Release Notes

FortiRecon 25.2.0

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 22, 2025
FortiRecon 25.2.0 Release Notes
75-252-1160438-20250522

TABLE OF CONTENTS

Change log

Date	Change Description
2025-05-22	Initial release of 25.2.0.

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.
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 25.2.0 release.

Feature	Description
Licensing	FortiRecon now offers flexible consumption-based licensing through FortiFlex.
Attack Surface Management (ASM)	• The *Attack Surface Management* > *Security Issues* > *IASM* page now displays *National Vulnerability Database (NVD)* severity ratings for identified *Common Vulnerabilities and Exposures (CVEs)* in addition to FortiRecon severity ratings. • The *Attack Surface Management* > *Asset Discovery* page now supports searching for specific assets within the false positives filtered list.
Adversary Centric Intelligence (ACI)	• The *Adversary Centric Intelligence* > *Reports* page now supports bulk indicators of compromise (IOCs) downloads. • Administrators can now view and export associated passwords within leaked stealer infection details in *Adversary Centric Intelligence* > *Stealer Infections* > *Compromised Systems (Leaked)* page.
Manage Security Service Providers (MSSPs)	• The *Provisioning Form* has been redesigned and enhanced for an improved client onboarding experience. • MSSP clients can now create and manage users directly within FortiRecon.
UI Enhancements	Improved filter and search options.

www.fortinet.com