

FortiSOAR



Highlights

- End-to-End Security Operations covering IT/OT incident response, threat intel, asset and vulnerability management
- Smart Automation with GenAI assistant, ML-driven recommendations, and no/low-code playbook creation
- Extensive Ecosystem with 600+ pre-built connectors

Unified Security Orchestration, Automation, and Response (SOAR)

FortiSOAR helps IT/OT security teams thwart attacks by centralizing incident management and automating the myriad of analyst activities required for effective threat investigation and response.

SOC teams are overloaded with investigating alerts and responding to threats across dozens of tools. Most have difficulty keeping pace and may be slow to discover and respond to serious attacks before a breach occurs. Using FortiSOAR as a central operations hub to standardize and execute these workflows speeds response and SOC operations, allowing analysts to focus on what matters most to protect the organization.



"FortiSOAR is the champion product when it comes to automation and having the ability to maximize existing tools."

FortiSOAR is a leader in the 2023 and 2024 KuppingerCole SOAR Leadership Compass

Highlights

Security Incident Response

Centralized and automated alert triage, enrichment, investigation, collaboration, and response actions for IT/OT security.

Case and Workforce Management

A complete solution for case management and managing and tracking task assignments, work queues, and shift calendaring.

Threat Intelligence Management

Automatically curates intel from FortiGuard Labs and any public source to enrich investigations, threat hunting, and collaboration.

Asset Management

Centralizes asset security and risk views along with automated change management process playbooks.

Vulnerability Management

Combines risk-based asset vulnerability views, task management, and automated patch and mitigation playbooks.

OT Security Management

Extended integrations and functions meet OT-specific monitoring and playbook automation requirements.

Compliance Validation and Reporting

Tracking, dashboards, SLAs, and reporting support IT/OT regulatory compliance management.

GenAI-powered Security Assistant

FortiAI uses GenAI to guide, simplify, and automate threat investigation, response actions, and more.

AI Recommendation Engine

ML powers automation and decisioning, including alert grouping, threat assessment, playbook creation, and playbook suggestions.

Content Hub and Community

An expanding library of connectors, playbooks, solutions, videos, and community contributions drive continued benefits.

No/Low-code Playbooks

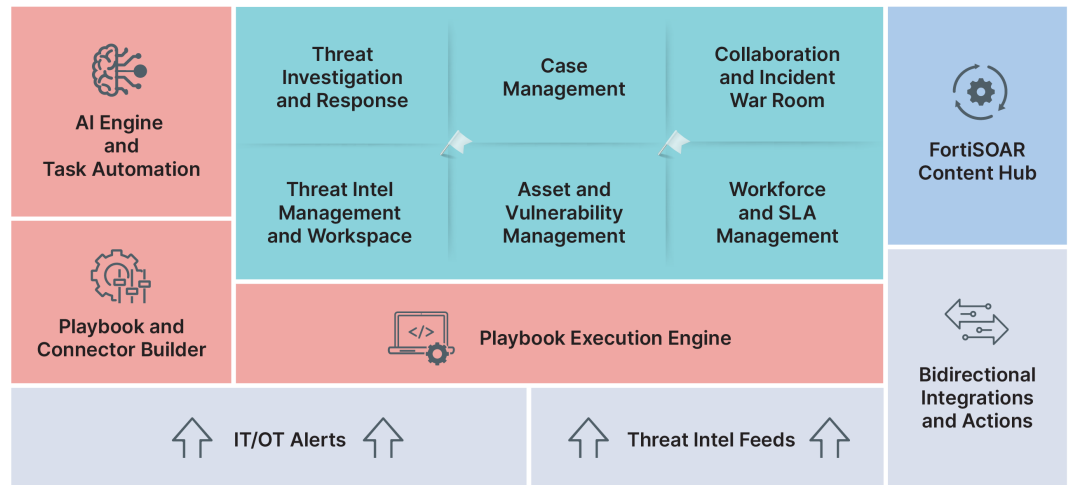
Patented design experience provides visual drag/drop and rapid development modes to create playbooks without technical coding skills.

Enterprise and MSSP-Ready

SaaS, on-prem, multi-tenant, dedicated and shared-tenant options support MSSP and global enterprise requirements.



Key Features



Centralize, Standardize, and Automate Security Operations

With broad integrations, rich functions, hundreds of pre-built playbooks and simple customization, FortiSOAR is designed to be the central hub for the critical operations that protect and power your organization.

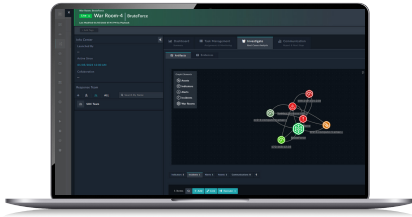
Alert Ingestion and Bi-directional Integrations

The foundation of FortiSOAR is connectivity. Integration flexibility and connectors to over 500 multivendor products allows FortiSOAR to ingest alerts from virtually any security source and interact with any IT system or application. The pre-built connectors each support an array of actions, typically bi-directional, that enable automated commands, queries, and actions useful for investigation, remediation, and notifications. Comprehensive Solution Packs include connectors, actions and full playbooks for typical integrations and use cases.

Investigation, Response, and Case Management

FortiSOAR can automatically triage, enrich, and assess alerts from virtually any security product. Routine alerts can be automatically handled and closed. Priority alerts are mapped to the MITRE ATT&CK framework and intelligently grouped into incidents for deeper investigation. ML-driven task automation and playbook recommendations augment rich investigation features, suggest actions, and execute complete remediation steps. FortiSOAR supports complete case management features as well as two-way linkages to ticketing and communications systems, and includes a secure mobile application.

Key Features Continued



Collaboration and Incident War Room

The FortiSOAR investigation interface makes it simple for analysts to collaborate, and supports communications and playbook permissions via email, Zoom, Slack, Teams and other popular methods. Analysts can also trigger a dedicated war room for streamlined and collaborative high-priority incident management. War room functions include invitation-only access, task management, collaboration tools, dedicated private communications, reporting, and full forensics-level logging of all activities.

Threat Intelligence Management

FortiSOAR automatically ingests, aggregates, normalizes and curates a wide range of IT/OT threat feeds, including Fortinet's FortiGuard threat intel data. Relevant intel automatically enriches alerts and is presented during analyst investigations. As a complete Threat Intel Platform, FortiSOAR supports IOC export via STIX, TAXII, and CSV, a dedicated goal-based threat intelligence management workspace, and request ticketing and assignment to facilitate threat research, collaboration and sharing.



Asset and Vulnerability Management

FortiSOAR integrates with asset management and vulnerability scanning systems to give you a complete risk-based picture of your IT/OT assets—including identification, criticality, vulnerability status, and alert conditions. Analysts and managers can use this information to launch automated remediation or other playbooks and assign and track tasks. Alert and incident investigation is enriched and accelerated by having complete asset profiles at hand without the need to access other systems or tools.

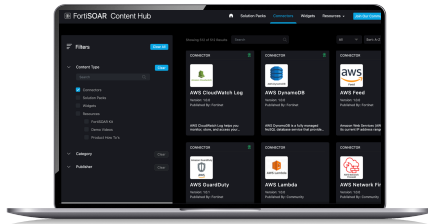
Workforce and SLA Management

FortiSOAR provides all of the key functions a SOC manager needs to run effective operations. The system can automatically assign tasks based on priority, expertise matching and analyst task backlog. Leaders can define and manage work queues, manage shift schedules, and staff calendaring. Team and individual SLA metrics can be defined and tracked. Standard reports suiting both enterprise and MSSP uses can be easily customized or newly created.

Playbook and Connector Creation

The patented playbook design experience provides a visual drag/drop graphical user interface (GUI) and a low-code rapid development mode that allows users to easily create playbooks without technical coding skills. Hundreds of prebuilt playbooks and automated actions can be used as building blocks, while the FortiSOAR Recommendation Engine provides inline step guidance. The designer function includes full CI/CD support as well as a simulation engine for testing. New connector creation is supported by an intuitive and guided wizard application.

Key Features Continued



AI-Driven Assistance and Automation

FortiAI uses augmented Generative AI to guide, simplify, and automate FortiSOAR analyst activities such as threat investigation, response, and playbook building. An integral part of analyst workflows, FortiAI extends and curates GenAI results with the latest Fortinet threat intel and product knowledge to give analysts the actionable guidance they urgently need.

The FortiSOAR Recommendation Engine uses ML to power automation and decision making for threat investigation and response workflows, task assignments, playbook recommendations and playbook building guidance. Key parameters of Recommendation Engine can be controlled, including ML algorithms, feature selection, and functional areas in which to apply ML recommendations and actions.

Compliance Automation and Reporting

FortiSOAR automates advisory update and overall compliance activities with advisory processing playbooks, specialized tracking, dashboards, and IT/OT compliance management reporting for regulations, including GDPR, HIPAA, US BOD 22-01, US NERC CIP, and more. FortiSOAR asset management, vulnerability management, SLA tracking, and other features support mandatory alerts and actions necessary for compliance adherence.



OT Security Operations

FortiSOAR fully supports OT security automation and consolidated IT/OT operations. You can monitor and manage OT SecOps with features such as risk-based OT asset and vulnerability management, MITRE ATT&CK industrial control system (ICS) views for threat investigation, OT threat remediation playbooks, and full OT vendor and threat intelligence ecosystem integration. FortiSOAR's design approach to OT is based on best practices aligned with Cybersecurity and Infrastructure Security Agency (CISA) operational directives.

Network Operations and Beyond

FortiSOAR bi-directional integrations and pre-built playbooks automate a full array of network operations for security response as well as standard NOC activities such as deployment, configuration, configuration updates and any move/update/change actions. Full experience customization and simple playbook creation allow automation of virtually any workflow.

Content Hub and Community

The FortiSOAR Content Hub provides an extensive and growing library of ready-made product content and valuable knowledge via an intuitive, web-based and in-product portal of hundreds of connectors and playbooks, dashboard widgets, and complete solution packs built by the Fortinet team or contributed by the user community. Demo and how-to videos deliver tutorials and best practices to help you get the most from your automation initiatives.

The FortiSOAR Community Portal keeps you in touch with your peers and the latest FortiSOAR news. A moderated discussion board and idea exchange provide immediate access to peer group Q&As, helpful insights, best practices, and a direct link to contact Fortinet experts.



MSSP and Global Enterprise Features

FortiSOAR Customers



Financial Services

Top 5 institutions in 10 countries



Government

Over 20 institutions in 15 countries



Energy

8 top producers/distributors
No. 1 O&G producer worldwide



Managed Security Services

Over 15 major MSSPs worldwide
4 of top 20 worldwide providers



Healthcare

Largest US healthcare insurer
Largest US healthcare provider



Technology and Software

Top Telecom solutions provider
Top CAD/CAM provider



Telecom

Over 10 major providers
5 of top 20 worldwide providers



Manufacturing

Top 5 automaker
Top 5 electronics maker

Over 400 Enterprise, Government, and MSSP Customers

Many of the biggest names across industry, government and security services depend on FortiSOAR as the mission-critical backbone of their security operations. You too, can depend on FortiSOAR to help protect your organization.

FortiSOAR is designed to support the flexible and sophisticated deployment models demanded by MSSPs and multinational enterprise operations. Shared and dedicated tenant models supported by on-premises agents allow hierarchical and global/regional SOC deployments and enable bespoke customer requirements.

FortiSOAR also offers global and per-tenant playbooks, agnostic playbooks that auto-translate into tenant-specific versions prior to execution, and a full range of tenant-specific functions, such as SLA tracking, alerts, incident views, reports, and dashboards. In addition, the FortiSOAR concurrent user licensing model helps MSSPs control costs and offer attractive customer pricing.

FortiSOAR is available as SaaS or can be deployed as a VM or container on-premises or in private and public clouds. With proven reliability, scalability, and high availability options, FortiSOAR meets the needs of the most demanding organizations.

Connectors and Bi-Directional Integrations

The following are notable integrations that FortiSOAR offers today. Most integrations are bidirectional, supporting API-commands and FortiSOAR playbooks to execute actions, inquiries, searches, and other external product commands useful to SOC/NOC analysts and managers. The connector list is always growing.



Fortinet Fabric Solutions

FortiAnalyzer, FortiAuthenticator, FortiCNP, FortiCWP, FortiDeceptor, FortiEDR, FortiEMS, FortiGate, FortiGuard, FortiMail, FortiManager, FortiMonitor, FortiNAC, FortiNDR, FortiSandbox, FortiSIEM, FortiWeb.



Network and Firewall Products

Check Point Firewall, Cisco ASA/Firepower/Meraki, F5 BIG-IP, Palo Alto Firewall, Zscaler



DevOps

Gitlab, Jenkins, Docker, Kubernetes, Terraform



Email and Email Security

FortiMail, Cisco Email Security Appliance (ESA), GSuite for Gmail, Microsoft Exchange, Mimecast, Symantec Email Security Cloud



Endpoint Security

FortiEDR, CrowdStrike Falcon, Microsoft Defender, SentinelOne, Symantec EDR Cloud, Tanium



Investigation

FortiAnalyzer, FortiSIEM, Have I Been Pwned, RSA NetWitness, Nmap Scanner, Securonix SNYPR, Symantec Security Analytics



Log Management and Analytics

FortiSIEM, FortiAnalyzer, IBM QRadar, Microsoft Sentinel, Rapid7 InsightIDR, Splunk, Sumo Logic



Sandbox

FortiSandbox, FireEye AX, Hybrid-Analysis, Joe Sandbox Cloud, Palo Alto WildFire, VMRay



Threat Intel

Fortinet FortiGuard, Anomali ThreatStream, CrowdStrike Falcon Intelligence, IBM X-Force Exchange, Mandiant Threat Intelligence, VirusTotal



Ticket Management

BMC Remedy AR System, JIRA SM, ManageEngine ServiceDesk, ServiceNow, Zendesk



Vulnerability Management

Kenna Security, Qualys VMDR, Rapid7 Nexpose, Tenable.io, Tenable Security Center

For the full catalog and descriptions of the functions supported for each integration, see the FortiSOAR Content Hub at fortisoar.contenthub.fortinet.com.



Ordering Information

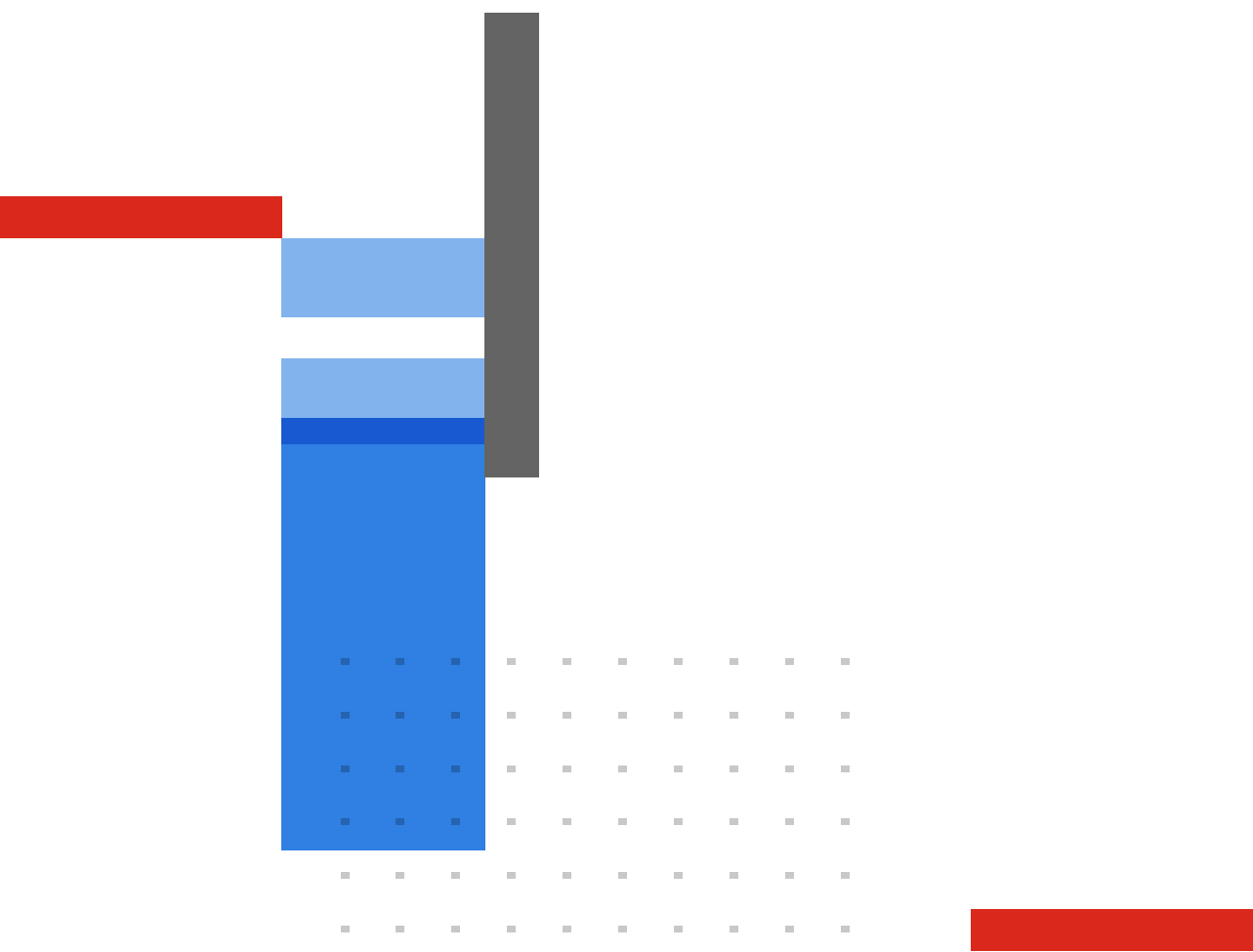
DEPLOYMENT OPTIONS AND LICENSING MODEL			
	FORTISOAR VM SUBSCRIPTION	FORTISOAR VM PERPETUAL	FORTISOAR PAAS
Deployment			
License Type	Subscription	Perpetual	Subscription
Hosting Type	On Premise or Public Cloud	On Premise or Public Cloud	Fortinet Hosted
Editions			
Enterprise Edition	FC-10-SRVMS-389-02-DD	LIC-FSRENT-2	FC-10-SRCLD-385-02-DD*
Multi Tenant Edition - Manager Node	FC-10-SRVMS-390-02-DD	LIC-FSRMTT-2	FC-10-SRCLD-386-02-DD*
Starter Edition (allowed 10 000 actions/day)	FC-10-SRVMS-1023-02-DD		
Add-on			
Multi-Tenant - Dedicated Node	FC-10-SRVMS-387-02-DD	LIC-FSRMTD-1	FC-10-SRCLD-387-02-DD
Multi-Tenant - Regional Node	FC-10-SRVMS-388-02-DD	LIC-FSRMTR-2	FC-10-SRCLD-388-02-DD
HA Node	FC-10-SRVMS-1121-02-DD	LIC-FSRHA-2	
Threat Intel Management Module (includes FortiGuard Threat Feed)	FC-10-SRVMS-592-02-DD	FC-10-SRVMP-592-02-DD	FC-10-SRCLD-592-02-DD
User Seat	FC-10-SRVMS-384-02-DD	LIC-FSRAUL-1	FC-10-SRCLD-384-02-DD
Cloud Storage (additional 1TB Storage, 8GB RAM, and 4 vCPU)			FC1-10-SRCLD-584-01-DD
FortiMonitor - subscription for Advanced Health Monitoring		FC2-10-MNCLD-437-01-DD **	
Subscription/Renewal			
Enterprise Edition Renewal with FortiCare Premium	FC-10-SRVMS-385-02-DD	FC1-10-SRVMP-248-02-DD	FC-10-SRCLD-385-02-DD
Multi-Tenant Manager Renewal with FortiCare Premium	FC-10-SRVMS-386-02-DD	FC2-10-SRVMP-248-02-DD	FC-10-SRCLD-386-02-DD
Multi-Tenant - Dedicated Node Renewal with FortiCare Premium	FC-10-SRVMS-387-02-DD	FC3-10-SRVMP-248-02-DD	FC-10-SRCLD-387-02-DD
Multi-Tenant - Regional SOC Node Renewal with FortiCare Premium	FC-10-SRVMS-388-02-DD	FC4-10-SRVMP-248-02-DD	FC-10-SRCLD-388-02-DD
HA Node Renewal with FortiCare Premium	FC-10-SRVMS-1121-02-DD	FC5-10-SRVMP-248-02-DD	—
Professional and Training Services			
Per Day Charge for Resource Service (SOW)		FP-10-00000-M08-00-00	
Per Hour Charge for Service Delivered After-Hours/Weekend. Must order a minimum of four hours, and must use a minimum of four hours at a time		FP-PS001-HR	
Custom Travel and Expenses for On Site Professional Services		FP-MISC-TE	
Deployment Quick Start Service		FP-10-QSSOAR-DP1-00-00	
NSE 6 FortiSOAR Administration Training		FT-FSR-ADM	
NSE 6 FortiSOAR Administration Exam Voucher		NSE-EX-SPL6	
NSE 7 FortiSOAR Design and Development Training		FT-FSR-DEV	
NSE 7 FortiSOAR Design and Development Exam Voucher		NSE-EX-CERT	
NSE 7 FortiSOAR Design and Development Lab Access		FT-FSR-DEV-LAB	

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.