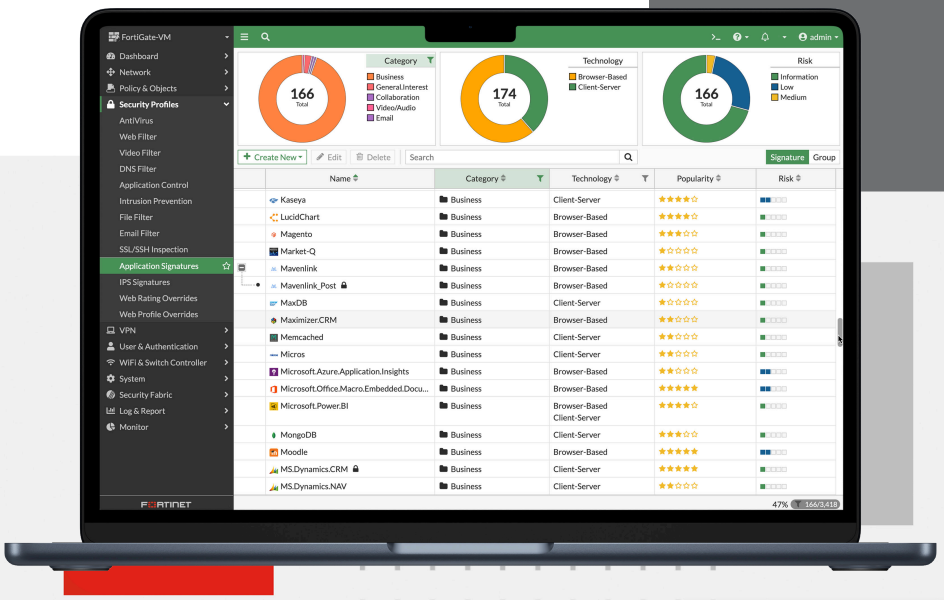
FortiGate®-VM with VMware NSX-T™



Highlights

- Advanced (L7) threat protection integrated with VMware NSX-T Data Center environments in SDDCs as well as private and public clouds
- Streamlined SecOps, with automation and orchestration via Fortinet Fabric Connectors
- Single-pane-of-glass management through VMware NSX Manager, with full visibility in FortiManager
- Wide array of licensing choices to fit any infrastructure requirement

Automated, Advanced Security for VMware NSX-T Data Center Environments

By extending the FortiGate-VM native integration with the VMware NSX-T Data Center, Fortinet delivers advanced security for east-west and north-south traffic. This deep integration provides customers with the confidence to extend their virtualized infrastructure across multi-hypervisor environments, private, and public clouds with a unified security layer.

Fortinet and VMware NSX-T deliver zero-trust security with advanced L7 protection and policy-based firewall controls. Automation is enabled through a built-in NSX-T fabric connector for dynamic updates between NSX Manager and FortiGate-VM.

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.

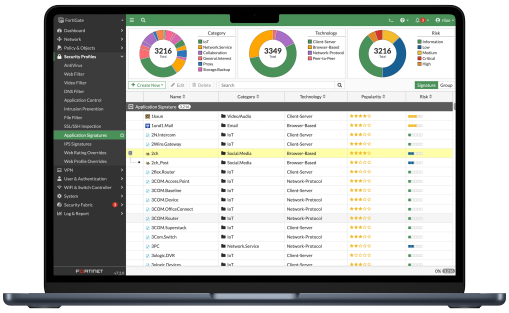
FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed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

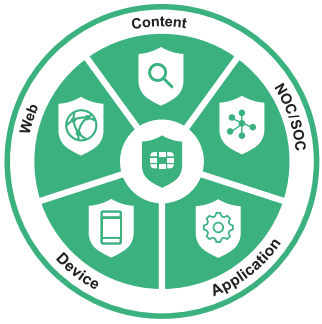
Intuitive easy to use view into the network and endpoint vulnerabilities



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

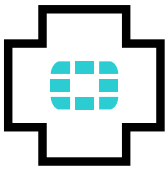
Advanced Virtual Security Processing Units (vSPUs)

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.
- 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.



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

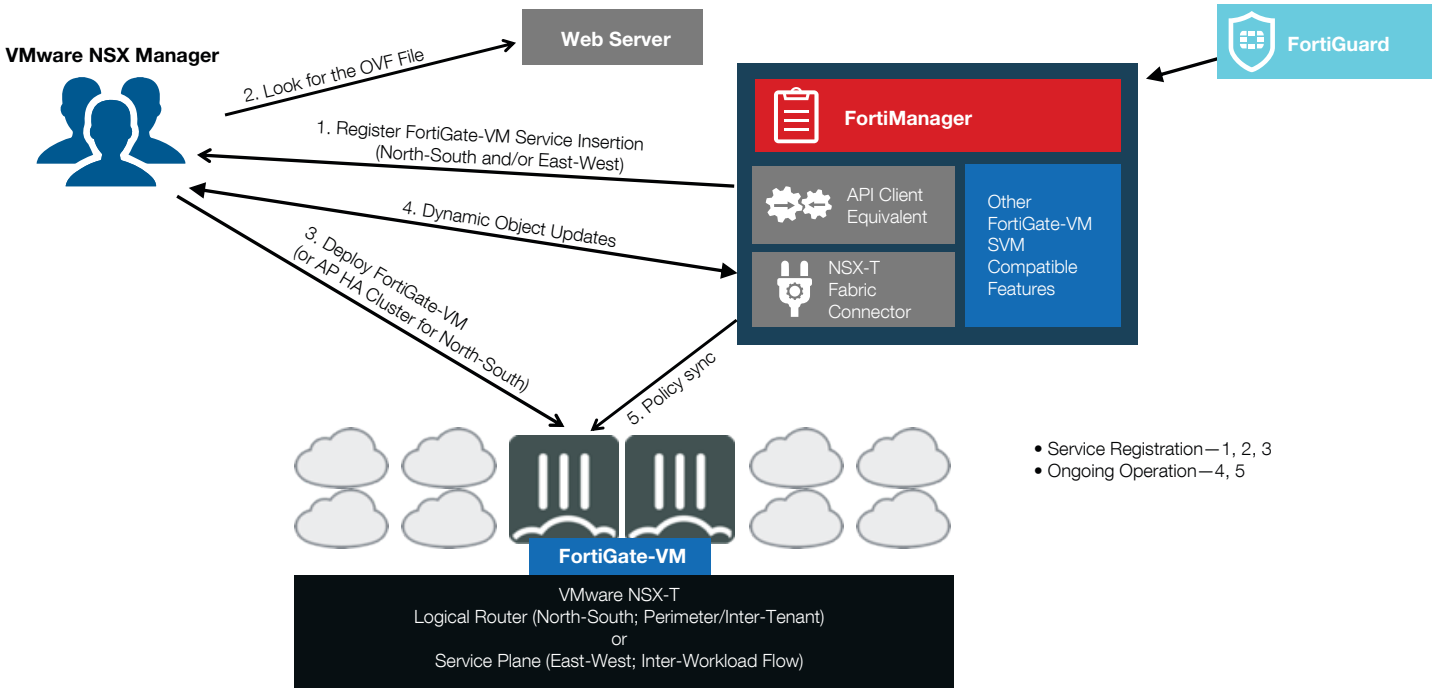


Figure 1: FortiGate-VM and FortiManager seamlessly integrate with VMware NSX Manager.

The FortiGate-VM provides interoperability with NSX-T Data Center through service insertion as a third-party edge firewall (Figure 1).

Core capabilities include:

- By means of Fabric Connectors activated from the FortiManager console, FortiGate-VM integrates with NSX-T Data Center to register both east-west and north-south service insertions.
- From that point on, security can be managed from the NSX-T dashboard and is automatically carried through to the FortiGate-VM instances running in the NSX-T Data Center.
- Fortinet Fabric Connector automatically updates security policies associated with dynamic objects in NSX-T whenever changes are made to underlying IP addresses, application metadata, and annotations. This capability, which also extends to public cloud infrastructures (such as AWS, Azure, and GCP), relieves organizations of the need to manually update security policies, freeing up their time for other business-critical duties.

Specifications

	FortiGate-VM01/01V	FortiGate-VM02/02V	FortiGate-VM04/04V
Technical Specifications			
vCPU Support (Minimum / Maximum)	1 / 1	1 / 2	1 / 4
Memory Support (Minimum)	2 GB	2 GB	2 GB
Storage Support (Minimum / Maximum)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	32 / 64	512 / 1024	512 / 1024
Virtual Domains (Default / Maximum) *	10 / 10	10 / 25	10 / 50
Firewall Policies	10 000	10 000	10 000
Maximum Number of Registered Endpoints	2000	2000	8000
Unlimited User License	Yes	Yes	Yes

	FortiGate-VM08/08V	FortiGate-VM16/16V	FortiGate-VM32/32V	FortiGate-VMUL/ULV
Technical Specifications				
vCPU Support (Minimum / Maximum)	1 / 8	1 / 16	1 / 32	1 / unlimited
Memory Support (Minimum)	2 GB	2 GB	2 GB	2 GB
Storage Support (Minimum / Maximum)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	1024 / 4096	1024 / 4096	1024 / 4096	1024 / 4096
Virtual Domains (Default / Maximum) *	10 / 500	10 / 500	10 / 500	10 / 500
Firewall Policies	200 000	200 000	200 000	200 000
Maximum Number of Registered Endpoints	20 000	20 000	20 000	20 000
Unlimited User License	Yes	Yes	Yes	Yes

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-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. Special licenses for offline network environments are available for VMxxV series (01V to ULV), and they have the same specifications as those of VMxxV shown in the table above. For ordering offline licenses, please consult Fortinet sales representatives.

System Requirements

NSX-T integration requires a deployment of FortiManager (as a physical appliance or VM instance) with a valid license/entitlement in addition to a FortiGate-VM. See the FortiManager datasheet for the spec for details: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf

FortiGate-VM 6.4.3 GA can be upgraded to 6.4.9+ GA. FortiGate-VM 7.0.6 GA can be upgraded to 7.2.0+ GA .

Software Compatibility Matrix

NSX-T	FortiGate-VM	FortiManager
4.0	7.0.6	7.0.5/7.2.1
3.1/3.2	7.0.6	7.0.5/7.2.1
3.0/3.1	6.4.3	6.4.4+

Certifications

Product	Version	Partner Product and Version	Certification Date	Listing URL
FortiGate-VM	7.0.6	NSX-T 3.1, 3.2, and 4.0	Aug-22	https://partnerweb.vmware.com/comp_guide2/detail.php?deviceCategory=nsxt&productid=56054
FortiGate-VM	6.4.3	NSX-T 2.5, 3.0, and 3.1	Nov-20	https://www.vmware.com/resources/compatibility/detail.php?productid=51464&deviceCategory=nsxt

Ordering Information

Product	SKU	Description
FortiGate-VM01	FG-VM01, FG-VM01V	FortiGate-VM 'virtual appliance'. 1x vCPU core and unlimited RAM. No VDOM by default for FG-VM01V model.
FortiGate-VM02	FG-VM02, FG-VM02V	FortiGate-VM 'virtual appliance'. 2x vCPU cores and unlimited RAM. No VDOM by default for FG-VM02V model.
FortiGate-VM04	FG-VM04, FG-VM04V	FortiGate-VM 'virtual appliance'. 4x vCPU cores and unlimited RAM. No VDOM by default for FG-VM04V model.
FortiGate-VM08	FG-VM08, FG-VM08V	FortiGate-VM 'virtual appliance'. 8x vCPU cores and unlimited RAM. No VDOM by default for FG-VM08V model.
FortiGate-VM16	FG-VM16, FG-VM16V	FortiGate-VM 'virtual appliance'. 16x vCPU cores and unlimited RAM. No VDOM by default for FG-VM016V model.
FortiGate-VM32	FG-VM32, FG-VM32V	FortiGate-VM 'virtual appliance'. 32x vCPU cores and unlimited RAM. No VDOM by default for FG-VM032V model.
FortiGate-VMUL	FG-VMUL, FG-VMULV	FortiGate-VM 'virtual appliance'. Unlimited vCPU cores and RAM. No VDOM by default for FG-VMULV model.
Optional Accessories		
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. Please 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
Optional Accessories		
VDOM Subscription License for FortiGate S Series	FC1-10-FGVVS-498-02-DD	Subscription license for adding VDOMs to FortiGate-VM S series running OS 6.4.8/7.0.2 or higher. This is a seat SKU where the total number of vdoms must be added as seats in an increment of 5 and the minimal order is 5 vdoms

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

FortiManager 6.2.3+ and 6.4.0+ support managing FortiGate-VM S-series devices. However, only specific FortiManager versions support NSX-T integration. Refer to System Requirements.

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 [1]	•			
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	included with FortiCare Subscription			
	FortiCloud ZTNA Inline CASB Service [1]				
	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

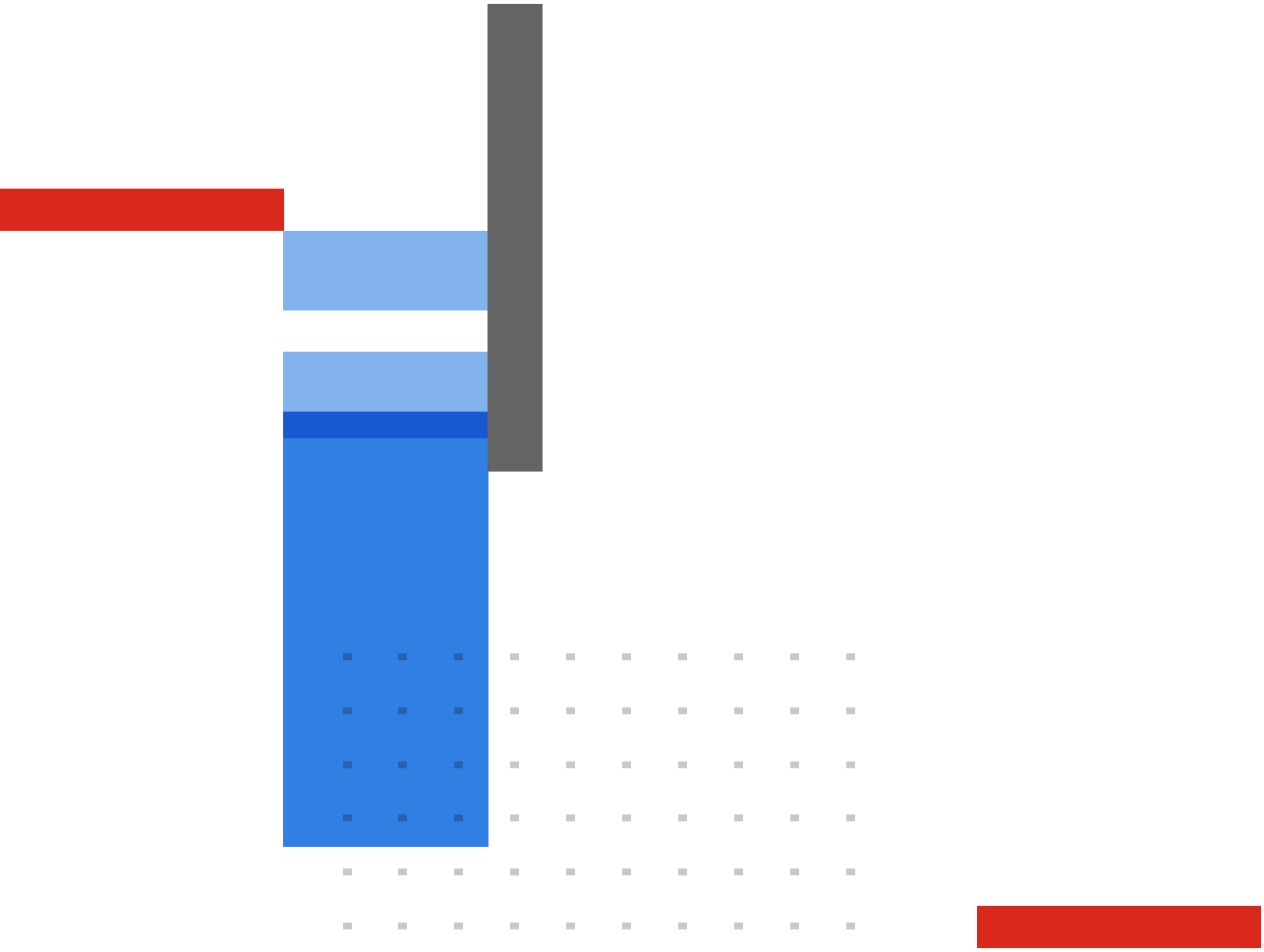
FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

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

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.

February 9, 2023

FG-VM-NSXT-DAT-R15-20230209