

DATA SHEET

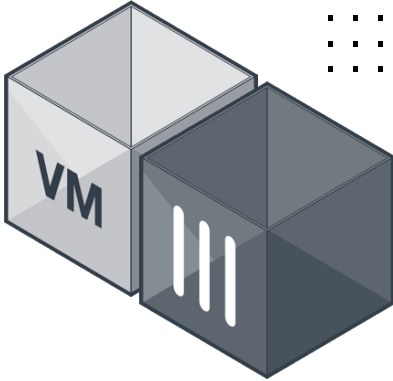
FortiGate® Virtual Appliances

Consolidated Security for Virtualized Environments

Complete end-to-end security ecosystem for the software-defined datacenter. Fortinet enables and facilitates the enterprise’s journey through the datacenter consolidation process.

Fortinet delivers both physical and virtualized security appliances to secure unique data planes. It offers on one side, unmatched performance and security capabilities, while allowing for the growth and evolution of the consolidating datacenter with no service degradation or bottlenecks, no compromise on security, and with an unmatched ROI — fulfilling the outcomes of a robust software-defined security framework.

FortiGate virtual appliances allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. With the addition of virtual appliances from Fortinet, you can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform.



Fortinet’s comprehensive security virtual appliance lineup supports in excess of 16 solutions.

Benefits

- 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
- Rapid deployment capability
- Ability to manage virtual and physical appliances from a single pane of glass management platform
- Simple licensing with no per-user fees
- Support for multiple virtualization and cloud platforms
- Full support for FortiHypervisor deployments enabling line-speed security in vCPE requirement
- Wide array of licensing choices to fit any infrastructure requirement
- VDOM-enabled models for multi-tenant environments

PLATFORMS

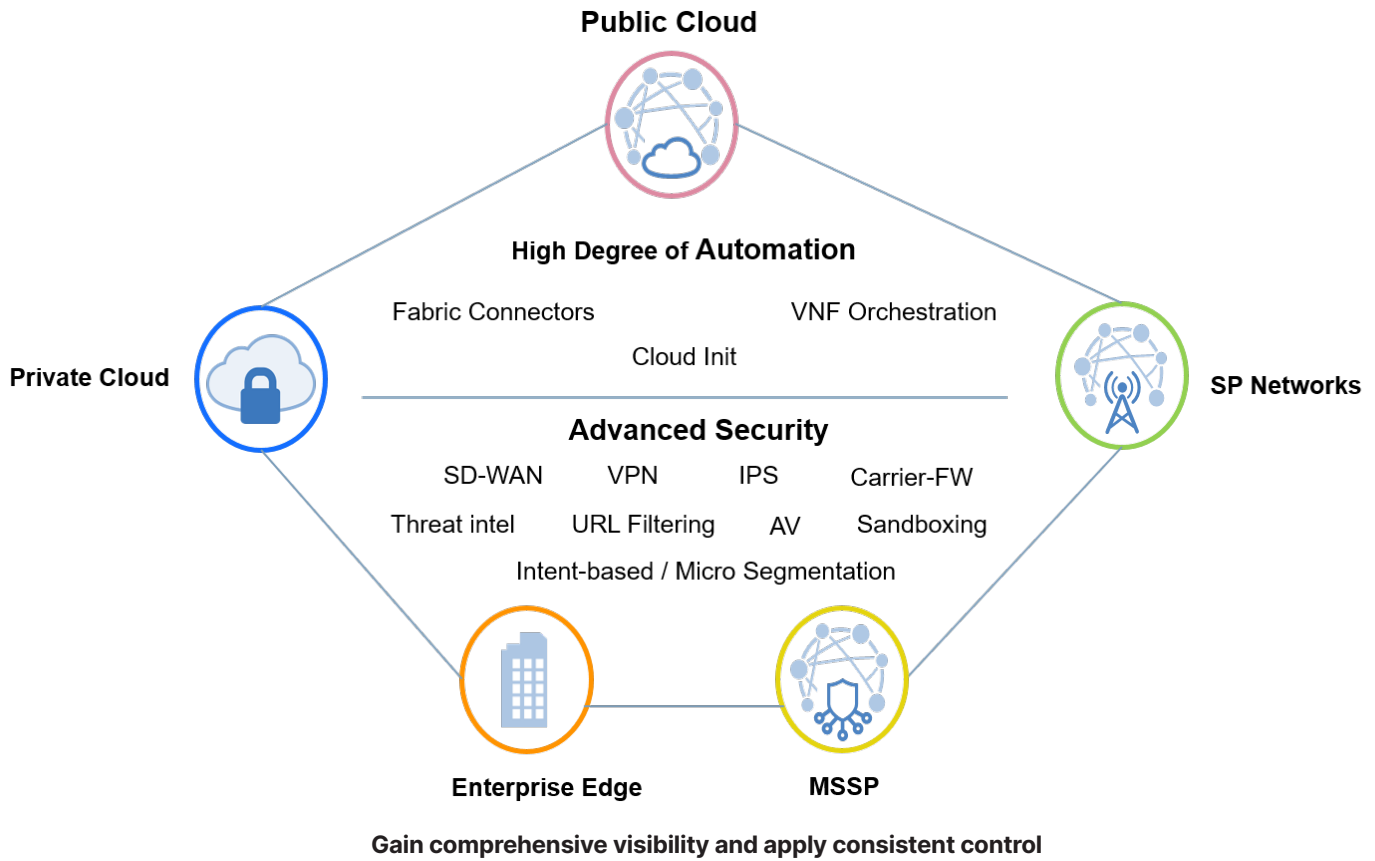
Choice of Form Factor

Few organizations use 100% hardware or 100% virtual IT infrastructure today, creating a need for both hardware and virtual appliances in your security strategy. Fortinet allows you to build the security solution that is right for your environment with hardware and virtual appliances to secure the core and the edge and increase visibility and control over communications within the virtualized infrastructure. FortiManager virtual or physical appliances allow you to easily manage and update your Fortinet security assets — hardware, virtual, or both — from a single pane of glass.

Multi-Threat Security

Using the advanced FortiOS™ operating system, FortiGate appliances effectively neutralize a wide range of security threats facing your virtualized environment. Whether deployed at the edge as a front-line defense, or deep within the virtual infrastructure for inter-zone security, FortiGate appliances protect your infrastructure with some of the most effective security available today by enabling security features you need.

DEPLOYMENT



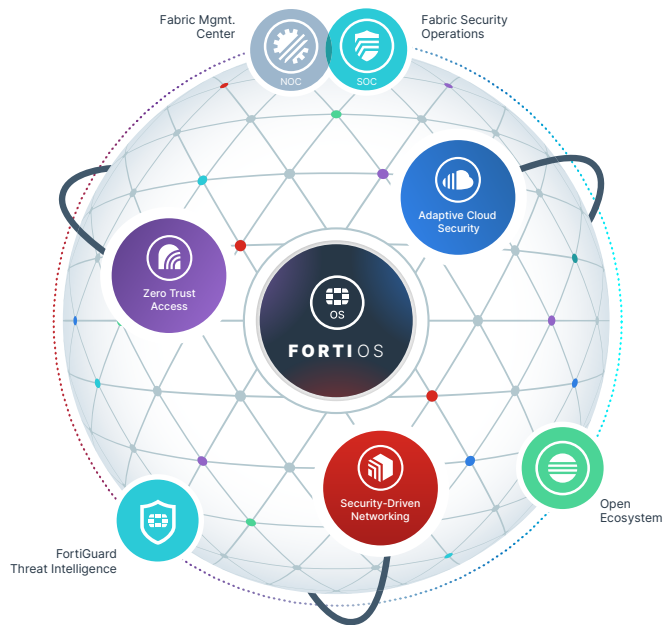
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad:** Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated:** Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated:** Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models consisting on appliances, software and As-a-Service with SASE, ZTNA and other emerging cybersecurity solutions.

SERVICES

FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1,000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.



SPECIFICATIONS

	VM-01/01V/01S	VM-02/02V/02S	VM-04/04V/04S	VM-08/08V/08S	VM-16/16V/16S	VM-32/32V/32S	VM-UL/ULV/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
Wireless Access Points Controlled (Tunnel / Global)	32 / 64	512 / 1,024	512 / 1,024	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096
Virtual Domains (Default / Maximum) *	10 / 10	10 / 25	10 / 50	10 / 500	10 / 500	10 / 500	10 / 500
Firewall Policies	10,000	10,000	10,000	200,000	200,000	200,000	200,000
Maximum Number of Registered Endpoints	2,000	2,000	8,000	20,000	20,000	20,000	20,000
Unlimited User License	Yes	Yes	Yes	Yes	Yes	Yes	Yes

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-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.

VENDOR
Private Clouds (Hypervisors)
VMware ESXi v5.5 / v6.0 / v6.5 / v6.7 / v7.0
VMware NSX-T* v2.3 / v2.4 / v2.5
Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019**
Microsoft AzureStack
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 (AOS 5.10, Prism Central 5.10)***
Cisco Cloud Services Platform 2100****
Cisco ENCS (NFVIS 3.12.3)****
* 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 6.0.3+ supports Nutanix AHV and Cisco CSP 2100. **** FortiGate-VM 6.2.3+ supports Cisco NFVIS 3.12.3.

VENDOR
Public Clouds (Marketplaces)
Amazon AWS (including GovCloud and AWS China)
VMware Cloud on AWS*
VMware Cloud on Dell EMC**
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. FG-VMxxV series require FortiOS 5.4.8+ / 5.6.1+ / 6.0.0+. * FortiGate-VM 6.0.4+ supports VMware Cloud on AWS. ** FortiGate-VM 6.2.3+ supports VMware Cloud on Dell EMC. *** IBM Cloud does not support the marketplace and requires manual deployment. FortiGate-VM 6.4.2+ supports IBM Cloud.

ORDERING INFORMATION

The following SKUs adopt the perpetual licensing scheme: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.

FortiGate-VM 6.2.2 no longer has RAM restriction on all vCPU models while prior versions still restrict RAM sizes per model. Upgrade to 6.2.2 is necessary to remove the restriction.



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)
Support Bundle		
258	FortiCare services (only) included	
815	Enterprise Bundle included	
820	360 Protection Bundle included	
990	UTP Bundle included	

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.

BUNDLES



FortiGuard Bundle

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.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	ASE ¹	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video ² Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard IoT Detection Service	•	•		
FortiGuard Industrial Service	•	•		
FortiConverter Service	•	•		
SD-WAN Orchestrator Entitlement	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
Fortinet SOCaas	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 7.0



Copyright © 2021 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.