FORTINET

Fortinet Solutions for Automation-driven Network Operations

Table of Contents

FORTINET

Executive Overview

The rapid influx of digital transformation (DX) technologies has made networks and network security much more complex—and vulnerable. While malicious cyber-attacks remain a serious problem, more than half of all breaches last year came from benign sources that could have been prevented. In this regard, a security strategy that prioritizes automation-driven network operations can help. As part of the Fortinet Security Fabric, FortiManager and FortiAnalyzer support network operations use cases for centralized management, compliance, and automation to provide better detection and protection against breaches.

- **Last year, 52% of all breaches were caused by human errors or system glitches.**
- **The average total cost of a data breach grew to $3.86 million.**
- **The average probability of a material breach in the next 24 months rose to 27.9 %.[1]**

[1] "2018 Cost of a Data Breach Study," Ponemon, July 2018.

The challenges of increasingly complex and naturally fragmented infrastructures continue to enable a rise in cyber events and data breaches. A paucity of security devices is not the problem. Rather, an assortment of point security products deployed by most enterprises almost always operate in isolated silos. Subsequently, network operations teams rarely have clear and consistent insight into what is happening across the network.

Ponemon's 2018 Cost of a Data Breach Study exposes some interesting trends. The average cost of a breach last year grew by 6.4% from the previous year to $3.86M. The global average likelihood of a breach occurring in the next 24 months continues to creep up—rising from 27.7% in 2017 to 27.9% in 2018. And more than half (52%) of all breaches were caused by either human errors or system glitches (as opposed to malicious or criminal attacks).[2]

An integrated security architecture with automation-driven network operations capabilities can eliminate breaches caused by these sorts of errors and glitches. The **Fortinet Security Fabric** includes the centralized management of **FortiManager** combined with centralized logging and reporting of **FortiAnalyzer** to address the key use cases for effective network operations.

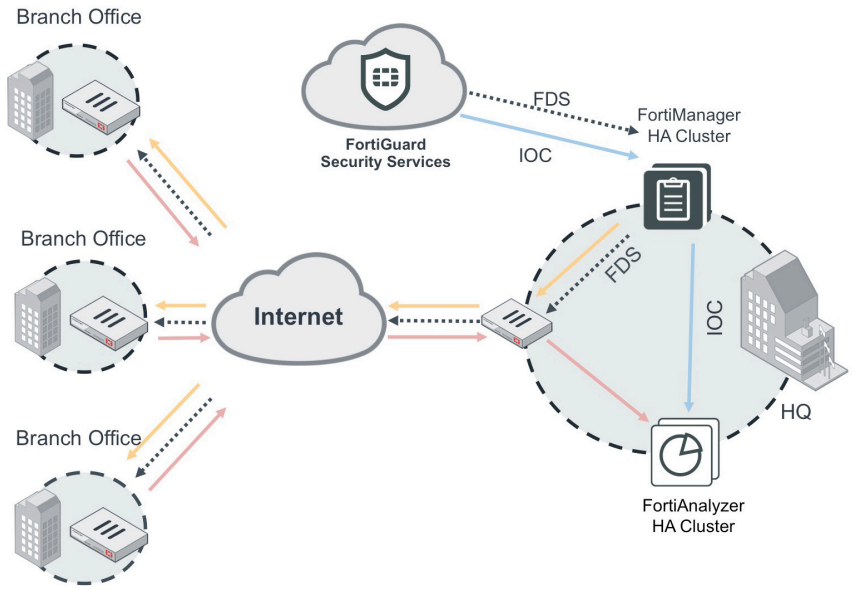

Figure 1: Network operations featuring FortiManager and FortiAnalyzer hardware appliances.

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

Use Case: Centralized Management and Visibility

When it comes to security, the average enterprise deploys solutions from 75 different vendors.[3] These disparate products typically cannot share threat intelligence or coordinate responses across an increasingly dispersed organizational infrastructure. This critical cybersecurity shortcoming is often compounded by a lack of skilled security personnel to manage a wide assortment of disconnected point products.

But even large organizations with dedicated IT staffs still have difficulty monitoring the network to keep track of which devices are connected, who has access to data, where data is stored, and which resources are needed by applications and workflows. However, a centralized management solution with a single-pane-of-glass view like FortiManager enables streamlined visibility that reduces complexity. It allows teams to monitor data movement and identify anomalous activity, simplifies solution optimization, and centralizes the management of firewalls and other security tools from a single location. It also streamlines operations for limited or under-resourced administrators and security staff.

3 Ways That FortiManager Centralizes Management and Visibility

Broad device management:

- Provides enterprise-grade controls across the network infrastructure
- Scales to support management of 100,000-plus Fortinet devices

Enterprise configuration and change management:

- Supports geographically dispersed high availability with up to five units
- Simplifies central configuration and change management with your existing tools
- Enables creation of administrative domains for better segregation of networks

Visibility:

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

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

There will be as many as 3.5 million unfilled cybersecurity positions by 2021.[4]

[4] Steve Morgan, "Cybersecurity Jobs Report 2018-2021," Cybersecurity Ventures, May 31, 2017.

Use Case: 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 each individual vendor's audit tools and then corollate that information to prove compliance. This complex and unwieldy auditing process is inefficient and often ineffective.

FortiManager and FortiAnalyzer automate compliance tracking and reporting of industry regulations and security standards—and this is integrated at the network operations layer. FortiManager natively provides the capability of evaluating the network environment against best practices. Network operations teams then apply and enforce them 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 identify where immediate response is required.

Three Ways That FortiManager 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), Center for Internet Security (CIS)
- Includes a security rating report based on hundreds of Fortinet Security Best Practices

Role-based visibility:

- Offers targeted dashboards for key enterprise stakeholders, including CIO, CISO, Network Architect, and Security Architect
- Includes a security assessment dashboard for Security and Operations (SecOps)

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%).[5]

[5] Steve Culp, "How The Compliance Function Is Evolving In 2018," Forbes, March 27, 2018.

Use Case: Automation and Integration

DX is driving a majority of workloads into the cloud—public, private, or hybrid—for greater efficiency. As part of this trend, DevOps brings together two teams that have historically worked in silos (software development and IT operations) to speed up processes through integration of effort and automation. While DevOps can help accelerate time to market, it also creates greater complexity in terms of security. Some of the ways security can increase the complexity of network operations include: constant application testing and security monitoring, time staff spends dealing with false positives, audit trail tracking and reporting, and the need to train developers and operations staff on security best practices. In addition to the efficiency impact, this also incurs more costs.

When the de facto security controls for DevOps environments are piecemeal and conducted in solution silos, critical protection becomes inefficient (slow time to remediation for threats, which escalates risk to operations and sensitive content), is costly, and is unable to address security or compliance requirements. Even worse, this approach to security can inhibit DevOps productivity. In response, DevOps teams often increase the risk of threats by compromising security controls to meet time-to-delivery objectives. For example, 52% of DevOps teams admit they scaled back security measures to meet a business deadline or objective.[6]

To be successful, security must be seamlessly integrated into DevOps. It requires full visibility of the entire attack surface from a single location. Advanced threat detection must be in place to minimize false positives, and security responses must be automated so that DevOps processes are not obstructed or slowed.

FortiManager helps decrease threat remediation time from months to minutes by coordinating policy-based automated response actions across the Security Fabric's integrated solutions. Detected incidents, combined with detailed evidence and forensics, not only allow network administrators to determine a resolution, but events can also trigger automatic changes to device configurations to close the loop on attack mitigation. FortiManager facilitates automation and orchestration by enabling zero-touch provisioning across distributed organizations, such as school districts, healthcare organizations, branch offices, and retail environments.

Three Ways That FortiManager Helps with Automation and Integration

Deployment and maintenance:

- Provides an application programming interface (API) that enables anyone to manage Fortinet deployments and integrate with external provisioning, monitoring, inventory, and change-management systems
- Includes command line interface (CLI) support via sample scripts provided on the Fortinet Developer Network (FNDN)

Integrations:

- Fabric Connectors provide integration for FortiGate or FortiManager to manage policies in a single console across multiple software-defined network (SDN), cloud, and partner technology platforms

Workflow and orchestration:

- Enables rapid or automated responses with FortiOS Automation Stitches—a simple way to define actions on triggers
- Provides interoperability with existing management and analytics tools

[6] "52% of Companies Sacrifice Cybersecurity for Speed," Threat Stack, March 13, 2018.

83%

of enterprise workloads will be in the cloud by 2020.[7]

[7] Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020," Forbes, January 7, 2018.

Improving Network Visibility, Compliance, and Automation

As part of the Fortinet Security Fabric, FortiManager and FortiAnalyzer provide automation-ready single-pane-of-glass management, transparent visibility, advanced compliance reporting, and network-aware rapid response across on-premises, cloud, and hybrid environments.

In combination, these automation-driven network management capabilities help reduce risk around key causes for cyberbreaches (i.e., system glitches and human errors). They also improve efficiency by providing administrators a centralized and simplified view for managing their entire infrastructure. And finally, they reduce the total cost of ownership (TCO) through automation that improves security while easing the burden on constrained IT resources.

www.fortinet.com

345418-0-A-EN

February 26, 2019 11:30 AM

ebook-fortinet-solution-for-automation-022619-1129am