Fortinet Analytics-Powered Security and Log Management

FortiAnalyzer for Increased Efficiencies, Faster Response, and Compliance

Table of Contents

Executive Overview

Rapid enterprise adoption of digital innovations like cloud services and greater mobility have caused the network attack surface to expand while increasing infrastructure complexity. Adding to these vulnerabilities, advanced threats continue to grow in both number and sophistication. As part of the Fortinet Security Fabric, FortiAnalyzer provides analytics-powered security features as well as log management capabilities to reduce risks and improve the organization's overall security posture.

Over the past 5 years, the number of data breaches increased by 67%.[1] And last year, the average probability of a breach over the next 24 months rose to 27.9%.[2]

Introduction: Solving Vulnerability with Visibility

The digital attack surface is expanding at an increasingly faster pace—making it hard to protect against advanced threats. Nearly 80% of organizations are introducing digitally fueled innovation faster than their ability to secure it against cyberattacks.[3] In addition, the challenges of complex and fragmented infrastructures continue to enable a rise in cyber events and data breaches. The assorted point security products in use at most enterprises typically operate in isolated siloes. And this obscures network operations teams from having clear and consistent insight into what is happening across the organization.

An integrated security architecture with analytics-powered security and log management capabilities can address this lack of visibility. As part of the Fortinet Security Fabric, FortiAnalyzer supports analytics-powered use cases to provide better detection against breaches. These use cases include:

- Advanced Threat Detection
- Audit and Compliance
- Rapid Response

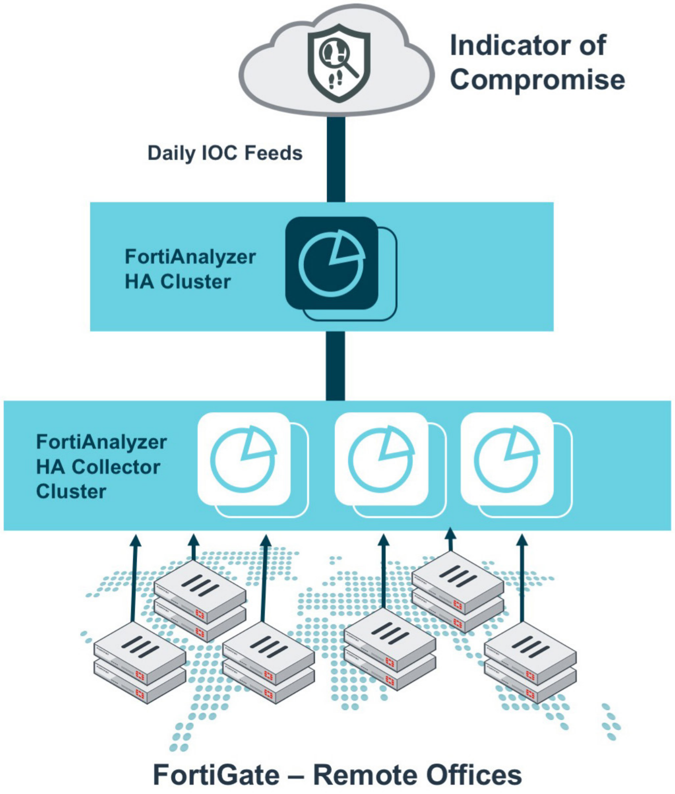

Figure 1: Analytics-powered security and log management appliances.

Last year, 52% of all breaches were caused by human error or system glitches, and 48% were caused by malicious or criminal attacks.[4]

The average enterprise deploys security solutions from 75 different vendors.[5]

Advanced Threat Detection

Attacks against enterprises are getting more sophisticated and harder to detect. To make matters worse, the widespread practice of deploying disparate and disconnected security products inhibits threat-intelligence sharing. This means that network defenses cannot quickly spot and coordinate timely responses to multivector or polymorphic threats across increasingly dispersed network infrastructures.

A centralized management solution with a single-pane-of-glass view enables streamlined security visibility. In this way, FortiAnalyzer reduces complexity and decreases the time to detection of threats. It allows teams to monitor data movement and identify anomalous activity.

Three Ways That FortiAnalyzer Provides Advanced Threat Detection

Visibility

- Delivers advanced reporting and dashboards for operations and security
- Provides tools to enable scheduling of reports

Indicators of Compromise (IOCs)

- References 4.4 million sensors around the world as well as partnerships with over 200 organizations
- FortiGuard Labs researchers use technologies like machine learning (ML) to detect anomalies to enable enterprise-class IOC identification

Security Fabric Advanced Correlation

- Compares all events associated with one incident across Security Fabric integrated solutions

Last year, the mean time to identify a data breach incident increased from 191 days (2017) to 197 days (2018), an indication that threats are becoming more sophisticated and harder to detect.[6]

Audit and Compliance

Compliance management is typically a very manual process. It often involves multiple full-time staff and can require months of work to get right. Data must be aggregated from multiple point security products and then normalized to ensure that regulatory controls are reported accurately. To do this, network and security staff must monitor security controls using separate audit tools for each vendor and then corollate that information to prove compliance. This complex and unwieldy auditing process is inefficient and often ineffective.

FortiAnalyzer automates compliance tracking and reporting of industry regulations and security standards for greater workflow efficiency across the Security Fabric. Plus, this is integrated at the network operations layer. FortiAnalyzer natively provides the capability to evaluate the network environment against best practices, thus measuring compliance risks. Network operations teams then apply and enforce controls on the network to protect against cyber threats. FortiAnalyzer offers an in-depth analysis of network operations to determine the scope of risk in the attack surface and then identifies where immediate response is required.

Three Ways That FortiAnalyzer Improves Audit and Compliance

Easy Demonstration of Compliance

- Provides real-time reports on industry standards such as Payment Card Industry Data Security Standard (PCI DSS)
- Supports security standards such as National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS)

Role-based Visibility

- Enables workflow approval process for policy/settings recommendations between security and network teams for collaborative implementation
- Offers targeted dashboards for key enterprise stakeholders (e.g., CIO, CISO, Network Architect, Security Architect)

Enterprise Integrations

- Schedules and shares reports via email, webhooks, etc.
- Interoperable with existing security information and event management (SIEM) solutions and other tools

Compliance technology is a top spending priority for enterprises—both over the next 12 months (57%) and within the next three years (51%).[7]

Rapid Response

Over half of organizations report a problematic shortage of cybersecurity skills. There are nearly 3 million unfilled cybersecurity jobs today, up 61% from the previous year.[8] As a result of this skills shortage, most enterprises do not have the resources to staff the detection and response of advanced threats. This compounds the problems of security complexity and lack of visibility. This, in turn, significantly slows down the process of detecting and remediating a breach event. The mean time to resolve a data breach incident rose to 69 days in 2018; companies that contain breaches in under 30 days save $1 million or more compared to those that take longer.[9]

FortiAnalyzer helps decrease threat remediation time from months to minutes by coordinating policy-based automated response actions across the integrated Security Fabric architecture. Detected incidents, combined with detailed evidence and analytics, allow network and security specialists to automate and orchestrate security responses. Events can also trigger automatic changes to device configurations to close the loop on attack mitigation. Log management capabilities in FortiAnalyzer further reduce the workflow burdens on limited human staff, allowing teams to focus on critical security decisions.

Automation, artificial intelligence, and machine learning are only being taken up by 38% of organizations—representing a lost opportunity for many.[10]

Three Ways That FortiAnalyzer Improves Detection and Response to Threats

Security Operations Center (SOC) Adoption

- Provides programmable event handlers for customized remediation of risks
- Includes dashboards, SOC reports, and incident timeline view for better investigation of incidents

Integrations

- Fortinet Fabric Connectors provide integration with external tools like SIEM, ITSM, and many others

Workflow and Orchestration

- Enables rapid or automated responses within the native interface
- Provides interoperability with existing management and analytics tools

Accelerating Responses Means Reducing Exposure

Part of the Fortinet Security Fabric, FortiAnalyzer provides analytics-powered single-pane-of-glass visibility, compliance reporting, and rapid response across on-premises, cloud, and hybrid environments.

The analytics-powered security and log management capabilities in FortiAnalyzer help reduce risk around key causes for cyber breaches. They also help organizations shrink the windows of detection and remediation in the event that a breach takes place. And faster response times directly equate to reduced exposure of sensitive data, operational disruptions, and remediation costs.

[1] Kelly Bissell, et al., "Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon, March 6, 2019.

[2] "2018 Cost of a Data Breach Study," Ponemon, July 2018.

[3] Kelly Bissell, et al., "Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon, March 6, 2019.

[4] "2018 Cost of a Data Breach Study," Ponemon, July 2018.

[5] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO Online, March 14, 2016.

[6] "2018 Cost of a Data Breach Study," Ponemon, July 2018.

[7] Steve Culp, "How The Compliance Function Is Evolving In 2018—Five Key Findings," Forbes, March 27, 2018.

[8] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens," (ISC)^2, October 2018.

[9] "2018 Cost of a Data Breach Study," Ponemon, July 2018.

[10] Kelly Bissell, et al., "Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon, March 6, 2019.

FORTINET®

www.fortinet.com

367440-0-0-EN

March 22, 2019 1:06 PM

eb-FortiAnalyzer-032219-115pm