SOLUTION BRIEF

Simplifying Security Operations with FortiAnalyzer

Executive Summary

Security teams worldwide are struggling with the growing complexity of security operations. As networks expand and evolve and cyber threats grow more sophisticated, security teams are challenged to keep up.

FortiAnalyzer, combined with the Fortinet Security Fabric, provides a solution. FortiAnalyzer offers advanced logging and reporting capabilities, centralized security analytics across the Fortinet Security Fabric, and security automation via Fabric Connectors and application programming interfaces (APIs). These use cases enable security teams to increase efficiency, reduce risk, and improve total cost of ownership (TCO).

FortiAnalyzer simplifies operations based on SOC maturity, including:

- Advanced logging and reporting
- Security Fabric analytics
- Security Fabric automation

Security Fabric to Simplify Complexity of Security Operations

Security teams around the world are struggling with the complexity of operations. Common issues include:

- Too many consoles
- Too many alerts
- Manual and slow response
- Shortage of cybersecurity personnel

The Fortinet Security Fabric provides a solution to these security challenges. Broad visibility and control of an organization's entire digital attack surface minimizes risk. An integrated solution reduces the complexity of supporting multiple point products. Automation of security workflows increases the speed of operation. All of these features enable an organization to maximize the impact and effectiveness of a lean security team.

FortiAnalyzer, a core part of the Security Fabric, enables teams to simplify security operations, enabling enterprises at any stage of security operations center (SOC) maturity to smoothly integrate security visibility and automation.

Advanced Logging and Reporting

Any organization, whether it has deployed only a few FortiGates or hundreds, needs to log network activity and generate reports. The Fortinet Security Fabric enables customers to realize the importance of consolidating vendors for common use cases, such as next-generation firewalls (NGFWs), software-defined wide-area networks (SD-WAN), intrusion prevention systems (IPS), and others. FortiAnalyzer provides a unified logging and reporting solution for all of these projects across the enterprise.

Organizations also require customizable reporting and tools that help demonstrate compliance to auditors. Fortinet's compliance reporting support via FortiAnalyzer includes prebuilt reports for standards such as the Payment Card Industry Data Security Standard (PCI DSS), Suspicious Activity Report (SAR), Center for Internet Security (CIS), and National Institute of Standards and Technology (NIST). FortiAnalyzer also provides audit logging and role-based access control (RBAC) to ensure that employees can only access the information they need to perform their duties.

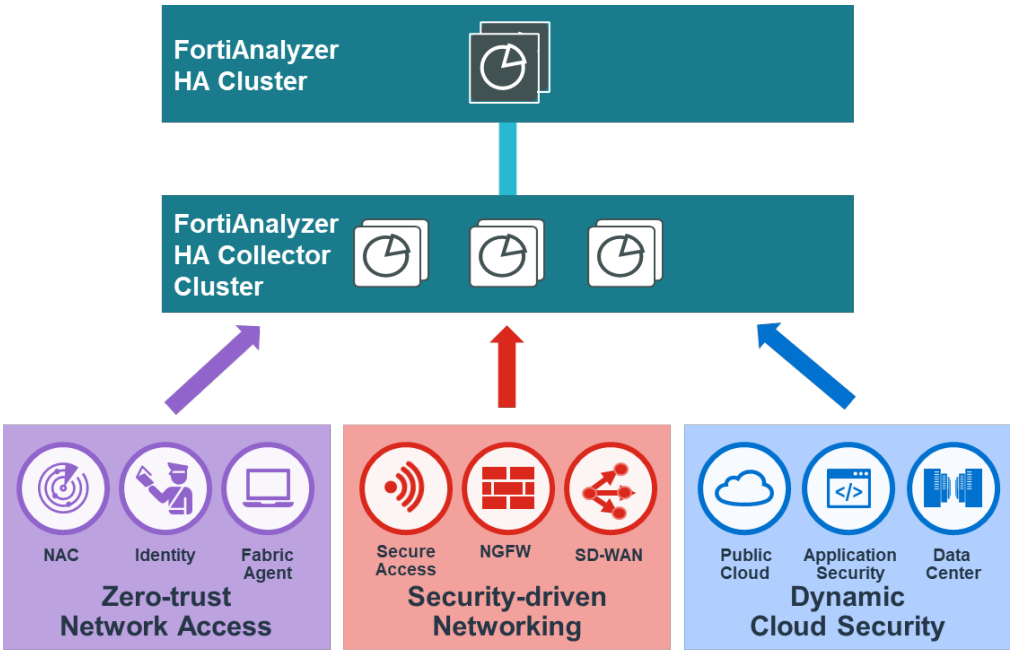

Figure 1: FortiAnalyzer provides advanced log aggregation and reporting.

Security Fabric Analytics

FortiAnalyzer enables organizations to leverage FortiGuard Labs threat intelligence to identify anomalies in their network—in real time. FortiAnalyzer leverages an integrated analytics engine to correlate threat data collected throughout the Security Fabric. Risk scoring is used to prioritize the identified anomalies and share this threat intelligence across the Security Fabric.

The Security Fabric analytics engine also powers visualization of the Security Fabric in real time. These visualizations enable members of the IT, security, and SOC teams to identify and investigate potential threats to the network immediately.

FortiAnalyzer comes with easily customized built-in dashboards and reports. Over 720 datasets are included in FortiAnalyzer to enable easy onboarding to reporting and dashboards. These include advanced queries that are optimized for quick response times in real time.

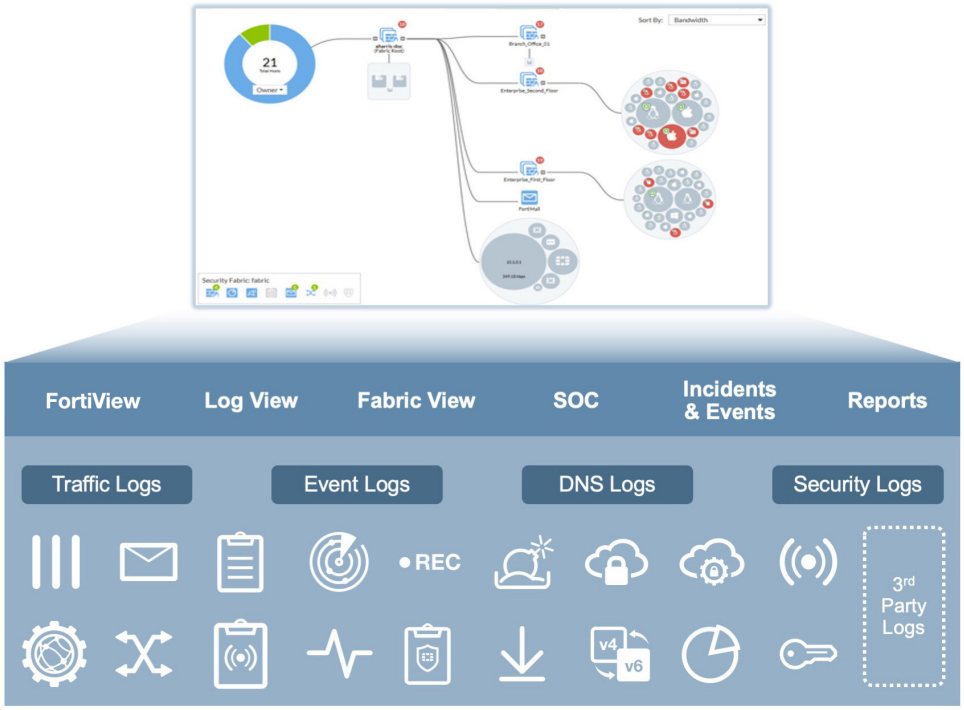

Figure 2: FortiAnalyzer provides unique network insights in real time.

Security Fabric Automation

FortiAnalyzer includes built-in automation through the FortiSOC module. This module comes with playbooks and connectors for the Security Fabric, enabling security teams across the SOC Maturity Model to take advantage of security automation.

Automation can originate in FortiOS via Automation Stitches, which leverage FortiAnalyzer as an advanced correlation engine. This process defines detailed event handlers and plugs into the FortiOS IF-THIS-THEN-THAT technology to optimize response times. Automation can also be triggered via FortiAnalyzer, providing integration with third-party solutions, such as IT service management (ITSM), security information and event management (SIEM), and webhook, or via the Security Fabric using native connectors.

FortiAnalyzer and the Fortinet Security Fabric deliver:

- Increased efficiency
- Reduced risk
- Improved TCO

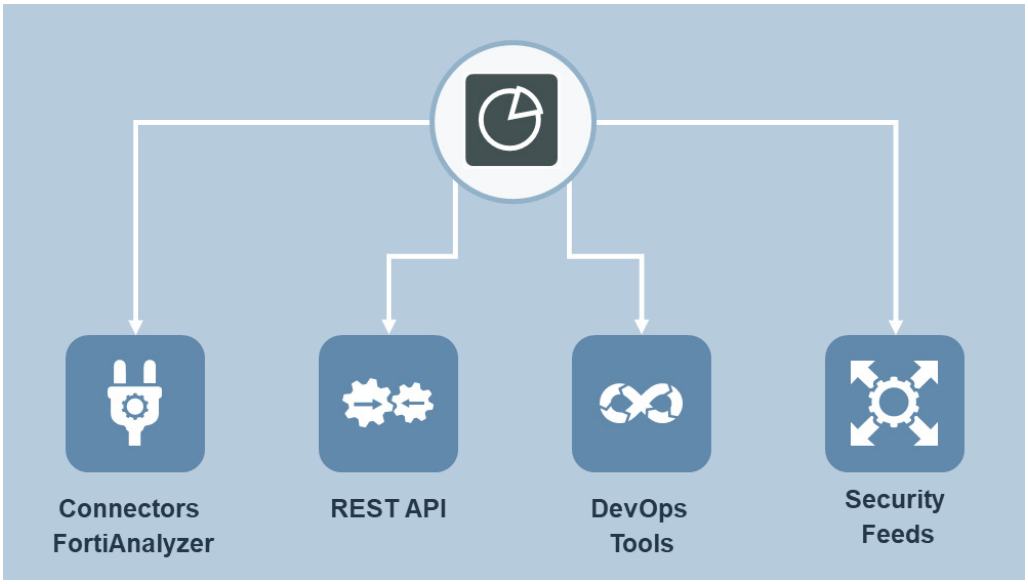

Figure 3: FortiAnalyzer enables centralized automation of security infrastructure via the Security Fabric.

Delivering ROI, Simplicity, and Security

The combination of the Fortinet Security Fabric and FortiAnalyzer delivers enterprise-class security capabilities with industry-leading benefits, including:

Increased Efficiency. Fortinet institutes a simplified infrastructure that reduces operational complexity across the organization. As enterprises advance through the SOC Maturity Model, they will always need an easy and automated way to respond to anomalies discovered within the network. FortiAnalyzer and FortiSOC (the add-on module in FortiAnalyzer) enable this with playbooks and connectors within the Security Fabric that improve the efficiency of IT and security teams.

Reduced Risk. Fortinet's tracking and reporting features help organizations ensure compliance with privacy laws, security standards, and industry regulations while reducing risks associated with fines and legal costs in the event of a breach. FortiAnalyzer tracks real-time threat activity, facilitates risk assessment, detects potential issues, and helps mitigate problems.

The average cost of a data breach ($3.92 million) increases due to system complexity (+$290,000). Both threat-intelligence sharing (-$240,000) and security analytics (-$200,000) decrease that cost.[1]

Improved TCO. The Fortinet Security Fabric and the integration of common uses cases, such as NGFWs and SD-WAN, into FortiGate NGFWs improve TCO by eliminating point products. Additionally, with FortiAnalyzer, which is integrated with other Fortinet offerings via the Security Fabric, organizations can leverage security analytics and automation without the need for additional third-party solutions.

[1] "2019 Cost of a Data Breach Study," Ponemon Institute and IBM Security, 2019.

May 11, 2020 4:44 PM

618026-0-0-EN

sb-simplifying-security-operations-with-fortianalyzer