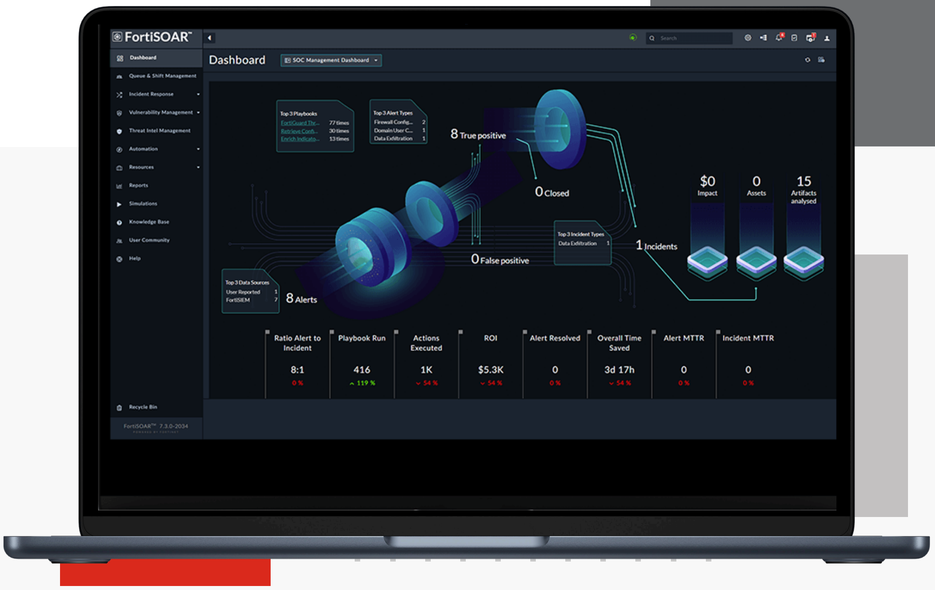
FortiSOAR



Ratio Alert to Incident	Playbook Run	Actions Executed	ROI	Alert Resolved	Overall Time Saved	Alert MTTR	Incident MTTR
8:1	416	1K	$5.3K	0	3d 17h	0	0
0 %	^ 119 %	v 54 %	v 54 %	0 %	v 54 %	0 %	0 %

Highlights

- IT/OT Security Incident Response
- Case and Workforce Management
- Threat Intelligence Management
- Asset and Vulnerability Management
- GenAI-powered Security Assistant
- ML-driven Recommendations
- No/Low Code Playbook Creation

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 breech 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.

600+
Connectors

400+
Enterprise/MSSP Customers

LEADERSHIP COMPASS kuppingercole ANALYSTS

“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.

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.

Available in

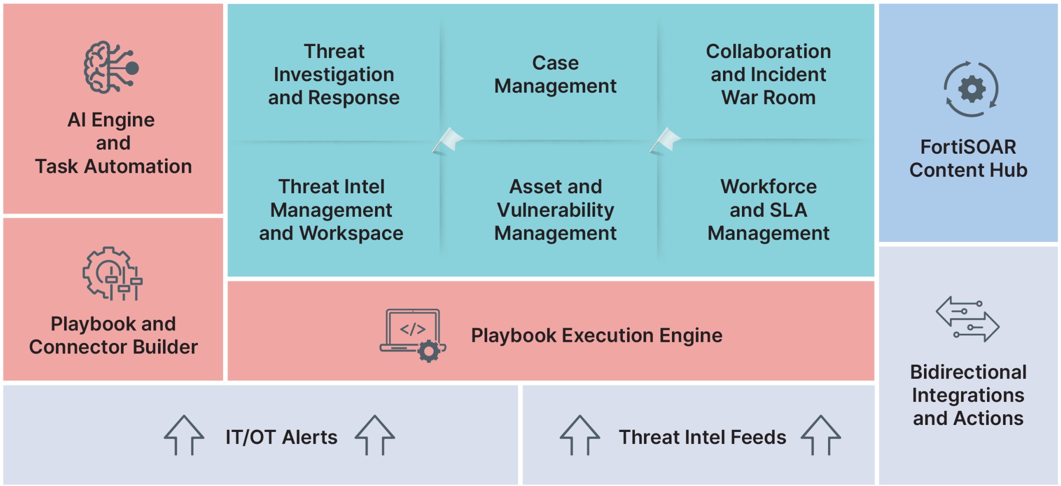
Virtual

Cloud

SaaS

MSSP

Key Features


AI Engine and Task Automation
Threat Investigation and Response
Case Management
Collaboration and Incident War Room
FortiSOAR Content Hub
Threat Intel Management and Workspace
Asset and Vulnerability Management
Workforce and SLA Management
Playbook and Connector Builder
Playbook Execution Engine
Bidirectional Integrations and Actions
IT/OT Alerts
Threat Intel Feeds

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.

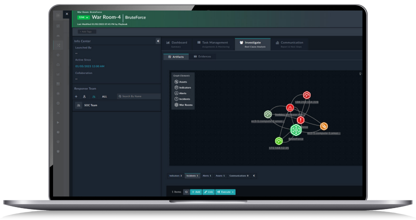
Alert Ingestion and Bi-directional Integrations

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

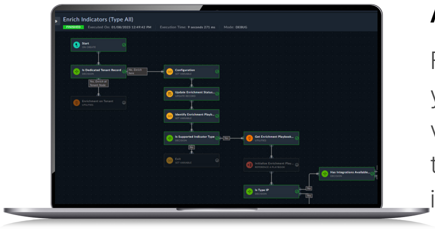


Collaboration and Incident War Room

The FortiSOAR investigation interface makes it simple to 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.


Enrich Indicators (Type All)
FINISHED
Executed On: 01/08/2023 12:49:42 PM
Execution Time: 9 seconds 271 ms
Mode: DEBUG
Start
ON CREATE
Is Dedicated Tenant Record
DECISION
No, Enrich here
Yes, Enrich at Tenant Node
Enrichment on Tenant
UTILITIES
Configuration
SET VARIABLE
Update Enrichment Status...
UPDATE RECORD
Identify Enrichment Playb...
SET VARIABLE
Is Supported Indicator Type
DECISION
Yes
No
Exit
SET VARIABLE
Get Enrichment Playbook...
UTILITIES
Initialize Enrichment Play...
REFERENCE A PLAYBOOK
Is Type IP
DECISION
Has Integrations Available...
DECISION

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.

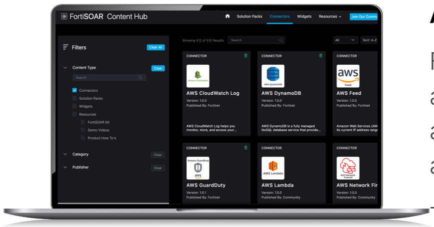
Workforce and SLA Management

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



AWS CloudWatch Log helps you monitor, store, and access your...

AWS DynamoDB is a fully managed NoSQL database service that provide...

Amazon Web Services (AW its current IP address range

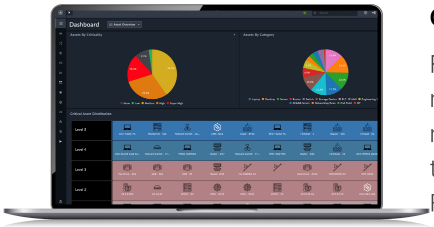
AI-Driven Assistance and Automation

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

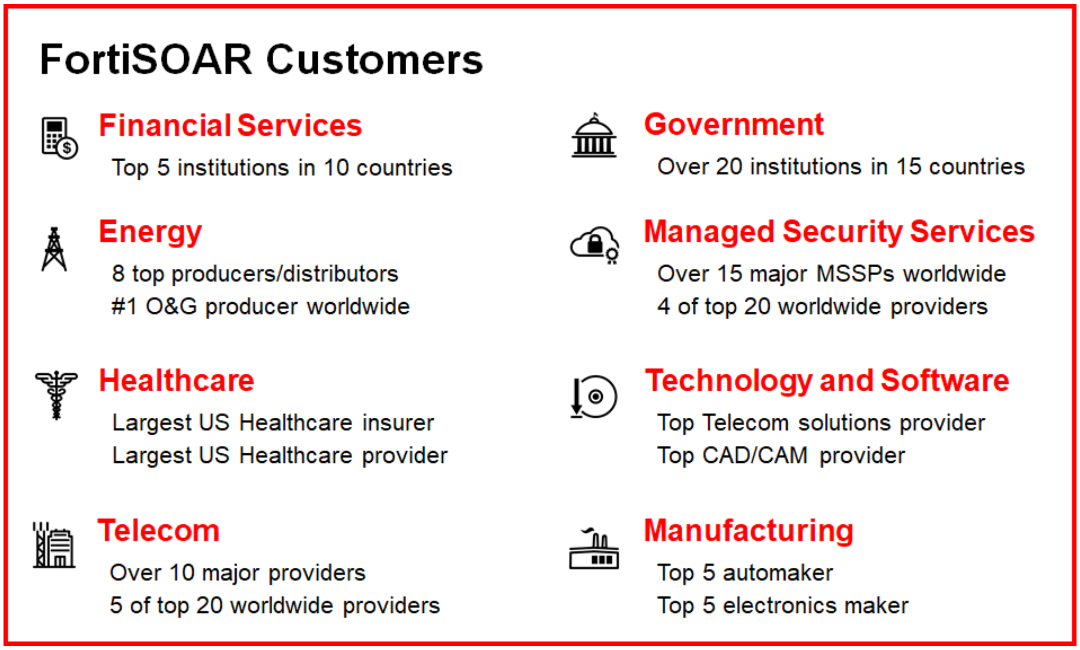
FortiSOAR bi-directional integrations and pre-built playbooks automate a full array of network operations for security response as well as standard NOC activities such as deployment, configuration, configuration updates and any move/update/change actions. Full experience customization and simple playbook 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
#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 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, FortiDeceptor, FortiEDR, FortiEMS, FortiGate, FortiGuard, FortiMail, FortiManager, FortiMonitor, FortiNAC, FortiNDR, 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

ConnectWise Manage, Foresight, Zendesk, ServiceAide, Manage Engine Service Desk Plus, Salesforce, BMC Remedy AR System, OTRS, Request Tracker, JIRA, Pagerduty, RSA Archer, Cherwell, ServiceNow.

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

FortiEDR, Endgame, Trend Micro Control Manager, CrowdStrike Falcon, FireEye HX, Carbon Black Defense, Malwarebytes, McAfee EPO, Symantec EDR Cloud, MicroSoft Defender, Microsoft WMI, TrendMicro Deep Security, Symantec EPM, Symantec DLP, WINRM, NetBIOS, Microsoft SCCM, Microsoft SCOM, CISCO AMP, Carbon Black Protection Bit9, CYLANCE Protect, SentinelOne, Carbon Black Response, TANIUM.

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

FortiSandbox, GitLab, ThreatSTOP, Intezer Analyze, FireEye AX, CISCO Threat Grid, URLSCAN. Io, Joe Sandbox Cloud, Koodous, Trend Micro DDAN, Symantec CAS, HYBRID-ANALYSIS, VMRAY, PaloAlto WildFire, Malwr, Lastline, SecondWrite, Cuckoo.

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

DEPLOYMENT OPTIONS AND LICENSING MODEL			
FortiSOAR Edition	Customer Hosted Subscription	Customer Hosted Perpetual	Fortinet Hosted Cloud Subscription
FortiSOAR Enterprise Edition	FC-10-SRVMS-389-02-DD	LIC-FSRENT-2	FC-10-SRCLD-385-02-DD*
FortiSOAR Enterprise Edition (Renewal)	FC-10-SRVMS-385-02-DD		
FortiSOAR Multi Tenant Edition - Manager	FC-10-SRVMS-390-02-DD	LIC-FSRMTT-2	FC-10-SRCLD-386-02-DD*
FortiSOAR Multi Tenant Edition - Manager (Renewal)	FC-10-SRVMS-386-02-DD		
Add User Seat	FC-10-SRVMS-384-02-DD	LIC-FSRAUL-1	FC-10-SRCLD-384-02-DD
Add Tenants on ManagerNode	Included	Included	Included
Add Tenant as Dedicate SOAR Node (Single User Locked) - aka Dedicated Tenant Node	FC-10-SRVMS-387-02-DD	LIC-FSRMTD-1	FC-10-SRCLD-387-02-DD
Add Tenant as Dedicated SOAR Node (Multiple User Capable) - aka Regional SOC Instance	FC-10-SRVMS-388-02-DD	LIC-FSRMTR-2	FC-10-SRCLD-388-02-DD
FortiSOAR Starter Edition (10 000 actions/day allowed)	FC-10-SRVMS-1023-02-DD		
FortiSOAR HA Edition	FC-10-SRVMS-1121-02-DD	LIC-FSRHA-2	
Add Cloud Storage (1000GB with 8GB RAM and 4vCPU)			FC1-10-SRCLD-584-01-DD
FortiMonitor subscription for Advanced Health Monitoring Requirements	FC2-10-MNCLD-437-01-DD **		
SECURITY SERVICES			
Subscription Service for FortiSOAR Threat Intel Management Service including FortiGuard Premium Threat Feed	FC-10-SRVMS-592-02-DD	FC-10-SRVMP-592-02-DD	FC-10-SRCLD-592-02-DD
Support Services			
FortiCare Premium Contract	Included	See Below	Included
FortiCare BPS	Included	See Below	Included
Support SKU for Perpetual Licensing Model			
FortiCare Premium Contract for FortiSOAR Enterprise Edition	—	FC1-10-SRVMP-248-02-DD	—
FortiCare Premium Contract for FortiSOAR Multi Tenant Manager Edition	—	FC2-10-SRVMP-248-02-DD	—
FortiCare Premium Contract for FortiSOAR Multi Tenant - Dedicated Tenant	—	FC3-10-SRVMP-248-02-DD	—
FortiCare Premium Contract for FortiSOAR Multi Tenant - Regional SOC Instance	—	FC4-10-SRVMP-248-02-DD	—
FortiCare Premium Contract for FortiSOAR HA Edition	—	FC5-10-SRVMP-248-02-DD	—
Support SKU with BPS for Perpetual Licensing Model			
FortiCare Premium Contract for FortiSOAR Enterprise plus FortiCare BPS	—	FC1-10-SRVMP-338-02-DD	—
FortiCare Premium Contract for FortiSOAR Multi Tenant plus FortiCare BPS	—	FC2-10-SRVMP-338-02-DD	—
FortiCare Premium Contract for FortiSOAR Multi Tenant - Dedicated Tenant plus FortiCare BPS	—	FC3-10-SRVMP-338-02-DD	—
FortiCare Premium Contract for FortiSOAR Multi Tenant - Regional SOC Instance plus FortiCare BPS	—	FC4-10-SRVMP-338-02-DD	—
Professional 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		
FortiSOAR Deployment QuickStart Service	FP-10-QSSOAR-DP1-00-00		
Training Services			
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		

* A FortiCloud Premium Account License (FC-15-CLDPS-219-02-DD) is required to use the FortiSOAR Cloud service.
** Recommended FortiMonitor 25-pack Device/Server Subscription Solution Bundle. For more information, see the FortiMonitor Data Sheet.

Sample BOQ

Customer One:
An enterprise customer wants to host FortiSOAR within their premises. They need a perpetual license for 10 analysts along with two years of support and want to add Threat Intelligence Service including FortiGuard feeds. They also need training for developers along with a development instance for ongoing playbook and connector creation:
LIC-FSRENT-2 (FortiSOAR Enterprise Edition with two seats included - Perpetual)
LIC-FSRAUL-8 (Eight Additional User Seats)
FC1-10-SRVMP-248-02-24 (FortiCare Premium Contract for FortiSOAR Enterprise Edition for 24 months)
FC-10-SRVMP-592-02-24 (Two year Subscription Service for FortiSOAR Threat Intel Management Service including FortiGuard Premium Threat Feed)
FortiSOAR Free Trial OR FC-10-SRVMS-1023-02-24 (FortiSOAR Starter Edition for two years) as a development instance
FT-FSR-DEV (NSE 7 FortiSOAR Design and Development Training)
If PS is needed, a quote from PS team can be requested.

Customer Two:
An MSSP customer wants to leverage Fortinet's Hosted Option and needs a license for 10 analysts. They also need training for their developers:
FC-10-SRCLD-386-02-DD (FortiSOAR Hosted Cloud Subscription - Enterprise Edition with two seats and support included)
FC-15-CLDPS-219-02-DD (FortiCloud Premium Account License)
FT-FSR-DEV (NSE 7 FortiSOAR Design and Development Training)
If PS is needed, a quote from PS team can be requested.

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

August 27, 2024