SOLUTION BRIEF

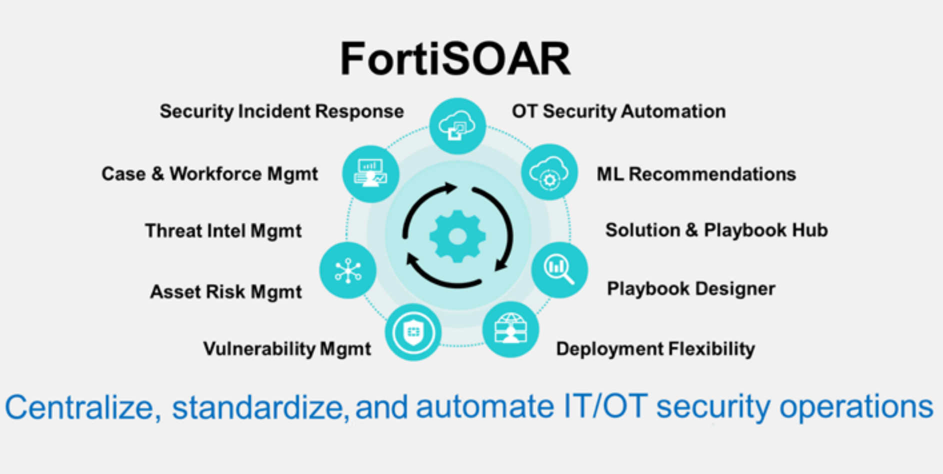
Optimize Security Operations with FortiSOAR

Centralize and Automate Attack Investigation and Response

Executive Summary

Security operations center (SOC) teams are overloaded with investigating alerts and responding to threats across dozens of tools.[1] Most teams struggle to keep pace, slowing their ability to discover serious attacks. Network operations center (NOC) and operational technology (OT) teams face their own monitoring and maintenance challenges, furthering security risks. Leading organizations and managed security service providers (MSSPs) use FortiSOAR to unify and optimize these critical workflows, ensuring better security while driving efficient IT/OT operations.

FortiSOAR enables organizations to centralize, standardize, and automate IT/OT security operations and critical enterprise functions. With broad integrations, rich use-case functions, hundreds of prebuilt workflows, and simple playbook creation, FortiSOAR supports best-in-class procedures tailored to your specific needs. FortiSOAR is the security operations hub that connects to everything and automates anything—helping protect your organization from attack.



FortiSOAR

500+ integrations

800+ prebuilt playbooks

300+ enterprise/MSSP customers

> "... FortiSOAR has advanced our threat detection and response capabilities by five years. It gives us this tremendous Swiss Army knife of functionality that we are excited to capitalize on."
>
> — CEO, Secure Cyber Defense

The Automation Imperative

From top to bottom, security teams are overloaded with too many tools to manage, too many alerts to investigate, and too many manual or repetitive processes—all of which slow down response times. Despite analyst efforts and SOC budget spending, typical incident detection and response performance remain inadequate to protect organizations against today's attackers.

Automation via FortiSOAR can dramatically change this dynamic by augmenting staff efficiency and enabling analysts to refocus on high-value activities. But automating repetitive or mundane tasks is only a tiny fraction of the potential value of FortiSOAR. Centralizing and standardizing complete investigation and response workflows that leverage artificial intelligence (AI), the latest available threat intelligence, and a rich analyst toolset can make the difference between attack deterrence and breach recovery.

Going further, FortiSOAR includes robust IT/OT functions for managing threat intelligence, threat hunting, risk-based assets, vulnerabilities, and more—all integrated into a single security operations hub. NOC and OT integrations, and playbooks, along with "automate anything" ease of customization make FortiSOAR an ideal operations hub.

The FortiSOAR platform is truly enterprise-grade, with proven reliability, scalability, flexible deployment options, and high-availability configuration support. Rich reporting and compliance capabilities track your security posture, forensic-level activities, and complete operations service-level agreements (SLAs). Whether you are looking for turnkey Software-as-a-Service (SaaS) automation, a mission-critical operations platform, or an MSSP value-added service, FortiSOAR is the right choice.

FortiSOAR Key Features

FortiSOAR delivers essential security orchestration, automation, and response features in a single platform.

> "FortiSOAR is the champion product when it comes to automation and having the ability to maximize existing tools."
>
> — Alejandro Leal, 2023 KuppingerCole Leadership Compass for SOAR, January 30, 2023

Security incident response: Offers centralized and automated alert triage, enrichment, investigation, collaboration, and incident response actions. Includes 500+ integrations, 800+ playbooks, robust features, and use-case solutions to support SOC/NOC/OT efficiency.

Case and workforce management: Provides a complete solution for managing and tracking task assignments, work queues, and shift calendaring.

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.

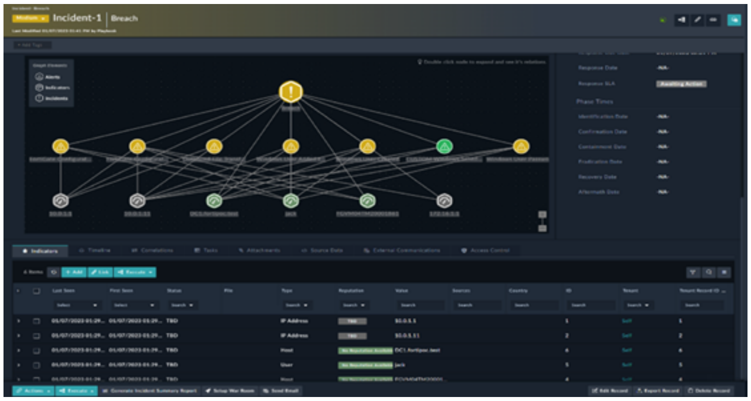
Machine learning-driven recommendation engine: Embedded AI powers automation and decision-making—including alert grouping, threat assessment, and suggested playbooks.

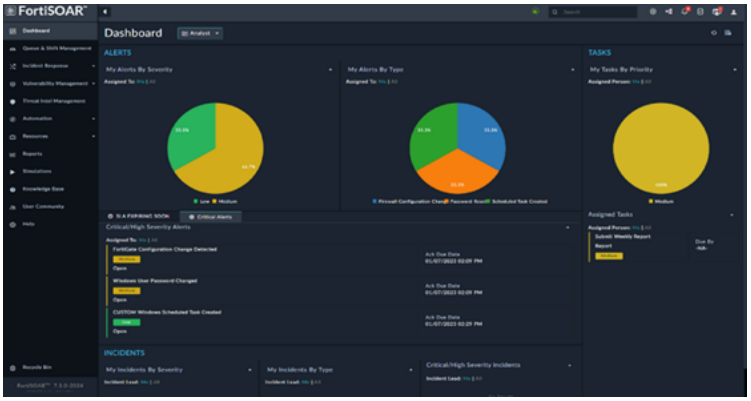
Built-in threat intelligence: Enriched investigations and threat hunting are powered by built-in FortiGuard Labs global intelligence as well as additional public sources.

FortiSOAR Content Hub and Community: An expanding library of connectors, playbooks, solutions, videos, and community contributions offers continued benefits.

No- and low-code playbook creation: Patented design experience provides visual drag/drop and rapid development modes to easily create custom playbooks without technical coding skills.

Flexible deployment options. Choose from SaaS, on-premises, public cloud hosting, or trusted MSSP partners—all with the same robust functionality.





FortiSOAR Use Case Spotlight

Critical use cases for FortiSOAR include:

SOC threat investigation and response

FortiSOAR is designed to be the central hub for threat management—automatically triaging, enriching, and assessing alerts from virtually any security product. Routine alerts are automatically handled and closed. Priority alerts are mapped to the MITRE ATT&CK framework and intelligently grouped into incidents for deeper investigation. Recommended playbooks augment rich investigation features, suggest actions, and execute complete remediation steps. Escalated incidents can activate a full war room that facilitates collaboration and includes detailed forensic logging. And analysts can take action anywhere and anytime via the FortiSOAR's secure mobile application.

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.

OT security operations

Increasing convergence with IT exposes OT assets to risks that demand comprehensive security protection.[2] FortiSOAR enables you to fully 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 ecosystem integration. The design approach of FortiSOAR for OT is based on best practices aligned with Cybersecurity and Infrastructure Security Agency (CISA) operational directives.[3]

Playbook 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 of all types to easily create custom playbooks. The FortiSOAR Content Hub contains hundreds of prebuilt playbooks and automated actions to use as building blocks, while the FortiSOAR Recommendation Engine provides inline step guidance. Even the most complicated playbook flows do not require technical coding skills. The designer function includes full versioning control as well as a simulation engine for testing.

MSSP operations

FortiSOAR is designed to uniquely enable the flexible and sophisticated deployment models demanded by MSSP 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 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.

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. You can easily add critical new use cases to your solution by leveraging the 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.

[1] "5 reasons why security operations are getting harder," CSO, October 6, 2022.

[2] "New Report Underscores Why OT Security Must Become a C-Suite Top Concern," Fortinet, June 17, 2022.

[3] "Cybersecurity Directives," CISA, accessed March 23, 2023.

www.fortinet.com

June 30, 2023 12:25 PM
2048834-0-0-EN