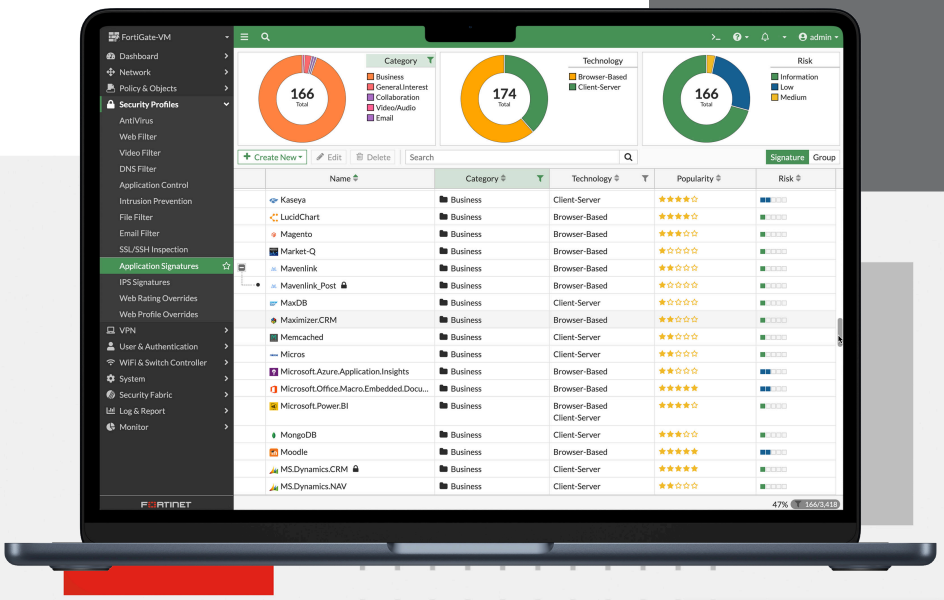
FortiGate®-VM on Amazon Web Services



Highlights

- Securely connect to your application workloads without performance bottlenecks
- Move at cloud speed without compromising security
- Seamlessly scale your cloud protection without increasing operational burden
- Secure your cloud transformation without impacting business outcomes, with flexible consumption models

Adaptive Multi-Cloud Security with AI-Powered Advanced Threat Protection

The FortiGate-VM on AWS delivers next-generation firewall capabilities for organizations of all sizes, with the flexibility to be deployed as next-generation firewall or VPN gateway. It protects against cyber threats with high performance, security efficacy, and deep visibility.

FortiGate-VM delivers protection from a broad array of network security threats. It offers the same security and networking services included in the FortiOS operating system and is available for public cloud, private cloud, and Telco Cloud (VNFs). With a consistent operational model across hybrid cloud, multi-cloud, and service provider environments, it reduces the training burden on security teams.

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

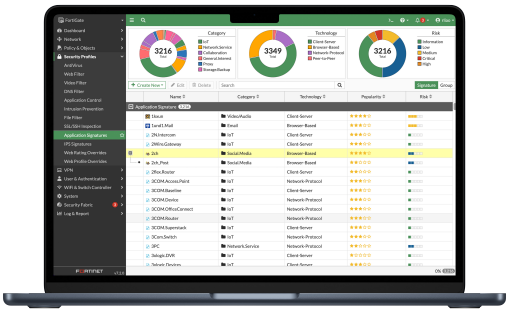
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations



Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Migration Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.



FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

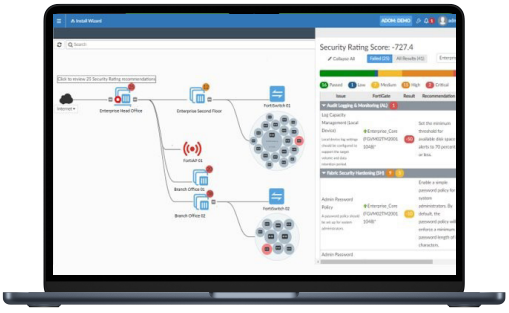
Advanced Virtual Security Processing Units (vSPUs)

Virtual firewalls are commonly used to protect virtualized environments in software-defined data centers and multi-cloud environments on the basis that they are the least expensive and the most portable, enabling users to easily move a virtual firewall from cloud to cloud. One disadvantage of most virtual firewalls is that they deliver significantly lower network throughput as compared with physical firewalls, creating bottlenecks throughout the network and reducing business agility and performance.

FortiGate virtual firewalls (FortiGate-VM), featuring advanced virtual security processing units (vSPUs), overcome the throughput barrier to provide top performance in private and public clouds. With FortiGate-VM, organizations can securely migrate any application and support a variety of use cases, including highly available large-scale virtual private networks (VPNs) in the cloud."

FortiGate-VM removes the cost-performance barriers to adopting virtual NGFWs, with several industry-leading features:

- The FortiGate-VM vSPU is a unique technology that enhances performance by offloading part of packet processing to user space, while using a kernel bypass solution within the operating system. With vSPU enabled, FortiGate-VM can achieve more than triple the throughput for a UDP firewall rule.
- Fortinet is the first NGFW vendor to support AWS C5n instances, which enables organizations to use a virtual firewall to secure compute-heavy applications in the cloud.



Intuitive view and clear insights into network security posture with FortiManager

Centralized Network and Security Management at Scale

FortiManager, the centralized management solution from Fortinet, enables integrated management of the Fortinet security fabric, including devices like FortiGate, FortiSwitch, and FortiAP. It simplifies and automates the oversight of network and security functions across diverse environments, serving as the fundamental component for deploying Hybrid Mesh Firewalls.

Deployment

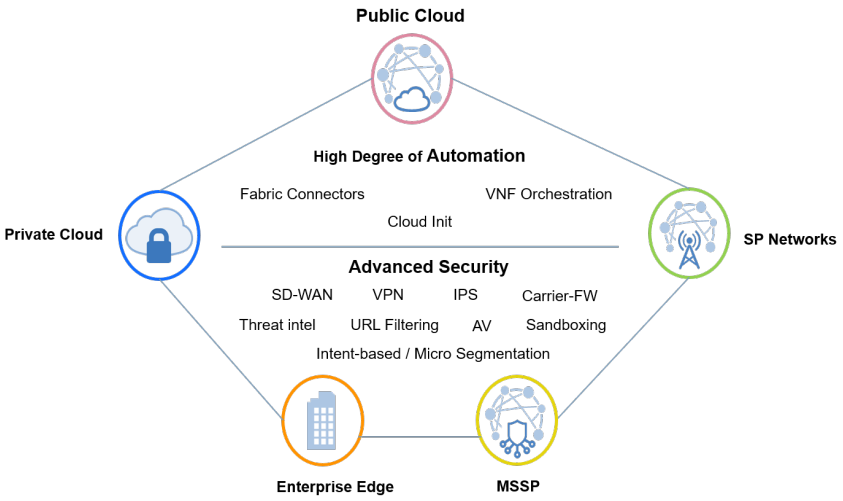
Next Generation Firewall (NGFW)

- Reduce complexity by combining threat protection security capabilities into single high-performance network security appliances
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in your network traffic
- Deliver the industry's highest SSL inspection performance using industry-mandated ciphers while maximizing ROI
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection

VPN Gateway

- Direct Connect utilizing FortiGate firewalls for SSL and IPsec VPNs into and out of the AWS VPCs
- VGW to FortiGate VPN between VPCs
- Hybrid cloud site to site IPsec VPN
- Remote access VPN

Gain Comprehensive Visibility and Apply Consistent Control



AWS Integration

- Fortinet embeds the latest AWS Auto Scaling functionality and FortiGate CloudFormation template configuration into our cloud Security Fabric, providing automation based on resource demand from your cloud workloads
- Accelerate time-to-protection for new threats detected by AWS GuardDuty by deploying native AWS scripting to automatically push malicious IP or DNS addresses into dynamic FortiGate policies
- Provide service resiliency with AWS native load balance

Specifications

The C6in instance family leverages the Intel IceLake Processors. FortiGate-VM is available for purchase in all regions, including AWS GovCloud and AWS China. The following is the system requirement for BYOL licenses:

	VM-01S	VM-02S		VM-04S		VM-08S		VM-16S		VM-32S		VM-ULS
System Requirement												
vCPU (Minimum / Maximum)	1 / 1	1 / 2		1 / 4		1 / 8		1 / 16		1 / 32		1 / Unlimited
Technical Specifications												
Network Interface Support (Minimum / Maximum) [1]	1 / 24	1 / 24		1 / 24		1 / 24		1 / 24		1 / 24		1 / 24
Virtual Domains (Default / Maximum) [2]	2 / 10	2 / 25		2 / 50		2 / 500		2 / 500		2 / 500		2 / 500
Firewall Policies	10 000	10 000		10 000		200 000		200 000		200 000		200 000
System Performance		**ENA Driver - Yes**		**ENA Driver - Yes**		**ENA Driver - Yes**		**ENA Driver - Yes**		**ENA Driver - Yes**		
Instance Shape to be Measured		**C6in.LARGE**		**C6in.XLARGE**		**C6in.2XLARGE**		**C6in.4XLARGE**		**C6in.8XLARGE**		
AWS Bandwidth [3]		**Up to 25 Gbps**		**Up to 30 Gbps**		**Up to 40 Gbps**		**Up to 50 Gbps**		**50 Gbps**		
		Native	**IPSEC**	**Native**	**IPSEC**	**Native**	**IPSEC**	**Native**	**IPSEC**	**Native**	**IPSEC**	
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes*		16 960	2020	21 200	3370	31 600	5350	50 000	9950	51 900	11 850	
Firewall Throughput (UDP Packets) in Mbps - 512 bytes*		5760	1020	9900	1630	10 900	2640	17 000	4600	18 500	5600	
Firewall Throughput (UDP Packets) in Mbps - 64 bytes*		720	170	1200	270	1420	450	2300	710	2380	850	
New Sessions / Second (TCP)		140 000	-	216 000	-	240 000	-	280 000	-	340 000	-	
HTTP Throughput w/ Application profile (64K size) [4] **in Mbps**		10 700	-	15 800	-	29 000	-	29 400	-	30 500	-	
HTTP Throughput w/ IPS profile (44K size) in Mbps		10 500	-	15 700	-	28 800	-	28 900	-	29 900	-	
HTTP Throughput w/ IPS profile (1M size) [5] **in Mbps**		10 800	-	15 800	-	29 000	-	29 100	-	30 000	-	
NGFW Throughput [6] **in Mbps**		790	-	1420	-	2790	-	5430	-	10 000	-	
Threat Protection Throughput [7] **in Mbps**		780	-	1380	-	2740	-	5340	-	9900	-	
SSL Inspection Throughput in Mbps [8]		1810	-	3350	-	6540	-	14 000	-	24 800	-	

Notes.

All performance values are “up to” and vary depending on system configuration.
Actual performance may vary depending on the network and system configuration.
Please note that these metrics are updated periodically as the product performance keeps improving through internal testing.
The discrepancy in the performance numbers may be noted in different versions of the document so please make sure to refer to the latest datasheets.
Performance metrics were observed using FortiGate-VM BYOL instances using FOS v7.6.0.

1. Applicable to 6.4.0+. The actual working number of consumable network interfaces varies depending on AWS instance types/sizes and may be less.
2. FG-VMxxS series do not come with a multi-VDOM feature by default. You can add it by applying separate VDOM addition perpetual licenses. See ORDER INFORMATION for VDOM SKUs.
3. The latest information about AWS bandwidth is found on https://aws.amazon.com/ec2/instance-types/.
4. Application Control performance is measured with 64 Kbyte HTTP traffic.
5. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
6. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
7. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
8. SSL Inspection Throughput is measured using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).

For the sizing guide, please refer to the sizing document available on www.fortinet.com

Specifications

The C8gn instance family uses the Graviton3 ARM based Processors. FortiGate-VM is available for purchase in all regions, including AWS GovCloud and AWS China. The following is the system requirement for BYOL licenses:

	VM-01S	VM-02S		VM-04S		VM-08S		VM-16S		VM-32S		VM-ULS
System Requirement												
vCPU (Minimum / Maximum)	1 / 1	1 / 2		1 / 4		1 / 8		1 / 16		1 / 32		1 / Unlimited
Technical Specifications												
Network Interface Support (Minimum / Maximum) [1]	1 / 24	1 / 24		1 / 24		1 / 24		1 / 24		1 / 24		1 / 24
Virtual Domains (Default / Maximum) [2]	2 / 10	2 / 50		2 / 50		2 / 50		2 / 500		2 / 500		2 / 500
Firewall Policies				10 000		200 000		200 000		200 000		200 000
System Performance		**ENA Driver - Yes**		**ENA Driver - Yes**		**ENA Driver - Yes**		**ENA Driver - Yes**		**ENA Driver - Yes**		
Instance Shape to be Measured		**C8gn.LARGE**		**C8gn.XLARGE**		**C8gn.2XLARGE**		**C8gn.4XLARGE**		**C8gn.8XLARGE**		
AWS Bandwidth [3]		**Up to 30 Gbps**		**Up to 40 Gbps**		**Up to 50 Gbps**		**50 Gbps**		**100 Gbps**		
		Native	**IPSEC**	**Native**	**IPSEC**	**Native**	**IPSEC**	**Native**	**IPSEC**	**Native**	**IPSEC**	
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes		27 000	1900	34 000	4600	50 000	5950	51 700	9450	74 500	14 000	
Firewall Throughput (UDP Packets) in Mbps - 512 bytes		9500	1280	11 800	2900	17 200	3750	17 800	5200	18 250	8200	
Firewall Throughput (UDP Packets) in Mbps - 64 bytes		1500	360	1920	750	2300	980	2900	1130	2950	2000	
New Sessions / Second (TCP)		200 000	—	200 000	—	220 000	—	290 000	—	350 000	—	
HTTP Throughput w/ Application profile (64K size)[4] **in Mbps**		18 000	—	26 000	—	27 500	—	29 500	—	30 500	—	
HTTP Throughput w/ IPS profile (44K size) in Mbps		17 500	—	25 700	—	27 000	—	29 000	—	29 900	—	
HTTP Throughput w/ IPS profile (1M size) [5] **in Mbps**		18 000	—	25 600	—	27 500	—	29 100	—	30 000	—	
NGFW Throughput in Mbps [6]		1230	—	2300	—	4300	—	8500	—	14 100	—	
Threat Protection Throughput in Mbps [7]		1200	—	2250	—	4180	—	8350	—	13 800	—	
SSL Inspection Throughput in Mbps [8]		3430	—	6250	—	11 400	—	22 550	—	28 300	—	

Notes.

Actual performance may vary depending on the network and system configuration.
Please note that these metrics are updated periodically as the product performance keeps improving through internal testing.
The discrepancy in the performance numbers may be noted in different versions of the document so please make sure to refer to the latest datasheets.
Performance metrics were observed using FortiGate-VM BYOL instances using FOS v7.6.4.

1. Applicable to 7.6.1+. The actual working number of consumable network interfaces varies depending on AWS instance types/sizes and may be less.
2. FG-VMxxV and FG-VMxxS series do not come with a multi-VDOM feature by default. You can add it by applying separate VDOM additional perpetual licenses. See ORDER INFORMATION for VDOM SKUs.
3. The latest information about AWS bandwidth is found on https://aws.amazon.com/ec2/instance-types/.
4. Application Control performance is measured with 64 Kbyte HTTP traffic.
5. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
6. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
7. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
8. SSL Inspection Throughput is measured using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).

For the sizing guide, please refer to the sizing document available on www.fortinet.com

Licensing

With a multitude of deployment methods supported across various private and public cloud deployments, FortiGate-VM for AWS supports both on-demand (PAYG) and bring-your-own-license (BYOL) licensing models.

On-demand licensing is a highly flexible option for both initial deployments and growing them as needed. With a wide selection of supported instance types, there is a solution for every use case. This license offers FortiOS with a UTP bundle.

BYOL is ideal for migration use cases, where an existing private cloud deployment is migrated to a public cloud deployment. When using an existing license, the only additional cost would be the price for the AWS instances.

Ordering Information

The following SKUs adopt the annual subscription licensing scheme:

Product	SKU	Description
FortiGate-VM01-S	FC1-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (1 vCPU core)
FortiGate-VM02-S	FC2-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (2 vCPU cores)
FortiGate-VM04-S	FC3-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (4 vCPU cores)
FortiGate-VM08-S	FC4-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (8 vCPU cores)
FortiGate-VM16-S	FC5-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (16 vCPU cores)
FortiGate-VM32-S	FC6-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (32 vCPU cores)
FortiGate-VMUL-S	FC7-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (Unlimited vCPU cores)

FortiOS 6.2.3+ and 6.4.0+ support the FortiGate-VM S-series. The FortiGate-VM S-series does not have RAM restrictions on all vCPU levels.
FortiManager 6.2.3+ and 6.4.0+ support managing FortiGate-VM S-series devices.

Optional Accessories/Spares	SKU	Description
Virtual Domain License Add 5	FG-VDOM-5-UG	Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 15	FG-VDOM-15-UG	Upgrade license for adding 15 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 25	FG-VDOM-25-UG	Upgrade license for adding 25 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 50	FG-VDOM-50-UG	Upgrade license for adding 50 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 240	FG-VDOM-240-UG	Upgrade license for adding 240 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.

FG-VMxx"V" 6.0.0 supports VDOM by adding separate VDOM licenses. The number of configurable VDOMs can be stacked up to the maximum number of supported VDOMs per vCPU model. Please refer to Virtual Domains (Maximum) under SPECIFICATIONS.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles: Enterprise Protection	Bundles: Unified Threat Protection	Bundles: Advanced Threat Protection	Bundles: SD-WAN
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•	
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct, AI-based Heurestic AV, FortiGate Cloud Sandbox[1]	•	•	•	•	
	URL, DNS and Video Filtering — URL, DNS and Video Filtering, Malicious Certificate[1]	•	•	•		
	Anti-Spam		•	•		
	AI-based Inline Malware Prevention	•	•			
	Data Loss Prevention (DLP)[2]	•	•			
	IoT Security — IoT Device Detection, IoT Vulnerability Correlation, and Virtual Patching[3]		•			•
	Security Rating (and Outbreak Check)[3]		•			•
	OT Security—OT Device Detection, OT Vulnerability Correlation and Virtual Patching, OT Application Control and IPS[2]	•				
	Application Control	----------included with FortiCare Subscription----------				
	Inline CASB[1]	----------included with FortiCare Subscription----------				
SD-WAN and SASE Services	SD-WAN SLA Database					•
	SD-WAN Underlay and Application Monitoring Service					•
	SD-WAN Overlay Orchestration Service					•
	SD-WAN Connector for FortiSASE Secure Private Access					•
	FortiSASE Starter Kit for n* Users[4]					•
	One Year Cloud-based Log Retention					•
	FortiTelemetry Cloud					•
NOC and SOC Services	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	•				
	FortiManagement Cloud—Management, Analysis, and One Year Log Retention	•				
	FortiManager Cloud	•				
	FortiAnalyzer Cloud	•				
	FortiGuard SOCaaS—24×7 Cloud-Based Managed Log Monitoring, Incident Triage, and SOC Escalation Service	•				
Hardware and Software Support	FortiCare Essentials	Desktop models only				
	FortiCare Premium[3]	•	•	•	•	•
	FortiCare Elite	•				
Base Services	Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing	----------included with FortiCare Subscription----------				

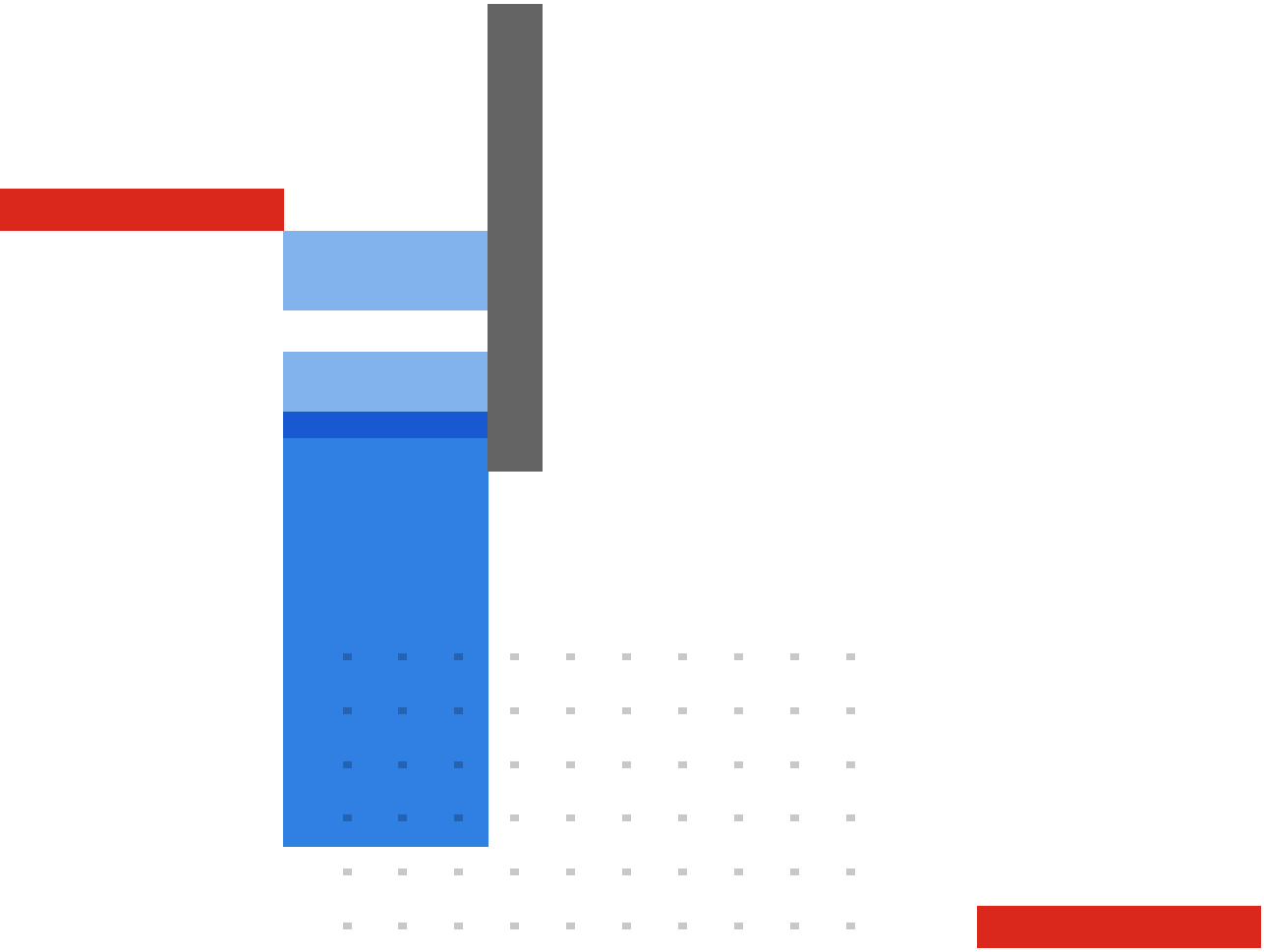
1. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Not available for SD-WAN Bundle SKU FC-10-XXXXX-1387-02-DD.
4. Only supported on FortiGate/FortiWiFi models from the 70F (F-series and all later series) and FGR-60G onwards. See the FortiSASE Ordering Guide for supported models and corresponding user license allocations.

FortiGuard AI-Powered Security Bundles offer curated security services to combat known, unknown, zero-day, and emerging AI threats. They protect against malicious content, web threats, and secure IT/OT/IoT devices, applications, users, and data. All bundles include FortiCare Premium Services with 24×7×365 support, one-hour critical response, and next-business-day noncritical response.

Fortinet's FortiCare Services support the Security Fabric throughout its lifecycle—Design, Deploy, Operate, Optimize, and Evolve. FortiCare Elite delivers enhanced SLAs, rapid issue resolution, dedicated support, 18 months of extended engineering support, and a unified portal for device and security health, improving operational efficiency and deployment performance.

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.



FORTINET

www.fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

October 1, 2026

FG-VM-AWS-DAT-R39-20261001