

Release Notes

FortiNDR Cloud 2023



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



September 15, 2025

FortiNDR Cloud 2023 Release Notes

78-254-1113279-20250915

TABLE OF CONTENTS

FortiNDR Cloud release notes	4
Version History (2023)	5
13 December 2023 Version 2023.12.0	5
15 November 2023 Version 2023.11.0	9
25 October 2023 version 2023.1.0	12
6 October 2023 version 2023.9.1	17
27 September 2023 version 2023.9	17
13 September 2023 version 2023.8.1	21
21 August 2023 version 2023.8	22
31 July 2023 version 2023.7	23
17 July 2023 version 2023.6.1	27
26 June 2023 version 2023.6	28
12 June 2023 version 2023.5.1	32
25 May 2023 version 2023.5.0	32
15 May 2023 version 2023.4.1	34
24 April 2023 version 2023.4	34
10 April 2023 version 2023.3.1	36
27 Mar 2023 version 2023.3	36
13 Mar 2023 version 2023.2.1	40
27 Feb 2023 version 2023.2	41
07 Feb 2023 version 2023.1.1	47
30 Jan 2023 version 2023.1	47
Resolved Issues	51
2023.12	51
2023.11	51
2023.10	52
2023.9.1	52
2023.9	52
2023.8.1	53
2023.8	53
2023.7	53
2023.6.1	53
2023.6	54
2023.5.1	54
2023.5.0	54
2023.4.1	54
2023.4	55
2023.3.1	55
2023.3	55
2023.2.1	56

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 (2023)

Date	Version
13 December 2023	2023.12
15 November 2023	2023.11
25 October 2023	2023.10
11 October 2023	2023.9.1
27 September 2023	2023.9
13 September 2023	2023.8.1
21 August 2023	2023.8
31 July 2023	2023.7
17 July 2023	2023.6.1
26 June 2023	2023.6
12 June 2023	2023.5.1
25 May 2023	2023.5.0
15 May 2023	2023.4.1
24 April 2023	2023.4.0
10 April 2023	2023.3.1
27 March 2023	2023.3
13 March 2023	2023.2.1
27 February 2023	2023.2
07 February 2023	2023.1.1
30 January 2023	2023.1

13 December 2023 Version 2023.12.0

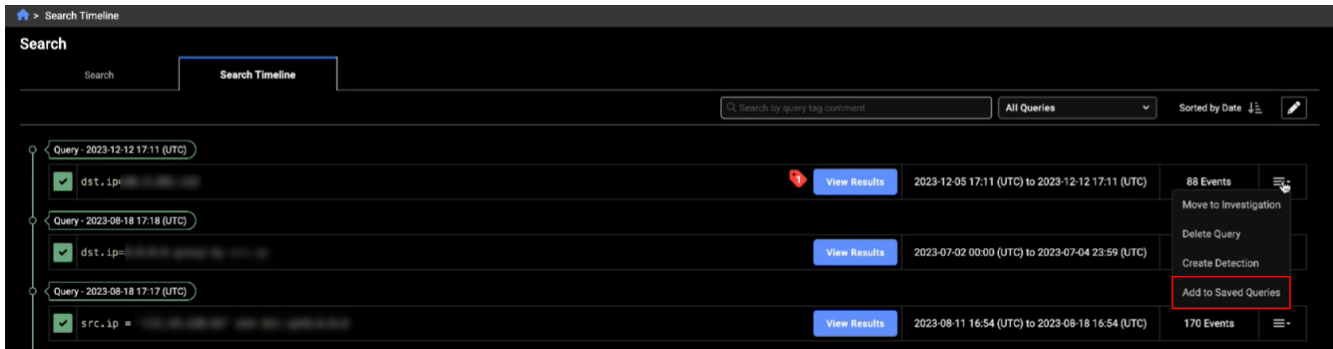
- [New Functionality](#)
 - [Search Timeline](#)
- [Improved functionality](#)
 - [Management Rules page](#)
 - [Entity panel](#)

- [Query History](#)
- [Resolved Issues](#)

New Functionality

Search Timeline

You can now save a query from the *Search Timeline* page. To save the query, click the *Actions* menu and select *Add to Saved Queries*.

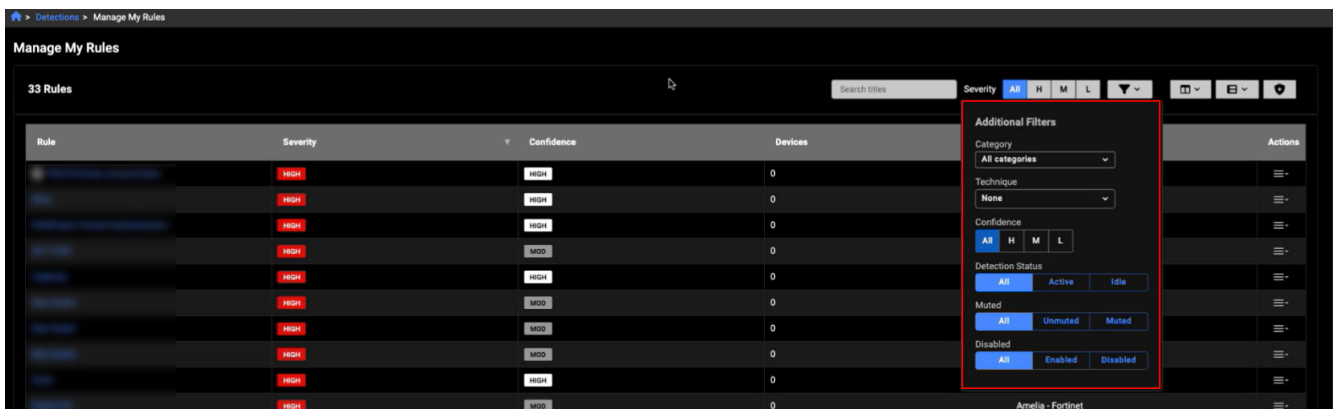


Improved functionality

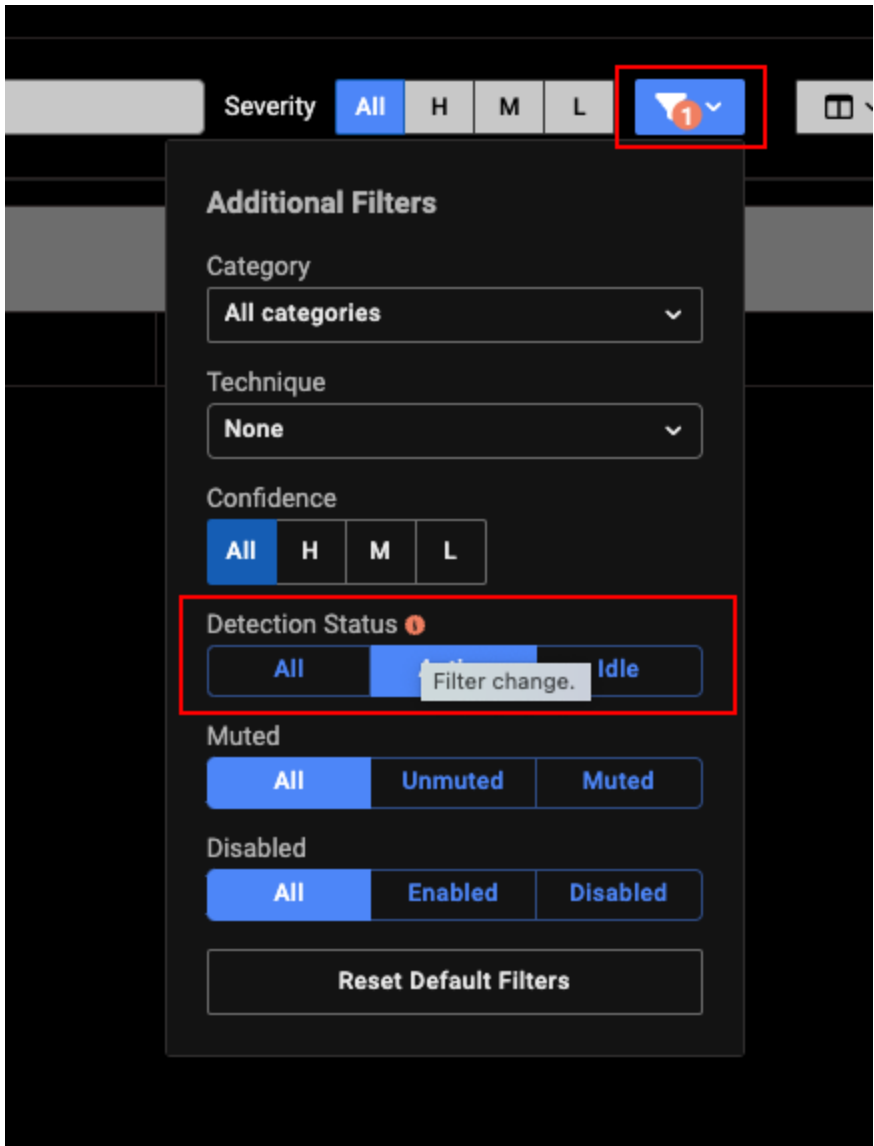
Management Rules page

When you edit a rule you are returned to the *Manage My Rules* page after you click *Cancel* or *Save Rule*. In previous versions, you remained on the rule page after saving or canceling your edits.

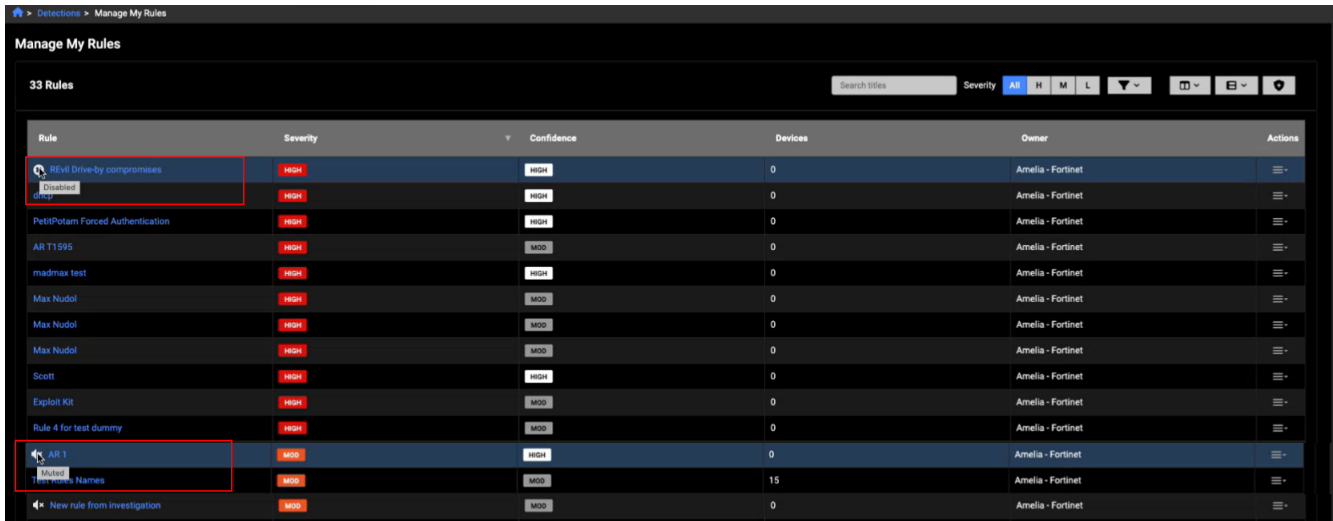
The *Additional Filters* menu now defaults to *All* for *Detection Status*, *Muted* and *Disabled*. This allows you to see all the rules at a glance.



The filters also persist until you refresh the page (except for the *Search* title). An indicator has been added to the filters when you change a filter from the default. A number indicates the number of changes that were applied. A *Reset to Default* was also added to the filter panel.

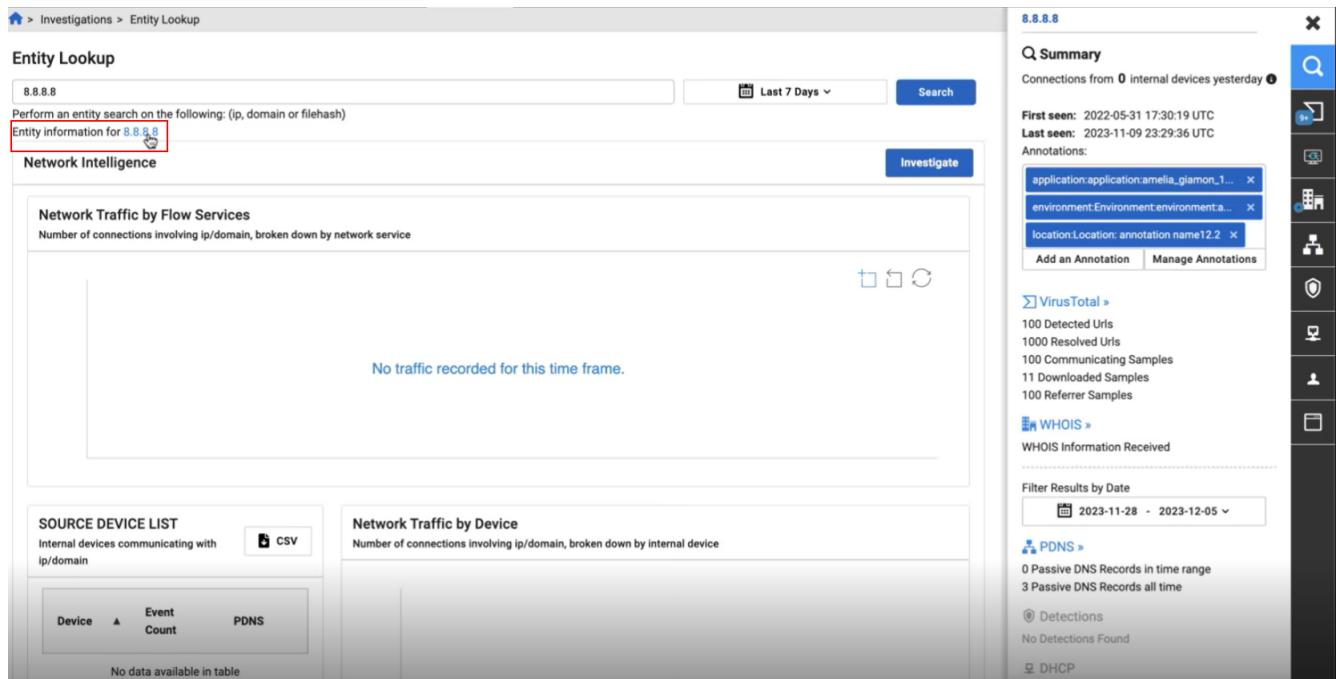


A *Muted* and *Disabled* icon has been added to the *Rules* column. This helps distinguish muted and disabled rules when the filter is set to *All*.



Entity panel

There is now a shortcut from the *Entity Lookup* page to the *Entity Panel*. This allows you to view information in the panel that is not in the lookup page.



Query History

A new *Search Timeline* section was added to the *Query History* tab allowing you to view adhoc queries without a filter.

Select a New Query
✕

Saved Queries
Query History

Investigations:

Queries:

	Query Name	Search	Result Count	Filtered	Date Created
Search Timeline		ip = '10.1.201.112'	87		2023-11-15 19:28 (UTC)
Do NOT touch it - AR 1		file.sha1 != null	100		2023-11-06 08:05 (UTC)
Ashok 2 - 2023-10-24 19:04:52 (UTC)		method='this is from adhoc'	0		2023-11-03 18:18 (UTC)
Do NOT touch it - AR 3 three		(suricata:sig_name LIKE "%RAT%") AND (uid != null)	0		2023-08-11 08:48 (UTC)
Ashok Raghunayakula - 2023-10-13 01:17:54 (UTC)		(suricata:sig_name LIKE "%RAT%") AND (uid != null)	0		2023-08-11 08:38 (UTC)
Network Security Posture Report Investigation 112					
Malicious PE File Enriched					
Max Nudol - 2023-08-31 21:13:08 (UTC)					

TIME FRAME: 2023-11-08 19:28 (UTC) to 2023-11-15 19:28 (UTC)
RESULT LIMIT: 100

Cancel
Select

15 November 2023 Version 2023.11.0

- New functionality
 - User management
 - Entity Panel: FortiGuard
- Resolved issues

New functionality

User management

We have reduced the amount of information in the CSV export making it easier to navigate in the file and find the information are looking for. Much of this information has been consolidated into the *user_role* column. If there is no account name in front of the role, this indicates the user belongs to the current account (*Admin*, *User*, *Limited User*). If the user has the same roles in two or more accounts, the account name is displayed followed by a colon (:) followed by the user role.

Version History (2023)

1	user_uuid	locked	last_login_date	account_name	user_roles
2	16-091d-4aae-880a-3c3efcd6198	FALSE	2023-11-07T18:22:59.272Z	Allegiance	Admin, User, Admin:Amelia - Fortinet Test, User:Amelia - Fortinet Test
3	11-003a-4cf8-a89e-a2968f5c299c	FALSE	2023-10-31T17:36:33.027Z	Allegiance	User
4	16-091d-4aae-880a-3c3efcd6198	FALSE		Allegiance	Admin, User
5	1-b6e7-4b1c-b087-26aeec23c94d	FALSE	2023-10-31T23:00:49.815Z	Allegiance	Admin, User

A new *Roles* column has been added to the *Users* page. When you can click the row the *User Details* pane displays all the roles and accounts assigned to the user.

Email	Full Name	Last Login	Created	Status	Locked Out	MFA	Roles	Actions
nn...	ADMIN	2023-11-07 18:22:59	2023-08-25 21:36:48	ENABLED	No	DISABLED	Admin, User, Admin:Amelia - Fortinet Test, User:Amelia - Fortinet Test	⋮
sm...	ADMIN	2023-10-31 23:00:49	2023-10-31 22:59:42	ENABLED	No	DISABLED	Admin, User	⋮
tes...	ADMIN	2023-10-25 21:52:24		ENABLED	No	DISABLED	Admin, User	⋮

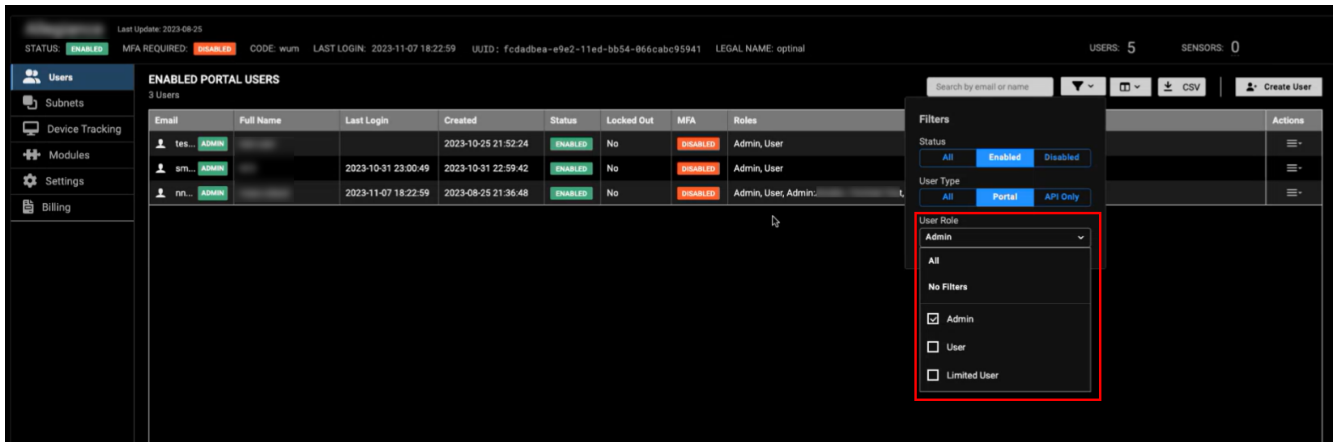
Role	Account
User	
Admin	
User	
Admin	

If you do not see the *Roles* column by default, you can add it manually.

Email	Full Name	Last Login	Created	Status	Locked Out	MFA	Roles	Actions
creed2	two	2023-10-31 17:36:33	2023-10-24 21:59:50	ENABLED	No	DISABLED	User	⋮
nn...	maxs dsasd	2023-11-07 18:22:59	2023-08-25 21:36:48	ENABLED	No	DISABLED	Admin, User, Admin:Amelia - Fortinet Test, User:Amelia - Fortinet Test	⋮
sm...	M S	2023-10-31 23:00:49	2023-10-31 22:59:42	ENABLED	No	DISABLED	Admin, User	⋮
tes...	test user	2023-10-25 21:52:24		ENABLED	No	DISABLED	Admin, User	⋮

- First Name
- Last Name
- UUID
- Last Login
- Created
- Updated
- Accepted TOU
- Status
- Locked Out
- MFA
- Roles

You can also filter the column by the user role.



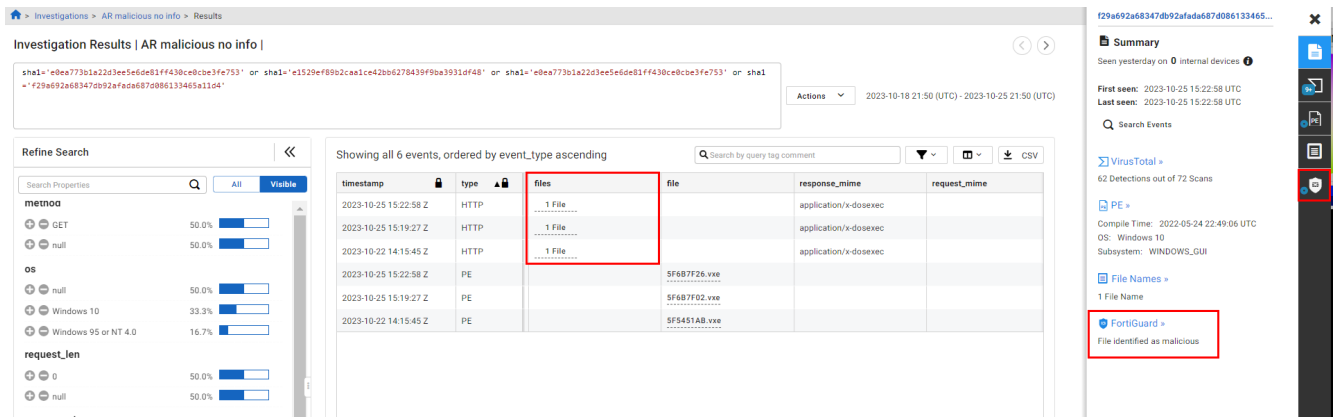
Entity Panel: FortiGuard

The *Entity Panel* now displays information about the malicious files when it is available.

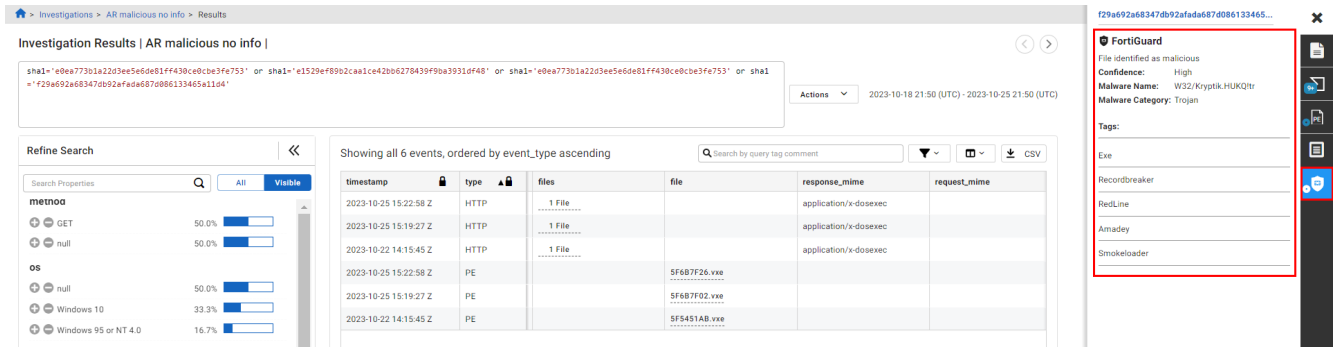
To view malicious file attributes in the Entity Panel:

1. Go to *Investigations > Investigate*.
2. Click an investigation in the list and then click *View Results*.
3. Navigate to the *files* column and click the file link.

When a malicious file is detected, you will see the *FortiGuard* section heading in the Entity Panel with the message *File identified as malicious*.



Click the section header or the FortiGuard icon to view the attributes about the malicious file. If the attributes are not available, then none are displayed.



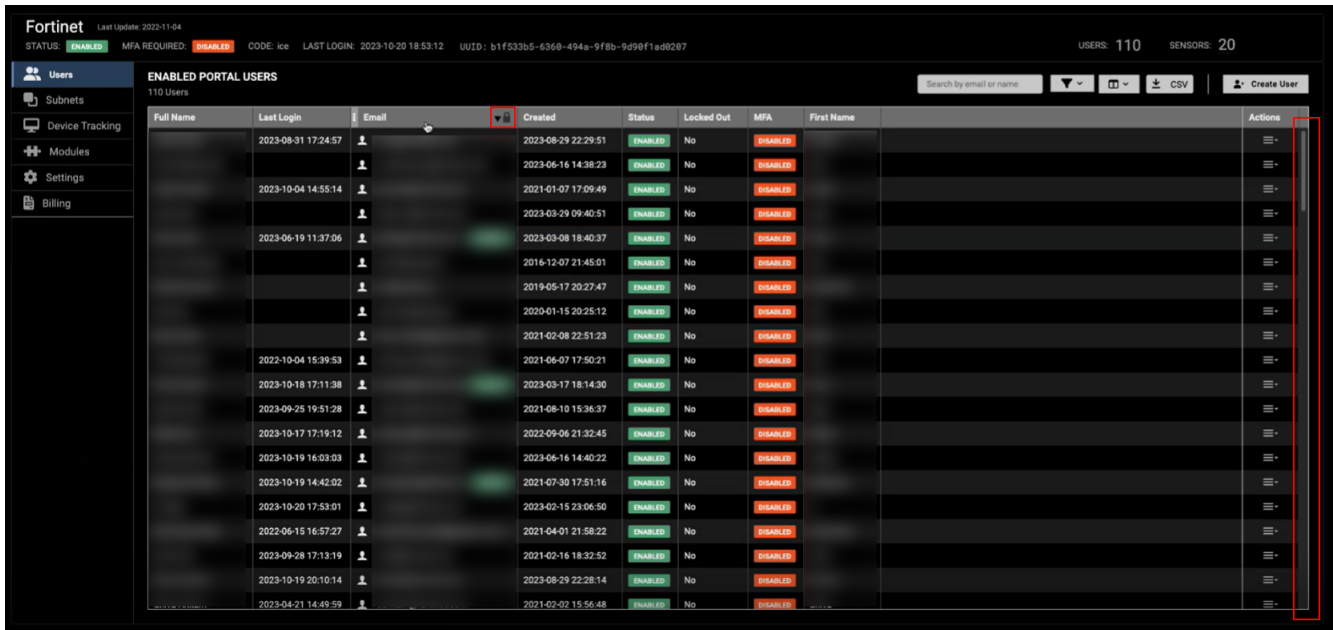
25 October 2023 version 2023.1.0

- New functionality
 - User management
- Improved functionality
 - Deleting tags
 - Entity Panel: PDNS
 - Detections table: Muting
- Resolved issues

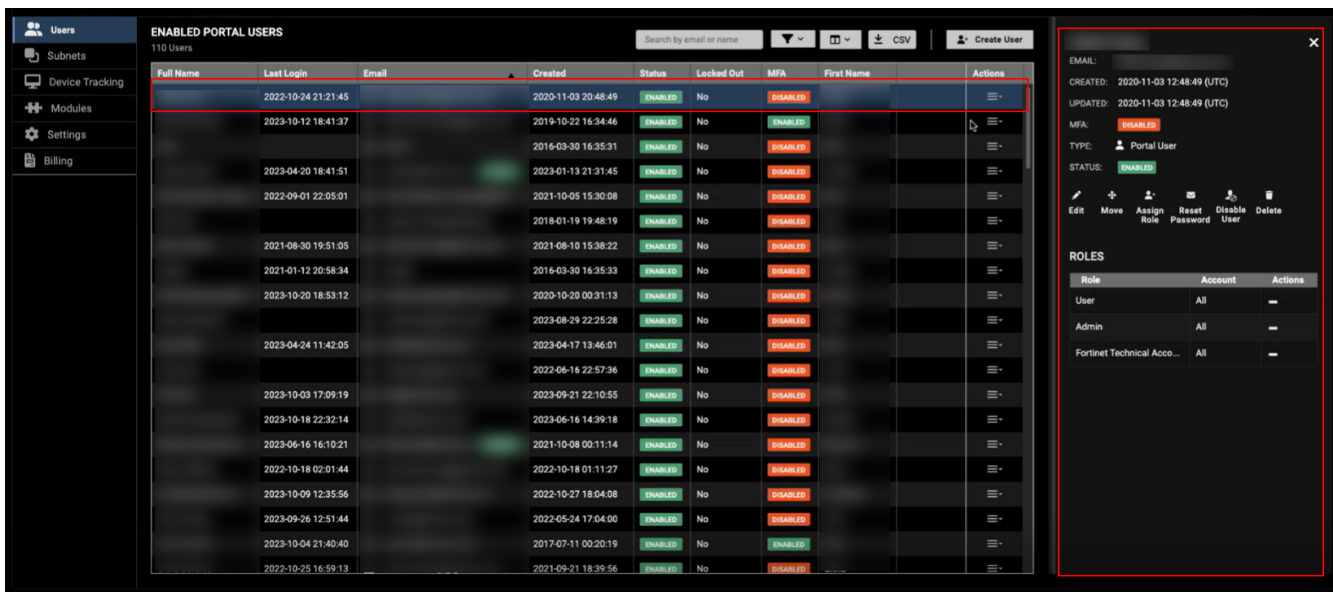
New functionality

User management

The columns in the *User Management* table can now be locked, re-sized and rearranged. Any changes you make to the page layout are saved when you refresh the page. Pagination at the bottom of the page has been replaced with a scroll bar.



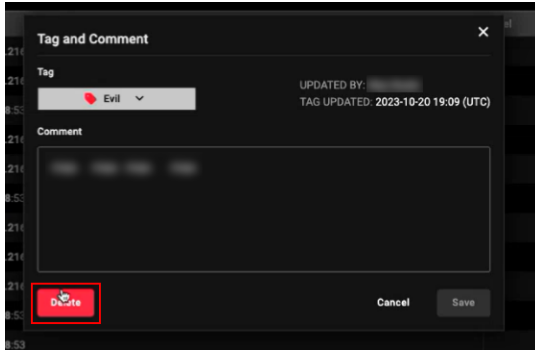
When a user is selected, the table width adjusts to accommodate the user profile pane so there is no overlap. The user is highlighted in blue until you close the pane.



Improved functionality

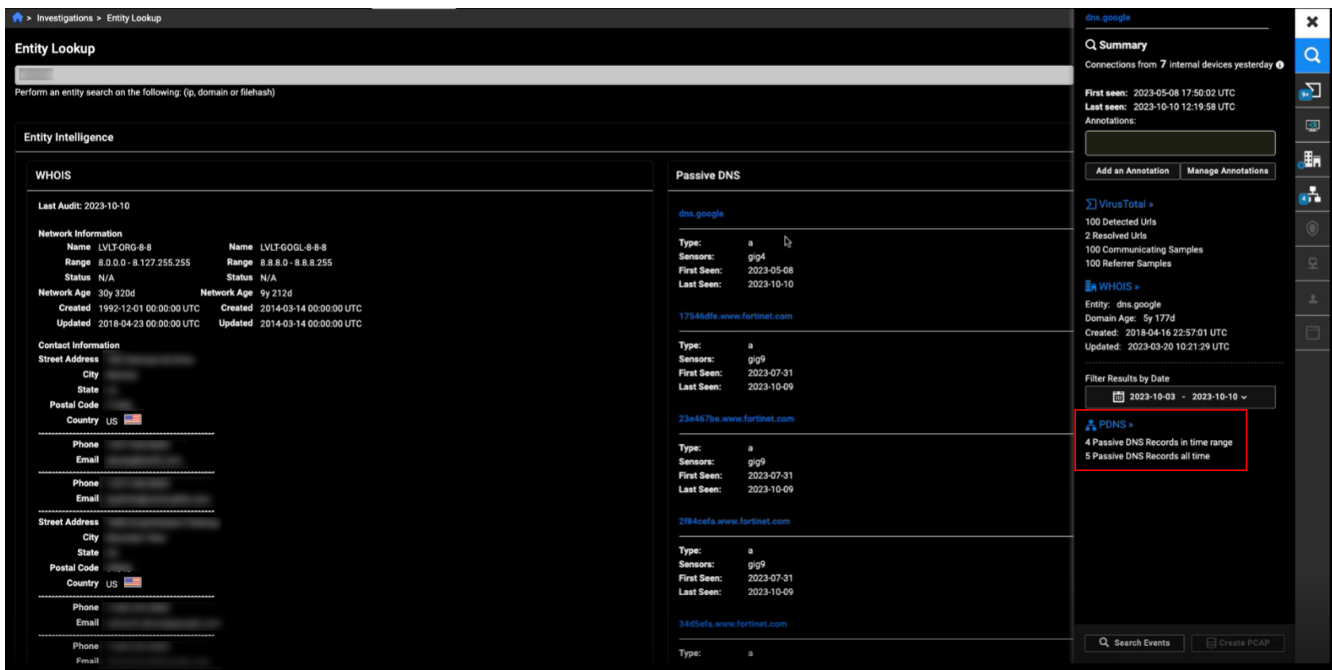
Deleting tags

The method for deleting tags has been improved. To delete a tag, open the item and click *Delete*. The tag and any comments will be removed.

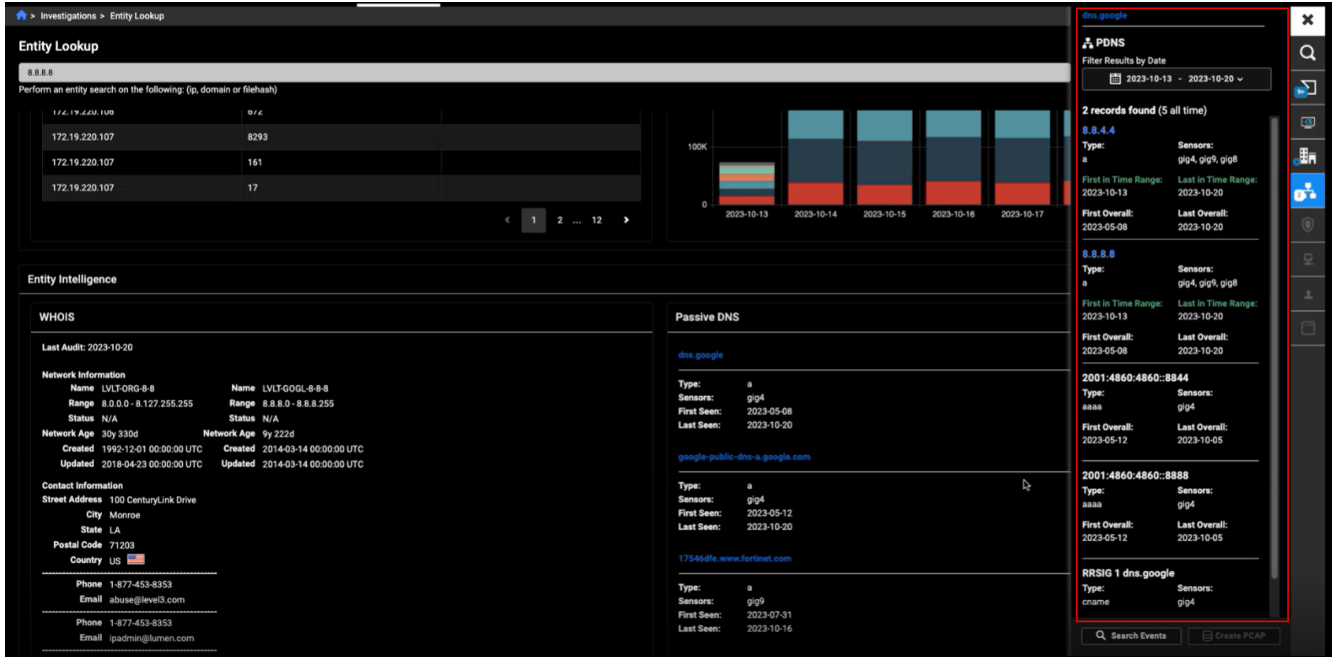


Entity Panel: PDNS

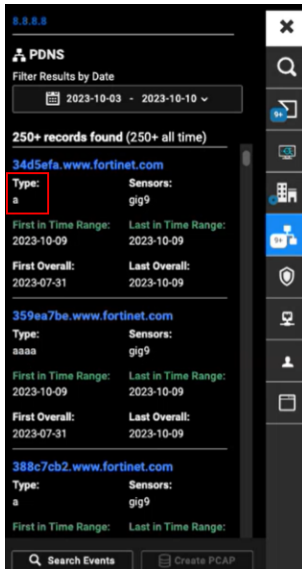
The PDNS tab in the in the *Entity Panel* contains more information. Two sets of data are displayed: the *DNS record in the time range* and *Passive DNS record all time*.



The records are displayed in the order they were last seen. The records within the time range appear at the top of the list. Records within the time range are highlighted by *First in Time Range* and *Last in Time Range*.



The Type field indicates if the DNS type such as IPv4 (a) or IPv6 (aaaa).



Detections table: Muting

Two new columns were added to the Detections Table. The *Detections Muted* and *Device Muted* work with the *Rule Muted* column to accommodate changes to the muting filter.

The screenshot shows the 'Detection List' interface with 13 detection rules and 6 devices from 19 detections. The table has columns for 'resolved', 'Resolved Comment', 'Detection Muted', 'Device Muted', 'Rule Muted', 'Rule Name', 'Rule Description', and 'Action'. The 'Detection Muted', 'Device Muted', and 'Rule Muted' columns contain speaker icons with a slash through them, indicating a muted state. A red box highlights these three columns.

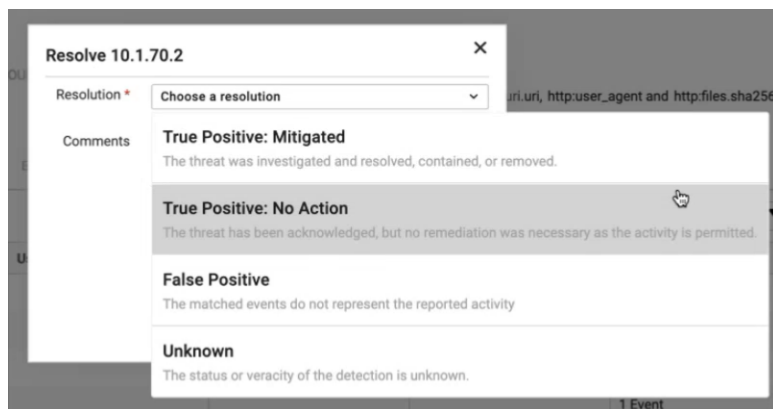
Muted detections are now flagged with *Muted* in the *Status* column.

The screenshot shows the 'Detection List' interface with 13 detection rules and 43 devices from 108 detections. The table has columns for 'First Seen', 'Last Seen', 'Created', 'Updated', 'Sensor Id', 'Account', 'Status', 'Muted By', and 'Date Muted'. The 'Status' column now contains text labels such as 'Resolved / Muted', 'Active / Muted', and 'Resolved'. A red box highlights the 'Status' and 'Muted By' columns.

Other enhancements

Resolution type

The definition of *True Positive: No Action* has been updated to *The threat has been acknowledged but no remediation was necessary as the act is permitted.*



6 October 2023 version 2023.9.1

FortiNDR Cloud 2023.9.1 includes bug fixes, but no new features. See [Resolved Issues](#) on page 51.

27 September 2023 version 2023.9

- New functionality
 - User roles
- Improved functionality
 - Search function
 - Entity Panel
 - Account management
 - Sensor versions
 - Other improvements

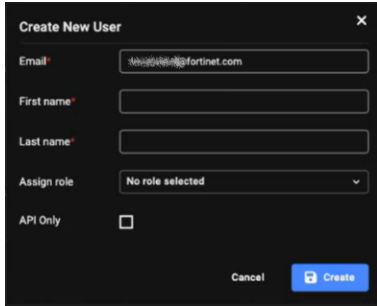
New functionality

User roles

You can now assign a user role or roles when you create new user, including *Admin*, *Training User*, and *User*.

New users are automatically assigned the Training User role on the Training Modern account, even if the administrator has not assigned any roles to the user. If the account is a parent account, and the administrator has access to child accounts, then a checkbox is available to include child accounts.

Required fields are identified with an asterisk.

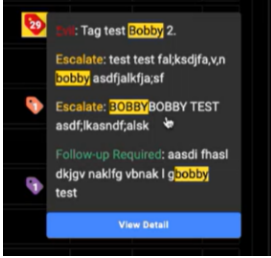


Improved functionality

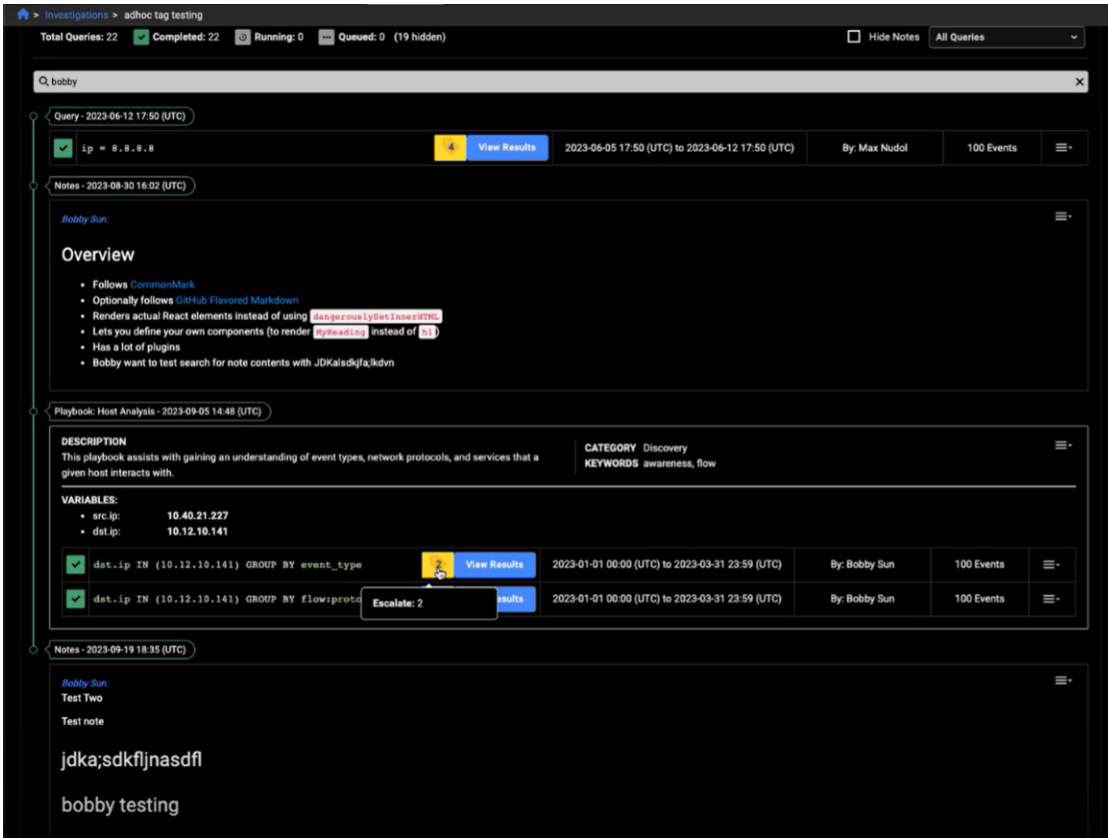
Search function

You can now use the search function in the Investigation list and details to search for text in comments and notes. Matching results are highlighted in yellow.

When you hover over the results in the Activities and notes column, you can click to open a window to view all the matches in the comments or notes. You can then click on one matched note to open the results table displaying only the matched results.

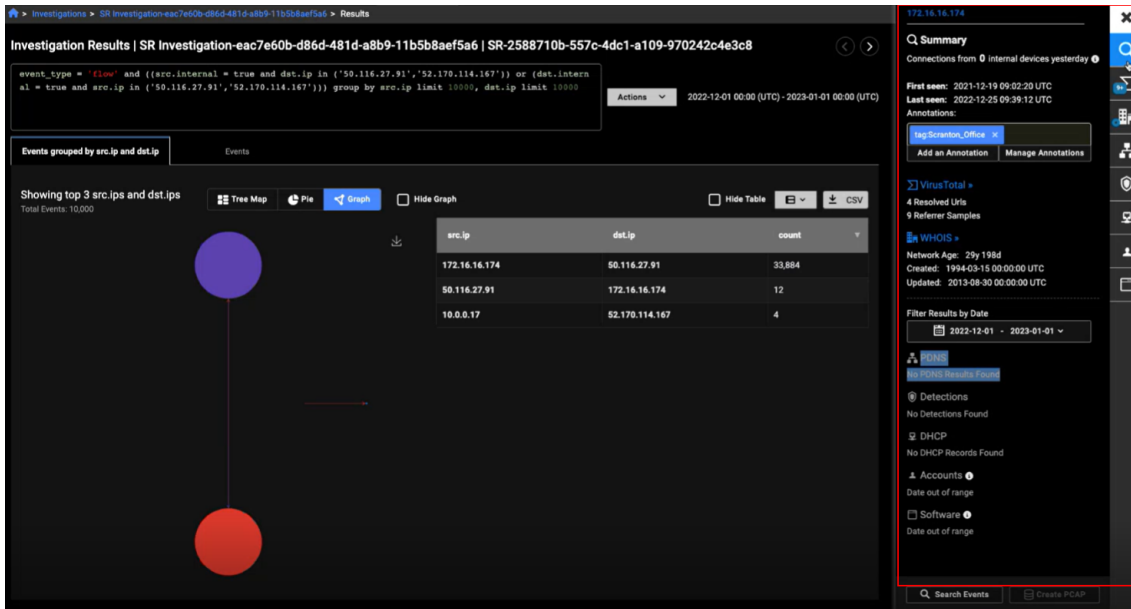


Click *View Details* to open the investigation. The matched text will be highlighted.



Entity Panel

The Entity Panel has been reorganized. Virus Total and WHOIS now appear at the top of the summary and the date range filters are the bottom. The navigation tabs have been updated to match the rest of GUI.

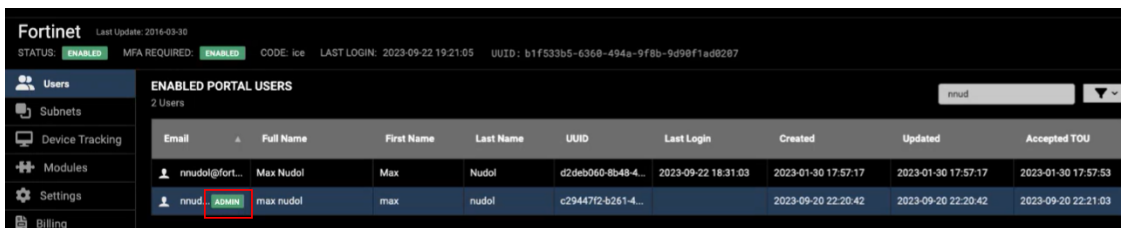


The date range on Entity Panel now defaults to the time range based on where the panel is opened.

- The time range in the Entity Panel will match the range entered in the following pages: Entity Lookup, Visualizer, Detection Table, Sensor Visibility, Investigate Results, Adhoc Search and Observation Detail.
- The default time range is 7 days in the following pages: Detection, Detection-Indicator and Detection-Triage.

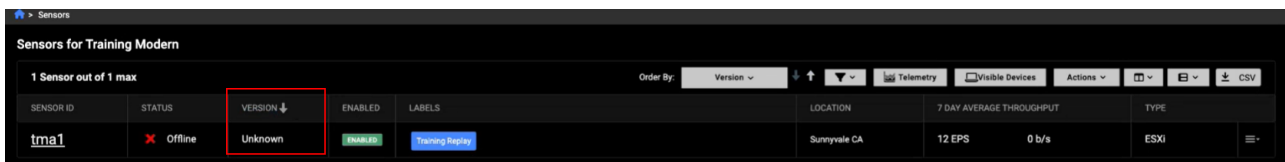
Account management

We have added a tag next to a user's email address to identify users with Admin roles. The tag is only visible the user is the Admin on the current account.



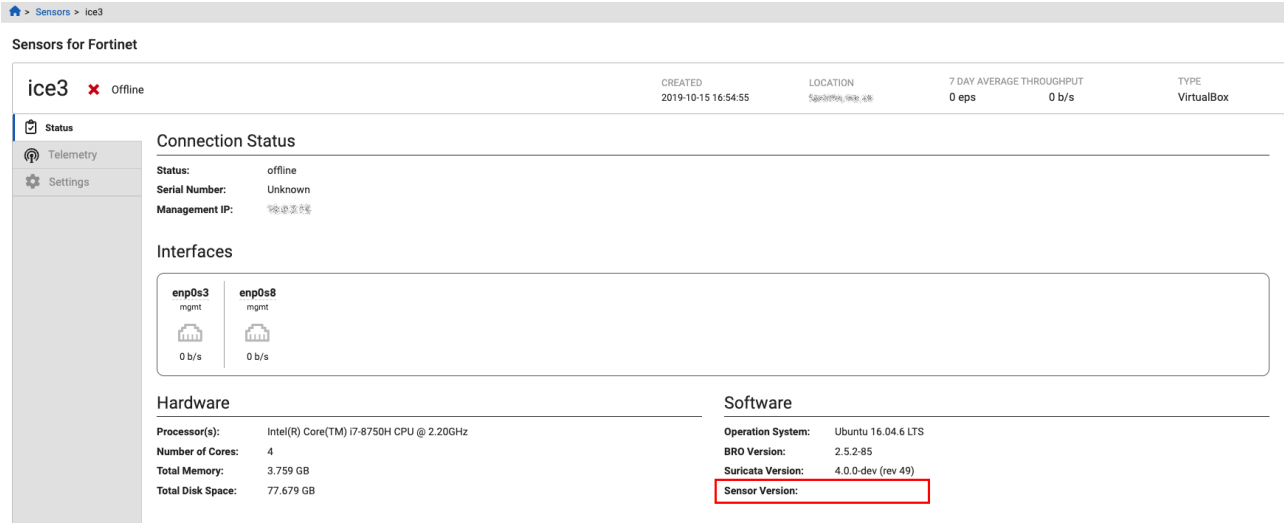
Sensor versions

The sensor version is now displayed in the in the *Version* column of the *Sensor* page. The column can be sorted, and when there is no data for the version, *Unknown* is displayed.



The sensor version is also shown on the *Sensor Detail* page in the *Software* section on the *Status* tab. When there is no data for the version, the field is blank.

Version History (2023)



Sensors for Fortinet

ice3 ✖ Offline

CREATED: 2019-10-15 16:54:55 | LOCATION: Singapore, Singapore | 7 DAY AVERAGE THROUGHPUT: 0 eps, 0 b/s | TYPE: VirtualBox

Connection Status

Status: offline
Serial Number: Unknown
Management IP: 10.1.70.2

Interfaces

enp0s3 mgmt 0 b/s
enp0s8 mgmt 0 b/s

Hardware

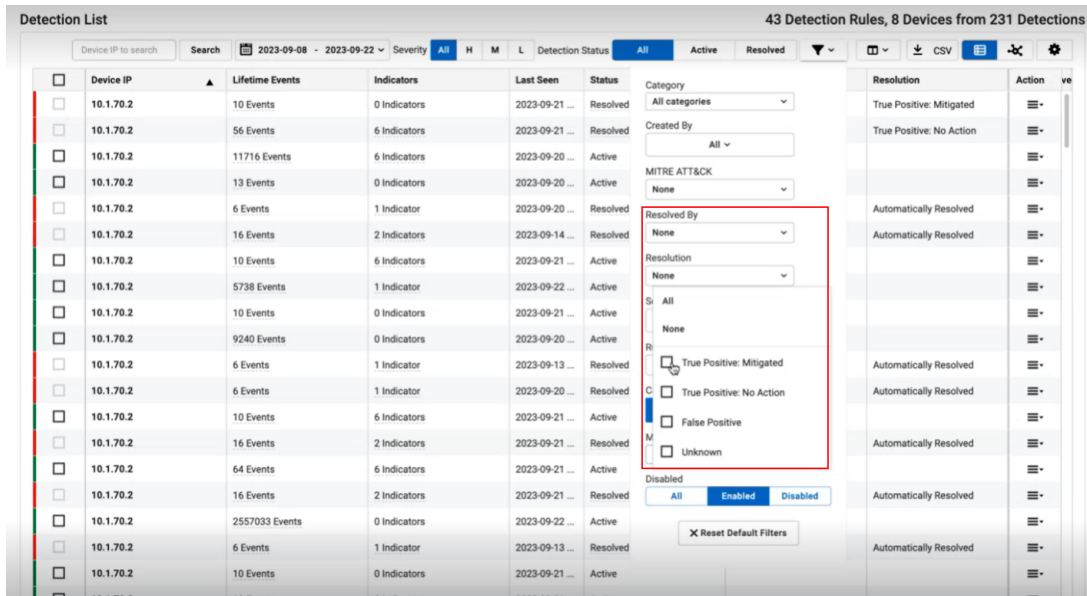
Processor(s): Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz
Number of Cores: 4
Total Memory: 3.759 GB
Total Disk Space: 77.679 GB

Software

Operation System: Ubuntu 16.04.6 LTS
BRO Version: 2.5.2-85
Suricata Version: 4.0.0-dev (rev 49)
Sensor Version:

Detection list filters

Two new filters were added to the detections table: Resolved by and Resolution.



Detection List 43 Detection Rules, 8 Devices from 231 Detections

Device IP	Lifetime Events	Indicators	Last Seen	Status	Category	Resolution	Action
10.1.70.2	10 Events	0 Indicators	2023-09-21 ...	Resolved	All categories	True Positive: Mitigated	
10.1.70.2	56 Events	6 Indicators	2023-09-21 ...	Resolved	Created By	True Positive: No Action	
10.1.70.2	11716 Events	6 Indicators	2023-09-20 ...	Active	MITRE ATT&CK	Automatically Resolved	
10.1.70.2	13 Events	0 Indicators	2023-09-20 ...	Active	None	Automatically Resolved	
10.1.70.2	6 Events	1 Indicator	2023-09-20 ...	Resolved	Resolved By	Automatically Resolved	
10.1.70.2	16 Events	2 Indicators	2023-09-14 ...	Resolved	None	Automatically Resolved	
10.1.70.2	10 Events	6 Indicators	2023-09-21 ...	Active	Resolution		
10.1.70.2	5738 Events	1 Indicator	2023-09-22 ...	Active	None		
10.1.70.2	10 Events	0 Indicators	2023-09-21 ...	Active	All		
10.1.70.2	9240 Events	0 Indicators	2023-09-20 ...	Active	None		
10.1.70.2	6 Events	1 Indicator	2023-09-13 ...	Resolved	True Positive: Mitigated	Automatically Resolved	
10.1.70.2	6 Events	1 Indicator	2023-09-20 ...	Resolved	True Positive: No Action	Automatically Resolved	
10.1.70.2	10 Events	6 Indicators	2023-09-21 ...	Active	False Positive		
10.1.70.2	16 Events	2 Indicators	2023-09-21 ...	Resolved	Unknown	Automatically Resolved	
10.1.70.2	64 Events	6 Indicators	2023-09-21 ...	Active	Disabled	Automatically Resolved	
10.1.70.2	16 Events	2 Indicators	2023-09-21 ...	Resolved	All	Automatically Resolved	
10.1.70.2	2557033 Events	0 Indicators	2023-09-22 ...	Active	Enabled	Automatically Resolved	
10.1.70.2	6 Events	1 Indicator	2023-09-13 ...	Resolved	Disabled	Automatically Resolved	
10.1.70.2	10 Events	0 Indicators	2023-09-21 ...	Active	Reset Default Filters		

Other improvements

- All columns in tables are sortable.

13 September 2023 version 2023.8.1

FortiNDR Cloud 2023.8.1 includes bug fixes, but no new features. See [Resolved Issues](#) on page 51.

21 August 2023 version 2023.8

- New functionality
 - Sensor email alerts
- Enhanced functionality
 - Malicious PE file observation
 - Other Enhancements
- Resolved Issues

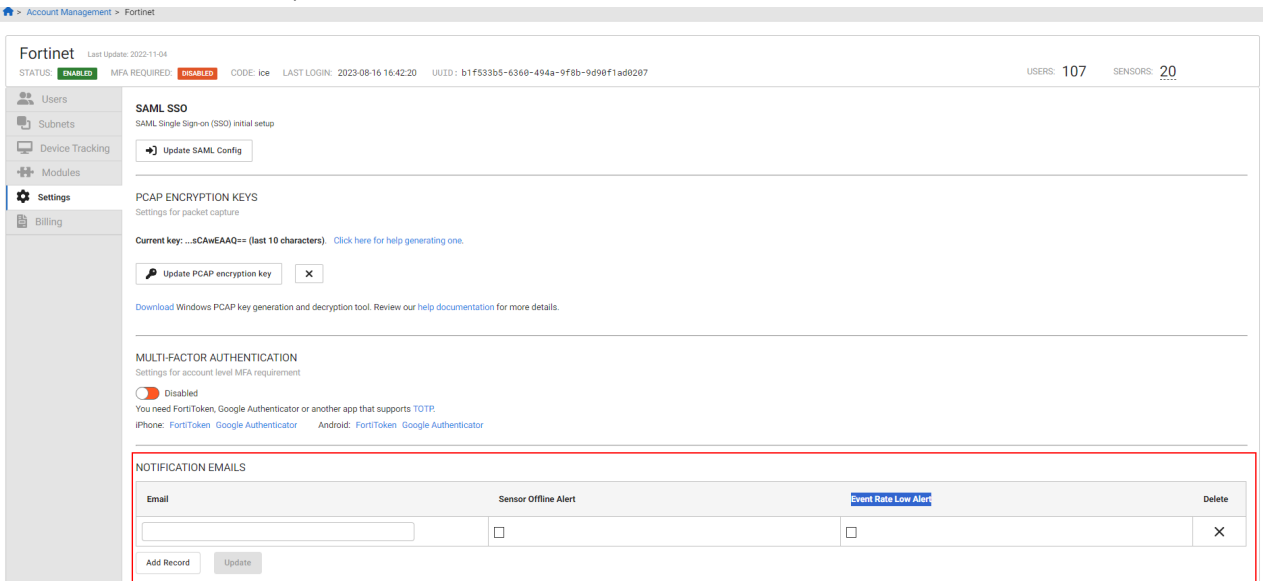
New functionality

Sensor email alerts

Administrators can now create email notifications alerts when a sensor is offline or the event rate is low.

To create a sensor email alert:

1. Go to *Account Management > Settings*.
2. Under *Notification Emails*, click *Add Record*.

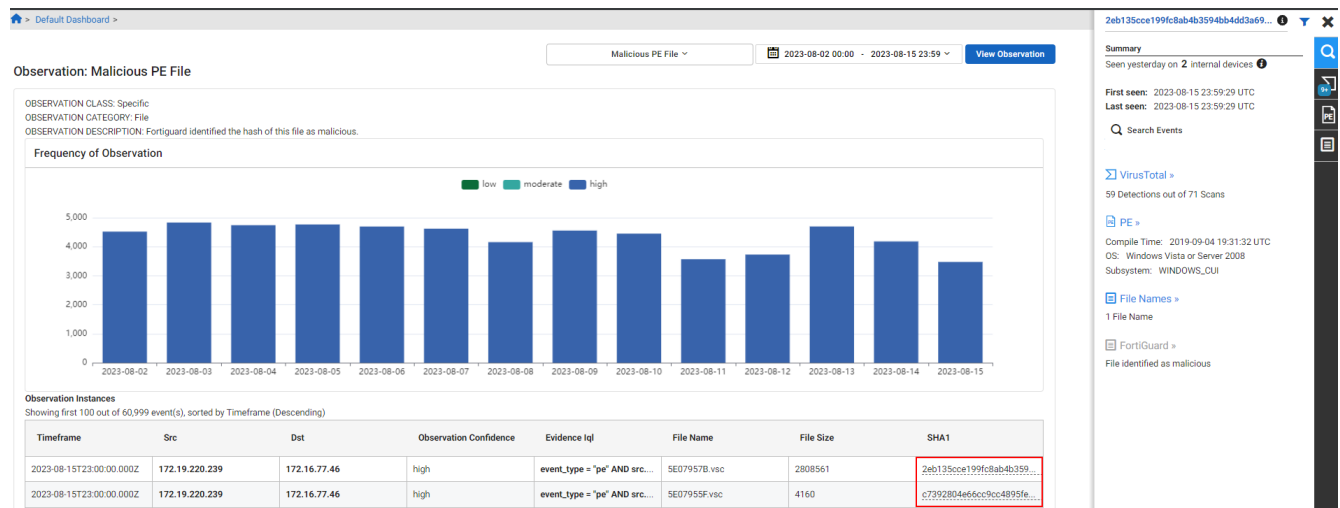


3. In the *Email* field, enter a recipient's email address.
4. Select *Sensor Offline Alert* and/or *Event Rate Low Alert*.
5. Click *Update*.

Enhanced functionality

Malicious PE file observation

The *Sha1* field is now linked to the Entity Panel.



Other Enhancements

- You can now sort the *Detections Table* by *Resolution*.
- In *Search Timeline*, you can use the *Date Picker* to search any time period within the last 365 days as long as it is limited to seven days.

31 July 2023 version 2023.7

- New Functionality
 - Investigate FortiEDR Host
 - Malicious files flag
 - Parent/Child Account Bandwidth View
- Resolved issues

New Functionality

Investigate FortiEDR Host

The *Entity Panel* now links directly to a specific host in FortiEDR.

To view the FortiEDR host:

1. Click the *FortiEDR* link in the Entity Panel.

Investigation Results | [Refresh](#) | 172.16.92.89

src.ip = '...' or dst.ip = '...' Actions 2023-06-27 15:58 (UTC) - 2023-07-27 15:58 (UTC)

Showing first 100 events, sorted by timestamp descending

timestamp	type	src.ge...	src.ge...	src.ge...	src.ge...	src.ge...	src.user...	src.hostn...	dst	dst.ip
2023-07-27 13:45:03 Z	FLOW									172.1
2023-07-27 13:30:04 Z	FLOW									172.1
2023-07-27 13:15:04 Z	FLOW									172.1
2023-07-27 13:00:04 Z	FLOW									172.1
2023-07-27 12:45:04 Z	FLOW									172.1
2023-07-27 12:30:03 Z	FLOW									172.1
2023-07-27 12:15:04 Z	FLOW									172.1
2023-07-27 12:00:04 Z	FLOW									172.1
2023-07-27 11:45:03 Z	FLOW									172.1
2023-07-27 11:30:04 Z	FLOW									172.1
2023-07-27 11:15:03 Z	FLOW									172.1
2023-07-27 11:00:04 Z	FLOW									172.1
2023-07-27 10:45:04 Z	FLOW									172.1

Entity Panel Summary:

- Connections from 0 internal devices yesterday
- First seen: 2023-05-03 17:30:04 UTC
- Last seen: 2023-07-27 15:45:04 UTC
- Annotations:
- WHOIS: Network Age: 29y 141d, Created: 1994-03-15 00:00:00 UTC, Updated: 2013-08-30 00:00:00 UTC
- VirusTotal: 2 Resolved Urls
- FortiEDR**: installed - 1901 events found
- PDNS: No PDNS Results Found
- Detections: No Detections Found
- Accounts

2. Click *Investigate* to open FortiEDR. If you are not logged into FortiEDR you will be redirected to login page.

Investigation Results | [Refresh](#) | 172.16.92.89

src.ip = '...' or dst.ip = '...' Actions 2023-06-27 15:58 (UTC) - 2023-07-27 15:58 (UTC)

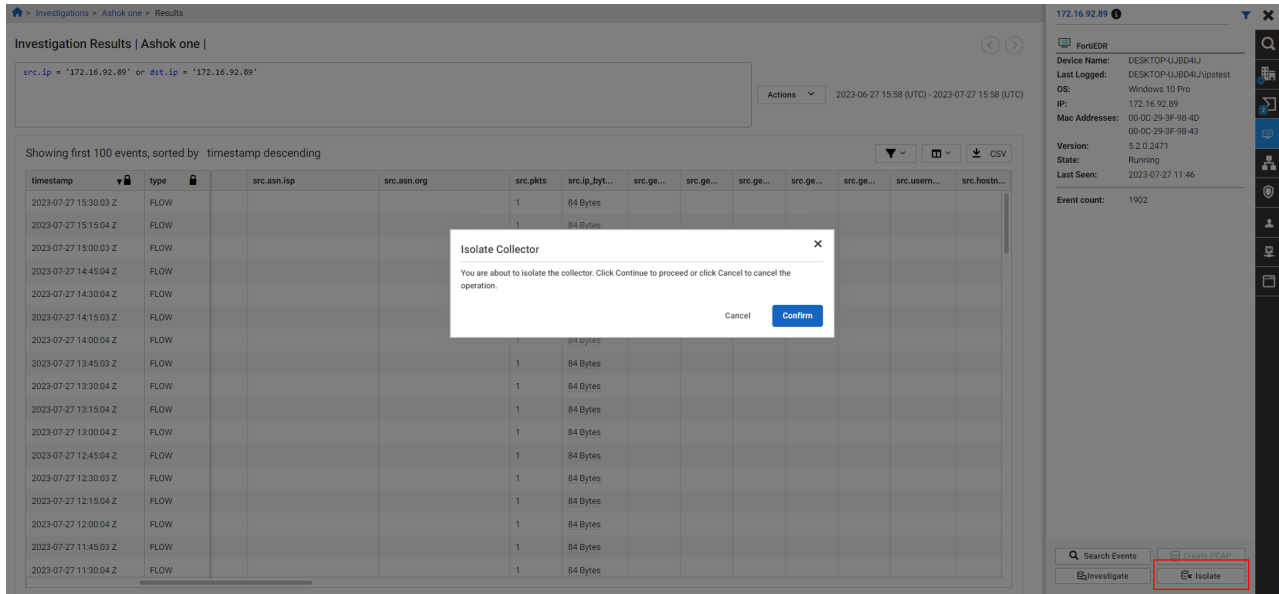
Showing first 100 events, sorted by timestamp descending

timestamp	type	src.ge...	src.ge...	src.ge...	src.ge...	src.ge...	src.user...	src.hostn...	dst	dst.ip
2023-07-27 13:45:03 Z	FLOW									172.1
2023-07-27 13:30:04 Z	FLOW									172.1
2023-07-27 13:15:04 Z	FLOW									172.1
2023-07-27 13:00:04 Z	FLOW									172.1
2023-07-27 12:45:04 Z	FLOW									172.1
2023-07-27 12:30:03 Z	FLOW									172.1
2023-07-27 12:15:04 Z	FLOW									172.1
2023-07-27 12:00:04 Z	FLOW									172.1
2023-07-27 11:45:03 Z	FLOW									172.1
2023-07-27 11:30:04 Z	FLOW									172.1
2023-07-27 11:15:03 Z	FLOW									172.1
2023-07-27 11:00:04 Z	FLOW									172.1
2023-07-27 10:45:04 Z	FLOW									172.1

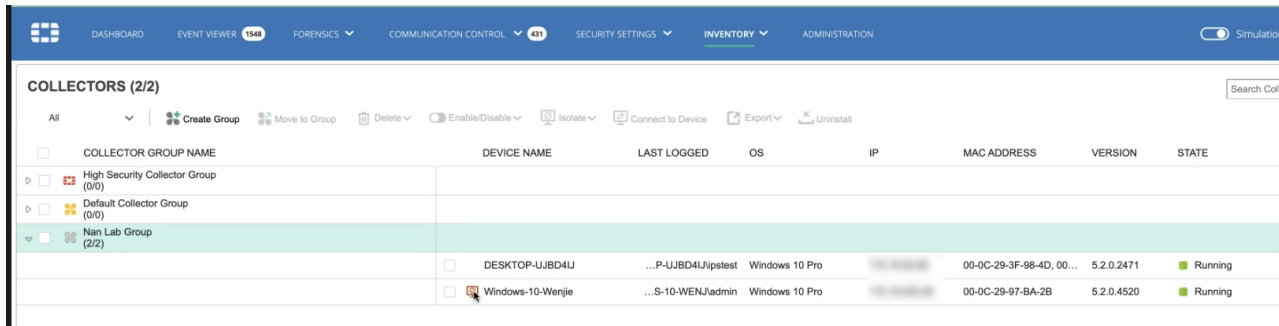
Entity Panel Summary:

- Device Name: DESKTOP-UJBD4IJ
- Last Logged: DESKTOP-UJBD4IJ\ipstest
- OS: Windows 10 Pro
- IP: ...
- Mac Addresses: ...
- Version: 5.2.0.2471
- State: Running
- Last Seen: 2023-07-27 09:13
- Event count: 1901
- Investigate**
- Isolate

3. Click *Isolate* to isolate the collector.



4. FortiEDR displays the isolated collector.

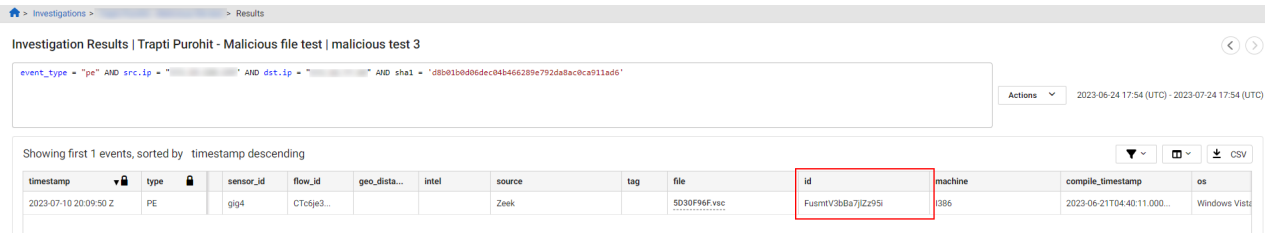


Malicious files flag

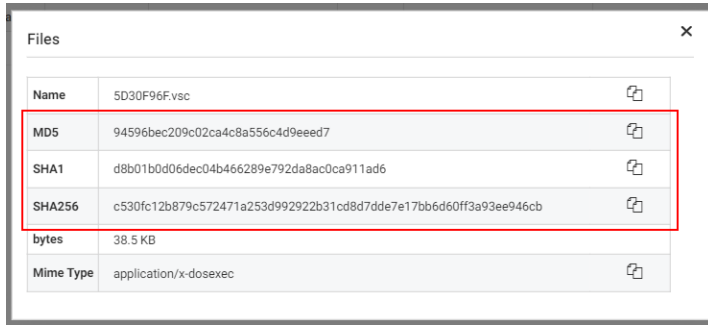
The *Entity Panel* now flags malicious files with FortiGuard.

To view the Malicious flag:

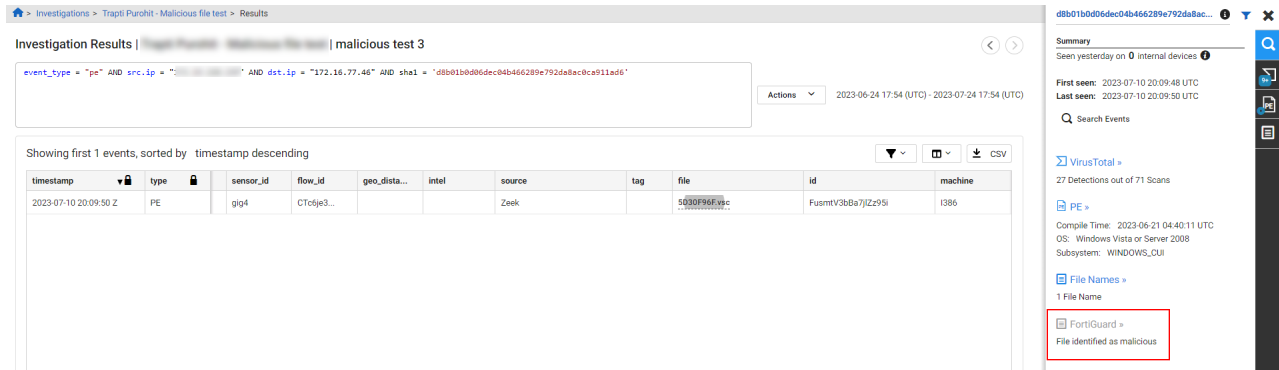
1. In the investigation results, click the link in the *File* column.



2. Click a link in the *Files* dialog.



3. The flag appears in the *FortiGuard* section.

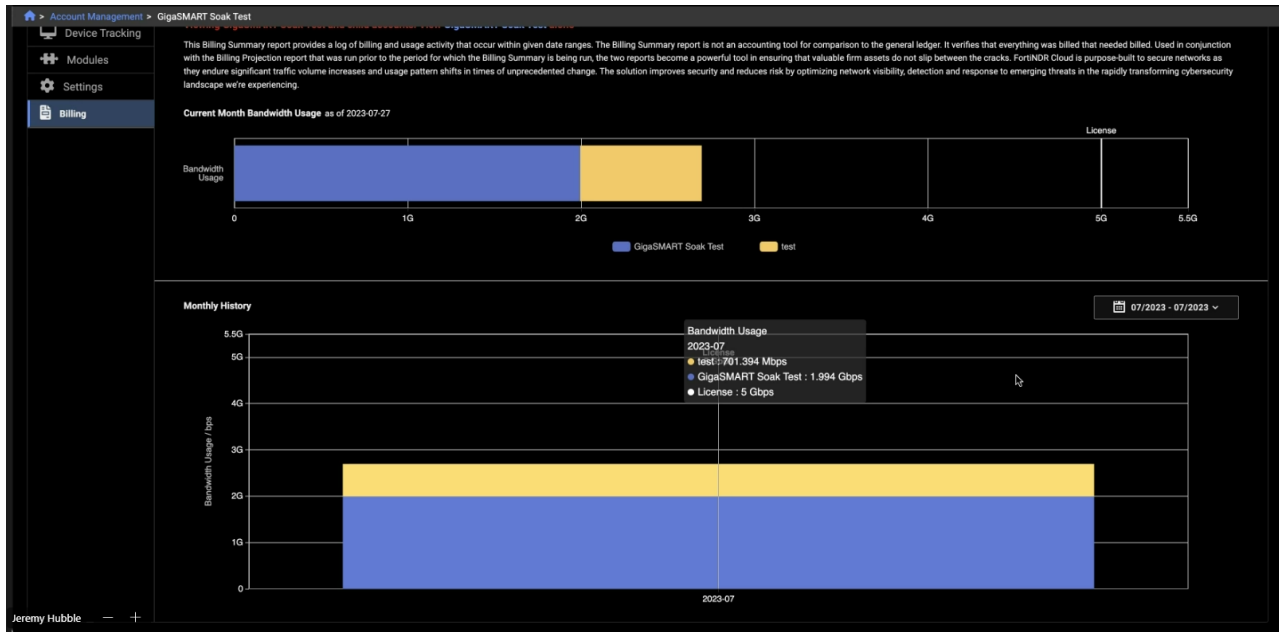


Parent/Child Account Bandwidth View

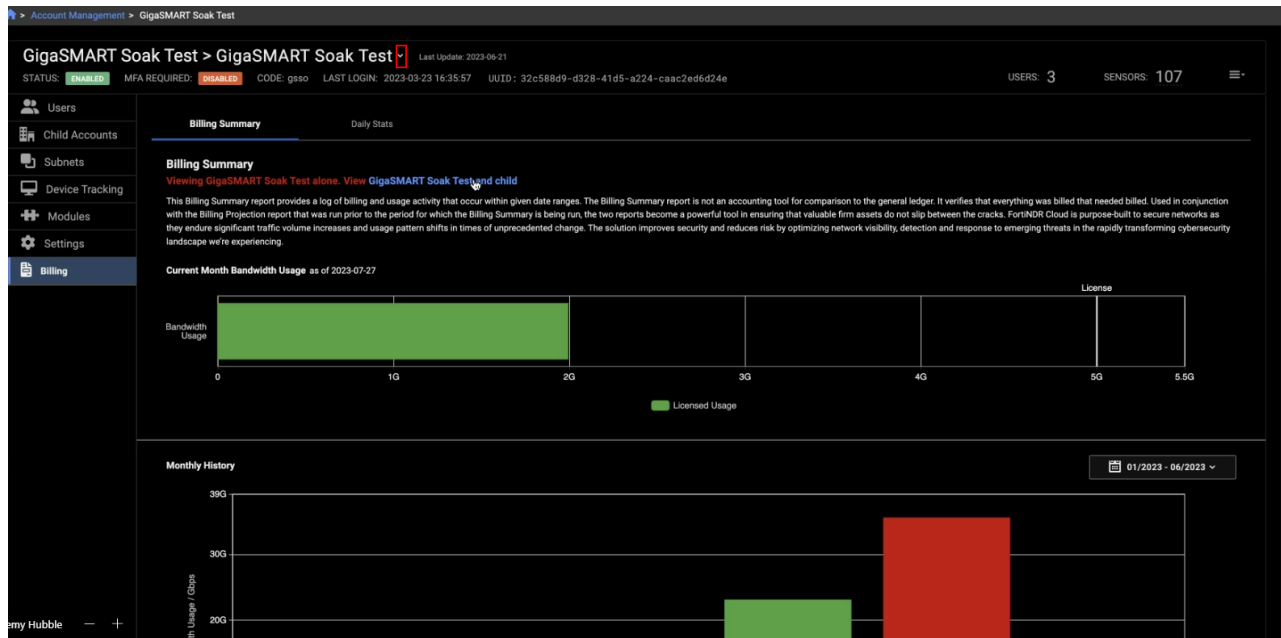
The *Account Management* page now displays the total bandwidth used by both parent and child accounts.

To view the *Parent/Child Account Bandwidth*:

1. Go to *Account Management > Billing*. The Parent/Child bandwidth is displayed.



2. Click the toggle to view only the parent account.



3. You can also view the usage for a previous month in the billing cycle.



17 July 2023 version 2023.6.1

FortiNDR Cloud 2023.6.1 includes bug fixes, but no new features. See [Resolved Issues](#) on page 51.

26 June 2023 version 2023.6

- New Functionality
 - FortiEDR integration
- Enhanced functionality
 - Pivot to Detections Table from the default dashboard
 - Enhanced date filtering
 - Enhanced tagging
 - GUI improvements: Detections Table
- New detection rules and observations

New Functionality

FortiEDR integration

Integration with FortiEDR is available and can be enabled from the *Account Management* page in the *Modules* tab. Once the integration is enabled, you can view the FortiEDR information in the *Entity Panel* from any events table in the portal.

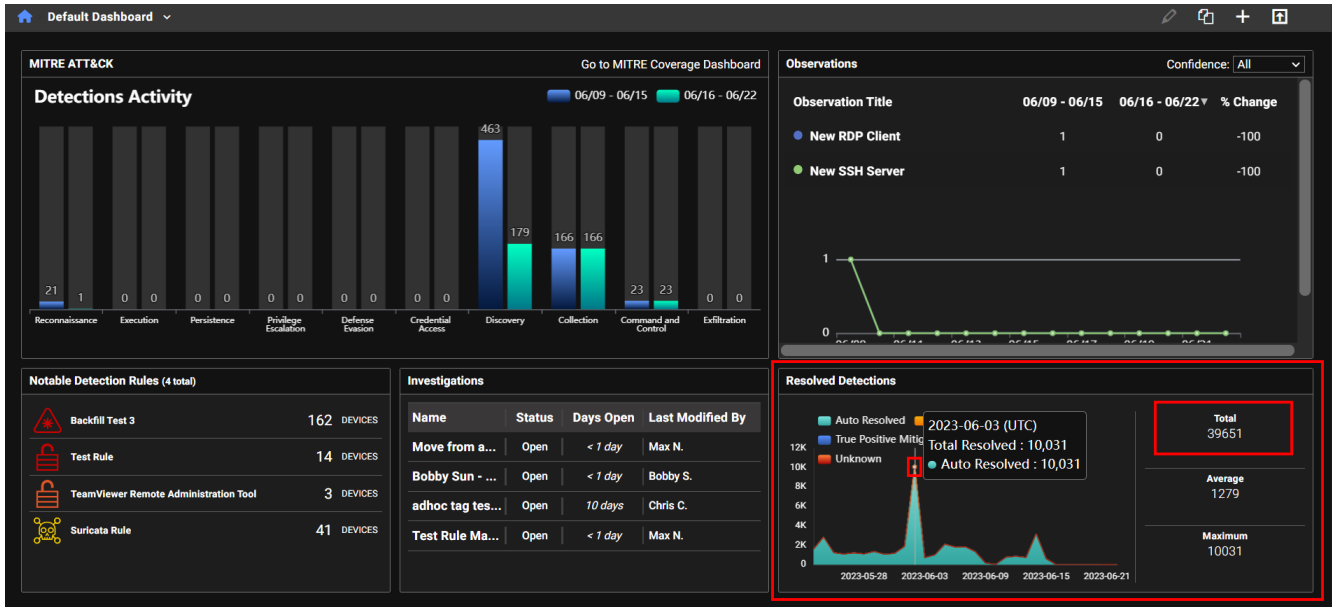
The screenshot displays the 'Investigation Results' page for 'Edmond Lau | FortiEDR UAT IPs'. The main table shows the first 100 events, sorted by timestamp descending. The table has columns for timestamp, type, src.user..., src.hostn..., dst, dst.ip, dst.port, and dst.internal. The 'dst' column is highlighted with a red box. The summary panel on the right shows details for IP 172.16.92.89, including connection counts, first/last seen times, annotations, WHOIS information, VirusTotal results, and PDNS results. The 'FortiEDR' status is highlighted with a red box, showing 'Installed - 1 collector found'.

timestamp	type	src.user...	src.hostn...	dst	dst.ip	dst.port	dst.internal
2023-06-02 04:45:04 Z	FLOW			🏠		0	True
2023-06-02 04:30:04 Z	FLOW			🏠		0	True
2023-06-02 04:15:04 Z	FLOW			🏠		0	True
2023-06-02 04:00:03 Z	FLOW			🏠		0	True
2023-06-02 03:45:04 Z	FLOW			🏠		0	True
2023-06-02 03:30:03 Z	FLOW			🏠		0	True
2023-06-02 03:15:04 Z	FLOW			🏠		0	True
2023-06-02 03:00:03 Z	FLOW			🏠		0	True
2023-06-02 02:45:04 Z	FLOW			🏠		0	True
2023-06-02 02:30:04 Z	FLOW			🏠		0	True

Enhanced functionality

Pivot to Detections Table from the default dashboard

In the *Resolved Detections* widget, you can click a data point in the chart or the *Total* detections to view all the resolved detections in the *Detections Table*.



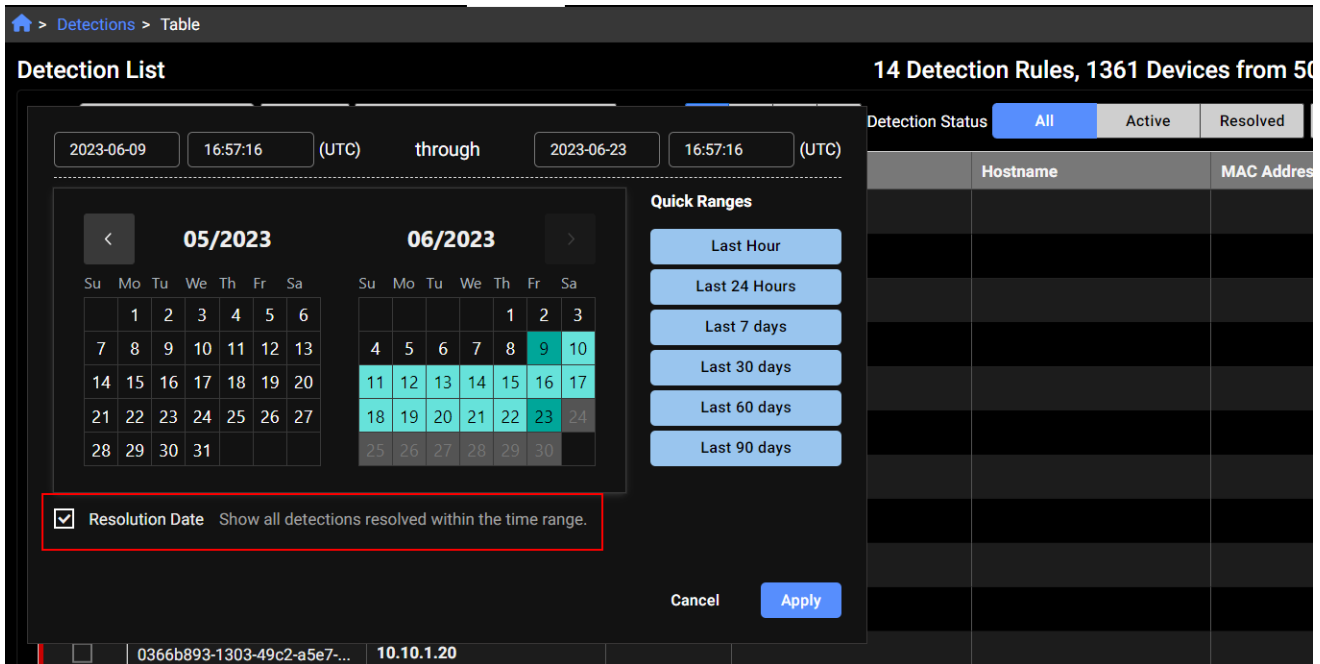
The *Detections Table* displays the resolved detections reported in the widget.

The screenshot shows the 'Detections > Table' view. At the top, it indicates '17 Detection Rules, 283 Devices from 5000 Detections (out of 39652 total Detections)'. Below this is a table with the following columns: Detection UUID, Device IP, DHCP Ho..., Username, Hostname, MAC Address, Lifetime Events, and Action. The first four rows of data are visible:

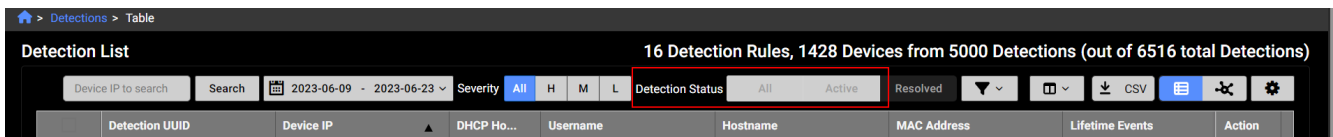
Detection UUID	Device IP	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Action
7f65fb64-42ad-49b3-bec7-3...						293 Events	
c088cb93-989a-42a0-80fd...						2 Events	
808329ec-306a-461e-a7a9...						4 Events	
7b4bd016-9cb7-4f32-81ef-3...						4 Events	

Enhanced date filtering

The date filter now includes an option to only show resolved detections within the selected time range.

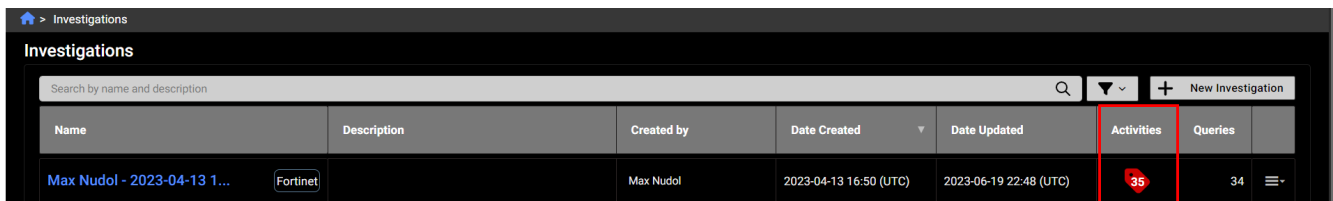


Enabling this option will disable the buttons in the Severity filter until you disable it again.

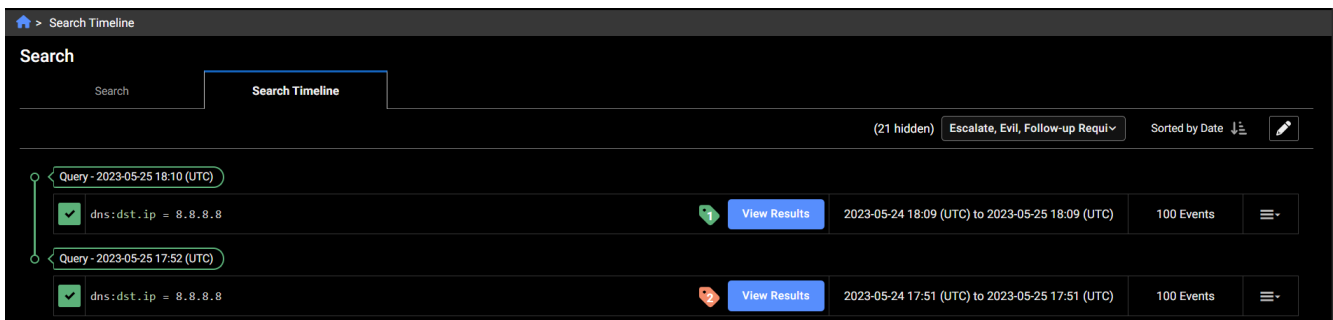


Enhanced tagging

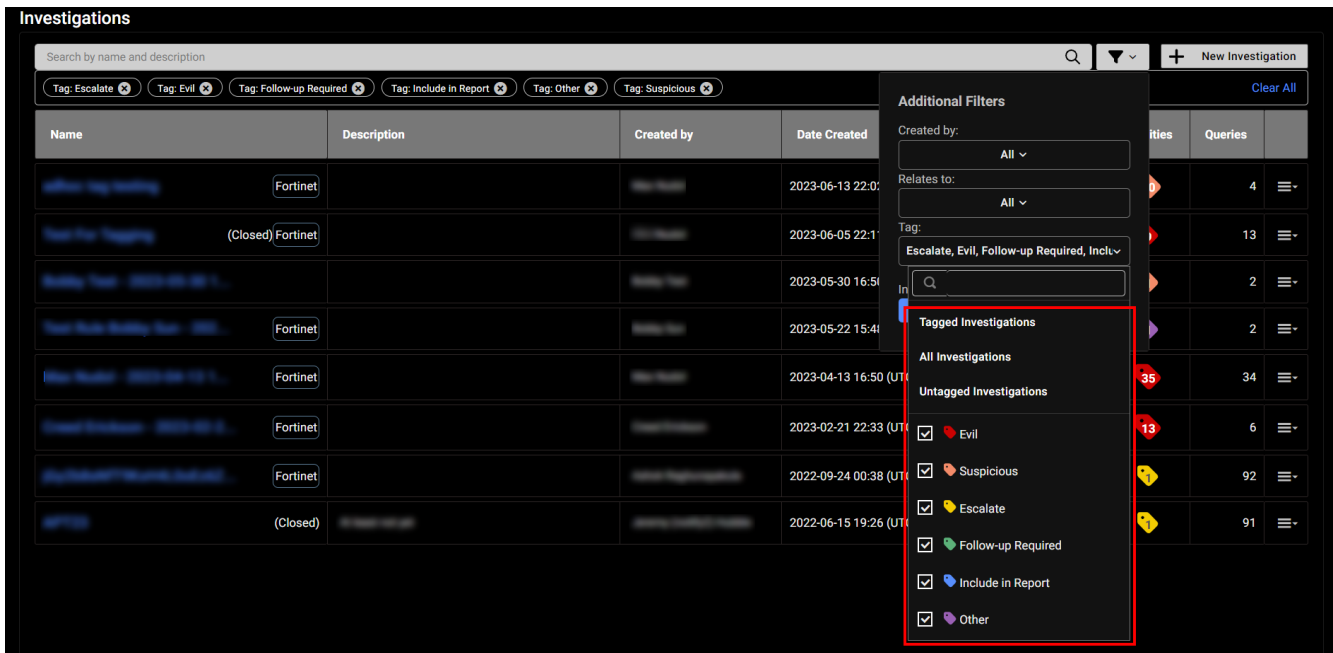
A new *Activities* column has been added to the *Investigate* tab. This column indicates the investigation was tagged, as well the number of tags, and the tag label.



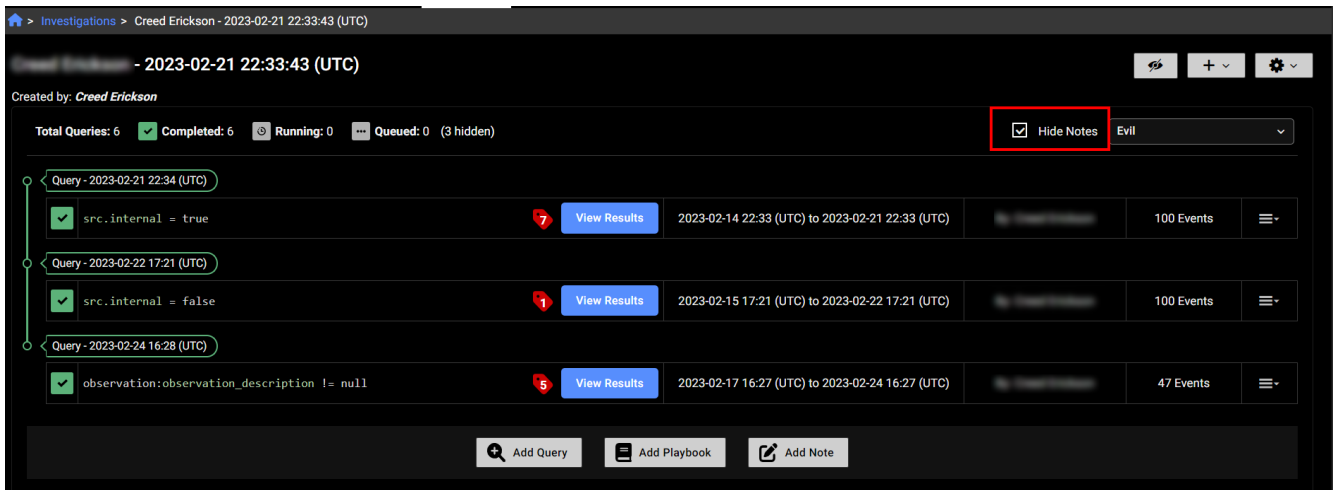
Tags are also visible in the *Search Timeline* tab.



You can filter the page to show only tagged Investigations, or tagged investigations by tag label.



As you drill down in the investigation, you are able to hide notes.



GUI improvements: Detections Table

A color-coded bar has been added to the left side of the *Detections Table*. A red bar indicates Resolved events and a green bar indicates Active events.

Detection UUID	Device IP	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Action
d0cc4097-866e-44f9-b15a-...						5 Events	
e7b153ca-07cd-46ee-96f4-5...						398 Events	
ec238bd7-a58a-40dd-8309-...						1500 Events	
f1197e80-2691-4d83-978e-...						391164 Events	
00cdf31-0c22-444a-b184-c...						40 Events	
026fcb30-2159-4dbd-bb7b-...						5 Events	
5213f110-50ec-4689-8932-...						2379 Events	

New detection rules and observations

The following table lists the new detections rules and observations in FortiNDR Cloud:

Name	Analytic Type	Description
Unusually High Bandwidth RDP Activity	Observation	This observation identifies a higher-than-normal volume of data exiting the device the user RDP'd into. This could indicate a user is trying to extract information from the system in an abusive use case.

12 June 2023 version 2023.5.1

FortiNDR Cloud 2023.5.1 includes bug fixes, but no new features. See [Resolved Issues on page 51](#).

25 May 2023 version 2023.5.0

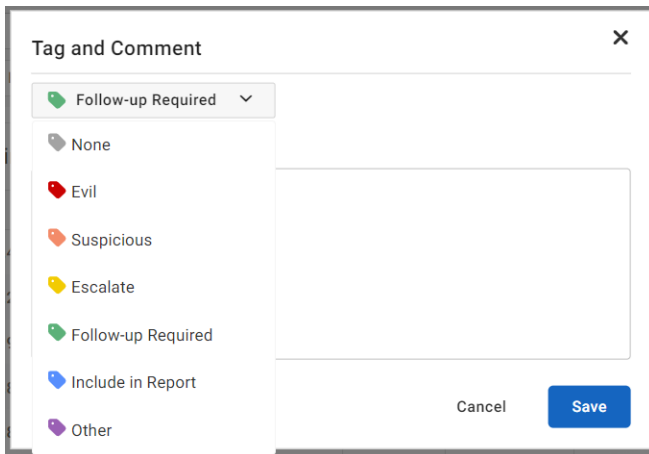
- New Functionality
 - Tag and comment events
- Improved Functionality
 - FortiNDR Cloud Sensor v1.9.0
- Resolved Issues

New Functionality

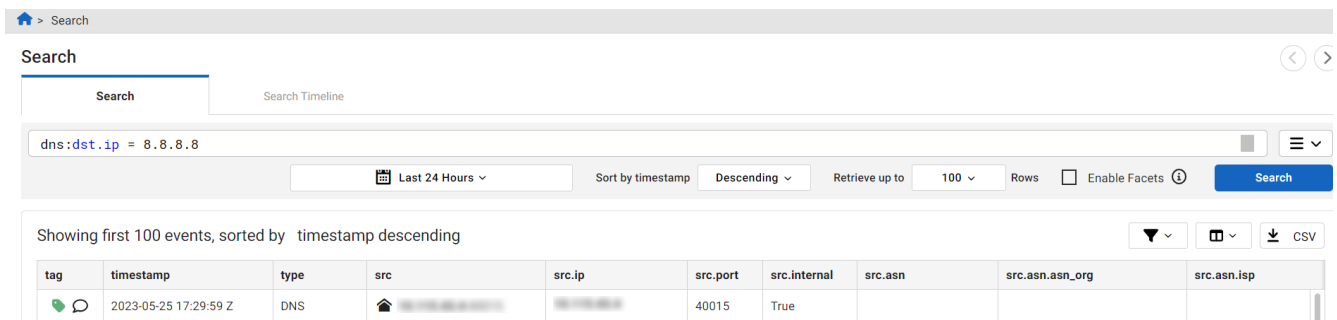
Tag and comment events

You can communicate with other members of the security team by adding a tag to an event in an investigation. The new Tags column is available from the investigation results and *Search Timeline* modules. To tag an event,

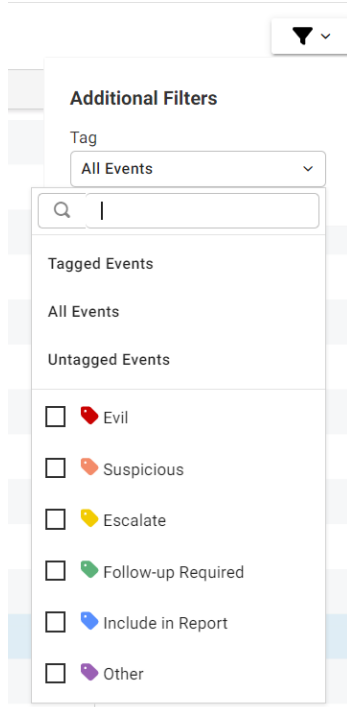
click the *Tag* column next to the event to open the *Tag and Comment* dialog.



After the tag and comment are saved, an icon appears in the *Tag* column informing other members of team further action is required.



You can also search for a tag using the *Additional Filters* dropdown.



Improved Functionality

FortiNDR Cloud Sensor v1.9.0

- The FortiNDR Cloud sensor image has been updated to version 1.9.0. For more information, see [FortiNDR Cloud sensor release notes](#).

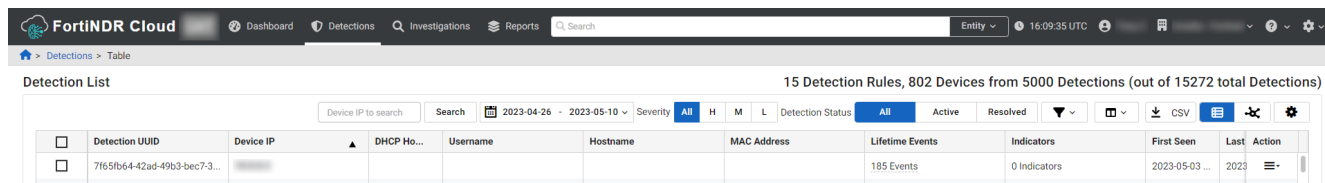
15 May 2023 version 2023.4.1

- Improved functionality
 - Detections table
- Resolved Issues

Improved functionality

Detections table

- The *Visualizer* view was added to the toolbar in the *Detections Table*.
- The total number of detections is displayed in the banner above the *Detections Table* in both *Visualizer* and *Table* views. This is useful when there are more detections that are visible in the view.



24 April 2023 version 2023.4

- New Functionality
 - Detections table
 - Bulk Entity Export
 - Muted Devices page
- Improved Functionality
 - Enable/Disable Subscriptions
- Resolved issues

New Functionality

Detections table

The new *Detections Table* view displays the detections visible on the *MITRE ATT&CK* dashboard widget as a filterable table. By default, the table displays detections for the last two weeks and displays information about the detection and the rule. Click the link in the *Lifetime Events* column to view related pages.

To access the *Detections Table*:

- Click a detection in the *MITRE ATT&CK* dashboard widget
- Go to *Detections > Detections Table*.

Home > Detections > Table

Detection List 1 Detection Rules | 125 Detections | 125 Devices

Device IP to search Search 2023-04-07 - 2023-04-13 Severity **All** H M L Detection Status **All** Active Resolved Filter View Refresh CSV Settings

<input type="checkbox"/>	Detection UUID	Device IP	DHCP Ho...	Username	Hostname	MAC Address	Lifetime Events	Indicators	First Seen	Last	Action
<input type="checkbox"/>	2968cac4-2096-4e71-873d-...	...					20217 Events	0 Indicators	2022-11-25 ...	2023	⋮
<input type="checkbox"/>	4fd8b470-b539-45f6-a425-b...	...					255132 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	870ab302-6e04-4916-ab49-...	...					100528 Events	0 Indicators	2022-11-25 ...	2023	⋮
<input type="checkbox"/>	69376f57-df10-4858-841f-2...	...					36 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	98923bb5-2560-409b-9a20-...	...					5948551 Events	0 Indicators	2022-11-25 ...	2023	⋮
<input type="checkbox"/>	b341207d-3889-4d78-ac8e-...	...					189567 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	ad234e8f-611c-460e-b68b-...	...					148578 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	06d816c0-aae3-443c-b886-...	...					182273 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	29893a7f-d518-477e-9473-...	...					158859 Events	0 Indicators	2022-11-29 ...	2023	⋮
<input type="checkbox"/>	126a56fc-206a-4372-802a-...	...					115210 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	8e02cc66-2cc1-4329-b492-...	...					207637 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	d2a57b8e-c228-41d4-8d59-...	...					6150116 Events	0 Indicators	2022-11-25 ...	2023	⋮
<input type="checkbox"/>	3fa76db4-6acc-49b9-a2b5-...	...					43739 Events	0 Indicators	2022-11-25 ...	2023	⋮
<input type="checkbox"/>	0c341960-d991-46a1-961e-...	...					65169 Events	0 Indicators	2022-11-25 ...	2023	⋮
<input type="checkbox"/>	6c15628d-6a05-4916-a041-...	...					390530 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	8462dee8-6534-4d88-a618-...	...					78469 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	9987703c-c012-49e0-abf0-...	...					78860 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	e80cc6eb-f7cc-43b2-8fb8-6...	...					178276 Events	0 Indicators	2022-11-28 ...	2023	⋮
<input type="checkbox"/>	3a45a306-7704-4cfe-b2e9-...	...					1127093 Events	0 Indicators	2022-11-25 ...	2023	⋮

Bulk Entity Export

The *Entity Lookup* page now supports bulk searches and exports. To use this feature, enter multiple IPs or domains in the search field separating each entity with a space. After the results are returned, you can click the *Export* button to download the data in CSV format.

Home > Investigations > Entity Lookup

Entity Lookup

12.12.12 13.13.13 13.13.13 Last 7 Days Search

Perform an entity search on the following: (ip, domain or filehash)

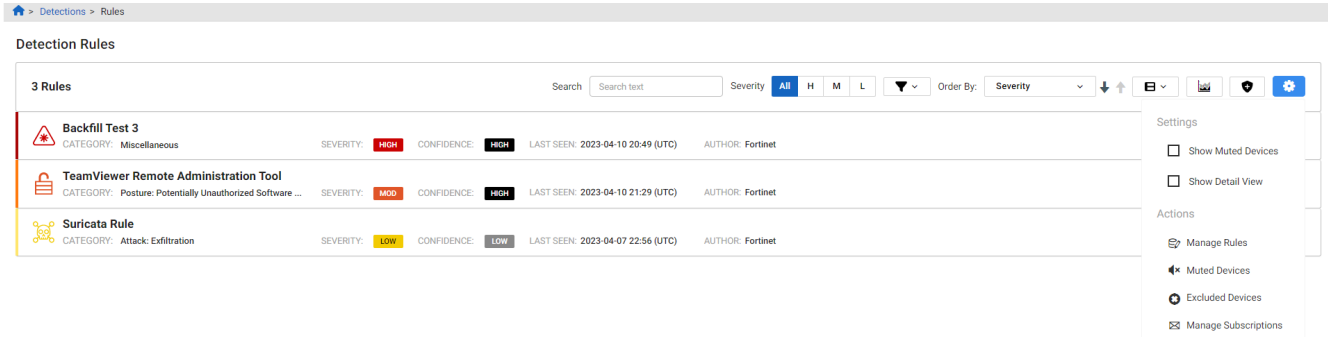
No Results Found.

No Activity Recorded CSV

Entity	Type
12.12.12	IP
13.13.13	IP

Muted Devices page

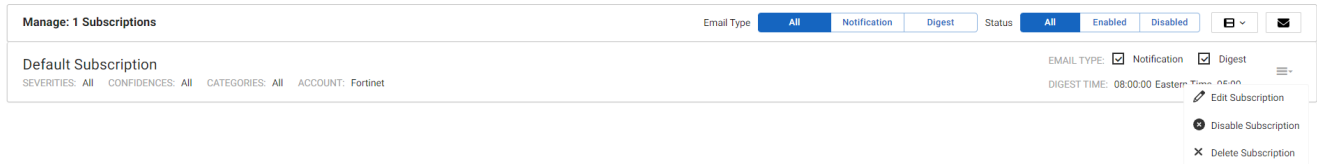
Muted devices are now displayed in their own page. To view the *Muted Devices* page, open a rule and click the *Settings* menu and then select *Muted Devices*.



Improved Functionality

Enable/Disable Subscriptions

The *My Subscriptions* page has been simplified. The *Disable* was removed from the left side of the page. To enable/disable click use the *Actions* menu at the right side of the page.



10 April 2023 version 2023.3.1

FortiNDR Cloud 2023.3.1 includes bug fixes but no new features were released.

27 Mar 2023 version 2023.3

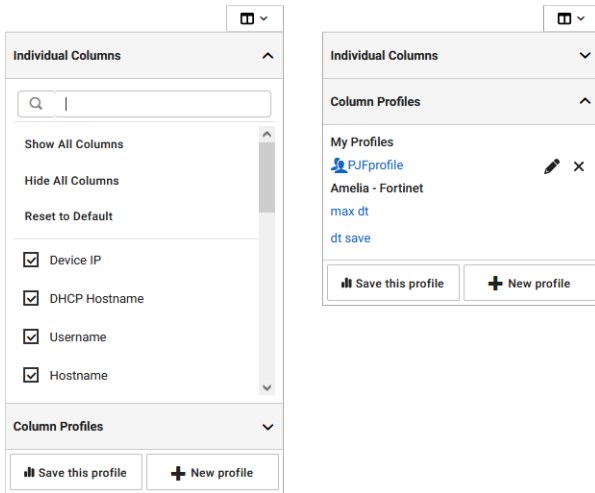
- New Functionality
 - Column profiles
 - Manage annotations
- Improved Functionality

- Observations
- MITRE ATT&CK drop-downs
- Sensor release notes
- Resolved issues

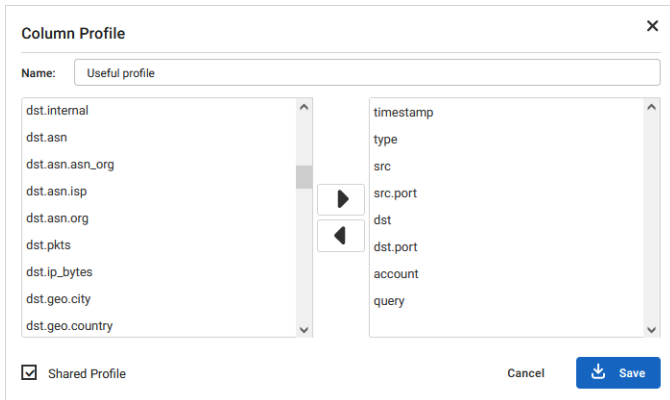
New Functionality

Column profiles

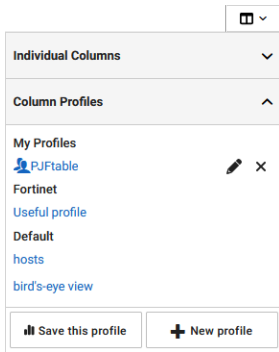
Custom column profiles can be created for any table that allows columns to be selected. When selecting the individual columns or column profile for a table, they are organized into groups.



Custom profiles can be shared with other users in your company by selecting *Shared Profile* when creating or editing a profile.

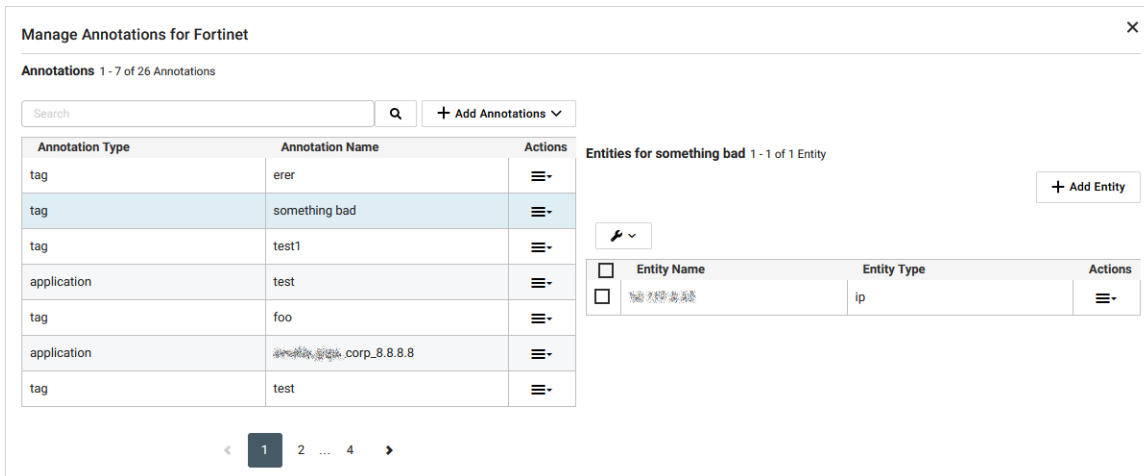
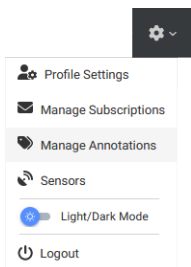


The profile will then be available to other users when they are selecting a column profile for a table.



Manage annotations

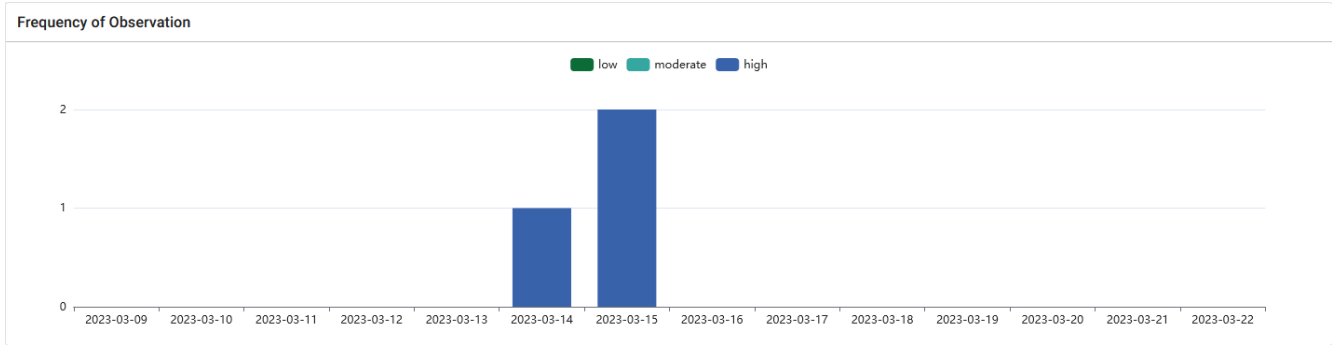
Annotations can now be accessed directly from the settings menu.



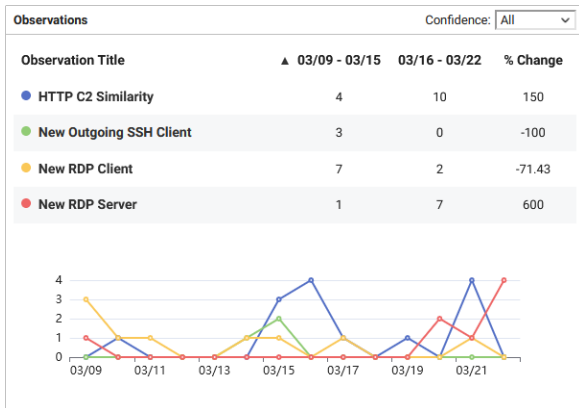
Improved Functionality

Observations

The y-axis of the Observation widget and observation details page tables no longer show decimal numbers, as all of the results are whole numbers.



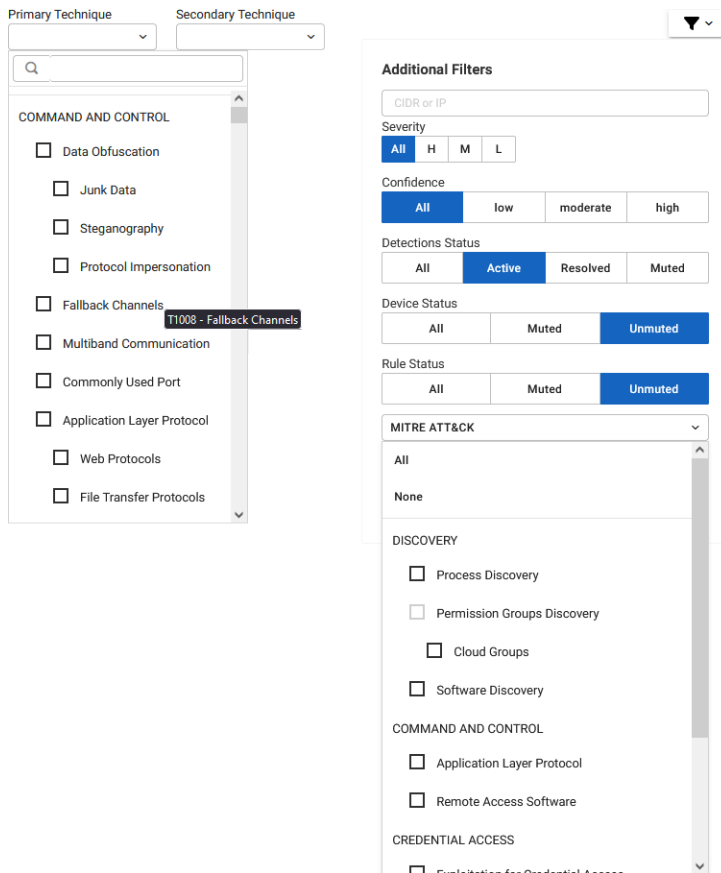
The legend is removed from the bottom of the table, and instead the colored dots are next the observation titles in the observation list.



MITRE ATT&CK drop-downs

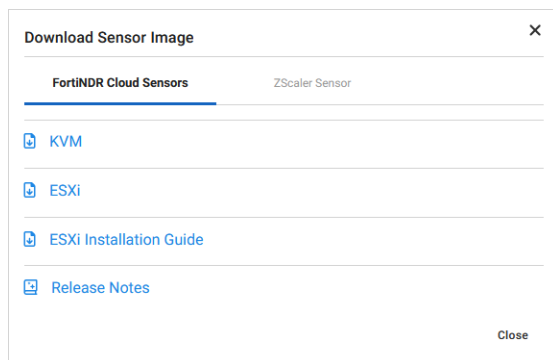
MITRE ATT&CK drop-down menus all use a tree menu to simplify selecting the requires technique or techniques. All of the techniques names are shown, and hovering over a name will show a tooltip that includes the ID and name. The MITRE ATT&CK list on the Visualizer page only shows the techniques that are present in the visualization.

The drop-downs can be searched using the ID or the name of the technique.



Sensor release notes

Sensor release notes can be accessed directly from the sensor image download page.



13 Mar 2023 version 2023.2.1

FortiNDR Cloud 2023.2.1 includes bug fixes, but no new features. See [Resolved Issues on page 51](#).

27 Feb 2023 version 2023.2

- New Functionality
 - Investigations API
 - Observation descriptions
- Improved Functionality
 - Playbook access
 - Playbook time frames
 - Impacted devices table
 - Persistent investigations table
 - Flow state pop-up
 - Default investigation names
- Discontinued Functionality
 - VPC option for new detection rules
 - Legacy account version

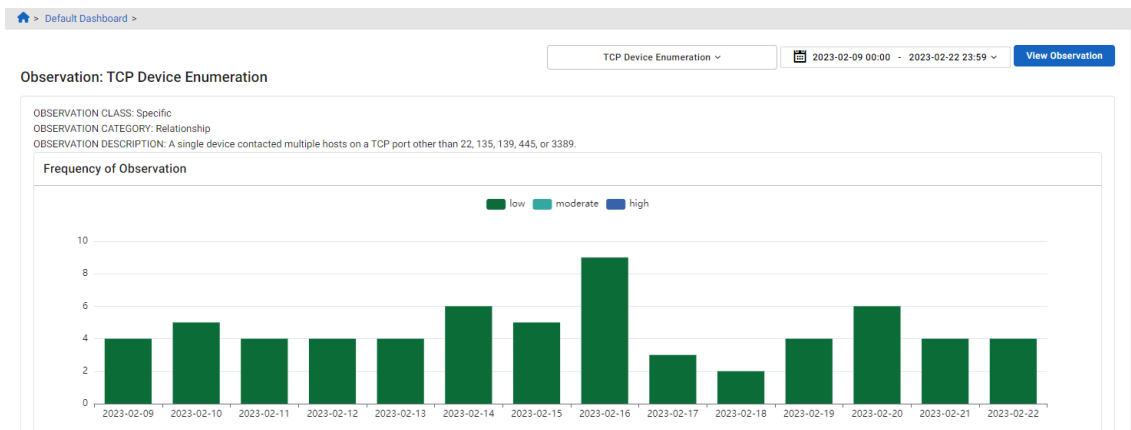
New Functionality

Investigations API

The Investigations API is a public API used to manage investigations and queries. With it, you can programmatically run queries in FortiNDR Cloud, run playbooks, and use other investigation functionality. Documentation is available upon request.

Observation descriptions

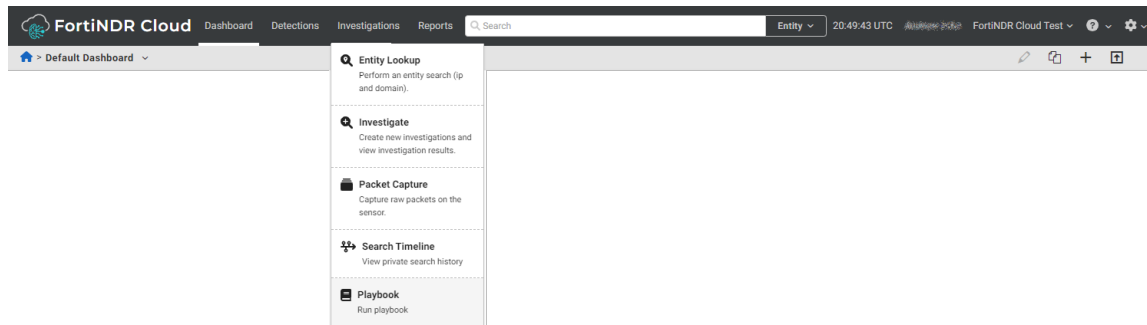
Observations include a description of the observation on the observation's detail page. The description is also available in the metastream and IQL.



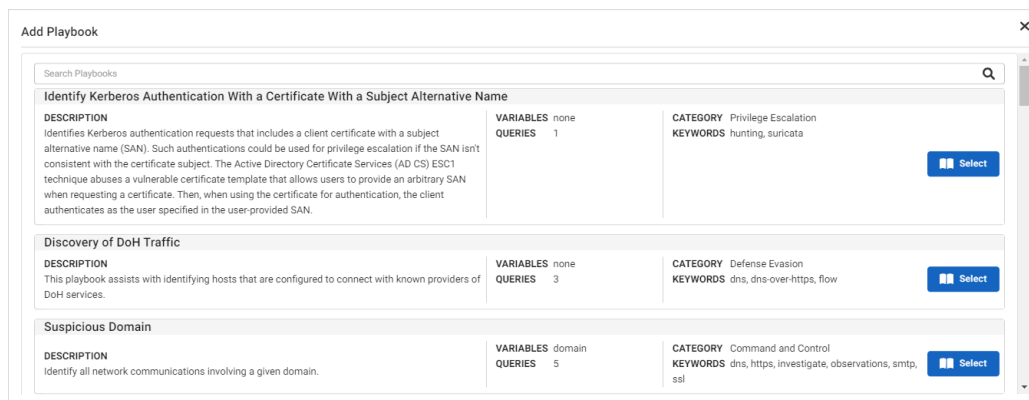
Improved Functionality

Playbook access

Playbooks can be added directly from the Investigations menu in the banner.



Clicking *Investigations > Playbook* opens the *Add Playbook* pop-up window.



Playbook time frames

The default playbook time frames are now based on the recommended time frame listed for each playbook, as opposed to defaulting to seven days for every playbook.

Add Playbook ✕

Playbook: Text4Shell Hunting

DESCRIPTION
This playbook identifies URI patterns used in the Text4Shell exploit, outbound connections from web servers using the Java user agent and any existing text4shell Suricata signatures. 1 input variable required for the second query which should be all web server IPs.

Date Range: Enable Facets ⓘ

Variables

src.ip
Press "tab" or "enter" to add an item

Playbook Queries - 3 total

http:uri MATCHES '!(%7Bscript%3Ajavascript%7Burl%3A(%7Bdns%3Aaddress%7Bbase64Decoder%3A(%7Benv%3A)%7Dnd)%7D)' AND http:uri NOT MATCHES '!(%7Dnd)' *

src.ip in (src.ip) AND src.internal = true AND dst.internal = false AND ((user_agent MATCHES '!(%7Bjava%7D)' OR user_agent MATCHES '!(%7Bjava%7D)' OR (software_name MATCHES '!(%7Bjava%7D)' OR software_name MATCHES '!(%7Bjava%7D)' OR (headers.server MATCHES '!(%7Bjava%7D)' OR headers.server MATCHES '!(%7Bjava%7D)')) GROUP BY dst.ip, host

suricata:signature LIKE '%text4shell%' OR suricata:signature LIKE '%CVE:2022-42889%'

Create a New Investigation Add to Existing Investigation

Choose Investigation:

CATEGORY Initial Access

KEYWORDS flow, http, hunting, software, suricata

Cancel ← Back to Playbooks Run Playbook

Impacted devices table

The impacted devices table is improved.

Impacted Devices											
Signature											
Events											
Indicators											
Detections Graph											
Type a device IP to search											
Search											
▼											
📄											
📄 CSV											
<input type="checkbox"/>	Lifetime Events	MAC A...	First Seen	Last Seen	Created	Sensor Id	Status	Date Muted	Muted By	Acti...	
<input type="checkbox"/>	94 Events	84	2022-10-29 ...	2023-02-23 ...	2022-11-02 ...	chf1	Active				☰
<input type="checkbox"/>	8 Events	106	2023-02-23 ...	2023-02-23 ...	2023-02-23 ...	chf1	Active				☰
<input type="checkbox"/>	143 Events	153	2023-01-23 ...	2023-02-23 ...	2023-01-23 ...	chf1	Active				☰
<input type="checkbox"/>	100 Events	90	2022-10-27 ...	2023-02-23 ...	2022-11-02 ...	chf1	Active				☰
<input type="checkbox"/>	24 Events	144	00:10:49:...	2023-02-21 ...	2023-02-21 ...	chf1	Active				☰
<input type="checkbox"/>	106 Events	67	2022-10-28 ...	2023-02-23 ...	2022-11-02 ...	chf1	Active				☰
<input type="checkbox"/>	35 Events	69	00:10:49:...	2023-02-15 ...	2023-02-23 ...	chf1	Active				☰
<input type="checkbox"/>	134 Events	64	2023-01-17 ...	2023-02-23 ...	2023-01-17 ...	chf1	Active				☰
<input type="checkbox"/>	214 Events	56	2022-11-15 ...	2023-02-23 ...	2022-11-15 ...	chf1	Active				☰
<input type="checkbox"/>	66 Events	58	2023-01-10 ...	2023-02-23 ...	2023-01-10 ...	chf1	Active				☰

- Columns can be added to and removed from the table.
- The column order and width can be adjusted by clicking and dragging the column headers.
- Columns can be locked to the left side of the table by clicking the lock icon in the column header when hovering over the header. These column will continue to be visible when you horizontally scroll through the columns in the table. The Action column is always locked to right side of the table.
- The table is not paginated; all of the rows can be seen by scrolling down.
- The table can be sorted by left clicking on a column header. Right clicking on a column gives the options to copy the column values as a comma or newline separated list, or to hide the column.
- The table layout is saved after leaving the page, and can be reset from the column selection menu.

Impacted Devices Signature Events Indicators Detections Graph

Type a device IP to search Search [Filter] [Columns] [Export] CSV

<input type="checkbox"/>	Lifetime Events	MAC A...	First Seen	Last Seen	Created	Sensor Id	Acti...
<input type="checkbox"/>	8648 Events	.10	2022-10-27 ...	2023-02-23 23:3	2022-11-02 22:22:11 Z	chf1	[Menu]
<input type="checkbox"/>	60 Events	.12	2022-10-27 ...	2023-02-20 00:1	2022-11-02 22:22:11 Z	chf1	[Menu]
<input type="checkbox"/>	60 Events	.57	2022-10-27 ...	2023-02-20 00:3	2022-11-02 22:22:11 Z	chf1	[Menu]
<input type="checkbox"/>	68 Events	.35	2022-10-27 ...	2023-02-22 20:27:02 Z	2022-11-02 22:22:11 Z	chf1	[Menu]
<input type="checkbox"/>	60 Events	.13	2022-10-27 ...	2023-02-20 00:39:25 Z	2022-11-02 22:22:11 Z	chf1	[Menu]
<input type="checkbox"/>	60 Events	.14	2022-10-27 ...	2023-02-20 00:47:32 Z	2022-11-02 22:22:11 Z	chf1	[Menu]
<input type="checkbox"/>	70 Events	.17	2022-10-27 ...	2023-02-20 00:52:04 Z	2022-11-02 22:22:11 Z	chf1	[Menu]
<input type="checkbox"/>	60 Events	.14	2022-10-27 ...	2023-02-20 00:45:57 Z	2022-11-02 22:22:11 Z	chf1	[Menu]
<input type="checkbox"/>	59 Events	.61	2022-10-27 ...	2023-02-20 00:55:18 Z	2022-11-02 22:22:11 Z	chf1	[Menu]
<input type="checkbox"/>	60 Events	.14	2022-10-27 ...	2023-02-20 01:22:40 Z	2022-11-02 22:22:11 Z	chf1	[Menu]

Copy Values as Comma Separated
Copy Values as Newline Separated
Hide column

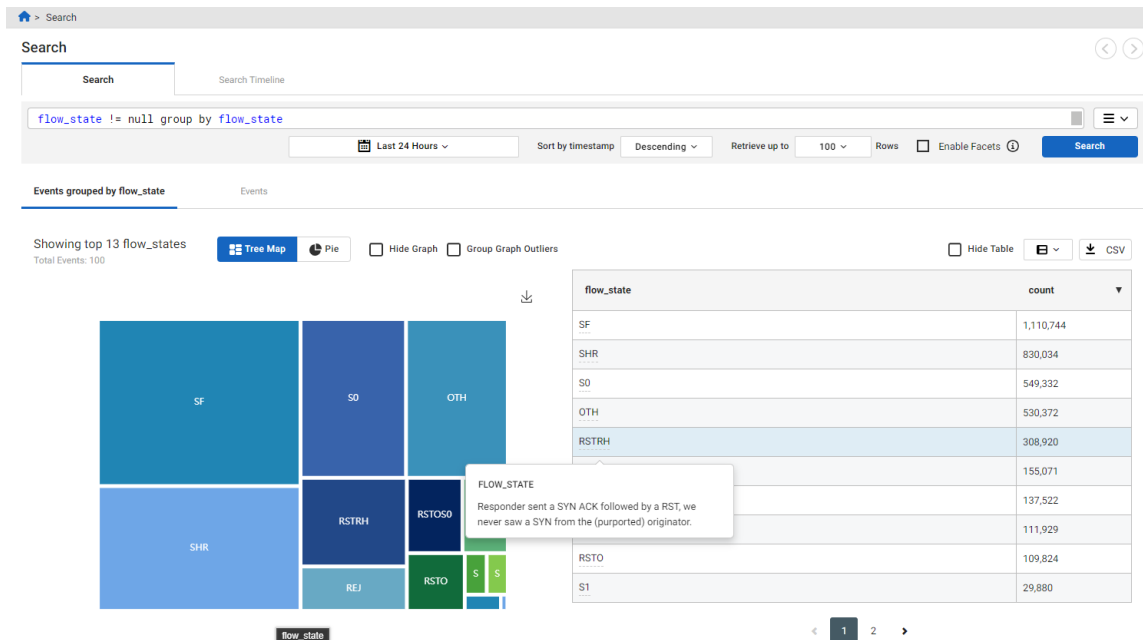
Show All Columns
Hide All Columns
Reset to Default
 Device IP
 DHCP Hostname
 Username
 Hostname
 MAC Address
 Lifetime Events
 First Seen
 Last Seen

Persistent investigations table

The selected sorting of the investigations table is persistent. For example, if you sort the table by date updated and then browse to a different page in the GUI, the investigations table will still be sorted by date updated when you return to the investigations page.

Flow state pop-up

After doing a timeline search, mousing over a flow state value shows a pop-up with the flow state details.



Search

Search Timeline

flow_state != null group by flow_state

Last 24 Hours | Sort by timestamp | Descending | Retrieve up to 100 | Rows | Enable Facets

Events grouped by flow_state

Showing first 100 events, sorted by timestamp descending

timestamp	type	flow_state	src	dst	intel	aws.action	aws.interface_id	aws.versi...	duration
2023-02-24 20:39:51 Z	FLOW	SU	192.168.1.100	192.168.1.1					< 1s
2023-02-24 20:39:51 Z	FLOW	RSTR	192.168.1.100	192.168.1.1					< 1s
2023-02-24 20:39:51 Z	FLOW	SD	192.168.1.100	192.168.1.1					< 1s
2023-02-24 20:39:51 Z	FLOW	RSTRH	192.168.1.100	192.168.1.1					< 1s
2023-02-24 20:39:51 Z	FLOW_STATE								< 1s
2023-02-24 20:39:51 Z									< 1s
2023-02-24 20:39:51 Z									< 1s
2023-02-24 20:39:51 Z	FLOW	RSTRH	192.168.1.100	192.168.1.1					< 1s
2023-02-24 20:39:51 Z	FLOW	SHR	192.168.1.100	192.168.1.1					< 1s
2023-02-24 20:39:51 Z	FLOW	RSTRH	192.168.1.100	192.168.1.1					< 1s
2023-02-24 20:39:51 Z	FLOW	SHR	192.168.1.100	192.168.1.1					< 1s

FLOW_STATE
Responder sent a SYN ACK followed by a RST, we never saw a SYN from the (purported) originator.

Default investigation names

When creating a new investigation from the Investigations list view, to prevent name collisions, instead of a default name of *New Investigation*, the default name for new investigations is now the first and last name of the user that is creating the investigation with a time and date stamp of when the investigation was created.

For example: *Philip Fry - 2023-03-01 00:17:42 (UTC)*.

Investigations

Search by name and description

Investigation name: Philip Fry - 2023-03-01 00:17:42 (UTC)

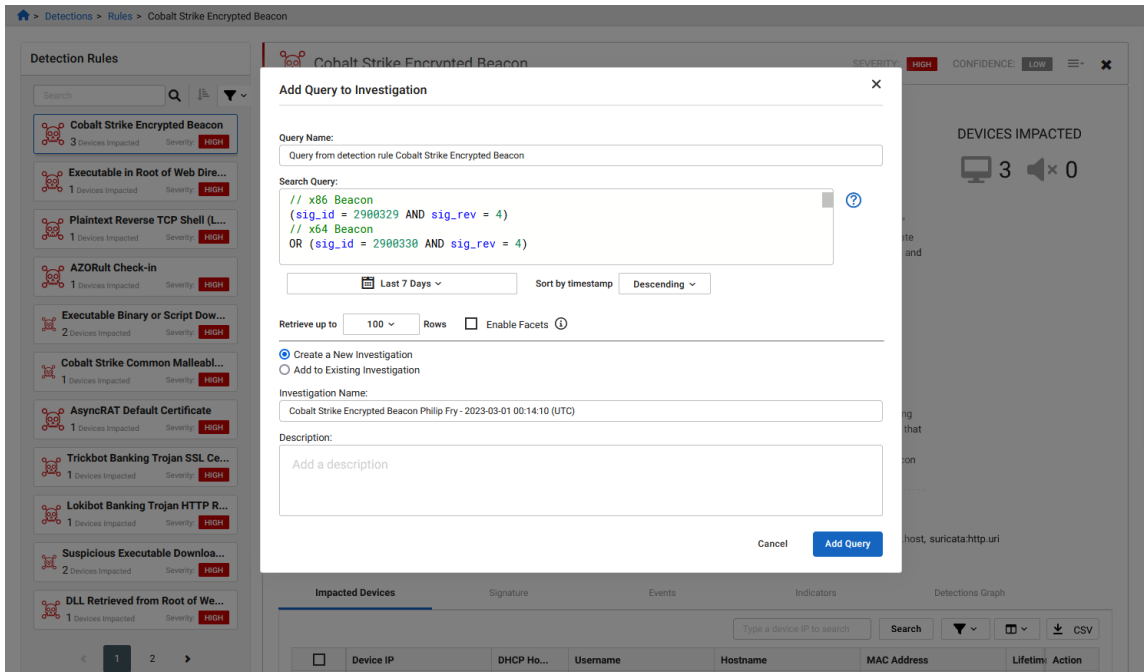
Description:

Cancel | Create Investigation

Name	Description	Created	Date Updated	Queries
Cobalt Strike - 2023-02-21 22:...	Fortinet	2023-02-21 22:33 (UTC)	2023-02-27 22:31 (UTC)	4
Service User - 2023-02-10 18:26:5...	Fortinet	2023-02-10 18:26 (UTC)	2023-02-17 15:47 (UTC)	6
dhcp Attack Rule - 20...	Fortinet	2023-02-08 23:30 (UTC)	2023-02-08 23:30 (UTC)	3
Attack Rule - 2023-02...	Fortinet	2023-02-08 23:29 (UTC)	2023-02-08 23:29 (UTC)	4
Attack Rule - 2023-02...	Fortinet	2023-02-08 22:31 (UTC)	2023-02-08 22:31 (UTC)	4

When creating a new investigation from a detection, to prevent the subject of the investigation from being truncated due to column width limitations, instead of a default name of *Investigation from detection rule <detection rule name>*, the default name for new investigations is now the name of the detection rule and the first and last name of the user that is creating the investigation with a time and date stamp of when the investigation was created.

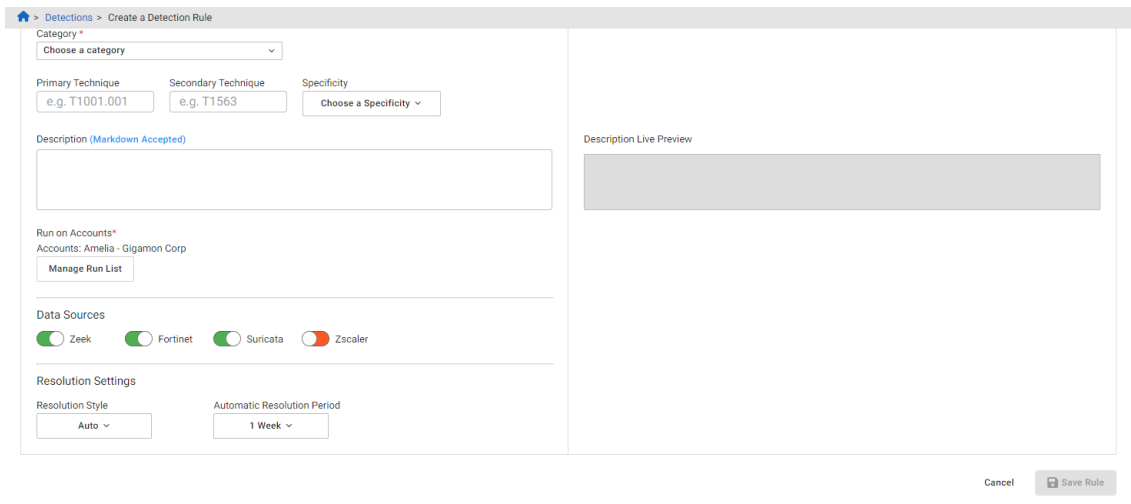
For example: *Cobalt Strike Encrypted Philip Fry - 2023-03-01 00:14:10 (UTC)*.



Discontinued Functionality

VPC option for new detection rules

When creating a new detection rule, VPC cannot be selected as a data source.



Legacy account version

When creating a new account, the FortiNDR Cloud version is set to *Modern*; *Legacy* can no longer be selected.

Create new account ✕

Account Name

Account Code

Legal Name (optional)

FortiNDR Cloud Version Modern

Data Retention 365 Days

Dashboard Retention 90 Days

Type

Cancel

07 Feb 2023 version 2023.1.1

FortiNDR Cloud 2023.1.1 released with updated Fortinet branding. No new features were released.

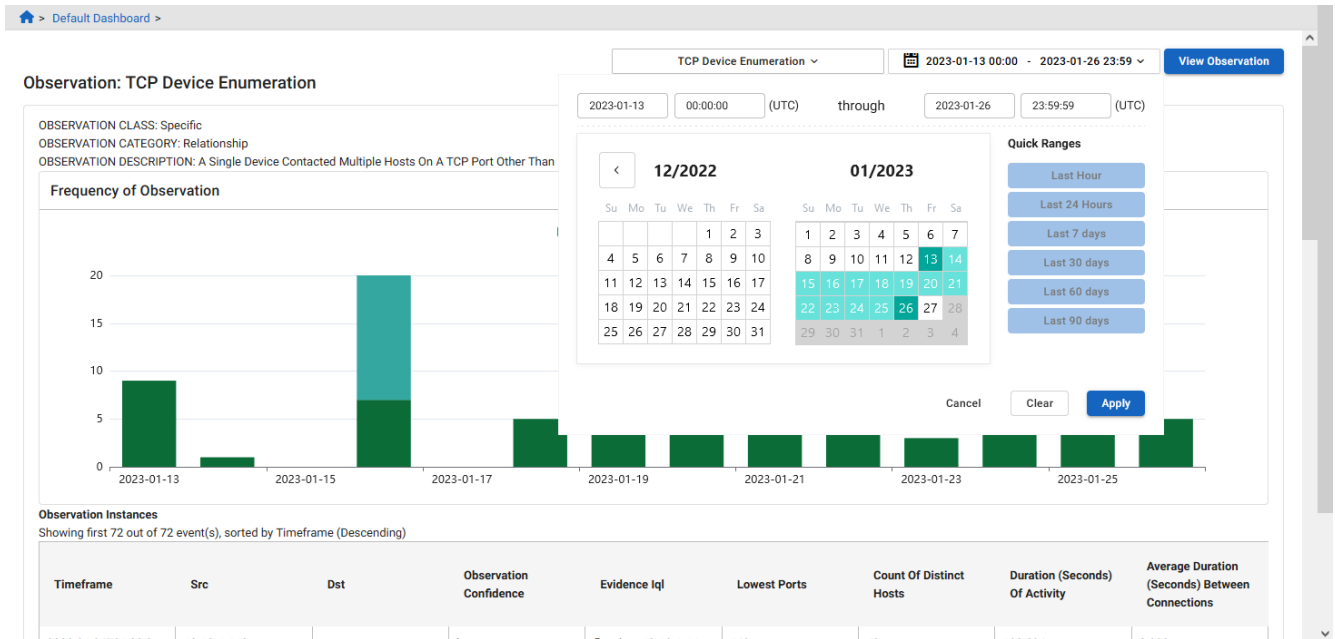
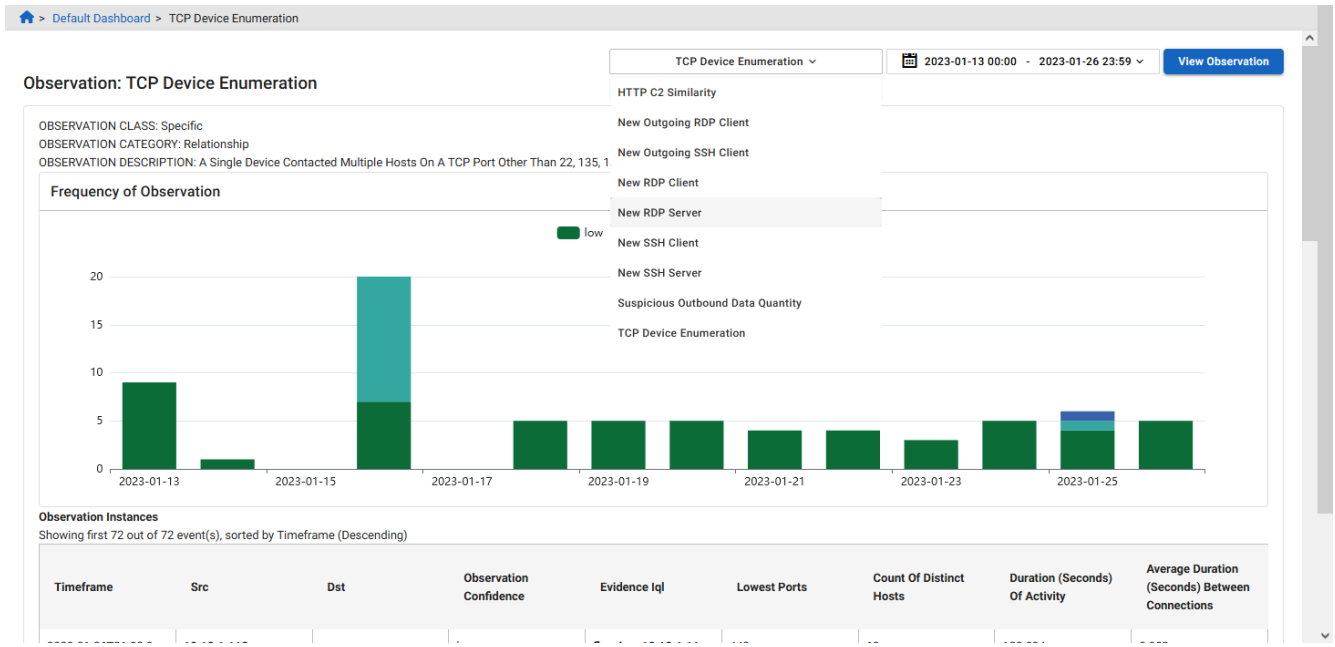
30 Jan 2023 version 2023.1

- New Functionality
 - Observation Detail Switcher
 - Forward and Back Keyboard Shortcuts
 - Bulk Entity Lookup
- Improved Functionality
 - Updated Detection API in Visualizer
 - PDNS Links on the Entity Panel

New Functionality

Observation Detail Switcher

On the Observation detail page, the observation drop down allows you to switch to other observation that are available for your account. The date range of the shown data can also be configured.



Forward and Back Keyboard Shortcuts

The keyboard arrow keys can be used to navigate to the previous and next query results in an investigation or ad hoc timeline when they are not active in another page element. The left arrow key navigates to the previous result, and the right arrow key navigates to the next result.

Bulk Entity Lookup

Multiple IP addresses and domain names can be looked up on the Investigation Entity Lookup page. Entries are separated by spaces.

Investigations > Entity Lookup

Entity Lookup

10.10.1.12 10.10.1.12 10.10.1.13 10.10.1.17 10.10.1.19

Perform an entity search on the following: (ip or domain)

Last 7 Days Search

4 Results

Entity	Type	Count	First Seen	Last Seen
10.10.1.17	IP	2	2022-06-06 04:17 (UTC)	2023-01-27 18:00 (UTC)
10.10.1.19	IP	586	2022-05-11 16:52 (UTC)	2023-01-27 19:53 (UTC)
10.10.1.12	IP	375867	2022-05-21 18:55 (UTC)	2023-01-27 20:09 (UTC)
10.10.1.13	IP	114	2022-05-31 15:52 (UTC)	2023-01-27 14:03 (UTC)

Right-click on a result and select Entity Lookup to view the intelligence panes.

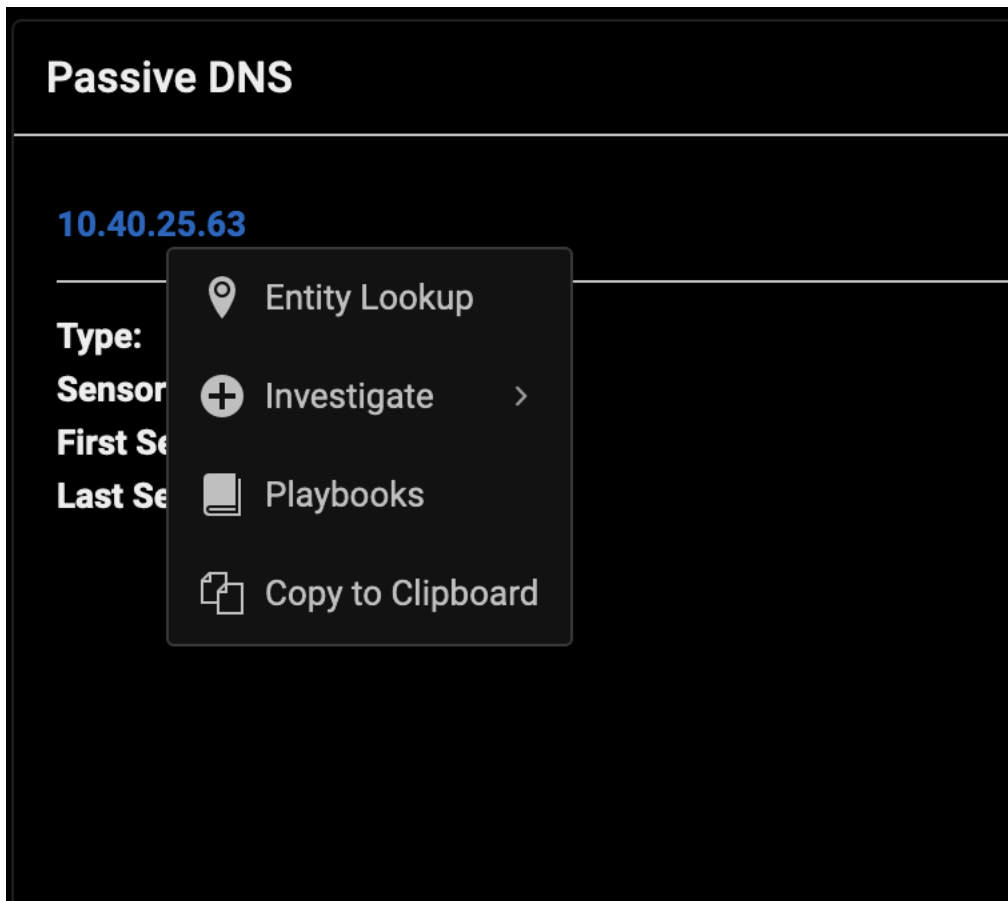
Improved Functionality

Updated Detection API in Visualizer

The time filters in the detection API are used to retrieve the detections for the selected time range, instead of retrieving all of the detections and then filtering them. This makes retrieving and filtering detections much faster. The detection limit is also increased from 1000 to 10000.

PDNS Links on the Entity Panel

PDNS links on the entity panel function like normal links. Clicking on the link replaces the entity panel with the panel for the clicked on element. Right-clicking opens a context menu.



Option	Description
Entity Lookup	Open the entity lookup page for the item.
Copy to Clipboard	Copy the item to the clipboard.
Playbooks	Launch playbooks. This options is not available for ad-hoc search result items
Investigate	Show appropriate pivots for the item type. This options is not available for ad-hoc search result items.
Search Events	Show the event searches appropriate for the type. The text in the search box is replaced, but the search will not run automatically. This options is only available for ad-hoc search result items. Types include: IP: - ip='IP' - dst.ip='IP' - src.ip='IP'domain: - domain='domain'

Resolved Issues

The following issues have been fixed in version 2023. To inquire about a particular bug, please contact [Customer Service & Support](#).

2023.12

Description

The GUI no longer displays all users from any account in a single account view.

Billing Dashboard: On the first and second days of the month, the GUI now displays Current Month Usage is not yet available instead of No Data.

Fixed the breadcrumb thread in the My Rules page.

Admins with access to single account can no longer view messages from all accounts.

Resolved an issue where a refresh was required to view results of a specific IQL query in an investigation.

Resolved an issue where the filters in the Detections Table did not close.

The pagination in the Sensor table no longer breaks when there are too many tags.

Resolved a minor issue with the Sensor label styles.

The Edit Features settings in the Sensor details page are working as designed.

Resolved a minor issue where changes to the Sensor location setting were not being saved.

Pivoting from the Manage Rules page to the Detection Rule detail view no longer displays a rule page with empty data.

Fixed an issue where clicking Account Management in the breadcrumb displayed all users.

2023.11

An issue where the URL format was blocking SAML logins has been resolved.

The UI no longer throws an error when viewing a parent account with no children accounts.

The User Management table no longer displays all the users from all the accounts the current user has access to.

2023.10

Fixed an issue in the Detections Table where resolved detections were not being refreshed.

Updating the logic for the first time will no longer return an error in the Detections Table .

The complete domain name is no longer hidden in Entity Panel.

The Mitre Attack widget no longer returns an error when there is no in the on Rules field.

2023.9.1

Resolved an issue in the monthly billing dashboard where September disappeared and was replaced with October.

Users with access to the parent account are now able to see overall bandwidth usage without an error message.

DHCP and Mac are no longer missing for some devices

Investigation list search now shows data when a user searches from a page other than page 1.

2023.9

Description

The time range when pivoting from adhoc timeline page to search page has been fixed.

The error in Create New User has been removed.

Selecting uri search on aggregation table now shows correct query.

The Sensor api no longer throws an error in the account management page

Do not allow "include child account" unless Admin has "include child accounts"

Include child account is now disabled until the Admin has enabled Include child accounts.

The alignment of the columns when the Sensor table is condensed has been fixed.

2023.8.1

Resolved an issue where logout and re-login directs user to an error page.

OSS vulnerabilities: CWE-843, CWE-915

2023.8

Observation Detail: The data displayed in the graph did not match the data displayed in the table.

Account Management: Fixed the width of Account Selection dropdown.

Billing Summary: Graph displayed incorrect bandwidth when switching accounts.

Date Picker: Error message was not appearing correctly.

2023.7

Fixed the color styling for empty table cells in dark mode.

In the child account selector, an issue with finding items in a long list has been resolved.

Portal sensor telemetry is able to display data when viewed as a group.

The Bulk Add indicator feature has been fixed.

An issue with resizing in the Investigation page has been fixed.

Resolved an issue where the sensor serial number becomes Unknown after an update.

In Detections, the custom filter test results table has been fixed.

The spacing in the date range picker has been fixed.

2023.6.1

Fixed display issues in Portal sensor telemetry view.

Improved color styling for empty columns in dark mode.

Fixed issues with the bulk indicator.

Improved user experience in the child account selector.

2023.6

Issue preventing users from accessing Account Management page has been fixed.

The Create Account button in Child Accounts tab is fixed.

Some rules will no longer display RangeError: Invalid time value when viewed from the All account

Resolved issues with Sensor Telemetry chart not showing data when Last 90 days is selected.

Unexpected behavior in custom detection has been resolved.

Fixed irregularities in Investigation List.

2023.5.1

Invalid tooltip in the Visualizer has been fixed.

Invalid dates in the date picker has been resolved.

An issue with overlapping icons in the Visualizer has been fixed.

The height selector in the Detections page has been fixed.

2023.5.0

The date picker no longer selects an invalid date when you add a query to an investigation.

The Add Notes feature in the Investigations module will no longer send blank notes.

The Enter key now works when searching annotations.

The scroll box in the Indicators in Impacted Devices pane have been improved.

Telemetry is not shown when All accounts are selected.

The rule information pane no longer takes up the entire screen in rules with long descriptions.

2023.4.1

The Detections table and Mitre-Detections widget can fetch inactive rules.

The Date Range filter in the Entity Panel shows the current range.

The row selection has been fixed in the Manage Subscription page and in Change Edit/Create Subscription Into Modal.

The digest time has been fixed in the Manage Subscription page.

The TimeZone values are now dynamic.

2023.4

Fixed styling issues for Exclude New Device dialog.

Data is copied to clipboard for the Intel field under Investigations > Events.

The Account column is no longer missing from the CSV export.

Date Picker in Adhoc search no longer shows an invalid date error for a valid date.

The Edit a excluded device/range dialog is now working as expected.

The Action column in Select New Query, no longer moves around the page.

2023.3.1

When configuring a time range, the date picker allows selecting a date outside the current month.

When managing annotations, the default resolution no longer prevents access to buttons at the bottom of the page.

Resizing a column now works as expected.

The notification widget is no longer the entire width of the browser.

2023.3

In the Resolved Detections widget, the chart no longer overlaps the legend and the chart tooltip is now constrained within the chart.

Could not add spaces to search fields in drop-down lists with checkboxes.

When adding a new query to an investigation, the date range picker now displays the correct date range.

On the Reports page, the date range picker now uses UTC instead of local time.

Packet capture breadcrumb links now work as expected.

2023.2.1

On detection details pages, the Devices Impacted number was not updated after a Bulk Resolve Detections.

Updated links to ISO images and documentation from the sensor ISO image download pane.

Extraneous This dashboard does not exist notification no longer displayed after deleting a dashboard.

Ad hoc queries can be saved from the action drop-down menu.

OSS vulnerabilities: CWE-843, CWE-915.



www.fortinet.com

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