FortiRecon

FortiRecon is a Digital Risk Protection (DRP) service that allows customers to gain visibility of their digital attack surface, receive targeted threat intelligence, and reduce organizational risk.

The solution consists of three main components:

External Attack Surface Management (EASM)

EASM continuously monitors your network perimeter, delivering an adversarial view of the organization's digital attack surface. The service prioritizes risks and exposures, enabling security teams to mitigate threats in a controlled manner before they become a problem.

Brand Protection (BP)

BP continually monitors the organization's external brand reputation for typosquatting, rogue applications, and impersonation via web sites and social media, which may impact brand value, integrity, and trust. The service monitors high value targets within the organization using Executive protection to identify loss of personal information which may be used by threat actors in targeted attacks.

Adversary Centric Intelligence (ACI)

ACI leverages FortiGuard Threat Research Team to provide organization-specific and expertly curated Dark Web, open source, and technical threat intelligence including threat actor insights. The approach enables organizations to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets.

Product Offering

The following shows a summary of FortiRecon product offerings. For details, see the FortiRecon datasheet.

SOLUTION BUNDLES	FEATURE	FORTIRECON EASM	FORTIRECON EASM AND BP	FORTIRECON EASM, BP, AND ACI
External Attack Service Management (EASM)	Asset Discovery	✓	✓	✓
	Security Issues	✓	✓	✓
	Asset Reports	✓	✓	✓
	Monthly Asset Identification	✓	✓	✓
	Weekly Asset Identification			✓
	Continuous Asset Scanning			✓
	Leaked Credentials	✓	✓	✓
	Merger and Acquisition Risk Assessment	✓	✓	✓
	Subsidiary Risk Management	✓	✓	✓
Brand Protection (BP)	Domain Threats – Typosquatting		✓	✓
	Domain Threats – Phishing (Digital Watermarking)		✓	✓
	Domain Threats – Brand Impersonation including Logo Detection		✓	✓
	Data leakage – Source Code Repositories		✓	✓
	Data leakage – Cloud Storage		✓	✓
	Rogue Mobile Application		✓	✓
	Executive Monitoring		✓	✓
	Social Media Monitoring – Fraudulent Accounts		✓	✓
	Takedowns		✓	✓
Adversary Centric Intelligence (ACI)	Intelligence Gathering - Darknet			✓
	Intelligence Gathering - Open Source (OSINT)			✓
	Intelligence Gathering – Technical Intelligence			✓
	Intelligence Gathering – Threat Actors			✓
	Darknet Marketplace Monitoring – Stealer Infections			✓
	Darknet Marketplace Monitoring – Credit Card Fraud			✓
	Supply Chain Security - Vulnerability intelligence			✓
	Supply Chain Security – Ransomware intelligence			✓
	Supply Chain Security – Vendor Risk Assessment			✓
	IoC Reputation Lookup (IP/Domain/Hash/CVE)			✓
Delivery	Executive Reporting	✓	✓	✓
	Portal Access 24×7	✓	✓	✓
	Analyst Support		✓	✓
	Realtime Alerting		✓	✓
	MSSP Multi Tenancy Support[1]			
Integrations	Open REST API	✓	✓	✓
	Orchestration (SOAR)	✓	✓	✓
	Public Cloud (AWS, GCP, Azure)	✓	✓	✓
	FortiGate	✓	✓	✓
	FortiDAST	✓	✓	✓

1 Requires FortiCare Premium License

Order Information

MONITORED ASSET QUANTITY	EASM	EASM, BP	EASM, BP, ACI
Up to 500	FC2-10-RNSVC-533-02-DD	FC2-10-RNSVC-534-02-DD	FC2-10-RNSVC-535-02-DD
Up to 1000	FC3-10-RNSVC-533-02-DD	FC3-10-RNSVC-534-02-DD	FC3-10-RNSVC-535-02-DD
Up to 2000	FC4-10-RNSVC-533-02-DD	FC4-10-RNSVC-534-02-DD	FC4-10-RNSVC-535-02-DD
Up to 10 000	FC5-10-RNSVC-533-02-DD	FC5-10-RNSVC-534-02-DD	FC5-10-RNSVC-535-02-DD
Up to 50 000	FC6-10-RNSVC-533-02-DD	FC6-10-RNSVC-534-02-DD	FC6-10-RNSVC-535-02-DD
Up to 100 000	FC7-10-RNSVC-533-02-DD	FC7-10-RNSVC-534-02-DD	FC7-10-RNSVC-535-02-DD
Up to 250 000	FC8-10-RNSVC-533-02-DD	FC8-10-RNSVC-534-02-DD	FC8-10-RNSVC-535-02-DD
Up to 500 000	FC9-10-RNSVC-533-02-DD	FC9-10-RNSVC-534-02-DD	FC9-10-RNSVC-535-02-DD
Up to 750 000	FCA-10-RNSVC-533-02-DD	FCA-10-RNSVC-534-02-DD	FCA-10-RNSVC-535-02-DD
Up to 1 000 000	FCB-10-RNSVC-533-02-DD	FCB-10-RNSVC-534-02-DD	FCB-10-RNSVC-535-02-DD

ADD ON SERVICES		
PRODUCT	**SKU**	**DESCRIPTION**
Service Credits 5 Takedowns	FRN-TKD-5	Stackable. License must be activated within one year of purchase. Unused Takedown credits expire three years after the date of activation.
Service Credits 10 Takedowns	FRN-TKD-10	Stackable. License must be activated within one year of purchase. Unused Takedown credits expire three years after the date of activation.
Service Credits 50 Takedowns	FRN-TKD-50	License must be activated within one year of purchase. Unused Takedown credits expire three years after the date of activation.

Frequently Asked Questions

What defines an asset?

An asset is any monitored resource, such as an ASN, IP address, domains, subdomains, or certificates. How can my customer find out the number of assets they have? Work with the Fortinet sales specialist to help scope the number of assets.

Are SKUs stackable?

Assets are licensed up to an asset count and are not stackable. To jump between ranges, you must coterm. Service credits for takedown are stackable.

How do I increase the service level or number of assets after the initial order?

Contact Customer Support who can advise on the upgrade process.

How do I extend a contract's time period?

FortiRecon is a term based license, therefore, it is possible to stack contract licenses to an existing subscription to extend the term.

How do I calculate asset sizing?

Each active asset (AS number, IP, domian, sub-domain) which is being monitored is chargeable as a full asset. Assets that are scanned but non-responsive are chargeable as 1/10 of an asset. This charge can be removed by excluding non-active IP ranges if necessary.

FRN-OG-R11-20250725