SOLUTION BRIEF

Built-in AI Assistance Streamlines Visibility and Improves Threat Response in Fortinet FortiAnalyzer

Executive Summary

In the rapidly evolving world of cybersecurity, the volume, sophistication, and escalating complexity of cyberthreats, combined with the growing interconnectivity of modern IT infrastructures, are challenging traditional security paradigms. New threats are further complicated using artificial intelligence (AI) technologies that lower the barrier for attackers and make it easier for them to evade detection. Security teams are increasingly stretched thin and confronted with the need for an AI-assisted solution that unifies data management, visibility, and automation.

FortiAnalyzer meets these challenges by centralizing log collection, analysis, and correlation while offering continuous security posture assessment reporting. It integrates built-in AI assistance for real-time threat detection and automated response across the Fortinet Security Fabric platform. This solution provides security teams with a single console to manage, automate, orchestrate, and respond to incidents, ensuring complete visibility across the entire attack surface. The lightweight FortiAnalyzer deployment that requires minimal configuration is a starting point for establishing a solid security foundation.

"... an increasing number of security organizations are layering security data lakes into their analytics architecture. These unstructured pools of security data provide a flexible place to quickly and cheaply ingest new data sources that can still be directly queried and upon which new security analytics capabilities can be built or integrated."[1]

The Challenges of Modern Security Operations

By taking advantage of new and more sophisticated AI techniques, adversaries are crafting more elusive threats, from malware to AI-generated phishing attacks. These new threats are outpacing conventional security measures, and many organizations are looking for solutions that can:

- Consolidate point products and offer seamless interaction between diverse security tools, ensuring a more robust, unified security infrastructure
- Cut through the noise by managing the deluge of low-fidelity alerts, alert fatigue, and evasive threats
- Simplify complex investigations with streamlined solutions that can handle the types of complex security inquiries that can bog down teams

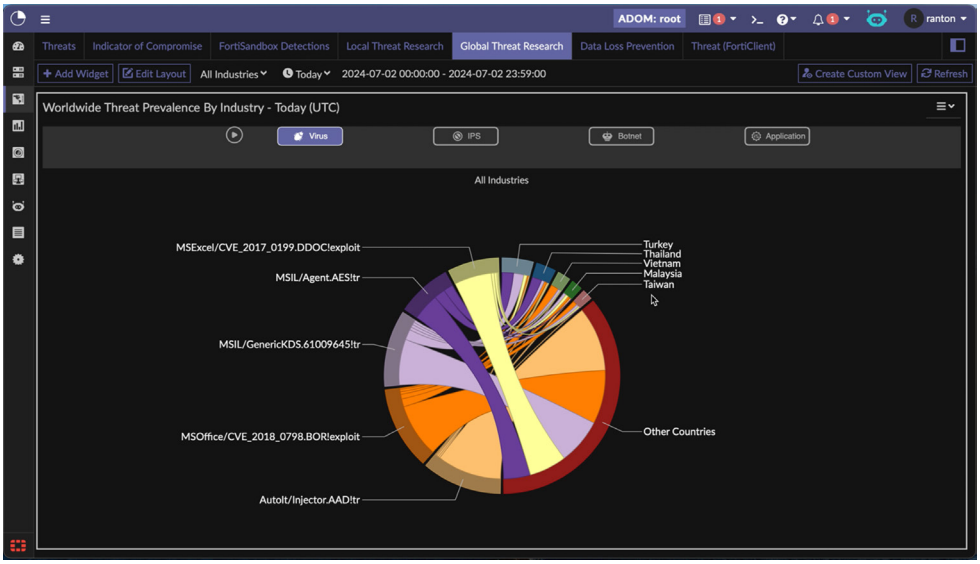


Figure 1: Intuitive FortiAnalyzer visualization dashboards

Organizations need solutions that offer ready-to-use security monitoring with AI for rapid threat detection and automation to expedite response and reduce operational complexity to meet these challenges.

Centralized Security Data Management

FortiAnalyzer responds to today's evolving threats with real-time detection capabilities, centralized security analytics, and end-to-end security posture awareness to help analysts identify advanced persistent threats and mitigate risks before a breach can occur. This integrated, automated, and AI-assisted approach addresses the complexities of today's evolving threat landscape and dynamic security infrastructures.

FortiAnalyzer provides a path to AI-powered security operations, simplifying complex investigations, managing alert noise, ensuring system interoperability, and continuously enhancing the organization's overall security posture. As the central data lake for the Fortinet Security Fabric, FortiAnalyzer consolidates security data from various sources, unifying all configurations, events, and alerts and improving visibility. Enriched by advanced threat visualization capabilities, this unification facilitates more efficient analysis and simplifies complex investigations.

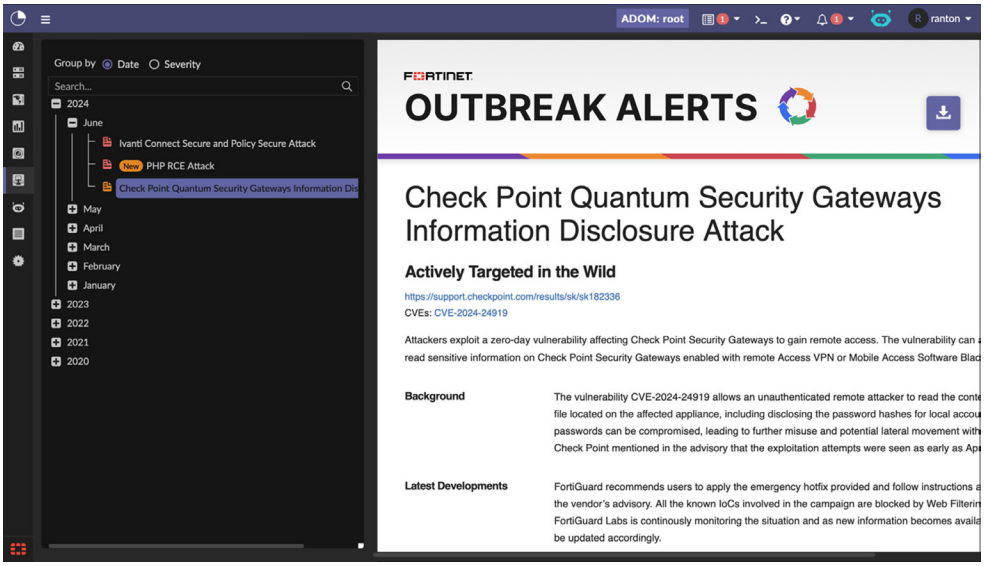


Figure 2: FortiGuard Labs Outbreak Alerts and Detections in FortiAnalyzer

By addressing the challenge of disjointed data and toolsets, FortiAnalyzer simplifies security operations and helps ensure compliance by guiding teams through complex security landscapes with a singular, cohesive view.

Advanced threat detection

FortiAnalyzer, with FortiGuard Labs AI-Powered Security Services, helps analysts stay ahead of emerging threats with detection alerts that automatically download event handlers, correlation rules, and reports for each outbreak. The integration with FortiGuard Labs ensures that security teams receive up-to-the-minute threat intelligence, enhancing their ability to detect and mitigate threats before they can cause harm.

FortiAnalyzer advanced threat detection capabilities include sophisticated threat visualization tools such as threat topologies and a MITRE ATT&CK dashboard, which maps investigations to the MITRE framework so security teams can quickly understand and respond to threats and maintain robust defense mechanisms.

FortiAnalyzer integrates with the FortiGuard Indicators of Compromise and Outbreak Detection Service to provide comprehensive threat detection and response. The Outbreak Detection Service delivers timely intelligence on global threat outbreaks, automatically updating FortiAnalyzer with relevant event handlers, correlation rules, and reports, so organizations to quickly adapt to emerging threats and implement appropriate defenses.

The Indicators of Compromise Service enhances FortiAnalyzer by continuously monitoring the network for indicators of compromise. This service identifies potential security breaches early so security teams can respond swiftly and effectively. FortiAnalyzer helps ensure that organizations can stay ahead of evolving threats with the integration of these advanced threat detection services.

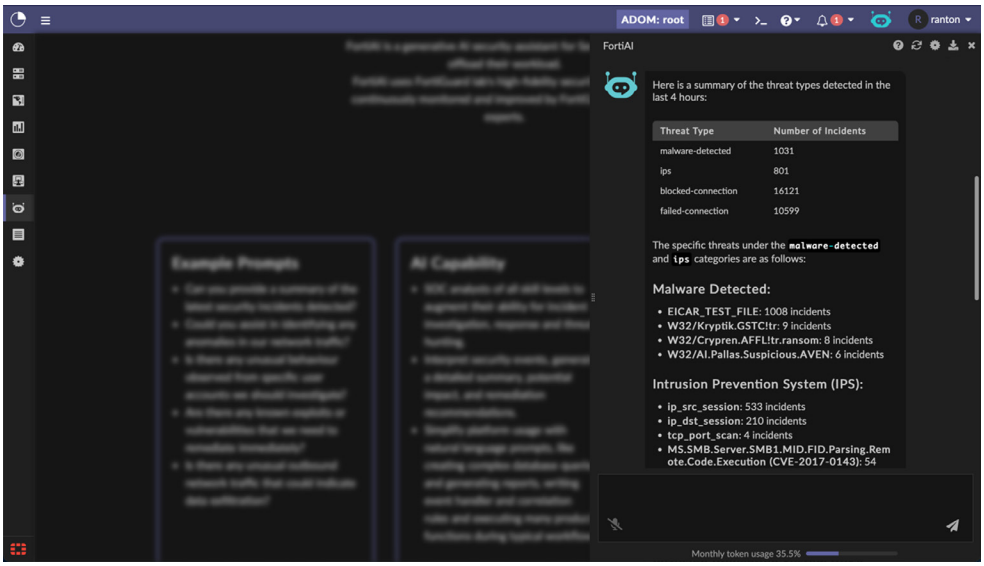


Figure 3: FortiAI offers context-aware GenAI built into the FortiAnalyzer user experience

AI-assistance with FortiAI for FortiAnalyzer

FortiAI for FortiAnalyzer interprets security events, offering insights and advising on actions for remediation, including suggestions for threat response and indicators for threat hunting. It informs analysts of malware characteristics, attacker profiles, and tactics. Analysts can query FortiAI in natural language to create complex database queries, build rich reports, and execute many product functions. Built-in menu prompts make it simple for FortiAnalyzer analysts to invoke FortiAI help during typical workflow activities.

Integrating FortiAI within FortiAnalyzer significantly lowers the complexity of managing advanced security systems. The AI-driven interface guides security personnel through detailed analyses, reducing the need for extensive technical expertise, effectively upskilling security teams and bridging skill gaps. FortiAI automates critical response actions, such as isolating affected systems and blocking malicious activities. This automation ensures rapid threat containment, reducing the operational burden on security teams and allowing them to concentrate on broader strategic analyses.

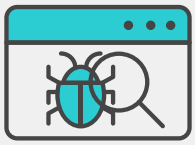
FortiAI offers an intuitive, conversational interface that simplifies security management tasks. Security personnel can now use simple commands to navigate complex and time-consuming investigations, from prompts querying detailed security data to generating comprehensive visualizations. This ease of use significantly reduces the barrier to effective security management, making sophisticated operations accessible to all team members, regardless of their technical expertise.

Recognizing the critical importance of securing AI processes, Fortinet has implemented stringent measures within the FortiAnalyzer-FortiAI integration. Using AI proxy servers within our data centers to manage all AI connections optimizes AI performance and significantly enhances customer data protection across all Fortinet products. By centralizing AI traffic through secure proxies, comprehensive monitoring and data security interactions are ensured, effectively mitigating risks associated with AI-driven operations.

Ready-to-use security automation

Security operations teams face relentless security alerts and need continuous threat investigations. FortiAnalyzer leverages ready-to-use automation to enhance the efficiency of threat identification, investigation, and remediation processes. FortiAnalyzer is enhanced with security automation content packs that include premium reports, event handlers, advanced correlation rules, third-party log parsers, automation connectors, data enrichment, and incident response playbooks. These tools are ready to use and continuously updated so teams can focus on strategic initiatives rather than creating and maintaining these resources.

FortiAnalyzer streamlines detection with advanced correlation rules covering the cyber kill chain, efficient investigation with extensive log parsers for seamless multidevice integration, and accelerated response with playbooks for immediate incident action and resolution. Additionally, FortiAnalyzer can 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 isolate infected endpoints from the network automatically.



51% of analysts reported improved threat detection using playbooks.[2]

Comprehensive AI-Powered Security Operations

FortiAnalyzer transforms the traditional security operations model by combining central log management, AI-driven analysis, automated operations, and continuous posture assessment in a lightweight deployment. This comprehensive approach addresses the immediate challenges of modern cybersecurity and sets the stage for future advancements, making FortiAnalyzer an indispensable tool for organizations aiming to harness the full potential of AI-powered security operations.

[1] Ericka Chickowski, "10 Tips for Better Security Data Management," Dark Reading, March 13, 2024.

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

FORTINET

www.fortinet.com

July 15, 2024 7:13 PM / 2622069-A-0-EN