ORDERING GUIDE

Telco Vertical

Fortinet has a comprehensive offering of security products and solutions to protect Telco networks, including dedicated purpose-built products and features for Telecommunications environments.

This ordering guide is a quick reference to the most relevant Fortinet products for the following areas in Telco:

- **5G and 4G User and Control Planes**: products used to protect the packet core and user equipment from other parts of the network and external networks. The most common use cases are Security Gateway, CG-NAT, NGFW, roaming firewall, and API security
- **Telco Cloud**: products used to protect the management and orchestration layers of the Telco Cloud and tenant workloads
- **NOC/SOC**: products that provide visibility, analysis, and control over the security events in the network
- **Private Networks**: products used for Industry 4.0 and other use cases enabled by small 5G deployments

Telco operators also provide services for Security Monetization: these are billable security services to end customers. The telco operator that offers these services is acting as an MSSP and therefore the products that enable them are covered in the **MSSP Ordering Guide**.

The following technologies, commercial models, and specific use cases are covered by different Fortinet Security Fabric products:

		5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS	SECURITY MONETIZATION
5G and IoT	Segmentation and Perimeter Firewall	✓	✓	✓	✓	Optional
	Roaming Firewall	✓	✓		Optional	
	Security Gateway Firewall	✓			Optional	
	CG-NAT and Gi/N6 Firewall	✓			✓	
	Hyperscale Firewall	✓	✓			
	API Security	✓	✓		Optional	Optional
	Central Management and Analytics	✓		✓	✓	✓
Cloud Transformation	ASIC Powered	✓	Optional		Optional	Optional
	Consumption Licensing	✓				
	VM/Flex-VM	✓	✓		✓	✓
	Containers	✓	✓		Optional	✓
	Cloud Platform Security		✓			
Security Fabric Platform	Automation		✓	✓		
	Connectors		✓	✓		
	Fabric-ready Integrations			✓		
	Compliance and Regulatory	✓	✓	✓	Optional	

The table shows the most common technologies, commercial models, and use cases. A missing checkmark does not mean that you cannot use the item for a specific area.

PRODUCT OFFERINGS

The following table summarizes the Fortinet product offerings that are frequently selected for these use cases. Refer to the individual Data Sheets for each product for more details. You can find them under https://www.fortinet.com/resources/datasheets.

		5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS	SECURITY MONETIZATION
Core Operations	FortiGate	✓	✓	✓	✓	✓
	FortiFirewall	✓				
	FortiManager	✓	✓	✓	✓	✓
	FortiAnalyzer	✓	✓	✓	✓	✓
Cloud Security	FortiWeb	✓	✓		Optional	Optional
	FortiCNP		✓			
	FortiDevSec		✓			
	FortiRecon			✓		Optional
Security Operations (SOC)	FortiSIEM	✓	✓	✓		Optional
	FortiSOAR	Optional	✓	✓		Optional
	FortiEDR			✓	Optional	Optional
	FortiDeceptor	✓	✓	Optional	✓	Optional
	FortiSandbox			✓		Optional
Identity and Access Management (IAM)	FortiAuthenticator	Optional	✓	✓	✓	
	FortiPAM	✓	✓	✓	Optional	

All Fortinet products are applicable to most Telco customers and a missing checkmark below does not mean you cannot use the product for a specific customer use case.

This ordering guide covers the CAPEX model of the different products. The corresponding product Ordering Guide lists other models (OPEX, MSSP, Cloud).

CORE OPERATIONS - SECURITY USE CASES

FortiGate is the flagship NGFW product family from Fortinet that delivers Telco-grade security-driven networking capabilities. Operators using the FortiGate NGFW can manage all of their security risks with the industry's best-of-breed IPsec, GTP, PFCP, IPS and SSL inspection, and threat protection. FortiGate is available in different form factors and sizes for deployment at the network edge, the core data center, the public cloud, and on customer premises. FortiGate is offered as appliances or virtual machines with different options for interface types, port density, security efficacy, and throughput to keep your network connected and secure wherever it is needed.

FortiGuard provides a threat intelligence and security service that allows FortiGate products to be updated with the latest security threats. 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. We use this to deliver 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.

FortiFirewall is an evolved product from FortiGate that uses a perpetual licensing model based on network-wide bandwidth peak usage. It allows operators to better adjust the capital expenditure to the demand from their customers. FortiFirewall was designed for the user plane security functions.

The following shows offerings information for FortiGate, FortiFirewall, and FortiGuard for Telco:

	5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS
FortiGate				
Most Commonly Deployed As	SecGW, CG-NAT, NGFW, Roaming Firewall, Internal Segmentation, IoT Detection	Internal Segmentation, Application Control	Internal Segmentation	Internal Segmentation, Industrial Security, IoT Detection
Use Cases				
SecGW	✓			Optional
CG-NAT and Gi/N6 FW (Hyperscale license)	✓			✓
GTP Roaming Firewall (FortiCarrier license)	✓			Optional
Internal Segmentation	✓	✓	✓	✓
FortiGuard Security Services				
Application Control		Optional		Optional
IPS		Optional		Optional
Antimalware		Optional		Optional
Web and Video Filtering		Optional		Optional
Security Rating		Optional		Optional
IoT Detection	Optional			✓
Industrial Security				✓
SD-WAN		Optional		Optional
Deployment				
Top Selling	FG-7121F1[1]	FG-1800F	FG-VM-KVM	FG-VM-KVM
	FG-7081F[1]			
	FG-4800F	FG-VM-KVM	FG-1800F	FG-1800F
	FG-4400F	FG-2600E		
	FG-4200F			

1 For roaming firewall

CORE OPERATIONS - SECURITY USE CASES

	5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS
FortiFirewall				
Most Commonly Deployed As	SecGW, CG-NAT			
Use Cases				
SecGW	✓			
CG-NAT and Gi/N6 FW (Hyperscale license)	✓			
Top Selling	FFW-4801F			
	FFW-4400F			
	FFW-2600F			
	FF-VMBB			

ORDER INFORMATION

SOLUTION BUNDLE		FG-1800F	FG-2600F	FG-3000F	FG-3700F	FG-4200F
FortiGate	**Firewall and CG-NAT Throughput[1]**	**197 Gbps**	**198 Gbps**	**389 Gbps**	**589 Gbps**	**788 Gbps**
	IPsec VPN and SecGW Throughput[2]	**55 Gbps**	**55 Gbps**	**105 Gbps**	**160 Gbps**	**210 Gbps**
	Interfaces	40G, 25G, 10G, 1G	100G, 40G, 25G, 10G	100G, 40G, 25G, 10G	400G, 50G, 25G, 10G	100G, 40G, 25G, 10G
	Base Product	FG-1800F	FG-2600F	FG-3000F	FG-3700F	FG-4200F
	Hyperscale Firewall License	LIC-FG18F-HYPSC	LIC-FG26F-HYPSC	LIC-FG35F-HYPSC	N/A	LIC-FG42F-HYPSC
	FortiCarrier Licenses[4]	N/A	Yes	FCR-EUPG	FCR-EUPG	FCR-EUPG
	Enterprise Hardware Bundle	FG-1800F-BDL-809-DD	FG-2600F-BDL-809-DD	FG-3000F-BDL-809-DD	FG-3700F-BDL-809-DD	FG-4200F-BDL-809-DD
	Enterprise Renewal Bundle	FC-10-F18HF-809-02-DD	FC-10-F26HF-809-02-DD	FC-10-F3K0F-809-02-DD	FC-10-F3K7F-809-02-DD	FC-10-F42HF-809-02-DD
	OT Security Service	FC-10-F18HF-159-02-DD	FC-10-F26HF-159-02-DD	FC-10-F3K0F-159-02-DD	FC-10-F3K7F-159-02-DD	FC-10-F42HF-159-02-DD
	Attack Surface Security Service	FC-10-F18HF-175-02-DD	FC-10-F26HF-175-02-DD	FC-10-F3K0F-175-02-DD	FC-10-F3K7F-175-02-DD	FC-10-F42HF-175-02-DD
		FG-4400F	**FG-4800F**	**FG-7081F**	**FG-7121F**	**FG-VM-KVM**
	Firewall and CG-NAT Throughput[1]	**1.14 Tbps**	**3.1 Tbps**	**1.88 Tbps**	**1.88 Tbps**	**44 Gbps**
	IPsec VPN and SecGW Throughput[2]	**310 Gbps**	**800 Gbps**	**378 Gbps**	**630 Gbps**	**47 Gbps[7]**
	Interfaces	100G, 40G, 25G, 10G	400G, 200G, 100G, 50G, 40G, 25G, 10G	400G, 100G, 40G, 25G, 10G	400G, 100G, 40G, 25G, 10G	N/A
	Base Product	FG-4400F	FG-4800F	FG-7081F	FG-7121F	FG-VM32
	Hyperscale Firewall License[3]	LIC-FG44F-HYPSC	LIC-FG48F-HYPSC			
	FortiCarrier Licenses[4]	FCR-EUPG	FCR-EUPG	FCR-EUPG	FCR-EUPG	FCR-EUPG
	Enterprise Hardware Bundle	FG-4400F-BDL-809-DD	FG-4800F-BDL-809-DD	FG-7081F-BDL-809-DD	FG-7121F-BDL-809-DD	FC6-10-FGVVS-814-02-DD
	Enterprise Renewal Bundle	FC-10-F44HF-809-02-DD	FC-10-F48HF-809-02-DD	FC-10-F78F1-809-02-DD	FC-10-F7CF1-809-02-DD	FC-10-FVM32-812-02-DD
	OT Security Service	FC-10-F44HF-159-02-DD	FC-10-F48HF-159-02-DD	FC-10-F78F1-159-02-DD	FC-10-F7CF1-159-02-DD	FC-10-FVM32-159-02-DD
	Attack Surface Security Service	FC-10-F42HF-175-02-DD	FC-10-F48HF-175-02-DD	FC-10-F78F1-175-02-DD	FC-10-F7CF1-175-02-DD	FC-10-FVM32-175-02-DD

ORDER INFORMATION

SOLUTION BUNDLE		FFW-2600F	FFW-4200F	FFW-4400F	FFW-4801F	FF-VMBB
FortiFirewall[5]	**Firewall and CG-NAT Throughput[1]**	**196 Gbps**	**788 Gbps**	**1.14 Gbps**	**3.1 Gbps**	**44 Gbps**
	IPsec VPN and SecGW Throughput[2]	**55 Gbps**	**210 Gbps**	**310 Gbps**	**800 Gbps**	**47 Gbps[7]**
	Interfaces	100G, 40G, 25G, 10G	100G, 40G, 25G, 10G	100G, 40G, 25G, 10G	400G, 200G, 100G, 50G, 40G, 25G, 10G	
	Base Product	FFW-2600F	FFW-4200F	FFW-4400F	FFW-4801F	FF-VMBB
	Support	FC-10-B260F-247-02-DD	FC-10-B420F-247-02-DD	FC-10-B440F-247-02-DD	FC-10-B481F-247-02-DD	
	Perpetual BW License for SecGW (10 Gbps)[6]	FG-PBW-10G	FG-PBW-10G	FG-PBW-10G	FG-PBW-10G	FG-PBW-10G
	Perpetual BW License for SecGW (100 Gbps)[6]	FG-PBW-100G	FG-PBW-100G	FG-PBW-100G	FG-PBW-100G	FG-PBW-100G
	Perpetual BW License for SecGW (1 Tbps)[6]	FG-PBW-1000G	FG-PBW-1000G	FG-PBW-1000G	FG-PBW-1000G	FG-PBW-1000G
	Perpetual BW License for CG-NAT (10 Gbps)[6]	FG-PBC-10G	FG-PBC-10G	FG-PBC-10G	FG-PBC-10G	FG-PBC-10G
	Perpetual BW License for CG-NAT (100 Gbps)[6]	FG-PBC-100G	FG-PBC-100G	FG-PBC-100G	FG-PBC-100G	FG-PBC-100G
	Perpetual BW License for CG-NAT (1 Tbps)[6]	FG-PBC-1000G	FG-PBC-1000G	FG-PBC-1000G	FG-PBC-1000G	FG-PBC-1000G
	Hyperscale Firewall License3	LIC-FG26F-HYPSC	LIC-FG42F-HYPSC	LIC-FG44F-HYPSC	LIC-FG48F-HYPSC	N/A

1. Firewall performance test uses 512 byte UDP.
2. IPsec VPN performance test uses AES256-CBC-SHA256. The use of the GCM algorithm instead of CBC can yield a performance improvement of 20% to 36% depending on the model.
3. The hyperscale license is only for the CG-NAT and Gi/N6-FW use case. FortiGate/FortiFirewall-VMs do not need it.
4. For GTP Firewall use case.
5. FortiFirewall only for SecGW and CG-NAT or Gi/N6-FW use cases. Requires the appropriate bandwidth licenses.
6. Stackable and network-wide bandwidth license. Use PBW for SecGW use case and PBC for CG-NAT use case.
7. For VM performance tests, IPsec VPN UDP Throughput-1360 (AES256GCM).

CORE OPERATIONS - SECURITY MANAGEMENT AND VISIBILITY

FortiManager provides automation-driven centralized management. FortiManager allows operators to manage all Fortinet 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 the Fortinet Security Fabric, FortiManager's automation-driven network operations capabilities provide a foundation for network security optimization.

FortiAnalyzer is a powerful log management, analytics and reporting platform, providing organizations with single-pane orchestration, automation, and response for simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack surface. FortiAnalyzer reads data from Fortinet products and is integrated with the Security Fabric.

The following shows offerings information for FortiManager and FortiAnalyzer for Telco:

	5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS
FortiManager				
Central Policy Management	✓	✓	✓	✓
Air-gapped Licensing and ZTP				✓
SD-WAN Management			Optional	Optional
Fabric Connectors	✓	✓	✓	Optional
Top Selling	FMG-VM	FMG-VM	FMG-VM	FMG-VM
	FMG-1000G	FMG-1000G	FMG-1000G	FMG-200G
FortiAnalyzer				
Reporting	✓	✓	✓	✓
Log Storage	✓	✓	✓	✓
SOC			✓	
SOAR			✓	
Real-time Monitoring	✓	✓	✓	✓
Top Selling	FAZ-VM	FAZ-VM	FAZ-VM	FAZ-VM
	FAZ-3000G	FAZ-3000G	FAZ-1000G	FAZ-300G
	FAZ-3700G		FAZ-3000G	FAZ-1000G

ORDER INFORMATION

SOLUTION BUNDLE		FMG-200G	FMG-1000G	FMG-VM
FortiManager	**Devices/VDOMs**	30	1000	10-100000
	Base Product	FMG-200G	FMG-1000G	
	Hardware Bundle	FMG-200G-BDL-447-DD	FMG-1000G-BDL-447-DD	
	Capacity Stack			FMG-VM-10-UG FMG-VM-100-UG FMG-VM-1000-UG FMG-VM-5000-UG
	Support	FC-10-M0302-247-02-DD	FC-10-FM1KG-247-02-DD	FC[1-6]-M3004-248-02-DD

SOLUTION BUNDLE		FAZ-1000F	FAZ-3000G	FAZ-3700G	FAZ-VM
FortiAnalyzer	**GB/day of Logs**	660 GB	3,000 GB	8,300 GB	Stackable*
	Base Product	FAZ-1000F	FAZ-3000G	FAZ-3700G	
	Hardware Bundle	FAZ-1000F-BDL-466-DD	FAZ-3000G-BDL-466-DD	FAZ-3700G-BDL-466-DD	
	Capacity Stack				FAZ-VM-GB1 FAZ-VM-GB5 FAZ-VM-GB25 FAZ-VM-GB100 FAZ-VM-GB500 FAZ-VM-GB2000
	Support	FC-10-L01KF-247-02-DD	FC-10-L03KG-247-02-DD	FC-10-L3K7G-247-02-DD	FC[1-6]-10-LV0VM-248-02-DD

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

CLOUD SECURITY - APPLICATION, CONTROL PLANE, AND API PROTECTION

FortiWeb provides web applications and API protection (WAPP) and help in maintaining compliance with regulations. Using machine learning to model each application, FortiWeb defends against known and unknown (zero day) vulnerabilities while significantly reducing false positives. Available in physical, virtual (VNF), and container (CNF) form factors, FortiWeb provides deployment flexibility at the network edge, core data centers, in the public cloud, and on customer premises. FortiWeb enables a secure migration to Telco interfaces based on REST and HTTP.

FortiRecon is a digital risk protection (DRP) service that allows customers to gain visibility of their digital attack surface, receive targeted threat intelligence, and reduce organizational risk. FortiRecon is sold as a service and only has an OPEX business model.

The following shows offerings information for FortiWeb and FortiRecon for Telco:

	5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS
Most Commonly Deployed As	API protection, exposure protection	API protection		API protection, IP reputation
FortiWeb				
Standard Subscription	✓	✓		
Advanced Subscription	Optional	Optional		Optional
Web Security Service	✓	✓		
IP Reputation Service	✓	✓		✓
Antimalware Service	✓	✓		Optional
FortiWeb Cloud Sandbox - Cloud Sandbox for FortiWeb	Optional	Optional		
FortiGuard Credential Stuffing Defense	Optional	Optional		Optional
Threat Analytics	Optional	Optional		Optional
Top Selling	FWB-VMC08	FWB-VMC08		FWB-VMC08
	FWB-VM16	FWB-VM16		FWB-VM16
	FWB-4000F	FWB-4000F		FWB-1000F
FortiRecon				
External Attack Surface Management (EASM)	✓		✓	Optional
Brand Protection (BP)	✓		✓	Optional
Adversary Centric Intelligence (ACI)	Optional		✓	Optional
Top Selling	EASM+BP		EASM+BP	EASM+BP
	EASM+BP+ACI		EASM+BP+ACI	EASM+BP+ACI

ORDER INFORMATION

SOLUTION BUNDLE		FWB-VMC08	FWB-VM16	FWB-1000F	FWB-3000F	FWB-4000F
FortiWeb	**HTTP Throughput**	3 Gbps	6 Gbps	2.5 Gbps	10 Gbps	70 Gbps
	Base Product	FWB-VMC08	FWB-VM16	FWB-1000F	FWB-3000F	FWB-4000F
	Standard Subscription	FC-10-VMC08-936-02-DD	FC-10-VVM16-936-02-DD	FWB-1000F-BDL-934-DD	FWB-3000F-BDL-934-DD	FWB-4000F-BDL-934-DD
	Advanced Subscription	FC-10-VMC08-581-02-DD	FC-10-VVM16-581-02-DD	FWB-1000F-BDL-580-DD	FWB-3000F-BDL-580-DD	FWB-4000F-BDL-580-DD
	IP Reputation Service	FC-10- VMC08-140-02-DD	FC-10-VVM16-140-02-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-VVM16-137-02-DD	FC-10-FV1KF-137-02-DD	FC-10-FW3KF-137-02-DD	FC-10-FW4KF-137-02-DD

SOLUTION BUNDLE		EASM+BP	EASM+BP+ACI
FortiRecon	**Number of Assets**	500-100,000	500-100,000
	Subscription	FC[2-7]-10-RNSVC-534-02-DD	FC[2-7]-10-RNSVC-535-02-DD

CLOUD SECURITY - CI/CD

FortiCNP, Fortinet's cloud-native protection product helps security teams prioritize risk management activities based on a broad set of security signals from their cloud environments. Beyond the built-in CSPM and data scanning capabilities, FortiCNP collects information from multiple cloud native security services that provide vulnerability scanning, permissions analysis, and threat detection as well as Fortinet cloud security products. Based on the information it collects, FortiCNP calculates an aggregate risk score for cloud resources, so customers can then manage risk management work based on resource risk insights (RRI) FortiCNP produces. Integrated with cloud native security services and other Fortinet Security Fabric products, FortiCNP provides deep security visibility across cloud infrastructures and helps prioritize security workflows for effective risk management.

FortiDevSec is Fortinet's new DevSecOps product. FortiDevSec offers a Cloud/SaaS-based continuous application security testing focused on software development and DevOps. FortiDevSec enables the shift-left architecture by integrating security visibility and control in the early stages of the development lifecycle, allowing developers to find and fix issues quickly before the application goes to production.

FortiDevSec integrates and sits natively in the application's DevOps CI/CD pipeline. It offers comprehensive application scanning, including scanning source code, third-party libraries, secrets, and live web application URLs. It then aggregates the security issues and presents them in an easy-to-use web portal. Intelligent noise reduction enables developers to prioritize working on the most critical vulnerabilities without overwhelming them.

The following shows offerings information for FortiCNP and FortiDevSec for Telco:

	5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS
FortiCNP				
Cloud Native Protection		✓		
Data Protection		Optional		
Container Protection		✓		
Top Selling		CONTAINER GUARDIAN PROTECTION		
		CLOUD NATIVE PROTECTION		
		DATA PROTECTION		
FortiDevSec				
Scanning Source Code (SAST), Libraries (SCA), and Secrets		✓		
Scanning Web Applications (DAST)		✓		
Easy integration with CI/CDs		✓		
Aggregated dashboard		✓		
Top Selling		FortiDevSec VM version		
		FortiDevSec SAAS version		

ORDER INFORMATION

SOLUTION BUNDLE		CONTAINER PROTECTION	CLOUD NATIVE PROTECTION	DATA PROTECTION
FortiCNP	**Capacity**	Four container hosts/work nodes, stackable	20-100 resources, stackable	100GB-1TB, stackable
	Base Subscription	FC1-10-FCWPC-327-02-DD	FC[1,2]-10-FCWPW-315-02-DD	FC[2,5]-10-FCWPS-316-02-DD
SOLUTION BUNDLE		**FORTIDEVSEC VM VERSION**	**FORTIDEVSEC SAAS VERSION**	
FortiDevSec	**Base Subscription**	FC1-10-DSCVM-594-02-12	FC1-10-DEVSC-513-01-DD	

SECURITY OPERATIONS - VISIBILITY AND AUTOMATION

FortiSIEM provides unified event correlation and risk management for multivendor Telco networks. Fortinet has developed an architecture that enables unified data collection and analytics from diverse information sources including logs, performance metrics, SNMP Traps, security alerts, and configuration changes. FortiSIEM brings that data together for a comprehensive view of business security and availability. Every piece of information is converted into an event which is first parsed and then fed into an event-based analytics engine for monitoring real-time searches, rules, dashboards, and adhoc queries. In Telco, event correlation can also be used to detect and prevent fraud.

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 and by managing the threat intelligence from FortiGuard Labs or other 20+ threat intelligence providers. This results in faster response, streamlined containment, and reduced mitigation times: from hours to seconds. In private network deployments, the service provider and customers can use a lightweight FortiSOAR agent to leverage the customer's on-premise integration, connected to a master FortiSOAR in the service provider's SOC. The following shows offerings information for FortiSIEM and FortiSOAR for Telco:

	5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS
FortiSIEM				
Device Monitoring and Analytics	✓	✓	✓	Optional
Performance and Digital Experience Monitoring	✓	✓	✓	Optional
Agent-based Monitoring*	✓	✓	✓	Optional
Insider Threat Monitoring	✓	✓	✓	
Threat Intelligence	Optional	Optional	✓	Optional
EPS	Optional	Optional	Optional	Optional
Top Selling	FSM-VM	FSM-VM	FSM-VM	FSM-VM
	FSM-2000G (supervisor or worker)	FSM-2000G (supervisor or worker)	FSM-3500G (supervisor or worker)	FSM-500G (collector)
				FSM-2000G (supervisor or worker)
FortiSOAR				
SOAR			✓	Optional (through free agent linked to central NOC/SOC)
Top Selling	Enterprise Edition			
	Multi Tenant Edition			
	Dedicated Tenant Node			
	Regional SOC Instance			

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

SECURITY OPERATIONS - VISIBILITY AND AUTOMATION

ORDER INFORMATION

SOLUTION BUNDLE		FSM-500G (COLLECTOR)	FSM-2000G	FSM-3500G	FSM-VM
FortiSIEM	**Performance Benchmark**	Up to 5000 EPS	Up to 15K EPS with Collectors[1]	Up to 40K EPS with Collectors[1]	
	Hardware Product	FSM-500G	FSM-2000G	FSM-3500G	
	Base Product		FSM-AIO-2000-BASE	FSM-AIO-3500-BASE	FSM-AIO-BASE
	Base Performance	5000 EPS[2]	100 devices and 1000 EPS[2]	500 devices and 5000 EPS[2]	50 devices and 500 EPS[2]
	All-in-one Expansions: Add XX devices and 10 EPS/device		FSM-AIO-XX-UG[3]	FSM-AIO-XX-UG[3]	FSM-AIO-XX-UG[3]
	Endpoint Expansions: Add XX endpoints and two EPS/endpoint		FSM-EPD-XX-UG[3]	FSM-EPD-XX-UG[3]	FSM-EPD-XX-UG[3]
	Agents (logs and FIM)		FSM-AGT-ADV-50-UG[5]	FSM-AGT-ADV-50-UG[5]	FSM-AGT-ADV-50-UG[5]
	UEBA Agent Telemetry		FSM-UEBA-XX-UG[6]	FSM-UEBA-XX-UG[6]	FSM-UEBA-XX-UG[6]
	Additional EPS		FSM-EPS-100-UG	FSM-EPS-100-UG	FSM-EPS-100-UG
	Support[4]	FC-10-FSM5G-247-02-DD	FC-10-FSM2G-247-02-DD	FC-10-FSM3G-247-02-DD	FC[1-K]-10-FSM99-248-02-DD

1. Requires device or EPS (events per second) licenses, which must be purchased separately, to reach this level.
2. Starting license limit.
3. Replace XX with the number of devices (100, 250, 450, 950, 1950, 2000, 3500, 3950).
4. Check the FortiSIEM Ordering Guide for definitions.
5. Replace XX with the number of devices (50, 100, 200, 500, 1000).
6. Replace XX with the number of devices (25, 500, 10000).

SOLUTION BUNDLE		ENTERPRISE EDITION	MULTI TENANT EDITION	DEDICATED	REGIONAL SOC
FortiSOAR	**Base Capacity**	2 User Login	Regional	1 User Login	2 User Logins
	Base Product	LIC-FSRENT-2	LIC-FSRMTT-2	LIC-FSRMTD-1	LIC-FSRMTR-2
	Expansions	LIC-FSRAUL-1	LIC-FSRAUL-1	LIC-FSRAUL-1	LIC-FSRAUL-1
	Support	FC1-10-SRVMP-248-02-DD	FC2-10-SRVMP-248-02-DD	FC3-10-SRVMP-248-02-DD	FC4-10-SRVMP-248-02-DD

SECURITY OPERATIONS - SANDBOX AND EPP-EDR

FortiSandbox provides top-rated AI-powered breach protection that integrates with the Security Fabric to address 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.

FortiEDR delivers real-time automated endpoint protection and behavior-based threat hunting repository with orchestrated incident response across any device, including data center and edge servers, as well as manufacturing and OT systems. FortiEDR is a single integrated platform with flexible deployment options and a predictable operating cost.

The following shows offerings information for FortiSandbox and FortiEDR for Telco:

	5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS
FortiSandbox				
AI-based Static Behavior Analysis			✓	
Antievasion Detection			✓	
C&C Detection			✓	
AV, IPS, Web Filtering			✓	
Top Selling			FSA-500G	
			FSA-3000F	
			FSA-VM-00	
FortiEDR				
Discover - IT Hygiene		✓	✓	
Endpoint Protection		✓	✓	
Endpoint Detection and Response		✓	✓	
Advanced Endpoint Detection and Response		✓	✓	
Top Selling		FortiEDR-500	FortiEDR-500	
		FortiEDR-2000	FortiEDR-2000	

ORDER INFORMATION

SOLUTION BUNDLE		FSA-500G	FSA-3000F	FSA-VM00
FortiSandbox	**Real-world Effective Throughput Upper Limit (Files/Hour)[1]**	1000	6720	Hardware dependent 100-1000
	Base Product	FSA-500G	FSA-3000F	FSA-VM00
	Expansions (Windows)	FSA-500G-UPG-WIN-LIC-4	FSA-3000F-UPG-WIN-LIC-32	FSA-VM-WIN10-1
	Expansions (Custom VM)	FSA-500G-UPG-LIC-BYOL	FSA-3000F-UPG-LIC-BYOL	FSA-VM00-UPG-LIC-BYOL
	Sandbox Threat Intelligence	FC-10-FS5HG-499-02-DD	FC-10-SA3KF-499-02-DD	FC-10-FSV00-500-02-DD
SOLUTION BUNDLE		**FORTIEDR-500**	**FORTIEDR-2000**	
FortiEDR	**Capacity[2]**	500-pack	2,000-pack	
	Discover, Protect & Respond	FC2-10-FEDR1-348-01-DD	FC3-10-FEDR1-348-01-DD	
	Discover, Protect, Respond and XDR	FC2-10-FEDR1-394-01-DD	FC3-10-FEDR1-394-01-DD	
	On Boarding Best Practices (by seat)	FC1-10-EDBPS-310-02-DD (up to 1K)	FC2-10-EDBPS-310-02-DD (up to 3K)	

1 Tested based on files with 80% documents and 20% executables. Includes both static and dynamic analysis with prefiltering enabled. Upper limit reached through expansions.
2 Minimum ordering quota of 500 seats, with 25/500/2,000/10,000 packs options.

SECURITY OPERATIONS - DECEPTION

FortiDeceptor is designed to deceive, expose, and eliminate external and internal threats early in the attack kill chain. Adding FortiDeceptor in a Telco network as part of a breach protection strategy helps evolve the operator's defenses by proactively automating the discovery and mitigation of attacks and attackers before any significant damage can occur. FortiDeceptor automatically lays out a layer of decoys and lures that reveals the presence of attackers on the operator's network.

The following shows offerings information for FortiDeceptor:

	5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS
FortiDeceptor				
Anti-Reconnaissance and Anti-Exploit (ARAE) Service	✓	✓	✓	✓
Telco Decoys	✓			
Linux Decoys	✓	✓	✓	✓
SCADA Decoys				✓
IoT Decoys	Optional			Optional
Custom Decoys	✓	✓	✓	✓
Top Selling	FDC-VM	FDC-VM	FDC-VM	FDC-VM
	FDC-1000G			

ORDER INFORMATION

SOLUTION BUNDLE		FDC-VM	FDC-1000G
FortiDeceptor	**Maximum Decoys**	480	480
	Maximum Decoy VM	20	20
	Maximum IP per Decoy	24	24
	Base Product		FDC-1000G
	24×7 FortiCare		FC-10-DC1KG-247-02-DD
	Add 1 VLAN Subscription (includes all FortiGuard Services)	FC1-10-DCVMS-496-02-DD (includes 24×7 FortiCare)	FDC-UPG-WIN10 FC1-10-DC1KG-495-02-DD
	Central Management License	FC-10-FDCCM-497-02-DD	FC-10-FDCCM-497-02-DD

FDC-1000G and FDC-VM allow deployment of any Decoy VMs from the inventory without limitation aside from the necessary Windows license. Each supports up to 20 Decoy VMs and is recommended for 128 VLANs.

IDENTITY ACCESS MANAGEMENT (IAM)

FortiAuthenticator builds on the foundations of Fortinet single sign-on, adding a greater range of user identification methods and greater scalability. FortiAuthenticator is the gatekeeper of network access authorization: identifying users, querying access permissions from third-party systems, and communicating this information to FortiGate devices for enforcement in identity-based policies. FortiAuthenticator delivers transparent identification via a wide range of methods.

FortiPAM protects privileged accounts against credential theft and privilege abuse by managing account credentials, controlling privileged user access, and monitoring privileged activity. Its aim is to protect against and to monitor the vast majority of damaging attacks, which rely on the exploitation of privileged credentials. Privileged Access is defined as access to an account with privileges beyond those of regular accounts, typically limited to IT Managers and System Administrators. Examples of privileged access include local administrative accounts, domain administrative accounts, Active Directory or domain service accounts, etc.

The following shows offerings information for FortiAuthenticator and FortiPAM:

	5G AND 4G USER AND CONTROL PLANES	TELCO CLOUD	NOC/SOC	PRIVATE NETWORKS
FortiAuthenticator				
PKI Certificate Management	✓	✓	✓	✓
TACACS+	✓			
SSO	Optional	✓	✓	✓
MFA		✓	✓	✓
Central User Management		✓	✓	✓
Portals	Optional	Optional	Optional	Optional
HA		✓	✓	✓
Top Selling	FAC-VM	FAC-VM	FAC-VM	FAC-VM
	FAC-800F	FAC-800F	FAC-800F	FAC-800F
	FAC-3000F	FAC-3000F	FAC-3000F	
FortiPAM				
Windows OS	✓	✓	✓	Optional
Linux OS	✓	✓	✓	Optional
macOS	✓	✓	✓	Optional
ZTNA	✓	✓	✓	Optional
Web SSH, Web-RDP, Web-VNC, Web-SFTP, Web-SMBA	✓	✓	✓	Optional
Proxy Mode Web Browsing	✓	✓	✓	Optional
Direct Mode Web Browsing	✓	✓	✓	Optional
Video Recording	✓	✓	✓	Optional
Instant Video Uploading	✓	✓	✓	Optional
Native Program Putty Key/ Password, mstsc, vncviewer, winscp Proxy Mode	✓	✓	✓	Optional
Native Program Putty Password, mstsc Direct Mode	✓	✓	✓	Optional
Top Selling	FortiPAM-VM			

ORDER INFORMATION

SOLUTION BUNDLE		FAC-VM	FAC-800F	FAC-3000F
FortiAuthenticator	**Local and Remote Users (Base/Upper Limit)**	100/10,000	8,000/18,000	40,000 / 240,000
	FortiTokens	200/20,000	16,000	80,000
	Base Product	FAC-VM-BASE	FAC-800F	FAC-3000F
	Expansions	FAC-VM-100-UG FAC-VM-1000-UG FAC-VM-10000-UG	FAC-HW-100UG FAC-HW-1000UG FAC-HW-10KUG	FAC-HW-100UG FAC-HW-1000UG FAC-HW-10KUG FAC-HW-100KUG
	Support	FC[1-7]-10-0ACVM-248-02-DD	FC-10-AC8HF-247-02-DD	FC-10-AC3KF-247-02-DD
SOLUTION BUNDLE		**FORTIPAM-VM**		
FortiPAM	**Subscription**	FC[1-6]-10-PAVUL-591-02-DD		

FREQUENTLY ASKED QUESTIONS

When should FortiFirewall be offered as an alternative to FortiGate?

FortiFirewall is used for Telco operators wanting to optimize their capital expenditure by delaying capacity licenses until they are needed. It allows operators to better allocate their capital expenditure by freeing it from initial phases of long-term projects. FortiFirewall allows Fortinet to reach the desired budget levels of the operators without overstretching the discounts and margin reductions.

With FortiFirewall, operators can buy the hardware they need for their three- or five-year traffic projection up front and delay the capacity licenses until the demand picks up at some point during the projected life time, when the demand for that capacity appears. Capacity licenses are network-wide, so they adapt to the actual traffic growth.

FortiFirewall is restricted to Telco user plane functionality that is projected to grow exponentially such as Security Gateway (SecGW), Carrier Grade NAT (CG-NAT), and NGFW for the user plane. For these use cases, FortiFirewall is functionally equivalent to FortiGate.

When is the Hyperscale license needed in FortiGate/FortiFirewall?

For the CG-NAT use case, when additional capacity is needed because all processing takes place in the security processing unit (SPU), such as in the NP7.

When is the FortiCarrier license needed in FortiGate?

For the GTP Firewall/PFCP Firewall/User-Plane Roaming Firewall use case.

CHEAT SHEET

THE SPACE

- Telco operators are subject to attacks because of their large cash flows and a failure affects millions of customers.
- Competition among Telco operators is very intense. Automation is key to lower OPEX.
- Telco operators must protect very large networks with different requirements per plane: user data, control, management, and cloud/orchestration.
- Telco operators deliver more and more critical used cases for critical industries and national critical infrastructure.
- Operators are moving workloads to cloud and slowly to containers and public cloud. Appliances still needed for large throughputs.

ORDERING GUIDE

Product Offerings: Paid in full up front or pay as you grow (PAYG) options

Paid in full up front: hardware appliances and VMs (FortiGate, FortiWeb, FortiManager appliance, FortiAnalyzer, FortiEDR) selected by throughput and paid up front for the full capacity of the appliance/VM

PAYG: two options available:

- **FortiFirewall (FFW)**: only for user plane use cases. Hardware platform is paid up front, but licensed capacity is PAYG, based on a network-wide perpetual bandwidth license.
- **FortiSIEM, FortiSoar, FortiDeceptor, FortiSandbox, FortiAuthenticator, FortiManager-VM:** preferably choose S-series though perpetual license is available.

CHEAT SHEET

MAJOR HIGHLIGHTS

- Fortinet has comprehensive security solution for Telco operators covering the different network areas.
- Market-leading TCO and scaling for user plane use cases thanks to our NP7. This is key to match exponential traffic growth.
- 5G is driving more RAN sharing and increasing the need for a Security GW.
- The move to cloud and containers is increasing the attack surface as the internals of the compute nodes are now open.
- In private networks, Fortinet has a single solution that can simultaneously secure the wired OT, Wi-Fi, and 5G access.
- Tools to detect zero-day attacks and lateral movements as they occur.

USE CASES

User and Control Plane (FortiGate, FortiAnalyzer, FortiFirewall, FortiWeb), where scalability is key:

- SecGW
- CG-NAT
- Roaming FW
- API protection

Telco cloud and containers:

- Protect the infrastructure (FortiGate, FortiWeb)
- Do not deploy vulnerable images (FortiCNP)
- Secure the traffic planes in real time (FortiGate, FortiEDR)

Private Mobile Networks (FortiGate, FortiAnalyzer, FortiSwitch, FortiAP): key to combine OT, Wi-Fi, and 4G/5G protection

Visibility, Control and New Threats (FortiSIEM, FortiSOAR, FortiDeceptor, FortiSandbox): understand the current situation and react fast to attacks

Areas of exploration for Telco (FortiGate):

- Edge Compute with or without hyperscalers
- O-RAN
- Neutral hosts

Visit www.fortinet.com for more details

TEL-OG-R9-20240124