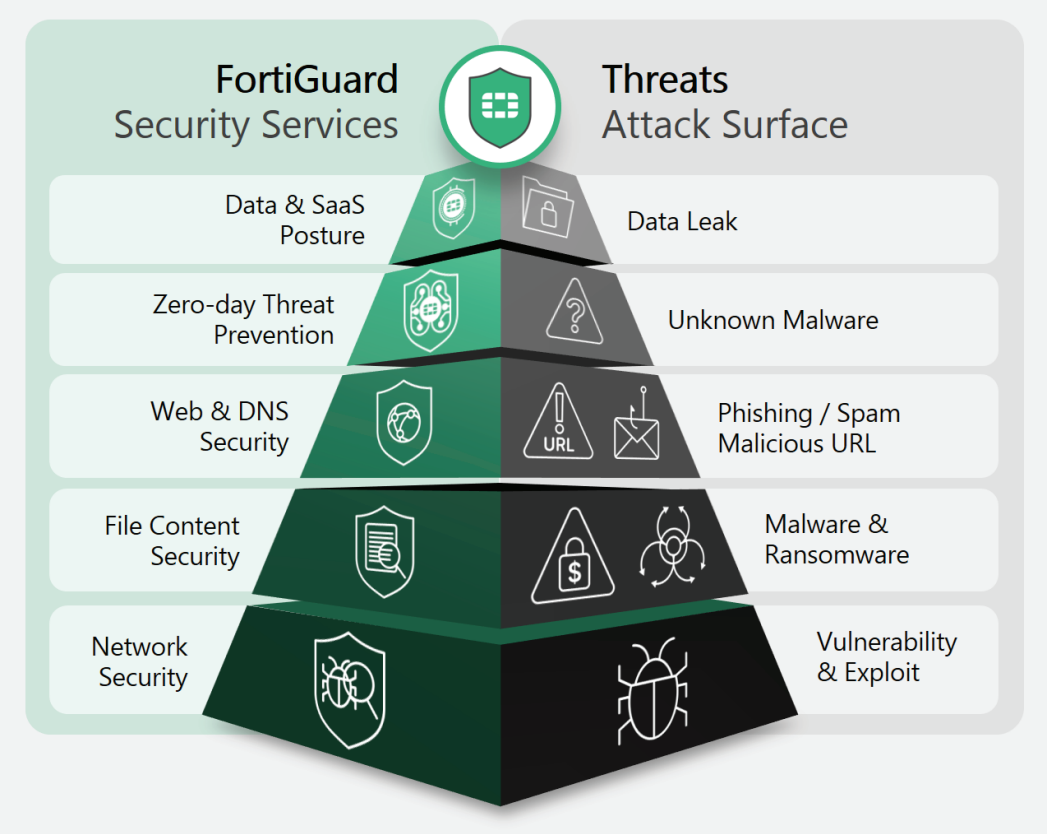
ORDERING GUIDE

FortiGuard AI-powered
Security Service Offerings

FortiGuard AI-powered Security Services offer a comprehensive array of security capabilities to protect networks, data, SaaS applications, and web usage while also providing security capabilities for enhanced NOC and SOC operations.



Imagine a pyramid representing your organization's attack surface. To effectively address your security needs, start by identifying the threats most relevant to your organization. Then, build your security strategy by selecting services that provide the appropriate coverage level for each attack surface pyramid layer. Crucially, this understanding of your threat landscape empowers you to make informed decisions about the security services you need, ultimately guiding you towards the right service bundles for your organization.

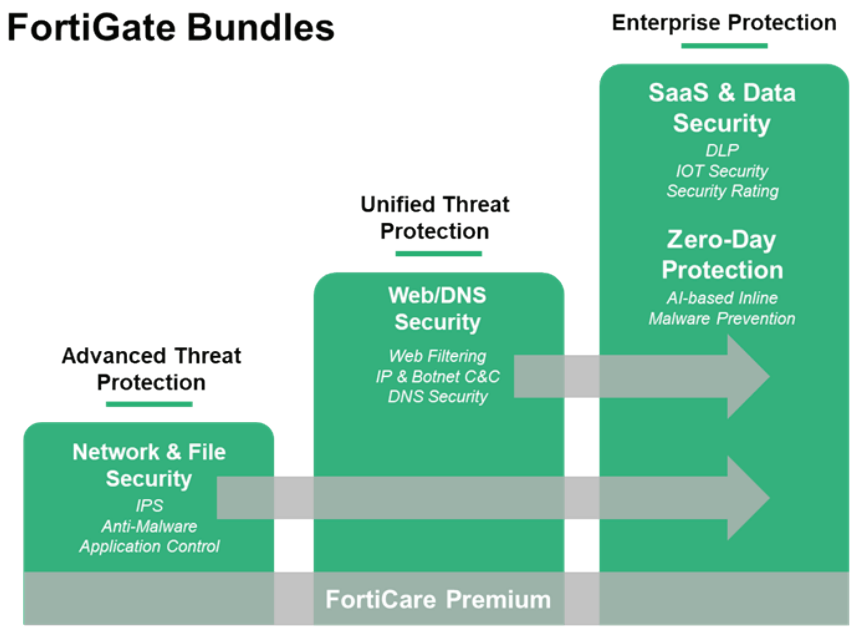
FORTIGUARD BUNDLE CORE ELEMENTS

Network & File Security: consists of IPS to monitor network traffic, analyzes for malicious content, and uses AI/ML for real-time threat detection with virtual patching, while antimalware offers real-time defense against all threats, enhances protection through threat intelligence, and provides multilayered security. Application Control enhances security compliance and offers real-time application visibility.

Web & DNS Security: offers URL filtering, which stops web-based threats, blocks malicious sites and content, and checks email links for potential threats. IP address reputation and antibotnet prevents botnet communication, blocks DDoS attacks from known sources, and offers "set and forget" functionality. DNS security defends against DNS attacks, encrypts DNS traffic for user privacy, and ensures DNS reliability with FortiGuard DNS filtering. Additionally, it includes DNSSEC, DNS tunneling blocking, and protection against DNS flood attacks; and defends against DoS/DDoS attacks.

Zero-day protection: available on all NGFWs. Inline malware prevention, included in the Enterprise Protection bundle or separately à la carte provides inline malware protection against unknown files and zero-day threats in real-time, offering sub-second verdicts. The built-in MITRE ATT&CK® matrix accelerates investigations, reducing breaches and security overhead. It focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts. Note: Zero-day threat detection is included in ATP and UTP bundles through cloud-based sandbox services.

Data & SaaS Security: consists of network DLP, which ensures visibility and protection of data in transit across networks.



You can choose our strategically curated high-value bundles tailored to meet your unique business requirements or customize your security strategy by ordering individual services à la carte.

All bundles include FortiCare Premium Technical Support services featuring 24×7×365 availability, one-hour response for critical issues, and next business-day response for non-critical matters.

PRODUCT OFFERINGS

For FortiGate hardware, virtual machines, and software-as-a-service (SaaS):

FORTIGUARD SECURITY SERVICES

INDIVIDUAL / BUNDLES				
Network Security	A La Carte	Enterprise	UTP	ATP
IPS	✓	✓	✓	✓
IPS	✓	✓	✓	✓
Malicious/Botnet URLs	✓	✓	✓	✓
File Content Security				
Advanced Malware Protection (AMP)	✓	✓	✓	✓
Antivirus	✓	✓	✓	✓
Botnet Domains	✓	✓	✓	✓
Mobile Malware	✓	✓	✓	✓
Virus Outbreak Protection	✓	✓	✓	✓
Content Disarm & Reconstruct*	✓	✓	✓	✓
AI-based Heuristic AV	✓	✓	✓	✓
FortiGate Cloud Sandbox	✓	✓	✓	✓
Zero-Day Threat Protection				
AI-based Inline Malware Prevention*	✓	✓		
Web & DNS Security				
URL, DNS & Video Filtering	✓	✓	✓	
URL Filtering	✓	✓	✓	
DNS Filtering	✓	✓	✓	
Video Filtering*	✓	✓	✓	
Malicious Certificate	✓	✓	✓	
Anti-spam		✓	✓	
Data & SaaS Posture				
Data Loss Prevention (DLP)	✓	✓		
Attack Surface Security	✓	✓		
IoT Device Detection	✓	✓		
IoT Vulnerability Correlation	✓	✓		
Security Rating	✓	✓		
Outbreak Check	✓	✓		
Operation Technology Security				
OT Security	✓			
OT Device Detection	✓			
OT vulnerability correlation & Virtual Patching	✓			
OT Application Control and IPS	✓			

SD-WAN AND SASE SERVICES

INDIVIDUAL / BUNDLES				
	A La Carte	Enterprise	UTP	ATP
SD-WAN Underlay Bandwidth and Quality Monitoring	✓			
SD-WAN Overlay-as-a-Service	✓			
SD-WAN Connector for FortiSASE Secure Private Access	✓			
SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth)	Desktop Models only			

NOC AND SOC SERVICES

INDIVIDUAL / BUNDLES				
	A La Carte	Enterprise	UTP	ATP
FortiConverter Service	✓	✓		
Managed FortiGate Service	✓			
FortiGate Cloud	✓			
FortiManager Cloud	✓			
FortiAnalyzer Cloud	✓			
FortiGuard SOCaaS	✓			

FORTICARE SUPPORT SERVICES AND INCLUDED SERVICES

INDIVIDUAL / BUNDLES				
	A La Carte	Enterprise	UTP	ATP
FortiCare Essentials	Desktop Models only			
FortiCare Premium	✓	✓	✓	✓
FortiCare Elite	✓			
Base Updates Services (Included with all FortiCare Support contracts)				
Application Control	✓	✓	✓	✓
Inline CASB*	✓	✓	✓	✓
Device/OS Detection	✓	✓	✓	✓
GeoIPs	✓	✓	✓	✓
Trusted CA Certificates	✓	✓	✓	✓
Internet Services & Botnet IPs	✓	✓	✓	✓
DDNS (v4/v6)	✓	✓	✓	✓
Local Protection	✓	✓	✓	✓
PSIRT Check	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓
Timezone	✓	✓	✓	✓

* Not available for FortiGate e/FortiWiFi 40F, 60E, 60F, 80E, 90E series, and FGR-60F series with from 7.4.4 onwards. Not available on FortiGate/FortiWiFi 30G and 50G series in any OS build.

PRODUCT DETAILS

These tables contain the service descriptions and use cases:

	SERVICE DESCRIPTION	USED IN 7.6
FortiGuard Security Services		
IPS		
IPS	FortiOS IPS features use signature-based detection and protocol analysis to identify and block malicious traffic, enhancing network security and threat response.	IPS Profile, IPS Signature and Filters
Malicious/Botnet URLs	Local URL database for drive-by exploits detection, updates IPS signatures with known malicious URLs, enabling detection and blocking of web-based threats, including botnet C&C communications and malware downloads.	IPS Profile, Block malicious URLS
Advanced Malware Protection (AMP)		
Antivirus	Antivirus signatures and engine updates provide regular updates on known virus and malware patterns, enabling detection and blocking of threats in real-time.	Antivirus profile, Antivirus scan
Botnet Domains	Domain blocking, utilizing threat intelligence to identify and prevent connections to malicious botnet command and control (C&C).	DNS Filter, Redirect botnet C&C requests to Block Portal
Mobile Malware	Detects and blocks malware threats to mobile devices, utilizing signature-based detection and behavioral analysis to safeguard these devices and prevent data breaches	Antivirus profile, Include mobile malware protection
Virus Outbreak Protection	Enhanced antivirus protection by querying malware hash signatures from FortiGuard's Global Threat Intelligence servers, enabling real-time zero-day threat detection before signatures arrive	Antivirus profile, Virus Outbreak Prevention
Content Disarm & Reconstruct	Detects and removes malicious code from files, reconstructing clean files to prevent threats, while maintaining original file functionality and format, supporting various file types and protocols.	Antivirus profile, Content Disarm and Reconstruction
AI-based Heuristic AV	Up-to-date heuristic AV Engine utilizes machine learning algorithms to detect unknown malware, analyzing file behavior and characteristics to identify and block threats in real-time, enhancing antivirus protection	CLI, "set machine-learning-detection"
FortiGate Cloud Sandbox	Submit files for advanced threat detection, analyzing files and URLs in a cloud-based environment, using behavioral analysis and machine learning to identify unknown threats	Antivirus profile, Send Files to FortiSandbox for Inspection
AI-powered Cloud sandbox	Provides Inline protection against unknown/0-day threats - holding a file for up to 50 seconds for the verdict to be returned and based on it, files can either be blocked or released.	Antivirus profile, Send Files to FortiSandbox for Inspection, Scan strategy to Inline
URL, DNS & Video Filtering		
URL Filtering	Categorizes billions of web pages, enabling users to block or allow access, with over 45 million website ratings, enhancing web filter features and providing real-time protection.	Web filter, FortiGuard filter
DNS Filtering	Blocks malicious domains and applies category-based filtering, using a vast database of known malicious and unwanted domains, to prevent DNS-based threats and enforce internet use policies	DNS Filter, FortiGuard Category Based Filter
Video Filtering	Categorizes and blocks access to videos based on FortiGuard categories, enabling control over video content, including YouTube and other video platforms, to enforce internet use policies	Video Filter, Video Filter Profile
Malicious Certificate	A dynamic package that maintains a fingerprint-based certificate blacklist, enabling the blocking of botnet communication that uses SSL, helping to prevent malware and IPS bypass attempts	SSL/SSH Inspection Profile, Blocked Certificates
Anti-Spam	Consults FortiGuard servers to help identify spammer IP address or emails, known phishing URLs, known spam URLs, known spam email checksums, and others	Email filter profile, FortiGuard Spam Filtering
Data Loss Prevention (DLP)	Comprehensive database of predefined patterns to detect sensitive data such as credit card numbers, helping to prevent data breaches and unauthorized disclosure.	DLP profile, dictionaries
Attack Surface Security		
IoT Device Detection	Up-to-date devices signature package which is used to identify and provide metadata of IoT devices. This service also query FortiGuard servers for devices that are not detected by the local Device Database or by the IoT Detection signatures	Device Detection on an interface
IoT Vulnerability Correlation	Enable mitigation of vulnerability exploits against IoT devices by supporting application of specific virtual patches on the FortiGate	NAC Policy, device patterns' category = Vulnerability, also Virtual patching profile
Security Rating	The security rating uses real-time monitoring to analyze your Security Fabric deployment, identify potential vulnerabilities, highlight best practices that can be used to improve the security. This subscription provides addition checks beyond the free base set provided	Security Rating
Outbreak Check	Add-on Security Rating checks that sourced from FortiGuard Outbreak alerts, which identify outbreaks of security incidents and exploits. This helps provide information and remediation methods within the Security Rating module.	Security Rating
OT Security		
OT Device Detection	Up-to-date devices signature package which is used to identify and provide metadata of OT devices.	Device Detection on an interface
OT vulnerability correlation & Virtual Patching	Enable mitigation of vulnerability exploits against OT devices by supporting application of specific virtual patches on the FortiGate	NAC Policy, device patterns' category = Vulnerability, also Virtual patching profile
OT Application Control and IPS	Additional signatures for industrial applications and protocols.	Application Control and IPS profiles

PRODUCT DETAILS

	SERVICE DESCRIPTION	USED IN 7.6
SD-WAN and SASE Services		
SD-WAN Underlay Bandwidth and Quality Monitoring	Speed test tool provides a convenient and accurate way to measure bandwidth speeds, helping users optimize SD-WAN configuration and ensure reliable network performance.	CLI, "execute speed-test"
SD-WAN Overlay-as-a-Service	Simplifies SD-WAN overlay network provisioning with a GUI wizard, enabling secure and efficient connectivity between branches and data centers through dynamic path optimization and shortcut tunnels.	Access via https://overlay-as-a-service.forticloud.com
SD-WAN Connector for FortiSASE Secure Private Access	This license allows FortiSASE to connect to a FortiGate SD-WAN network as a new spoke.	Refer to KB article 293562
SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth)	Entitles a FortiGate to connect to FortiSASE as a "Secure Edge". Internet traffic is optionally inspected in FortiSASE rather than on-premise.	Refer to FortiOS Admin Guide article 231401
NOC and SOC Services		
FortiConverter Service	FortiConverter Service for one time configuration conversion	
Managed FortiGate Service	Available 24×7, with Fortinet NOC experts performing device setup, network, and policy change management.	
FortiGate Cloud	Management, Analysis, and 1 Year Log Retention.	
FortiGuard SOCaaS	24×7 cloud-based managed log monitoring, incident triage and SOC escalation service.	
Base Updates Services (Included with all FortiCare Support contracts)		
Application Control	Use for Identifying applications with precise signatures, enabling granular policy enforcement, improved security, and optimized network performance, covering a wide range of applications and protocols.	Application Control Profile
Inline CASB	Real-time updated definitions support Inline CASB security profile used in firewall policies to enables visibility, control, and security for cloud-based applications.	Inline CASB Profile
Device/OS Detection	Allows FortiOS to monitor networks and gather information about devices operating on those networks. These information is then made available on GUI, providing deep visibility to users.	Interfaces. Device Detection and Assets & Identities dashboard
GeoIPs	A database that maps IP addresses to geographical locations, enabling FortiGate to enforce geo-based policies, block traffic from specific countries, and meet compliance requirements, with regular updates for accuracy.	Policy & Objects, Addresses
Trusted CA Certificates	This database comprises of popular and default trusted CA Certificates so it can be excluded from the action to take when a server certificate is not issued by a trusted CA.	SSL/SSH Inspection profile, Untrusted SSL certificates
Internet Services & Botnet IPs	The Internet Service Database is a comprehensive public IP address database that combines IP address range, IP owner, service port number, and IP security credibility. It also hosts list of Botnet IPs.	Firewall, policy, Destination, Internet Service and IPS, Botnet C&C, scan outgoing connections to botnet sites
DDNS (v4/v6)	A hosted service entitlement that enables FortiGate to maintain accurate domain-name-to-IP-address mappings, supporting dynamic IP addresses and ensuring reliable connectivity for remote access and VPNs.	Network, DNS, Dynamic DNS
Local Protection	A virtual patching solution that enables Fortinet to push a subset of IPS signatures to protect FortiGate management interfaces (GUI/SSH) from vulnerabilities, without requiring an upgrade.	CLI, "config firewall local-in-policy ", "set virtual-patching enable"
PSIRT Check	Enhances Security Rating with this add-on package, identifying PSIRT vulnerabilities of connected Fabric devices, then encourage administrators to updating any affected devices.	Security Rating and various alerts on GUI
Anti-Phishing	Pre-defined username and password field patterns for credential phishing prevention scanning under web filtering feature.	CLI, "config webfilter profile", "config antiphish"
Timezone	Dynamically updated IANA timezone database	N/A

OTHER OFFERINGS

IMPORTANT ADD-ONS

	INDIVIDUAL / BUNDLES
FortiDeploy	Add-on (1 unit per P.O. to route all FortiGates for Zero Touch provisioning)
FortiCloud Premium	Add-on
FortiAnalyzer Cloud Storage Top-up	Add-on

ORDER INFORMATION

The following provides an example for the FortiGate 60F:

BUNDLES

	SKU
Hardware and Service Bundles	
FG-60F plus Enterprise Bundle	FG-60F-BDL-809-DD
FG-60F plus UTP Bundle	FG-60F-BDL-950-DD
Service Bundles	
Enterprise Bundle	FC-10-0060F-809-02-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
AI-based Inline Malware Prevention	FC-10-0060F-577-02-DD
OT Security	FC-10-0060F-159-02-DD
A La Carte - NOC/SOC Services	
FortiGate Cloud	FC-10-0060F-131-02-DD
FortiAnalyzer Cloud	FC-10-0060F-585-02-DD
Managed FortiGate (NOC)	FC-10-0060F-660-02-DD
SOC-as-a-service (including FortiAnalyzer Cloud)	FC-10-0060F-464-02-DD
Attack Surface Security	FC-10-0060F-231-02-DD
FortiConverter Migration Service	FC-10-0060F-189-02-DD
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	FC-15-CLDPS-219-02-DD
FortiAnalyzer Cloud Log Storage Add-on (FC1/FC2/FC3 = 5/50/500 GB/day add-on to cloud account)	FCx-10-AZCLD-463-01-DD

FREQUENTLY ASKED QUESTIONS

How does the ordering process work?
Consider in three parts:

New Order. Order one of the following:

- Hardware with a bundle that includes FortiCare and FortiGuard services.
- Hardware only (a la carte) and add FortiCare and FortiGuard services to it.

Renew Services

You can order service renewals as bundles or a La Carte and applied to the device under the FortiCare account. Services will be extended based on the contract purchased.
NOTE: Renewal services purchased with a FortiCare quote ID generated by Disti are automatically registered to the serial number.

Add Services to an Existing Unit
Normally, customers want to align the end date, so that all components (existing and new) renew/expire together. This can be performed with a co-term. You can request a co-term quotation to your Fortinet-authorized partner.

FORTINET TRAINING AND CERTIFICATION

Security Operations (SOP)- 2 Days Training
Explore the practical use of Fortinet security operations solutions to detect, investigate, and respond to Advanced Persistent Threats (APTs). With the hands-on labs, helps understand how to execute advanced threats, how threat actors behave, and how security operations handle such threats.

Web Application Security (WAS) - 1 Day Training
Explore web application threats and countermeasures focused on Fortinet solutions. This course will guide you from the very motivations of attacks on web applications through to understanding and executing attack techniques, recognizing such attacks, and, finally, configuring Fortinet solutions to mitigate them.

Malware Analysis (MWA) - 2 Days Training

Explore practical use of 3rd party (open source), Fortinet solutions for malware analysis, the fundamental concepts of malware analysis, perform basic analysis using open-source tools, and leverage Fortinet solutions for advanced and automated malware analysis.

Threat Hunting (FTH) - 3 Days Training

Explore the practical use of Fortinet solutions as threat intelligence and threat hunting platforms, explore fundamental concepts about cyber threat intelligence and how to leverage Fortinet solutions to perform threat intelligence management (collection, enrichment, and so on) and threat hunting.

Ordering Information

SKU	DESCRIPTION
FT-PRIVATE / FT-PRIVATE-MIN	Contact regional training team for quote.
FT-CST-WAS-LAB	On-demand self-paced labs
FT-CST-MWA-LAB	

Certification
No certification

Course Description

For more information about prerequisites, agenda topics and learning objectives, please refer to the course description at:

COURSE	LINK
Security Operations	https://training.fortinet.com/local/staticpage/view.php?page=library_security-operations
Web Application Security	https://training.fortinet.com/local/staticpage/view.php?page=library_web-application-security
Malware Analysis	https://training.fortinet.com/local/staticpage/view.php?page=library_malware-analysis
Threat Hunting	https://training.fortinet.com/local/staticpage/view.php?page=library_threat-hunting

Visit www.fortinet.com for more details