FORTINET

How to Simplify Network Operations Complexity

Executive Overview

By rapidly adopting new digital technologies like cloud services and Internet-of-Things (IoT) devices, network infrastructures have become increasingly complex and fragmented. At the same time, most organizations face a shortage of skilled employees and ever-increasing demands from evolving compliance requirements. To help mitigate this perfect storm of operational complexity, enterprises must embrace the greater simplicity of an integrated architecture. This enables transparent network visibility, centralized management, simplified compliance auditing and reporting, and automation of manual workflows and network operations.

Table of Contents

FORTINET

01 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, most organizations lack the staff and skills to manage all these individual tools. This is largely due to network and security organizations feeling the pinch of a continuing worldwide talent shortage of skilled security positions. Finally, ever-increasing compliance requirements require manual compilation for reports and audits—which puts an escalating burden on already strained human resources.

Embracing an integrated network security infrastructure is the first step toward eliminating these critical problems. A network security architecture that connects all deployed solutions across the organization provides the foundation for critical capabilities such as unified visibility, automated workflows, and simplified compliance management.

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

02 Centralized Management

Operations must be able to monitor data movement and identify anomalous activity—but security complexity obscures this ability. The average enterprise uses upwards of 75 different security solutions, 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 have to juggle multiple management consoles from different vendors, this inhibits clear, consistent, and timely insight into what is happening across the organization.

To address these challenges, organizations need an integrated security architecture with centralized management capabilities. This 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 console to track all the solutions deployed to protect the network across the organization and apply policy-based controls with ease and consistency.

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.[3]

03 Automation and Orchestration

A recent study reports that 51% of companies have a problematic shortage of both cybersecurity staff and specific skills, and that most companies lack the staff needed to manage a vast set of individual security tools.[4] Subsequently, analyst investigations take longer, remediation steps get missed, and incidents may be handled inconsistently from day to day.

More than half (59%) of organizations report that a cybersecurity staff shortage puts them at extreme or moderate risk.[5]

Security integration 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 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.

As another related benefit, security orchestration can remedy many complexity challenges by bringing together disparate tools and systems to work in concert with one another. Here, orchestration helps to codify and streamline the processes that surround the technologies. For example, as the business grows or adds new offices through mergers and acquisitions (M&A), zero-touch deployment and flexible onboarding capabilities allow for fast and seamless scalability of security to all reaches of the organization's expanding network.

In a recent four-year study of security cost savings, automation offered the second-highest net savings among the reporting group of businesses.[6]

04 Compliance Support

Virtually all compliance regulations require documentation. A strong audit trail that tracks every incident, action, and outcome provides organizations the data they need to prove their compliance with all requirements.[7] But compliance management is very often a 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.

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) and the Center for Internet Security (CIS) Cybersecurity Framework.

Effective security management should also include tools—such as security ratings—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.

57%

of enterprises will prioritize compliance technology investments over the next 12 months.[8]

05 Evolving to Automation-driven Network Management

An integrated security 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 single-pane-of-glass visibility, automation and orchestration capabilities, advanced compliance reporting tools, and network-aware rapid responses across all parts of the network (on-premises, cloud, and hybrid environments). These features improve efficiency by providing network administrators with a centralized and simplified view for overseeing their entire infrastructure. At the same time, they also reduce costs, ease the burden on limited staff resources, and improve the organization's overall security posture.

[1] "The Network Engineering and Operations Leader and Cybersecurity Report," Fortinet, Forthcoming.

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

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

[4] Jon Oltsik, "The problems plaguing security point tools," CSO Online, January 30, 2019.

[5] "Cybersecurity Workforce Study, 2018," (ISC)², October 2018.

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

[7] Stan Engelbrecht, "Five Strategies for Extending Automation and Orchestration Beyond the SOC," SecurityWeek, June 8, 2018.

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

www.fortinet.com

367628-0-0-EN

June 1, 2019 7:26 PM

eb-simplify-network-operations