F: RTINET

FortiGuard Security Services

To break the attack sequence and protect your organization, you need to detect and rapidly adjust your security posture to newly discovered attacks across the ever-expanding attack surface.
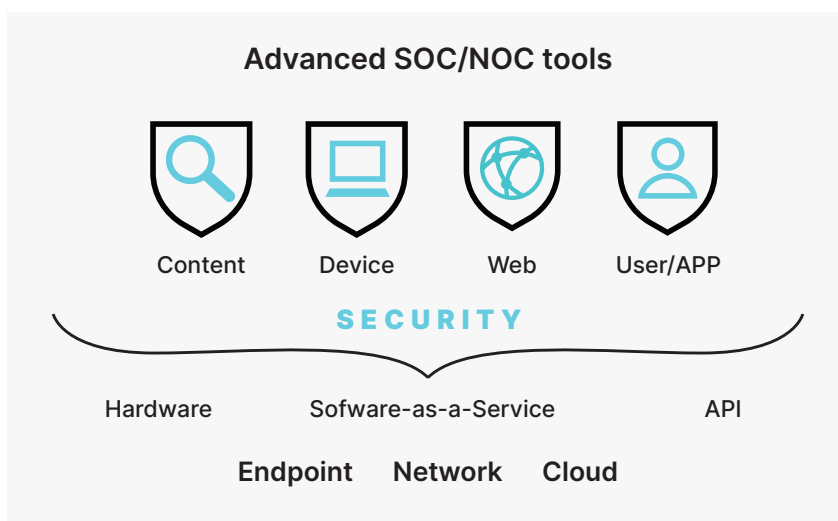
Can your security do that?

FortiGuard Security Services is a suite of market-leading, AI-enabled security capabilities providing application Content, Web, Device, and User security that continuously assesses the risks and automatically adjusts the Fortinet Security Fabric and ecosystem. It provides coordinated and consistent real-time defense for the latest attacks across network endpoints and clouds.

Why FortiGuard

Comprehensive. You can only protect against what you see, and in places that you can influence the enforcement in real time. We close the security gaps.

Be everywhere. Coordinated and consistent security detection and response across the attack surface and cycle with the largest portfolio of products supporting hybrid models of hardware, software, and as-a-service.

Impact everything. The largest technology and threat intelligence ecosystem with native and API-based integration.

Advanced SOC/NOC tools

Content   Device   Web   User/APP

SECURITY

Hardware   Sofware-as-a-Service   API

Endpoint   Network   Cloud

Quality of the analysis. AI and analytics systems are only as good as the inputs and training that go into them. We deliver credible security analysis results based on a unified dataset.

Trainers matters. Our AI is trained by one of the largest and most experienced security research organizations in the industry—FortiGuard Labs.

Data matters. Our AI is trained on one of the largest and most diverse datasets in the industry, spanning intelligence from endpoints, networks, and clouds.

Scale matters. Our platform ingests and analyzes more than 100 billion events every day, on average, to deliver over 1 billion security updates daily across the Fortinet Security Fabric and ecosystem.

Community matters. We see and protect you against millions of events from our global fabric deployments and from our partners, preventing a "second" Patient Zero for community known threats.

Time to protection for newly discovered threats.

You can only break the attack sequence if you can update your security posture, in time. We deliver coordinated and automated protection in near real time.

Break the sequence. We generate in near real time a holistic set of new protection for all relevant security technologies, enabling coordinated enforcement that is tailored for the attack sequence.

Have the reach. We automatically distribute the newly created protections, adjusting the Fortinet Security Fabric and ecosystem with coordinated market-leading defense.

Empower. We continually invest in advanced SOC and NOC tools, training, and capabilities, making sure that your teams are set for success.

Security efficacy that is backed up by leading certifications and testing organizations

Simplicity. Faster time to activation is key in supporting the pace of digital innovation. We deliver easy to choose, attach, and consume high-performing security.

Operation. Mix and match security capabilities to fit your diverse set of use cases across the organization, attaching them to the desired product across HW, VM, and as-a-service models. Rest assured that they are all designed from the ground up to work together in synergy. Leverage our Fabric Management Center to gain a unified view across your deployment.

Purchasing. We provide you with the freedom of choosing a la carte, optimized bundles for NGFW, cloud, mail, endpoint, etc., AND Enterprise Agreement.

Coordinated, market-leading security capabilities providing protection across the attack life cycle and surface.

Web Security

Optimized to monitor and protect data and applications against web-based attack tactics while assisting you with meeting compliance.

Web and Video Filtering	FortiGuard's massive web content rating, URL databases, and AI-enabled analysis environments power our accurate web and video filtering services. Providing granular blocking and filtering for web and video categories to allow, log, or block for rapid and comprehensive protection and regulatory compliance.
DNS	Consistent protection against malicious domain blocking attack tactics like DNS tunneling, C2 server identification, and Domain Generation Algorithms.
Antibot and CS	Block unauthorized attempts to communicate with compromised remote servers for both receiving malicious commands or extracting information.
Geo IP	Geo IP adds additional protection to this category by providing location information on IP traffic to help manage region-based threats.
WAF	In conjunction with our WAF product, this service delivers automated continuous signature updates that protect against SQL injection, cross-site scripting, and various other attacks, with hundreds of data-type and web robot patterns, vulnerability scan signatures, and suspicious URLs.

Content Security

Optimized to monitor and protect against file-based attack tactics, while assisting you with meeting compliance.

Cloud Sandbox

Top-rated behavior-based AI-powered static and dynamic malware analysis to address the rapidly evolving and more targeted threats including ransomware, crypto-malware, and others across a broad digital attack surface. Delivers real-time actionable intelligence and prevention through the automation of zero-day advanced malware detection and response. MITRE ATT&CK-based reporting and investigation tools.

AV

FortiGuard Antivirus delivers automated updates that protect against the latest polymorphing attack components, viruses, spyware, and other content-level threats. It uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network, endpoint, and clouds and access invaluable content.

Innovative Capabilities

Additional capabilities like mobile malware, credential protection, content disarm and reconstruction, virus outbreak prevention, DLP, and dynamic adult image analysis add additional protection to this category.

Antispam

Work in conjunction with our mail product to dramatically reduce spam volume at the perimeter, giving you unmatched control of email attacks and infections, providing greater protection than standard real-time blacklists.

Device Security

Optimized to monitor and protect against device and vulnerability-based attack tactics while assisting you with meeting compliance.

IPS

IPS blocks the latest stealthy network-level threat and network intrusions working with the most comprehensive IPS library with thousands of signatures AND backed up by FortiGuard research credited with 850+ zero-day discoveries. Natively embedded in our context-aware policies for full control of attack detection methods to suit complex security applications and resistance to evasion techniques.

OT and IoT

Identify and police common ICS/SCADA protocols and equipment for granular visibility and control with our OT service, and reduce your attack surface with automated discovery, real-time query, segmentation, and enforcement for IoT devices.

Additional capabilities like device and OS detection and IoT hardware MAC address vendor mapping updates provide additional protection within this category.

Consistent and Coordinated Security Detection and Response

The Fortinet Security Fabric is natively integrated with FortiGuard actionable threat intelligence that is continuously updating a rich set of capabilities for content, web, device, and user security across the Fabric.

FortiGuard maintains AI-powered analysis environments across unified databases, ensuring that all products operate from the same up-to-the-minute data. Different products gain access to all relevant security technologies appropriate to their function and location across the attack plane, ensuring security is deployed consistently and enforced cohesively.

The Fabric is based on common standards and open APIs, so you can connect and leverage your existing investments with our threat insights.

		Content Security						Web Security						Device Security					
		AV	Sandbox Cloud	Credential Defense	DLP Native	Virus Outbreak	Antispam	IP Rep	Web and Video Filtering	Botnet DP	Geo IP	DNS	Web Application	Vulnerability Scan	IPS	IoT mac to Vendor Mapping	IoT Real-Time Query	OT Detection and Protection	Device/OS Detection
Security-Driven Networking	FortiGate (HW, VM, SWG)	●	●		●	●		●	●	●	●	●			●	●	●	●	●
	FortiProxy	●			●		●		●		●			●	●				
	Linksys HomeWRK	●							●	●					●				
Endpoint Security	FortiClient (ZTNA, EPP, XDR)	●	●						●	●	●	●		●	●				
Cloud Security	FortiWeb	●	●	●				●		●	●		●	●					
	FortiCASB	●									●								
	FortiADC	●	●					●	●	●		●	●		●				
	FortiMail	●	●			●	●												
	FortiDDoS							●											
Security Operation	FortiSandbox	●						●	●			●	●		●				
	FortiAnalyzer																		
	FortiSIEM																		
Open Ecosystem	+Developers Network																		●

Shared threat intelligence, IoC, Analysis & Recommendations

From our threat researchers to yours

Advanced Tools for SOC/NOC

Security Operational Teams / Network Operational Teams
Continuously evaluate and advance your security posture and set your team for success

Fabric Rating	Provide you with guided experience to design, implement, and continually advance your security posture. Fabric Rating Service provides audit checks, identifies critical vulnerabilities and configuration weaknesses, and recommends best practice implementations.
IoC	Automated breach defense system that continuously monitors your network for attacks, vulnerabilities, and persistent threats. It provides protection against legitimate threats, guarding your data, defending against fraudulent access, malware, and breaches.
Vulnerability Scan	Vulnerability scan network assets for security weaknesses, with on-demand or scheduled scans. Comprehensive reports on the security posture of your critical assets and automated scanning of remote location.
SOC-as-a-Service	Free your teams to focus on major executions by offloading all tier one analysis to our team of experts. We will notify you of any significant events that need your attention and recommend an action plan.

Purchasing Options

We provide you with the freedom to choose and mix and match between:

- A la carte
- Optimized bundles for products and use cases
- Enterprise Agreement

This data sheet includes purchasing options and bundles for the FortiGate product line. For enabling FortiGuard Security Services on all other products and for other use cases, please refer to the relevant product data sheet.

FortiGate Hardware and VM

SD-WAN and ZTNA capabilities are made available with FortiOS on all FortiGates.

FortiGuard Security Services	INDIVIDUAL		BUNDLES		
	A La Carte	Enterprise	SMB[1]	UTP	ATP
IPS	✓	✓	✓	✓	✓
Advanced Malware Protection (AMP)	✓	✓	✓	✓	✓
Antivirus	✓	✓	✓	✓	✓
Botnet	✓	✓	✓	✓	✓
Mobile Malware	✓	✓	✓	✓	✓
FortiGate Cloud Sandbox	✓	✓	✓	✓	✓
Outbreak Prevention	✓	✓	✓	✓	✓
Web Security	✓	✓	✓	✓	
Web and Content Filtering	✓	✓	✓	✓	
Secure DNS Filtering	✓	✓	✓	✓	
Video Filtering	✓	✓	✓	✓	
Antispam		✓	✓	✓	
IoT Query Service	✓	✓			
OT Protocols Signature Service	✓	✓			
NOC Services					
FortiGate Cloud (SMB Logging and Cloud Management)	✓		✓		
FortiManager Cloud [2]	✓				
Security Fabric Rating and Compliance Monitoring	✓	✓			
FortiConverter Service	✓	✓			
SD-WAN Bandwidth Monitoring	✓				
SOC Services					
FortiCloud SOCaaS (managed service)	✓				
FortiCare Support Services					
24×7	✓	✓	✓	✓	✓
Web, Chat, and Telephone	✓	✓	✓	✓	✓
1-hour Response Time SLA	✓	✓	✓	✓	✓
Base Services (included with all FortiCare support contracts)					
Application Control	✓	✓	✓	✓	✓
Geo IP Updates	✓	✓	✓	✓	✓
Device/OS Detection	✓	✓	✓	✓	✓
IoT Mac Database	✓	✓	✓	✓	✓
Trusted Certificate Database	✓	✓	✓	✓	✓
Internet Service (SaaS) Database	✓	✓	✓	✓	✓
DDNS (v4/v6)	✓	✓	✓	✓	✓
Important Add-ons					
FortiDeploy	Add-on (1 unit per P.O. to route all FortiGates for zero-touch provisioning)				
FortiCloud Premium	Add-on (required to deploy base VMs for FortiManager Cloud and FortiAnalyzer Cloud)				
FortiAnalyzer Cloud Storage top-up	Top up as needed using central FortiCloud account add-on				

[1] SMB Bundle is available for FortiGate 80F-series and below.
[2] Requires FortiCloud Premium to deploy the base FortiManager Cloud.

Order Information

The following table provides an example for the FortiGate-60F:

BUNDLES

	SKU
Hardware and Service Bundles	
FG-60F plus Enterprise Bundle	FG-60F-BDL-811-DD
FG-60F plus SMB Bundle	FG-60F-BDL-879-DD
FG-60F plus UTP Bundle	FG-60F-BDL-950-DD
FG-60F plus ATP Bundle	FG-60F-BDL-928-DD
Service Bundles	
Enterprise Bundle	FC-10-0060F-811-02-DD
SMB Bundle	FC-10-0060F-879-02-DD
UTP Bundle	FC-10-0060F-950-02-DD
ATP Bundle	FC-10-0060F-928-02-DD

A LA CARTE

	SKU
Hardware and Support	
FG-60F	FG-60F
24×7 FortiCare Support	FC-10-0060F-247-02-DD
A la Carte – FortiGuard Security Services	
IPS	FC-10-0060F-108-02-DD
AMP	FC-10-0060F-100-02-DD
Web Security	FC-10-0060F-112-02-DD
IoT Query Service	FC-10-0060F-231-02-DD
OT Signature Service	FC-10-0060F-159-02-DD
A la Carte – NOC/SOC Services	
FortiGate Cloud	FC-10-0060F-131-02-DD
FortiAnalyzer Cloud (including SOCaaS)	FC-10-0060F-464-02-DD
FortiManager Cloud	FC-10-0060F-179-02-DD
Security Fabric Rating and Compliance Service	FC-10-0060F-175-02-DD
FortiConverter Migration Service	FC-10-0060F-189-02-DD
FortiGuard Bandwidth Monitor Service	FC-10-0060F-288-02-DD
Frequently Ordered Together	
FortiDeploy (order 1 unit per Purchase Order to route all devices to FortiDeploy ZTP portal)	FDP-SINGLE-USE
FortiCloud Premium (required to launch base FortiAnalyzer Cloud and/or FortiManager Cloud instances)	FC-15-CLDPS-219-02-DD
FortiAnalyzer Cloud Log Storage Upgrade (FC1/FC2/FC3 = 5/50/500 GB/day add-on to cloud account)	FCx-10-AZCLD-463-01-DD

F:ERTINET®

www.fortinet.com