INSIGHTS | TECH BRIEF

FortiAnalyzer: Security Fabric Analytics, Automation & Response

Security Challenges in the Digital Transformation Era

The acceleration of digital transformation initiatives has given rise to network security challenges for organizations of all sizes and across various sectors. As business architecture has evolved and expanded, security infrastructure has grown increasingly complex. Managing and securing data, applications, and systems has become more arduous and time consuming with the rise of cloud adoption and the expansion of the digital attack surface. Many companies are dependent on fragmented security infrastructure, forcing them to manage multiple solutions. This leads to operational inefficiencies, security blind spots, and threat detection response delays. In fact, 77% of organizations rely on non-integrated point security products to some degree within their organization, leaving gaps in security effectiveness.[2]

Rapidly evolving cyberthreats have increased in frequency and sophistication, making them harder to detect. Inefficient manual processes and inconsistent configurations can further delay threat detection and response, placing an undue burden on security teams. These challenges are compounded by the high volumes of network logs and security data, which can be difficult to correlate and analyze effectively. Moreover, ever-increasing compliance requirements typically necessitate the manual compilation of reports and audits by already overburdened staff. And lastly, the global scarcity of cybersecurity skills has further strained IT resources.[3]

Shift Towards Streamlined Security

The biggest operational challenges experienced by companies often stem from the lack of integration amongst vendor point products. Many modern enterprises have now prioritized implementing a converged set of security capabilities within a united framework, enabling security staff to more efficiently and effectively fortify and secure complex network infrastructures. According to a Gartner survey, 75% of organizations are pursuing security vendor consolidation.[4]

An integrated solution streamlines the support of multiple point products and provides broad visibility and control of the entire digital attack surface, including on-premises and cloud. Implementing an analytics-powered security and log management approach correlates data from multiple devices

80%

of organizations are introducing innovations faster than their ability to secure themselves against cyberattacks.[1]

and combats alert fatigue by providing real-time critical insight into threats. Security teams need the ability to automate workflows, such as policy application and enforcement, as well as responses to security incidents. Finally, a comprehensive solution should include tools that map operations to industry best practices and security standards as well as generate reports as evidence of compliance with regulations.[5,6]

Introducing FortiAnalyzer

Fortinet addresses today's complex security challenges with FortiAnalyzer, a centralized network security platform that provides enterprises with consolidated network information and automated processes. FortiAnalyzer is a powerful log management, analytics, and reporting platform that features a single console to manage, orchestrate, and respond. This enables simplified security operations, complete visibility of the entire landscape, real-time threat intelligence, and the proactive identification and remediation of risks. FortiAnalyzer can be deployed as a physical hardware appliance, virtual machine (VM) and virtual machine subscription (VM-S), as well as a private or public cloud instance, with scalability, redundancy and backup, and high availability capabilities.[7,8]

The Analytics Engine of Fortinet Security Fabric

As part of the Security Fabric, FortiAnalyzer integrates with other Fortinet offerings without the need for additional consoles. The solution utilizes an integrated analytics engine to correlate threat data collected throughout the Fortinet Security Fabric, and serves as the central log management offering for all the products in the fabric. This integration enables unified policies and coordinated threat response, enhancing the overall efficacy of your organization's security setup. The Fortinet Security Fabric is a broader framework that encompasses various Fortinet security products and solutions, ensuring a cohesive and integrated security posture.[9] The Fabric is built on three fundamental attributes:[10]

- **Broad:** Fortinet's broad portfolio includes converged networking and security offerings across endpoints, networks, and clouds. It enables high-performing connectivity and coordinated real-time threat detection and policy enforcement across the entire digital attack surface and lifecycle, enabling companies to enforce security everywhere.
- **Integrated:** Best of breed technologies are integrated with AI-powered centralized analysis and automated prevention. This delivers cohesive and consistent security, and simplified operations across different technologies, locations, and deployments to close security gaps and reduce complexity.
- **Automated:** A context aware, self-healing network and security posture leverages cloud-scale and advanced AI to automatically deliver near real-time, user-to-application coordinated protection across the Fabric, delivering faster time-to-prevention. Process automation simplifies operations and frees IT teams to focus on innovation.

FortiAnalyzer Core Capabilities

Sophisticated network security analytics ensure advanced threat detection and comprehensive reporting across various deployment locations, and automation capabilities simplify policy management and system configurations. The solution correlates log data from multiple Fortinet devices, providing valuable context to IT teams. By analyzing this data using machine learning (ML) and indicators of compromise (IOCs) provided via a global threat intelligence feed, FortiAnalyzer can help even the smallest security teams to pinpoint and rapidly respond to threats within their network. Core capabilities include:[11,12]

- **Interoperability:** Enable seamless communication with your security components, enabling quicker identification, isolation, and remediation of threats across the network.
- **Consolidation of Operations:** The solution offers centralized logging, analytics, and reporting to reduce the complexity of security operations. Consolidating disparate tasks into a single platform reduces operational overhead and ensures consistency in security policy application and enforcement.

- **Log Management:** FortiAnalyzer collects, stores, and analyzes log data from all Fortinet security devices, including FortiGate Next-Generation Firewalls, VPNs, and intrusion detection and prevention systems. Your organization can manage large volumes of logs and search for specific events using various criteria, such as time range, source or destination IP, and protocol.
- **Actionable Insights:** The solution delivers advanced security analytics that transform raw network data into actionable insights. These insights can be leveraged to fine-tune your organization's security posture, identify potential vulnerabilities, and ensure ongoing compliance with regulatory standards.
- **Automation:** Automate routine tasks. This includes automating responses to security incidents, generating reports, and adjusting security policies based on network behavior.
- **Incident Response:** The platform delivers real-time detection and response capabilities for incidents. Comprehensive visibility into network traffic and security events is achieved though correlating and analyzing events generated from all Fortinet devices. This consolidated view provides an accurate picture of security threats. Alerts are generated when security events occur, such as when a user attempts to access a restricted website.
- **Advanced Threat Detection:** FortiAnalyzer integrates with FortiGuard Labs to provide real-time information on emerging trends and vulnerabilities. It analyzes and correlates threat data from multiple sources, including third-party threat feeds.

Achieve Key Security and Business Benefits

As enterprises advance, they need an easy and automated way to respond to anomalies discovered within their networks to prevent operational disruptions. For example, over the past five years, the number of data breaches has increased by an alarming 67%.[13] FortiAnalyzer capabilities enable proactive operations, maximizing resources and security posture to avoid breaches. The solution reduces risk with tracking and reporting features that help ensure compliance with privacy laws, security standards, and industry regulations. In addition, FortiAnalyzer ensures that IT leaders are equipped with data-driven insights, fostering swift and accurate business decisions that align with company objectives. Let's examine some key security and business benefits:[14,15,16,17]

Amplify Visibility and Threat Identification: FortiAnalyzer enhances visibility across network traffic, user activities, and system configurations. It combines sophisticated event correlations across different types of log sources, network traffic analysis, and advanced AI techniques with an intuitive rules editor mapped to MITRE ATT&CK® use cases. FortiAnalyzer allows you to preemptively set if-this-then-that criteria, identify potential breaches, and understand user behavior. Integrated machine learning establishes behavior baselines, detects anomalies, and allows for predictive analysis and trend spotting. The solution helps score risk across the attack surface, accelerates the detection of threats, and pinpoints where immediate response is required. Ultimately, your organization can significantly reduce your threat entry points and stop previously hidden threats before they escalate.

Improve Operational Efficiency and Fortify Security Posture: A single dashboard offers a united, real-time view of data across the Fortinet Security Fabric and other integrated systems. With FortiAnalyzer, your organization will experience a sharp reduction in threat response times, increased operational efficiency, and a stronger security posture. The solution enables zero-touch deployment of security configurations across the enterprise, minimizing human errors and misconfigurations. IT staff can easily manage large volumes of logs and search for specific events using various search criteria. The fusion of data and analytics into one comprehensive viewpoint simplifies network management tasks and offers faster, actionable insights. These capabilities reduce response times to minutes rather than days and enable limited staff to focus on expert-level decision-making rather than monitoring and information routing. With quicker decision-making, analysts reduce the risk of oversight errors and gain an agile response mechanism ready to tackle emerging threats.

Simplify Audit and Compliance: Compliance management is typically a manual process involving the aggregation of data from multiple point security products. FortiAnalyzer automates compliance tracking to help your organization comply with numerous global and industry-specific regulations with prepackaged compliance reports and customizable report options. Predefined compliance reports tailored to standards such as GDPR, HIPPA, and PCI-DSS make it simpler for organizations to maintain a steady compliance posture. Beyond reporting, FortiAnalyzer offers real-time tracking of user activities and network configurations against compliance benchmarks. Having this data easily accessible is critical in the event of an audit. FortiAnalyzer frees up resources, reduces potential penalties, and, most importantly, reinforces an organization's reputation as a trustworthy data custodian by simplifying compliance processes.

FortiAnalyzer Use Cases

FortiAnalyzer reduces operational complexity with the following use cases, enabling staff to focus on more critical business priorities. These use cases leverage FortiAnalyzer's integration with other Fortinet Security Fabric components and its collaboration capabilities with other security tools, processes, and systems.[18,19,20]

- **Faster Threat Detection:** FortiGuard's Indicators of Compromise (IOC) subscription quickly identifies threats across your network, helping reduce time to detection. FortiGuard, Fortinet's threat intelligence service, delivers threat intelligence feeds and security updates to detect known IOCs while FortiAnalyzer provides centralized log analysis and alerting.
- **Consolidated Visibility and Operations:** Analytics provide real-time visibility across all the telemetry for the Security Fabric and enable visibility natively with FortiView, a comprehensive monitoring system that integrates real-time and historical data into a single view.
- **Protection with Threat Intelligence (TI) and Rules:** FortiAnalyzer integrates with FortiGuard Labs to share real-time information on emerging threats and vulnerabilities gathered from multiple sources. Threat intelligence rules are predefined criteria that leverage threat intelligence feeds from FortiGuard Labs to help in the detection and prevention of security incidents.
- **Security Automation:** FortiAnalyzer reduces complexity and cost with automation enabled via REST APIs, scripts, connectors, and automation stitches. Organizations can create customized and automated responses to various security scenarios.
- **Automated Compliance Tracking and Reporting:** Compliance is simplified with hundreds of pre-built reports and regulation-specific templates. Integrated at the network operations layer is the ability for FortiManager and FortiAnalyzer to automate compliance tracking and reporting of industry regulations and security standards. FortiManager enables centralized management with automation-driven network configuration, visibility, and security policy management.
- **Security Operations Center as a Service (SOCaaS) for Staff Augmentation:** Outsourced SOC services will proactively monitor, manage, and strengthen your organization's security posture around the clock. FortiAnalyzer transforms FortiGate's detailed threat reports into a comprehensive summary of threats and recommendations for reducing risk and improving security. These logs and reports are triaged and analyzed by Fortinet's SOC team, who provides your staff with prompt security alerts and response recommendations for confirmed incidents. SOCaaS eliminates the need to hire and retain experienced professionals for critical 24x7 security operations.

Talk to WEI today

FortiAnalyzer provides automation-ready single-pane-of-glass management, transparent visibility, advanced compliance reporting, and network-aware rapid response across on-premises, cloud, and hybrid environments. The solution streamlines security operations and brings unparalleled value to modern security network management. Talk to WEI about advancing your organization's security posture by optimizing Fortinet Security Fabric with FortiAnalyzer.[21,22,23]

Sources:

1. Accenture Security and the Ponemon Institute, The Cost of CyberCrime – Ninth Annual Cost of Cybercrime study: https://iapp.org/media/pdf/resource_center/accenture_cost_of_cybercrime_study_2019.pdf

2. Fortinet, The CIO and Cybersecruity – A Report on Current Priorities and Challenges: https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-cio-and-cybersecurity.pdf

3. Fortinet Solution Brief, Simplify Operations with the Fortinet Security Fabric and FortiAnalyzer: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-simplifying-security-operations-with-fortianalyzer.pdf

4. Gartner Press Release, Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022: https://www.gartner.com/en/newsroom/press-releases/2022-09-12-gartner-survey-shows-seventy-five-percent-of-organizations-are-pursuing-security-vendor-consolidation-in-2022

5. Fortinet Solutions for Automation-driven Network Operations: https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-solution-for-automation.pdf

6,7. Fortinet Solution Brief, Simplify Operations with the Fortinet Security Fabric and FortiAnalyzer: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-simplifying-security-operations-with-fortianalyzer.pdf

8. Fortinet Data Sheet, FortiAnalyzer – Security Fabric Network Analytics: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf

9. Fortinet Solution Brief, Simplify Operations with the Fortinet Security Fabric and FortiAnalyzer: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-simplifying-security-operations-with-fortianalyzer.pdf

10. Fortinet Security Fabric: https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric

11. Fortinet, Accelerate Efficiency of Security Operations Across the Security Fabric with Rapid Response: https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-accelerate-efficiency-of-security-operations-across-the-security.pdf

12. Fortinet Solution Brief, Simplify Operations with the Fortinet Security Fabric and FortiAnalyzer: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-simplifying-security-operations-with-fortianalyzer.pdf

13. Accenture Security and the Ponemon Institute, The Cost of CyberCrime – Ninth Annual Cost of Cybercrime study: https://iapp.org/media/pdf/resource_center/accenture_cost_of_cybercrime_study_2019.pdf

14. Fortinet Solution Brief, Simplify Operations with the Fortinet Security Fabric and FortiAnalyzer: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-simplifying-security-operations-with-fortianalyzer.pdf

15. Fortinet Analytics-Powered Security and Log Management: https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-fortianalyzer.pdf

16. Fortinet, Strategies That Reduce Complexity and Simplify Security Operations: https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-cybersecurity-architect-fortianalyzer.pdf

17,18. Fortinet, FortiAnalyzer – Security Fabric analytics, automation, and response: https://www.fortinet.com/products/management/fortianalyzer

19. Fortinet solutions for Automation-driven Network Operations: https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-solution-for-automation.pdf

20. Fortinet, SOC-as-a-Service – FortiGuard SOCaaS Provides 24x7 Monitoring and Incident Management: https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/socaas

21. Fortinet White Paper – Network Complexity Creates Inefficiencies While Ratcheting Up Risks: https://www.infosecpartners.com/wp-content/uploads/2022/05/fortinet-fortimanager-whitepaper-network-complexity-2022.pdf

22. Fortinet Analytics-Powered Security and Log Management: https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-fortianalyzer.pdf

23. Fortinet Solutions for Automation-driven Network Operations: https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-solution-for-automation.pdf

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.