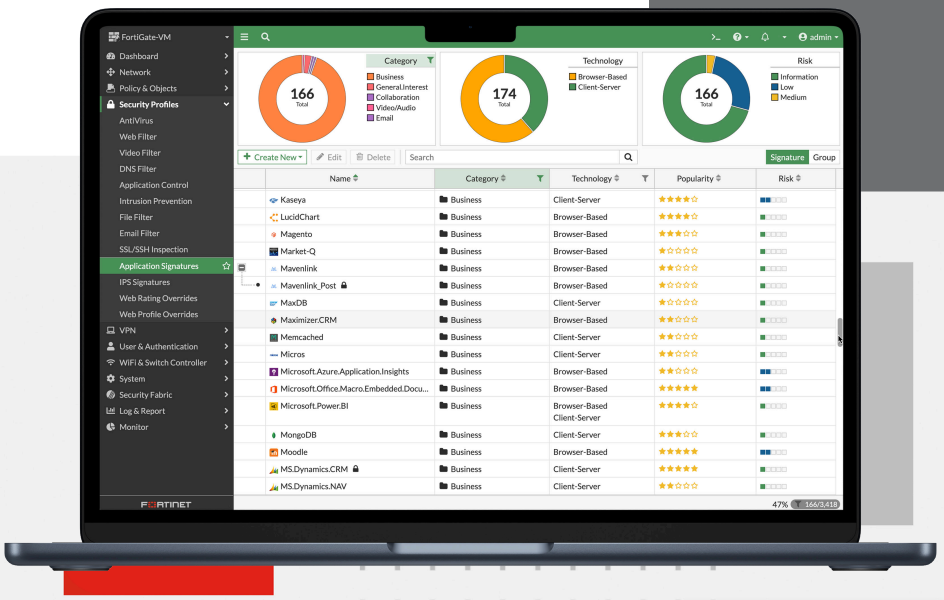
FortiGate® Virtual Appliances



Highlights

- Protection from a broad array of threats, with support for all of the security and networking services that the FortiOS operating system offers
- Increased visibility within virtualized infrastructure monitoring
- Consistent security with central management across your entire compute infrastructure
- Move and scale your cloud firewalls without impacting business outcomes, with flexible consumption models

Consistent Security for Cloud and Virtualized Environments

Fortinet FortiGate VM is a cloud firewall that provides robust, consistent security across cloud and hybrid environments. By consolidating security tools into a single platform, it optimizes your security investment while improving threat response.

FortiGate VM delivers exceptional performance and security with no degradation of service or protection. As part of the Fortinet Security Fabric, it extends across clouds and distributed locations, mitigating blind spots in virtual infrastructures. FortiGate VM can be rapidly deployed, managed through a centralized platform, and offers a range of purchasing options to suit every need.

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



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 service 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

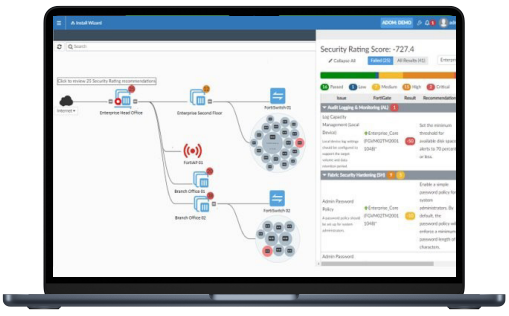
Advanced Virtual Security Processing Units (vSPUs)

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.
- Support for Intel QuickAssist Technology (Intel QAT), working on the latest QuickAssist Adapters, accelerates traffic processing through site-to-site IPSec VPNs. With QAT enabled, FortiGate-VM can achieve two to three times throughput improvements depending on the packet frame size.
- 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

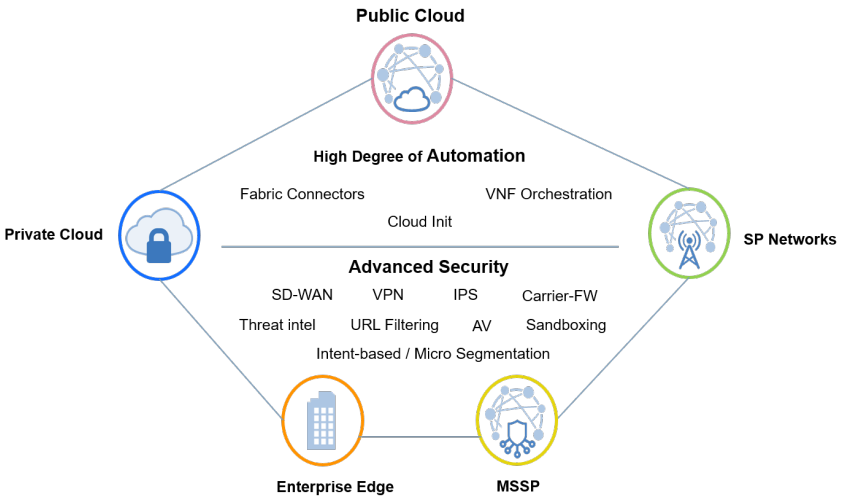
Next Generation Firewall (NGFW)

- 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 VPNs into and out of the VPCs
- VGW to FortiGate VPN between VPCs
- Hybrid cloud site to site IPsec VPN
- Remote access VPN

Gain Comprehensive Visibility and Apply Consistent Control



Available in

Appliance

Virtual

Hosted

Cloud

Container

Deployment and Automation

FortiGate VM offers versatile deployment options across both public and private clouds, supporting all major public clouds including AWS, Azure, and Google as well as most hypervisors such as VMware, Hyper-V, and KVM. These deployments enable organizations to create scalable, high-performance firewalls that can be tailored to different virtualized environments and hyper-scale public cloud infrastructures. FortiGate VM integrates seamlessly with various infrastructure as code (IaC) tools such as Jenkins and GitLab, supporting security as code practices. Common IaC methods include Terraform modules for cloud resource orchestration, AWS CloudFormation templates, Ansible playbooks for automated configuration management, and REST API integration for fine-grained control and rapid deployment.

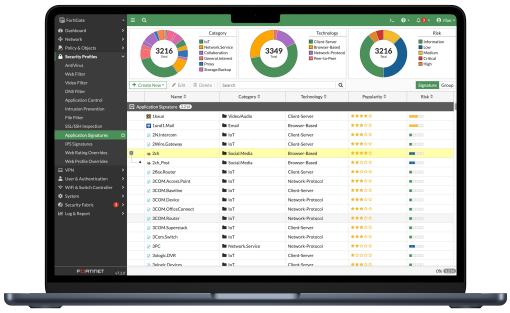
Cloud Integration

The FortiGate VM deep, native integrations with public clouds that empower organizations to:

- Automate security operations: Leverage cloud-native tools and serverless functions for rapid response and scaling
- Centralize visibility and analytics: Streamline log forwarding and event correlation into leading cloud SIEM and SOAR platforms
- Scale protection dynamically: Use auto scaling, load balancing, and IaC along with flexible licensing to match security capacity with business needs
- Enforce consistent policies: Integrate with cloud identity, tagging, and networking services for unified policy enforcement across environments



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.

Specifications

	VM-01S	VM-02S	VM-04S	VM-08S	VM-16S	VM-32S	VM-ULS
Technical Specifications							
vCPU Support (Minimum / Maximum)	1 / 1	1 / 2	1 / 4	1 / 8	1 / 16	1 / 32	1 / unlimited
Storage Support (Minimum / Maximum)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
Firewall Policies	10 000	10 000	10 000	200 000	200 000	200 000	200 000
Virtual Domains (Default / Maximum) *	2 / 10	2 / 25	2 / 50	2 / 500	2 / 500	2 / 500	2 / 500
Maximum Number of Wireless Access Points Controlled (Tunnel / Global)	32 / 64	512 / 1024	512 / 1024	1024 / 4096	1024 / 4096	1024 / 4096	1024 / 4096
Maximum Number of FortiSwitches	8	24	64	300	300	300	300
Maximum Number of Registered Endpoints	2000	2000	8000	20 000	20 000	20 000	20 000
Unlimited User License	✓	✓	✓	✓	✓	✓	✓

Note: All performance values are “up to” and vary depending on system configuration.

Network Interface Support

The maximum number of network interfaces consumable by a FortiGate instance is 24 starting with FortiGate version 6.4.0. Prior versions allow 18. The minimum number is 1. The actual number of network interfaces attachable to instances varies depending on cloud platforms and instance types, and they may not allow you to attach the greater number of interfaces to an instance than their maximum limits even while FortiGate allows up to 24.

* FG-VM S-Series does not come with a multi-VDOM feature by default. You can add it by applying separate subscription VDOM licenses. See ORDERING INFORMATION for VDOM SKUs.

VENDOR
Private Clouds (Hypervisors)
VMware ESXi v6.7 / v7.0 / v8.0
VMware NSX-T* v3.2 / v4.0
Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019**
Microsoft AzureStack
Red Hat OpenShift Virtualization 4.17.13***
Citrix Xen XenServer v5.6 sp2, v6.0, v6.2 and later
Open source Xen v3.4.3, v4.1 and later
KVM qemu 0.12.1 & libvirt 0.10.2 and later for Red Hat Enterprise Linux / CentOS 6.4 and later / Ubuntu 16.04 LTS (generic kernel)
KVM qemu 2.3.1 for SuSE Linux Enterprise Server 12 SP1 LTSS
Nutanix AHV 7.3****
CSP 5000 Series*****

* See the NSX-T on VMware Compatibility Guide for the latest supported platforms

** FortiGate-VM 6.2.3+ supports Microsoft Hyper-V 2019

*** FortiGate-VM 7.6.0+

**** FortiOS 7.6.3+

***** FortiOS 6.4.10, 7.0.8, 7.2.3

VENDOR
Public Clouds (Marketplaces)
Amazon AWS (including GovCloud and AWS China)
VMware Cloud on AWS
Microsoft Azure (including regional Azure: US Gov, Germany, and China) and AzureStack syndication
Google GCP (Google Cloud Platform)
Oracle OCI
Alibaba Cloud (AliCloud)
IBM Cloud (Gen1 / Gen2)

Virtualization/Cloud Platform Support varies by model and FortiOS builds.
Please refer to appropriate release notes.

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 6.4.0+ and 7.x+ support the FortiGate-VM S-series. The FortiGate-VM S-series does not have RAM restrictions on all vCPU levels.
FortiManager 6.4.0+ and 7.x+ support managing FortiGate-VM S-series devices.

Optional Accessories/Spares	SKU	Description
VDOM Subscription License for FortiGate S Series	FC1-10-FGVVS-498-02-DD	Subscription license for adding VDOMs to FortiGate-VM S-series running FortiOS 6.4.9/7.0.2 or higher. This is a seat-based SKU where each seat is equal to 5 vdoms and max number of seats is 100 (500 vdoms)

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

For hard-coded firmware ceilings for a specific software version, visit: Maximum Values Table Tool.

The link to the max value table: https://docs.fortinet.com/max-value-table?product_family=fortigate&family=fortigate

Product Offerings

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

FortiGuard Security Services

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles. FG VM subscribed through cloud marketplaces comes with the UTP bundle.

	INDIVIDUAL / BUNDLES			
NETWORK SECURITY	A LA CARTE	ENTERPRISE	UTP	ATP
IPS	✓	✓	✓	✓
IPS	✓	✓	✓	✓
Malicious/Botnet URLs	✓	✓	✓	✓
FILE CONTENT SECURITY				
Advanced Malware Protection (AMP)	✓	✓	✓	✓
Antivirus (AV)	✓	✓	✓	✓
Botnet Domains	✓	✓	✓	✓
Mobile Malware	✓	✓	✓	✓
Virus Outbreak Protection	✓	✓	✓	✓
Content Disarm and Reconstruct*	✓	✓	✓	✓
AI-based Heuristic AV	✓	✓	✓	✓
FortiGate Cloud Sandbox	✓	✓	✓	✓
ZERO-DAY THREAT PROTECTION				
AI-based Inline Malware Prevention*	✓	✓		
WEB AND DNS SECURITY				
URL, DNS, and Video Filtering	✓	✓	✓	
URL Filtering	✓	✓	✓	
DNS Filtering	✓	✓	✓	
Video Filtering*	✓	✓	✓	
Malicious Certificate	✓	✓	✓	
Anti-Spam		✓	✓	
DATA AND 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 and Virtual Patching	✓			
OT Application Control and IPS	✓			

* 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.

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 and 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.

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----------				

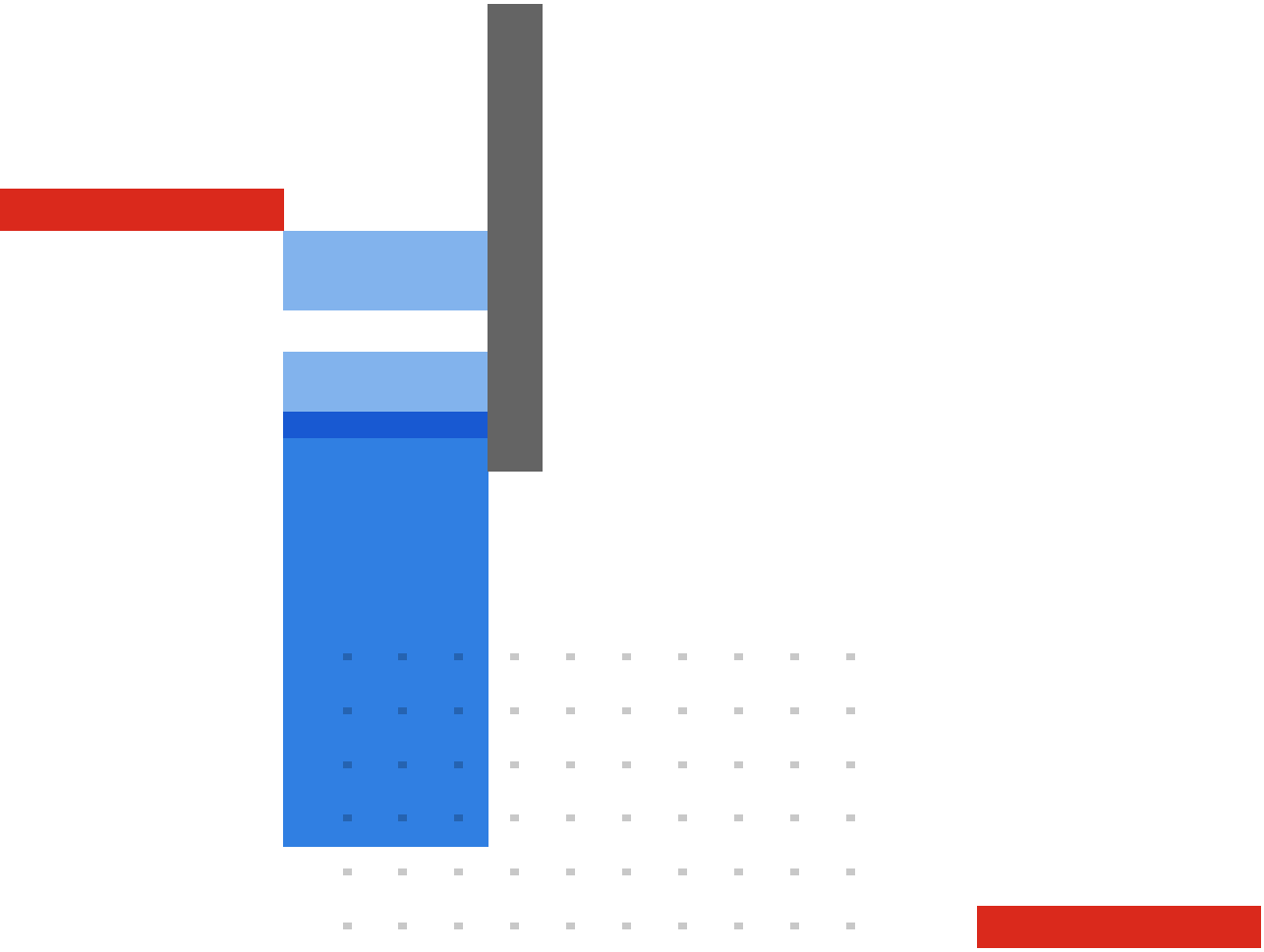
1. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available 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-DAT-R63-20261001