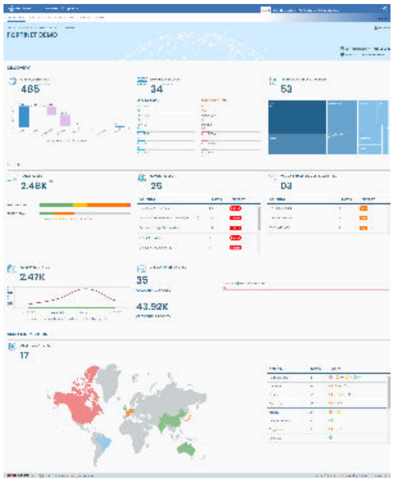
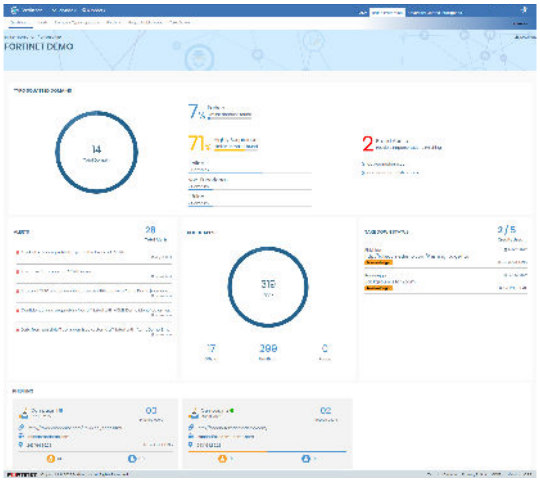
DATA SHEET

FortiRecon





Digital Risk Protection Service

FortiRecon is a Digital Risk Protection (DRP) service that operates alongside existing security solutions to provide security teams with the visibility an adversary can have of their infrastructure. This early warning of any malicious activity targeted at their organization enables fast detection and mitigation. Operating solely from outside the organizational perimeter, 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 External Attack Surface Management. Provides an adversary's view of the organization's digital attack surface and prioritizes risks and exposures, enabling security teams to mitigate threats in a controlled manner before they become a problem.

FortiRecon Brand Protection. Continually monitors the organization's digital footprint for unauthorized changes, typosquatting, rogue applications, credential leaks, brand impersonation on social media, and web-based phishing attacks, which may impact brand value, integrity, and trust.

FortiRecon Adversary Centric Intelligence. Leverages FortiGuard Threat Research Team to provide comprehensive coverage of Dark Web, open source, and technical threat intelligence, including threat actor insights to enable organizations to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets.

Challenge

- Threat actors are constantly scanning the internet looking for gaps in defenses which can be exploited to gain a foothold in the organization's network
- The fast pace of change for cybersecurity means security teams struggle to keep up with the latest threats

Service

- FortiRecon scans the organization's attack surface and identifies risks to assets. FortiGuard Threat Intelligence delivers early warning of risks to the organization through targeted, curated intelligence

Benefits

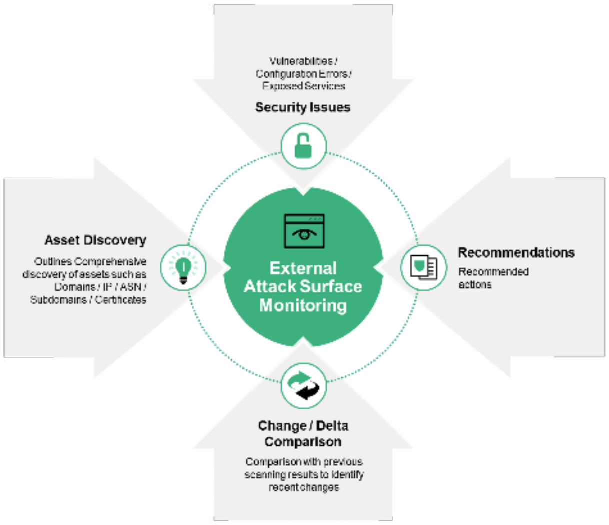
FortiRecon provides visibility and intelligence allowing the customer to take controlled risk-based security actions:

- Understand the diverse threats to the organization and protect brand reputation
- Respond faster to incidents, better understand attackers, and safeguard assets
- Expand view and early warning of adversarial activity from Dark Web and other sources

FEATURE HIGHLIGHTS

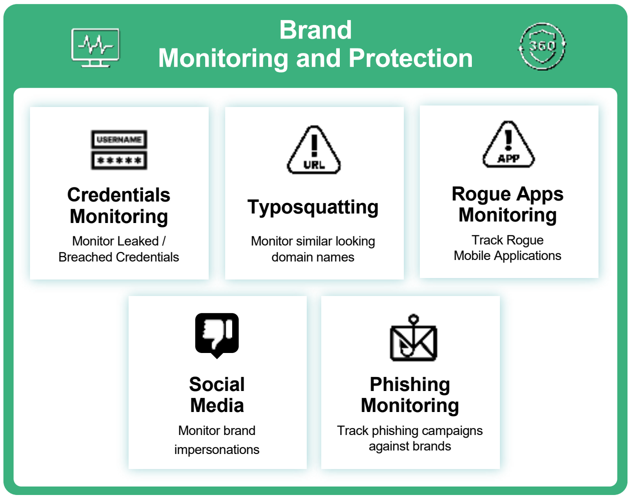
External Attack Surface Management (EASM)

FortiRecon External Attack Surface Management provides an external outside-in view of the organization and its subsidiaries, to identify exposed known and unknown enterprise assets and associated vulnerabilities to help prioritize remediation and focus on the most critical issues. EASM will helps identify servers, credentials, public cloud service misconfigurations, and third-party software code vulnerabilities which can potentially be exploited by malicious actors.


Vulnerabilities /
Configuration Errors /
Exposed Services
Security Issues
Asset Discovery
Outlines Comprehensive discovery of assets such as Domains / IP / ASN / Subdomains / Certificates
External Attack Surface Monitoring
Recommendations
Recommended actions
Change / Delta Comparison
Comparison with previous scanning results to identify recent changes

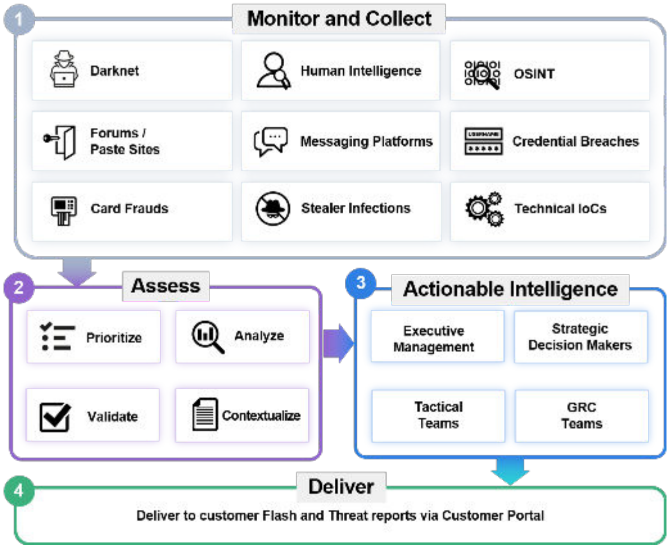
Brand Protection (BP)

FortiRecon Brand Protection uses proprietary algorithms to detect web-based phishing attacks, typosquatting, rogue apps, credential leaks, and brand impersonation on social media; all common techniques used by Cyber Threat Actors. By detecting activity early and taking action, such as takedowns of fake sites or applications, Brand Protection helps organizations to protect their brand value, trust, integrity, and reputation.


Brand
Monitoring and Protection
360
USERNAME
Credentials Monitoring
Monitor Leaked / Breached Credentials
URL
Typosquatting
Monitor similar looking domain names
APP
Rogue Apps Monitoring
Track Rogue Mobile Applications
Social Media
Monitor brand impersonations
Phishing Monitoring
Track phishing campaigns against brands

Adversary Centric Intelligence (ACI)

FortiRecon Adversary Centric Intelligence provides curated, relevant and contextual insights into imminent threats to organizations, and allows them to respond faster to incidents, better understand their attackers, and safeguard their assets. ACI provides comprehensive coverage of Dark Web, Open Source, and Technical Threat Indicators from dominant and emerging threats. The intelligence includes threat actor insights to help organizations proactively assess risks, look for vulnerabilities in the existing setup, and increase the security awareness of their staff.



FORTIRECON SOLUTION BUNDLES

SOLUTION BUNDLES	FEATURE	FORTIRECON EASM	FORTIRECON EASM AND BP	FORTIRECON EASM, BP, AND ACI
EASM	Asset Discovery	✓	✓	✓
	Security Issues	✓	✓	✓
	Asset Reports	✓	✓	✓
	Monthly Scanning	✓	✓	✓
	Weekly Scanning			✓
	On-demand Scans (Two per Year)			✓
BP	Third-party Credential Leaks	✓	✓	✓
	Source Code Sensitive Leaks		✓	✓
	Open Cloud Storage Buckets		✓	✓
	Domain Typosquatting		✓	✓
	Rogue Mobile Apps		✓	✓
	Phishing Monitoring - Digital Watermarking		✓	✓
	Takedowns		✓	✓
	Social Media Brand Impersonations		✓	✓
ACI	Social Media			✓
	Dark Web Monitoring			✓
	Technical Intelligence			✓
	IoC Reputation Lookup (IP/Domain/Hash/CVE)			✓
	Dark Web Marketplace Monitoring (Stealer Logs)			✓
	OSINT Cyber Threats			✓
Delivery	Executive Reporting	✓	✓	✓
	24×7 Portal Access	✓	✓	✓
	Analyst Support		✓	✓
	Realtime Alerting		✓	✓
	Orchestration/Integrations (Ticketing/SOAR)		✓	✓

Powered by FortiGuard Labs Threat Research

Learn more about support from FortiCare Worldwide 24/7 Support

www.support.fortinet.com

ORDER INFORMATION

SOLUTION BUNDLE	SKU	DESCRIPTION
FortiRecon EASM	FC2-10-RNSVC-533-02-DD	FortiRecon External Attack Surface Monitoring - Up to 500 monitored assets
	FC3-10-RNSVC-533-02-DD	FortiRecon External Attack Surface Monitoring - Up to 1000 monitored assets
	FC4-10-RNSVC-533-02-DD	FortiRecon External Attack Surface Monitoring - Up to 2000 monitored assets
	FC5-10-RNSVC-533-02-DD	FortiRecon External Attack Surface Monitoring - Up to 10 000 monitored assets
	FC6-10-RNSVC-533-02-DD	FortiRecon External Attack Surface Monitoring - Up to 50 000 monitored assets
	FC7-10-RNSVC-533-02-DD	FortiRecon External Attack Surface Monitoring - Up to 100 000 monitored assets
FortiRecon EASM and BP	FC2-10-RNSVC-534-02-DD	FortiRecon External Attack Surface Monitoring & Brand Protect - Up to 500 monitored assets
	FC3-10-RNSVC-534-02-DD	FortiRecon External Attack Surface Monitoring & Brand Protect - Up to 1000 monitored assets
	FC4-10-RNSVC-534-02-DD	FortiRecon External Attack Surface Monitoring & Brand Protect - Up to 2000 monitored assets
	FC5-10-RNSVC-534-02-DD	FortiRecon External Attack Surface Monitoring & Brand Protect - Up to 10 000 monitored assets
	FC6-10-RNSVC-534-02-DD	FortiRecon External Attack Surface Monitoring & Brand Protect - Up to 50 000 monitored assets
	FC7-10-RNSVC-534-02-DD	FortiRecon External Attack Surface Monitoring & Brand Protect - Up to 100 000 monitored assets
FortiRecon EASM, BP, and ACI	FC2-10-RNSVC-535-02-DD	FortiRecon External Attack Surface Monitoring Brand Protect & Adversary Centric Intelligence - Up to 500 monitored assets
	FC3-10-RNSVC-535-02-DD	FortiRecon External Attack Surface Monitoring , Brand Protect & Adversary Centric Intelligence - Up to 1000 monitored assets
	FC4-10-RNSVC-535-02-DD	FortiRecon External Attack Surface Monitoring , Brand Protect & Adversary Centric Intelligence - Up to 2000 monitored assets
	FC5-10-RNSVC-535-02-DD	FortiRecon External Attack Surface Monitoring , Brand Protect & Adversary Centric Intelligence - Up to 10 000 monitored assets
	FC6-10-RNSVC-535-02-DD	FortiRecon External Attack Surface Monitoring , Brand Protect & Adversary Centric Intelligence - Up to 50 000 monitored assets
	FC7-10-RNSVC-535-02-DD	FortiRecon External Attack Surface Monitoring , Brand Protect & Adversary Centric Intelligence - Up to 100 000 monitored assets
FortiRecon Takedown Service	FRN-TKD-5	FortiRecon Takedown Service Credits - 5 Takedowns. License must be activated within one year of purchase. Unused Takedown credits expire three years after the date of activation.
	FRN-TKD-10	FortiRecon Takedown Service Credits - 10 Takedowns. License must be activated within one year of purchase. Unused Takedowns credits expire three years after the date of activation.
	FRN-TKD-50	FortiRecon Takedown Service Credits - 50 Takedowns. License must be activated within one year of purchase. Unused Takedowns credits expire three years after the date of activation.

www.fortinet.com

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with Fortinet's EULA (https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf) and to report any suspected violation of the EULA via Fortinet's online reporting tool operated by independent third-party EthicsPoint (http://www.ethicspoint.com) or directly to Fortinet's legal team at legal@fortinet.com