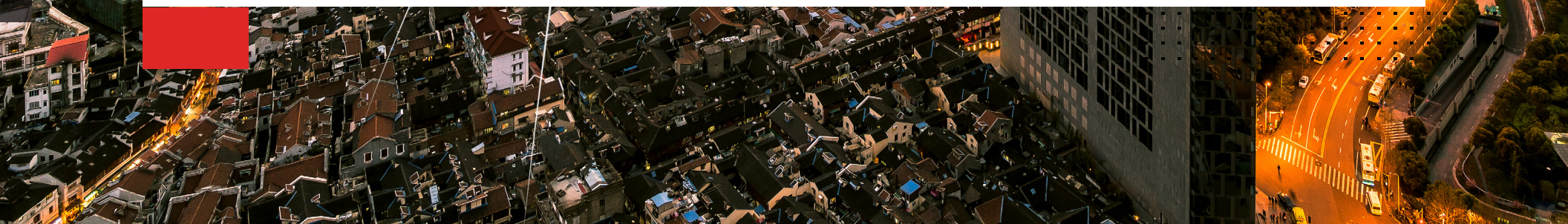
FORTINET

# How Network and Security Convergence Simplifies and Automates Network Operations



# Table of Contents

# Executive Overview

The pandemic has increased the rate of digital acceleration, as organizations adapt to new work models and users' demands to stay competitive. Adoption of technologies and architectures such as software-defined WAN (SD-WAN), software-defined branch (SD-branch), Internet-of-Things (IoT), multi-cloud, and zero-trust access (ZTA), have 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 are embracing the simplicity and efficiency of an integrated architecture. Network integrations enable zero-touch provisioning, centralized management, real-time security 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. Gartner calls this idea a “Cybersecurity Mesh Architecture.”[1]

**According to Gartner, by 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a cooperative ecosystem will reduce the financial impact of individual security incidents by an average of 90%.[2]**

## Simplified Provisioning

An integrated security architecture can enable advanced security orchestration capabilities for provisioning and configuration. These can alleviate many complex 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 areas 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. 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.

Stanford University researchers found that approximately 88% of all data breaches are caused by an employee mistake. Human error is still very much the driving force behind an overwhelming majority of cybersecurity problems.[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.

**“Shortages of the cybersecurity professionals that organizations need to act fast enough to keep their data secure have motivated managed security service providers to move up the stack to offer a breadth of advanced technologies… across multiple environments in a consolidated security platform.”[4]**

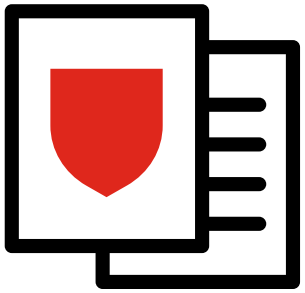
## Compliance Reporting

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. This is most likely why 85% of IT compliance and risk management professionals plan to evaluate new tools in 2022 to streamline and automate their compliance processes.[5]

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) 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. Then, network operations teams can apply recommendations to protect against threat exposures.



**45% of IT compliance and risk management professionals said they plan to spend 10-25% more on IT risk management and compliance in 2022 vs. 2021.[6]**

## Network Automation and Real-time Security 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 also can 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.

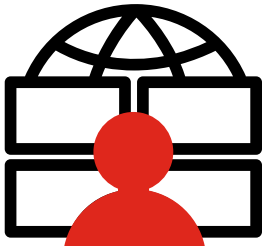
**“The human element continues to drive breaches. This year 82% of breaches involved the human element.”[7]**

## Cybersecurity Staff Shortages

According to the International Information System Security Certification Consortium, there are now more than 4.07 million unfilled cybersecurity positions across the world.[8] As a result, analyst investigations take longer, remediation steps get missed, and incidents may be handled inconsistently from day to day.

The longer it takes to remediate a breach, the more damage and expense to the organization. Both the length of time to contain a breach and total cost increased last year. The average number of days it takes to identify and contain a breach is 287. And, according to the same report, "Data breach costs rose from $3.86 million to $4.24 million, the highest average total cost in the 17-year history of the report."[9]

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.



**“The Cybersecurity Workforce Estimate and Cybersecurity Workforce Gap suggest the global cybersecurity workforce needs to grow 65% to effectively defend organizations’ critical assets.”[10]**

## Evolving to Automation-driven Network Management

An integrated architecture can help detangle complex 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 Network Operations, which includes FortiManager and FortiAnalyzer, provides 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] John Maddison, "Fortinet Security Fabric: The Industry's Highest-Performing Cybersecurity Mesh Platform," Fortinet, November 16, 2021.

[2] Gartner®, "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi, 18 October 2021.

[3] "Psychology of Human Error 2022: Understand the Mistakes That Compromise Your Company's Cybersecurity," Tessian, 2022.

[4] Martha Vasquez and Craig Robinson, "IDC Technology Spotlight: The Next Chapter in Managed Security Services is About Consolidation," March 2021.

[5] Jingcong Zhao and Cat Hausler, "2022 IT Compliance Benchmark Report," Hyperproof, 2022.

[6] Ibid.

[7] "2022 Data Breach Investigation Report (DBIR)," Verizon, 2022.

[8] "2021 Cybersecurity Workforce Study: A Resilient Cybersecurity Profession Charts the Path Forward," (ISC)², 2021.

[9] "Cost of a Data Breach Report 2021," IBM, July 2021.

[10] "2021 Cybersecurity Workforce Study: A Resilient Cybersecurity Profession Charts the Path Forward," (ISC)², 2021.

FORTINET®

www.fortinet.com



June 30, 2022 12:54 PM

667870-A-0-EN