FORTINET

SOLUTION BRIEF

Streamline Visibility and Improve Threat Response with Fortinet FortiAnalyzer

Executive Summary

Today's organizations balance network and security operations against an ever-evolving threat landscape. As adversaries use AI-driven evasion techniques, threats are increasingly dynamic and challenging to detect. At the same time, security teams face an overwhelming number of security incidents requiring investigation, compounded by limited resources that hinder their ability to deploy, configure, and maintain security tools, leaving gaps in coverage. These constraints prevent teams from achieving the unified visibility, automation, and threat intelligence necessary to effectively mitigate risks.

FortiAnalyzer delivers a turnkey, unified security operations platform, helping teams streamline security monitoring, automate threat detection, and operationalize security intelligence. As the unified data lake of the Fortinet Security Fabric, FortiAnalyzer enables organizations of all sizes to consolidate data, simplify investigations, and coordinate response efforts efficiently. With embedded GenAI-assisted investigations, built-in SIEM, SOAR, and threat intelligence, FortiAnalyzer lets you simplify and scale security operations.

87% of organizations experienced one or more breaches in the past year, highlighting the critical need for solutions that can enhance security operations and mitigate risks.[1]

Bridging Network and Security Operations

FortiAnalyzer bridges network and security operations by aggregating and correlating data across IT infrastructure, firewalls, cloud environments, and endpoints. Instead of managing separate platforms for network health monitoring and security event detection, teams gain a consolidated view of system performance, security alerts, and operational insights. This unified approach to security monitoring allows you to detect threats faster, minimize blind spots, and improve collaboration between IT and security teams—all while maintaining scalability for evolving security requirements.

FortiAnalyzer makes it easy to expand from NOC to SOC, mature security capabilities, and optimize security workflows for greater collaboration. A number of core capabilities address today's network and security operations challenges.

Unified data lake for operational efficiency and visibility

FortiAnalyzer provides a unified data lake that ingests, normalizes, and enriches security telemetry from the Fortinet Security Fabric and third-party solutions, ensuring that security teams have instant access to correlated insights across their environment. This data is presented through structured dashboards that help analysts digest complex security events, track SOC efficiency, and monitor endpoint and IoT risks in a single console.

Enterprises managing large-scale environments benefit from FortiAnalyzer Fabric, which enables centralized security management across multiple FortiAnalyzer instances. Supervisor-mode FortiAnalyzer synchronizes logs, incidents, and security events across distributed deployments, ensuring consistent security operations. By leveraging API-based communications, FortiAnalyzer Fabric streamlines security event correlation across geographically dispersed teams, enhancing overall security posture and operational resilience.

Advanced threat detection

FortiGuard AI-Powered Security Services natively integrates with FortiAnalyzer. The FortiGuard Outbreak Detection Service delivers timely intelligence on global threat outbreaks, automatically updating FortiAnalyzer with relevant event handlers, correlation rules, and reports. This allows you to quickly adapt to emerging threats, implement appropriate defenses, and reduce the burden of manual rule creation.

Security teams can further refine threat assessments with the FortiGuard Indicators of Compromise Service, which evaluates IP addresses, domains, and URLs. The indicators' view consolidates all detected indicators, allowing analysts to efficiently analyze threats, prioritize alerts, and map adversary activity using the MITRE ATT&CK framework in a single interface.

FortiAnalyzer also includes safeguarding to detect potential physical security threats using 6,000 prebuilt keywords across five categories. By broadening security intelligence to include both digital and physical threats, FortiAnalyzer extends protective measures across multiple security domains.

SOC automation

FortiAnalyzer delivers built-in SIEM, SOAR, and XDR capabilities, enabling real-time event correlation, automated investigations, and orchestrated response actions. This is supported by the SOC Automation subscription, which provides preconfigured playbooks, curated connectors, and monthly content updates, ensures that security teams can rapidly deploy security automation without manual scripting.

FortiAnalyzer can use these capabilities to, for instance, identify unusual outbound traffic indicating data exfiltration, detect multiple failed login attempts revealing possible brute-force attacks, automate log analysis of suspicious activity during off-hours, cross-reference incidents with threat intelligence for context, and deploy playbooks to automatically isolate infected endpoints from the network.

By integrating natively with the Fortinet Security Fabric and leveraging curated third-party security tools, FortiAnalyzer allows security teams to prioritize, investigate, and contain threats while reducing response times and manual effort.

AI assistance with FortiAI for FortiAnalyzer

The embedded GenAI assistant, FortiAI, enhances security workflows by automating investigations, analyzing malware characteristics, mapping adversary tactics, and providing actionable remediation guidance.

Analysts can interact with FortiAI using natural language queries to extract insights, generate detailed incident summaries, and receive AI-driven remediation recommendations. FortiAI also enables faster data correlation by automating forensic analysis and reducing manual threat investigation time, allowing security teams to focus on high-priority incidents.

10

The ESG Economic Validation on the Fortinet SecOps Platform showed that customers reduced the time to thoroughly investigate and remediate incidents from 18.5 hours to an average of just 10 minutes using Fortinet SOC solutions.[2]

Cybercriminals are increasingly harnessing the power of AI, leading to a proliferation of sophisticated attacks such as automated phishing campaigns and advanced malware deployment.[3]

Through an intuitive, AI-driven interface, FortiAI simplifies complex security operations, reducing the need for extensive technical expertise while upskilling security teams. It automates key response actions such as isolating compromised endpoints and blocking malicious activity, ensuring rapid threat containment, and minimizing operational burdens.

Security personnel can leverage talk-to-text capabilities to query detailed security data, visualize attack pathways, and navigate investigations more efficiently. FortiAI integrates with FortiAnalyzer to ensure that AI-driven insights enhance situational awareness and streamline security management across diverse environments.

Recognizing the critical importance of securing AI processes and consistency, Fortinet has implemented stringent measures within the FortiAnalyzer-FortiAI integration. AI proxy servers within Fortinet data centers manage AI traffic, optimizing performance while enhancing data protection. FortiAnalyzer ensures comprehensive monitoring and audits and mitigates risks associated with AI-driven security operations by centralizing AI interactions through secure proxies.

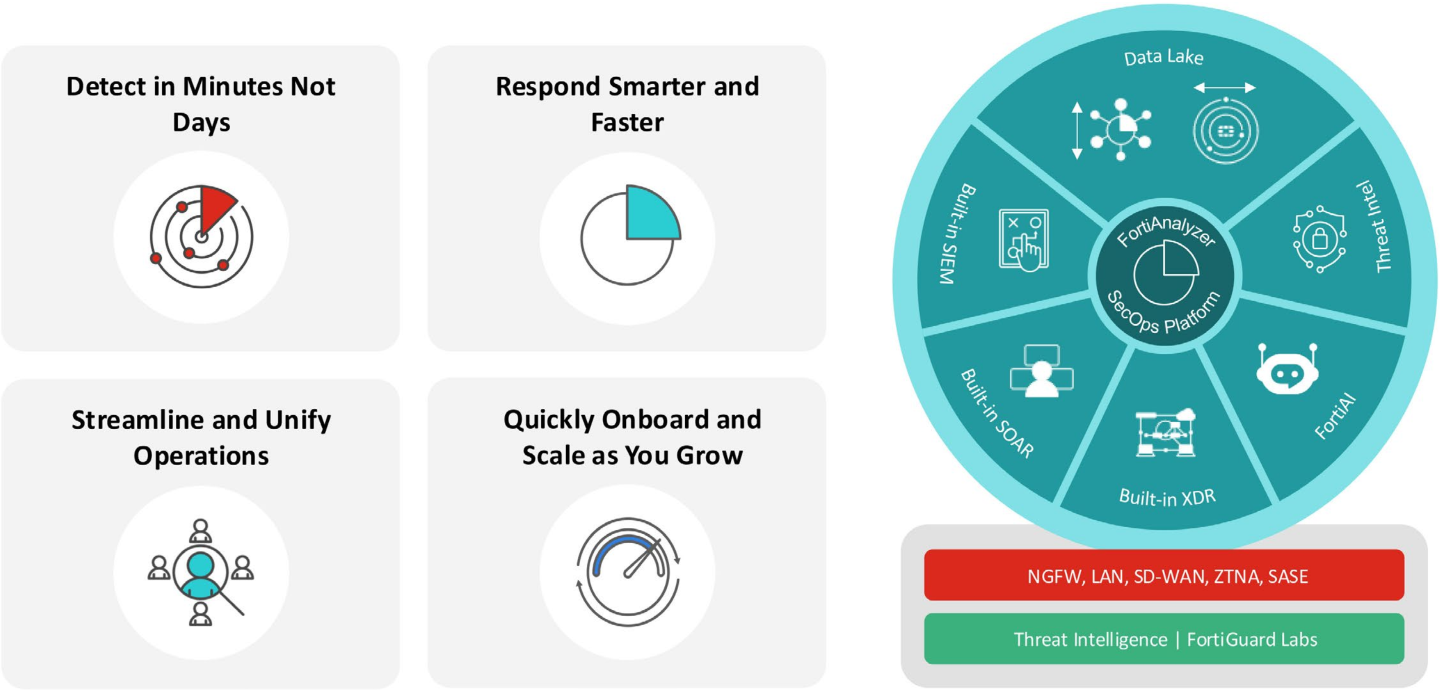
Detect in Minutes Not Days
Respond Smarter and Faster
Streamline and Unify Operations
Quickly Onboard and Scale as You Grow
Data Lake
Threat Intel
FortiAI
Built-in XDR
Built-in SOAR
Built-in SIEM
FortiAnalyzer
SecOps Platform
NGFW, LAN, SD-WAN, ZTNA, SASE
Threat Intelligence | FortiGuard Labs

Figure 1: FortiAnalyzer delivers a comprehensive set of SecOps tools in one solution.

A Unified and Scalable Security Operations Platform

FortiAnalyzer provides a turnkey, AI-assisted security operations platform that integrates security intelligence, automation, and investigation workflows into a cohesive, high-impact solution. By bridging network and security operations, consolidating security data, and enhancing response capabilities, FortiAnalyzer enables organizations to protect against evolving threats while improving operational efficiency.

[1] 2024 Cybersecurity Skills Gap Global Research Report, Fortinet, 2024.

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

[3] Cyberthreat Predictions for 2025: An Annual Perspective from FortiGuard Labs, Fortinet, 2025.

www.fortinet.com

February 18, 2025 5:19 PM

MKTG-901-0-0-EN