FORTINET

Simplify and Automate Network Operations

Table of Contents

Executive Overview

Rapid adoption of new digital innovations like cloud services and Internet-of-Things (IoT) devices has caused network infrastructures to become increasingly complex and fragmented. At the same time, most organizations face a shortage of skilled employees and ever-increasing compliance requirements. To help mitigate this perfect storm of operational complexity, enterprises must embrace the simplicity and efficiency of an integrated architecture. Security integration enables simplified provisioning, centralized management, real-time analytics, simplified compliance auditing and reporting, and automation of manual workflows and network operations.

Network Integration Untangles Complexity Challenges

Complexity creates several challenges for network engineering and operations leaders when it comes to protecting their infrastructures. First, visibility and control of network defenses is reduced due to an accumulation of disconnected point network and security products. On top of this issue, a continuing worldwide shortage of security talent means most organizations lack the staff and skills to manage all these individual tools. Finally, ever-increasing compliance requirements often require manual compilation for reports and audits—which puts an escalating burden on already-strained teams.

Embracing an integrated network security infrastructure is the first step toward solving these critical problems. A network security architecture that connects all deployed solutions across the organization provides the foundation for critical capabilities such as simplified provisioning, centralized management, security fabric analytics, seamless compliance reporting, and automated operations.

More than one-quarter (27%) of network engineers feel they lack transparent visibility across the entire attack surface.[1]

Simplified Provisioning

An integrated security architecture can enable advanced security orchestration capabilities for provisioning and configuration. These can alleviate many complexity challenges for growing organizations—all while improving efficiency or operations and reducing the workflow burdens on limited staff resources. As a business expands or adds new offices through mergers and acquisitions (M&A), automated onboarding capabilities allow for fast and seamless scalability of security to all reaches of the organization's expanding network.

An effective security architecture should support capabilities like zero-touch deployment to help organizations simplify and accelerate bringing new locations online. Here, zero-touch deployment enables a security device—such as a next-generation firewall (NGFW)—to be plugged in at a branch office or remote location and then automatically configured at the main office via broadband connection to avoid the time and cost of truck rolls. It should also leverage existing configurations as a template to accelerate deployment of new branches and remote sites at scale.

Centralized Management

Operations must be able to monitor data movement and identify anomalous activity, but security complexity obscures this ability. Companies deploy on average 47 different security solutions and technologies, many of which only address a single attack vector or compliance requirement.[2] Siloed devices in a disaggregated security architecture do not communicate with one another or share threat intelligence. When network engineering and operations teams must juggle multiple management consoles from different vendors, this inhibits clear, consistent, and timely insight into what is happening across the organization.

An integrated security architecture with centralized management capabilities simplifies visibility and control by consolidating the multiple management consoles associated with a disaggregated architecture of point devices. Here, an effective management solution should provide a single-pane-of-glass view to track all the solutions deployed to protect the network across the organization and apply policy-based controls with ease and consistency. As more than half (52%) of all breaches are caused by human errors or system glitches (as opposed to malicious or criminal attacks),[3] centralized management of all distributed networks across the organization helps network leaders drastically reduce the opportunities for configuration errors that lead to security risks and outages.

Two-thirds of organizations (66%) are actively consolidating the number of cybersecurity vendors with which they do business for better operational efficiency and cost savings.[4]

Real-time Analytics

As the number of branches grows within an organization and the network-edge attack surface grows, network engineering and operations leaders increasingly need to rely on real-time analytics to instantly measure and identify network and security risks. To address this, an integrated security architecture can coordinate data across all deployed parts of the infrastructure to provide comprehensive reports that combine network traffic, applications, and overall network health.

Features such as enterprise-grade configuration management and role-based access controls (RBAC) can help network operations and engineering leaders easily track changes and mitigate human errors. It can also provide service level agreement (SLA) logging and history monitoring as well as customizable SLA alerting. Additional capabilities include network bandwidth monitoring reports and adaptive response handlers for network events.

Compliance Reporting

Virtually all compliance regulations require documentation. A strong audit trail that tracks every incident, action, and outcome offers organizations data to prove compliance with regulations. Compliance management, however, is very often a heavily manual, labor-intensive process. Depending on the industry and organization, it can require months of work involving multiple full-time staff.

For organizations with multiple point security products, data must be assembled from each of them and then normalized to ensure that regulatory controls are reported accurately. To do so, network operations staff must monitor security controls using each individual vendor's audit tools and subsequently correlate that information to prove compliance. These complex and unwieldy auditing processes are inefficient and very often ineffective due to human errors.

Two-thirds (66%) of security professionals report that compliance mandates are a driving factor for security spending.[5]

Automation of compliance tracking and reporting at the network operations layer can streamline these processes, allowing limited networking and security staff to focus on more critical operations activities. An effective security management solution should provide compliance templates for both best practices and regulations to help reduce the cost and burdens of complexity. Specifically, the solution should provide real-time reports on industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS). Further, it should also support security standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS) Security Controls.

Effective security management should also include tools to help networking leaders evaluate their environment against industry best practices. Part of this process includes aggregation and reconciliation of threat data from multiple sources. Network operations teams then apply recommendations to protect against threat exposures.

Privacy regulations have sharpened the focus on protecting personally identifiable information (PII)—59% of security professionals say it is now their top priority.[6]

Network Automation

According to a recent study, the global cybersecurity workforce gap estimate is now 4.07 million with 65% of companies currently reporting a shortage of skilled staff in critical areas.[7] As a result, analyst investigations take longer, remediation steps get missed, and incidents may be handled inconsistently from day to day.

The global cybersecurity workforce needs to grow by 145% to meet the current demand for skilled cybersecurity talent.[8]

Enter security integration, which unlocks the power of automation across the network—coordinated responses to threats that help organizations protect their network with limited staff resources. Automated workflow optimizations eliminate manual steps requiring human intervention (e.g., alert correlation and research) to shrink the window between detection of and response to threats. It also helps to omit operational anomalies caused by human errors. Intelligence sharing and automation capabilities are now critical to protecting data and operations.

In a four-year study of security cost savings, automation offered the second-highest net savings among the reporting group of businesses.[9]

Evolving to Automation-driven Network Management

An integrated architecture can help detangle complexity challenges and reduce risk around key causes of cyber breaches (i.e., system glitches, misconfigurations, and human errors) through what is sometimes called automation-driven network management.

This includes simplified provisioning capabilities, single-pane-of-glass management, analytics, advanced compliance reporting tools, and network-aware rapid responses across all parts of the network (on-premises, cloud, and hybrid environments). Fortinet's Fabric Management Center, which includes FortiManager and FortiAnalyzer, provides customers with these capabilities and helps improve efficiency of operations of network administrators with a centralized and simplified view for overseeing their entire Fortinet Security Fabric infrastructure.

When evaluating solutions, all teams should examine how best to invest to improve efficiency, reduce risk, and reduce total cost of ownership (TCO). An integrated network security architecture that prioritizes network automation capabilities can solve the persistent challenges of infrastructure complexity.

[1] "Cybersecurity and the Network Engineering and Operations Leader: A Report on Current Priorities and Challenges," Fortinet, September 4, 2019.

[2] "53% of enterprises have no idea if their security tools are working," Help Net Security, July 31, 2019.

[3] "2019 Cost of a Data Breach Study," Ponemon Institute and IBM Security, July 2019.

[4] Jon Oltsik, "The cybersecurity technology consolidation conundrum," CSO, March 26, 2019.

[5] Michael Nadeau, "Compliance mandates, cybersecurity best practices dominate 2019 security priorities," CSO, October 23, 2019.

[6] Ibid.

[7] "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study 2019," (ISC)², November 2019.

[8] Ibid.

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

www.fortinet.com

667870-0-0-EN

May 9, 2020 6:36 AM

eb-simplify-and-automate-network-operations-V1-592020-522AM