SOLUTION BRIEF

Fortinet FortiSOC: Unify SOC Operations and Accelerate Response with Agentic AI

Executive Summary

Security teams are under pressure from faster attacks, broader attack surfaces, and a growing volume of investigations. At the same time, many organizations still struggle to operationalize SecOps because their tools, workflows, and fragmented operating models lack centralization and the power of agentic AI and automation.

FortiSOC is designed to change that. It delivers a unified SaaS offering that brings together SIEM, SOAR, identity threat detection, threat intelligence, and more into a single platform experience powered by agentic AI. Through tiered capability subscriptions, a single console, and embedded best-practice workflows, FortiSOC helps teams of any size move from alert to investigation to response with more automation, less friction, fewer handoffs, and faster response to attacks.

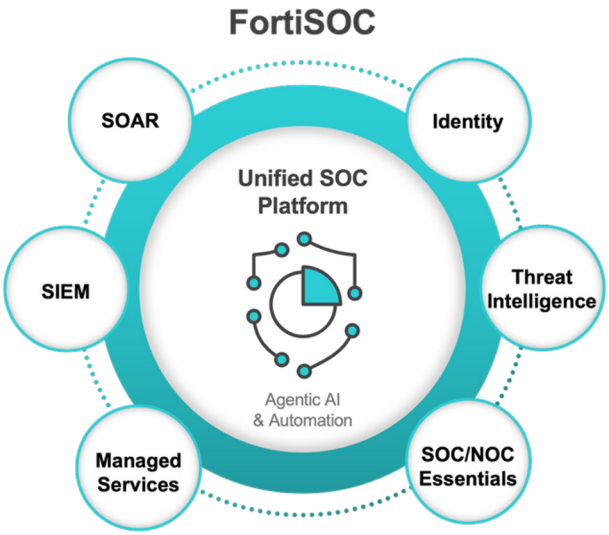

Figure 1: FortiSOC

Why FortiSOC

FortiSOC unifies detection, investigation, automation, threat intelligence, and identity threat detection together in a single SaaS platform, enabling security teams to move beyond fragmented SOC operations. Powered by agentic AI and embedded best-practice workflows, FortiSOC gives teams a faster, more consistent way to investigate alerts, prioritize threats, and execute responses across any environment.

FortiSOC Benefits

- **Reduce complexity, accelerate response:** FortiSOC consolidates key SOC capabilities and AI-driven operations to reduce tool sprawl, simplify operations, and improve analyst efficiency.
- **The power of AI SOC:** Agentic AI and thousands of SOAR playbooks power autonomous functions, automatically investigate alerts, and guide and execute remediation and other tasks.
- **Built to connect, designed to secure:** Bidirectional integration across Fortinet and third-party environments centralizes detection and response across security, IT, and business systems.
- **Ready on day one and beyond:** Continual intelligence and content for detections, playbooks, and more from FortiGuard Labs and Fortinet SOC operations keep your defense up to date.
- **Start anywhere, scale everywhere:** FortiSOC supports turnkey SOC adoption, modernization initiatives, and advanced operations with a unified platform architecture.

Key FortiSOC Capabilities and Features

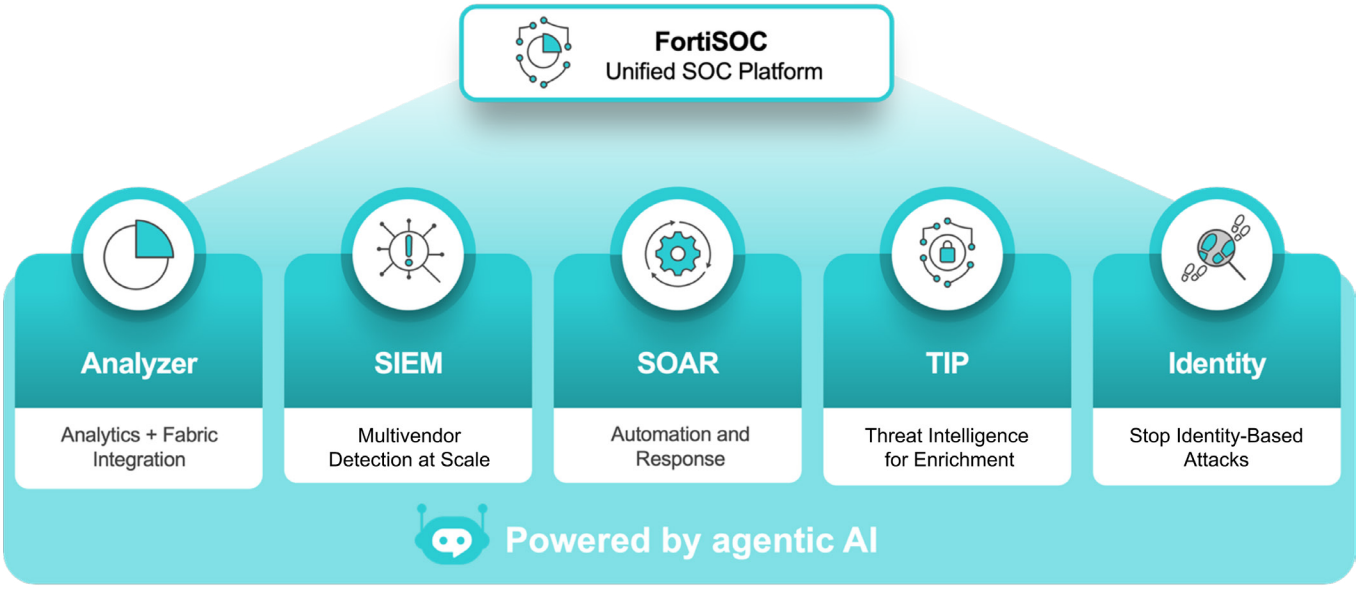

Figure 2: FortiSOC Unified SOC Platform

What is FortiSOC?

FortiSOC is an advanced cyber defense and a comprehensive SaaS platform designed to be the foundation of modern SOC operations. FortiSOC unifies and extends Fortinet's best-in-class SOC technologies—FortiAnalyzer, FortiSIEM, FortiSOAR, FortiTIP, and FortiAI-Assist. It adds best-practice content and workflows from Fortinet's SOC operations and provides FortiGuard Labs threat intelligence and monthly content updates, delivering immediate and lasting value. FortiSOC is not a portal for separate products. It integrates proven Fortinet capabilities into a single, unified platform and user experience that serves a wide range of customers. Flexible capability subscriptions support turnkey SOC, advanced SOC, and NOC/IT essentials, enabling growth for customers of all sizes and maturity levels as requirements evolve.

How FortiSOC works

FortiSOC operates on a common data pipeline that ingests telemetry from multivendor network, endpoint, cloud, and identity sources, then normalizes, enriches, and correlates it once, so detections, analytics, and workflows operate on the same dataset. The data is mapped to a shared schema, enabling consistent analysis and response across users, devices, applications, and sessions without requiring cross-tool reconciliation.

Correlation is enriched with FortiGuard Labs and any other threat intelligence sources, including indicators, reputation, and campaign context, and is applied across both rule-based detections and behavioral analytics. With this processing centralized, alerts become part of a continuously updated activity graph that maps relationships among users, assets, and observed behaviors, providing consistent context for investigation and response.

Agentic AI and thousands of SOAR playbooks power autonomous functions, automatically investigating alerts and, per customer preference, guide and even execute remediation. Analysts can pivot from an alert to a broader investigation context, including timelines, related events, affected assets, and prior activity, with guidance from agentic AI. Response actions are executed through integrated agentic SOAR workflows that can trigger containment steps such as isolating endpoints, blocking indicators, updating policies, or initiating ticketing and escalation.

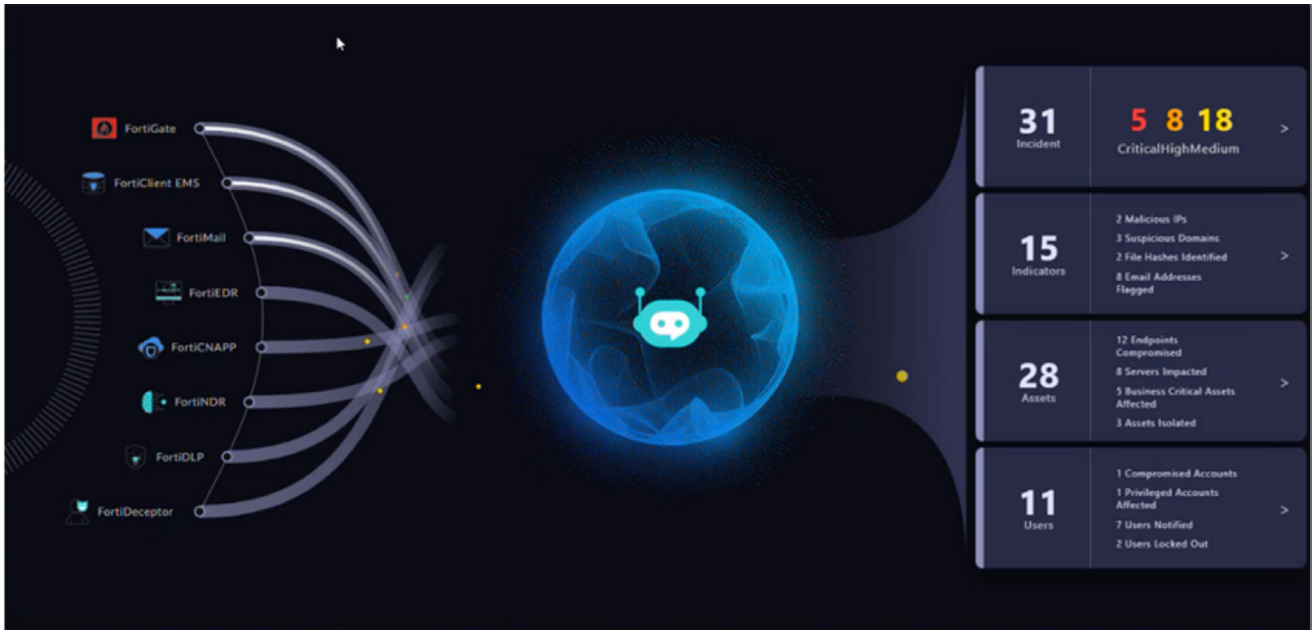

Figure 3: FortiSOC security posture overview

Aligned with Evolving SOC Requirements

SecOps continues to move toward more integrated, platform-based approaches that unify detection, investigation, and response. At the same time, cloud delivery has become the default for new deployments, and agentic AI is increasingly embedded directly in operational workflows.

FortiSOC aligns with these requirements by delivering a unified, AI-driven SaaS platform built on Fortinet's integrated architecture. Because these capabilities are designed to work together natively, data, workflows, and intelligence remain consistent across the platform rather than relying on post-deployment integration.

Built for Every Stage of the SOC Journey

SecOps does not follow a single model. Some organizations are building their first SOC capability. Others are standardizing and scaling mature operations. Still others are expanding into managed services. FortiSOC is designed to support SOC teams at different stages without requiring them to re-architect their environment.

FortiSOC supports organizations at every stage of SOC adoption, from resource-constrained teams establishing foundational monitoring capabilities to highly sophisticated SecOps teams that require deeper automation, broader correlation, and AI-assisted investigation at scale. For customers seeking to augment or outsource their SOC operations, FortiSOC is also available as a managed service through the FortiGuard SOC-as-a-Service offering.

FortiSOC Core delivers turnkey SOC detection and response, along with network monitoring, focused primarily on the Fortinet Security Fabric. It includes agentic AI, playbook automation, and FortiGuard Labs threat intelligence. FortiSOC Advanced builds on FortiSOC Core to add full multivendor integration, UEBA, identity-based detection, additional advanced detection methods, and full SOAR automation.

FortiSOC Subscription Options

Key Features	Description	Core Tier	Advanced Tier
Log/Event Ingestion	Fortinet and limited third party	☑	☑
	Full multivendor ingestion	-	☑
IT/OT Detection Analytics	Fortinet Fabric-focused analytics	☑	☑
	UEBA, advanced SIEM analytics	-	☑
Identity Threat Detection	Identity-based detection rules and response playbooks	-	☑
Agentic AI	FortiAI-Assist AI agents to automate or aid in any task	☑	☑
SOAR Automation & Content Hub	Playbook editor, default playbooks	☑	☑
	Curated content packs and connectors with monthly updates	☑	☑
	Full content access and advanced SOAR functions	-	☑
Threat Intelligence Management	Native FortiGuard Labs Intelligence plus full threat intel management capabilities	☑	☑
Configuration Management Database	IT/OT asset discovery, classification, and health monitoring	-	☑
Case Management	Built-in incident tracking, collaboration, and workflows	☑	☑

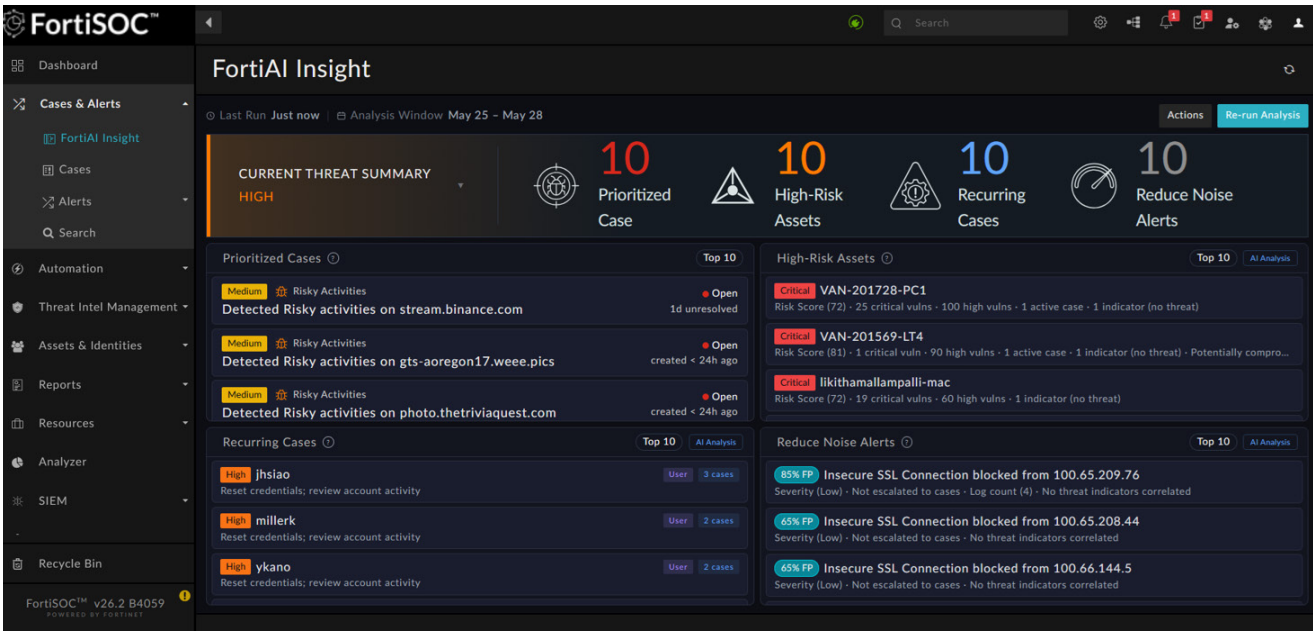

Figure 4: FortiSOC agentic AI insight dashboard

Expanding the Fortinet SOC Platform Portfolio

FortiSOC expands Fortinet's SOC platform portfolio by introducing a unified SaaS option for organizations seeking an integrated, cloud-delivered operating model. At the same time, FortiAnalyzer, FortiSIEM, and FortiSOAR remain key components of the portfolio and continue to be available as standalone solutions for organizations that need product-level flexibility, bespoke deployment models, or more tailored architectures.

That flexibility matters because SOC teams do not all start from the same place or have the same requirements. Fortinet supports both approaches: a unified SaaS platform for teams seeking a more streamlined path and standalone products for organizations that want to build and scale in different ways.

A Practical Path Forward

Modern security operations increasingly rely on data-driven, automated processes that preserve context across the environment and enable teams to act faster and more consistently. FortiSOC brings these capabilities together in a single platform that simplifies operations without sacrificing flexibility, giving organizations a practical way to strengthen and scale security operations over time.

June 15, 2026 10:07 AM / MKTG-3666-0-0-EN