Release Notes

FortiRecon 26.2.0

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

May 21, 2026
FortiRecon 26.2.0 Release Notes
75-262-1293950-20260521

TABLE OF CONTENTS

Change log

Date	Change Description
2026-05-21	Initial release of 26.2.0.

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.

What's new

The following new features and enhancements are included in the FortiRecon 26.2.0 release.

Module	Feature	Description
Brand Protection (BP)	Social Media Threats	FortiRecon now monitors *TikTok* for social media threats. You can review, manage, and take action on *TikTok* profiles impersonating your organization.
	Domain Threats widget	The *Brand Protection* > *Domain Threats* page includes updated dashboard widgets. The page now displays *Live Domain Threats* and *All Discovered Threats* tabs, each with dedicated widgets for threat counts, distribution, and available takedown credits.
User Interface	Feedback button	You can now submit feedback using the new *Feedback* button in the top navigation bar.
	Enhancements	The *Attack Surface Management* > *Security Issues* and *Adversary Centric Intelligence* > *Dashboard* pages include UI enhancements.

Red Teaming Service (Coming Soon)

FortiRecon is introducing a *Red Teaming* service in a future release. *Red Teaming* is a realistic, controlled emulation of how an actual attacker would attempt to breach your organization, validating how far an adversary can go beyond what attack surface scanning reveals.

To register your interest in the early access and design partner program, go to the *Red Teaming* tab in the top navigation bar and click *Create Red Teaming Assessment* to complete a short survey.

For details, see the FortiRecon User Guide.

www.fortinet.com