WHITE PAPER

Navigating Network Complexity: Unraveling the Inefficiency and Risks of Digital Transformation

Executive Summary

The heart of digital transformation involves integrating digital technologies into every aspect of business operations. This approach can significantly change how businesses operate and interact with their customers, suppliers, and partners. It can also enable organizations to gain a competitive advantage by improving their business processes, developing new products, enhancing customer experiences, and expanding into new markets. And the benefits from digital transformation are significant, including increased revenue and market share, reduced costs, improved customer experience and loyalty, and increased efficiency and productivity.

76% of organizations use two or more clouds to integrate multiple services, scalability, or business continuity reasons.[1]

In this new model, the network is the backbone of the business, and its flexibility, performance, and availability play crucial roles in enabling digital transformation. However, for many organizations, digital transformation inevitably makes the network more complex and unwieldy through the rapid adoption of new technologies, the move to hybrid networks, the increasing number of connected devices and users, and the amount of data shared across a growing number applications, devices, and platforms. And this increasingly complex network, with distributed locations and often different infrastructures at each site, also makes security more difficult. Visibility is often fragmented, and coordination between discrete devices is impossible, increasing the likelihood of a critical cyber event or exploitable misconfiguration being overlooked. And the data bears this out. According to the 2023 Global Future of Cyber Survey by Deloitte, 91% of organizations reported at least one cyber incident or breach in 2022, compared to 88% in the 2021 survey.[2]

Network as a Challenge

Today, as companies grow, they also become more distributed. This allows them to remain close to their customers and suppliers. But as a result, their networks become more complex, often leading to dozens of vendors, solution sprawl, and isolated or even incompatible solutions deployed at different locations or in various lines of business. Such complexity leads to challenges in managing their network and security tools, particularly as the number of point products increases. The result is poor visibility, limited controls, gaps in coverage, and increased risk to the organization.

To keep up with the pace of transformation, businesses increasingly rely on acquiring new technologies. While this may help address new opportunities in the short term, they inevitably complicate their networks and security. The same challenge occurs as companies increasingly rely on cloud-based technologies that require additional layers of defense against cyberattacks. Likewise, adopting new technologies like Internet-of-Things (IoT) can exponentially increase the number of connected devices and endpoints on the network, significantly increasing the attack surface and making networks more complex and difficult to secure. Even the shift to essential new solutions, like zero-trust network access (ZTNA), adds complexity to network security through strict access controls and authentication requirements.

Inconsistency in Configuration and Security Policies

As digital transformation continues to connect growing numbers of mobile users and devices with applications and data that may be deployed anywhere, the underlying network has to keep evolving. Unfortunately, most legacy security tools were never designed to protect such highly dynamic environments, leading to misconfiguration or inconsistent security policy enforcement.

For instance, if a firewall is not configured correctly to restrict access, it could allow unauthorized users to enter the network. And if an application or workflow needs to move between different areas of the network, the handoff between various security tools may result in gaps in protection. Misconfiguration in access controls can result in improper permissions, allowing unauthorized users to gain elevated privileges and access sensitive data or resources they shouldn't be able to access.

Inconsistent network configuration can also hinder network visibility, making it difficult to detect and respond to security incidents promptly. And it can inadvertently expand the attack surface by leaving certain areas of the network more vulnerable than others.

Network Segmentation Becomes Complicated

As companies adopt more applications, users, and devices, the need for granular network segmentation also increases. For example, as the number of devices inside the network grows, the potential for a compromised system to generate enough bad traffic to cause network-wide performance issues also increases. And an attacker who manages to gain access to a remote segment of the network, perhaps through an undersecured home network, can easily move laterally to access resources in other areas. However, managing and maintaining network segmentation can be complicated and time-consuming, especially when dealing with a highly distributed hybrid network.

Network and Security Functions in Different Form Factors

As companies adopt hybrid environments, the need to deploy network and security functions in different form factors increases. For example, a retail company may want virtualized network and security tools deployed at its retail outlets while maintaining physical appliances at its headquarters.

Any network that combines hardware appliances, VMs, software tools, cloud-based services, and containerized solutions—each with its own set of functionalities and configurations—invariably introduces complexity, especially when trying to integrate and manage them. That's because solutions in different form factors often have their own management interfaces, protocols, and monitoring mechanisms. Administering and monitoring these diverse elements can be complex while scaling and optimizing these network and security functions can introduce additional complexity.

Differing Security Tools and Responsibilities

Modern network complexity translates to a lack of visibility for managing, monitoring, and securing users and devices. Physical firewall appliances, cloud and cloud-native virtual firewalls, SD-WAN solutions, Firewall-as-a-Service (FWaaS) solutions, and even access points and switches use different management consoles with often overlapping controls.

Adding to the complexity, digital transformation initiatives often require organizations to adopt new tools and technologies. But as companies adopt these new tools, IT teams may be unfamiliar with the best practices for securing them. The result is often a mishmash of devices that don't work together, resulting in security gaps and an increased risk of a security breach.

Misconfiguration of cloud security remains the biggest cloud security risk, according to 62% of cybersecurity professionals.[3]

"The advantage of the Fortinet Security Fabric is the single pane of glass. I do not want to have to go to five different interfaces to figure out a problem. With a team as lean as ours, we cannot be there in person every time someone has a security question. We use FortiManager for monitoring traffic, watching every event that might require a response."

Troy Neal
Executive Director, Cybersecurity and Technology Operation, Spring Branch Independent School District

And finally, digital transformation initiatives often require greater collaboration between IT and development teams. In the past, however, these teams often worked independently, with IT responsible for securing the network and development teams owning the building and maintenance of applications. However, these new initiatives require these teams to work together to ensure security is woven into the application development process. But this increased collaboration can be challenging, especially if IT and development teams have different priorities.

Human Error and IT Staff Shortages

Managing configurations across numerous devices and systems can be challenging, especially in complex network environments. And since few tools can span disparate systems, things like configurations, updates, and enforcement policies need to be manually deployed and coordinated. As a result, human error becomes more likely, leading to things like misconfigured access control lists (ACLs) on firewalls that can result in unintended network access or compromised security.

For companies taking a piecemeal approach, as their networks become more complex, managing them becomes increasingly time-consuming. This can be challenging for IT teams, particularly when combining the growing number of security alerts that must be addressed with the worldwide shortage of cybersecurity professionals.

By 2026, more than 60% of organizations will have more than one type of firewall deployment, which will prompt the adoption of hybrid mesh firewalls.[4]

A Hybrid Mesh Firewall Helps Reduce the Complexity Introduced by Digital Transformation

A hybrid mesh firewall (HMF) provides coordinated security protection across multiple areas of enterprise IT, including the branch, campus, data center, public and private clouds, and remote workers. An HMF architecture bridges on-premises and cloud-native security through a single control point. And its common policy framework enables organizations to define and enforce security policies between different workloads, workloads and users, and workloads spanning mixed IT environments.

An HMF also helps address network and security complexities due to its support of various form factors, including appliances, virtual machines, cloud-native firewalls, and FWaaS. This enables organizations to choose the form factor that best suits their network architecture and security requirements and then integrate it into their larger HMF framework.

An HMF also enables granular control over security policies that span workloads, users, and mixed IT environments. With coordinated security protection across multiple areas of enterprise IT, HMF can help pinpoint and respond to security threats more quickly and efficiently.

Why Fortinet

Fortinet has been innovating the convergence of security and networking for over two decades to reduce network complexity while increasing overall security effectiveness across today's expanding networks. This starts with a unified platform built on our unifying operating system, FortiOS, to support every Fortinet product. AI/ML threat intelligence from FortiGuard Labs feeds the latest threat intelligence back into the Fortinet Security Fabric, enabling FortiManager and FortiAnalyzer—our centralized and unified management tools—to provide consistent visibility and security across today's complex hybrid environments.

This approach uniquely enables the deployment of FortiGate Hybrid Mesh Firewall deployments across on-premises and cloud environments—and it also includes Secure SD-WAN, Secure WLAN/LAN, Universal ZTNA, and FortiSASE.

When deployed as part of the Fortinet Security Fabric, FortiGate HMFs help organizations address the network and security complexities introduced by their digital transformation efforts with the following:

- Deep visibility across all edges
- Central and unified management of distributed solutions
- Consistent policies and enforcement
- Automated workflows for configurations, changes, and responses
- Real-time global threat intelligence across Fortinet Security Fabric and Fabric-Ready Partner deployments

[1] "Top Cloud Security Trends in 2021," Fortinet, June 8, 2021.
[2] "2023 Global Future of Cyber Survey," Deloitte, 2023.
[3] "2022 Cloud Security Report," Cybersecurity Insiders, 2023.
[4] Gartner, "Magic Quadrant for Network Firewalls," Rajpreet Kaur, Adam Hils, Tom Lintemuth, December 20, 2022.

FORTINET

www.fortinet.com

June 20, 2023 8:23 AM
2172943-0-0-EN