

Release Notes

FortiNDR Cloud 26.1.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



January 12, 2026

FortiNDR Cloud 26.1.0 Release Notes

78-261-1243236-20260112

TABLE OF CONTENTS

FortiNDR Cloud release notes	4
Version history	5
Version 26.1.0	5
Improved functionality	5
Other improvements	7
Product integration and support	8
Integrations	8
Fortinet Automation Service	9
Resolved issues	10
26.1.0	10
Known issues	11
25.4.a	11

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
12 January 2026	Version 26.1.0 on page 5

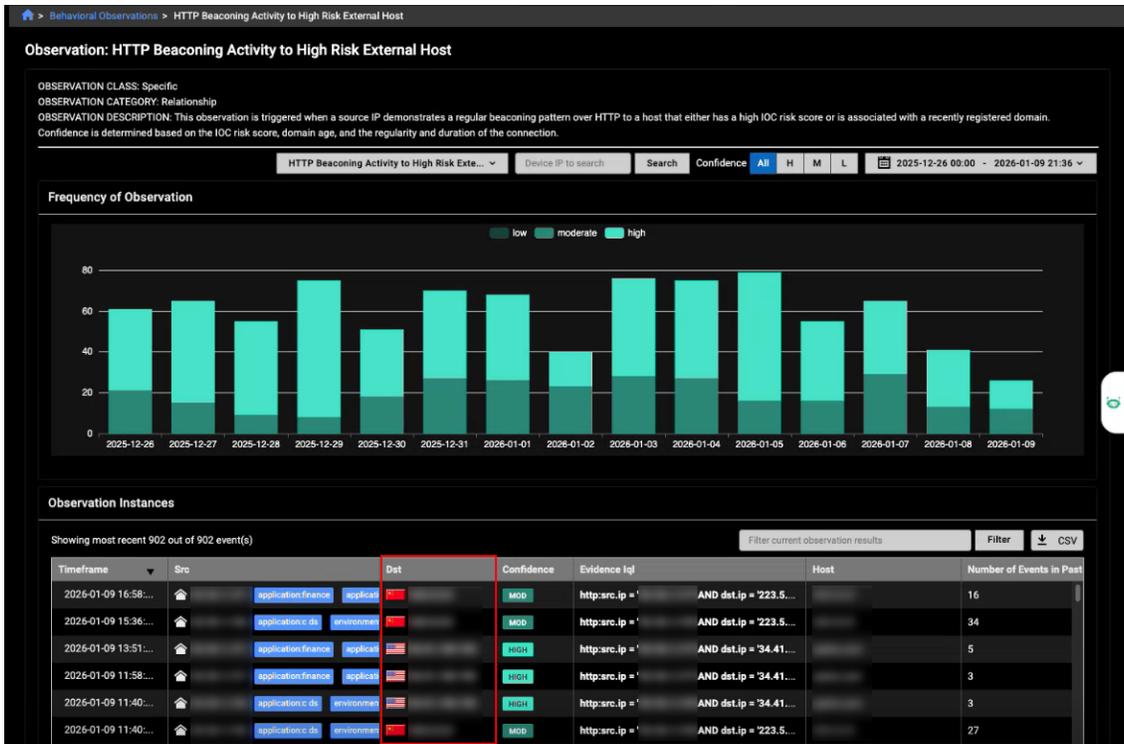
Version 26.1.0

- Improved functionality
 - Behavioral observations
 - FortiNDR Essentials Solution Pack v1.0.2
- Other improvements
- Resolved issues on page 10

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.

Investigation Results | - FAS via FCP | FAS-FortiClientEMS

Showing all 1 event, ordered by timestamp descending

tag	timestamp	type	src	dst	intel	observation_title
	2025-11-10 21:20:32 Z	observation				No EDR Solutions Installed

Fortinet Automation Service

Available Playbooks (15)

- FortiEDR - (3)
- FortiGate - (2)
- SentinelOne - (4)
- FortiClientEMS - (3)
- FortiProxy - (2)
 - Ban User by IP
 - Unban User by IP
- FortiDeceptor - (1)

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](#).

SIEM	CrowdStrike	Tested with Parser 1.0.2
	FortiSIEM	7.1.0 or higher
	Microsoft Sentinel	Not applicable
	QRadar	IBM QRadar SIEM version 7.3.3 or higher
	Splunk	Splunk Cloud versions: 9.3, 9.2, 9.1
SOAR	Cortex-XSOAR	Tested on: 6.6
	FortiSOAR	Tested on: 7.3.2-2150
	Splunk SOAR	7.3.2-2150 or higher
EDR / Firewall	CrowdStrike EDR	Latest Falcon EDR APIs
	FortiEDR	Not applicable
	FortiEDR Manager	6.2.0 or higher
	FortiEDR Collector	5.2.0 or higher
	FortiManager	7.4.2 or higher
	FortiGate	7.4.2 or higher
Intelligence Feeds	CrowdStrike Falcon Intel	Included with FortiNDR Cloud
	Fortinet Botnet IP 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	Included with FortiNDR Cloud
	Recorded Future connect	Included with FortiNDR Cloud
	ThreatConnect	Included with FortiNDR Cloud
	Tor Nodes	Included with FortiNDR Cloud
	URLHaus	Included with FortiNDR Cloud
Other	Endace	7.2.2 or higher
	Netskope	Not applicable
	Zscaler	Not applicable

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 26.1.0. To inquire about a particular bug, please contact [Customer Service & Support](#).

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 <i>All</i> accounts during portal login prevented customers from accessing the portal.

Known issues

The following issues have been identified in version 26.1.0. 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.