SOLUTION BRIEF

# Unify Security Operations with the Fortinet SOC Platform

## Executive Summary

Attackers are more determined and resourceful than ever. Whether you have a lean security team or a fully staffed advanced security operations center (SOC), security depends on your team's ability to detect and rapidly respond to advanced threats. The most useful technology and services will vary by strategy, staffing, and security maturity. All teams need advanced threat detection and response. Still, some will benefit most from simplicity and automation of operation, others from the sophistication of SIEM and SOAR, and many from staff augmentation or outsourcing via managed services.

With the Fortinet SOC platform, security teams of any size can swiftly identify and respond to threats using advanced detection, automation, and generative AI (GenAI) assistance. With flexible solutions tailored to both turnkey and advanced SOC operations backed by expert managed security services, Fortinet solutions can meet the security needs of any organization. The Fortinet SOC platform delivers these capabilities to match how an organization's security maturity evolves over time. Whether starting from essential monitoring or scaling to an advanced SOC, the Fortinet SOC platform provides a unified foundation for detection, triage, investigation, response, and continuous operational improvement.

**Fortinet SOC Platform Results**

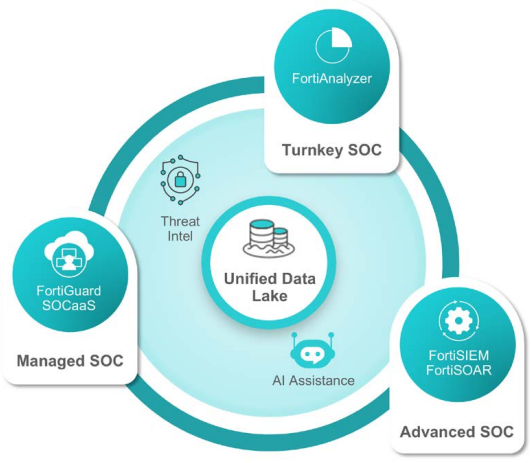
**76%**
reduction in cyber incidents

**45%**
reduction in response time

**7x**
improvement in threat detection[1]

## The Fortinet SOC Platform

The Fortinet SOC platform has been designed to protect against attackers who can exploit vulnerabilities within days of disclosure, execute billions of automated scans, and use AI for sophisticated social engineering, malware generation, and deepfake impersonation. It combines FortiAnalyzer, FortiSIEM, FortiSOAR, and FortiGuard SOC-as-a-Service into a unified operating layer. These solutions can be deployed individually or as an integrated system, enabling organizations to start with turnkey analytics and baseline automation with FortiAnalyzer, scale to a multivendor SIEM and full SOAR orchestration, and opt for managed services assistance at any point. The SOC platform consolidates telemetry, analytics, AI reasoning, and automation across IT, operational technology (OT), endpoint, cloud, and identity controls to enable early detection, streamline investigation, and reduce investigation and remediation from hours to minutes.




**Fortinet SOC Platform**

Unified threat detection and response for any size organization

Figure 1: The Fortinet SOC platform

## FortiAnalyzer: Turnkey SOC for Resource-Constrained Teams

As the unified data lake of the Fortinet Security Fabric, FortiAnalyzer provides a streamlined, scalable entry point for building or expanding a SOC by centralizing logs, alerts, configurations, and incidents into a single source of truth. It consolidates networking and security telemetry, enabling earlier detection through automated correlation, intuitive threat topologies, and real-time threat intelligence from FortiGuard Labs, including outbreak detection and indicator-of-compromise tracking.

FortiAnalyzer includes built-in SOC automation and baseline SIEM, SOAR, and XDR capabilities. It also includes ready-to-deploy content packs, updated monthly by Fortinet experts so that teams can expand their SecOps coverage without increasing engineering overhead. FortiAI-Assist is embedded in FortiAnalyzer and provides GenAI and agentic AI guidance for investigation, summarization, and workflow acceleration, enabling faster, more confident actions. Delivered as an appliance, virtual machine, or cloud service, FortiAnalyzer provides a modern, lightweight SOC foundation that improves threat management efficiency without adding operational complexity.


Figure 2: Fortinet FortiAnalyzer

## FortiSIEM: Advanced Threat Detection and Response for the Enterprise

Protecting a modern enterprise that operates across a dynamic infrastructure spanning on-premises data centers, cloud resources, and distributed offices and employees requires the enterprisewide visibility, advanced threat detection, automated incident management, and the flexibility and scalability of a modern SIEM.

FortiSIEM delivers centralized IT and OT event visibility, advanced detection analytics, and incident management designed to meet the demands of enterprise SOC teams. Featuring rich prebuilt content, a unique configuration management database, built-in SOAR automation, threat intelligence, and GenAI assistance, FortiSIEM speeds detection, investigation, and response while providing the flexibility and scalability required by organizations and service providers.

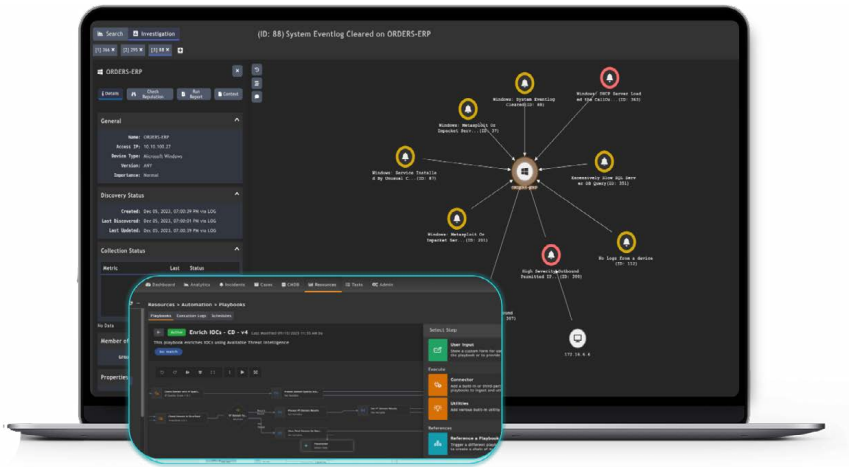



Figure 3: Fortinet FortiSIEM

## FortiSOAR: Providing the Power and Efficiency of SecOps Automation

A mature enterprise SOC encompasses much more than threat detection and response. Vulnerability management, threat intelligence, proactive threat hunting, pen testing, and detection engineering are core responsibilities often carried out by specialized teams. For SOC efficiency and effectiveness, centralizing and automating functions across a complex security infrastructure is a necessity.

FortiSOAR centralizes, standardizes, and automates IT and OT security and enterprise operations. It features more than 1,000 multivendor integrations and prebuilt playbooks. It also includes GenAI-assisted playbook creation and rich use-case solution packs, including automation and management for incident response, threat intelligence, vulnerabilities, compliance actions, OT security, and IT and network operations center operations. These FortiSOAR capabilities are available out of the box along with flexible customization, creating a SOC operating foundation for enterprises and MSSPs.

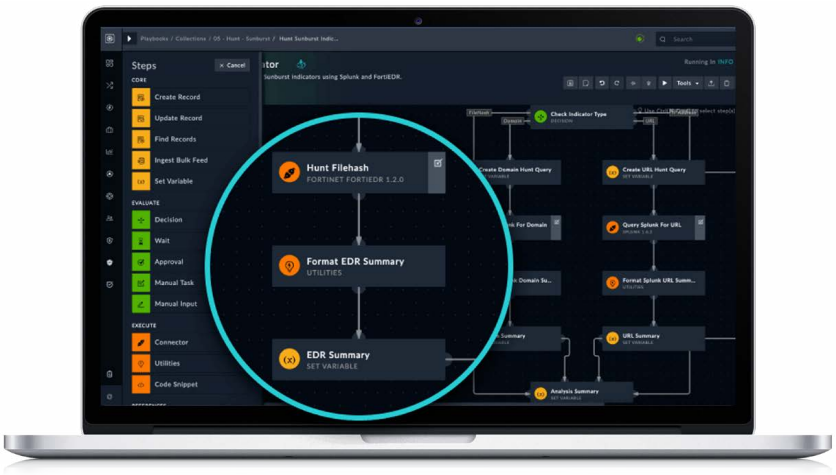



Figure 4: Fortinet FortiSOAR

### SOC Platform Benefits

- **Start anywhere:** From the lean team to the advanced SOC and from in-house to outsourced
- **Automate anything:** Built-in GenAI and SOAR automation power efficient operations
- **Deploy with flexibility:** Flexibility and economical total cost of ownership, whether deployed on-premises, private cloud, or SaaS

## FortiGuard SOCaaS: 24×7 Support

Distributed workforces and cloud-first operations create continuous security exposure, including during nights, weekends, and holidays when adversaries often strike. Building an internal SOC requires expensive technology, mature processes, and highly trained analysts that many organizations, MSSPs, and enterprises often struggle to resource at scale. FortiGuard SOCaaS provides around-the-clock threat monitoring, AI-driven alert triage, and expert-led incident escalation powered by the Fortinet SOC platform, eliminating the overhead of building and running a SOC in-house.

FortiGuard SOCaaS analyzes alerts using advanced AI, machine learning, and Fortinet's global analyst expertise to quickly reduce noise and identify true threats. Confirmed incidents are escalated with prioritized guidance in as little as 15 minutes, and customers can access a unified portal for real-time visibility, analyst communications, trend insights, and reporting. FortiGuard SOCaaS is designed for organizations that lack after-hours monitoring or full SOC staffing. It reduces false positives by up to 85% while accelerating time-to-value and strengthening security without expanding staff.[2]

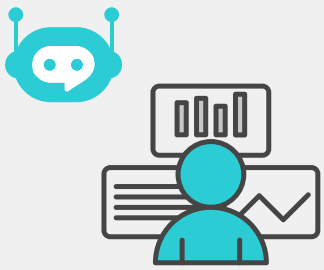

Figure 5: FortiGuard SOCaaS

## FortiAI-Assist GenAI: AI Embedded Across the SOC Life Cycle

Fortinet integrates FortiAI-Assist GenAI across every layer of the SOC platform to enhance detection accuracy, speed investigations, and reduce analyst workload. It assists analysts by interpreting logs, artifacts, anomalies, and attack sequences. It can generate investigations, write queries, assemble timelines, and produce analyst-grade summaries.

Trained on Fortinet's global telemetry, threat intelligence, and SOC workflows, FortiAI-Assist has domain specificity that general-purpose AI systems lack. Integrated natively across FortiAnalyzer, FortiSIEM, FortiSOAR, and SOCaaS, FortiAI-Assist accelerates:

- Multisurface incident reconstruction
- Exposure and vulnerability analysis
- Playbook creation and workflow design
- Threat hunting and hypothesis testing
- Reporting, ticketing, and executive summaries



- 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 6: FortiAI-Assist

## Solutions to Meet Evolving Needs

Fortinet offers a continuous security maturity path that extends to advanced SOC solutions. From managed security services to SOC products tailored to security teams of all sizes, the Fortinet SOC platform delivers solutions that meet the evolving needs of any organization.

Whether you're an organization seeking a turnkey solution, a large enterprise or MSSP with advanced requirements, or you need expert security services to augment or manage your SOC, the Fortinet SOC platform can meet your needs.

[1] Enterprise Strategy Group, The Quantified Benefits of Fortinet Security Operations Solutions, January 2025. https://www.fortinet.com/content/dam/fortinet/assets/reports/esg-economic-validation-fortinet-automated-soc.pdf

[2] Ibid.





December 11, 2025 2:45 AM / MKTG-2634-0-0-EN