SOLUTION BRIEF

Optimize MSSP Operations with FortiSOAR

Executive Summary

Security-conscious organizations are increasingly turning to managed security service providers (MSSPs) to augment or completely manage critical security operations functions. The expanding enterprise attack surface across IT and OT devices, more AI-driven attack techniques, and the need for increasingly complex security tools, such as endpoint detection and response (EDR), extended detection and response (XDR), and network detection and response (NDR), accelerates the trend of outsourcing key capabilities. Given that speed matters more than ever as malicious actors advance their efforts, organizations are also demanding rapid and in-depth detection and analysis capabilities from the MSSP services they use.

MSSPs face many challenges in meeting these critical customer demands. Tracking and meeting customer SLA metrics is vital, making alert processing automation and standardization a must. Yet running a services business across complex multivendor environments while managing customer demands requires a central operating platform for all service-related operations. MSSPs need a platform that enables efficient and effective operations and the opportunity for differentiation in a competitive marketplace.

FortiSOAR enables MSSPs to deliver impactful and differentiated customer value by centralizing and automating provider operations. By combining best-in-class IT/OT security orchestration, automation, and response (SOAR) capabilities with an MSSP-optimized feature set and architecture, FortiSOAR is the cornerstone of efficient and cost-effective service operations. Leading MSSPs around the world depend on FortiSOAR as their core platform to deliver multivendor alert investigation services, MDR capabilities, SOAR-as-a-Service, and complete security operations outsourcing.

500+
integrations

800+
playbooks

300+
enterprise and MSSP customers

Fortinet named a leader in the KuppingerCole Leadership Compass for SOAR, Q1 2023

FortiSOAR

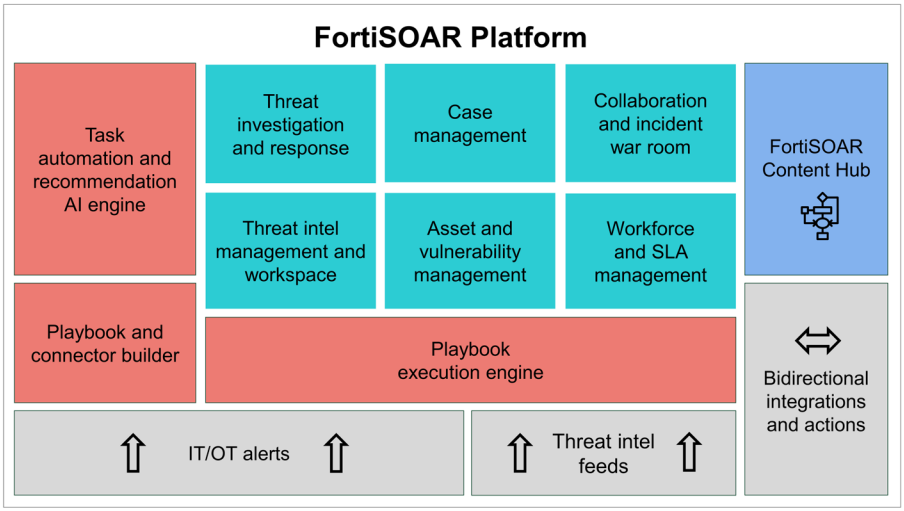
Best-in-Class SOAR Features

- Threat investigation and response
- Case management and ticketing
- Threat intelligence management
- Collaboration and war room
- Asset and vulnerability management
- No/low-code playbook creation

MSSP-Optimized Platform

- Flexible deployment options
- Security and compliance built-in
- Tenant and cross-tenant functions
- Management visibility and control
- Workforce and SLA management
- Scaling and high availability

FortiSOAR Platform and Analyst Features



FortiSOAR provides a best-in-class SOAR platform, including broad integrations, rich analyst functions driven by intelligent automation, simple playbook creation, and the flexibility to automate virtually any workflow. FortiSOAR is designed to be the central hub for IT/OT incident management and is the automation engine for workflows to support security operations centers (SOCs) and network operations centers (NOCs).

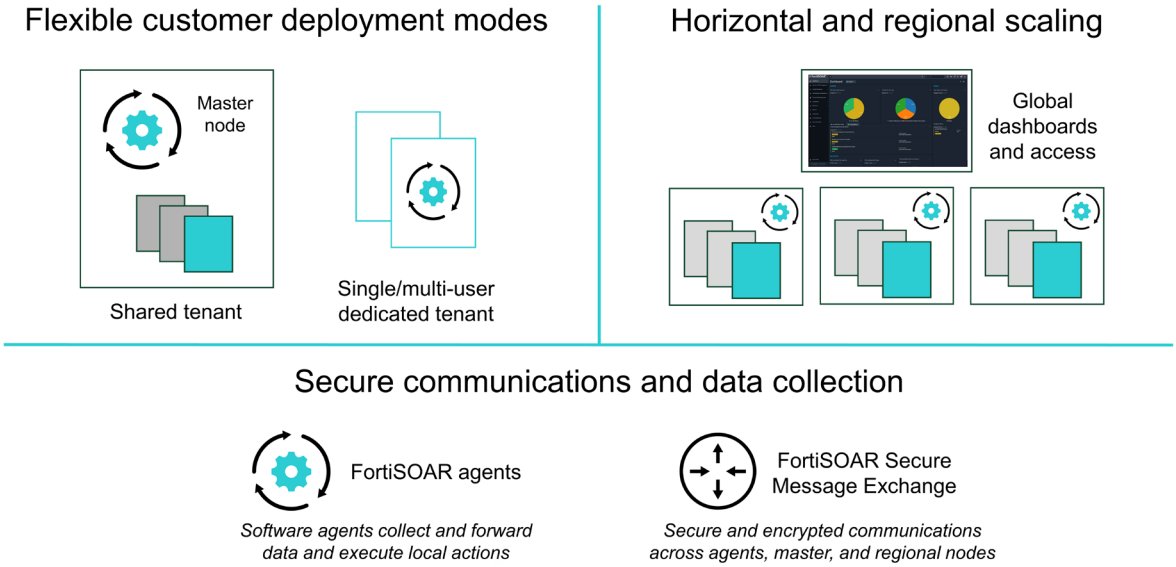
FortiSOAR Benefits	Description
Threat investigation and response	Offers centralized and automated alert triage, enrichment, investigation, collaboration, and response actions for IT/OT security
Case management	Offers a complete solution for incident case management, including prioritization, assignment, tracking, and reporting
Threat intelligence management	Automatically manages curated intel from FortiGuard Labs and any public source to enrich investigations and threat hunting
Collaboration and war room	Allows analysts to easily collaborate during investigations, in dedicated war rooms, or via common communication tools
Asset management	Centralizes asset security and risk views along with automated change management process playbooks
Vulnerability management	Provides risk-based asset vulnerability views, task management, and automated patch and mitigation playbooks
OT security management	Offers extended integrations and functions to meet OT-specific monitoring and playbook automation requirements
Workforce and SLA management	Enables leaders to define and manage work queues and schedules, and to define and track team and individual SLAs
No/low code playbook creation	Provides visual drag-and-drop and rapid development modes to build playbooks without coding skills
Content hub and community	Offers 500+ connectors, 800+ playbooks, solution packs, videos, and community contributions to drive rapid benefits

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. Users can control key parameters of the recommendation engine, including ML algorithms, feature selection, and functional areas in which to apply ML recommendations and actions.

See the FortiSOAR data sheet for additional feature information.

MSSP Operations and Management



Beyond best-in-class SOAR platform and analyst features, FortiSOAR provides comprehensive deployment, operations, and management capabilities designed for flexible, scalable, secure, and compliant MSSP services that can meet any customer need. You can depend on FortiSOAR as your operations backbone for any SOC or NOC service, as well as a superior direct SOAR-as-a-Service offering.

Deployment options

FortiSOAR MSSP master nodes can be deployed within the MSSP infrastructure of choice or hosted by Fortinet in a FortiCloud regional data center. MSSPs have several onboarding options:

- **Shared tenant** deployments reside within an MSSP master node FortiSOAR system. This is the typical deployment scenario for most managed services customers, giving the full SOAR benefits to the provider while ensuring secure data collection, role-based access control, and tenant data isolation. MSSP master nodes can scale horizontally.
- **Single-user dedicated tenant** deployments are separate FortiSOAR instances that may reside in the MSSP or customer infrastructure. This option is designed for MSSP providers whose customers require physical data isolation. It is also suitable for a low-cost SOAR-as-Service offering.
- **Multi-user dedicated instance** deployments are separate, autonomous FortiSOAR instances typically residing within the customer infrastructure. This option is suitable for MSSP customers that require full isolation, greater options for control, and open FortiSOAR product access. It is also optimal for delivering a full SOAR-as-a-Service offering.

Security and compliance

FortiSOAR enables MSSPs to support the varying security, data protection, and regulatory compliance requirements of any customer. The FortiSOAR platform meets stringent security criteria, provides data segregation, and enforces role-based access controls for all users. Regional- and country-specific data privacy needs can be supported via regional MSSP master node deployment. Customer-specific requirements can be met with dedicated tenant deployment, as well as FortiSOAR agent and dedicated tenant data forwarding configurations.

Data collection and communications

FortiSOAR agents collect and forward alert and intelligence data to the appropriate FortiSOAR master node. Filter settings allow customers to restrict the forwarding of sensitive data. Communications security and data encryption for agent–tenant and dedicated tenant–MSSP master messaging is provided by the FortiSOAR Secure Message Exchange, avoiding the need for VPN communications.

Scaling and high availability

FortiSOAR MSSP master nodes support hierarchical and regional deployment and horizontal scaling, along with active-active and active-passive high availability configurations. All inter-node communications use the FortiSOAR secure message exchange mechanism.

Management visibility and control

FortiSOAR provides all the key functions MSSP management needs to run effective operations, including:

- **Overall client views:** Cross-tenant summary dashboards and drilldowns enable management to track metrics and monitor performance across customers.
- **Shared tenant functions:** Assigned analysts have access to all FortiSOAR features to manage their designated alerts and incidents.
- **Dedicated tenant control:** MSSP master nodes can remotely manage dedicated tenants, including replicating alerts, pushing playbooks, conducting configuration management, and more.
- **SLA tracking:** Customer (tenant), team, and individual SLA metrics can be defined and tracked and used in priority decisioning. SLA goals and timelines are always visible to analysts.
- **Workforce management:** Leaders can define and manage tenant assignments, work queues, shift schedules and handovers, and complete staff calendaring.
- **Ticketing:** FortiSOAR provides a complete independent ticketing system or can interoperate with popular ticketing systems.
- **Reporting:** FortiSOAR provides standard MSSP report templates and flexible reporting and export capabilities, including support for Microsoft Word–based templates.
- **Playbook execution:** FortiSOAR supports global and per-tenant playbooks, as well as agnostic playbooks that auto-translate into tenant-specific versions prior to execution.

Network operations and beyond

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

Connectivity and playbooks

The FortiSOAR Content Hub provides over 500 ready-made product and threat intelligence connectors. We continually add new connectors to the library, while the connector wizard makes it simple to create new connectors in-house. FortiSOAR provides over 800 prebuilt SOC and NOC playbooks, a patented low/no-code designer, as well as full CI/CD support, archiving, rollback, and a simulation engine for testing.

Powering MSSP Success with FortiSOAR

FortiSOAR enables MSSPs to deliver impactful and differentiated customer value by enhancing and automating provider operations. Leading MSSPs depend on FortiSOAR as their core platform to deliver multivendor alert investigation services, MDR capabilities, SOAR-as-a-Service, and complete security operations outsourcing. Whether you plan to utilize SOAR to optimize your services' backend and customer experience, or you're interested in offering customers a direct SOAR-as-a-Service, FortiSOAR is the right choice for your business.

Beyond driving operational efficacy, FortiSOAR minimizes MSSP technology costs in several respects:

- Shared tenants can reside within a master node, eliminating the need for costly dedicated infrastructure per customer.
- There is no shared tenant license cost nor a license restriction on the number of shared tenants per master node.
- Concurrent user pricing reduces the per-agent software costs for MSSP and customer operations.

FortiSOAR for Any Customer

Managed Security Services

Customer Type	Small-Medium Organization	Any Regulated Organization	Large Org with In-House SOC
Customer Objective	MSSP SOC/NOC turnkey services	Services and data isolation and controls	Services, isolation and SOAR access
SOAR Deployment	Shared tenant	Single-user dedicated tenant	Multi-user dedicated tenant
MSSP Benefit	Simple deployment of no additional cost	Low-cost compliance offering	Open platform plus services value

Managed SOAR-as-a-Service

Customer Type	Small-Medium Organization	Mature Operations Profile
Customer Objective	Fully managed SOAR expertise and service	Co-managed SOAR and service expertise
SOAR Deployment	Single-user dedicated tenant	Multi-user dedicated tenant
MSSP Benefit	Low-cost customer entry point	Flexibility to meet any customer demand

October 23, 2023 3:19 PM

2378841-0-0-EN