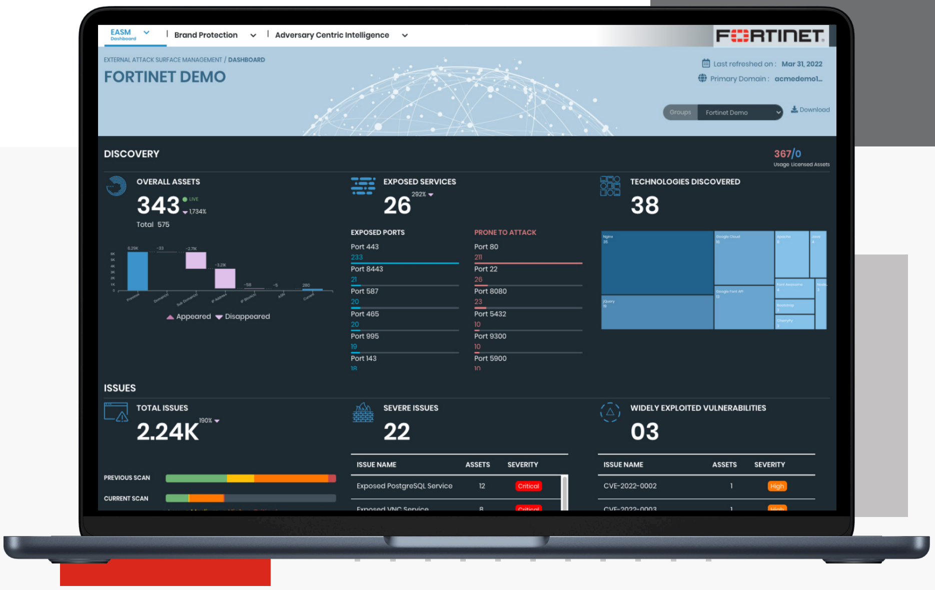
Data Sheet

FortiRecon



EXPOSED PORTS		PRONE TO ATTACK	
Port 443	233	Port 80	211
Port 8443	21	Port 22	26
Port 587	20	Port 8080	23
Port 465	20	Port 5432	10
Port 995	19	Port 9300	10
Port 143	18	Port 5900	10

ISSUE NAME	ASSETS	SEVERITY
Exposed PostgreSQL Service	12	Critical
Exposed VNC Service	8	Critical

ISSUE NAME	ASSETS	SEVERITY
CVE-2022-0002	1	High
CVE-2022-0003	1	High

Highlights

Scan the attack surface and quickly identify risks to assets.

Understand the diverse threats to the organization and protect brand reputation.

Respond faster to incidents, better understand attackers, and safeguard assets.

Expand view and gain early warning of adversarial activity from Darknet and other sources.

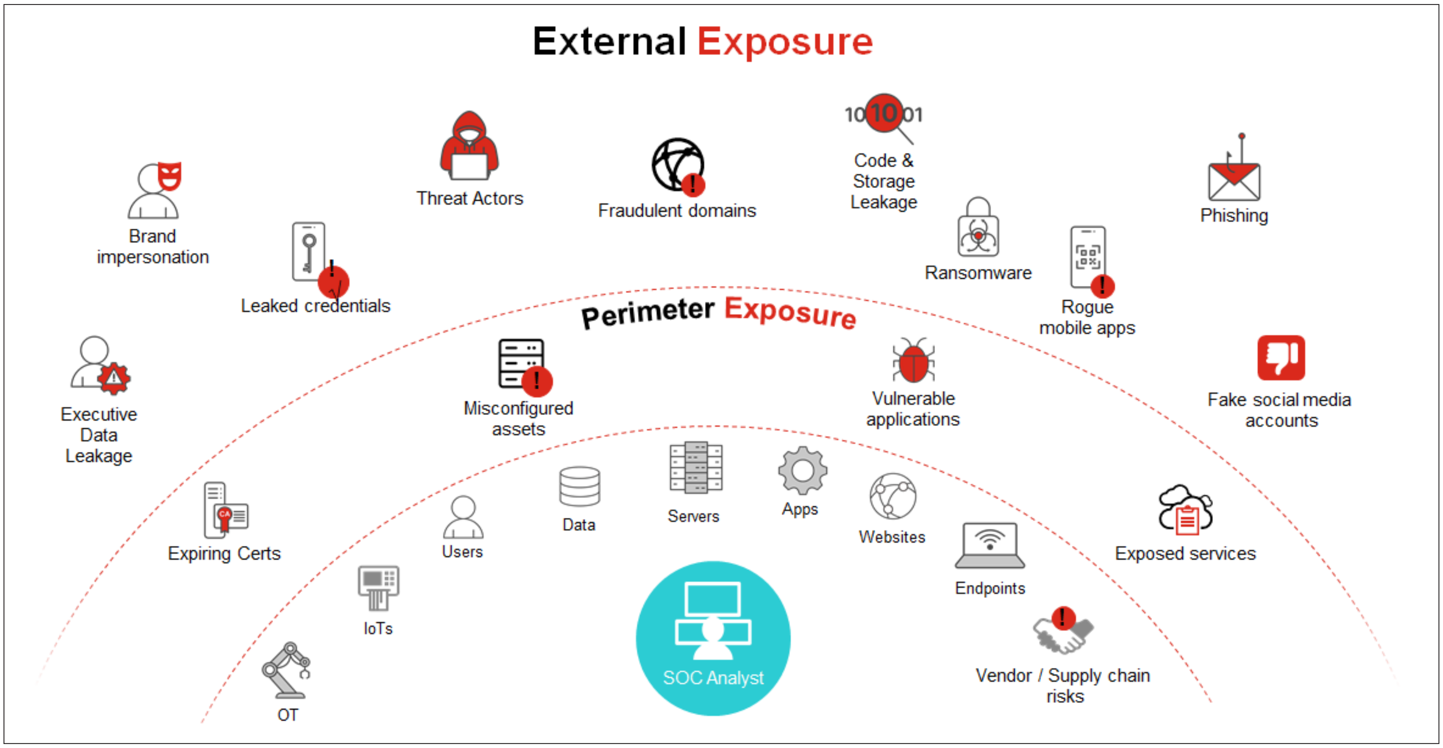
Digital Risk Protection Service

The threat landscape is the sum of all potential access points attackers can exploit to gain access to an organization's sensitive assets.
It includes the External and Internal Attack Surface that contains thousands, or even tens of thousands of internet-facing assets, for example, websites, cloud apps, S3 buckets, and more. Some of these assets are known, while others are unknown, for example, abandoned and orphaned domains, database services (for example, MongoDB and MySQL), often created by Shadow IT that may be unpatched or misconfigured, and therefore, exposed to threats. It also includes the Internal Attack Surface, including vulnerable or misconfigured internal applications, ports, and services, that can be exploited for lateral movement by threat actors.

Digital Risk Protection Service

But today's threat landscape is even bigger, since it also includes cyber-related risks to your supply chain vendors, as well as to your brand. Attackers often use fraudulent websites, fake social media accounts, and rogue mobile apps to deceive customers and employees, for example, for the purpose of capturing credentials and selling them on the dark web. When leaked credentials are up for sale on hacker forums, there's a high probability that they will be used in an attack against the organization. However, organizations' security teams do not often monitor, nor do they have the tools to track and identify these types of risks.

FortiRecon is Fortinet's AI and HUMINT-fueled Digital Risk Protection (DRP) service. A SaaS-based solution, it combines three robust modules—Attack Surface Management, Brand Protection, and Adversary Centric Intelligence, to provide security professionals with a complete view of all potential and imminent internal and external risks attackers can exploit.



Operating from outside and inside the organizational perimeter, the service maps an organization's digital footprint and continuously monitors and alerts on known/unknown exposed, vulnerable assets, impersonations and brand abuse, phishing campaigns, malicious dark web activities, attack intel related to the organization and its supply chain vendors/third parties, and more, providing early threat indicators of attacks and potential threats for proactive mitigation.

FortiGuard Labs' cybersecurity experts enhance the offering with guidance on prioritization of remediation efforts, and targeted threat research and intelligence. The team's unparalleled visibility and access to adversary forums, some of which are invite-only, provide a rich understanding of threat actors' motivations, TTPs (Tools, Techniques, and Procedures), as well as detect early evidence of attacks against the organization and its third-party vendors. With this type of intel, and using the integration with FortiSIEM and FortiSOAR, it becomes exceedingly easier for security professionals to act fast.

FortiRecon combines three powerful technologies and services

FortiRecon Attack Surface Management

Continuously monitors and delivers an adversary's view of the organization's internal and external digital attack surface, and prioritizes risks and exposures, enabling security teams to proactively mitigate threats before they become an attack.

FortiRecon Brand Protection

Continually monitors the organization's external brand reputation for typosquatting, rogue applications, phishing campaigns, and brand impersonations via websites and social media, which may impact brand value, integrity, and trust. The service also monitors high value targets within the organization using Executive Monitoring to identify account takeovers, darknet mentions, social media threats, stealer infections, and more, which may be used by threat actors in targeted attacks.

FortiRecon Adversary Centric Intelligence

Leverages FortiGuard Threat Research teams to provide organization-specific and expertly curated dark web, open source, and technical threat intelligence, including threat actor insights, past and potential ransomware attacks on your organization or your supply chain vendors, to enable security professionals to better prepare for potential attacks, proactively assess risks, and adjust security posture accordingly.

Key Benefits

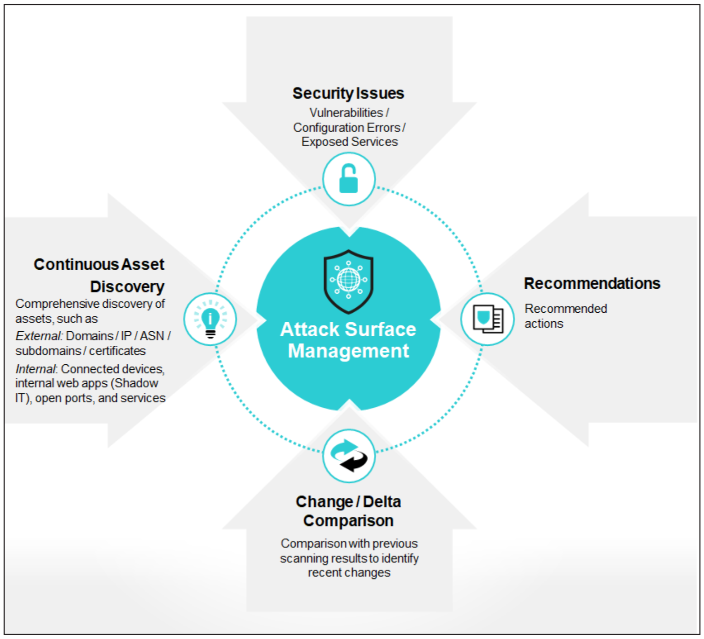
FortiRecon provides comprehensive visibility and threat intelligence, enabling organizations to take controlled risk-based security actions.

- Map the organization and its subsidiaries' digital attack surface to identify external visibility gaps, and security risks
- Prioritize remediation activities based on business risks
- Identify and mitigate brand attacks before they impact reputation
- Reduce SOC analyst operational overhead with a curated threat intelligence feed tailored to your organization and gain early warning of adversarial activity from darknet and other sources

Attack Surface Management

Attack Surface Management for Early Detection and Mitigation of Internal/External Risks

FortiRecon Attack Surface Management provides security professionals with in-depth visibility, continuous discovery, and monitoring of the internal/ external attack surface to identify internet-facing, exposed and vulnerable assets, and internal vulnerable assets that can be exploited by attackers. This intel generates prioritized actionable alerts, allowing security professionals to focus on high-value tasks that make the biggest impact.


Security Issues
Vulnerabilities / Configuration Errors / Exposed Services
Continuous Asset Discovery
Comprehensive discovery of assets, such as
External: Domains / IP / ASN / subdomains / certificates
Internal: Connected devices, internal web apps (Shadow IT), open ports, and services
Attack Surface Management
Recommendations
Recommended actions
Change / Delta Comparison
Comparison with previous scanning results to identify recent changes

Features and Highlights

Continuous External Attack Surface Monitoring (EASM)

Provides an attacker's view into your environment, by identifying known/unknown attacker-exposed assets (for example, domains, sub-domains, ASNs, IP blocks, and IP addresses), and alerts on exploited vulnerabilities, configuration errors, SSL certificate issues, prone-to-attack ports, exposed database services, DNS-related issues, leaked data/credentials, public cloud misconfigurations, and provides prioritization by actual risk.

Continuous Internal Attack Surface Monitoring (IASM) and Asset Discovery

Using a lightweight scanner container deployed within the network, FortiRecon IASM scans the internal network to discover and map connected devices, internal web applications and their vulnerabilities, open ports, and services. The scan results are then cross-referenced with FortiRecon threat intel on actively exploited vulnerabilities, providing analysts with updated vulnerability scores and prioritization.

Leaked credentials

Continuously monitors the dark web, private chat rooms, and alerts on an organization's credential leaks.

Location and subsidiary-based asset monitoring

Inventories and labels assets per location, department or based on subsidiary organizations.

Change comparison

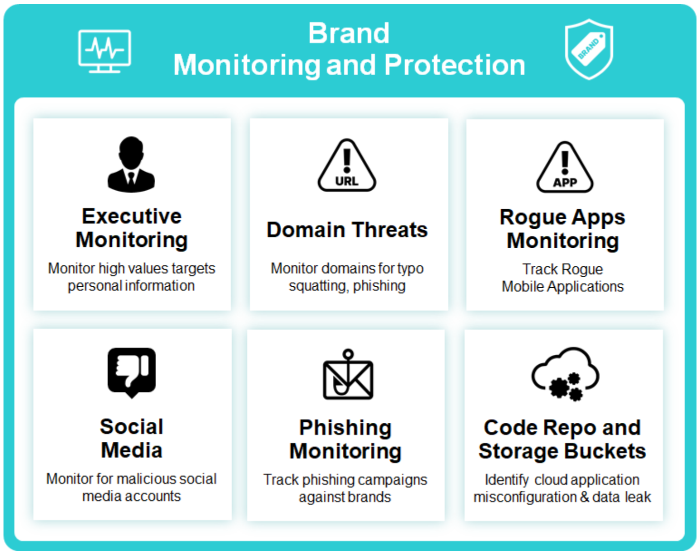
Continuously analyzes and tracks changes in asset exposure and remediation trends. FortiRecon provides historical data to help identify patterns of change, policy violations, areas for improvement, and other potential risk areas for the organization over time.

Brand Protection (BP)

Identify and stop brand threats in their tracks

FortiRecon Brand Protection uses proprietary algorithms to monitor and detect similar looking domains, brand and executive impersonations, rogue mobile applications on multiple app stores, data leaks in code repo, open bucket exposure, phishing campaigns, and helps protect executive online presence. These common techniques are used by cybercriminals to deceive customers, employees, and partners into providing sensitive information, passwords, and credit card information.

With FortiRecon Brand Protection service, you can quickly identify real threats to your brand, and we can take them down for you, helping you to protect brand value, trust, integrity, and reputation.


Brand
Monitoring and Protection
BRAND
Executive Monitoring
Monitor high values targets personal information
URL
Domain Threats
Monitor domains for typo squatting, phishing
APP
Rogue Apps Monitoring
Track Rogue Mobile Applications
Social Media
Monitor for malicious social media accounts
Phishing Monitoring
Track phishing campaigns against brands
Code Repo and Storage Buckets
Identify cloud application misconfiguration & data leak

Features and Highlights

Domain threats

Detects domain impersonations, for example, typo-squatted domains and phishing URLs. FortiRecon uses digital watermarks on official login and sensitive pages to track cloning and re-hosting of the web pages as phishing sites on another IP address.

Social media threats

Detects impersonations of an organization's social media accounts (for example, Facebook, Twitter, Instagram, LinkedIn), and monitors discussions against the brand

Rogue mobile apps

Tracks and takes down rogue mobile applications on various app stores

Code repo exposure

Discovers exposure of sensitive information on public code repositories

Open bucket exposure

Detects publicly accessible files over cloud storage platforms

Executive Monitoring

Monitors and defends against identity impersonations on social media platforms

Logo abuse

Identifies unapproved logo use on phishing sites and typosquatted domains

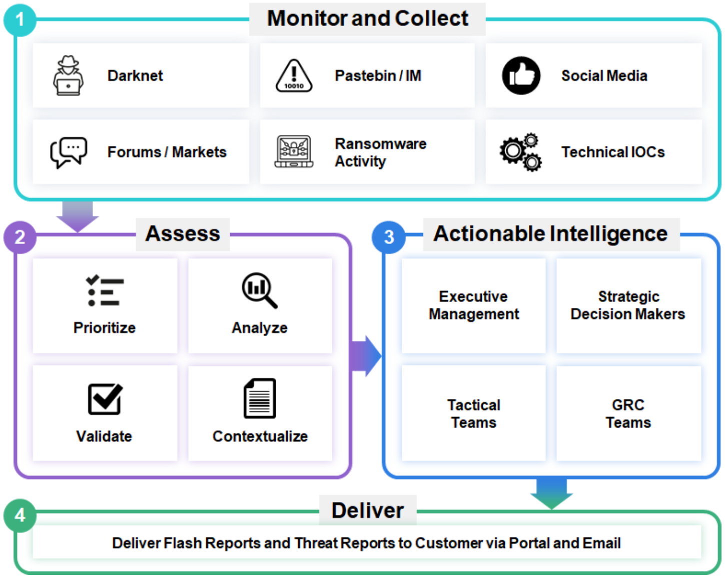
Takedown service

Provides rapid response using the FortiGuard Labs' takedown service, helps reduce investigation time, and requires no efforts from your security teams

Adversary Centric Intelligence (ACI)

Actionable threat intelligence tailored to your organization

FortiRecon Adversary Centric Intelligence leverages FortiGuard Labs' Threat analysts to provide curated, tailored, and contextual insights into potential and imminent threats to the organization and its supply chain vendors. ACI provides comprehensive coverage of dark web, open source, and technical threat intel. The intelligence includes threat actor insights to help security professionals proactively assess risks, to respond faster to incidents, and to increase the security awareness of their staff.



Features and Highlights

Vulnerability intelligence and prioritization

Monitors and reports on vulnerabilities and exploits being actively used and discussed on the dark web and open source. FortiRecon re-rates vulnerability scores based on scan results, wide usage, CVEs, and CVSS, for effective remediation prioritization.

Ransomware intelligence

Monitors ransomware threat actors' activities and reports on past and potential targets and TTPs relevant to the organization's profile and its vendors

Supply chain/vendor risk assessment

Continuous monitoring and early visibility into vendors risks, including attack surface exposure, past and potential ransomware incidents, leaked credentials/data, dark web chat mentions, and vulnerabilities exposure.

MITRE ATT&CK view

Map detections to MITRE ATT&CK framework, gain accurate picture of the tactics, techniques, and procedures (TTPs) that can be uses or are currently used against your organization

OSINT cyber threats intel

Helps you stay up to date with information on current cyber threats or events published on open source platforms, for example, social media and GitHub repositories.

Data leakage intel

Alerts on leaked credentials and data related to your organization

Stealer infections

Detects stealer infections and compromised user credentials

Card fraud monitoring

Provides information on credit/debit cards for sale on darknet marketplaces, including breach info, images, and more (available for Financial Services organizations)

Threat research, intel collection, and advanced querying

Gain immediate access to the latest cyber intelligence, including notable cyber events from around the globe, and historical threat activity, with early warning exposure and reports.

Recommendations

Analysis, assessment, risk prioritization, and remediation recommendations

Additional Features

Third-Party and Fortinet Security Fabric Integrations

FortiRecon includes a wide range of integrations into both the Fortinet Security Fabric and third-party solutions, as follows.

- Integration with the key cloud service providers (AWS, Azure, Google Cloud Platform) allows for continuous detection and reporting on cloud-based assets
- Collaboration tool integration (for example, Microsoft Teams, Slack, email)
- FortiGate NGFW integration enables FortiRecon to retrieve internet-facing device metadata from FortiGate (for example, PAT/NAT, public IP, port mappings, OS), and adds them to its routine scans
- FortiSOAR integration allows automated actions to be taken from the information collected by FortiRecon (for example, to reset a user’s password if compromised)
- FortiSIEM can ingest and correlate results of the FortiRecon reporting
- FortiDAST integration enables the initiation of web application scanning directly from the FortiRecon UI
- A REST based API is available for orchestration and integration into third-party solutions

FortiRecon Product Summary

SOLUTION BUNDLES	FEATURE	FORTIRECON EASM	FORTIRECON EASM AND BP	FORTIRECON EASM, BP, AND ACI
External Attack Surface Management (EASM)	Asset Discovery	✓	✓	✓
	Security Issues	✓	✓	✓
	Asset Management	✓	✓	✓
	Continuous Asset Scanning	✓	✓	✓
	Leaked Credentials	✓	✓	✓
	Merger and Acquisition Risk Assessment	✓	✓	✓
	Subsidiary Risk Management	✓	✓	✓
Internal Attack Surface Management	Asset Discovery	✓	✓	✓
	Security Issues	✓	✓	✓
Brand Protection (BP)	Domain Threats - Typosquatting		✓	✓
	Domain Threats - Phishing Monitoring (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	✓	✓	✓
	24×7 Portal Access	✓	✓	✓
	Analyst Support		✓	✓
	Realtime Alerting		✓	✓
	MSSP Multi Tenancy Support*			
Integrations	Open REST API	✓	✓	✓
	Orchestration (SOAR)	✓	✓	✓
	Public Cloud (AWS, GCP, Azure)	✓	✓	✓
	FortiGate	✓	✓	✓
	FortiDAST	✓	✓	✓

* Requires FortiCare Premium License

Ordering Information

	SKU	DESCRIPTION
SOLUTION BUNDLE		
FortiRecon External Attack Surface Monitoring Service (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.
	FC8-10-RNSVC-533-02-DD	FortiRecon External Attack Surface Monitoring - up to 250 000 monitored assets.
	FC9-10-RNSVC-533-02-DD	FortiRecon External Attack Surface Monitoring - up to 500 000 monitored assets.
	FCA-10-RNSVC-533-02-DD	FortiRecon External Attack Surface Monitoring - up to 750 000 monitored assets.
	FCB-10-RNSVC-533-02-DD	FortiRecon External Attack Surface Monitoring - up to 1M monitored assets.
FortiRecon External Attack Surface Monitoring and Brand Protect	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.
	FC8-10-RNSVC-534-02-DD	FortiRecon External Attack Surface Monitoring & Brand Protect - up to 250 000 monitored assets.
	FC9-10-RNSVC-534-02-DD	FortiRecon External Attack Surface Monitoring & Brand Protect - up to 500 000 monitored assets.
	FCA-10-RNSVC-534-02-DD	FortiRecon External Attack Surface Monitoring & Brand Protect - up to 750 000 monitored assets.
	FCB-10-RNSVC-534-02-DD	FortiRecon External Attack Surface Monitoring & Brand Protect - up to 1M monitored assets.
FortiRecon External Attack Surface Monitoring, Brand Protect, and Adversary Centric Intelligence	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.
	FC8-10-RNSVC-535-02-DD	FortiRecon External Attack Surface Monitoring, Brand Protect & Adversary Centric Intelligence - up to 250 000 monitored assets.
	FC9-10-RNSVC-535-02-DD	FortiRecon External Attack Surface Monitoring, Brand Protect & Adversary Centric Intelligence - up to 500 000 monitored assets.
	FCA-10-RNSVC-535-02-DD	FortiRecon External Attack Surface Monitoring, Brand Protect & Adversary Centric Intelligence - up to 750 000 monitored assets.
	FCB-10-RNSVC-535-02-DD	FortiRecon External Attack Surface Monitoring, Brand Protect & Adversary Centric Intelligence - up to 1M monitored assets.
ADD-ON SERVICES		
FortiRecon Take Down Service Add-on	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.
FortiRecon Internal Attack Surface Management	FC1-10-RNSVC-754-01-DD	FortiRecon internal Attack Surface Monitoring - 1 x /24 Network.
	FC2-10-RNSVC-754-01-DD	FortiRecon internal Attack Surface Monitoring - 5 x /24 Networks.
FortiRecon Executive Monitoring	FC1-10-RNSVC-755-01-DD	FortiRecon Executive Monitoring. Additional 5 Executives (Stackable).
	FC2-10-RNSVC-755-01-DD	FortiRecon Executive Monitoring. Additional 10 Executives (Stackable).
	FC3-10-RNSVC-755-01-DD	FortiRecon Executive Monitoring. Additional 50 Executives (Stackable).
FortiRecon Vendor Monitoring	FC1-10-RNSVC-756-01-DD	FortiRecon Vendor Monitoring. Additional 5 Vendors (Stackable).
	FC2-10-RNSVC-756-01-DD	FortiRecon Vendor Monitoring. Additional 10 Vendors (Stackable).
	FC3-10-RNSVC-756-01-DD	FortiRecon Vendor Monitoring. Additional 50 Vendors (Stackable).

Fortinet Corporate Social Responsibility Policy

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 the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

www.fortinet.com

May 10, 2024