FortiSOAR

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.

500+ Multi-vendor integrations
800+ Pre-built playbooks
300+ Enterprise/MSSP Customers

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

KuppingerCole 2023 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.

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

**Alert Ingestion and Bi-directional Integrations**

The foundation of FortiSOAR is connectivity. Integration flexibility and connectors to over 500 multivendor products allow 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.

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.
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 Automation and Recommendations
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. Examples include alert triage, enrichment, risk assessment, and grouping into incidents; in-line playbook suggestions; field completions; best suitable analyst assignment; and recommended Action blocks for playbook building. Key parameters of Recommendation Engine can be controlled, including ML algorithms, feature selection, and functional areas in which to apply ML recommendations and actions.

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 across the organization.

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 500+ connectors, 800+ 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

Over 300 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, in private and public clouds, or as a FortiCloud-hosted private solution. 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 bi-directional, 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. Please see the FortiSOAR Content Hub (fortisoar.contenthub.fortinet.com) for the full catalog and descriptions of the functions supported for each integration.

Fortinet Fabric Solutions

Virtually all Fortinet solutions, including: FortiAnalyzer, FortiAuthenticator, FortiCNP, FortiCWP, FortiDeception, FortiEDR, FortiEMS, FortiGate, FortiGuard, FortiMail, FortiManager, FortiMonitor, FortiNAC, FortiINDR, FortiSandbox, FortiSIEM, FortiWeb.

Network and Firewall Products

FortiGate, Cisco Meraki MX VPN Firewall, Infoblox DDI, CISCO Umbrella Enforcement, Cisco Meraki MX L7 Firewall, Empire, CISCO Firepower, ForeScout, Zscaler, Imperva Incapsula, NetSkope, RSA Netwitness Logs And Packets, Palo Alto Firewall, CISCO ASA, SOPHOS UTM-9, Arbor APS, F5 Big-IP, Proofpoint TAP, Check Point Firewall, CISCO Catalyst, Citrix NetScaler WAF, Sophos XG, Cisco Stealthwatch, Pfsense, Symantec Messaging Gateway, PRTG, Centreon.

Ticket Management


Log Management, Analytics, and SIEM

FortiSIEM, FortiAnalyzer, RSA Netwitness SIEM, Sophos Central, Rapid7 InsightIDR, LogPoint, Micro Focus ArcSight Logger, Alienvault USM Anywhere, xMatters, Sumo Logic, LogRhythm, Syslog, Elasticsearch, McAfee ESM, IBM QRadar, ArcSight, Splunk, Microsoft Sentinel.

Vulnerability Management

Rapid7 Nexpose, Kenna, Qualys, Tripwire IP360, Symantec CCSVM, Tenable IO, ThreadFix, Tenable Security Center.
Connectors and Bi-Directional Integrations Continued

**Endpoint Security**


**Threat Intel**

Over 120 sources, including: Fortinet FortiGuard, AbuseIPDB, AlienVault OTX/USM Central, Anomali Enterprise/Limo/Threat/STAXX, AWS Feed, Cisco Talos, Code42, CRITS, CrowdStrike Falcon Intelligence, Cybereason, DNS, Dragos WorldView, Facebook Threat Exchange, , Google Cloud, IBM X-Force, Mandiant Feed/Threat Intelligence, Microsoft Management Activity/Office365 Feed, MITRE ATT&CK, Palo Alto WildFire, PhishMe, Threat Connect, Trend Micro SMS/Vision One, Virus Total.

**DevOps**

AWS Athena, AWS S3, Twilio, IBM BigFix, AWS EC2.

**Sandbox**


**Email and Email Security**

GSuite For GMail, Microsoft Exchange, SMTP, IMAP, Mimecast, Symantec Email Security Cloud, FireEye EX, CISCO ESA.

**Investigation**

FortiAnalyzer, FortiSIEM, FortiMail, Securonix SNYPR, Symantec ICDx, Symantec Security Analytics, NMAP Scanner, Protectwise, PhishTank, CloudPassage Halo, TruSTAR, Have I Been Pwned, Farsight Security DNSDB, Cofense PhishMe, RSA Netwitness.
### Ordering Information

<table>
<thead>
<tr>
<th>Product</th>
<th>Customer Hosted Subscription</th>
<th>Customer Hosted Perpetual</th>
<th>Fortinet Hosted Cloud Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiSOAR Enterprise Edition</td>
<td>FC-10-SRVM-389-02-DD</td>
<td>LIC-FSRENT-2</td>
<td>FC-10-SRCLD-385-02-DD*</td>
</tr>
<tr>
<td>FortiSOAR Enterprise Edition (Renewal)</td>
<td>FC-10-SRVM-385-02-DD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiSOAR Multi Tenant Edition - Master</td>
<td>FC-10-SRVM-390-02-DD</td>
<td>LIC-FSRMTT-2</td>
<td>FC-10-SRCLD-386-02-DD*</td>
</tr>
<tr>
<td>FortiSOAR Multi Tenant Edition – Master (Renewal)</td>
<td>FC-10-SRVM-386-02-DD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add User Seat</td>
<td>FC-10-SRVM-384-02-DD</td>
<td>LIC-FSRAUL-1</td>
<td>FC-10-SRCLD-384-02-DD</td>
</tr>
<tr>
<td>Add Tenants on Master</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Add Tenant as Dedicated SOAR Node (Single User Locked) - aka Dedicated Tenant Node</td>
<td>FC-10-SRVM-384-02-DD</td>
<td>LIC-FSRMTD-1</td>
<td>FC-10-SRCLD-387-02-DD</td>
</tr>
<tr>
<td>Add Tenant as Dedicated SOAR Node (Multiple User Capable) - aka Regional SOC Instance</td>
<td>FC-10-SRVM-388-02-DD</td>
<td>LIC-FSRMTR-2</td>
<td>FC-10-SRCLD-388-02-DD</td>
</tr>
<tr>
<td>Add Cloud Storage (1000GB with 8GB RAM and 4vCPU)</td>
<td></td>
<td></td>
<td>FC1-10-SRCLD-584-01-DD</td>
</tr>
<tr>
<td>Add Health Monitoring using FortiMonitor</td>
<td>FC2-10-MNCLD-437-01-DD **</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subscription Service for FortiSOAR Threat Intel Management Service including FortiGuard Premium Threat Feed</td>
<td>FC-10-SRVM-592-02-DD</td>
<td>FC-10-SRVMP-592-02-DD</td>
<td>FC-10-SRCLD-592-02-DD</td>
</tr>
<tr>
<td>Support Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiCare Premium Contract</td>
<td>Included</td>
<td>See <a href="#">Ordering Guide</a></td>
<td>Included</td>
</tr>
<tr>
<td>FortiCare Premium Contract for FortiSOAR Enterprise Edition</td>
<td>-</td>
<td>FC1-10-SRVMP-248-02-DD</td>
<td>-</td>
</tr>
<tr>
<td>FortiCare Premium Contract for FortiSOAR Multi Tenant Edition</td>
<td>-</td>
<td>FC2-10-SRVMP-248-02-DD</td>
<td>-</td>
</tr>
<tr>
<td>FortiCare Premium Contract for FortiSOAR Multi Tenant - Dedicated Tenant</td>
<td>-</td>
<td>FC3-10-SRVMP-248-02-DD</td>
<td>-</td>
</tr>
<tr>
<td>FortiCare Premium Contract for FortiSOAR Multi Tenant - Regional SOC Instance</td>
<td>-</td>
<td>FC4-10-SRVMP-248-02-DD</td>
<td>-</td>
</tr>
<tr>
<td>FortiCare Premium Contract for FortiSOAR Enterprise plus FortiCare BPS</td>
<td>-</td>
<td>FC1-10-SRVMP-338-02-DD</td>
<td>-</td>
</tr>
<tr>
<td>FortiCare Premium Contract for FortiSOAR Multi Tenant plus FortiCare BPS</td>
<td>-</td>
<td>FC2-10-SRVMP-338-02-DD</td>
<td>-</td>
</tr>
<tr>
<td>FortiCare Premium Contract for FortiSOAR Multi Tenant - Dedicated Tenant plus FortiCare BPS</td>
<td>-</td>
<td>FC3-10-SRVMP-338-02-DD</td>
<td>-</td>
</tr>
<tr>
<td>FortiCare Premium Contract for FortiSOAR Multi Tenant - Regional SOC Instance plus FortiCare BPS</td>
<td>-</td>
<td>FC4-10-SRVMP-338-02-DD</td>
<td>-</td>
</tr>
<tr>
<td>Professional Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per Day Charge for Resource Service (SOW)</td>
<td>FP-10-00000-M08-00-00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per Hour Charge for Service Delivered After–Hours/Weekend. Must order a minimum of 4 hours, and must use a minimum of 4 hours at a time</td>
<td>FP-PS001-HR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Travel and Expenses for On Site Professional Services</td>
<td>FP-MISC-TE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/15 days JumpStart Programme and customised PS packages</td>
<td>Ask for Quote based on specific requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSE 6 FortiSOAR Administration Training</td>
<td>FT-FSR-ADM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSE 6 FortiSOAR Administration Exam Voucher</td>
<td>NSE-EX-SPL6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSE 7 FortiSOAR Design and Development Training</td>
<td>FT-FSR-DEV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSE 7 FortiSOAR Design and Development Exam Voucher</td>
<td>NSE-EX-CERT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSE 7 FortiSOAR Design and Development Lab Access</td>
<td>FT-FSR-DEV-LAB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* A FortiCloud Premium Account License (FC-15-CLDPS-219-02-DD) is required to use the FortiSOAR Cloud service.

** Recommended FortiMonitor’s 25-pack Device/Server Subscription Solution Bundle. For more information, see the [FortiMonitor Data Sheet](#)
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.