SOLUTION BRIEF

Choose the Fortinet SOC Platform for Unified Threat Response

Executive Summary

Security operations teams of all sizes face alert overload, tool-switching inefficiencies, an abundance of manual processes, and fragmented threat data, limiting their ability to rapidly identify and mitigate critical threats. In today's world of sophisticated ransomware, AI-driven campaigns, and determined threat actors, overcoming these common hurdles is key to minimizing your risk of a breach.

Fortinet provides a unified threat response product suite that employs advanced detection, automation, and GenAI assistance to rapidly identify, investigate, and respond to the threats that matter. These products work together and independently to enable security teams of any size or maturity to deliver the most effective and efficient protection to their organization.

Organizations that adopt Fortinet security operations solutions experience up to a 99% improvement in security team productivity.[1]

The Unified Threat Response Solution

FortiAnalyzer, FortiSIEM security information and event management, and FortiSOAR security orchestration, automation, and response together form a unified threat response capability designed to meet the evolving needs of any business. Whether you have a smaller IT and security team and are looking for a turnkey Fortinet-focused solution or have a dedicated security operations center (SOC) ready to harness the full power of SIEM and SOAR, the unified threat response suite is designed to meet your needs today and tomorrow.

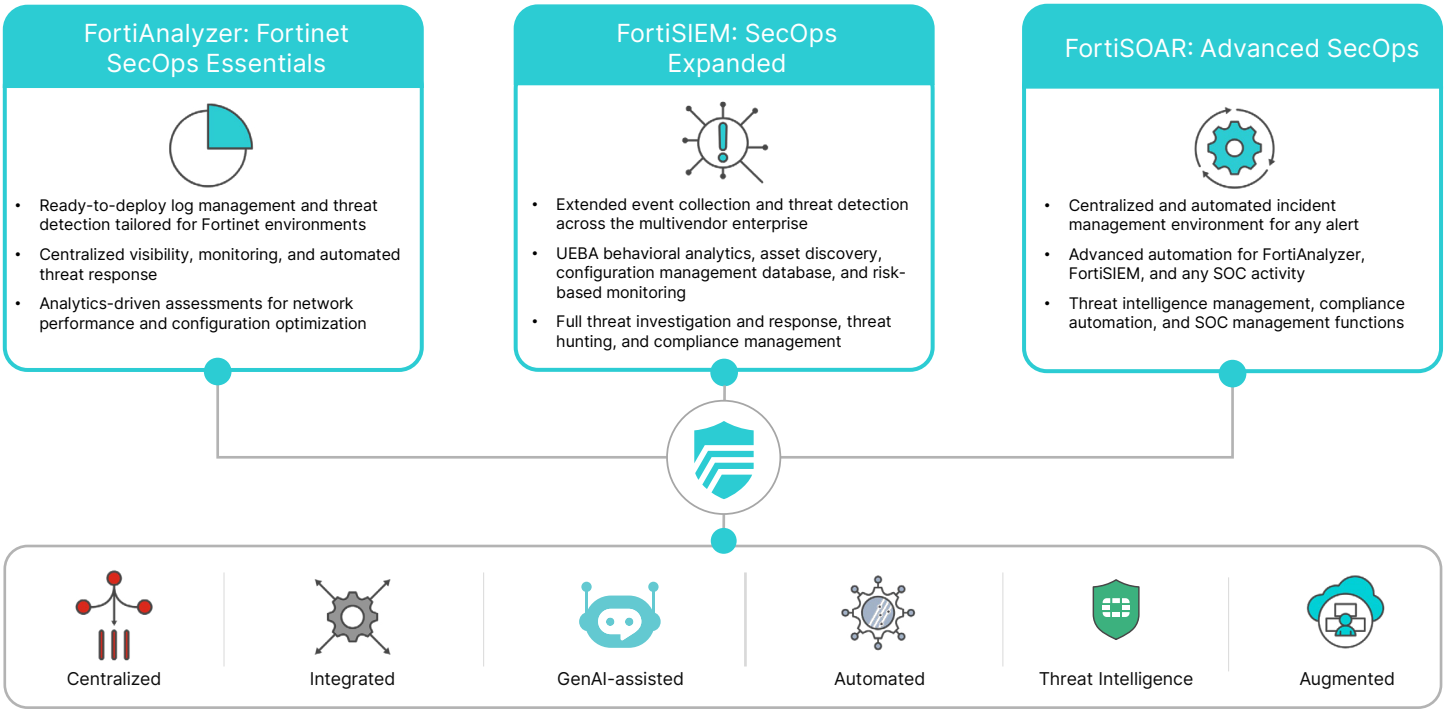


Figure 1: Fortinet offers a unified threat response solution.

FortiAnalyzer Overview

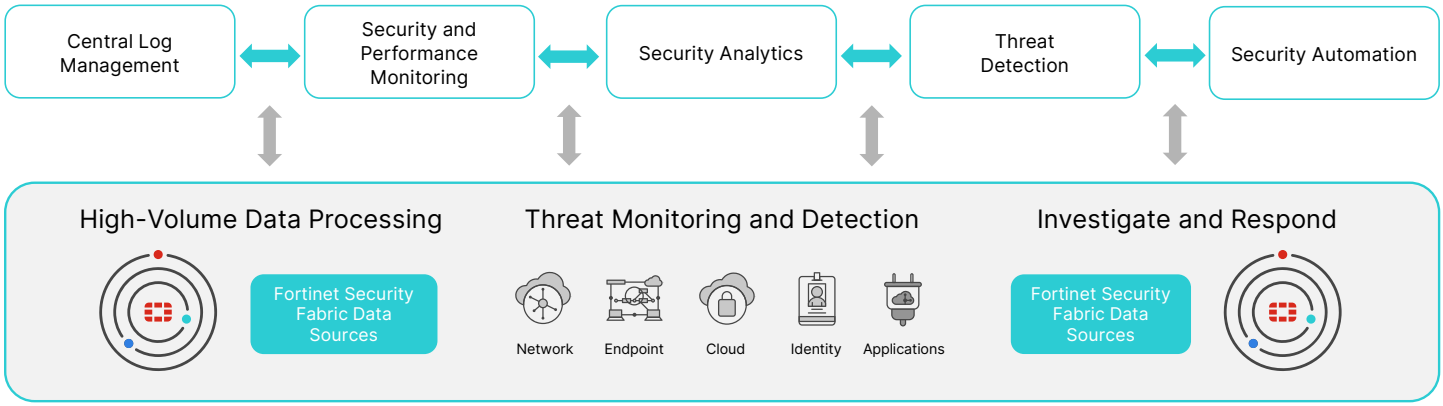


Figure 2: FortiAnalyzer provides monitoring, threat detection, and remediation across the Fortinet Security Fabric.

FortiAnalyzer is the Fortinet Security Fabric data lake, providing log aggregation, analysis, and event correlation. It unifies configurations, events, and alerts into a single view, enhancing threat detection, analysis, and management. FortiAnalyzer streamlines the deployment process, requiring minimal configuration, and lays the groundwork for security operations. Offering analysts broader detection capabilities and smarter responses that scale as their business grows, FortiAnalyzer offers threat detection and response backed by FortiGuard Labs rich threat intelligence. Key features include:

- Centralized log aggregation and analysis
- Seamless Fortinet Security Fabric integration
- Real-time threat detection and analytics
- Native threat intelligence
- Minimal configuration deployment
- GenAI assistance for complex tasks
- Security automation with prebuilt content

FortiSIEM Overview

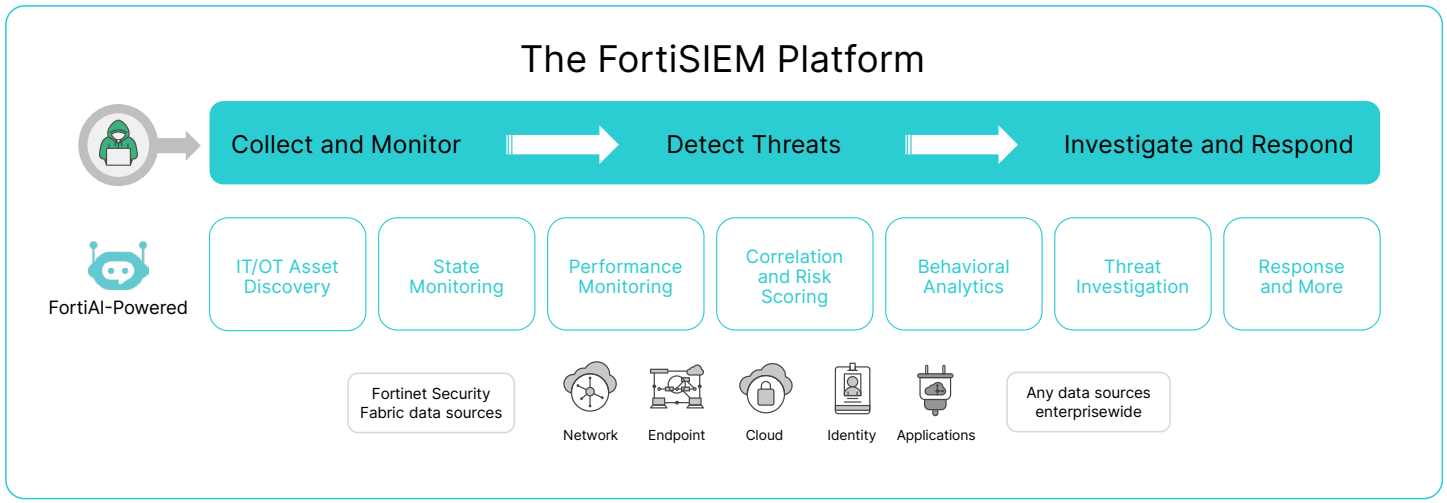


Figure 3: FortiSIEM provides enterprisewide threat detection, investigation, and response.

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 interface 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
- Native FortiSOAR automation
- Scalable, multitenant architecture

FortiSOAR Overview

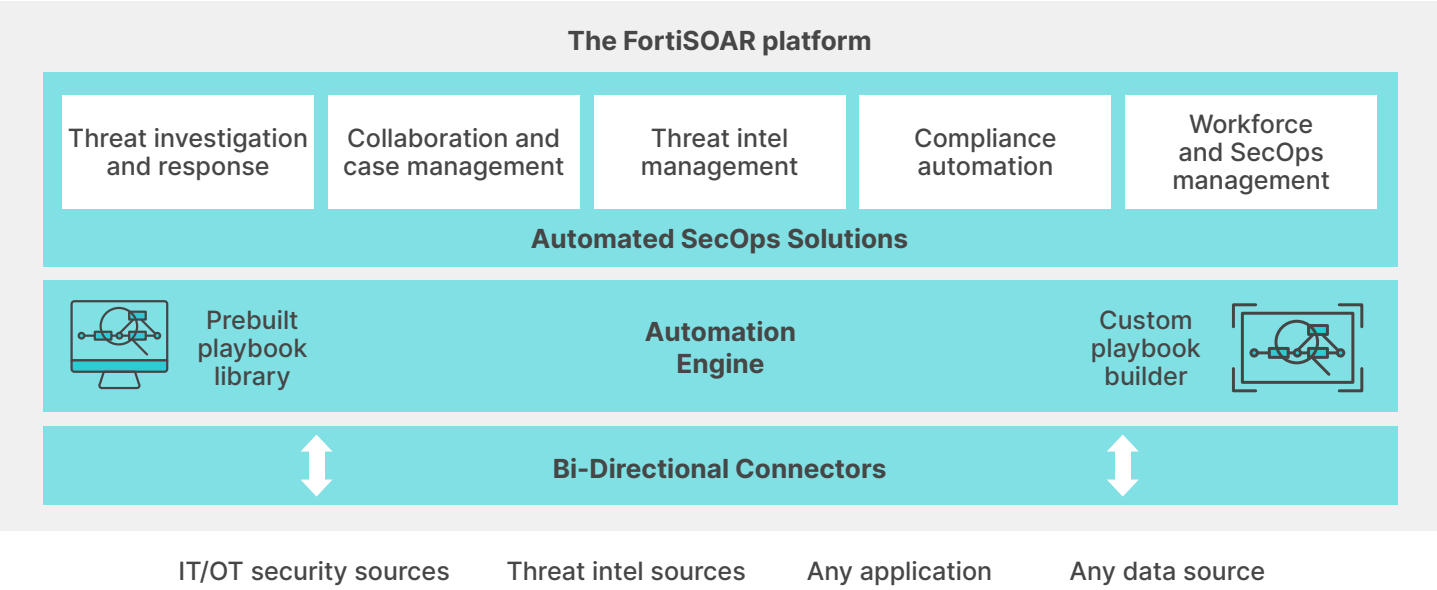


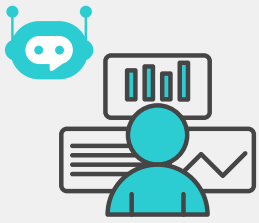
Figure 4: FortiSOAR automates and optimizes key SOC and NOC activities.

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 operating foundation of the enterprise and managed security service provider's (MSSP) SOC. 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

Leveraging GenAI in Fortinet Solutions

The FortiAI assistant is embedded in FortiAnalyzer, FortiSIEM, and FortiSOAR to guide, simplify, and automate security analyst activities, such as investigating and responding to incidents, threat hunting, reporting, and much more.



- ☑ 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.

Figure 5: These are examples of actions driven by FortiAI.

Integrating Fortinet Products and Solutions Across the Enterprise

FortiAnalyzer provides deep integration and functionality for Fortinet Security Fabric products. FortiSIEM and FortiSOAR provide your SOC with complete visibility and threat detection for multivendor security products, enterprise systems, databases, and threat intelligence sources across any environment. Below are several benefits of using all three products together:

Consolidated IT/OT security

When using these solutions, you gain support for various OT-specific functions that enable the protection of OT assets using standard IT security operations technologies and processes and featuring Purdue and MITRE ATT&CK ICS mapping, as well as integration with leading OT security products (FortiSIEM and FortiSOAR only).

MSSP features and flexibility

The products are designed to scale to support the performance 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 FortiAnalyzer, FortiSIEM, and FortiSOAR as the backbone of their operations.

Managed service options

FortiGuard SOC-as-a-Service is a managed services offering for FortiAnalyzer, providing 24×7 monitoring, threat detection, response guidance, and more. FortiSIEM and FortiSOAR managed services are available through Fortinet partners around the world.

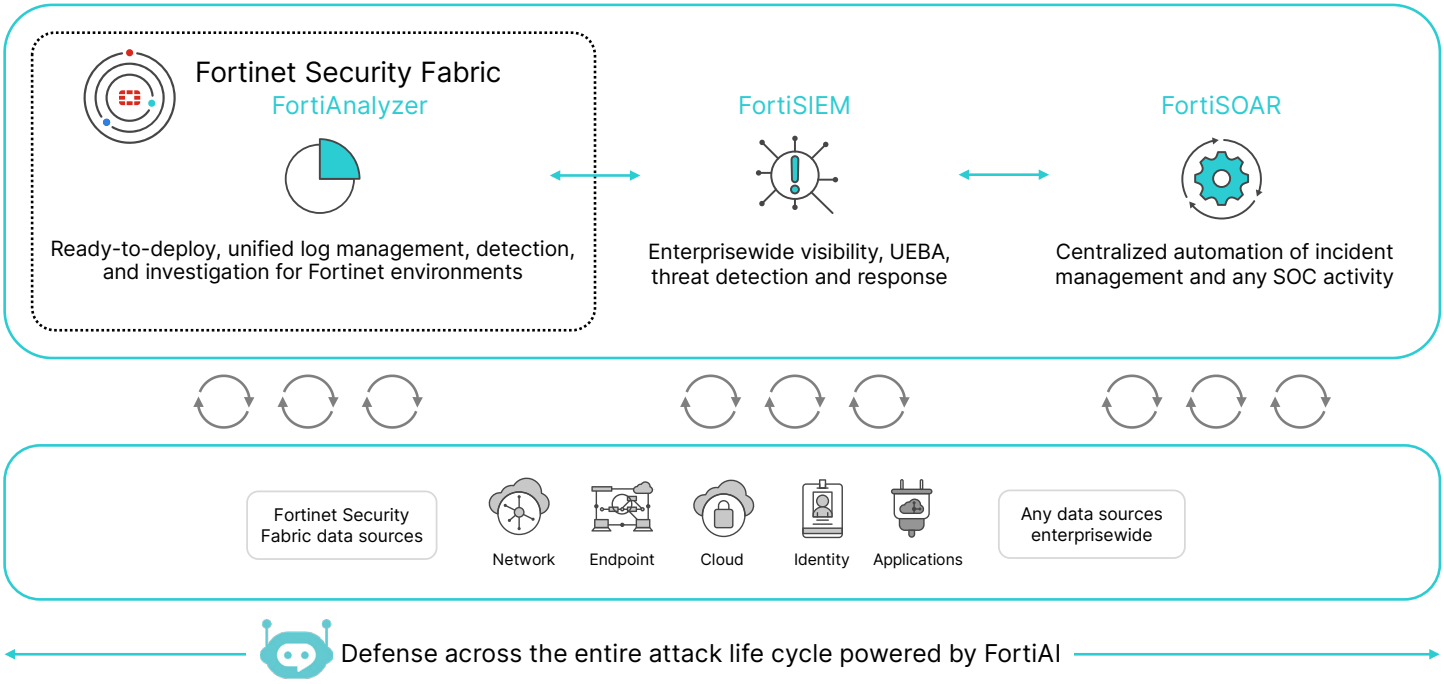


Figure 6: Organizations can leverage AI across Fortinet solutions.

The Path to AI-Powered Security Operations

Fortinet unified threat response products meet the evolving needs of any security and IT team. From the out-of-the-box functionality of FortiAnalyzer to the enterprisewide detection and automation capabilities of FortiSIEM and FortiSOAR, the products provide unique standalone value and a tightly integrated SOC platform.

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

FORTINET

www.fortinet.com

September 5, 2024 11:12 AM / 2817642-0-0-EN