SOLUTION BRIEF

Simplifying Operations With the Fortinet Security Fabric and FortiAnalyzer

Executive Summary

Cybersecurity teams worldwide are struggling with the growing sophistication and volume of cybercriminal attacks. And as their organizations' networks evolve and expand, their siloed point products add complexity, manual processes, and fragmentation to security operations—which, of course, prevents timely detection of threats and stopping intrusions.

Contributing factors to the current dysfunction in many security operations include:

- Too many siloed point products with lack of integration
- High data and alert volume, producing security noise
- Repetitive manual processes, slowing responses
- The lack of cybersecurity personnel and expertise

FortiAnalyzer, combined with the Fortinet Security Fabric, provides a solution to address current difficulties and strengthen security posture.

To address these factors and improve their security operations, teams at leading organizations are implementing a vendor consolidation and automation strategy—and turning to Fortinet for industry-leading solutions.

A Solution for the Dysfunction

FortiAnalyzer, combined with the Fortinet Security Fabric, provides a solution to address current difficulties and strengthen security posture. As an integrated solution, FortiAnalyzer reduces the challenges of supporting multiple point products. It is also designed to include broad visibility and control of an organization's entire digital attack surface to minimize risk.

With advanced logging and reporting capabilities, FortiAnalyzer centralizes security analytics across the Fortinet Security Fabric and provides security automation via Fabric Connectors and application programming interfaces (APIs). It also includes easy-to-implement security workflow automation to accelerate operations.

These unique features enable an organization to maximize the impact and effectiveness of a lean security team without extensive configuration. FortiAnalyzer, a core part of the Security Fabric, force multiplies teams, simplifies security operations, and allows enterprises at any stage of security operations center (SOC) maturity to smoothly integrate security visibility and automation.

Increase efficiency, reduce risk, and improve TCO

These functionalities 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

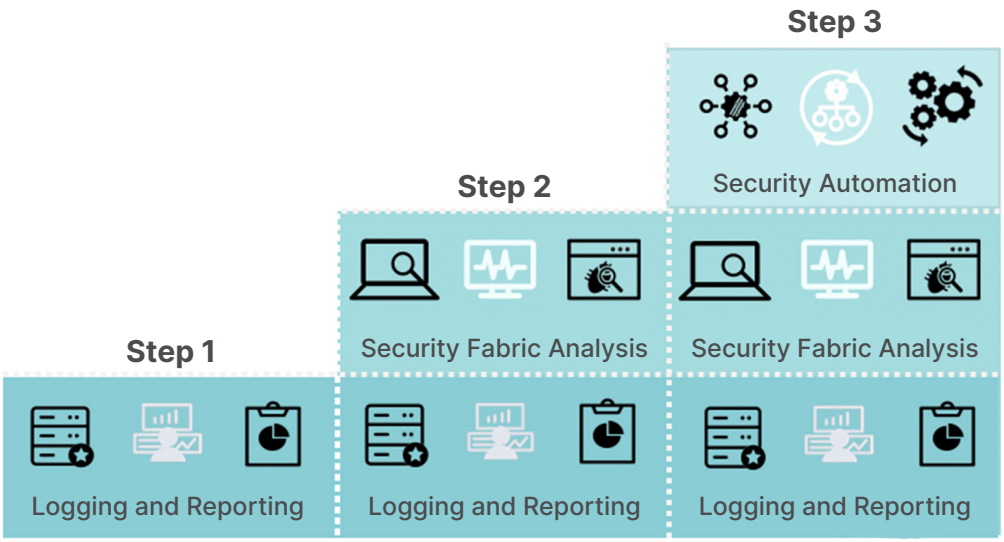

Figure 1: The FortiAnalyzer Three Stages of Deployment.

Advanced logging reporting

The modern organization, whether it has deployed only a few FortiGates or hundreds, is required to log network activity and generate reports. The Fortinet Security Fabric enables customers to strategically consolidate 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 is the unified logging and reporting solution for all these projects across the enterprise. Organizations also need customizable reporting and tools that help demonstrate compliance to auditors or leadership. Fortinet compliance reporting is supported via FortiAnalyzer and 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 more.

Also, FortiAnalyzer provides audit logging and role-based access control (RBAC) to ensure segmentation of data and processes for employees to only access the information they need to perform their duties.

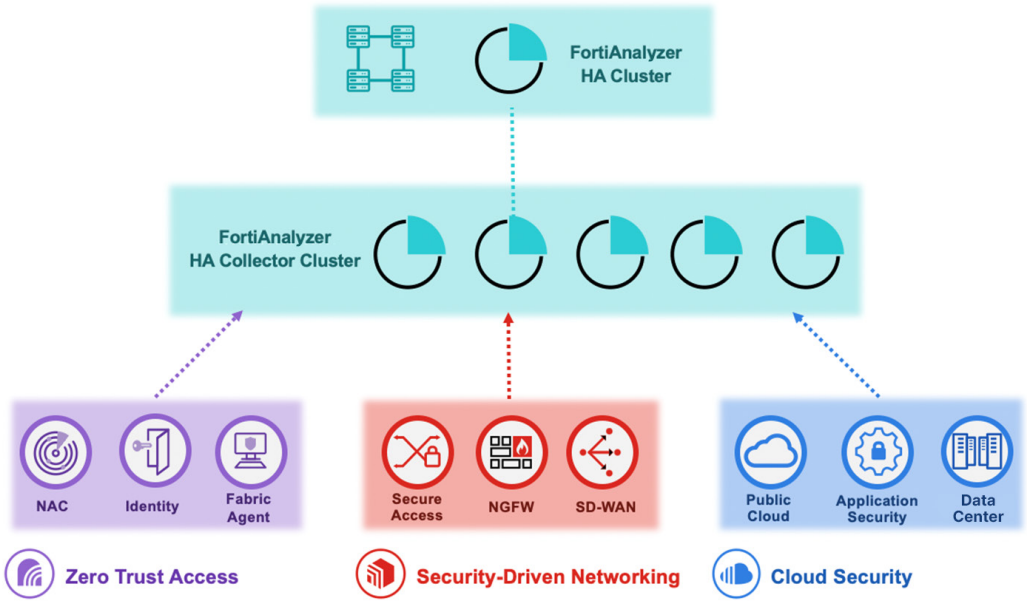

Figure 2: FortiAnalyzer provides advanced log aggregation and reporting.

Security Fabric Analytics

FortiAnalyzer enables organizations to leverage FortiGuard Labs threat intelligence to identify anomalies in their network—in real time. FortiAnalyzer uses 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 allow members of the IT, security, and SOC teams to immediately identify and investigate potential threats to the network. FortiAnalyzer comes with easily customized built-in dashboards and reports.

Over 800 datasets are included in FortiAnalyzer to enable easy onboarding to reporting and dashboards. These include advanced queries that are optimized for quick responses in real time.

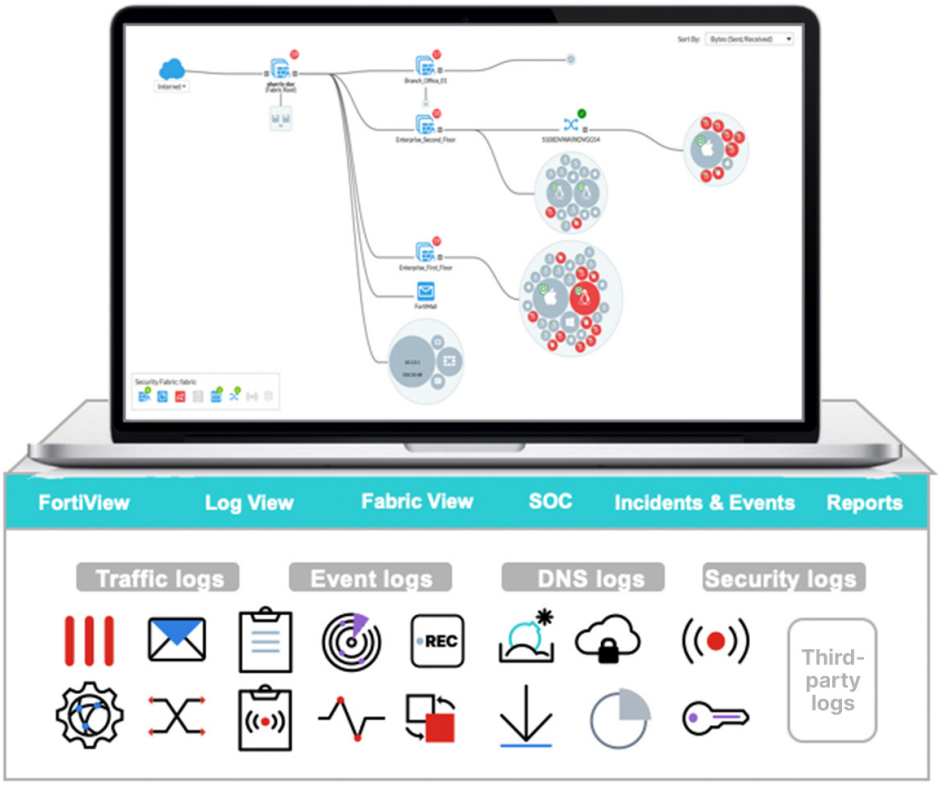

Figure 3: FortiAnalyzer provides unique network insights in real time.

Automation and AI

Automation and security artificial intelligence (AI), when fully deployed, provide the biggest cost mitigation—not only around filling the cybersecurity skill shortage gap, but also costs associated with breaches due to the weaponization of AI and persistent cyberattacks.

FortiAnalyzer includes built-in automation through the FortiSOC module. This module comes with playbooks and connectors for the Security Fabric. This is can be used as an organization's foundation to the SOC Maturity Model to take advantage of security automation. Automation can originate in FortiOS via Automation Stitches, which uses FortiAnalyzer as an advanced correlation engine. This process defines detailed event handlers and plugs in to the FortiOS IFTTT (if this, then that) technology to optimize response times.

Automation can also be triggered via FortiAnalyzer, supporting 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.

ROI, Simplicity, and Security

The blend of the Fortinet Security Fabric and FortiAnalyzer delivers enterprise-class security capabilities and frameworks that include benefits, such as:

- **Increased SOC effectiveness**
  Fortinet institutes a simplified infrastructure that reduces operational complexity throughout the organization. As enterprises advance with the SOC Maturity Model, they will always need an easy and automated way to respond to anomalies discovered within the network. FortiAnalyzer, FortiSOC (the add-on module in FortiAnalyzer), SOC-as-a-Service, and the FortiSOAR management extension enable this with playbooks and connectors within the Security Fabric that improve the efficiency of IT and security teams.
- **Reduced risk and improved situational awareness**
  Fortinet has tracking and reporting features that 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.

"Through our FortiGuard Labs recent study, we can see how critical automation is due to the weaponization of AI. Organizations with no security automation experienced breach costs of $6.71 million on average in 2021 vs. $2.90 million on average at organizations with fully deployed security automation."[1]

- **Controlled 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.

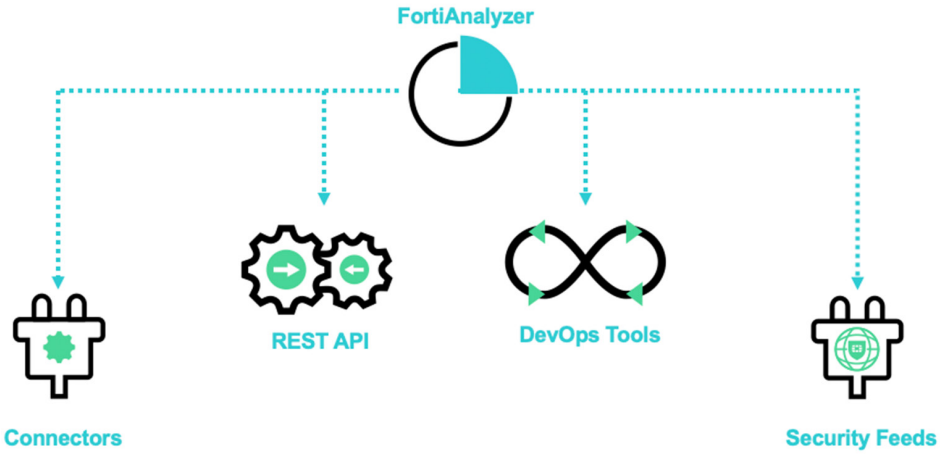

Figure 4: FortiAnalyzer enables centralized automation of security infrastructure via the Security Fabric.

[1] FortiGuard Labs, 2021.

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

May 24, 2022 11:02 AM

618026-A-0-EN