



ORDERING GUIDE

Operational Technology (OT)

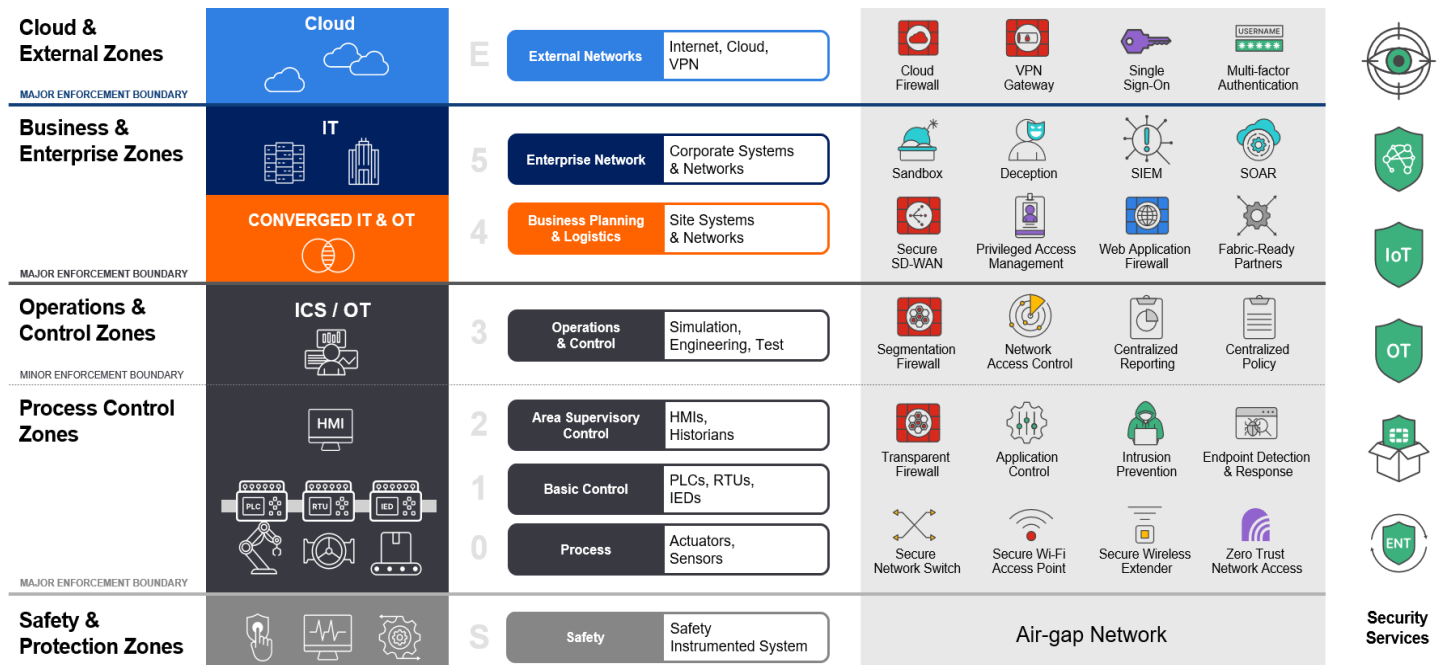
Fortinet secures operational technology (OT) with best-of-breed enterprise threat protection and offers a broad, integrated, and automated cybersecurity platform to securely drive IT/OT convergence – across the network perimeter, datacenter, and the cloud.

PRODUCT OFFERINGS

Fortinet offers a broad range of cybersecurity solutions that provide visibility, control, and actionable intelligence for ICS/OT and converged IT/OT environments while supporting compliance with several industry regulations, standards, and best practices.

Additionally, the Fortinet Security Fabric platform approach for IT/OT minimizes complexity, streamlines security operations, and reduces the operating expense (OpEx) for asset owners and operators compared to point security solutions in siloed IT and OT environments.

OT CYBERSECURITY SOLUTION MAPPING FOLLOWING PURDUE MODEL ARCHITECTURE



FORTINET SECURITY FABRIC FOR OT

The Fortinet Security Fabric for OT combines best-of-breed Fortinet products and solutions into a broad, integrated, and automated cybersecurity platform enabling organizations to achieve robust, simple, and cost-efficient cybersecurity across the IT/OT infrastructures.







The Fortinet Security Fabric improves operational efficiencies through consistent security policies, enables security automation, offers visibility across all the security infrastructure, and supports interoperability across a broad range of networking and security solutions.



USE CASES

Fortinet has a comprehensive portfolio of cybersecurity solutions for both IT and OT environments that includes purpose-built products and features for securing industrial automation and control systems, cyber-physical systems, and critical infrastructures. This ordering guide is a quick reference to the most deployed Fortinet Security Fabric solutions aligned with the cybersecurity use cases across IT and OT environments.

The following table lists the Fortinet Security Fabric solution offerings mapped to the cybersecurity use cases and applicable Purdue levels. The table is based on the industry-recommended best practices and cybersecurity requirements for IT and OT environments and can be used as a quick reference to navigate the ordering guide.

		Cloud & External Zones	Business & Enterprise Zones	IT/OT Boundary	Operations & Control Zones	Process Control Zones
 Secure Networking	Network Segmentation	✓	✓	✓	✓	✓
	Network Microsegmentation				✓	✓
	Secure SD-WAN / SD-Branch	✓	✓	✓	✓	
	Web Application Security		✓	✓	✓	
 Zero Trust Access	Network Access Control			✓	✓	
	Role Based Access Control	✓	✓	✓	✓	
	Secure Remote Access	✓	✓	✓	✓	✓
 Network Operations	Logging, Monitoring and Reporting		✓		✓	
	Network Operations Center	✓	✓		✓	
 Security Operations	Security Automation and Orchestration		✓		✓	
	Security Operations Center	✓	✓		✓	
 Threat Intel & Response	Endpoint Detection & Response	✓	✓	✓	✓	✓
	Advanced Threat Protection	✓	✓	✓	✓	✓
	OT Security Service			✓	✓	✓
	Attack Surface Security Rating Service	✓	✓	✓	✓	✓
 Specialized Industrial Solutions	Rugged Hardware Appliances			✓	✓	✓
	Virtual Machine Appliances	✓	✓	✓	✓	✓
	3G/4G/5G Wireless Appliances		✓	✓	✓	✓

USE CASES TO SOLUTION MAPPING

Each solution offering is based on a single or combination of multiple products from Fortinet and the solutions can be deployed as standalone or integrated with other products.

The following table lists the specific Fortinet products that builds the solution offering. The solutions map to the most commonly deployed products listed in the Recommended column to help customers with selecting the appropriate solution for their use cases.

	USE CASES	DESCRIPTION	SOLUTIONS	
			RECOMMENDED	OPTIONAL
Secure Networking	Network Segmentation	Logical and physical division of a network into multiple segments or zones, interconnected by a next generation firewall (NGFW) with single-pane-of-glass management for network and security operations.	FortiGate FortiSwitch FortiAP	FortiManager
	Network Microsegmentation	Logical and physical division of a network into multiple micro-segments or sub-zones, interconnected by an NGFW with single-pane-of-glass management for network and security operations.	FortiGate FortiSwitch	FortiManager
	Secure SD-WAN / SD-Branch	Security and SD-WAN bundled in a single WAN-edge device, powered by a unified operating system, FortiOS. Integrated with FortiSwitch and FortiAP, it can offer complete network and security solution for remote site or branch with single-pane-of-glass management for network and security operations.	FortiGate FortiManager	FortiExtender FortiSwitch FortiAP FortiSASE
	Web Application Security	Protect web applications and APIs from internal and external attacks that target applications using known vulnerabilities and zero-day threats.	FortiWeb	
Zero Trust Access	Network Access Control	Network access control solution that enhances the visibility, control, and automated response for everything that connects to the network.	FortiNAC	FortiGate FortiSwitch FortiAP
	Role Based Access Control	Enforce authorization for users based on their roles through centrally defined access control policy for accessing network resources.	FortiAuthenticator FortiToken	FortiGate FortiManager
	Secure Remote Access	Remote access VPN with multi-factor authentication, network traffic inspection, and advanced threat protection to secure the organizations and its remotely accessed digital assets.	FortiGate FortiAuthenticator FortiToken FortiPAM	FortiGuard Services
Network Operations	Logging, Monitoring, and Reporting	Keep up with the volume, sophistication, and speed of today's cyberthreats, using security operations that can function at machine speed, providing advanced threat detection and response capabilities, centralized security monitoring, and automation across the entire Fortinet Security Fabric.	FortiAnalyzer FortiManager FortiSIEM	FortiGuard Services
	Network Operations Center	Enable automation-driven centralized management of Fortinet solutions from a single console, supporting visibility and administration of network devices through unified dashboards, streamlined provisioning for software updates, and automation tools for troubleshooting network issues.	FortiManager	FortiAnalyzer
Security Operations	Security Automation and Orchestration	Security orchestration, automation and response (SOAR) providing management, automation, and orchestration across the entire security infrastructure to reduce the mean time to respond to security issues and incidents.	FortiSOAR	FortiAnalyzer FortiSIEM
	Security Operations Center	Enable unified data collection and analytics from diverse information sources including logs, performance metrics, SNMP, security alerts, and configuration changes.	FortiSIEM	FortiSOAR

USE CASES TO SOLUTION MAPPING

	USE CASES	DESCRIPTION	SOLUTIONS	
			RECOMMENDED	OPTIONAL
Threat Intel & Response	Endpoint Detection & Response	Identify and stop endpoint breaches automatically in real-time while reducing the overhead of false alarms and supporting the security teams with forensic analysis and investigation without disrupting business operations.	FortiEDR	FortiClient
	Advanced Threat Protection	Detect and stop zero-day threats and intrusions using a combination of proactive detection and mitigation tools with actionable threat insight and integrated deployment architecture.	FortiSandbox FortiDeceptor FortiGuard Services FortiRecon	FortiGate FortiINDR
	OT Security Service	Monitor, detect, and protect against network-level threats targeting OT environments, support virtual patching, and provide extensive visibility into OT applications and protocols.	FortiGate FortiGuard Services	FortiManager
	Attack Surface Security Service	Automatically discover and identify IoT devices, support asset visibility for enforcing appropriate security policies, including virtual patching. Furthermore, the Security Rating Service assists in establishing and maintaining an optimal security posture by detecting vulnerabilities and configuration issues through audit checks.	FortiGate FortiGuard Services	FortiManager
Specialized Industrial Solutions	Rugged Hardware Appliances	Industrially-hardened hardware appliances provide NGFW, NGIPS, and network connectivity capabilities for ICS and OT environments.	FortiGate FortiSwitch	FortiAP FortiExtender
	Virtual Machine Appliances	Fortinet Security Fabric solutions offered as virtual machine package.	FortiGate-VM	The majority of all Security Fabric products are available in VM format.
	3G/4G/5G Wireless Appliances	Hardware appliances providing wireless WAN connectivity or wireless extension using Wi-Fi and 3G/4G LTE/5G wireless technologies to connect remote locations.	FortiGate FortiExtender	FortiAP

PRODUCT OFFERINGS AND ORDERING INFORMATION

FortiGate is the flagship NGFW product family from Fortinet that delivers best-in-class security, high-speed networking, hardware-accelerated performance features for NGFW/NGIPS, and built-in market-leading SD-WAN. FortiGate comes in different form factors and sizes, including ruggedized appliances to withstand harsh environmental conditions and support industrial applications.

FortiGuard provides security services that keep FortiGate products up-to-date with the latest security updates and threat intelligence. FortiGuard security services are offered through subscription bundles and include several advanced threat protection services for enterprise networks, web, cloud, OT, and so on. The Industrial Security Service and IoT Detection Service are part of the FortiGuard subscription offering.

FORTIGATE	BASE PRODUCT	ENTERPRISE HARDWARE BUNDLE	ENTERPRISE RENEWAL BUNDLE	OT SECURITY SERVICE	ATTACK SURFACE SECURITY
FGR-60F	FGR-60F	FGR-60F-BDL-809-DD	FC-10-0069F-809-02-DD	FC-10-0069F-159-02-DD	FC-10-0069F-175-02-DD
FGR-60F-3G4G	FGR-60F-3G4G	FGR-60F-3G4G-BDL-809-DD	FC-10-F60FI-809-02-DD	FC-10-F60FI-159-02-DD	FC-10-F60FI-175-02-DD
FGR-70F	FGR-70F	FGR-70F-BDL-809-DD	FC-10-F70FB-809-02-DD	FC-10-F70FB-159-02-DD	FC-10-F70FB-175-02-DD
FGR-70F-3G4G	FGR-70F-3G4G	FGR-70F-3G4G-BDL-809-DD	FC-10-F70FM-809-02-DD	FC-10-F70FM-159-02-DD	FC-10-F70FM-175-02-DD
FG-40F-3G4G	FG-40F-3G4G	FG-40F-BDL-809-DD	FC-10-0040F-809-02-DD	FC-10-F40FG-159-02-DD	
FG-100F	FG-100F	FG-100F-BDL-809-DD	FC-10-F100F-809-02-DD	FC-10-F100F-159-02-DD	FC-10-F100F-175-02-DD
FG-200F	FG-200F	FG-200F-BDL-809-DD	FG-200F-BDL-809-DD	FC-10-F200F-159-02-DD	FC-10-F200F-175-02-DD
FG-1000F	FG-1000F	FG-1000F-BDL-809-DD	FG-1000F-BDL-809-DD	FC-10-F1K0F-159-02-DD	FC-10-F1K0F-175-02-DD
FG-1800F	FG-1800F	FG-1800F-BDL-809-DD	FC-10-F18HF-809-02-DD	FC-10-F18HF-159-02-DD	FC-10-F18HF-175-02-DD
FG-VM	FG-VM08		FC-10-FVM08-812-02-DD	FC-10-FVM08-159-02-DD	FC-10-FVM08-175-02-DD

FortiSwitch is a secure access switch family that delivers outstanding performance, scalability, and manageability. FortiSwitch allows OT customers to extend networking and security across their network infrastructure. FortiSwitch seamlessly integrates with the Security Fabric via FortiLink. FortiCloud or FortiGate can manage FortiSwitch. The unified management of FortiSwitch via FortiGate offers complete visibility and control of users and devices in the network.

FORTISWITCH	BASE PRODUCT	SUPPORT
FSR-112D-POE	FSR-112D-POE	FC-10-W112D-247-02-DD
FS-448E-FPOE	FS-448E-FPOE	FC-10-S448F-247-02-DD
FS-548D-FPOE	FS-548D-FPOE	FC-10-W0501-247-02-DD
FS-1048E	FS-1048E	FC-10-1E48F-247-02-DD
FSR-424F-POE	FSR-424F-POE	FC-10-R24FP-247-02-DD

FortiAP is a series of Wi-Fi access points that FortiCloud or FortiGate can manage. FortiAPs offer high throughput, optimal coverage, and enterprise class 802.11ax services. FortiAPs can seamlessly integrate with the Security Fabric and enable security and access control policy enforcement for end users as devices try to access the network.

FORTIAP	BASE PRODUCT	SUPPORT
FAP-221E	FAP-221E-X *	FC-10-PE221-247-02-DD
FAP-234F	FAP-234F-X *	FC-10-P234F-247-02-DD
FAP-431F	FAP-431F-X *	FC-10-F431F-247-02-DD
FAP-433F	FAP-433F-X *	FC-10-F433F-247-02-DD
FAP-432FR	FAP-432FR-X *	FC-10-F432FR-247-02-DD

* Replace X with the country code.

PRODUCT OFFERINGS AND ORDERING INFORMATION

FortiExtender provides a bridge between local Ethernet LANs and wireless LTE/5G WAN connections. FortiExtender can support diverse wireless applications with a high level of backhaul redundancy using a single LTE/5G modem platform over redundant SIM cards attaching to different mobile networks. You can use FortiExtender as the LTE/5G backhaul of an on-premise FortiGate with maximum wireless LTE/5G signal strength. FortiGate can centrally manage FortiExtender.

FORTIEXTENDER	BASE PRODUCT	SUPPORT
FEX-212F	FEX-212F	FC-10-X212F-247-02-DD
FEX-311F	FEX-311F	FC-10-X311F-247-02-DD
FEX-511F	FEX-511F	FC-10-X511F-247-02-DD
FEV-211F-AM*	FEV-211F-AM	FC-10-FV21F-247-02-DD

* AM variant is for USA. Global variant is coming soon.

FortiAnalyzer offers a centralized log management, analytics, and reporting platform, providing customers with single-pane orchestration, automation, and response for simplified security operations, proactive identification, risk remediation, and complete visibility of the entire attack surface. FortiAnalyzer can collect different types of logs and events from Fortinet products via Security Fabric integration.

FORTIANALYZER	BASE PRODUCT	HW/VM BUNDLE	OT SECURITY SERVICE	SUPPORT
FAZ-300G	FAZ-300G	FAZ-300G-BDL-466-DD	FC-10-L03HG-159-02-DD	FC-10-L03HG-466-02-DD
FAZ-1000F	FAZ-1000F	FAZ-1000F-BDL-466-DD	FC-10-L01KF-159-02-DD	FC-10-L01KF-466-02-DD
FAZ-3000G	FAZ-3000G	FAZ-3000G-BDL-466-DD	FC-10-L03KG-159-02-DD	FC-10-L03KG-466-02-DD
FAZ-VM	-	FC1-10-AZVMS-465-01-DD	FC1-10-LV0VM-159-02-DD	-

FortiManager provides automation-driven centralized management. FortiManager allows end users to centrally manage FortiGate, FortiSwitch, and FortiAP devices in their network with a single-console centralized management platform.

FORTIMANAGER	BASE PRODUCT	VM SUBSCRIPTION LICENSE WITH SUPPORT	HW SUPPORT
FMG-400G	FMG-400G	-	FC-10-M400F-247-02-DD
FMG-1000F	FMG-1000F	-	FC-10-FM1KF-247-02-DD
FMG-VM	-	FC2-10-FMGVS-258-01-DD	-

FortiSIEM provides unified event correlation and risk management for multivendor implementations. It enables analytics from diverse information sources including logs, performance metrics, SNMP traps, security alerts, and configuration changes. It feeds all the information into an event-based analytics engine and supports real-time searches, rules, dashboards, and ad hoc queries.

FORTISIEM	BASE PRODUCT	SUPPORT
FSM-2000G	FSM-2000G	FC-10-FSM2G-247-02-DD
	FSM-AIO-2000-BASE	FC[2-Y]-10-FSM99-240-02-DD
FSM-AIO-BASE	FSM-AIO-BASE	FC[1-Y]-10-FSM97-248-02-DD
FSM-AIO-UG	FSM-AIO-XX-UG *	Included with FC[1-Y]-10-FSM97-248-02-DD and FC[2-Y]-10-FSM99-240-02-DD
FSM-EPD-UPG	FSM-EPD-XX-UG *	-

* Replace XX with the number of devices.

FortiSOAR offers 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 resource shortages. Its 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 reduces mitigation times from hours to seconds.

FORTISOAR	BASE PRODUCT	+1 ANALYST ADD-ON
Enterprise Edition	FC-10-SRVMS-389-02-DD	FC-10-SRVMS-384-02-DD
Multi Tenant Edition	FC-10-SRVMS-390-02-DD	FC-10-SRVMS-384-02-DD

PRODUCT OFFERINGS AND ORDERING INFORMATION

FortiSandbox provides a top-rated AI-powered breach protection that integrates with the Security Fabric platform to address the rapidly evolving and targeted threats, including ransomware, cryptomalware, and others across a broad digital attack surface. Specifically for OT, it delivers real-time actionable intelligence through automating zero-day advanced malware detection and response for detecting threats targeting OT systems and protocols.

FORTISANDBOX	BASE PRODUCT	UPGRADE	THREAT INTELLIGENCE AND SUPPORT
FSA-500F	FSA-500F	FSA-500F-UPG-LIC-BYOL	FC-10-FS5HF-499-02-DD
FSA-3000F	FSA-3000F	FSA-3000F-UPG-LIC-32	FC-10-SA3KF-499-02-DD

FortiDeceptor offers honeypot and deception technology to deceive, expose, and eliminate external and internal threats early in the attack kill chain and it proactively blocks these threats before any significant damage occurs. It automates blocking of the attackers targeting IT and OT systems and devices by laying out a layer of decoys and lures that helps with redirecting attackers focus while revealing their presence on the network.

FORTIDECEPTOR	BASE PRODUCT	SUPPORT	ADD 1 VLAN SUBSCRIPTION *	CENTRAL MANAGEMENT	WINDOWS DECOYS
FDR-100G	FDR-100G	FC-10-DR1HG-247-02-DD	FC1-10-DR1HG-495-02-DD	FC1-10-FDCCM-497-02-DD	LIC-FDC-WIN
FDC-1000G	FDC-1000G	FC-10-DC1KG-247-02-DD	FC1-10-DC1KG-495-02-DD	FC1-10-FDCCM-497-02-DD	LIC-FDC-WIN
FDC-VMS	Subscription	Included with subscription	FC1-10-DCVMS-496-02-DD	FC1-10-FDCCM-497-02-DD	LIC-FDC-WIN

* Minimum order of two VLANs.

FortiEDR delivers real-time automated endpoint protection with orchestrated incident response across IT and OT endpoints. All in a single integrated platform, with flexible deployment options, and a predictable operating cost, FortiEDR provides real-time proactive risk mitigation, endpoint security, preinfection protection via a kernel-level Next Generation AntiVirus (NGAV) engine, postinfection protection, and forensics.

FORTIEDR	FORTIEDR DISCOVER, PROTECT & RESPOND	BEST PRACTICES SERVICE FIRST-TIME DEPLOYMENT
25 endpoints *	FC1-10-FEDR1-348-01-DD *	FC1-10-EDBPS-310-02-DD
500 endpoints	FC2-10-FEDR1-348-01-DD	FC1-10-EDBPS-310-02-DD
2000 endpoints	FC3-10-FEDR1-348-01-DD	FC2-10-EDBPS-310-02-DD

* Add-on option. Minimum Order Quantity (MOQ) 500 seats.

FortiClient includes the ZTNA, SASE, and EPP capabilities:

- **ZTNA** enables remote users to access their corporate applications while ensuring strict authentication and verifiable endpoint security posture before any access is granted.
- **SASE** ensures remote users can securely connect to the corporate following the same corporate security policies regardless of their location. SASE integrates seamlessly with ZTNA to deliver a transparent user experience while offering security protection for all endpoints from advanced threats.
- **EPP** offers vulnerability detection and protection, auto-patching Antivirus, application firewall, anti-ransomware, and endpoint management.

FORTICLIENT	25-PACK (ADD-ON)	500-PACK (ADD-ON)	2000-PACK (ADD-ON)
On-premise EPP/APT	FC1-10-EMS04-429-01-DD	FC2-10-EMS04-429-01-DD	FC3-10-EMS04-429-01-DD
Cloud EPP/APT	FC1-10-EMS05-429-01-DD	FC2-10-EMS05-429-01-DD	FC3-10-EMS05-429-01-DD
Managed	FC1-10-EMS05-485-01-DD	FC2-10-EMS05-485-01-DD	FC3-10-EMS05-485-01-DD

PRODUCT OFFERINGS AND ORDERING INFORMATION

FortiNAC offers network access control that enhances the Security Fabric with visibility, control, and automated response for everything that connects to the network. FortiNAC provides protection against malicious access, extends access control to 3rd party devices, offers greater visibility for devices, supports dynamic network access control, and orchestrates automatic responses to a wide range of networking events.

FORTINAC	BASE PRODUCT	SUPPORT	PLUS LICENSE PERPETUAL 1000 ENDPOINTS	PLUS LICENSE SUBSCRIPTION 500 ENDPOINTS
FNC-CA-VM	FNC-CA-VM	FC-10-NCVCA-248-02-DD	LIC-FNAC-PLUS-1K	FC2-10-FNAC1-213-01-DD
FNC-CA-700C	FNC-CA-700C	FC-10-NC700-247-02-DD	LIC-FNAC-PLUS-1K	FC2-10-FNAC1-213-01-DD

FortiAuthenticator offers single sign-on and user authorization into the Fortinet secured enterprise network identifying users, querying access permissions from 3rd party systems, and communicating the access requests to FortiGate to implement identity-based security policies. FortiAuthenticator supports wide array of methods and tools for authentication and authorization, such as Active Directory, RADIUS, LDAP, SAML SP/IdP, PKI, and multi-factor authentication.

FORTIAUTHENTICATOR	BASE PRODUCT	SUPPORT
FAC-300F	FAC-300F	FC-10-AC3HF-247-02-DD
FAC-800F	FAC-800F	FC-10-AC8HF-247-02-DD
FAC-VM	FAC-VM-BASE	FC1-10-0ACVM-248-02-DD

FortiToken enables two-factor authentication with One-Time Password (OTP) Application with Push Notifications or a Hardware Time-Based OTP Token. FortiToken Mobile (FTM) and hardware OTP Tokens are fully integrated with FortiClient, secured by FortiGuard, and leverage direct management and use within the FortiGate and FortiAuthenticator security solutions. FortiGate, FortiToken, and FortiAuthenticator integrated solution is easy to implement, use, and manage for multi-factor authentication use case.

FORTITOKEN	BASE PRODUCT
FTM-ELIC	FTM-ELIC-XX *
FTK-200B	FTK-200B-XX *

* Replace XX with the number of tokens.

FortiPAM enables privileged access and session management, controlling privileged user access, and monitoring activity on privileged accounts. FortiPAM provides tightly controlled privileged access to the most sensitive resources within an organization. It enables end-to-end management of privileged accounts, control of privileged user access, and visibility of account usage including monitoring and audit capabilities.

FORTIPAM	SUBSCRIPTION
FortiPAM-VM - 5 to 9 users	FC1-10-PAVUL-591-02-DD
FortiPAM-VM - 50 to 99 users	FC4-10-PAVUL-591-02-DD

FortiRecon scans the organization's attack surface and identifies risks to assets. FortiGuard Threat intelligence delivers early warning of risks to the organization through targeted, curated intelligence. It provides visibility into the diverse threats to the organization and brand reputation, allowing customers to respond more quickly to incidents, better understand attackers, and safeguard assets while expanding view and early warning of adversarial activity from Dark Web and other sources.

FORTIRECON	500 ASSETS	1000 ASSETS	50000 ASSETS
FortiRecon EASM	FC2-10-RNSVC-533-02-DD	FC3-10-RNSVC-533-02-DD	FC6-10-RNSVC-533-02-DD
FortiRecon EASM+BP+ACI	FC2-10-RNSVC-535-02-DD	FC3-10-RNSVC-535-02-DD	FC6-10-RNSVC-535-02-DD

PRODUCT OFFERINGS AND ORDERING INFORMATION

FortiSASE integrates networking and security for secure access and connectivity anywhere. It ensures enterprise-grade security and user experience across physical and virtual networks, addressing the limitations of many cloud-delivered solutions for hybrid IT/OT environments. FortiSASE extends FortiGuard services to remote users, edge computing environments, and cloud deployments delivering consistent security posture.

FORTISASE	SUBSCRIPTION
FortiSASE User Subscription - 50 to 499 Users	FC2-10-EMS05-547-02-DD
FortiSASE User Subscription - 500 to 1999 Users	FC3-10-EMS05-547-02-DD

FortiWeb offers security protection for business-critical web applications and APIs from attacks that target known and unknown vulnerabilities. Using an advanced multilayered approach backed by a sophisticated machine learning engine, FortiWeb protects against the OWASP Top 10 and more. The FortiWeb product line offers solutions and deployment options across SaaS, VMs, and hardware appliances.

FORTIWEB	BASE PRODUCT	ADVANCED HARDWARE BUNDLE	ADVANCED BUNDLE RENEWAL
FWB-1000F	FWB-1000F	FWB-1000F-BDL-580-DD	FC-10-FV1KF-580-02-DD
FWB-4000F	FWB-4000F	FWB-4000F-BDL-580-DD	FC-10-FW4KF-580-02-DD
FWB-VM08	FWB-VM08	-	FC-10-VVM08-581-02-DD

FortiNDR offers next-generation AI-driven breach protection technology to defend against various cyberthreats, including advanced persistent threats through a trained Virtual Security Analyst™. The virtual analyst helps with identifying, classifying, and responding to threats including those well-camouflaged. Employing – patent-pending – Deep Neural Networks based on Advanced AI and Artificial Neural Network, it provides sub-second security investigation by harnessing deep learning technologies that assist in an automated response to remediate different types of attacks.

FORTINDR	BASE PRODUCT	APPLIANCE BUNDLE WITH NDR AND ANN	SUPPORT WITH NDR AND ANN	NETFLOW AND OT SECURITY
FNR-3500F	FNR-3500F	FNR-3500F-BDL-331-DD	FC-10-AI3K5-331-02-DD	FC-10-AI3K5-588-02-DD - Netflow FC-10-AI3K5-723-02-DD - OT Security
FortiNDR-VM	-	FC3-10-AIVMS-461-02-DD	-	FC3-10-AIVMS-588-02-DD - Netflow FC3-10-AIVMS-723-02-DD - OT Security

ADDITIONAL INFORMATION AND RESOURCES

PRODUCT	DATASHEET
FortiGate	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf
FortiGate Rugged	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_Rugged_Series.pdf
FortiGate VM	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-vm.pdf
FortiSwitch	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSwitch_Secure_Access_Series.pdf
FortiAP	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-series.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
FortiAnalyzer	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf
FortiManager	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.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
FortiDeceptor	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiDeceptor.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
FortiNAC	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf
FortiAuthenticator	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAuthenticator.pdf
FortiToken	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortitoken.pdf
FortiPAM	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortipam.pdf
FortiRecon	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortirecon.pdf
FortiSASE	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisase.pdf
FortiWeb	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiWeb.pdf
FortiNDR	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortindr.pdf

FREQUENTLY ASKED QUESTIONS

Can FortiGuard OT Security Service be purchased without the Enterprise Protection subscription?

Yes. FortiGuard OT Security Service is not offered as part of the Enterprise Protection bundle and only as à la carte. However, it is recommended to acquire it with Enterprise Protection or Advanced Threat Protection subscription as this approach enables leveraging the full spectrum of threat protection capabilities and accessing other FortiGuard services when using FortiGate hardware or VM appliance.

Where can I find the information about latest Application Control and IPS signatures available in the FortiGuard OT Security Service? Where can I find the information about Attack Surface Security Service coverage?

The up-to-date information and latest release of Application Control and IPS signatures for FortiGuard OT Security Service can be found on the [FortiGuard website](#). The information about Attack Surface Security Service is available on the [FortiGuard website](#).

If the license on FortiGate hardware or VM appliance has expired, can the IPS signature database get signature updates?

No. Once the license on FortiGate hardware or VM appliance has expired, the appliance will not get any future updates for the IPS signatures from the date of license expiry until the license is renewed. However, the IPS signatures existing in the appliance's database will still function while the license has expired although the database will not be up to date.

Does FortiGate rugged hardware appliances come with a power supply unit?

No. The FortiGate rugged hardware appliances are equipped with power input connectors only and the customers would be required to purchase a suitable external power supply unit from 3rd party suppliers to power the appliances.

What license or subscription is required for running the OT decoys and lures in FortiDeceptor?

The "Deceptor Bundle Contract" subscription for FortiDeceptor includes the OT decoys and lures.

Why are some products listed as "Optional" in the use case to solution mapping in the Ordering Guide?

The "Optional" products can be integrated with the "Recommended" products and offer added value for the use case implementation. In addition, the customers can benefit additional features and functionalities offered in the "Optional" products such as, centralized management, monitoring, logging, etc. and extend the solution capabilities beyond "Recommended" products in their projects.

Why does the Ordering Guide only list limited SKUs for each Fortinet product line?

The SKUs that are listed in the Ordering Guide are representing the most deployed products for the use case implementations from our current customer base. However, additional information on the other SKUs can be obtained from the [Fortinet website](#).

Are all Fortinet products available in rugged hardware appliance form?

No. Currently, only the select Fortinet products are offered in the rugged hardware appliance form, such as FortiGate Rugged, FortiSwitch Rugged, and FortiDeceptor Rugged. Additionally, the customers have option to use a 3rd party Fortinet certified Industrial PC (IPC) hardware to host VM appliance of Fortinet products.

Where can I find more information about product installation and configuration?

The product installation manuals, user guides, and quick start guides are available on the [Fortinet website](#).

Where can I find more information about product certifications?

The information on product certifications is available on the [Fortinet website](#).

FORTINET TRAINING AND CERTIFICATION

FCSS – OT Security Training and Certification

Learn how to secure your OT infrastructure using Fortinet solutions; and design, deploy, administrate, and monitor FortiGate, FortiNAC, FortiAnalyzer, and FortiSIEM devices to secure OT infrastructures. These skills provide you with a solid understanding of how to design, implement, and operate an OT security solution based on Fortinet products.

Course description

For information about prerequisites, agenda topics, and learning objectives, see the course description at https://training.fortinet.com/local/staticpage/view.php?page=library_ot-security

Visit www.fortinet.com for more details

Ordering Information

SKU	DESCRIPTION
FT-OTS	Instructor-led training - 3 full days or 4 half days
FT-OTS-LAB	Self-paced on-demand labs
NSE-EX-FTE4	Certification exam

