

SOLUTION BRIEF

# Swiftly Find and Remediate Security Issues in the External Attack Surface With FortiRecon EASM

## Executive Summary

With converging networks, expanding supply chains, cloud, and third-party-vendor reliance, every CISO and security team needs ongoing visibility. Understanding what impacts those changes are having on the organization's digital footprint is critical. Seeing the full risk surface means knowing about all new assets, software, and accounts added to the network—and the security status of each.

FortiRecon External Attack Surface Management (EASM), part of the Fortinet Digital Risk Protection (DRP) solution, continuously assesses an organization's digital surface. It discovers, identifies, and alerts to new weaknesses and vulnerabilities, as well as new digital assets. EASM provides immediate visibility to, and remediation actions for, any newly discovered asset, vulnerability, or public exposure.

## Assessing Risk and Managing Assets Are Complex in Today's Dynamic Environments

Networks are in constant flux, adopting and expanding cloud and Software-as-a-Service (SaaS) solutions, licensing new third-party software, acquiring companies, and adding new assets and services. When the network footprint changes, the risk surface expands. With the rapid evolution of sophisticated threats, it's increasingly important to swiftly discover misconfigurations, unprotected or unpatched systems, and exposed services in devices, software, applications, and services.

In addition, new on-premises, virtual, cloud, and remote assets have made managing corporate assets more challenging. Unapproved assets and services (shadow IT), other policy violations, and authorized but compromised corporate assets make today's asset management complex. Gaining immediate knowledge of newly acquired devices, software, applications, and services is an important part of today's security strategy.

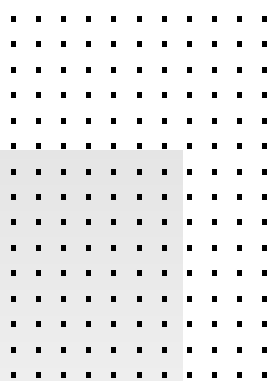
## FortiRecon External Attack Surface Management Identifies Risks and New Assets Across Environments

FortiRecon EASM assesses on-premises, virtual, and cloud assets, and that of subsidiaries and new acquisitions, to provide comprehensive digital asset discovery and management.

In addition to digital asset discovery, EASM empowers the security, governance, risk management, and compliance (GRC) and other teams responsible for company risk with ongoing insights. Seeing what has changed, been remediated, and remains outstanding, the insights can improve accountability for compliance. Identifying patterns of weakness and areas for increased education, plus other insights enables the enterprise to understand contributing factors to its risk and programmatically address it.

EASM identifies the following to swiftly address potential weaknesses:

- Newly discovered assets and services, including shadow IT by:
  - ASN
  - IP address
  - Domain
  - Subdomain
  - Port

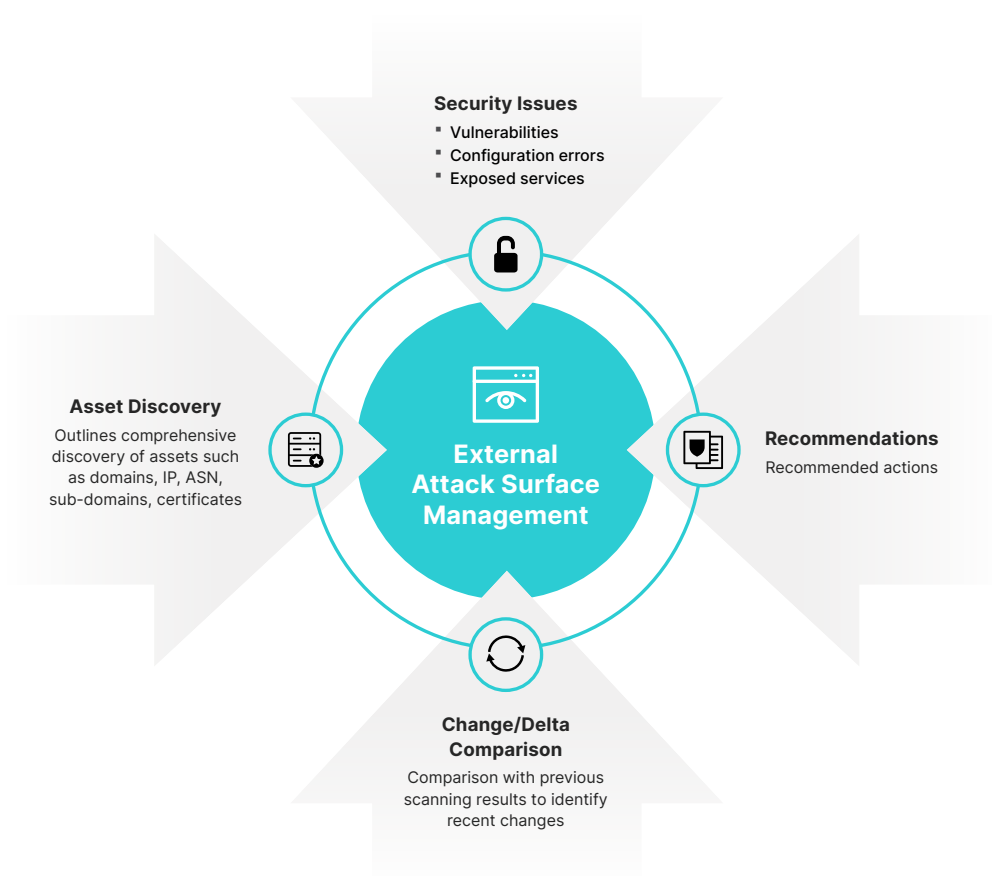


**“Between failures and change management, shadow IT, proliferation of cloud technologies, and newly announced vulnerabilities, the attack surface of every organization is constantly changing.”<sup>1</sup>**



- Security issues, including those in the public cloud, such as:
  - SSL certificate issues
  - Vulnerabilities
  - Misconfigurations
- Third-party credential leaks

EASM historical views can help identify patterns of change, policy violations, areas for improvement, and other potential risk areas for the company over time. With current and historical perspectives, security teams can resolve issue areas while better understanding those risks in need of more scrutiny. EASM remediation guidance helps prioritize and focus scarce resources on the highest-priority risks while security teams can make mitigation plans for others.



## FortiRecon Digital Risk Protection

FortiRecon EASM may be licensed by itself, with FortiRecon Brand Protection, or with both Brand Protection and FortiRecon ACI. The full FortiRecon solution with Brand Protection, EASM, and ACI includes the following features:

- A breadth of coverage that includes digital asset discovery, data leak detection on underground and open forums, and brand attacks for swift action
- Takedown service for accounts, websites, and rogue mobile applications
- Licensing flexibility, for “outside-in” visibility when it’s needed
- Executive to technical level views with an intuitive graphical user interface (GUI)
- Threat and incident expertise access from additional FortiRecon analyst time to incident response and assessment services

## Fortinet Delivers Comprehensive Security and Services

The Fortinet Security Fabric delivers end-to-end security across every stage of the attack lifecycle with FortiGuard threat intelligence for up-to-date protection. We also provide on-demand analysis, assessments, readiness services, and exercises. The FortiGuard Labs threat research team is skilled at collecting, analyzing, and discerning the relevance of billions of threat events worldwide. We bring together this wealth of expertise, skilled dark web researchers, multi-language intelligence collection, and human intelligence (HUMINT) specialists. This enables unrivaled access to threat intelligence and data on the latest threat activity, including restricted and invite-only forums. Almost a quarter of the total generated FortiRecon reports are done purely on the human intelligence that we collect, providing the most realistic view of risks.

### Summary

As an extension of the Fortinet Security Fabric and early stage attack-lifecycle protection, FortiRecon EASM builds upon security controls already employed in the network to deliver a digital asset risk profile and remediation steps. Visit our [website](#) to learn more about all of the FortiRecon capabilities.

### FortiRecon EASM Benefits

- Confidence in third-party applications
- Safer assimilation of new acquisitions
- Swift remediation of new vulnerabilities and exposures
- Quick discovery of newly attached assets
- Easy change management
- Better visibility of remediated risks

<sup>1</sup> Jake Williams and Jim Wachhaus, "[Maximizing Security Value Through External Attack Surface Management](#)," SANS, September 2021.

