SOLUTION BRIEF

Improve Visibility and Simplify Data Management with 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 by the use of 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 and ensures lightweight deployment.

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.

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

To meet these challenges, 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.

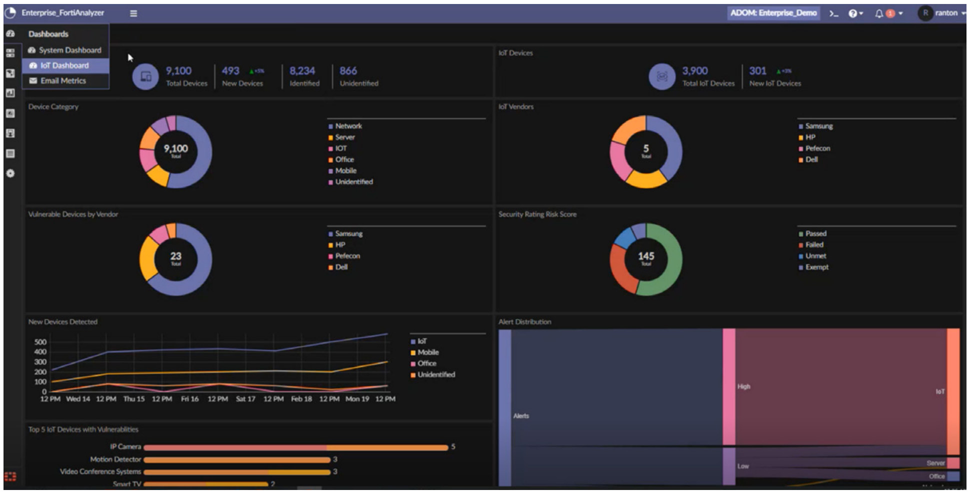


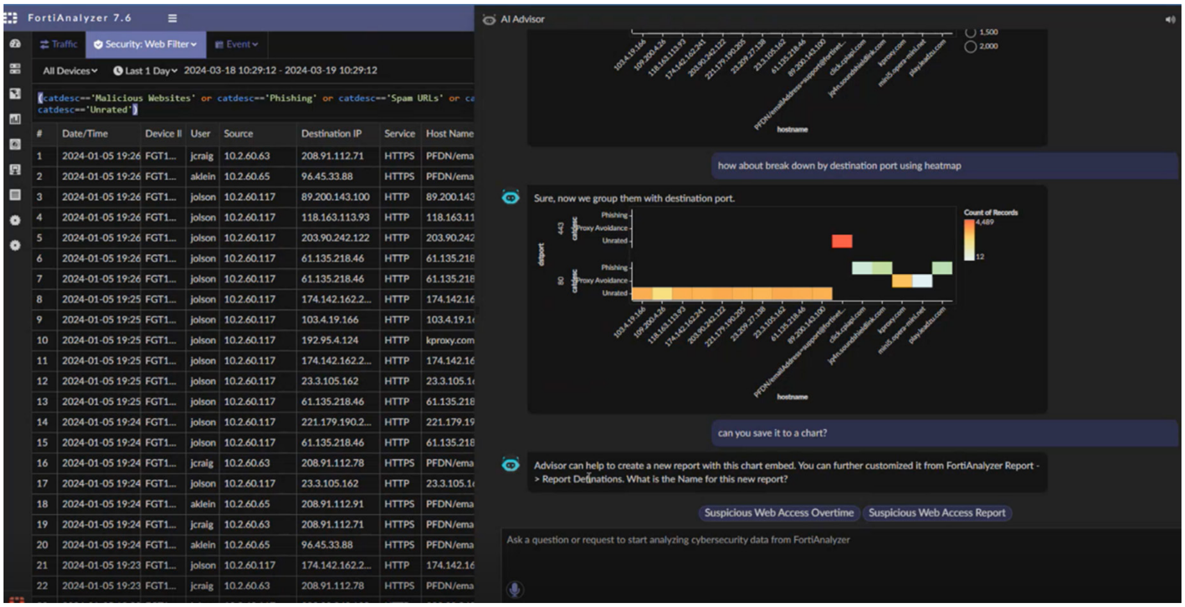
Figure 1: Intuitive FortiAnalyzer visualization dashboards

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 (APTs) 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. Acting 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. 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. FortiAnalyzer offers:

- Lightweight deployment with minimal configuration, which can act as a starting point to establish a solid security foundation
- Threat visualization with advanced tools, including threat topologies and a MITRE ATT&CK dashboard, to map investigations to the framework for intuitive and actionable insights
- Report consolidation to address disjointed data and toolset challenges and to help demonstrate compliance demonstration and navigate complex security landscapes
- Unified management to address disjointed data and tool set challenges and navigate complex security landscapes



2024-03-18 10:29:12 - 2024-03-19 10:29:12

```
(catdesc=='Malicious Websites' or catdesc=='Phishing' or catdesc=='Spam URLs' or ca
catdesc=='Unrated')
```

#	Date/Time	Device II	User	Source	Destination IP	Service	Host Name
1	2024-01-05 19:26	FGT1...	jcraig	10.2.60.63	208.91.112.71	HTTPS	PFDN/ema
2	2024-01-05 19:26	FGT1...	aklein	10.2.60.65	96.45.33.88	HTTPS	PFDN/ema
3	2024-01-05 19:26	FGT1...	jolson	10.2.60.117	89.200.143.100	HTTP	89.200.143
4	2024-01-05 19:26	FGT1...	jolson	10.2.60.117	118.163.113.93	HTTP	118.163.11
5	2024-01-05 19:26	FGT1...	jolson	10.2.60.117	203.90.242.122	HTTP	203.90.242
6	2024-01-05 19:26	FGT1...	jolson	10.2.60.117	61.135.218.46	HTTP	61.135.218
7	2024-01-05 19:26	FGT1...	jolson	10.2.60.117	61.135.218.46	HTTP	61.135.218
8	2024-01-05 19:25	FGT1...	jolson	10.2.60.117	174.142.162.2...	HTTP	174.142.16
9	2024-01-05 19:25	FGT1...	jolson	10.2.60.117	103.4.19.166	HTTP	103.4.19.1
10	2024-01-05 19:25	FGT1...	jolson	10.2.60.117	192.95.4.124	HTTP	kproxy.com
11	2024-01-05 19:25	FGT1...	jolson	10.2.60.117	174.142.162.2...	HTTP	174.142.16
12	2024-01-05 19:25	FGT1...	jolson	10.2.60.117	23.3.105.162	HTTP	23.3.105.1
13	2024-01-05 19:25	FGT1...	jolson	10.2.60.117	61.135.218.46	HTTP	61.135.218
14	2024-01-05 19:24	FGT1...	jolson	10.2.60.117	221.179.190.2...	HTTP	221.179.19
15	2024-01-05 19:24	FGT1...	jolson	10.2.60.117	61.135.218.46	HTTP	61.135.218
16	2024-01-05 19:24	FGT1...	jcraig	10.2.60.63	208.91.112.78	HTTPS	PFDN/ema
17	2024-01-05 19:24	FGT1...	jolson	10.2.60.117	23.3.105.162	HTTP	23.3.105.1
18	2024-01-05 19:24	FGT1...	aklein	10.2.60.65	208.91.112.91	HTTPS	PFDN/ema
19	2024-01-05 19:24	FGT1...	jcraig	10.2.60.63	208.91.112.71	HTTPS	PFDN/ema
20	2024-01-05 19:24	FGT1...	aklein	10.2.60.65	96.45.33.88	HTTPS	PFDN/ema
21	2024-01-05 19:23	FGT1...	jolson	10.2.60.117	174.142.162.2...	HTTP	174.142.16
22	2024-01-05 19:23	FGT1...	jcraig	10.2.60.63	208.91.112.78	HTTPS	PFDN/ema

how about break down by destination port using heatmap

Sure, now we group them with destination port.

can you save it to a chart?

Advisor can help to create a new report with this chart embed. You can further customized it from FortiAnalyzer Report -> Report Definations. What is the Name for this new report?

Ask a question or request to start analyzing cybersecurity data from FortiAnalyzer

Figure 2: FortiAI offers context-aware GenAI built into the FortiAnalyzer user experience.

AI Assistance and Security Automation

Security operations teams have long been challenged by the relentless influx of security alerts and the need for continuous threat investigation. FortiAnalyzer leverages AI assistance and ready-to-use automation to enhance the efficiency of threat identification, investigation, and remediation processes. Integrated with the Fortinet FortiAI generative AI assistant, FortiAnalyzer harnesses context-aware GenAI to streamline security operations activities with best-practice recommendations and guidance.

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.

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

Continuous Security Posture Assessment

Continually assessing an organization’s security posture has traditionally been a lengthy, difficult, and fragmented process. An innovative feature in FortiAnalyzer addresses this challenge. The FortiAnalyzer Attack Surface and Compliance Management (ASCM) Service comprehensively assesses an organization’s security posture. It evaluates unpatched vulnerabilities, configurations, and security settings to provide real-time monitoring and analysis of an organization’s Security Fabric deployment.

The ASCM Service provides critical security scores, including security posture and Security Fabric coverage and optimization, which aids in executive decision-making and highlights the logical next steps in security architecture development.

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.