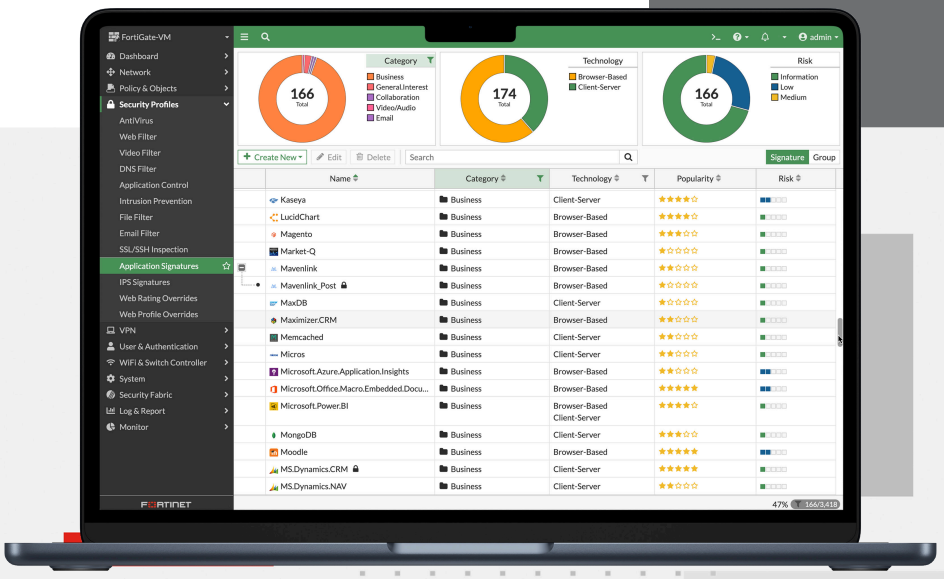
FortiGate® VM on Microsoft Azure



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 Microsoft Azure 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.

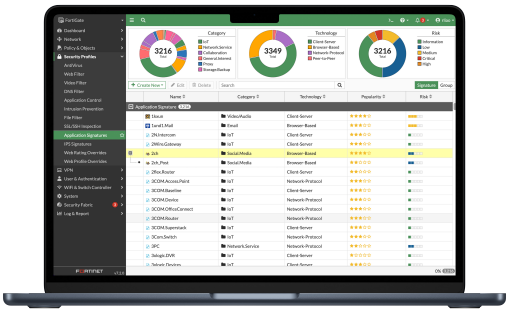
FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed 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

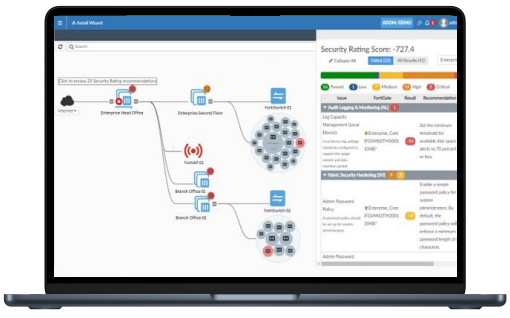
Advanced Virtual Security Processing Units (vSPUs)

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.
- 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.



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

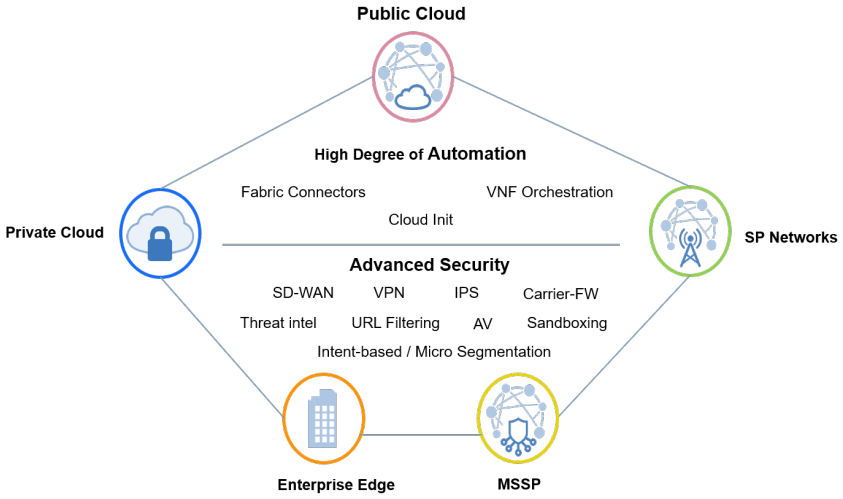
Next Generation Firewall (NGFW)

- 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

- VGW to FortiGate VPN between VPCs
- Hybrid cloud site to site IPsec VPN
- Remote access VPN

Gain Comprehensive Visibility and Apply Consistent Control



Azure Integration

FortiOS embeds the latest autoscaling functionality, providing automation based on resource demand from your cloud workloads.

Designed to ensure easy, consistent deployment for the most efficient systems and applications uptime with minimal disruption using Azure load balancing and two FortiGate-VMs.

FortiOS works with Azure Traffic Manager to provide local access for customers for low latency while providing redundancy.

Licensing

With a multitude of deployment methods supported across various private and public cloud deployments, FortiGate-VM for Microsoft Azure 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 is the price for the Microsoft Azure instances.

You can deploy FortiGate-VM in regional Azure such as Azure Government, Germany, and China.

FortiGate-VM also supports Azure Stack (BYOL only).

Specifications

The FortiGate-VM supports multiple instance families that leverage Intel and AMD based x64 processors as well as the ARM64 instance families that leverages the Ampere® Altra® Arm-based processor.

For a full list of supported instance families See Azure Administration Guide: Instance type Support.

The following shows performance of x64 (Standard DSv2 and Dsv3) Instance families with BYOL License.

Specifications

	VM-01/01V/01S	VM-02/02V/02S			VM-04/04V/04S			
System Requirement								
vCPU (Minimum/Maximum)	1/1	1/2			1/4			
Technical Specifications								
Network Interface Support (Minimum/Maximum)[1]	1/24	1/24			1/24			
VDOMs (Default/Maximum)[2]	10/10	10/25			10/50			
Firewall Policies	10 000	10 000			10 000			
System Performance		Accelerated Networking ON						
Instance Shape to be Measured		Standard_D2s_v5 (2vCPU)			Standard_D4s_v5 (4vCPU)			
Azure Expected Bandwidth[3]		12 500 Mbps			12 500 Mbps			
		Standard		DPDK		Standard		DPDK
		standalone	IPSEC	standalone	IPSEC	standalone	IPSEC	standalone	IPSEC
Firewall Throughput (UDP Packets) in Mbps - 1280 bytes		8400	1150	9500	1550	12 500	1780	10 900	2500
Firewall Throughput (UDP Packets) in Mbps - 512 bytes		3600	720	6200	840	6800	1150	7500	1100
Firewall Throughput (UDP Packets) in Mbps - 64 bytes		580	170	1000	170	1100	200	1150	240
New Sessions/Second (TCP)		9200	-	8800	-	16 000	-	16 700	-
HTTP Throughput w/ Application profile (64K size) in Mbps		4800	-	12 700	-	9440	-	12 700	-
HTTP Throughput w/ IPS profile (44K size) in Mbps		6100	-	12 690	-	11 850	-	12 700	-
HTTP Throughput w/ IPS profile (1M size) in Mbps		6300	-	12 690	-	12 000	-	12 700	-
NGFW Throughput (Mbps)		780	-	900	-	1580	-	1900	-
Threat Protection Throughput (Mbps)		770	-	890	-	1540	-	1850	-
SSL Inspection throughput (Mbps)		1500	-	3800	-	2920	-	7760	-

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

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

PAYG supports only up to 32 vCPU instances.

Actual performance may vary depending on the network and system configuration. Note that these metrics are updated periodically as the product performance keeps improving through internal testing. Different versions of the document may note the discrepancy in the performance numbers so ensure that you refer to the latest datasheets.

Accelerated networking is required and turned on by default on all Dv5 and Dsv5 virtual machines. For more info see Dv5 and Dsv5-series Specifications here.

Performance metrics were observed using FortiGate-VM BYOL instances using FOS v7.4.0.

1. Applicable to 6.4.0+. The actual working number of consumable network interfaces varies depending on Microsoft Azure instance types/sizes and may be less. Current test version is FortiOS 7.4.0.
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 addition perpetual licenses. See ORDER INFORMATION for VDOM SKUs.
3. The latest information about Microsoft Azure bandwidth is found on https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general.
4. IPS performance is measured using HTTP Throughput with IPS Profile enabled at 44k and 1M packet sizes.
5. Using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).
6. Application Control performance is measured with 64 Kbyte HTTP traffic.
7. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
8. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.

Specifications

	VM-08/08V/08S				VM-16/16V/16S				VM-32/32V/32S				VM-UL/ ULV/ULS
System Requirement													
vCPU (Minimum/ Maximum)	1/8				1/16				1/32				1/ Unlimited
Technical Specifications													
Network Interface Support (Minimum/ Maximum) [1]	1/24				1/24				1/24				1/24
VDOMs (Default/ Maximum) [2]	10/500				10/500				10/500				10/500
Firewall Policies	200 000				200 000				200 000				200 000
System Performance	**Accelerated Networking ON**												
Instance Shape to be Measured	**Standard_D8s_v5 (8vCPU)**				**Standard_D16s_v5 (16vCPU)**				**Standard_D32s_v5 (32vCPU)**				
Azure Expected Bandwidth [3]	**12 500 Mbps**				**12 500 Mbps**				**16 000 Mbps**				
	Standard		**DPDK**		**Standard**		**DPDK**		**Standard**		**DPDK**		
	standalone	**IPSEC**	**standalone**	**IPSEC**	**standalone**	**IPSEC**	**standalone**	**IPSEC**	**standalone**	**IPSEC**	**standalone**	**IPSEC**	
Firewall Throughput (UDP Packets) in Mbps - 1280 bytes	12 500	3400	12 000	4400	14 000	5100	13 800	6300	17 500	6750	17 500	6800	
Firewall Throughput (UDP Packets) in Mbps - 512 bytes	11 900	2000	11 900	2200	14 000	3000	13 800	3300	17 500	3300	16 000	3550	
Firewall Throughput (UDP Packets) in Mbps - 64 bytes	1950	500	2200	500	3000	600	3000	650	3400	620	3400	720	
New Sessions / Second (TCP)	17 200	-	17 500	-	17 000	-	17 000	-	19 000	-	19 000	-	
HTTP Throughput w/ Application profile (64K size) in Mbps	12 700	-	12 700	-	12 700	-	12 700	-	16 290	-	16 290	-	
HTTP Throughput w/ IPS profile (44K size) in Mbps	12 700	-	12 700	-	12 700	-	12 700	-	16 290	-	16 290	-	
HTTP Throughput w/ IPS profile (1M size) in Mbps	12 700	-	12 700	-	12 700	-	12 700	-	16 300	-	16 300	-	
NGFW Throughput (Mbps)	2960	-	3500	-	5500	-	6800	-	7700	-	11 200	-	
Threat Protection Throughput (Mbps)	2950	-	3400	-	5400	-	6700	-	7400	-	11 000	-	
SSL Inspection throughput (Mbps)	5510	-	12 000	-	10 700	-	12 730	-	15 000	-	16 370	-	

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

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

PAYG supports only up to 32 vCPU instances.

Actual performance may vary depending on the network and system configuration. Note that these metrics are updated periodically as the product performance keeps improving through internal testing. Different versions of the document may note the discrepancy in the performance numbers so ensure that you refer to the latest datasheets.

Accelerated networking is required and turned on by default on all Dv5 and Dsv5 virtual machines. For more info see Dv5 and Dsv5-series Specifications here.

Performance metrics were observed using FortiGate-VM BYOL instances using FOS v7.4.0.

1. Applicable to 6.4.0+. The actual working number of consumable network interfaces varies depending on Microsoft Azure instance types/sizes and may be less. Current test version is FortiOS 7.4.0.
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 addition perpetual licenses. See ORDER INFORMATION for VDOM SKUs.
3. The latest information about Microsoft Azure bandwidth is found on https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general.
4. IPS performance is measured using HTTP Throughput with IPS Profile enabled at 44k and 1M packet sizes.
5. Using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).
6. Application Control performance is measured with 64 Kbyte HTTP traffic.
7. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
8. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.

Ordering Information

The following are SKUs that can be acquired for the BYOL scheme. For the PAYG/On-Demand subscription, various instance/VM types are available on the Marketplace. BYOL is perpetual licensing, as opposed to PAYG/On-Demand, which is an hourly subscription available with marketplace-listed products.

Product	SKU	Description
FortiGate-VM01	FG-VM01, FG-VM01V	FortiGate-VM 'virtual appliance'. 1x vCPU core. No VDOM by default for FG-VM01V model.
FortiGate-VM02	FG-VM02, FG-VM02V	FortiGate-VM 'virtual appliance'. 2x vCPU cores. No VDOM by default for FG-VM02V model.
FortiGate-VM04	FG-VM04, FG-VM04V	FortiGate-VM 'virtual appliance'. 4x vCPU cores. No VDOM by default for FG-VM04V model.
FortiGate-VM08	FG-VM08, FG-VM08V	FortiGate-VM 'virtual appliance'. 8x vCPU cores. No VDOM by default for FG-VM08V model.
FortiGate-VM16	FG-VM16, FG-VM16V	FortiGate-VM 'virtual appliance'. 16x vCPU cores. No VDOM by default for FG-VM016V model.
FortiGate-VM32	FG-VM32, FG-VM32V	FortiGate-VM 'virtual appliance'. 32x vCPU cores. No VDOM by default for FG-VM032V model.
FortiGate-VMUL	FG-VMUL, FG-VMULV	FortiGate-VM 'virtual appliance'. Unlimited vCPU cores. No VDOM by default for FG-VMULV model.
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.

The number of configurable VDOMs can be stacked up to the maximum number of supported VDOMs per vCPU model. Refer to Virtual Domains (Maximum) under SPECIFICATIONS.

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.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles: Enterprise Protection	Bundles: Unified Threat Protection	Bundles: Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials [2]	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Internet Service (SaaS) DB Updates	included with FortiCare Subscription			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Full features available when running FortiOS 7.4.1
2. Desktop Models only

FortiGuard Bundles

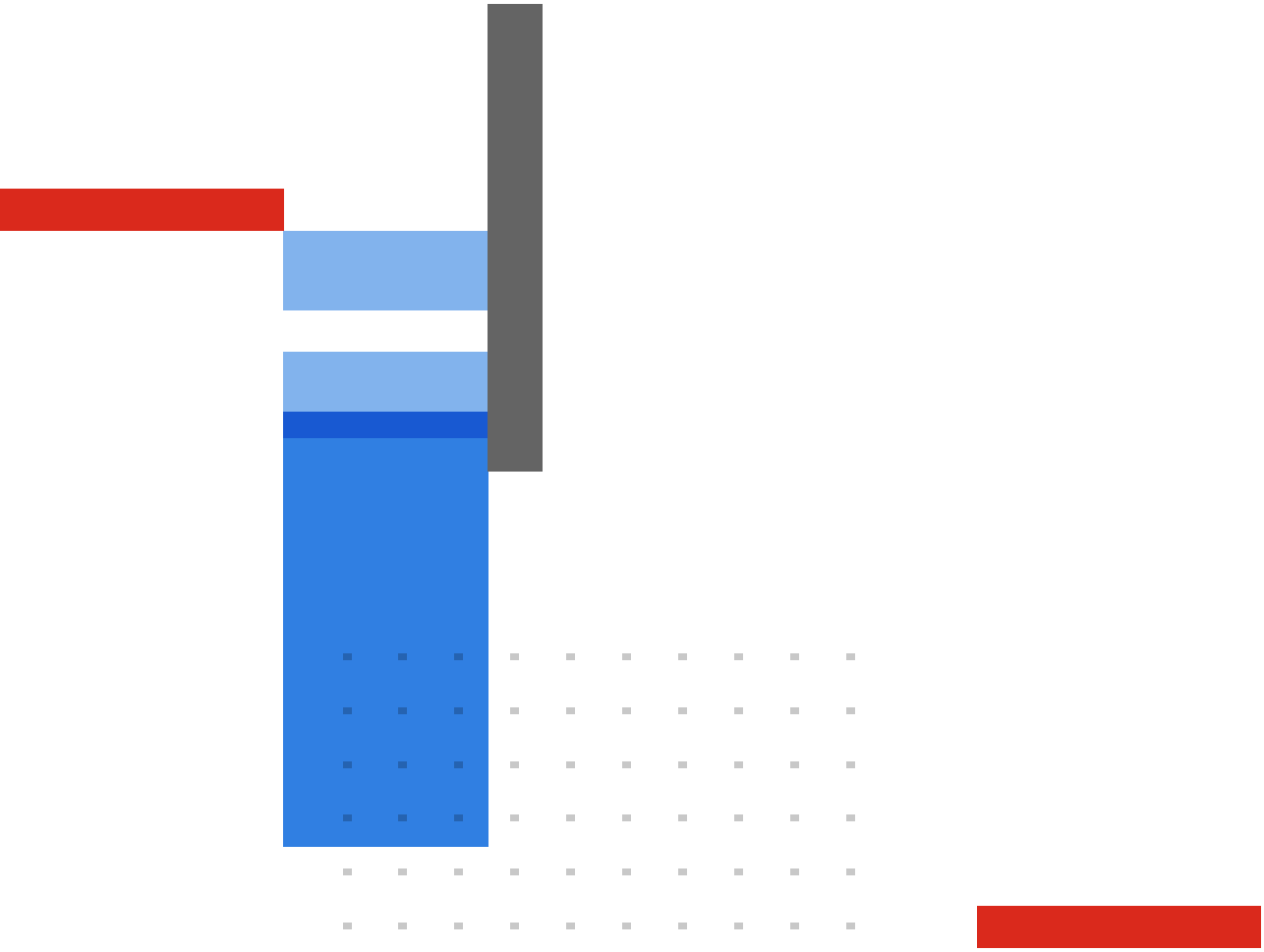
FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive lifecycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service variants, offers heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an Extended End-of-Engineering-Support of 18 months, providing flexibility. Access the intuitive FortiCare Elite Portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

Fortinet CSR 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

January 5, 2024

FG-VM-AZU-DAT-R35-20240105