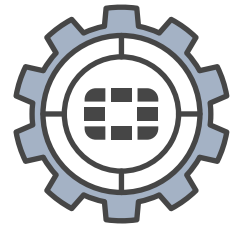# Operational Technology (OT)

Industry's Most Advanced and Integrated OT Security Platform

The Fortinet OT Security Platform delivers a comprehensive suite of integrated security solutions specifically engineered for operational technology (OT) environments.

It encompasses secure networking, security service edge (SSE), security operations, dedicated threat intelligence, and a robust technology alliance ecosystem. The platform's seamless integration enables vendor consolidation, centralized visibility and control, and seamless IT/OT convergence—driving operational efficiency, strengthening cyber resilience, and lowering total cost of ownership.

Product Offerings

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

The Security Platform approach for IT/OT minimizes complexity, streamlines security operations, and reduces operational expenses (OpEx) for asset owners and operators—offering a more efficient alternative to siloed point security solutions in separate IT and OT environments.
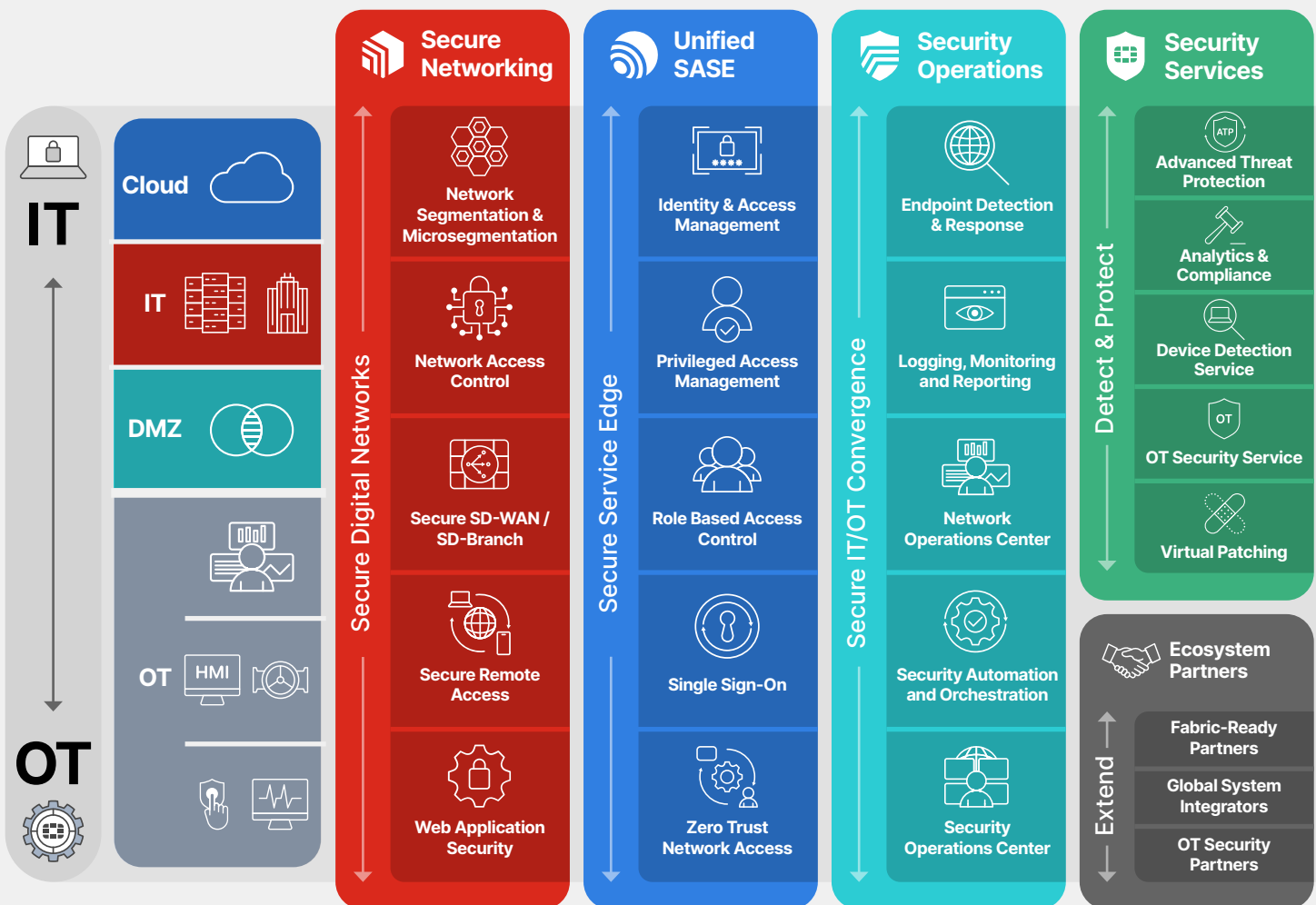
The Fortinet OT Security Platform
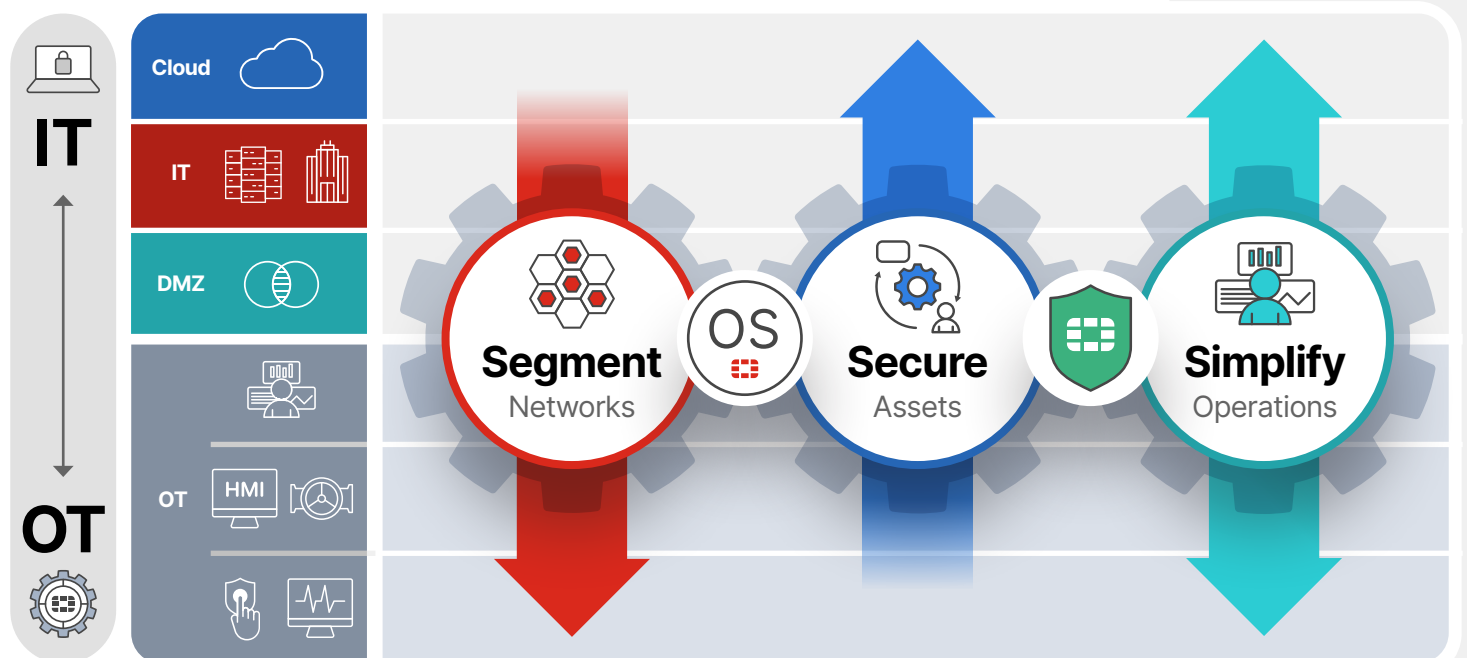
Fortinet OT Security Platform Solutions and Use Cases

The Fortinet OT Security Platform supports a wide range of use cases for securing industrial automation and control systems, cyber-physical systems, and critical infrastructure sectors. This ordering guide provides a quick reference to the most widely deployed OT Security Platform solutions aligned with key cybersecurity use cases across both IT and OT environments.

The following sections present the OT Security Platform solutions mapped to these use cases, based on industry best practices and cybersecurity requirements—serving as a practical reference for navigating the guide.

IT

OT

Cloud

IT

DMZ

OT

Secure Networking
Secure Digital Networks
- Network Segmentation & Microsegmentation
- Network Access Control
- Secure SD-WAN / SD-Branch
- Secure Remote Access
- Web Application Security

Unified SASE
Secure Service Edge
- Identity & Access Management
- Privileged Access Management
- Role Based Access Control
- Single Sign-On
- Zero Trust Network Access

Security Operations
Secure IT/OT Convergence
- Endpoint Detection & Response
- Logging, Monitoring and Reporting
- Network Operations Center
- Security Automation and Orchestration
- Security Operations Center

Security Services
Detect & Protect
- Advanced Threat Protection
- Analytics & Compliance
- Device Detection Service
- OT Security Service
- Virtual Patching

Ecosystem Partners
Extend
- Fabric-Ready Partners
- Global System Integrators
- OT Security Partners

Use Cases to Solution Mapping

Each solution offering is based on a single product or a combination of multiple products from Fortinet, and these solutions can be deployed either as standalone or integrated with other products to meet the intended use case.

The following table lists the specific Fortinet products that make up each solution offering, mapped to the relevant use cases. These use cases correspond to the most commonly deployed products in the "Recommended Solutions" column, guiding customers in selecting the right solution for their needs. Additional products can be chosen from the "Optional Solutions" column based on the organization's risk exposure and maturity level.

Secure Digital Networks

USE CASES	DESCRIPTION	RECOMMENDED SOLUTIONS	OPTIONAL SOLUTIONS
Network Segmentation	Logical and physical division of a network into multiple segment 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 microsegments or sub-zones, interconnected by an NGFW with single-pane-of-glass management for network and security operations.	FortiGate FortiSwitch	FortiManager FortiGuard Services
Network Access Control	Network access control solution that enhances the visibility, control, and automated response for everything that connects to the network.	FortiNAC	FortiGuard Services
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	FortiSwitch FortiAP FortiExtender FortiSASE
Secure Remote Access	Enable secure remote access to critical IT/OT assets with VPN, multi-factor authentication, network traffic inspection, and advanced threat protection to secure the organizations and its remotely accessed digital assets.	FortiPAM	FortiGate FortiAuthenticator FortiToken FortiGuard Services
Web Application Security	Protect web applications and APIs from internal and external attacks that target applications using known vulnerabilities and zero-day threats.	FortiWeb	FortiGuard Services

Secure Service Edge

USE CASES	DESCRIPTION	RECOMMENDED SOLUTIONS	OPTIONAL SOLUTIONS
Identity and Access Management	Implement enhanced user verification controls and go beyond username and password to provide user verification requiring another factor. Multi-factor authentication (MFA) such as a one-time passcode (OTP) is a key security feature of the Fortinet IAM solution because it requires verification of multiple credentials.	FortiAuthenticator FortiToken	FortiGate FortiToken
Privileged Access Management	Take control of privileged accounts and enable monitoring of elevated user access, processes, and critical systems across the IT/OT environments.	FortiPAM FortiClient	FortiGate FortiAuthenticator FortiToken
Role Based Access Control	Enforce authorization for users based on their roles through centrally defined access control policy for accessing network resources.	FortiPAM FortiClient	FortiGate FortiAuthenticator FortiToken
Single Sign-On	Deploy single sign-on (SSO) with centralized identity management and centrally manage user identities and their access to assets. SSO authenticates users with both traditional and modern web and cloud authentication protocols.	FortiAuthenticator	FortiGate FortiToken
Zero Trust Network Access	Critical assets need to be protected with the highest level of security. Fortinet IAM solutions allow for enhanced security including zero-trust network access (ZTNA) controls when users try to access critical assets. Zero trust starts with user identities. Fortinet IAM product portfolio offers an end-to-end solution to implement least-privilege access to assets with enterprise-grade MFA. Plus, improve user experience with SSO.	FortiPAM FortiClient FortiNAC FortiAuthenticator FortiToken	FortiGate FortiAnalyzer FortiManager

Use Cases to Solution Mapping

Secure IT/OT Convergence

USE CASES	DESCRIPTION	RECOMMENDED SOLUTIONS	OPTIONAL SOLUTIONS
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
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 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

Detect & Protect

USE CASES	DESCRIPTION	RECOMMENDED SOLUTIONS	OPTIONAL SOLUTIONS
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 FortiNDR
Analytics & Compliance	Fortinet soltuions include hundreds of pre-built, ready-to-use reports and enables easy-to-schedule delivery of reports. The report builder comes with 400+ charts and 35+ templates for report customization. Risk scoring and assessment provides risk assessment across a variety of Fortinet practices, NIST, and CIS best practices. The Fortinet Security Rating Service can also be used to compare against specific industries.	FortiGate FortiAnalyzer FortiGuard Services	FortiManager
Device Detection Service	Automatically discover and identify 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
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
Virtual Patching	Virtual Patching or Vulnerability Shielding acts as a compensating security control against threats that have the potential to exploit known or unknown vulnerabilities. Virtual patching works by implementing layers of security controls that intercept and prevent an exploit from compromising the vulnerable assets connected on the network(s). OT-specific IPS signatures can provide a virtual patch to the environment so that unpatched systems can continue to operate within the OT network with minimized risk of exploitation. A security team can wait until the next scheduled outage to apply an underlying patch or continue to operate the vulnerable OT systems with a virtual patch in place in case no security fix is available for it.	FortiGate FortiGuard Services	FortiManager

# 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 OT Security Service and Attack Surface Security Service are part of the FortiGuard subscription offering.

FORTIGATE	BASE PRODUCT	ENTERPRISE HARDWARE BUNDLE	ENTERPRISE RENEWAL BUNDLE	OT SECURITY SERVICE	ATTACK SURFACE SECURITY
FGR-50G-5G	FGR-50G-5G	FGR-50G-5G-BDL-809-DD	FC-10-FR5G5-809-02-DD	FC-10-FR5G5-159-02-DD	FC-10-FR5G5-175-02-DD
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-70G	FGR-70G	FGR-70G-BDL-809-DD	FC-10-GR70P-809-02-DD	FC-10-GR70P-159-02-DD	FC-10-GR70P-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
FGR-70G-5G-DUAL	FGR-70G-5G-DUAL	FGR-70G-5G-DUAL-BDL-809-DD	FC-10-F70G5-809-02-DD	FC-10-F70G5-159-02-DD	FC-10-F70G5-175-02-DD
FG-40F-3G4G	FG-40F-3G4G	FG-40F-BDL-809-DD	FC-10-0040F-809-02-DD	FC-10-F40FG-159-02-DD	FC-10-F40FG-175-02-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-200G	FG-200G	FG-200G-BDL-809-DD	FC-10-FG2HG-809-02-DD	FC-10-FG2HG-159-02-DD	FC-10-FG2HG-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-VM02	-	FC-10-FVM02-812-02-DD	FC-10-FVM02-159-02-DD	FC-10-FVM02-175-02-DD
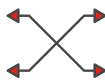
FortiSwitch is a secure access switch family that delivers outstanding performance, scalability, and manageability. FortiSwitch allows OT customers to extend networking and security across their network infrastructure. FortiSwitch seamlessly integrates with the Security Fabric via FortiLink. FortiCloud 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-108F	FSR-108F	FC-10-S08FN-247-02-DD
FSR-112F-POE	FSR-112F-POE	FC-10-SR2FP-247-02-DD
FSR-216F-POE	FSR-216F-POE	FC-10-SR16F-247-02-DD
FSR-424F-POE	FSR-424F-POE	FC-10-R24FP-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

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-234G	FAP-234G-X*	FC-10-P234G-247-02-DD
FAP-431G	FAP-431G-X*	FC-10-PG431-247-02-DD
FAP-432FR	FAP-432FR-X*	FC-10-F432FR-247-02-DD
FAP-432G	FAP-432G-X*	FC-10-P432G-247-02-DD
FAP-433F	FAP-433F-X*	FC-10-F433F-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
FER-511G	FER-511G-X	FC-10-XR51G-247-02-DD
FEV-211F	FEV-211F-X	FC-10-FG21F-247-02-DD
FEV-211F-AM	FEV-211F-AM	FC-10-FV21F-247-02-DD
FEV-212F	FEV-212F-X*	FC-10-FG22F-247-02-DD
FEV-212F-AM	FEV-212F-AM	FC-10-FV22F-247-02-DD
FEV-511G	FEV-511G-X	FC-10-FV51G-247-02-DD
FEX-200F	FEX-200F	FC-10-X200F-247-02-DD
FEX-311F	FEX-311F	FC-10-X311F-247-02-DD
FEX-511F	FEX-511F	FC-10-X511F-247-02-DD

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

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-200G	FMG-200G		FC-10-M200G-247-02-DD
FMG-410G	FMG-410G		FC-10-FM41G-247-02-DD
FMG-1000G	FMG-1000G		FC-10-FM1KG-247-02-DD
FMG-VM		FC2-10-FMGVS-258-01-DD	

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-CAX-VM	FC-10-FNVXA-248-02-DD	LIC-FNAC-PLUS-1K	FC5-10-FNAC1-213-01-DD
FNC-CA-700F	FNC-CA-700F	FC-10-NF700-247-02-DD	LIC-FNAC-PLUS-1K	FC5-10-FNAC1-213-01-DD

* Minimum order quantity 500

Product Offerings and Ordering Information

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 AV, application firewall, antiransomware, and endpoint management.

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

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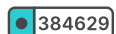
FORTISASE	SUBSCRIPTION
FortiSASE User Subscription - 50 to 499 Users	FC2-10-EMS05-547-02-DD
FortiSASE User Subscription - 500 to 1999 Users	FC3-10-EMS05-547-02-DD

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

Product Offerings and Ordering Information

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-210	FTK-210-XX*

* Replace XX with the number of tokens.

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-1000G	FAZ-1000G	FAZ-1000G-BDL-466-DD	FC-10-AZ1KG-159-02-DD	FC-10-AZ1KG-466-02-DD
FAZ-3100G	FAZ-3100G	FAZ-3100G-BDL-466-DD	FC-10-AZ31G-159-02-DD	FC-10-AZ31G-466-02-DD
FAZ-VM	–	FC1-10-AZVMS-465-01-DD	FC1-10-LV0VM-159-02-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-2200G	FSM-2200G FSM-AIO-2200-BASE	FC-10-FM22G-247-02-DD FC[2-Y]-10-FSM99-240-02-DD
FSM-AIO-BASE	FSM-AIO-BASE	FC-10-FM22G-247-02-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
FortiSOAR Starter Edition	FC-10-SRVMS-1023-02-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-500G	FSA-500G	FSA-500G-UPG-LIC-BYOL	FC-10-FS5HG-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
FDC-as-a-Service	Subscription	Included with subscription	FC1-10-DCDAS-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.

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

Product Offerings and Ordering Information

FortiPAM is a robust privileged access and session management solution designed to secure critical assets across both IT and OT environments. It combines secure remote access with advanced control over privileged accounts — all within a unified, integrated solution. Whether supporting third-party contractors or remote employees, FortiPAM ensures that access to sensitive systems is secure, monitored, and tightly controlled. Key features include session monitoring and auditing, web-based antivirus scanning, and secure file exchange — all working together to reduce cybersecurity risks from both internal and external users. With FortiPAM, organizations gain complete visibility and control over privileged access, enhancing security, compliance, and operational resilience.

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
FortiPAM-VM - 250 or more users	FC6-10-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.

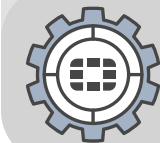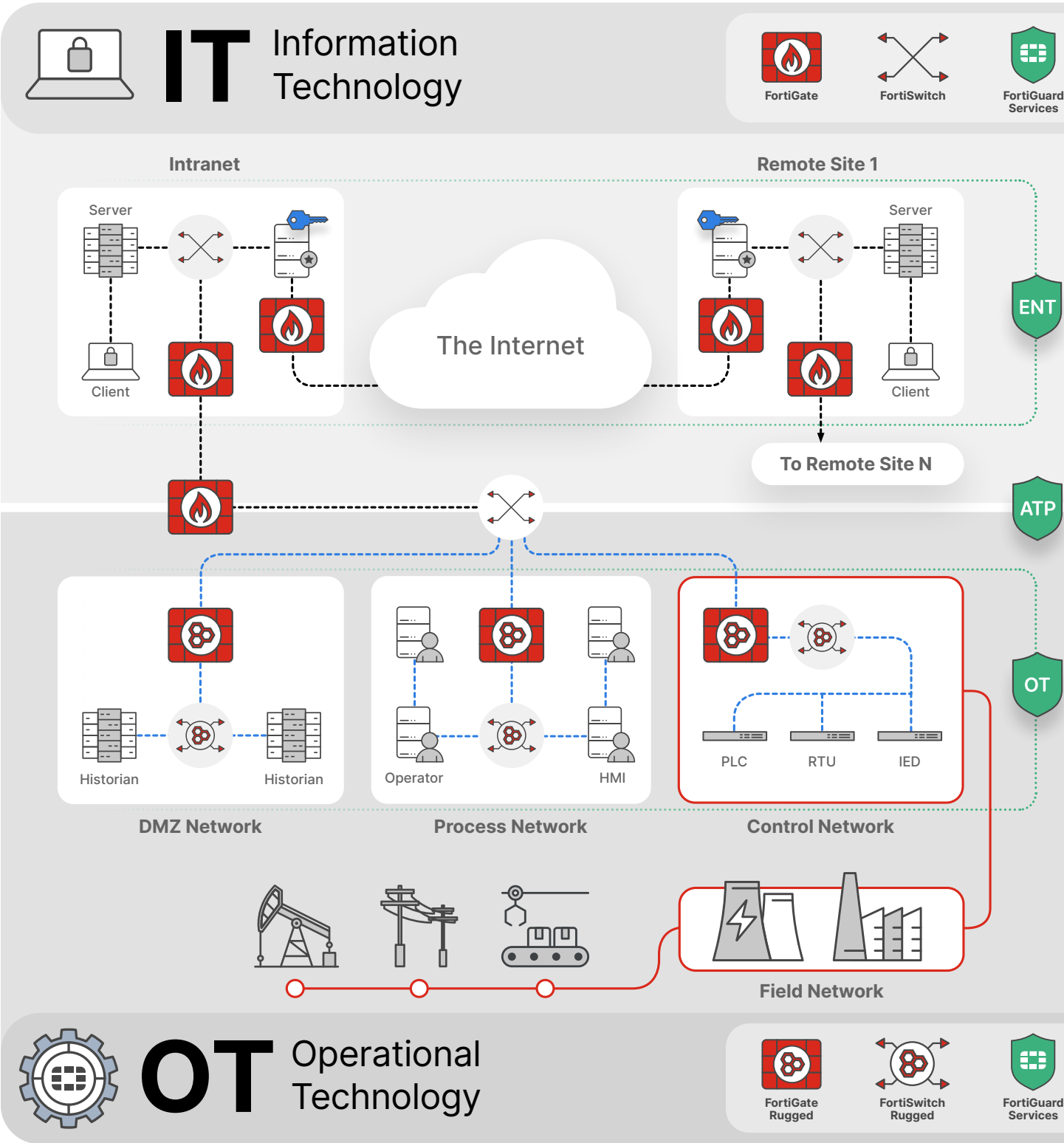| FORTIRECON	500 ASSETS	1000 ASSETS	50000 ASSETS
FortiRecon EASM	FC2-10-RNSVC-533-02-DD	FC3-10-RNSVC-533-02-DD	FC6-10-RNSVC-533-02-DD
FortiRecon EASM+BP+ACI	FC2-10-RNSVC-535-02-DD	FC3-10-RNSVC-535-02-DD	FC6-10-RNSVC-535-02-DD

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-1000F-BDL-331-DD	FC-10-AI1KF-331-02-DD	FC-10-AI1KF-588-02-DD - Netflow FC-10-AI1KF-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

Fortinet Accessories include several standard and rugged hardware accessories designed specifically for Fortinet products. See the Additional Information and Resources section for more details.

Typical Deployment of FortiGate NGFWs in IT/OT Networks

IT Information Technology

FortiGate **FortiSwitch** **FortiGuard Services**

Intranet

Server

Client

Remote Site 1

Server

Client

The Internet

ENT

To Remote Site N

ATP

Historian Historian

DMZ Network

Operator HMI

Process Network

PLC RTU IED

Control Network

OT

Field Network

OT Operational Technology

FortiGate Rugged **FortiSwitch Rugged** **FortiGuard Services**

FortiGuard OT Security Service Coverage – September 2025

OT Application Control Signatures

No arrow: Only application/protocol detection
➔ **One arrow:** Application/protocol and message inspection
⇒ **Double arrows:** Application/protocol, message, and parameter inspection
[N]: Number of IPS signatures available

ABB Controller SysCmd	Ether-S-Bus [120] ➔	Modbus TCP/IP [84] ⇒	Rockwell FactoryTalk View SE
Allen-Bradley CSP	Ether-S-I/O [2] ➔	Moxa UDP Device Discovery	Rockwell FactoryTalk ViewPoint
Allen-Bradley DF-1 [46] ➔	Ewon M2web	MTConnect	SafetyNET p [16] ➔
Allen-Bradley PCCC [12] ➔	Ewon Talk2M Access	Niagara Fox	Schneider UMAS [20] ➔
BACnet [130] ➔	Ewon Talk2M VPN	oBIX	SECS-II/GEM [245] ➔
Beckhoff AMS [9] ➔	FactorySuite NMXSVC	OCPP [125] ➔	SEL Fast Messaging [33] ➔
Bristol BSAP	FANUC FOCAS [33] ➔	Omron FINS [59] ➔	Siemens Epoc EDM
CC-Link [9] ➔	FL-NET [30] ➔	OPC AE [67] ➔	Siemens LOGO [6] ➔
CN/IP CEA-852 [14] ➔	GE EGD [8] ➔	OPC Common [19] ➔	Siemens OCG ATCS [564] ➔
CoAP [4] ➔	GE SRTP [20] ➔	OPC DA [109] ➔	Siemens S7 [46] ⇒
CODESYS [101] ➔	Hart IP [29] ➔	OPC DA Automation	Siemens S7 1200 [3] ➔
DDSI-RTPS	IEC 60870-5-104 [86] ⇒	OPC HDA [66] ➔	Siemens S7 Plus [22] ➔
Digi ADDP [8] ➔	IEC 60870-6 (ICCP/TASE.2) [41] ➔	OPC HDA Automation [11] ➔	Siemens SIMATIC CAMP [6] ➔
Digi RealPort (Net C/X)	IEC 61850 [44] ➔	OPC UA [45] ➔	STANAG 4406 Military Messaging
Digi RealPort (Net C/X) DNP3 [37] ⇒	IEC 61850-90-5 R-GOOSE	OpenADR [28] ➔	STANAG 5066
Direct Message Profile [5] ➔	IEC 61850-90-5 R-SV	OSIsoft Asset Framework	ToolsNet Open Protocol
DLMS/COSEM(IEC62056) [8] ➔	IEEE 1278.2 DIS [46] ➔	OSISoft PI	TRDP [10] ➔
DNP3 [57] ➔	IEEE C37.118 Synchrophasor [13] ➔	Panasonic MEWTOCOL [26] ➔	Triconex TSAA [8] ➔
ECHONET Lite [138] ➔	Inductive Automation Ignition	Profinet CBA [27] ➔	TriStation [212] ➔
ECOM100	ITCM [20] ➔	Profinet IO [4] ➔	Unitronics PCOM [40] ➔
ELCOM 90 [9] ➔	KNXnet/IP (EIBnet/IP) [15] ➔	Rockwell Drive Peripheral Interface [7] ➔	V2G EXI
Emerson DeltaV	LonTalk IEC14908-1 CNP [4] ➔	Rockwell FactoryTalk AssetCentre	V2G SDP
Emerson ROC	Matrikon OPC Tunneller	Rockwell FactoryTalk Diagnostic	Veeder-Root ATG
EtherCAT [2] ➔	Mitsubishi MELSEC [41] ➔	Rockwell FactoryTalk Live Data	Vnet/IP
Ethernet POWERLINK	MMS [84] ➔	Rockwell FactoryTalk RNA Alarming	WITS0
EtherNet/IP-CIP [139] ⇒	Modbus RTU [8] ➔	Rockwell FactoryTalk RNA Server Ping	WITSML [6] ➔

OT Vulnerability Protection Signatures

ABB [29]	GE [6]	Pepperl+Fuchs [4]
Advantech [110]	Iconics [4]	PnP SCADA [2]
AVEVA [2]	Inductive Automation [14]	PTC [4]
B&R Automation [1]	InHand Networks [3]	Ricon [1]
Contec [5]	KeySight [5]	Rockwell Automation [23]
Delta Electronics [51]	Korenix [4]	Schneider Electric [91]
DUT CCE [4]	Moxa [31]	SEL [1]
Eaton [10]	mySCADA [7]	Siemens [58]
EIP Stack Group [3]	Open Automation Software [1]	Sierra Wireless [7]
ETIC [3]	Omron [13]	WECON [23]
Fuji [10]	Osprey [4]	Wibu Systems [3]

For an up-to-date list of supported signatures, please visit fortiguard.com.
Click here to submit a new signature request.

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
FortiExtender Rugged	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiextender-rugged.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
Fortinet Accessories	FortiAP Antennas: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinet-antennas.pdf FortiExtender Antennas: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiextender-accessories.pdf Rugged Power Supply: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortinet-rugged-accessories.pdf

Visit the OT Security Solutions Hub for additional technical information on Fortinet solutions for operational technology.

? 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

This course focuses on securing OT infrastructures using Fortinet solutions. It covers designing, deploying, administering, and monitoring FortiGate, FortiNAC, FortiAnalyzer, and FortiSIEM devices to secure OT infrastructures. These skills provide a comprehensive understanding of designing, implementing, and operating an OT security solution based on Fortinet products.

Course Details

For prerequisites, agenda topics, and learning objectives, visit the Fortinet training website.

Training Offering

For training SKUs, purchasing, and delivery options, visit the Fortinet training website.

F:::RTINET.

www.fortinet.com

September 1, 2025 5:11 PM

OT-OG-R22-01092025