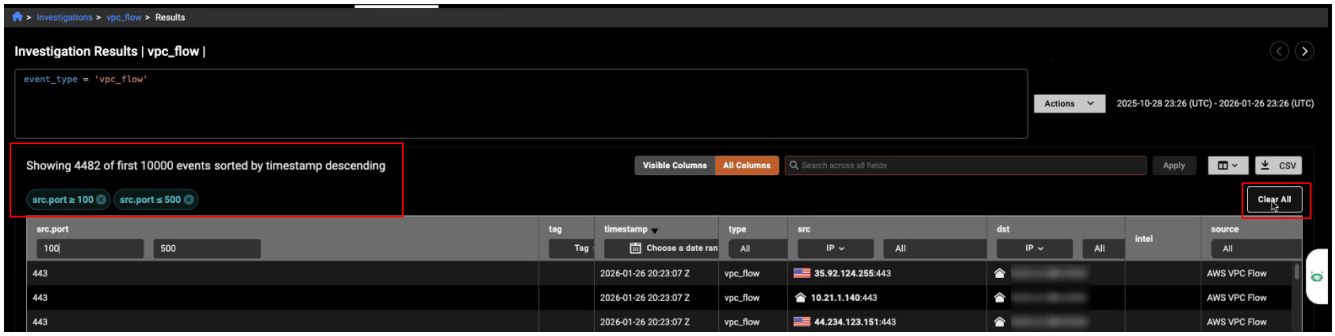


The *Tag* column filter provides two fields, allowing you to filter events either by tag type or by comment, with the filter automatically switching to the appropriate field based on your selection.



The table automatically updates its row count as filters change, showing how many rows are currently displayed compared to the total available events so you can see.

Active filters are displayed as filter pills above the table that indicate which columns are filtered and the selected values. You can remove individual filters by clicking their pill or clear all filters at once using *Clear all*.



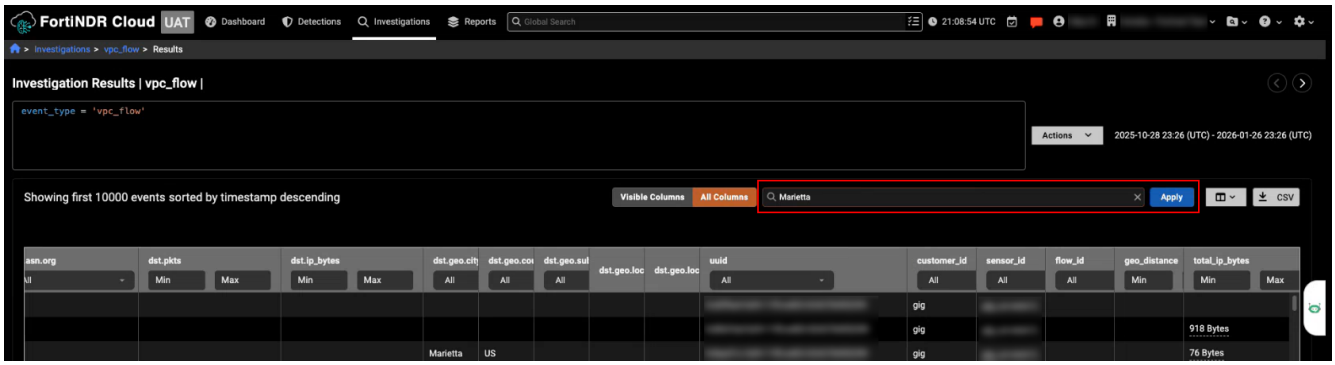
Keyword search

We have added a keyword filter to the following tables: Detection details (Events tab), Investigation query results, and Private search results. You can filter by *All columns* (including hidden columns) or *Visible columns* (only those currently displayed).

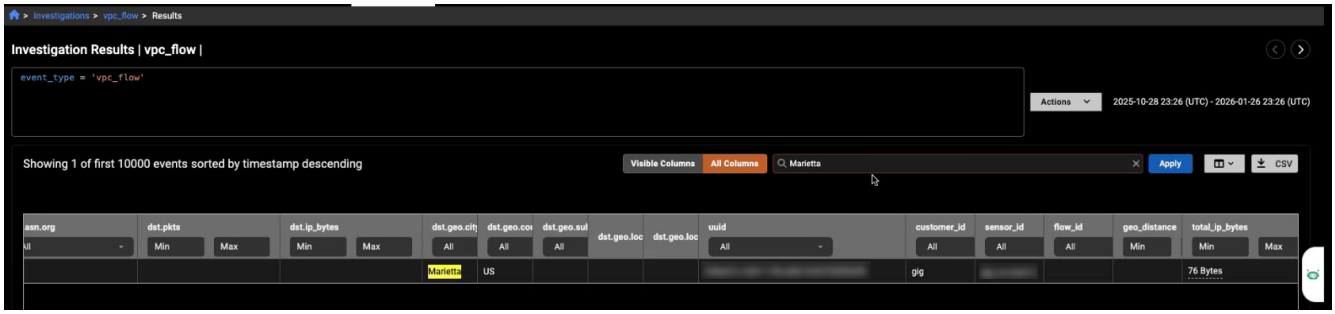
Filtering applies only to the results visible in the table:

- Detection events: up to 1,000 records
- Investigation and Private search results: up to 10,000 records

You can use the *Search* field to filter the events. You are required to hit *Enter* or click *Apply* to start the search.



The results show only the rows that meet the search criteria. When *All Columns* is enabled, hidden columns are included in the results. The yellow highlight shows text that matches the underlying data for that column. Some values shown on the screen are formatted to be easier to read, so they may look different from the actual value used by the system. Searches always check against that underlying value, not the formatted display.

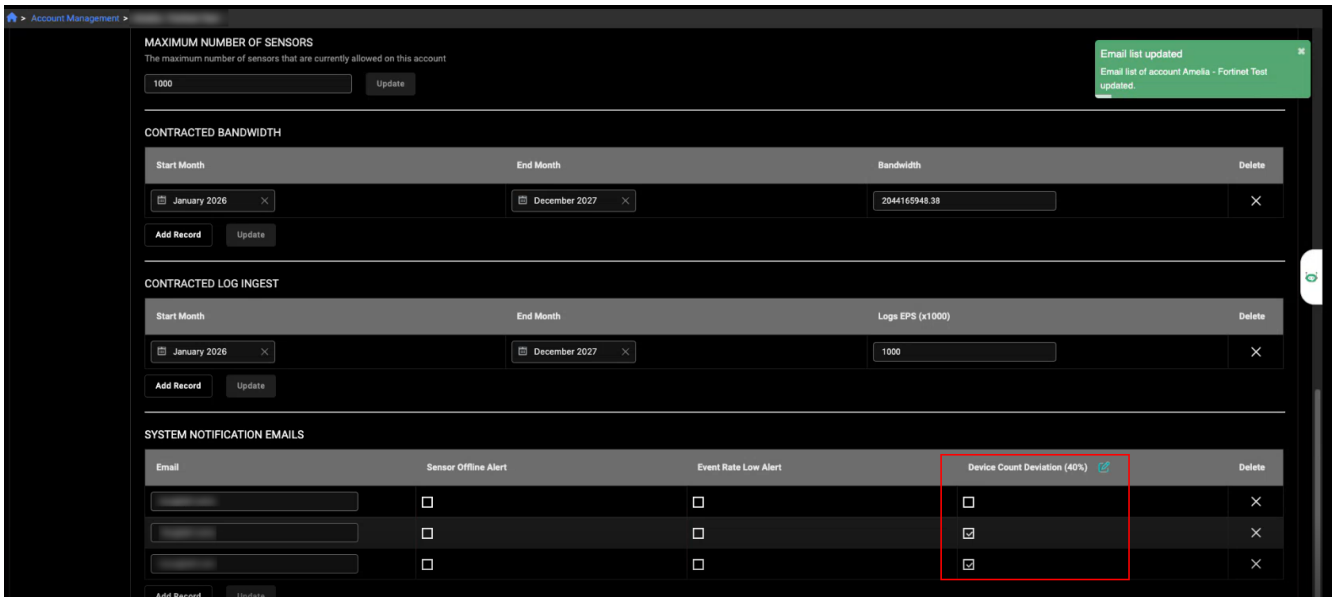


Device count deviation alert

The new *Device Count Deviation* alert notifies you when a sensor suddenly detects fewer internal devices than expected, providing a new layer of sensor health monitoring beyond event rate and offline alerts. This alert improves visibility into situations where a sensor appears “alive” but is detecting fewer devices than normal. A decrease in internal device visibility often indicates:

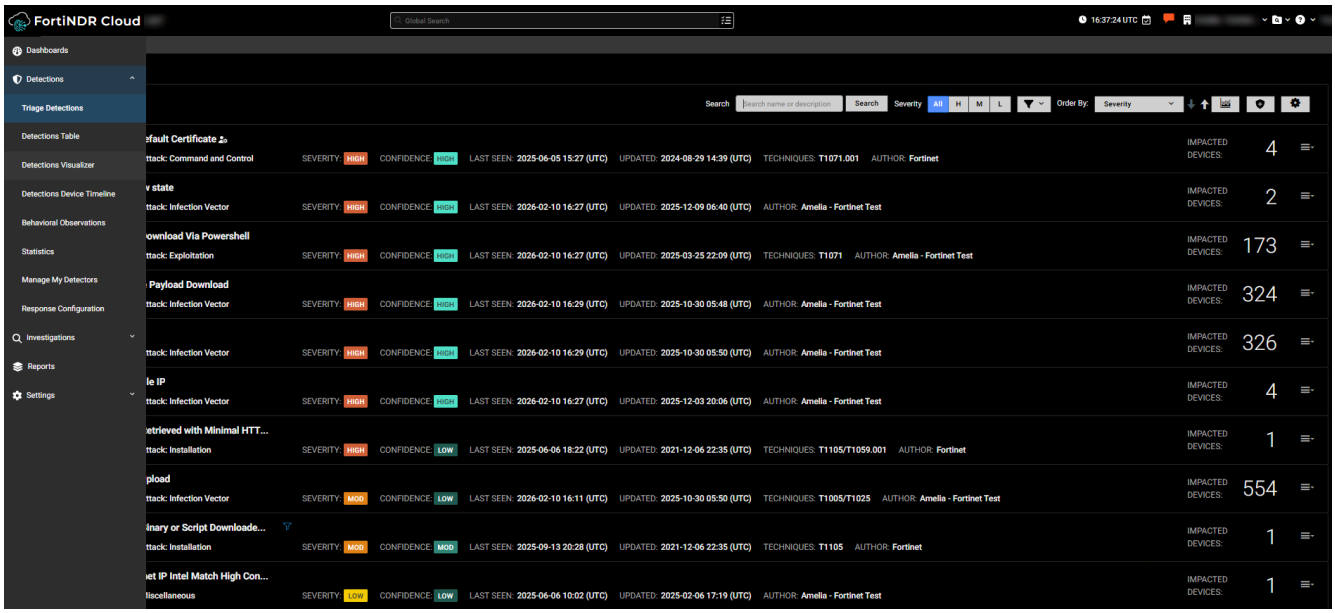
- A network connectivity issue
- A switch or tap misconfiguration
- A change in routing
- A partial failure where the sensor is still up but not seeing full traffic

The system continuously monitors visibility for each sensor. These counts are already displayed in the *Device View* page. Instead of a fixed system-wide baseline, the deviation is now calculated using a floating 7-day window. When the visible device count for a sensor falls below that threshold, the system automatically sends a *Device Count Deviation* alert to the configured recipients.

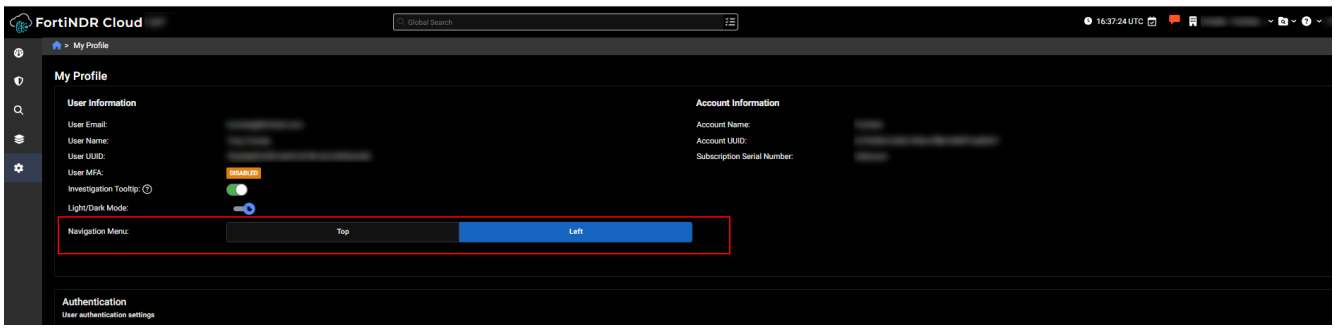


Left navigation

You now have the option to display the navigation menu on the left side of the portal. This is a user-specific preference available in the *My Profile* page, allowing each user to set their preferred layout without affecting others. When enabled, the left navigation appears as a collapsible vertical menu. It automatically expands on hover, displays navigation options based on the user's permissions, and highlights the current section and page.



To enable left navigation, click the *Gear icon* > *Profile settings* and select *Left* next to *Navigation Menu*.



The new left navigation menu is designed to improve access to an expanding set of menu options as FortiNDR Cloud continues to grow. Many Fortinet Fabric products already use a left-side navigation layout, and this enhancement aligns the experience while providing analysts with a more streamlined way to navigate the portal. Although the left navigation is optional in this release, it is planned to become the default navigation layout in a future release.

Customizable Detection Resolution Methods

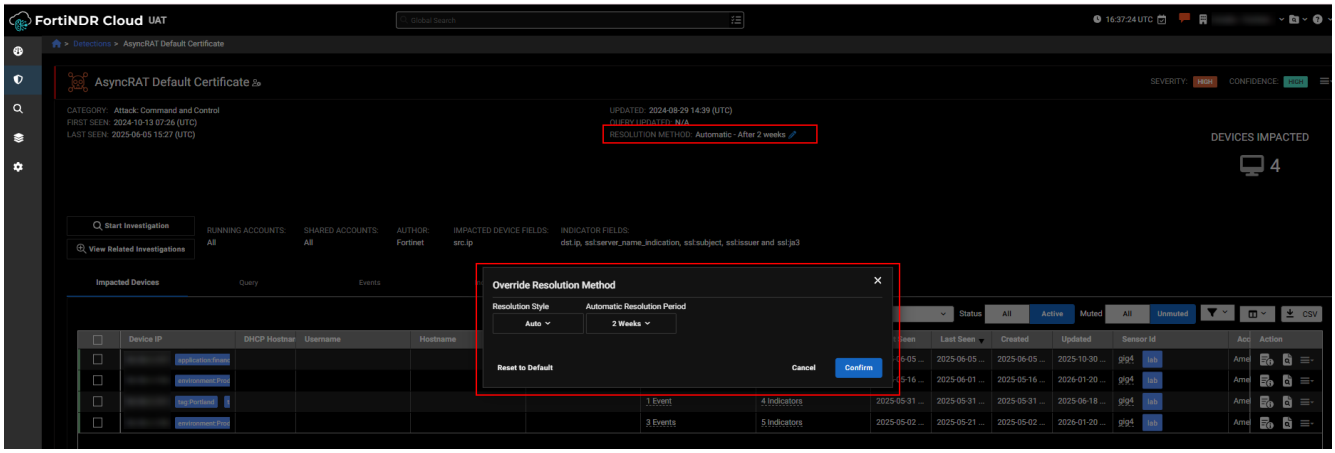
You can now override the default resolution method and resolution time for detectors created by other accounts. Previously, accounts that did not create the detector were required to use the resolution settings defined by the detector's creator.

With this enhancement, detectors now include an edit icon that allows you to:

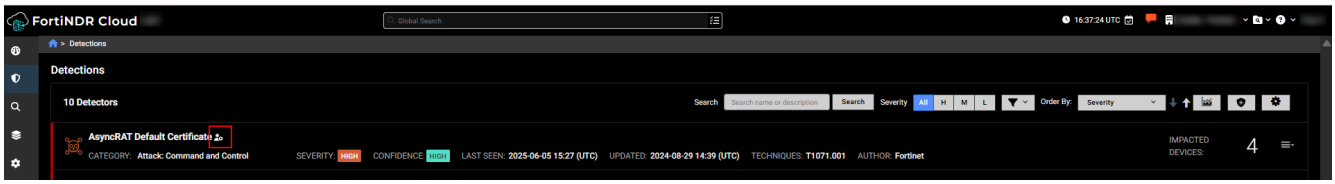
- Change the resolution method (auto or manual)
- Adjust the resolution time
- Restore the original creator-defined settings if needed

This option is only available for detectors your account did not create. If your account is the detector creator, the override option is hidden.

To override the resolution method, go to *Detections* > *Triage detections* and open a detector created by another account. Click the pencil icon to change the resolution method.



When a detector has a customized resolution method, an override indicator appears both in the detector header and in the list view, similar to the existing custom filter icon.



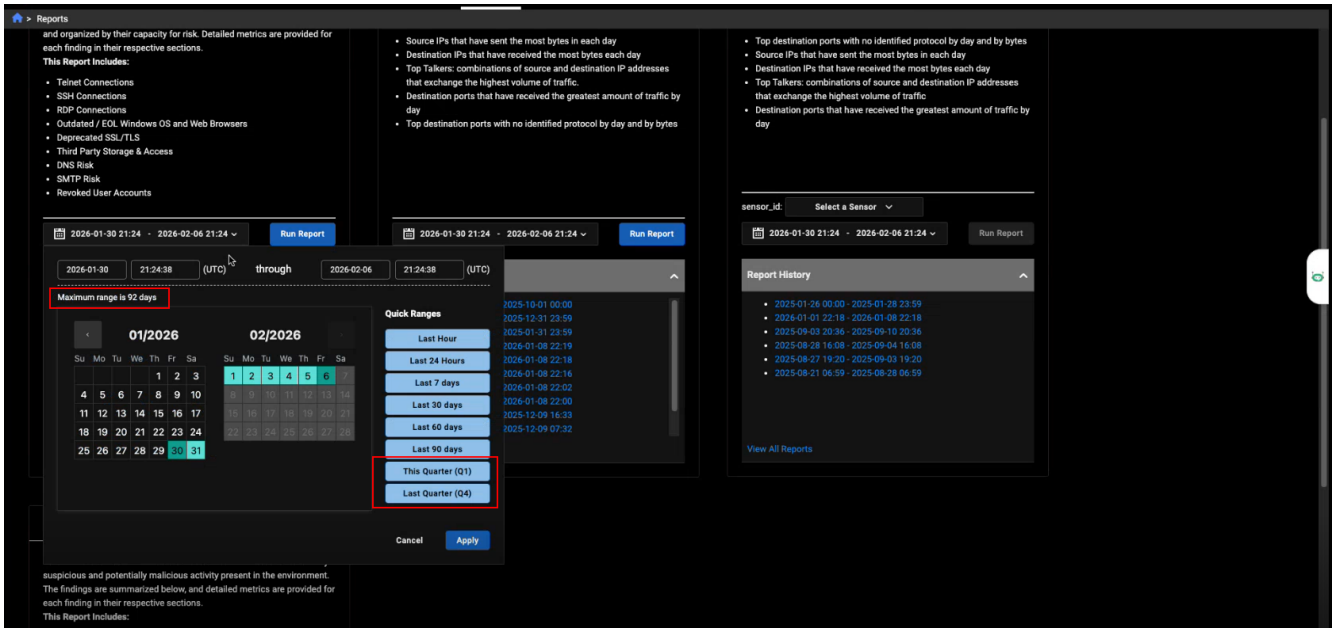
VPC Flow fields

A VPC Flow fields event occurs when raw VPC Flow Log data is parsed and its individual fields are extracted and normalized into a structured event. These events are only visible when the VPC feature is enabled. To enable it, contact your TSM or Customer Support.

Improved functionality

Report filtering

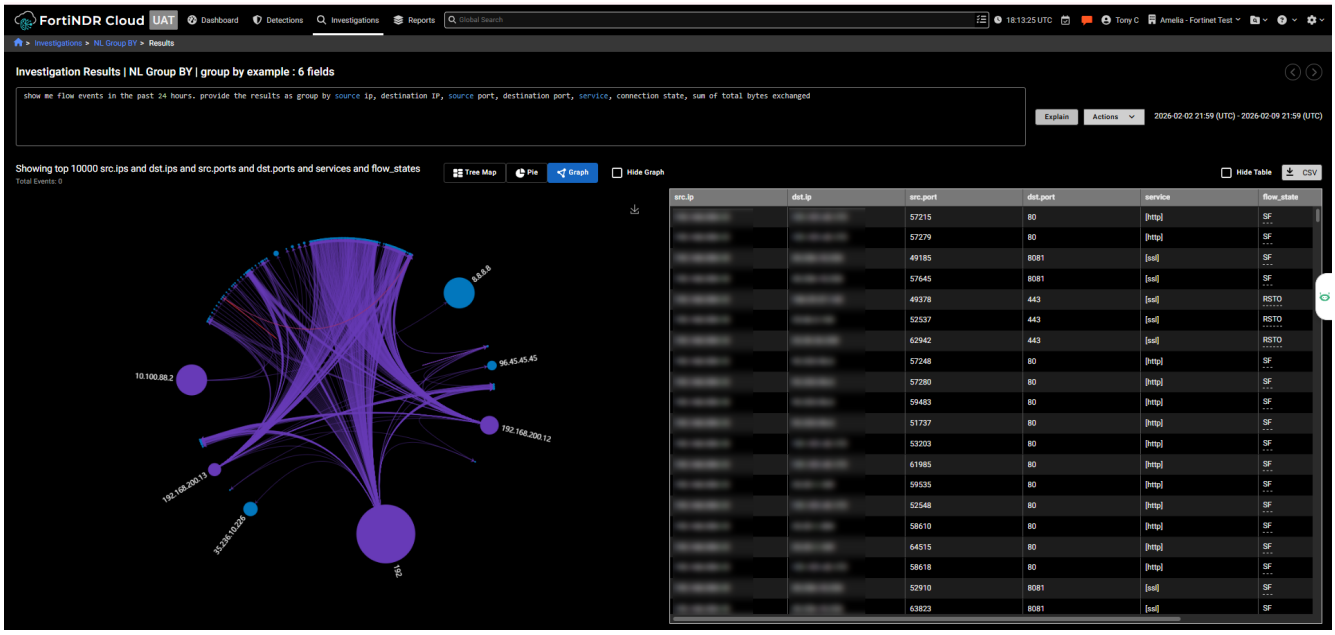
The time-range filter in *Reports* now supports date ranges up to 92 days instead of the previous 90, allowing you to select full calendar quarters (including quarters with 31-day months). It also introduces quick-select buttons for *This Quarter* and *Last Quarter*, which automatically adjust based on the current quarter.



Natural Language Query Enhancements

This release introduces several improvements to Natural Language Queries, expanding event coverage and improving query results.

- **Broader event type support**: Natural Language Query now supports all event types, aligned with those listed on the Event Fields page. Some exceptions apply, such as annotations and device enrichment fields, which are not currently supported.
- **Group By enhancements**: Users can now request grouped query results directly through natural language. The *Group By* operation supports up to 10 columns, allowing for more detailed summary and analysis.
- **UI improvements**: We have improved the clarity of query results, including improved display of aggregated counts and fixes to toast notifications.
- **Query-specified time period precedence**: When a time period is explicitly mentioned in the natural language query, that time period now takes precedence over the time selection in the GUI, ensuring results match the user's intended timeframe.

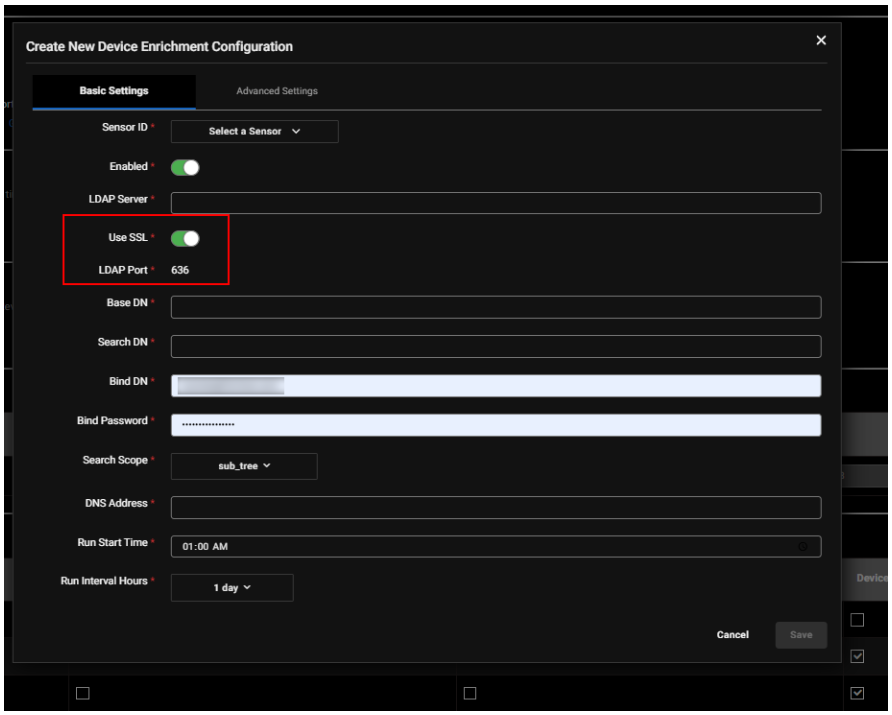


Device enrichment configuration

The *LDAP port* field in the *Device Enrichment* configuration has been updated to ensure consistent and secure configuration. Previously, the LDAP port was a free-form field, allowing users to enter any value. With this enhancement, the LDAP port is now automatically determined based on the SSL setting:

- When SSL is enabled, the configuration automatically applies the secure LDAP port.
- When SSL is disabled, the configuration switches to the standard LDAP port.
- Manual entry of custom port values is no longer allowed.

This change prevents invalid or unsupported port selections.



Netflow event fields

Improved NetFlow logs with additional fields and included a fix for the direction issue.

FortiAI updates and improvements:

- Enhanced response accuracy for detection-related queries.
- Improved precision and clarity when providing coverage information.

Other improvements

- On the *Sensors* page, you can now right-click on a sensor and open it in a new tab.
- Any IPs excluded from *Detections* are also excluded from *Observations*. This ensures that scanner or mirrored traffic, which is common in environments without packet brokers, no longer triggers unnecessary observations.
- The *Detections Table* now supports searching by last seen date.
- A new training scenario is now available in the portal: *DCSync and Enumeration*.

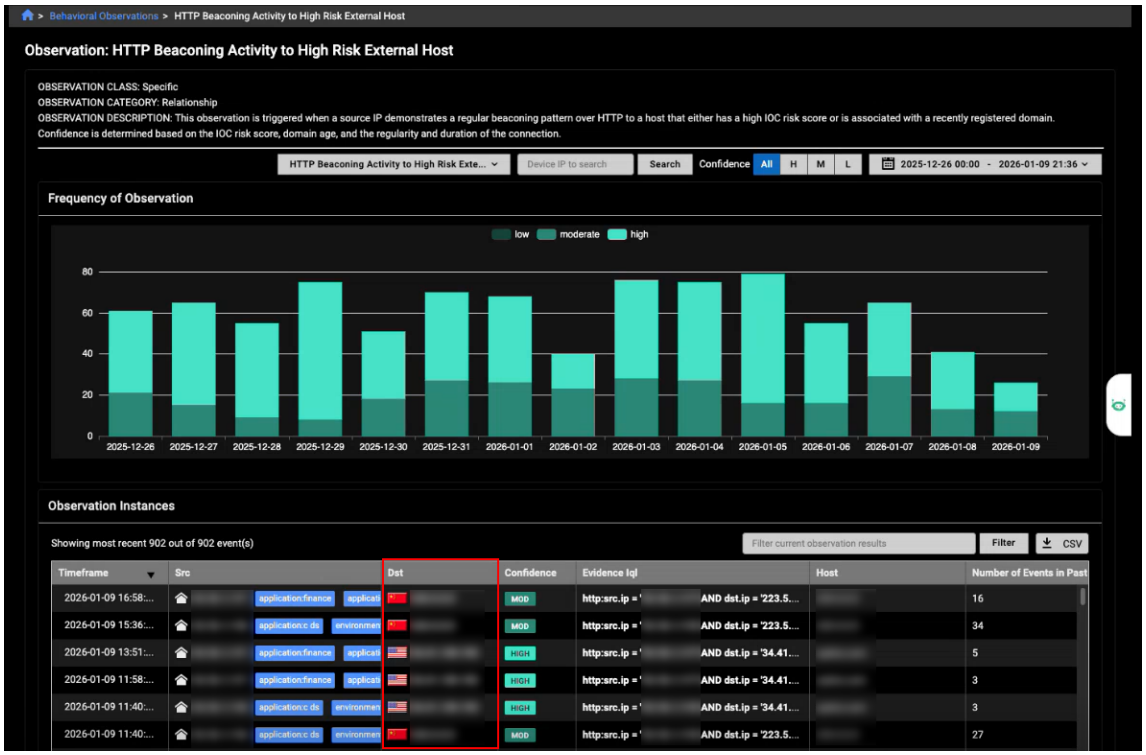
Version 26.1.0

- Improved functionality
  - Behavioral observations
  - FortiNDR Essentials Solution Pack v1.0.2
- Other improvements
- Resolved issues on page 25

Improved functionality

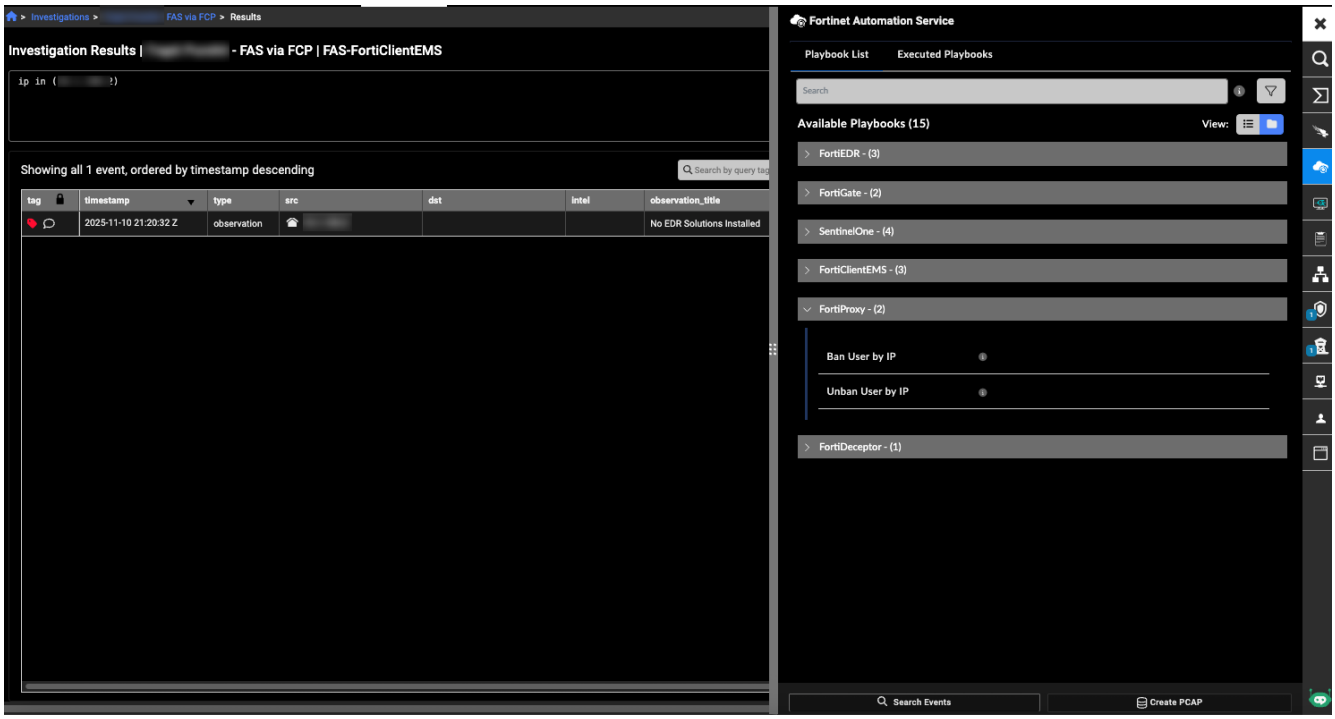
Behavioral observations

The *Destination IP* column on the *Behavioral Observations* details page now includes geolocation indicators: a flag icon appears next to the IP to show the country, and a house icon is displayed for internal IPs.



FortiNDR Essentials Solution Pack v1.0.2

The FortiNDR Essentials Solution Pack version 1.0.2 contains connectors and playbooks for FortiProxy.



Other improvements

- Improved the *High Risk Devices* widget so that the text in the pop-up wraps correctly and adjusts responsively to the page size.
- The layout for upload-related observations in the *Gen AI* dashboard has been updated so that the source IP is displayed on the left and the destination is on the right.
- The search function on the *Behavioral Observations* page has been enhanced to handle trailing spaces. Additionally, you can now search observations by UUID.

Product integration and support

Integrations

The following table lists FortiNDR Cloud product integration and support information. Integration guides are available on the FortiNDR Cloud Integrations page.

Category	Integration	Supported Version/Notes
Deception	FortiDeceptor	Requires Automation Service
SIEM	CrowdStrike	Tested with Parser 1.0.2
	FortiSIEM	7.1.0 or higher
	Microsoft Sentinel	Integration supported via API-based ingestion.
	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	FortiEDR	Manager 6.2.0 or higher Collector 5.2.0 or higher
	FortiClientEMS	Requires Automation Service
	FortiManager	7.4.2 or higher
	FortiGate	7.4.2 or higher
	CrowdStrike EDR	Requires latest Falcon EDR APIs
	SentinelOne	Requires Automation Service
Intelligence Feeds	CrowdStrike Falcon Intel	License required
	Fortinet Botnet Domain List	Included with FortiNDR Cloud
	Fortinet Botnet IP List	Included with FortiNDR Cloud
	Fortinet Malicious Domain List	Included with FortiNDR Cloud
	Fortinet Phishing List	Included with FortiNDR Cloud
	Fortinet Proxy List	Included with FortiNDR Cloud
	Fortinet Spam List	Included with FortiNDR Cloud

Category	Integration	Supported Version/Notes
	Fortinet Tor List	Included with FortiNDR Cloud
	Internet Scan Data B (Shodan)	Included with FortiNDR Cloud
	Known Sinkholes	Included with FortiNDR Cloud
	PhishTank	Included with FortiNDR Cloud
	Proofpoint TAP	License required
	Recorded Future connect	License required
	Threat Connect	License required
	Tor Nodes	Included with FortiNDR Cloud
	URLHaus	Included with FortiNDR Cloud
Other	Endace	7.2.2 or higher
	ERSPAN	Type II and Type III
	Netskope	Integration via Cloud TAP Stitcher.
	Netflow	NetFlow v5, v9, IPFIX and UDP/6343 (SFlow)
	Zscaler	Integration supported through NSS for traffic and threat logs.

Fortinet Automation Service

The following table lists the current Fortinet Automation Service solution pack versions. For information about the Fortinet Automation Service, see the FortiNDR Cloud User Guide.

Solution Pack Version	Connectors and Playbooks
1.0.0	FortiClientEMS, FortiEDR, FortiDeceptor
1.0.1	FortiClientEMS, FortiEDR, FortiDeceptor, FortiGate, Sentinel One
1.0.2	FortiClientEMS, FortiEDR, FortiDeceptor, FortiGate, FortiProxy, Sentinel One

Resolved issues

The following issues have been fixed in version 26.1.b. To inquire about a particular bug, please contact Customer Service & Support.

26.1.b

Bug ID	Description
1180323	An issue where selecting *View Related Investigation* redirected to the wrong page has been fixed.
1236879	An issue where the EPS graph failed to display days or hours with zero values has been resolved.
1256916	An issue where the selected account in the left navigation would revert to the previously selected account after clicking a menu item has been resolved.
1259166	Resolved an issue that caused the CSV download button to disappear.
1259201	Error messages that were previously cut off in the Date Range Picker's Date or Time fields have been fixed.
1263463	An issue where switching accounts on the dashboard left the entity panel open and displaying data from the previous account has been fixed.
1268422	Fixed an issue where the *Sensor* page could not display all enabled feature tags because the row was too narrow.
1271342	Resolved an issue where columns containing numeric data were being sorted as strings.
1271352	Resolved an issue where the *Observation* page displayed an irrecoverable error when no observations were available in the selected time range.
1273176	Fixed an issue where the *Query History* tab was not working in the *Query Picker*.

26.1.a

Bug ID	Description
1238020	Resolved an issue where actions performed through integrations did not include the username, email address, or first and last name of the user.

Bug ID	Description
1238020	In the *Entity Panel*, the Audit Logs for the FortiEDR, CrowdStrike, and FortiNDR integrations display usernames and email addresses.
1248347	Resolved an issue where the default dashboard was taking longer than expected to load.
1252131	Added a link to the User Guide in the *Device Enrichment Configuration Setting* section.
1255293	Resolved an issue where the *Observation* detail page was not displaying the latest observation name.
1255296	Resolved an issue where the *Whois* section in the *Entity Panel* was displaying incorrect data.
1255300	The *WHOIS* field in the *Entity Panel* now displays a spinner indicating it is waiting for a response.
1255303	Resolved an issue where the *FortiManager* section was throwing an error when authentication failed.
1255308	Resolved an issue where an incorrect toast message was displayed.

26.1.0

Description
Fixed an issue where the portal retrieved only the most recent 1,000 records from the past 30 days.
Fixed an issue where the Network Security Posture Report did not display the Deprecated SSL and TLS section as intended.
Fixed an issue where the FortiManager integration triggered unnecessary configuration calls, causing invalid credential errors.
Fixed an issue where selecting *All* accounts during portal login prevented customers from accessing the portal.

Known issues

The following issues have been identified in version 26.1.b. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

25.4.a

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

www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.