

Release Notes

FortiTiP Cloud 25.2



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



August, 2025

FortiTIP Cloud 25.2 Release Notes

00-400-000000-20221031

TABLE OF CONTENTS

FortiTIP Cloud Release 25.2	4
Features	4
Product Integration and Support	5
Web Browsers & Recommended Resolution	5

FortiTIP Cloud Release 25.2

FortiTIP Cloud is a cloud-hosted threat intel platform designed to enhance an organization's ability to identify, manage, and respond to cyber threats in an effective and coordinated manner. The platform integrates several key functions including *Outbreak Management*, *Threat Intel Search*, *Threat Intel Management*, and *CVE Correlation with Threat Feeds*. These features work in tandem to provide a unified view of potential threats, vulnerabilities, and incidents across an organization's network and digital assets on customizable pre-built dashboards.

For information on all FortiTIP Cloud features and how to use and configure them, see the [FortiTIP Cloud Documentation Library](#).

Features

The following are the key features of this solution:

- **Outbreak Management:** Provided by FortiGuard, this feature equips the platform with tools to monitor and manage the containment and resolution of widespread attacks or breaches. It enables organizations to rapidly assess the scope and impact, ensuring efficient coordination of response efforts.
- **Threat Intel Search:** The platform enables users to query FortiGuard's extensive threat intelligence database to uncover details about Indicators of Compromise (IOCs), including associated malware, threat actors, CVEs, and related threat correlations. This empowers analysts with contextual insights to accelerate threat validation and informed response.
- **Threat Intelligence Management:** This component allows users to collect, analyze, and store threat intelligence from multiple sources. It facilitates the enrichment of data with contextual insights to better understand the nature, intent, and tactics behind threats.
- **CVE Correlation with Threat Feeds:** By correlating CVE (Common Vulnerabilities and Exposures) data with active threat feeds, the platform helps organizations quickly identify which vulnerabilities are actively being targeted by adversaries. This feature enables proactive defense by focusing resources on high-risk vulnerabilities.

This Threat Intelligence Platform is a vital tool in enhancing cybersecurity resilience, providing organizations with the tools to stay ahead of evolving threats and mitigating risks before they become significant issues.

Product Integration and Support

FortiTIP Cloud version 25.2 can be accessed via a web browser.

Web Browsers & Recommended Resolution

- FortiTIP Cloud 25.2 user Interface has been tested on the following browsers:
 - Google Chrome version 126.0.6478.127
 - Mozilla Firefox version 128.0.2
 - Microsoft Edge version 126.0.2592.113
 - Safari version 17.5 (19618.2.12.11.6)
- The recommended minimum screen resolution for the FortiTIP Cloud user interface is 1920 x 1080. Adjust the screen resolution accordingly for optimum user experience.



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.