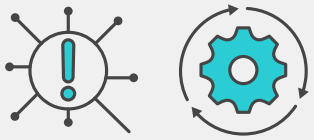
SOLUTION BRIEF

Make FortiSIEM and FortiSOAR the Foundation of Your Modern SOC

Executive Summary

Even the most skilled, well-staffed security operations center (SOC) teams typically suffer from alert overload. Manual processes, the need to use multiple tools, and siloed threat data also limit their ability to detect and investigate threats across the entire environment. Legacy or basic security information and event management (SIEM) solutions and simple automation scripts are insufficient to relieve SOC performance pressures or defend the organization from today's sophisticated attackers.

Security teams can adopt FortiSIEM and FortiSOAR (security orchestration, automation, and response) to provide advanced enterprisewide threat detection, complete incident management capabilities, and critical SOC functions, all based on AI and automation. Whether you're exploring the benefits of a next-generation SIEM, intrigued by the benefits of modern SOAR, or are ready to create the complete foundation of an advanced SOC, FortiSIEM and FortiSOAR offer unique benefits as an integrated SOC platform or as independent components of a multivendor SOC solution.



When used together, FortiSIEM and FortiSOAR can improve security team productivity by over 90%.[1]

FortiSIEM and FortiSOAR Offer Essential SecOps Functions

FortiSIEM and FortiSOAR use AI and automation to provide critical threat detection, investigation, and response capabilities and the full range of essential security operations functions across the multivendor IT/OT security infrastructures of today's enterprise.

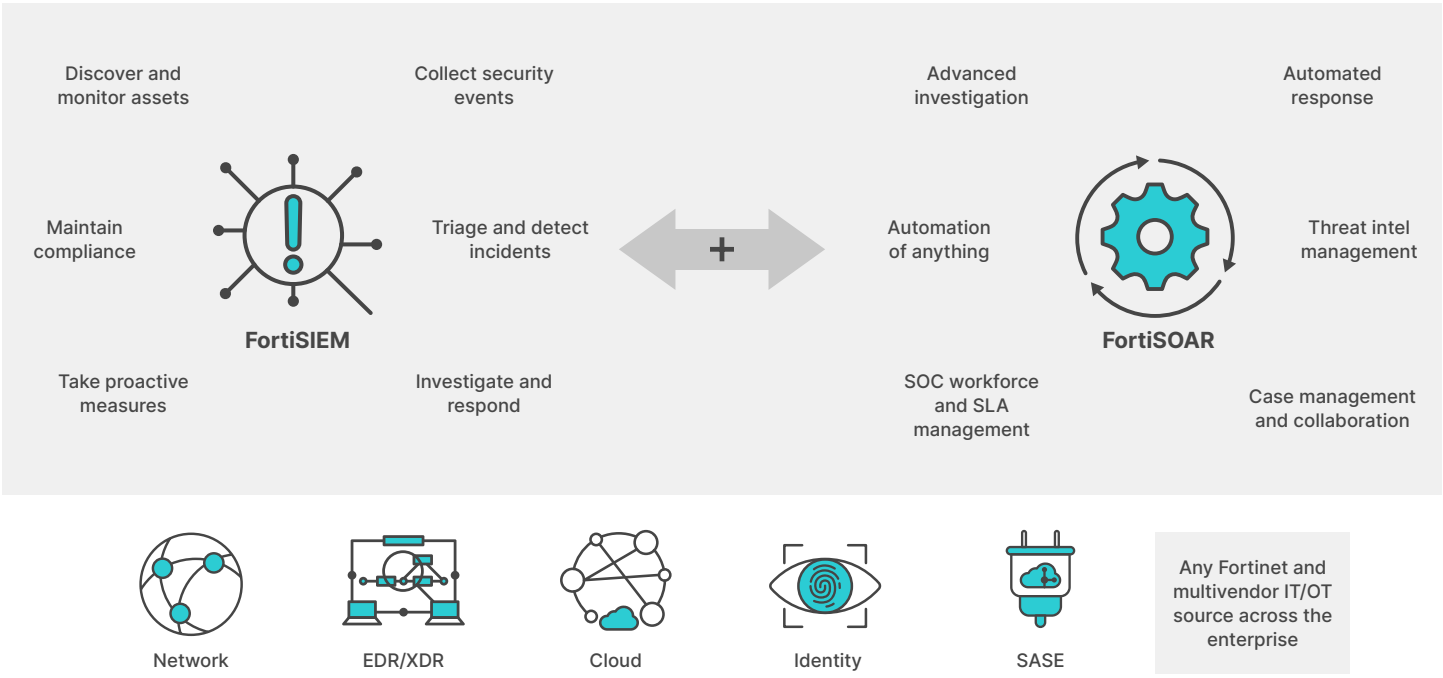


Figure 1: FortiSIEM and FortiSOAR provide essential security operations functions.

How FortiSIEM Works

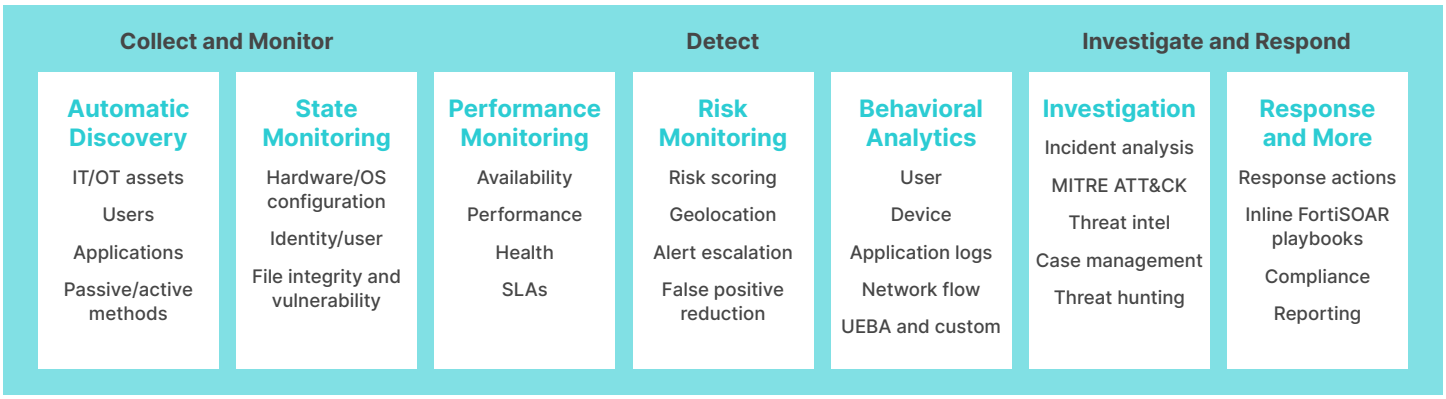


Figure 2: FortiSIEM monitors enterprisewide events, detects threats, and allows for rapid investigation and response.

FortiSIEM provides a complete SIEM feature set and unique capabilities spanning network operations center (NOC), SOC, and IT/OT security use cases. The intuitive user experience supports all aspects of threat investigation and response, threat hunting, and robust compliance validation and reporting. The highly scalable platform is available as an integrated hardware appliance, software virtual machine, and an AWS-hosted SaaS offering. Key features include:

- Configuration management database
- IT/OT asset discovery and monitoring
- User and entity behavior analytics
- GenAI analyst assistance
- Dynamic user identity mapping
- Risk-based scoring and incident management
- Embedded integration to FortiSOAR
- Scalable, multitenant architecture

How FortiSOAR Works

FortiSOAR centralizes, standardizes, and automates IT/OT security and NOC operations. With broad integrations, rich use-case solutions, hundreds of playbooks, and full SecOps management features, FortiSOAR is the enterprise and MSSP SOC's operating foundation. The highly scalable platform is available as on-premises and cloud-deployable software and as a FortiCloud-hosted SaaS offering. Key features include:

- 600+ integrations and 800+ playbooks
- Complete incident management
- Threat intelligence management
- GenAI analyst assistance
- ML-based recommendation engine
- No/low-code playbook creation
- SOC staff and SLA management
- Scalable, multitenant architecture

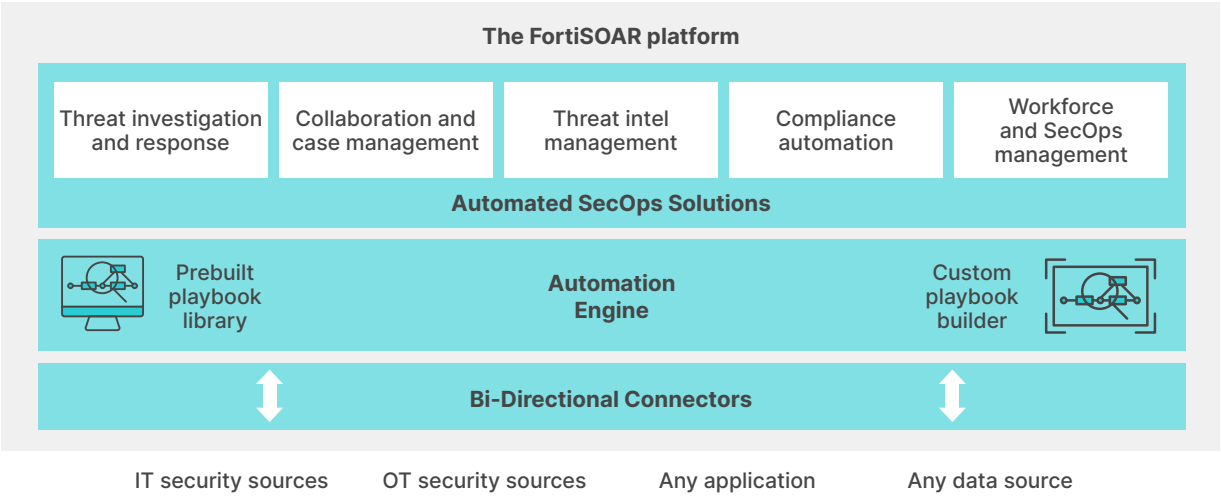


Figure 3: FortiSOAR automates and optimizes key SOC activities.

Key Features of Using FortiSIEM and FortiSOAR Together

When used together, security teams can take advantage of the many features of FortiSIEM and FortiSOAR, such as:

GenAI assistance

The FortiAI generative AI assistant is embedded in FortiSIEM and FortiSOAR to guide, simplify, and automate security analyst activities, such as investigating and responding to incidents, running SIEM queries and reports, and creating SOAR playbooks.

- ☑ Analyze this incident and tell me what action to take.
- ☑ Tell me about this malware and the attackers who use it.
- ☑ What response playbooks do you recommend for this alert?
- ☑ Create a report of events per critical incident of the last 30 days.
- ☑ Build a playbook to hunt for IOCs from this attack campaign.

Easy integration with the Fortinet Security Fabric and third-party security technologies

FortiSIEM and FortiSOAR offer hundreds of multivendor connections and provide unique benefits to customers who have adopted other Fortinet products. When combined with other Fortinet offerings, customers benefit from FortiGuard threat intelligence services, unique integration levels, cross-product functions, and automation capabilities, adding powerful threat detection and SecOps capabilities.

Consolidated IT/OT security

FortiSIEM and FortiSOAR support various OT-specific functions that enable customers to protect OT assets using standard IT security operations technologies and processes. For example, FortiSIEM includes OT asset discovery and monitoring and CMDB support. Both products feature Purdue and MITRE ATT&CK ICS mapping and integration with leading OT security products.

MSSP features and greater flexibility

FortiSIEM and FortiSOAR are designed to support the performance, scalability, and resiliency demanded by large enterprises and service provider organizations. Distributed processing, multitenancy, flexible deployment options, and dedicated MSSP features are among the many reasons that leading MSSPs and large-scale enterprise organizations use FortiSIEM and FortiSOAR as the backbone of their operations.

FortiSIEM and FortiSOAR Deployment Options

FortiSIEM and FortiSOAR give you the benefits of full automation with the option of choosing where to conduct incident management. Many organizations prefer that their analysts perform incident investigation and response in FortiSOAR, while others prefer the focus to be FortiSIEM, and others may vary based on incident characteristics. With natively integrated FortiSOAR playbooks available in FortiSIEM, you'll have robust, automated threat detection and response capabilities and much more, no matter your choice.

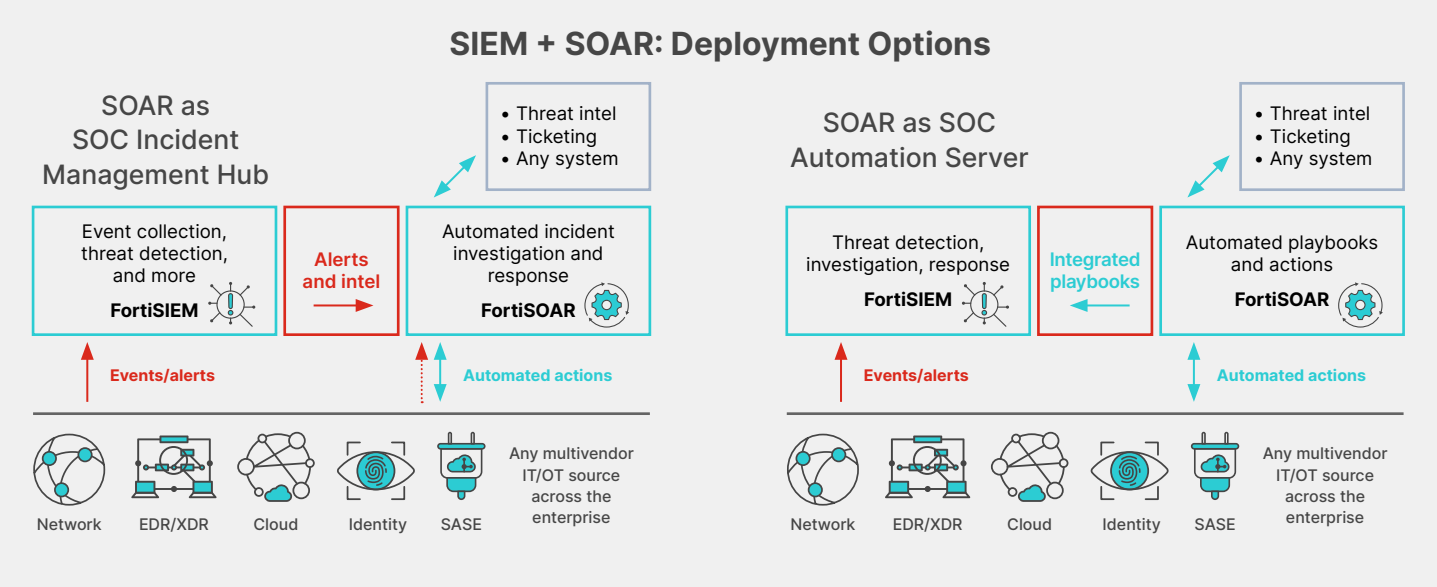


Figure 4: FortiSIEM and FortiSOAR deployment options

Get Started with FortiSIEM and FortiSOAR Today

Whether you adopt a complete SOC platform, FortiSIEM, or FortiSOAR, you'll see a profound improvement in threat investigation, response, and overall security operations.

Adopting FortiSIEM and FortiSOAR provides a complete, next-generation SOC platform that leverages AI and automation to optimize your attack defense and end-to-end SOC operations.

Replacing a legacy SIEM or log analysis tool with FortiSIEM offers advanced IT/OT threat detection, greater analyst effectiveness, more scalability, lower total cost of ownership, and much more.

Extending your FortiSIEM investment with FortiSOAR integrated playbooks brings powerful automation to your investigation and response processes, driving rapid attack identification and response and expediting any SOC task.

Enhancing your SIEM investment with FortiSOAR can centralize, standardize, and automate all analyst tasks, improving SOC operations and enabling analysts to focus on critical activities.

Security Task	Baseline (Manual Operations)	Fortinet CARA Technologies
Time to investigate threats	6 hours	1 minute
Time to remediate threats	12.5 hours	5–10 minutes

Figure 5: FortiSIEM and FortiSOAR together improve SOC threat response.

FortiSOAR can enhance threat investigation and response activities and standardize and automate almost any SOC activity across a multivendor environment or the Fortinet Security Fabric platform.

Maximize Your ROI with FortiSOAR		
Steps	**Manual**	**FortiSOAR**
Enrich artifacts to identify IOCs	45 to 60 minutes	3 minutes
Perform triaging on events from SIEM	20 minutes	1 minute
Submit a zip to the detonation engine	1 hour to 6 hours	1 minute
Isolate affected devices	10 minutes	1 minute
Analyze, create, and annotate an incident	60 minutes	5 minutes
Block IOCs on a firewall (e.g. FortiGate)	45 minutes to 2 hours	2 minutes
Remediation and incident reponse	60 minutes to 6 hours	5 minutes
Prepare and send an incident summary report	2 to 3 hours	2 minutes
TOTAL	**4.5 to 15 hours**	**20 minutes**

Figure 6: FortiSOAR automates and speeds investigation and response.

To learn more, read an overview of Fortinet Security Operations or review the FortiSIEM and FortiSOAR data sheets.

[1] Aviv Kaufmann, The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, August 1, 2023.

FORTINET

www.fortinet.com

April 4, 2024 12:55 PM

2587872-0-0-EN