SOLUTION BRIEF

Defend against Evasive Cyberattacks with FortiSIEM Security

Executive Summary

AI tools, attacker specialization, and a more exposed attack surface mean that stopping cyberattacks has never been more difficult. Industry experts, regulatory guidelines, and proven best practices recommend a security information and event management solution (SIEM) for organizations of all sizes to provide advanced threat detection, incident management, and compliance. A next-generation SIEM solution based on the latest in generative AI (GenAI) and automation is core to a modern defense, offering a major upgrade to legacy SIEM solutions and an accessible entry point for new adopters.

The global average cost of a data breach in 2024 was $4.9 million.[1]

FortiSIEM is designed to be the backbone of your security operations team and your organization's protection from attacks. It provides a unique, high-performance IT/OT SIEM feature set built on advanced analytics, built-in configuration management database (CMDB), native security orchestration, automation, and response (SOAR), and the latest in GenAI assistance. Delivering out-of-the-box value, complete flexibility, and ultimate scale, it's the right solution for organizations and managed sercurity service providers (MSSPs) of any size.

A Comprehensive Solution for SecOps Teams

The modern SOC requires a SIEM that handles more than log aggregation, simple correlation rules, search, and compliance reporting. FortiSIEM builds upon those basics to provide unique capabilities to meet today's SecOps needs. Our comprehensive approach to SIEM combines full-spectrum visibility, advanced analytics, and built-in automation across IT and OT environments.

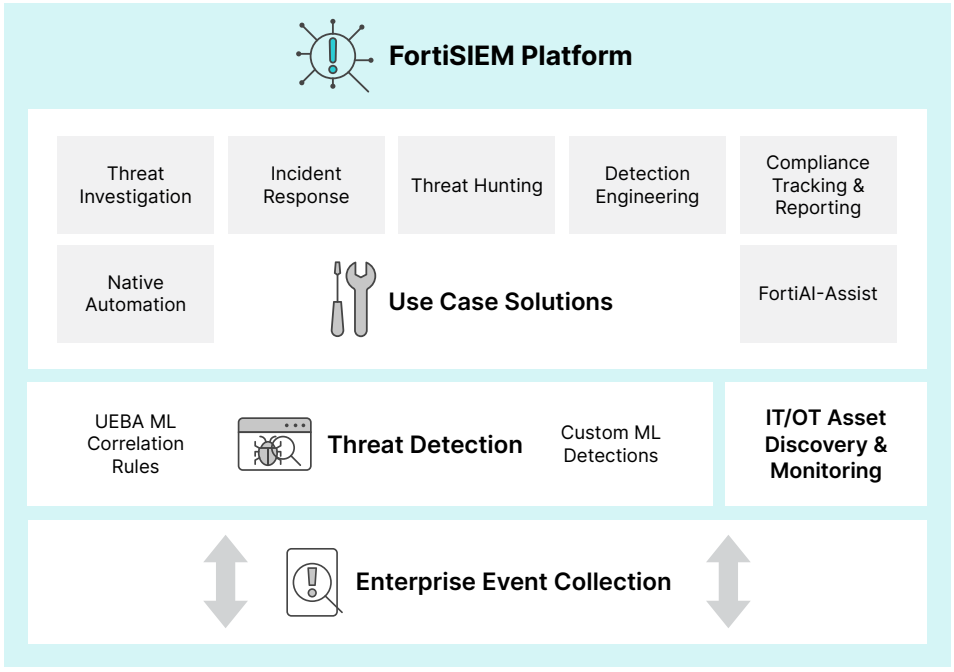

Figure 1: Comprehensive capabilities deliver enterprisewide next-gen SIEM.

Key FortiSIEM Capabilities and Features

This section highlights the key capabilities that make FortiSIEM a cornerstone for operational effectiveness in organizations and MSSPs seeking effective threat detection, streamlined compliance, and efficient response. From universal event collection and native SOAR to GenAI-powered assistance and multitenancy support, FortiSIEM is designed for real-world complexity at enterprise scale.

FortiSIEM Highlights

Universal event collection	Built-in SOAR automation	Massive scalability
Tight integration with the Fortinet Security Fabric	Rich investigation and response features	Multitenancy and other MSSP-focused features
IT/OT asset CMBD with discovery and monitoring	FortiAI-Assist GenAI for analyst workflows	Simple management and exceptional TCO
Advanced behavioral threat detection using AI	Compliance tracking and reporting	Available on-prem, in cloud, or SaaS

Figure 2: FortiSIEM at a glance

Universal event collection

FortiSIEM collects, filters, correlates, and normalizes events and alerts from hundreds of IT/OT multivendor sources across any cloud or on-premises environment. Advanced endpoint agents with file integrity monitoring and built-in Osquery support can be used to directly collect detailed information for advanced threat hunting and investigations.

IT/OT asset CMDB with discovery and monitoring

FortiSIEM includes a full IT/OT CMDB to facilitate asset health monitoring and security analyst investigations. Featuring automatic asset discovery and classification, Purdue model mapping, asset health-metric collection and condition alerting, and import and export capabilities, it provides important IT information and aids security incident management.

Advanced behavioral threat detection using AI

FortiSIEM uniquely detects attacks with user and entity behavior analytics (UEBA) machine learning (ML), over 2,800 IT/OT correlation rules, and the latest threat intelligence. You can import additional rules from the open-source Sigma library and create or customize your own. Additionally, the built-in ML workbench makes it simple to build, train, and deploy your own ML-based detections, all within FortiSIEM.

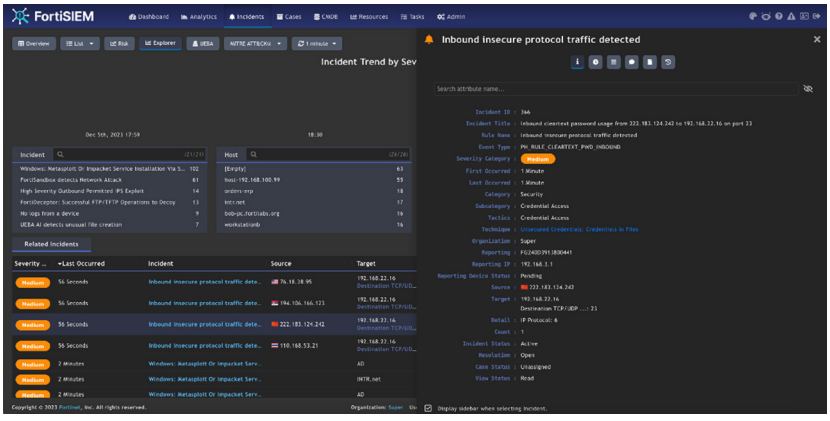

Figure 3: FortiSIEM incident investigation

Rich investigation and response

FortiSIEM offers a robust incident investigation experience, starting with auto-enrichment and automatic risk evaluation. Events are grouped into incidents, and a visual display graphs their relationship. Common investigation and response actions are available as built-in scripts or prebuilt automation playbooks. Complete case management and features are also supported.

Built-in SOAR automation

Rich, built-in SOAR automation is available to accelerate investigation and response and any analyst workflow or task. A prebuilt playbook library provides common use cases that can be customized, and new playbooks are added continuously. Based on FortiSOAR technology, the intuitive playbook builder supports playbooks of any complexity and provides access to the entire library of FortiSOAR connectors.

FortiAI-Assist GenAI

FortiAI-Assist is natively built into common FortiSIEM workflows to guide, simplify, and automate analyst activities. These include event analysis, incident management tasks, and query building and guidance. FortiAI-Assist for FortiSIEM offers the choice of the latest OpenAI and Microsoft Azure OpenAI large language models (LLMs), utilizing a standard retrieval-augmented generation (RAG) method to privatize, augment, shape, and ensure the accuracy of responses and actions.

Compliance reporting

FortiSIEM provides over 1,300 out-of-the box compliance reports, including coverage for CIS, COBIT, FISMA, GLBA, GPR13, HIPAA, ISO 27001, ITIL, NERC, NESA UAE, NIST800-53/171, PCI, SOX, SANS Critical Control, and KSA ECC. To meet GDPR requirements, personally identifiable information (PII) can be obscured based on the user role.

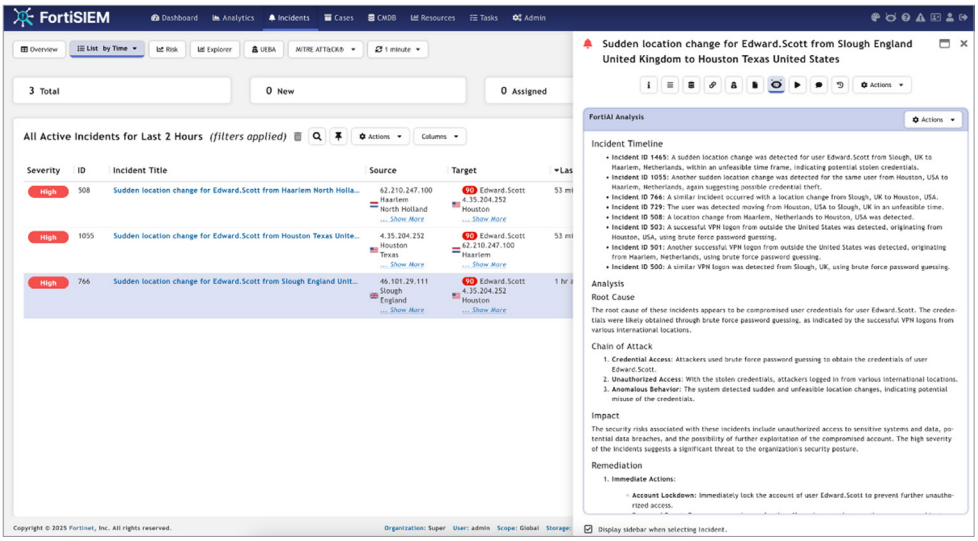

Figure 4: FortiAI-Assist incident analysis and recommendations

Why FortiSIEM?

FortiSIEM offers a number of benefits that further increase its value and efficacy, ranging from deep integrations to flexible form factors, including:

Integration with the Fortinet Security Fabric

FortiSIEM is tightly integrated with Fortinet Security Fabric solutions from network to cloud, providing added customer value and operations simplicity. Native capabilities include event and alert collection, shared intelligence, fabric-wide data queries, and direct product controls for threat remediation or other actions.

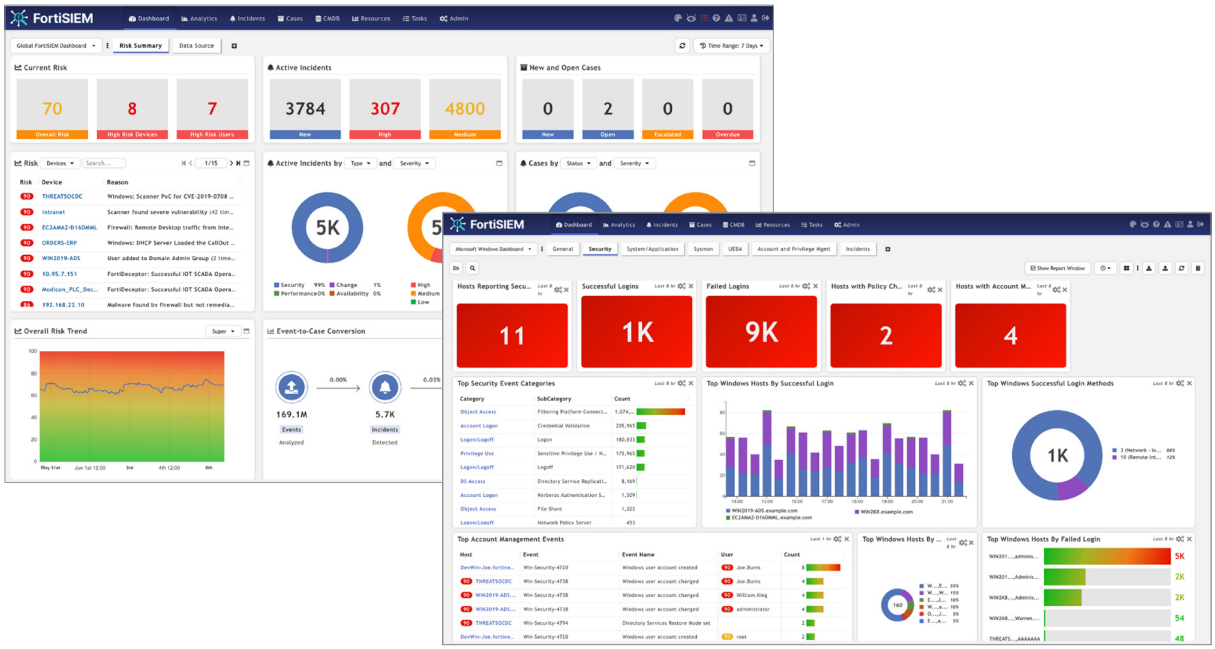

Figure 5: FortiSIEM management dashboards

FortiGuard intelligence and services

FortiSIEM uses real-time FortiGuard Labs intelligence and independent sources to power threat detection, incident enrichment, and threat hunting. FortiGuard value-added services for FortiSIEM include outbreak detections, which provide real-time intelligence, detection rules, and threat hunting procedures for newly discovered security attacks.

Simple management and exceptional TCO

For self-managed deployments, the efficient FortiSIEM architecture featuring distributed processing, 10x data compression, and flexible storage configurations simplify system management and assure a minimum TCO. These attributes contribute to our cost-effective FortiSIEM SaaS offering as well.

Deployment flexibility

A Fortinet-managed SaaS offering is available in 19 AWS locations worldwide. You can also choose to deploy FortiSIEM VM or hardware appliances on-premises in your infrastructure. FortiSIEM can also be deployed directly in AWS, GCP, Oracle, Azure, and other cloud providers that support Kernel-based Virtual Machine (KVM).

The FortiSIEM Advantage

FortiSIEM is the SOC technonolgy and operations foundation for thousands of enterprise, government, and service provider organizations. With advanced features, an automated, AI-driven experience, and attractive TCO, it offers unique value to the cybersecurity defense of any sized entity. Learn more, see a demo, or contact us.

[1] Cost of a Data Breach Report 2024, IBM, July 30, 2024.

July 11, 2025 2:58 PM / MKTG-1646-0-0-EN