



ORDERING GUIDE

MSSP

Fortinet fuels the hyperscale growth of our MSSP partners, enabling rapid monetization of network and security. To enable this transformation, products and services are designed around how and where security is implemented within each customer deployment, including:

- **MSSP DC:** accelerated FortiGate hardware or VMs power MSSP data center offerings to provide “clean pipe” services
- **CPE:** scalable portfolio of on-premise equipment, delivering ASIC-powered NGFW, SSL inspection, 5G/LTE backup, and more
- **Endpoint:** managed connectivity combined with SASE or endpoint-based security

The following table captures the most common features of each base offering:

	SECURITY ENFORCEMENT POINT		
	MSSP DC	CPE	ENDPOINT
Most Commonly Deployed As	NGFW Nodes or SD-WAN Hubs Deployed in MSSP Data Center	On-premise NGFW or SD-WAN	SASE or FortiClient Cloud Agent
NGFW - Botnet/IOC, IPS, Application Control - AV, Web and Video Filtering	☑	☑	☑ via SASE
Remote Access	☑	☑	☑
ZTNA		☑	☑
SD-WAN	☑ Hubs	☑ Spokes	N/A
Zero-touch Provisioning		☑	☑
Inline CASB - Application Control, DLP - Device and User Posture Check		☑	☑ via SASE
Endpoint Vulnerability			☑

In addition, for MSSP operations, each deployment type supports single pane management, central logging, reporting and incident handling, a customer-facing portal for self-service operations, as well as further options for network and security monetization:

	MSSP DC	CPE	ENDPOINT
Operations (NOC/SOC)			
Single Pane Management	☑	☑	☑ via SASE (Future release)
Logging, Reporting, Incident Response	☑	☑	☑ via SASE (Future release)
Self-service Portal	☑	☑	☑ via SASE (Future release)
Network and Security Monetization			
Advanced SOC Services	☑	☑	☑
Remote Workforce Management	☑	☑	☑
LAN Edge/SD-Branch Management		☑	
Cloud Security Services	☑ Future Release	☑ Future Release	

NOTE: FortiCloud Organizational Unit structure for MSSPs is now available

MSSP SERVICE OFFERINGS

FLEXIBLE AND HYPERSCALE FORTIGATE OFFERINGS

Product Offerings: FortiGate and FortiGuard Security Services

FortiGate is the flagship NGFW product family from Fortinet that delivers high-speed networking, hardware-accelerated performance features, and built-in market-leading SD-WAN. MSSPs using the FortiGate NGFW can deliver high quality of service with SD-WAN and manage all security risks of end customers with the industry's best-of-breed and SPU/vSPU accelerated NGFW, IPS, UTM, and TLS inspection.

FortiGate comes in different form factors and sizes from entry level to hyperscale chassis, all running the same operating system, FortiOS, with a consistent single-pane management experience. This ensures a consistent experience both on-premise/ at the branch, and in the cloud or data center. FortiGate is available with different options for interface types, port density, security efficacy, and throughput to keep your network connected and secure wherever it is needed. For high density MSSP deployments, you can employ a centralized FortiGate with virtual domains (VDOMs) to divide it for use by multiple customers in an efficient manner.

FortiGuard provides a threat intelligence and security service that allows FortiGate products to be updated with the latest security threats information. It is provided by FortiGuard Labs, the threat intelligence and research organization at Fortinet, which develops, innovates, and maintains one of the most recognized and seasoned artificial intelligence and machine learning systems in the industry. It delivers proven unparalleled protection, visibility, and business continuity across the Fortinet Security Fabric, protecting our customers against the wide range of ever-changing and sophisticated threats.

The following shows offerings information for FortiGate and FortiGuard for MSSP:

	MSSP DC	CPE
FortiGate		
NGFW	☑	☑
SD-WAN	☑	☑
ZTNA and Remote Access		☑
Hyperscale Hardware	☑	
Hyperscale VM	☑	
WAN Link Options	☑ 1Gbps to 100Gbps	☑ Ethernet, 5G/LTE, DSL
LAN Edge/SD-Branch Management		☑
Zero Touch Provisioning (ZTP)		☑
FortiGuard Security Services		
IPS	☑	☑
Advanced Malware Protection	☑	☑
Web and Video Filtering Service	☑	☑
Industrial Security Service	Optional for OT customers	Optional for OT customers
Security Rating Service	☑	☑
IoT Detection and Virtual Patching Service		☑
	FG-1800F	FG-40F
	FG-VM-32	FG-60F
	FG-7121F	FG-80F
Top Sellers		FG-100F
		FG-200F
		FG-1800F
		FG-VM-32

SEE ALSO

For virtual machine deployments in data center or SDWAN hub locations, flexible pay-as-you-go options are available. Refer to the FortiFlex Ordering Guide and Datasheet for more details.

ORDER INFORMATION

The following table summarizes the platforms most-often selected for CPE-based deployments:

	FG-40F	FG-60F	FG-80F	FG-100F	FG-200F
Interfaces (up to)	1G	1G	1G	10G	10G
Threat Protection	600 Mbps	700 Mbps	900 Mbps	1 Gbps	3 Gbps
IPsec VPN Throughput ¹	4.4 Gbps	6.5 Gbps	6.5 Gbps	11.5 Gbps	13 Gbps
Firewall Throughput ²	5 Gbps	10 Gbps	10 Gbps	18 Gbps	27 Gbps
Hardware Enterprise Service Bundle	FG-40F FC-10-0040F-809-02-DD	FG-60F FC-10-0060F-809-02-DD	FG-80F FC-10-0080F-809-02-DD	FG-100F FC-10-F100F-809-02-DD	FG-200F FC-10-F200F-809-02-DD
Built-in Storage	N/A	FG-61F FC-10-0061F-809-02-DD	FG-81F FC-10-0081F-809-02-DD	FG-101F FC-10-F101F-809-02-DD	FG-201F FC-10-F201F-809-02-DD
Built-in Wireless	FWF-40F-X ³ FC-10-W040F-809-02-DD	FWF-60F-X ³ FC-10-W060F-809-02-DD	FWF-80F-X ³ FC-10-W080F-809-02-DD	N/A	N/A
Built-in Wireless and Storage	N/A	FWF-61F-X ³ FC-10-W061F-809-02-DD	FWF-81F-X ³ FC-10-W081F-809-02-DD	N/A	N/A
Built-in 3G/4G LTE	FG-40F-3G4G FC-10-F40FG-809-02-DD	N/A	FG-80F-DSL FC-10-F80FD-809-02-DD	N/A	N/A

1. IPsec VPN performance test uses AES256-SHA256.

2. Firewall performance test uses 512 byte UDP.

3. Replace X with the region code.

The following table summarizes the platforms most-often selected for data center (or very large CPE) deployments:

	FG-1000F	FG-1800F	FG-2600F	FG-3000F	FG-3500F	FG-3700F	FG-7121F	FG-VM-32
Interfaces (up to)	100G	40G	100G	100G	100G	400G	100G	Hardware-dependent
Threat Protection	13 Gbps	15 Gbps	17 Gbps	33 Gbps	63 Gbps	75 Gbps	520 Gbps	12 Gbps
IPsec VPN Throughput ¹	55 Gbps	55 Gbps	55 Gbps	105 Gbps	165 Gbps	160 Gbps	630 Gbps	18 Gbps
Firewall Throughput ²	196 Gbps	197 Gbps	196 Gbps	389 Gbps	590 Gbps	589 Gbps	1.88 Tbps	116 Gbps
Base Enterprise Service Bundle	FG-1000F FC-10-F1K0F-809-02-DD	FG-1800F FC-10-F18HF-809-02-DD	FG-2600F FC-10-F26HF-809-02-DD	FG-3000F FC-10-F3K0F-809-02-DD	FG-3500F FC-10-F3K5F-809-02-DD	FG-3700F FC-10-F3K7F-809-02-DD	N/A	FG-VM32 FC-10-FVM32-812-02-DD
With Storage	FG-1001F FC-10-F1K1F-809-02-DD	FG-1801F FC-10-F18F1-809-02-DD	FG-2601F FC-10-F26F1-809-02-DD	FG-3001F FC-10-F3K1F-809-02-DD	FG-3501F FC-10-F35F1-809-02-DD	FG-3701F FC-10-F37F1-809-02-DD	FG-7121F ³ FC-10-F7CF1-809-02-DD FPM-7620F FIM-7921F	

1. IPsec VPN performance test uses AES256-SHA256.

2. Firewall performance test uses 512 byte UDP.

3. Base 7121F includes 2xFPM-7620F and 2xFIM-7921F modules

MSSP OPERATIONS

CORE OPERATIONS (NOC/SOC)

Product Offerings: FortiManager

FortiManager provides automation-driven centralized management. FortiManager allows MSSPs to manage large volumes of FortiGate, FortiSwitch, and FortiAP devices in their network with a single-console central management system. FortiManager provides full visibility of the network, offering streamlined provisioning and innovative automation tools. Integrated with Fortinet's Security Fabric, the security architecture and FortiManager's automation-driven network operations capabilities provide a foundation to optimize network security. FortiManager is a multitenancy solution with quota management, leveraging ADOMs to separate customer data and manage domains for operational effectiveness and compliance. FortiManager is deployed in the central MSSP environment/platform.

Product Offerings: FortiAnalyzer

FortiAnalyzer is a powerful log management, analytics, and reporting platform, providing MSSPs with single-pane orchestration, automation, and response for simplified security operations, proactive identification, and remediation of risks, including complete visibility of the entire attack surface. FortiAnalyzer reads data from Fortinet products and is integrated with the Security Fabric. FortiAnalyzer is a multitenancy solution with quota management, leveraging ADOMs to separate customer data according to domains for operational effectiveness and compliance. FortiAnalyzer is deployed in the central MSSP environment/platform.

ORDER INFORMATION

The following tables highlight the models that are most commonly selected options for core operations by MSSP partners across deployments of different types, sizes, and geographical locations:

SOLUTION BUNDLE	FMG-VM SUBSCRIPTION	FMG-1000G	FMG-3700G	
FortiManager	Devices/VDOMs	100	1 000	10 000
	Base Product	FC2-10-FMGVS-258-01-DD*	FMG-1000G	FMG-3700G
	Support	N/A	FC-10-FM1KG-247-02-DD	FC-10-M3K7G-247-02-DD
	Expansion	FMG-VM-{10, 100, 1000, 5000}-UG		FMG-DEV-100-UG

* VM subscription license including FortiCare premium support.

SOLUTION BUNDLE	FAZ-300G	FAZ-1000G	FAZ-3700G	FAZ-VM	
FortiAnalyzer	GB/day	100 GB	660 GB	8 300 GB	Stackable ¹
	Base Product	FAZ-300G	FAZ-1000G	FAZ-3700G	FC1-10-AZVMS-465-01-DD ²
	Hardware Bundle	FAZ-300G-BDL-466-DD	FAZ-1000G-BDL-466-DD	FAZ-3700G-BDL-466-DD	
	Renew ³	FC-10-L03HG-466-02-DD	FC-10-AZ1KG-466-02-DD	FC-10-L3K7G-466-02-DD	FC[1-3]-10-AZVMS-465-01-DD

1. Depends on the VM deployment (hypervisor, number and type of CPUs, IOPS setup, amount of memory allocated, and so on).

2. VM subscription license including FortiCare premium support.

3. Includes support.

MSSP OPERATIONS

CORE OPERATIONS

Product Offerings: FortiPortal

FortiPortal is a comprehensive end-user self-service portal designed for enterprises, education institutions, and governments — specifically optimized for service providers. It provides cloud-based security policy management and analytics and enables MSSPs to assign common firewall configuration and monitoring tasks to users in different geographical locations, while easily integrating cyber security management products to provide end customer services for security management, configuration, and analytics. FortiPortal is deployed in the central MSSP premises. Its scalability and multitenancy offers a complete solution for service providers to manage hundreds of FortiGates and APs across multiple customers with complete data isolation and control over users.

FortiPortal is built on the top of Fortinet's management platforms and allows MSSPs to delegate the common firewall configuration and monitoring tasks to their end customers such as network policy management, controlled access to configuration, management tasks, and analytics.

FortiPortal is deployed in the central MSSP premises. Its scalability and multitenancy offer a complete solution for service providers to manage hundreds of FortiGates and APs across multiple customers with complete data isolation and control over users.

ORDER INFORMATION

SOLUTION BUNDLE	FPC-VM-BASE
	FortiPortal-VM Base License FPC-VM-BASE
	FortiPortal-VM Upgrade License FPC-VM-XXXX-UG*
FortiPortal	FortiPortal-VM Subscription License with Support FC1-10-PCVMS-258-01-DD
	Expansions FPC-VM-XXXX-UG*
	Expansions Support FC[1-7]-10-FPC00-248-02-DD

* Replace XXXX with number of devices.

NETWORK AND SECURITY MONETIZATION

Additional services can be easily added on top of the base offerings, including:

- **Augmented SOC:** SIEM-less addition of SIEM, SOAR, Sandboxing, and EDR services
- **Remote Access/Work-from-Anywhere:** SASE, ZTNA, and VPN options
- **LAN Edge:** fully managed wireless, switch, and wireless WAN (5G) networks
- **Cloud Security:** expanded service options including WAF, mail security, SaaS protection, and more

The following table highlights the most common options to expand each offering:

	SECURITY ENFORCEMENT POINT		
	MSSP DC	CPE	ENDPOINT
Augmented SOC Expansion			
SIEM and SOAR	☑	☑	☑
Sandbox	☑	☑	☑
EDR			☑
Remote Workforce Expansion			
SASE	☑ with SD-WAN	☑ with SD-WAN	☑
VPN/ZTNA		☑	☑
LAN Edge Expansion			
Managed WiFi		☑	
Managed Switch		☑	
Managed 5G/LTE		☑	
Cloud Expansion			
WAF-as-a-Service	Optional	Optional	
ZTNA-as-a-Service	Optional	Optional	
SecureMail-as-a-Service	Optional	Optional	
Public Cloud Migration and CI/CD Pipeline Security	Optional	Optional	

AUGMENTED SOC

Product Offerings: FortiSIEM

FortiSIEM provides unified event correlation and risk management for multivendor MSSP networks. It enables unified data collection and analytics from diverse information sources including logs, performance metrics, SNMP traps, security alerts, and configuration changes. FortiSIEM converts every piece of information into an event, first parsing and then feeding it into an event-based analytics engine for monitoring real-time searches, rules, dashboards, and ad-hoc queries. With FortiSIEM, service providers can get visibility and security analysis of not only their own network, but also their end customers' equipment and endpoints. FortiSIEM's multitenant architecture and granular RBAC controls allow varying levels of access to administrators and tenants/customers. For large MSSPs, you can configure collectors as multitenant to reduce the overall deployment footprint. FortiSIEM is deployed in the central premises of the MSSP.

The following shows offerings information for FortiSIEM for MSSP:

MSSP OPERATIONS	
FortiSIEM	
Device monitoring and analytics	✓
Performance and digital experience monitoring	✓
Security automation and response	✓
Agent-based monitoring*	✓
Insider threat monitoring	✓
Advanced insider threat monitoring: * Endpoint-based UEBA * Remote worker monitoring * On- and off-network endpoint monitoring	Optional
Threat intelligence	✓
EPS (events per second)**	✓
Training services	✓
	FSM-AIO-BASE
Top Selling	FSM-2000G
	FSM-3600G

* Agent license requires a device or endpoint license. For example, one Windows server with FIM requires one device and one agent license.

** See MSSP agreement for unlimited EPS.

ORDER INFORMATION

SOLUTION BUNDLE ¹	FSM-3600G	FSM-2200G	FSM-AIO-BASE
Performance benchmark	Up to 50K EPS with Collectors ²	Up to 20K EPS with Collectors ²	50 devices and 500 EPS ³
Base product	FSM-3600G FSM-AIO-3600-BASE	FSM-2200G FSM-AIO-2200-BASE	FSM-AIO-BASE
FortiSIEM			
All-in-one expansion: add XX devices and EPS/device⁴	FSM-AIO-XX-UG	FSM-AIO-XX-UG	FSM-AIO-XX-UG
Endpoint expansions: add XX endpoints and 2 EPS/endpoint⁴	FSM-EPD-XX-UG	FSM-EPD-XX-UG	FSM-EPD-XX-UG
Support	FC-10-FSM36G-247-02-DD FC[2-Y]-10-FSM99-240-02-DD	FC-10-FM22G-247-02-DD FC[2-Y]-10-FSM99-240-02-DD	FC[1-G]-10-FSM97-248-02-DD

¹ This table only lists CAPEX/perpetual licensing. For OPEX/subscription, refer to the FortiSIEM Ordering Guide. For MSSP PAYG licensing, contact your local Fortinet sales team.

² Requires device or EPS licenses, which you must purchase separately, to reach this level.

³ Starting license limit.

⁴ For these SKUs, replace XX with the number of devices.

AUGMENTED SOC

Product Offerings: FortiSOAR

FortiSOAR is a holistic security orchestration, automation, and response workbench designed for SOC teams to efficiently respond to the ever-increasing influx of alerts, repetitive manual processes, and shortage of resources. This patented and customizable security operations platform provides, automated playbooks and incident triaging, and real-time remediation for enterprises to identify, defend, and counter attacks.

FortiSOAR optimizes SOC team productivity by seamlessly integrating with over 300+ security platforms and 3000+ actions. This results in faster responses, streamlined containment, and mitigation times reduced from hours to seconds. FortiSOAR can be used to automate both the response to security events in the MSSP's own network as well as in the nodes devoted to specific end customers. FortiSOAR provides a truly multitenant, distributed architecture, from a single, collaborative console. It is deployed in the central premises of the MSSP.

The following shows offerings information for FortiSOAR for MSSP:

MSSP OPERATIONS	
FortiSIEM	
SOAR for MSSPs	☑
	LIC-FSRMTT-2
Top selling	LIC-FSRMTD-1
	LIC-FSRMTR-2

ORDER INFORMATION

SOLUTION BUNDLE	LIC-FSRMTT-2	LIC-FSRMTD-1	LIC-FSRMTR-2	
FortiSOAR	Base capacity	2 user logins	1 user login	2 user logins
	Base product	LIC-FSRMTT-2	LIC-FSRMTD-1	LIC-FSRMTR-2
	Expansions	LIC-FSRAUL-1	LIC-FSRAUL-1	LIC-FSRAUL-1
	Support	FC2-10-SRVMP-248-02-DD	FC3-10-SRVMP-248-02-DD	FC4-10-SRVMP-248-02-DD

AUGMENTED SOC

Product Offerings: FortiSandbox

FortiSandbox provides a top-rated AI-powered breach protection that integrates with the Security Fabric platform to address the rapidly evolving and more targeted threats including ransomware, cryptomalware, and others across a broad digital attack surface. Specifically, it delivers real-time actionable intelligence through the automation of zero-day advanced malware detection and response. FortiSandbox can be bought as CAPEX or PAYG depending on the service provider's financial preferences. The CAPEX model involves a multitenant centralized deployment with perpetual licenses. The PAYG model is described in the FortiSandbox Ordering Guide.

The following shows offerings information for FortiSandbox for MSSP:

USER AND ENDPOINT SECURITY	
FortiSandbox as CAPEX	
OT Environment Support	Optional
AI-based Behavior Analysis	☑
AV, IPS, Web Filtering	☑
Antievasion Detection	☑
CandC Detection	☑
Top selling	FSA-500G
	FSA-3000F

ORDER INFORMATION

SOLUTION BUNDLE	FSA-500G	FSA-3000F
FortiSandbox		
Effective Sandboxing Throughput (Files/Hr)	10 000	68000
Base Product	FSA-500G	FSA-3000F
Threat Intelligence and Support	FC-10-FS5HG-499-02-DD	FC-10-SA3KF-499-02-DD
Expansions	FSA-500G-UPG-LIC-BYOL	FSA-3000F-UPG-LIC-BYOL

AUGMENTED SOC

Product Offerings: FortiEDR

FortiEDR delivers real-time automated endpoint protection with the orchestrated incident response across one of a broad variety of current and legacy operating systems for Windows, Linux, and MacOS workstations and servers as well as manufacturing and OT systems — all in a single integrated platform with flexible deployment options and a predictable operating cost.

Managed service options are available for all endpoint protection options, however, cannot be supported for on-prem deployments.

FortiEDR post-paid program for MSSP

The FortiEDR for MSSP licensing solution has been developed to allow MSSP Partners to utilize FortiEDR using pay-as-you-grow-based billing. This distribution-led solution allows a Partner to be billed monthly based on the number of endpoint licenses used above the initial 1000 seat/annual licenses.

The program contains these components:

- FortiEDR Discover-Protect-and-Response subscription for 1 000 assets: Support - 24x7 phone support
- Digital Forensics and Incident Response consulting - 10 service hours
- FortiEDR professional services day

The Partner will be provisioned with a FortiEDR Cloud region, where they will be able to create the customer account and deploy FortiEDR to their customer base. The program fee will be renewed on an annual basis.

High-level requirements of FortiEDR for MSSP program:

The Partner must be an active MSSP Partner with Fortinet to qualify for this program. The FortiEDR instance must be used for a service to be delivered by the Partner. This program is not available to Enterprise customers or for resell.

Program Prerequisites:

- Eligible MSSP Partner - Select or Advanced or Expert Level

PAYG program Fee is renewed yearly, which includes the initial 1 000 licenses.

ORDER INFORMATION

For more information on the FortiEDR MSSP PAYG licensing, contact your local Fortinet representative.

REMOTE WORKFORCE

Product Offerings: FortiClient

ZTNA enables remote users to access their corporate applications while ensuring strict authentication and endpoint posture/security checks before any access is granted. ZTNA helps minimize the attack surface for today's remote workforce.

SASE ensures remote users are protected and enforced using the same corporate security policies regardless of location. SASE integrates seamlessly with ZTNA to deliver a transparent user experience while protecting all endpoints from advanced threats.

EPP protection, including Vulnerability Detection and Auto-patching Anti-virus, Application Firewall, Anti-Ransomware and more are included in all remote workforce options.

The following shows offerings information for FortiClient for MSSP:

USER AND ENDPOINT SECURITY	
FortiClient	
VPN (IPsec and SSL)	✓
ZTNA	✓
Vulnerability Detection and Autopatching	✓
EPP Protection	✓
Antiransomware	✓
SASE	✓
Top selling	

ORDER INFORMATION

ORDERING OPTIONS	MANAGED VULNERABILITY AND EPP	MANAGED VULNERABILITY AND EPP + FORENSICS	
Per-Endpoint	25-pack	FC1-10-EMS05-485-01-DD	FC1-10-EMS05-539-01-DD
	500-pack	FC2-10-EMS05-485-01-DD	FC2-10-EMS05-539-01-DD
	2,000-pack	FC3-10-EMS05-485-01-DD	FC3-10-EMS05-539-01-DD
	10,000-pack	FC4-10-EMS05-485-01-DD	FC4-10-EMS05-539-01-DD

LAN EDGE/SD-BRANCH

Product Offerings: FortiAP

FortiAP is a series of Wi-Fi APs that are managed by FortiCloud or FortiOS. They are high throughput, optimal coverage, enterprise class 802.11ax indoor APs. This top-of-the-line access point allows MSSPs to extend the security services and network protection to the end customer premises, whether small branches or large enterprise campuses. The AP is a key part of an SD-Branch solution that the MSSP centrally operates. The AP is tightly integrated with the Security Fabric and enforces the security and access policies set forth for the end customer as devices try to access the network. FortiAP is deployed on the end customer's premises.

The following shows offerings information for FortiAP for MSSP:

NETWORK AND APPLICATION SECURITY	
FortiAP	
Most Commonly Deployed As	Wi-Fi AP
Use Cases	
Cloud Management License	☑
Presence Analytics License	Optional
	FAP-231G
Top selling	FAP-231F
	FAP-431F
	FortiPresence-VM

ORDER INFORMATION

SOLUTION BUNDLE		FAP-231G	FAP-231F	FAP-431F
	Access Point Type	WiFi 6 Tri Radio	WiFi 6 Tri Radio	WiFi 6 Tri Radio
	MIMO	2×2	2×2	4×4
	Ethernet ports	2	2	2
FortiAP	Base Product	FAP-231G-suffix*	FAP-231F-suffix*	FAP-431F-suffix*
	Support	FC-10-PG231-247-02-DD	FC-10-PF231-247-02-DD	FC-10-F431F-247-02-DD
	Cloud Management License	FC-10-90AP1-639-02-DD	FC-10-90AP1-639-02-DD	FC-10-90AP1-639-02-DD
	Presence Analytics License	FC-10-FPCLD-169-02-DD	FC-10-FPCLD-169-02-DD	FC-10-FPCLD-169-02-DD
SOLUTION BUNDLE		FORTIPRESENCE-VM		
	Hardware/Base	LIC-FPA-VM + LIC-FPA-AP-[50,250,500,1000]		
FortiAP	Support	FC-10-FPAVM-248-02-DD		

* Refer to the latest pricelist for the list of available suffixes.

LAN EDGE/SD-BRANCH

Product Offerings: FortiSwitch

FortiSwitch is a secure access switch family that delivers outstanding security, performance, and manageability. FortiSwitch is secure, simple, and scalable. FortiSwitch allows MSSPs to extend the security services and network protection to the end customer premises, whether mid-size branches or large enterprise campuses. Tightly integrated into the Security Fabric via FortiLink, FortiSwitch is operated centrally by the MSSP. Its single pane of glass management provides complete visibility and control of users and devices on the network regardless of how they connect. This makes the FortiSwitch ideal for SD-Branch deployments, enabling businesses to converge their security and network access. FortiSwitch is deployed on the end customer's premises.

The following shows offerings information for FortiSwitch for MSSP:

NETWORK AND APPLICATION SECURITY	
FortiSwitch	
Most Commonly Deployed As	Managed and secure switch
Use Cases	
Advanced Switching License*	<input checked="" type="checkbox"/>
Presence Analytics License	Optional
Top selling	FSW-224E
	FSW-124F
	FSW-448E

* The Advanced Switching license enables dynamic routing protocols in standalone mode and does not apply in FortiLink mode.

ORDER INFORMATION

SOLUTION BUNDLE	FSW-224E	FSW-124F	FSW-448E
Target location	Branch	Medium Campus	Medium Campus
Ports	24	24	48
Uplink Speed	1G (SFP)	10G (SFP+)	10G (SFP+)
Downlink Speed	1G (RJ45)	1G (RJ45)	1G (RJ45)
Base Product	FSW-224E	FSW-124F	FSW-448E
Support	FC-10-W0300-247-02-DD	FC-10-S124N-247-02-DD	FC-10-S448N-247-02-DD
Cloud Management License	FC-10-FSW00-628-02-DD	FC-10-FSW10-628-02-DD	FC-10-FSW10-628-02-DD
Advanced Switching License*	FS-SW-LIC-200		FS-SW-LIC-400

* The Advanced Switching license enables dynamic routing protocols in standalone mode and does not apply in FortiLink mode.

LAN EDGE/SD-BRANCH

Product Offerings: FortiExtender

FortiExtender provides a bridge between local Ethernet LANs and a stable LTE/5G WAN connection. It can support diverse applications with a high level of backhaul redundancy using a single LTE/5G modem platform with redundant SIM cards attaching to different mobile networks. FortiExtender are placed at allocation of the end customer's premises to achieve the maximum LTE/5G wireless signal strength. FortiExtender can be used as the LTE/5G backhaul of an on-premise FortiGate. You can also combine FortiExtender with FortiAP and FortiSwitch to allow the MSSP to offer an SD-Branch for distributed light branch offices. In this case, FortiExtender can be connected either a centralized FortiGate providing a clean pipe service or to security- and networking-as-a-service offerings, such as SASE.

The following shows offerings information for FortiExtender for MSSP:

NETWORK AND APPLICATION SECURITY	
FortiExtender	
PKI (SD-WAN)	☑
FortiExtender Cloud Management	Optional
	FEX-201F
Top selling	FEX-211E
	FEX-511F

ORDER INFORMATION

SOLUTION BUNDLE	FEX-201F-AM/EA	FEX-211E	FEX-511F
Supported technology	LTE CAT-7	LTE CAT-12	LTE CAT-20/5G NR
Regional Compatibility	AM: America EA: EMEA, APAC carriers	Global carriers	North and South America and EMEA carriers, and some APAC carriers
FortiExtender			
Base Product	FEX-201F-AM FEX-201F-EA	FEX-211E	FEX-511F
FortiExtender Cloud Management	FC-10-FEXC0-583-02-DD	FC-10-FEXC0-583-02-DD	FC-10-FEXC2-583-02-DD
Support	FC-10-FA21F-247-02-DD FC-10-FE21F-247-02-DD	FC-10-F211E-247-02-DD	FC-10-X511F-247-02-DD

CLOUD

Product Offerings: FortiWeb

FortiWeb is a web application firewall (WAF) that protects web applications and APIs from attacks that target known and unknown exploits and helps maintain compliance with regulations. Using machine learning to model each application, FortiWeb defends applications from known vulnerabilities and from zero-day threats. High-performance physical and virtual appliances and containers can be deployed on the end customer's premises, or at the MSSP's data center or public cloud zone. FortiWeb can bring security to end customers that migrate to interfaces based on REST and HTTP. For high-density MSSP deployments, a centralized FortiWeb with VDOMs can be employed to divide it for use by multiple customers in an efficient manner. FortiWeb can be bought as CAPEX or PAYG depending on the service provider's financial preferences. The CAPEX model involves a multitenant centralized deployment with perpetual licenses. The PAYG model is described in the FortiFlex Ordering Guide.

FortiWeb can be bought as CAPEX or PAYG depending on the service provider's financial preferences.

- The CAPEX model involves a multitenant centralized deployment with perpetual licenses.
- The PAYG model is described in the FortiFlex Ordering Guide.

The following table shows service offerings for FortiWeb:

	A LA CARTE	STANDARD BUNDLE	ADVANCED BUNDLE
FortiWeb			
IP Reputation	☑	☑ Included	☑ Included
FortiGuard AV	☑	☑ Included	☑ Included
FortiWeb Application Security	☑	☑ Included	☑ Included
FortiWeb Cloud Sandbox	☑		☑ Included
Credential Stuffing Defense	☑		☑ Included
		FWB-VMC08	
		FWB-VM08	
Top selling		FWB-1000F	
		FWB-3000F	
		FWB-4000F	

ORDER INFORMATION

SOLUTION BUNDLE	FWB-VMC08	FWB-VM08	FWB-1000F	FWB-3000F	FWB-4000F
HTTP Throughput	3 Gbps	3 Gbps	2.5 Gbps	10 Gbps	70 Gbps
Base Product	FWB-VMC08	FWB-VM08	FWB-1000F	FWB-3000F	FWB-4000F
FortiWeb Standard Bundle and Support	FC-10-VMC08-936-02-DD	FC-10-VVM08-936-02-DD	FC-10-FV1KF-934-02-DD	FC-10-FW3KF-934-02-DD	FC-10-FW4KF-934-02-DD
FortiWeb Advanced Bundle and Support	FC-10-VMC08-581-02-DD	FC-10-VVM08-581-02-DD	FC-10-FV1KF-580-02-DD	FC-10-FW3KF-580-02-DD	FC-10-FW4KF-580-02-DD
FortiWeb IP Reputation Service	FC-10-VMC08-140-02-DD	FC-10-VVM08-140-02-DD	FC-10-FV1KF-140-02-DD	FC-10-FW3KF-140-02-DD	FC-10-FW4KF-140-02-DD
FortiWeb Application Security Service	FC-10-VMC08-137-02-DD	FC-10-VVM08-137-02-DD	FC-10-FV1KF-137-02-DD	FC-10-FW3KF-137-02-DD	FC-10-FW4KF-137-02-DD

SEE ALSO

For virtual machine deployments in data center locations, flexible pay-as-you-go options are available for FortiWeb. Refer to the FortiFlex Ordering Guide and Datasheet for more details.

CLOUD

Product Offerings: FortiMail

FortiMail provides powerful and scalable email security protection. With best-in-class performance that independent testing firms have validated, FortiMail delivers advanced multilayered protection against the full spectrum of email-borne threats. Powered by FortiGuard Labs threat intelligence and integrated into the Security Fabric, FortiMail helps your organization prevent, detect, and respond to email-based threats including spam, phishing, malware, zero-day threats, impersonation, and Business Email Compromise (BEC) attacks. FortiMail can be bought as CAPEX or PAYG depending on the service provider's financial preferences. The CAPEX model involves a multitenant centralized deployment with perpetual licenses. The PAYG model is described in the FortiMail Cloud datasheet.

FortiMail can be bought as CAPEX or PAYG depending on the service provider's financial preferences.

- The CAPEX model involves a multitenant centralized deployment with perpetual licenses.
- The PAYG model is described in the FortiMail Cloud datasheet.

The following shows offerings information for FortiMail for MSSP:

NETWORK AND APPLICATION SECURITY	
FortiMail as CAPEX	
FortiGuard Base Bundle	☑
Enterprise ATP Bundle	☑
Email Continuity	☑
Advanced Administration for MSSPs	☑
	FML-900F
	FML-3000F
Top selling	FML-VM08
	FML-VM16

ORDER INFORMATION

SOLUTION BUNDLE	FML-900F	FML-3000F	FML-VM08	FML-VM16
Protected Email Domains	800	2000	1000	1500
Server Mode Mailboxes	1500	3000	2000	3000
Email Routing (per hour)	800 K	3.5 M	675 K	875 K
FortiGuard Base Bundle	FML-900F-BDL-640-DD	FML-3000F-BDL-640-DD	FML-VM08 + FC-10-0VM08-642-02-DD	FML-VM16 + FC-10-0VM16-642-02-DD
FortiMail as CAPEX				
FortiGuard Base Renewal Bundle	FC-10-FE9HF-640-02-DD	FC-10-FE3KF-640-02-DD	FC-10-0VM08-642-02-DD	FC-10-0VM16-642-02-DD
Enterprise ATP Bundle	FML-900F-BDL-641-DD	FML-3000F-BDL-641-DD	FML-VM08 + FC-10-0VM08-643-02-DD	FML-VM16 + FC-10-0VM16-643-02-DD
Enterprise ATP Renewal Bundle	FC-10-FE9HF-641-02-DD	FC-10-FE3KF-641-02-DD	FC-10-0VM08-643-02-DD	FC-10-0VM16-643-02-DD
Email Continuity	FC-10-FE9HF-309-02-DD	FC-10-FE3KF-309-02-DD	FC-10-0VM08-309-02-DD	FC-10-0VM16-309-02-DD
Advanced Administration for MSSPs	FC-10-FE9HF-408-02-DD	FC-10-FE3KF-408-02-DD	FC-10-0VM08-408-02-DD	FC-10-0VM16-408-02-DD

ADDITIONAL INFORMATION AND RESOURCES

PRODUCT	DATASHEET
FortiGate	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf
FortiGate VM	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-vm.pdf
FortiManager	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
FortiAnalyzer	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf
FortiGuard	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf
FortiExtender	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiExtender.pdf
FortiPortal	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiPortal.pdf
FortiSIEM	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf
FortiSOAR	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisoar.pdf
FortiSandbox	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf
FortiEDR	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf
FortiClient	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/forticlient.pdf
FortiAP	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-series.pdf
FortiSwitch	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSwitch_Secure_Access_Series.pdf
FortiWeb	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiWeb.pdf
FortiMail	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail.pdf
FortiFlex	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-flex-vm.pdf

FREQUENTLY ASKED QUESTIONS

How does the MSSP market's needs differ from the Telco market's?

As a Telco operator can also be an MSSP, this may lead to some confusion. Often, a Telco operator has an MSSP division that bundles security and connectivity services together.

MSSP sales include the following:

- Large sales-through part for pieces that are dedicated to a given end customer and an enterprise
- Smaller sales-to part for pieces that are deployed centrally on the MSSP data centers and needed to run any managed service

With the exception of private networks, Telco sales generally do not include a sales-through part. Telco sales are sales-to and meant to protect the operator's network or individual subscribers as part of a service bundle.

Visit www.fortinet.com for more details



Copyright © 2024 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 Chief Legal Officer, 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 all 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.