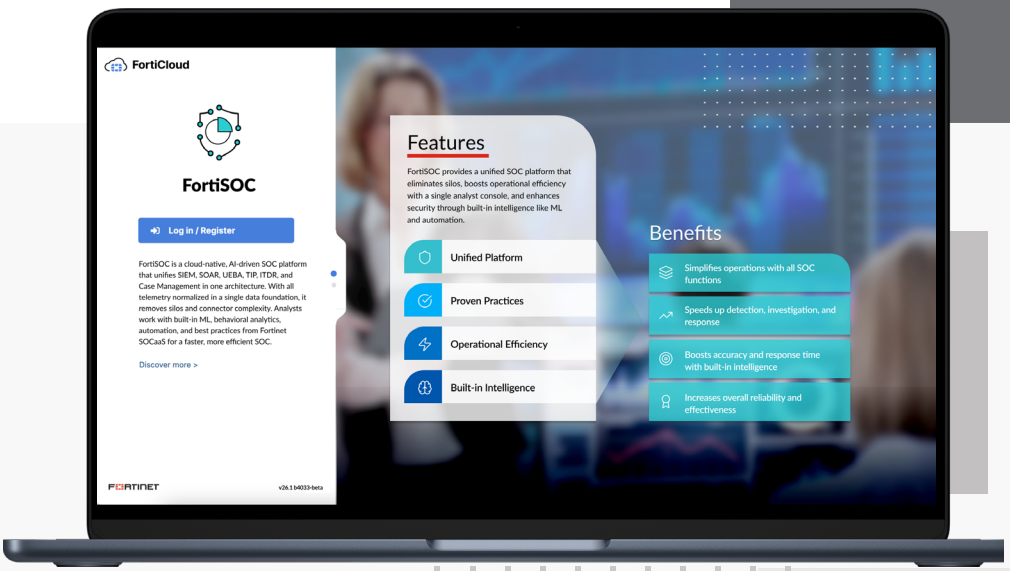
FortiSOC

The Unified, AI-driven Cloud SOC Platform

Available in:

Cloud



Highlights

- Unified Operations: SIEM, SOAR, UEBA, TIP, ITDR, Case management.
- Single data model & console - no silos, no stitching.
- Simple subscription licensing.
- Built-in AI/ML & Gen AI
- Scales easily, future-proof architecture.

The Challenges Enterprise SOCs Face

Security Operations Centers (SOCs) today are under enormous strain. Analysts face relentless alert fatigue, drowning in thousands of notifications where critical threats are easily buried among false positives. At the same time, siloed tools and fragmented data force teams to manually stitch information together, slowing investigations and creating dangerous blind spots. The challenge is compounded by a persistent shortage of skilled staff, leaving fewer people to handle a growing volume of incidents. Meanwhile, adversaries are becoming more sophisticated, using advanced techniques that outpace traditional defenses and even employing AI and automation to amplify their attacks. Together, these pressures lead to slower response times, higher operational costs, and an increased risk of successful breaches that can disrupt business, cause financial loss, and damage enterprise trust.

- Unified SOC platform
- Built on Proven SIEM, SOAR and TIP Technologies
- Built with Operational Expertise from SOCaaS
- Agentic AI for SOC Workflows
- AI Visibility and Governance

FortiSOC

FortiSOC is a cloud-native SOC platform that centralizes all SOC capabilities into a single integrated solution. With built-in AI/ML and automation, it enhances efficiency and empowers analysts through a consistent, unified interface - eliminating the need to switch between multiple tools.

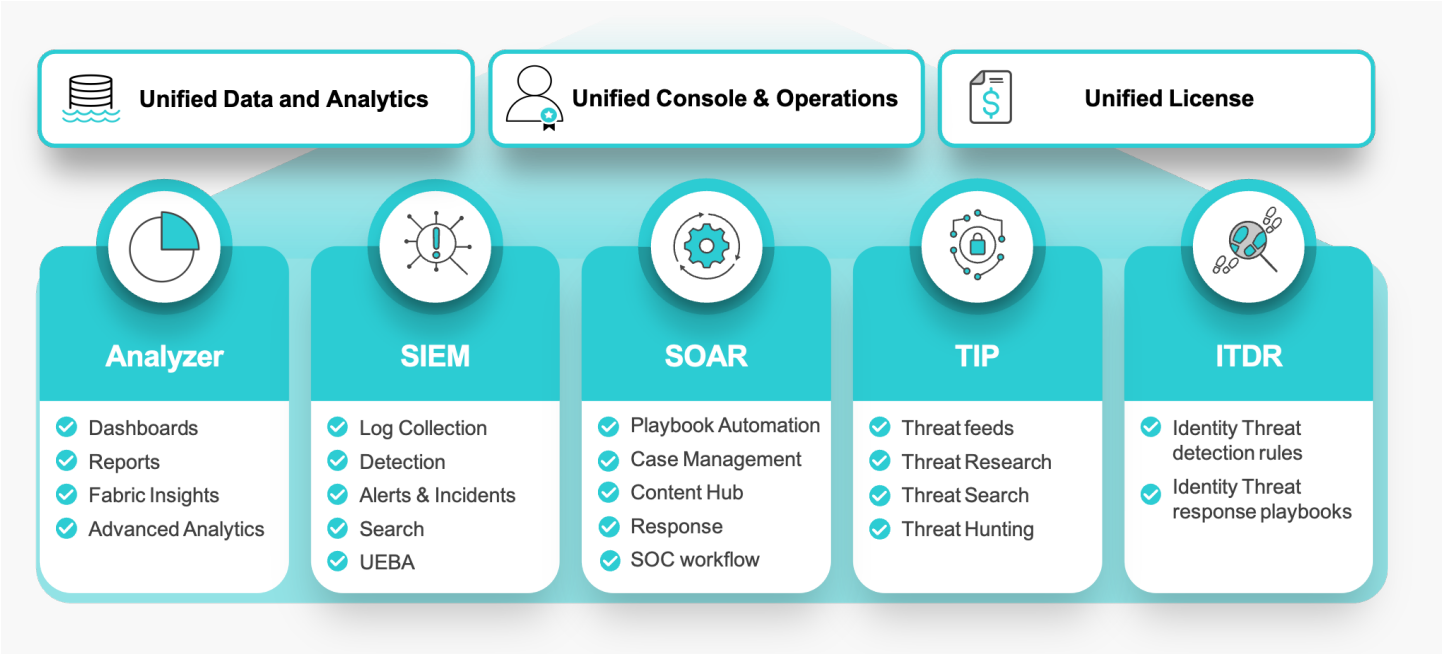
Built on Proven SOC Platforms

FortiSOC combines the industry-proven analytics and detection capabilities of FortiAnalyzer, FortiSIEM and the powerful automation and orchestration capabilities of FortiSOAR into a unified cloud-native Security Operations platform. By bringing detection, investigation, and response together under a single data model and user experience, FortiSOC eliminates operational silos while preserving the full capabilities security teams rely on today, enhanced with AI-driven automation and cloud-scale performance.

Built with Real SOC Experience

FortiSOC incorporates operational best practices developed through Fortinet's SOCaaS operations, where security teams monitor and respond to real-world threats across global customer environments.

These proven workflows and operational models are embedded directly into the platform, enabling organizations to operate with mature SOC practices from day one.



Key Capabilities

Unified Security Operations

FortiSOC consolidates multiple SOC functions into a single cloud platform:

Centralized log analytics and correlation

- Incident investigation and case management
- Automated response workflows
- Behavioral threat detection
- Integrated threat intelligence

One platform. One data model. One operational experience.

Agentic AI for SOC Automation

FortiSOC introduces Agentic AI designed to assist and scale security teams. AI capabilities include:

- Automated alert triage
- Investigation assistance
- Incident summarization
- Guided response actions
- AI-assisted workflow creation

AI agents handle repetitive tasks so analysts can focus on high-impact threats.

Advanced Threat Detection

FortiSOC improves detection accuracy using:

- Machine learning behavioral analytics
- Identity-aware detection
- Threat intelligence correlation
- Risk-based prioritization

The result: fewer false positives and faster threat identification.

Built-In SOC Best Practices

FortiSOC embeds operational knowledge gained from real-world SOC operations.

Organizations benefit from:

- Predefined investigation workflows
- Standard incident handling models
- Ready-to-use dashboards and reports
- Operational metrics and visibility

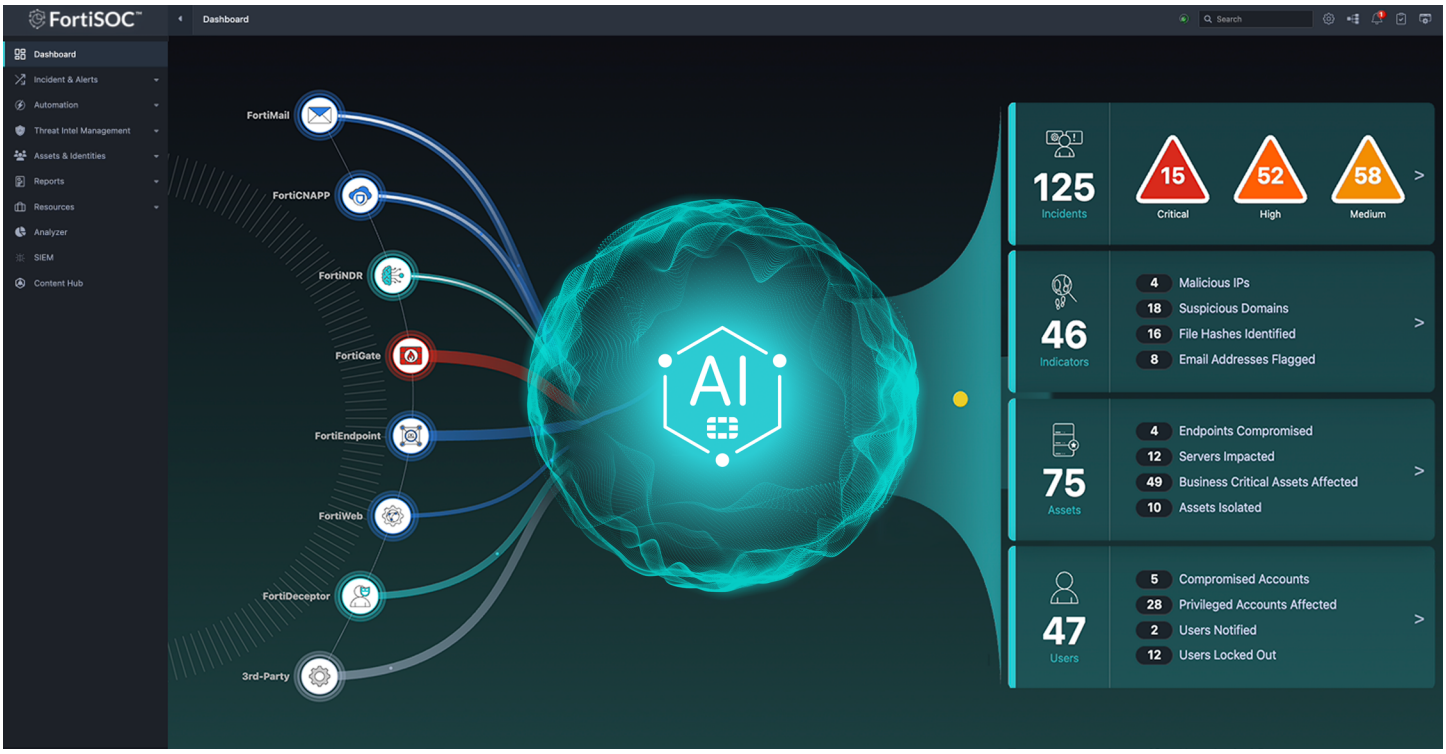
Teams can operate like a mature SOC from day one.

Central AI Visibility & Governance

As AI adoption grows, FortiSOC provides visibility and protection for AI usage:

- Monitoring AI agents and interactions
- Shadow AI detection
- AI activity auditing
- Governance and oversight controls

Security teams gain confidence in managing AI risks.



Differentiator

Unified SOC Platform

Unified analytics, automation, investigation, and AI operate on a shared data model and single workflow engine.

AI Assisted Operations

Applies Agentic AI directly to SOC operations for Alert triage, Investigation assistance, automated response execution and workflow orchestration.

Intelligent Prioritization

Alerts and incidents are dynamically ranked based on risk, context, behavior, threat intel, and AI analysis not just rule severity.

Built-in Workflows

Build standardized SOC processes into the platform on proven SOAR automation capabilities and real-world SOC best practices.

Operational from Day One

A ready-to-run SOC platform with preconfigured analytics, workflows, dashboards, automation, and real-world SOCaaS operational experience.

Benefits

Reduce Complexity

Replace multiple tools with a unified SOC platform.

Increase Analyst Productivity

Automate repetitive investigations and response tasks.

Improve Detection Quality

Behavioral analytics and intelligence-driven prioritization reduce noise.

Accelerate SOC Maturity

Built-in best practices shorten deployment and tuning time.

Scale with Confidence

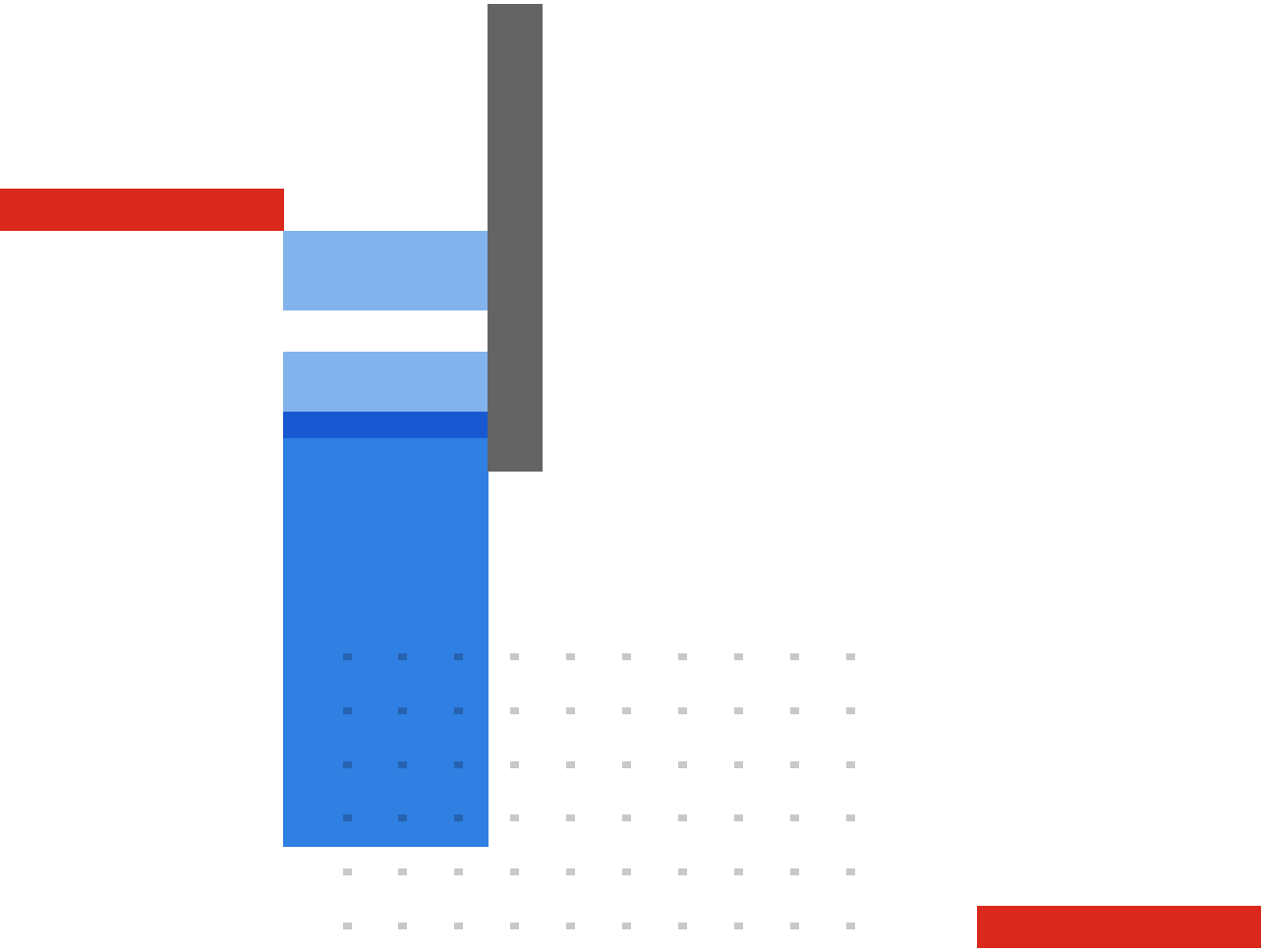
Cloud-native architecture supports enterprise and MSSP environments.

Ordering Information

Product	Description	SKU
FortiSOC Base Subscription	FortiSOC Base Subscription for 1 GB/Day Ingestion. Includes FortiCare premium and 1-month analytics. Support -1, -3 and -5 year terms.	FC1-10-FSCLD-1309-02-DD
FortiSOC Advanced Subcripiton	FortiSOC Advanced Subscription for 1 GB/ Day Ingestion. Includes FortiCare premium and 1-month analytics. Support -1, -3 and -5 year terms.	FC1-10-FSCLD-1318-02-DD
Service Add-On		
Analytics Retention	Adds one month of analytics retention per GB/ day of licensed ingestion.	FC1-10-FSCLD-1311-02-DD
Archive Retention	Adds one month of archive retention per GB/day of licensed ingestion.	FC1-10-FSCLD-1312-02-DD

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

February 27, 2026

FortiSOC-DAT-R1-20260227