Release Notes

FortiRecon 25.3.a

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 29, 2025
FortiRecon 25.3.a Release Notes
75-253-1205681-20250929

TABLE OF CONTENTS

Change log

Date	Change Description
2025-09-29	Initial release of 25.3.a.

Introduction

FortiRecon is a Digital Risk Protection (DRP) service that operates alongside existing security solutions to provide you with the visibility that an adversary can have of your infrastructure. This early warning of any malicious activity targeted at your organization enables swift detection and mitigation. Operating purely from outside the organizational boundary, the service maps an organization's digital footprint and monitors it for abnormal activity. The service gives organizations the intelligence to mitigate credible security threats in a controlled manner as part of ongoing security efforts.

FortiRecon scans the organization's attack surface and identifies risks to assets while FortiGuard Threat Intelligence delivers early warning of risks to the organization through targeted, curated intelligence to provide an early warning of any malicious activity targeted to the organization.

The FortiRecon portal includes the following modules:

Overview	The *Overview* module provides a centralized view of your organization's digital risk posture across *Attack Surface Management (ASM)*, *Brand Protection (BP)*, and *Adversary Centric Intelligence (ACI)* modules. Discovered issues are mapped to relevant MITRE ATT&CK techniques and sub-techniques, providing a valuable framework for understanding attacker motivations and potential attack paths.
Attack Surface Management	The *External Attack Surface Management (EASM)* module provides an adversary's view of the organization digital attack surface and prioritizes risks and exposures, enabling administrators to mitigate threats in a controlled manner before the threats become a problem.
	The *Internal Attack Surface Management (IASM)* module provides visibility into internal network, identifying vulnerabilities within the organization's perimeter. It helps administrators discover internal assets, assess associated risks, and take mitigation steps.
Brand Protection	The *Brand Protection (BP)* module continually monitors the organization's public-facing visibility for unauthorized changes, including web-based phishing attacks, typo-squatting, rogue applications, credential leaks, and brand impersonation in social media, which may impact brand value, integrity, and trust.
Adversary Centric Intelligence	The *Adversary Centric Intelligence (ACI)* module leverages FortiGuard Threat Analysts to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights. This information enables administrators to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets.
Security Orchestration	The *Security Orchestration* module helps you investigate and respond to security threat findings from Attack Surface Management, Brand Protection, and Adversary Centric Intelligence. This solution reduces the time responders require to prioritize and take appropriate actions by automating and streamlining security workflows. It provides preconfigured playbooks to help you get started quickly. You can also create playbooks using connectors, add playbook variables, and view execution logs. Install and connect agents if required.

Profile Settings	The Profile Settings module allows you to personalize your FortiRecon account and provide information on your organization.

For details, see the FortiRecon User Guide.

What's new

The following new features and enhancements are included in the FortiRecon 25.3.a release.

Module	Feature	Description
Attack Surface Management	Web Application Assessment	FortiRecon now includes the *Web Application Assessment* feature, performing a rapid, attacker-centric surface scan to proactively identify critical, unauthenticated vulnerabilities—such as SQLi, XSS, and RCE—and automatically discover exposed APIs on your external application attack surface.
Brand Protection	Dashboard	The *Brand Protection* > *Dashboard* now features clickable elements to allow you to quickly drill down and view the corresponding details for each metric.
	Domain Threats	• The *Brand Protection* > *Domain Threats* page now groups different URLs under their primary domain to simplify viewing and analysis. • The *Domain Threats* page now includes the *By Source* filter, which allows you to narrow the list of domain threats.
	Rogue Mobile Apps	In *Brand Protection* > *Rogue Mobile Apps* page, you can now select the official application's platform or store from a predefined list when adding an application.
	Takedown	• In *Brand Protection* > *Takedown* page, you can now initiate takedowns for impersonating profiles and groups on instant messaging platforms, including *WhatsApp* and *Telegram*. • You can now revoke takedown requests that are in the *Requested*, *Acknowledged*, *Approved*, *Awaiting Response*, and *Initiated* statuses directly from the *Takedown* page.
Adversary Centric Intelligence	Reports	The *Report* details page in *Adversary Centric Intelligence* now includes a *Victims* tab to provide detailed context about affected entities.
Security Orchestration	Tasks	The *Security Orchestration* page now features a new *Tasks* tab, which displays a list of automations that are awaiting user input before they can continue.
Profile Settings	Notification Center	In the *Profile Settings* > *Notification Center*, you can now manage *Stealer Infection* notifications by using the *Select All* option and by filtering domains based on their subscribed or unsubscribed status.

Module	Feature	Description
Organizations	Takedown	The *Organization* license details page now displays comprehensive takedown details.

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.