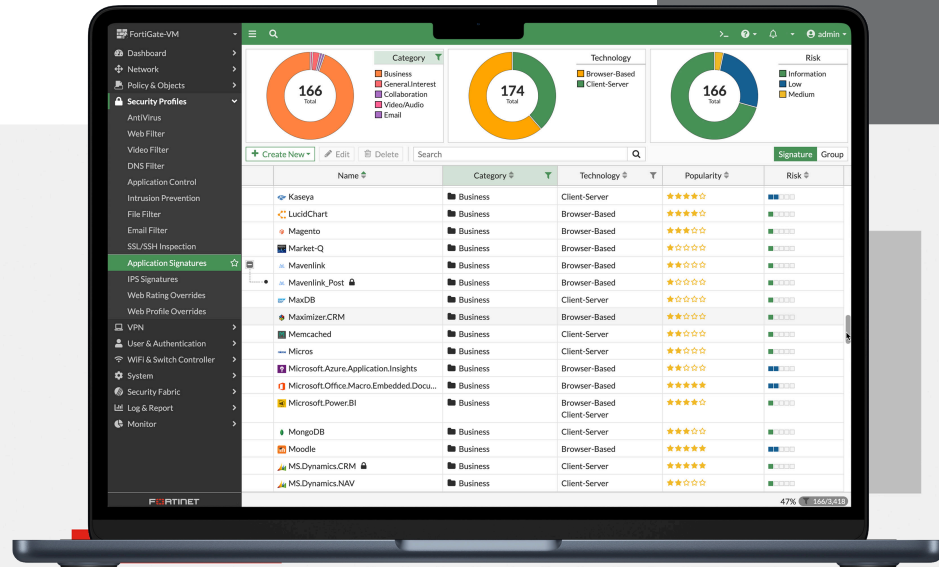


# FortiGate® VM on Microsoft Azure



## 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

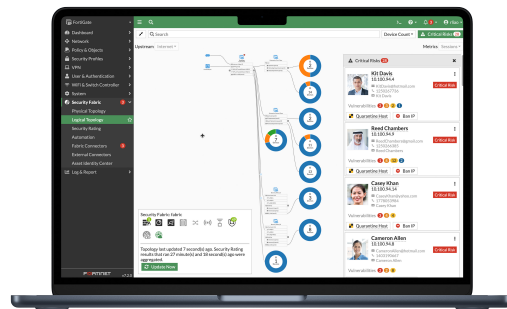
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

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.

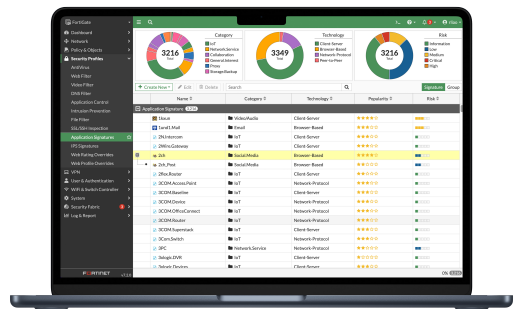
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

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



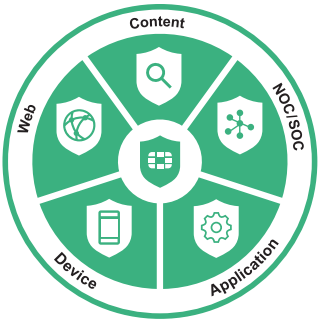
*Intuitive easy to use view into the network and endpoint vulnerabilities*



*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

### FortiGuard AI-Powered Security

FortiGuard's rich suite of security services counter threats in real time using AI-powered, coordinated protection designed by FortiGuard Labs security threat researchers, engineers, and forensic specialists.

### Web Security

Advanced cloud-delivered URL, DNS (Domain Name System), and Video Filtering providing complete protection for phishing and other web born attacks while meeting compliance.

Additionally, its dynamic inline CASB (Cloud Access Security Broker) service is focused on securing business SaaS data, while inline ZTNA traffic inspection and ZTNA posture check provide per-sessions access control to applications. It also integrates with the FortiClient Fabric Agent to extend protection to remote and mobile users.

### Content Security

Advanced content security technologies enable the detection and prevention of known and unknown threats and file-based attack tactics in real-time. With capabilities like CPRL (Compact Pattern Recognition Language), AV, inline Sandbox, and lateral movement protection make it a complete solution to address ransomware, malware, and credential-based attacks.

### Device Security

Advanced security technologies are optimized to monitor and protect IT, IIoT, and OT (Operational Technology) devices against vulnerability and device-based attack tactics. Its validated near-real-time IPS intelligence detects, and blocks known and zero-day threats, provides deep visibility and control into ICS/OT/SCADA protocols, and provides automated discovery, segmentation, and pattern identification-based policies.

### Advanced NOC and SOC Management

Advanced NOC and SOC management tools attached to your NGFW provide simplified and faster time-to-activation.

### SOC-as-a-Service

Includes tier-one hunting and automation, log location, 24×7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

### Fabric Rating Security Best Practices

Includes supply chain virtual patching, up-to-date risk and vulnerability data to deliver quicker business decisions, and remediation for data breach situations.

## 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.”

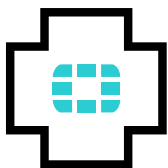
FortiGate-VM removes the cost-performance barriers to adopting virtual NGFWs, with several industry-leading features:

- 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.

---

### FortiCare Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.



## Deployment



### Next Generation Firewall (NGFW)

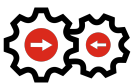
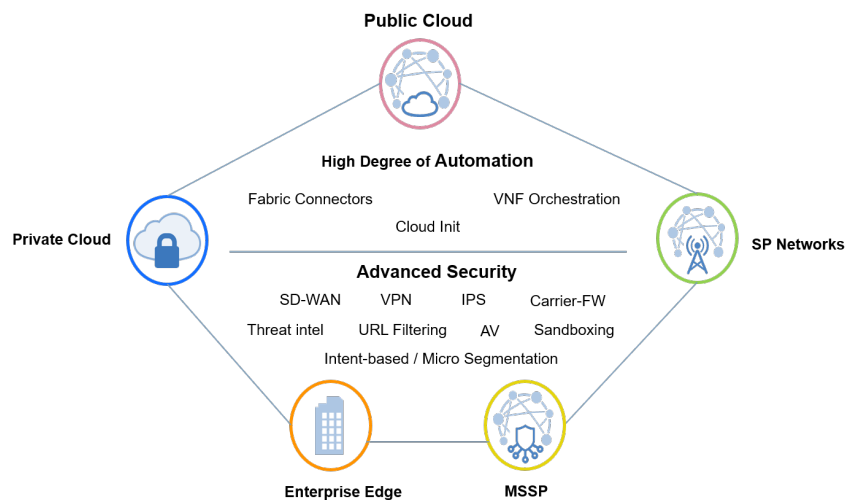
- Reduce complexity by combining threat protection security capabilities into single high-performance network security appliances
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in your network traffic
- Deliver the industry's 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) <sup>1</sup>	1/24	1/24				1/24			
VDOMs (Default/Maximum) <sup>2</sup>	10/10	10/25				10/50			
Firewall Policies	10 000	10 000				10 000			
System Performance		Accelerated Networking OFF		Accelerated Networking ON		Accelerated Networking OFF		Accelerated Networking ON	
Instance Shape to be Measured		DS2_v2 (2vCPU)				D4s_v3 (4vCPU)			
Azure Expected Bandwidth <sup>3</sup>		1500 Mbps				2000 Mbps			
		standalone	IPSEC	standalone	IPSEC	standalone	IPSEC	standalone	IPSEC
Firewall Throughput (UDP Packets) in Mbps - 1280 bytes		1200	1300	1600	1600	1350	1250	2150	1800
Firewall Throughput (UDP Packets) in Mbps - 512 bytes		500	550	1600	1250	560	500	2140	1200
Firewall Throughput (UDP Packets) in Mbps - 64 bytes		80	80	750	250	80	80	1000	230
New Sessions/Second (TCP)		6000	-	4500	-	6000	-	4600	-
HTTP Throughput w/ Application profile (64K size) in Mbps		690	-	1530	-	1310	-	2000	-
HTTP Throughput w/ IPS profile (44K size) in Mbps		720	-	1510	-	1300	-	2000	-
HTTP Throughput w/ IPS profile (1M size) in Mbps		700	-	1540	-	1310	-	2000	-
NGFW Throughput (Mbps)		560	-	600	-	710	-	810	-
Threat Protection Throughput (Mbps)		560	-	590	-	700	-	800	-
SSL Inspection throughput (Mbps)		560	-	1080	-	850	-	1670	-



For the sizing guide, please refer to the sizing document available on [www.fortinet.com](http://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.

Performance metrics were observed using FortiGate-VM BYOL instances using FOS v7.0.1.

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 7.2.3.
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) <sup>1</sup>		1/24			1/24			1/24			1/24		
VDOMs (Default/Maximum) <sup>2</sup>		10/500			10/500			10/500			10/500		
Firewall Policies		200 000			200 000			200 000			200 000		
System Performance		Accelerated Networking OFF		Accelerated Networking ON		Accelerated Networking OFF		Accelerated Networking ON		Accelerated Networking OFF		Accelerated Networking ON	
Instance Shape to be Measured		D8s_v3 (8vCPU)				D16s_v3 (16vCPU)				D32s_v3 (32vCPU)			
Azure Expected Bandwidth <sup>3</sup>		4000 Mbps				8000 Mbps				16 000 Mbps			
	standalone	IPSEC	standalone	IPSEC	standalone	IPSEC	standalone	IPSEC	standalone	IPSEC	standalone	IPSEC	
Firewall Throughput (UDP Packets) in Mbps - 1280 bytes		1550	1450	4100	4000	1840	1780	8000	7200	1900	1780	16 500	7600
Firewall Throughput (UDP Packets) in Mbps - 512 bytes		720	600	4000	2500	800	720	8000	3600	820	720	14 500	3800
Firewall Throughput (UDP Packets) in Mbps - 64 bytes		100	90	1800	500	120	120	3750	700	125	120	1950	750
New Sessions / Second (TCP)		7800	-	6600	-	12 500	-	19 000	-	15 500	-	19 000	-
HTTP Throughput w/ Application profile (64K size) in Mbps		1320	-	4080	-	1470	-	8160	-	1750	-	16 290	-
HTTP Throughput w/ IPS profile (44K size) in Mbps		1300	-	4070	-	1410	-	8180	-	1700	-	16 290	-
HTTP Throughput w/ IPS profile (1M size) in Mbps		1360	-	4090	-	1500	-	8170	-	1780	-	16 280	-
NGFW Throughput (Mbps)		1020	-	1560	-	1100	-	2950	-	1240	-	5000	-
Threat Protection Throughput (Mbps)		1000	-	1550	-	1100	-	2900	-	1240	-	4900	-
SSL Inspection throughput (Mbps)		890	-	2310	-	1050	-	6000	-	1230	-	8100	-



For the sizing guide, please refer to the sizing document available on [www.fortinet.com](http://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.

Performance metrics were observed using FortiGate-VM BYOL instances using FOS v7.0.1.

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 7.2.3.
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
<b>FortiGate-VM01</b>	FG-VM01, FG-VM01V	FortiGate-VM 'virtual appliance'. 1x vCPU core. No VDOM by default for FG-VM01V model.
<b>FortiGate-VM02</b>	FG-VM02, FG-VM02V	FortiGate-VM 'virtual appliance'. 2x vCPU cores. No VDOM by default for FG-VM02V model.
<b>FortiGate-VM04</b>	FG-VM04, FG-VM04V	FortiGate-VM 'virtual appliance'. 4x vCPU cores. No VDOM by default for FG-VM04V model.
<b>FortiGate-VM08</b>	FG-VM08, FG-VM08V	FortiGate-VM 'virtual appliance'. 8x vCPU cores. No VDOM by default for FG-VM08V model.
<b>FortiGate-VM16</b>	FG-VM16, FG-VM16V	FortiGate-VM 'virtual appliance'. 16x vCPU cores. No VDOM by default for FG-VM016V model.
<b>FortiGate-VM32</b>	FG-VM32, FG-VM32V	FortiGate-VM 'virtual appliance'. 32x vCPU cores. No VDOM by default for FG-VM032V model.
<b>FortiGate-VMUL</b>	FG-VMUL, FG-VMULV	FortiGate-VM 'virtual appliance'. Unlimited vCPU cores. No VDOM by default for FG-VMULV model.
Optional Accessories/Spares	SKU	Description
<b>Virtual Domain License Add 5</b>	FG-VDOM-5-UG	Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
<b>Virtual Domain License Add 15</b>	FG-VDOM-15-UG	Upgrade license for adding 15 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
<b>Virtual Domain License Add 25</b>	FG-VDOM-25-UG	Upgrade license for adding 25 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
<b>Virtual Domain License Add 50</b>	FG-VDOM-50-UG	Upgrade license for adding 50 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
<b>Virtual Domain License Add 240</b>	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
<b>FortiGate-VM01-S</b>	FC1-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (1 vCPU core)
<b>FortiGate-VM02-S</b>	FC2-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (2 vCPU cores)
<b>FortiGate-VM04-S</b>	FC3-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (4 vCPU cores)
<b>FortiGate-VM08-S</b>	FC4-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (8 vCPU cores)
<b>FortiGate-VM16-S</b>	FC5-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (16 vCPU cores)
<b>FortiGate-VM32-S</b>	FC6-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (32 vCPU cores)
<b>FortiGate-VMUL-S</b>	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	Unified Threat Protection	Advanced Threat Protection
Security Services	FortiGuard IPS Service	•	•	•	•
	FortiGuard Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	FortiGuard Web Security — URL and web content, Video and Secure DNS Filtering	•	•	•	
	FortiGuard Anti-Spam		•	•	
	FortiGuard IoT Detection Service	•	•		
	FortiGuard Industrial Security Service	•	•		
	FortiCloud AI-based Inline Sandbox Service <sup>1</sup>	•			
NOC Services	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiGuard Security Fabric Rating & Compliance Monitoring Service	•	•		
	FortiConverter Service	•	•		
	FortiGuard SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
SOC Services	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaas	•			
Hardware and Software Support	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	FortiGuard Application Control				
	FortiCloud ZTNA Inline CASB Service <sup>1</sup>				
	Internet Service (SaaS) DB Updates				
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Available when running FortiOS 7.2



### 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.

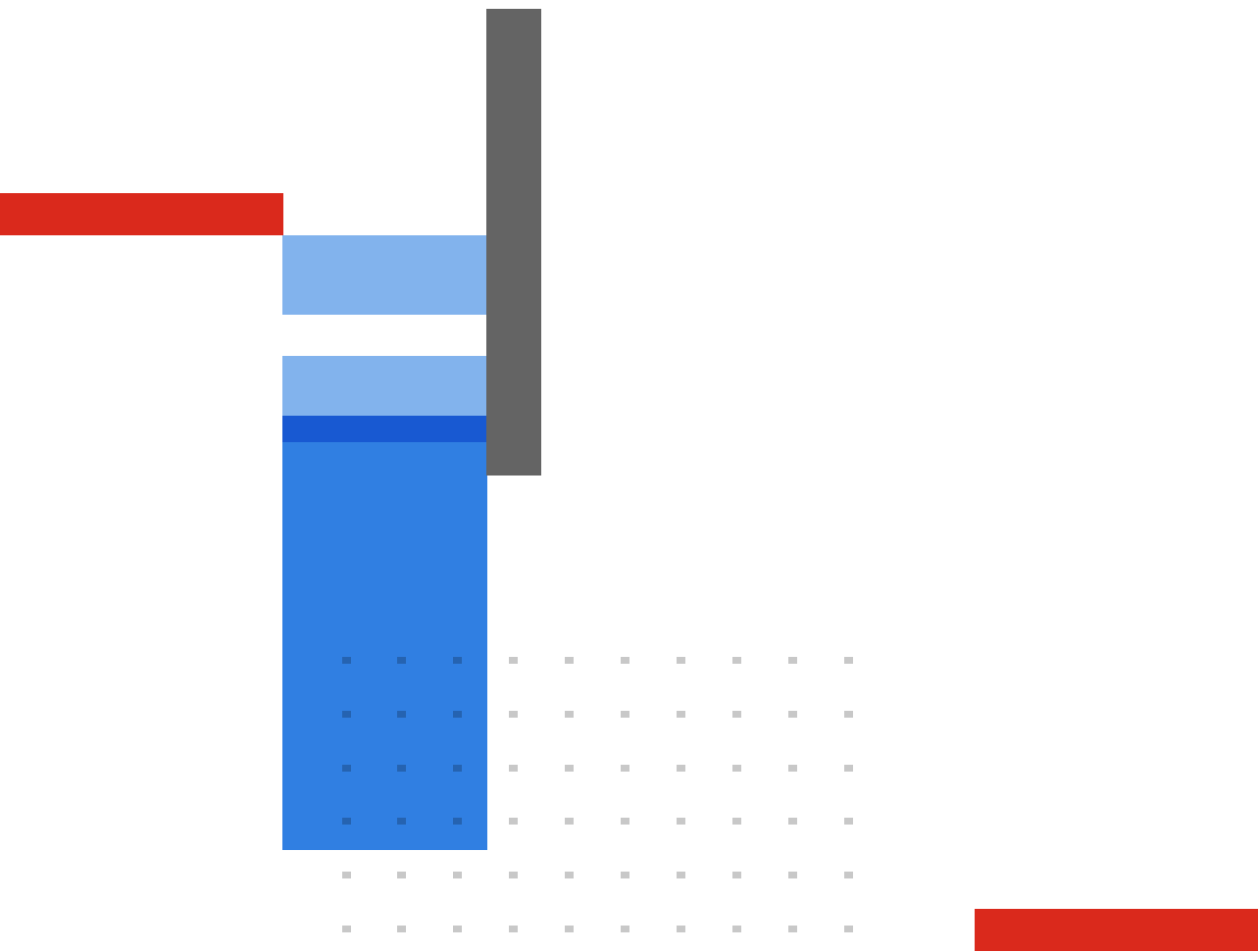
### FortiCare Elite

FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (EoE's) of 18 months for added flexibility and access to the new FortiCare Elite Portal. This intuitive portal provides a single unified view of device and security health.

### 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](#).





[www.fortinet.com](http://www.fortinet.com)

Copyright © 2023 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 General Counsel, 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.