FORTINET

Staying Ahead of Cyberthreats: Leveraging the Power of Secure Networking

Table of Contents

Executive Overview

While digital acceleration delivers many benefits, such as reduced costs, faster growth, and better user experience, it has also led to a rapid expansion of attack surfaces and new network edges. These include the local area network (LAN), the wide area network (WAN), 5G, remote workers, and clouds.

The overarching challenge of digital acceleration is that rapid IT changes often result in new vulnerabilities, which are outpacing the security team's ability to protect them from cyberthreats.

Networks today are the center of innovation and enable digital acceleration using network modernization. Adopting a secure networking strategy helps fortify organizations so they can be safe and successful in their digital acceleration efforts.

“Eighty-nine percent of board directors say that digital business is now embedded in all business growth strategies. However, just 35% of board directors report that they have achieved or are on track to achieving digital transformation goals.”[1]

Introduction

Growing and scaling digital business while protecting a distributed infrastructure has never been more critical or complex. The result has been disastrous because most traditional network architectures were built using disparate and statically deployed point products that provide implicit access to all applications. Ransomware, phishing, botnets, and other criminal activity are now at an all-time high.

It's also problematic when the user experience is hampered and slowed by traffic rerouted for inspection to fixed security tools that cannot adequately examine encrypted applications, data, or video streams. Furthermore, when the cybersecurity solutions are not integrated and cannot work together with the network to protect against any of the discovered threats, things can get extremely unpleasant for the workforce.

A new approach is needed to provide secure access to critical resources across the entire corporate footprint. The key security, networking, and operations tools and integrations that are required to implement secure networking are covered in this ebook.

Components to Achieve Secure Digital Acceleration

A modern enterprise network needs solutions spanning three areas to achieve robust, secure networking: robust security at the edges and for remote users, innovative networking solutions that can adapt to evolving business demands, and a unified and simplified network operations solution to address issues before they become a disruption.

Hybrid mesh firewall architecture: unified security and management across the organization

Today's cybercriminals exploit the lack of consistent security and visibility across various distributed network segments found in most enterprises. Because data centers, campuses, multi-cloud, and branch environments are now interconnected, east-west traffic across the network has increased. This allows a successful breach in one area of the network to quickly spread to others. The most effective way to address this challenge is to deploy consistent security in every part of the network—but differences between various network ecosystems have made that difficult.

Hybrid mesh firewalls (HMFs) are designed to consistently integrate critical next-generation firewall (NGFW) features across your network, including campus, data center, and public and private cloud environments, as well as Firewall-as-a-Service and secure access service edge (SASE) to secure remote users and locations—all run under a centralized and cohesive management solution. This approach creates a single, integrated platform that spans, scales, and adapts to today's dynamic and distributed networks. An HMF approach coordinates protection across IT domains (corporate sites, public and private clouds, and remote workers) from a unified management console. This integration allows IT teams to automate threat detection and response, orchestrate configurations, and enforce policies without investing needless manual hours, especially when the cybersecurity skills gap is already constraining resources.

Security for Edges and Users

Powerful next-generation firewalls

Next-generation firewalls, especially HMF solutions, are essential for modern enterprises needing to secure their increasing attack surface driven by the growth in network edges. But today's advanced firewalls must also utilize artificial intelligence (AI) and machine learning (ML) to enhance threat intelligence and accelerate the prevention, detection, and response to various attacks, including zero-day attacks, APTs, and unknown threats.

And with the majority of internet traffic being encrypted, these firewalls must also be able to inspect encrypted traffic without performance loss, especially as users rely on latency-sensitive business applications. To ensure robust automated protection, they must provide comprehensive visibility and threat detection, even through SSL/ Transport Layer Security (TLS 1.3) encrypted traffic. They must also be optimized for flexibility, enabling them to be deployed consistently across various enterprise environments, including distributed branches, campuses, data centers, and cloud infrastructures, supporting a unified, holistic security posture.

In addition to proven security controls, a cutting-edge NGFW should encompass:

1. **Unified management:** Integration of on-site and cloud security under a single HMF system for streamlined operations
2. **Dynamic segmentation:** Adaptive structuring to safeguard essential applications and user groups through dynamic segmentation of the network
3. **Embedded access control:** Real-time validation of user and device access to maintain continuous security integrity
4. **Microsegmentation:** Detailed oversight and defense mechanisms tailored to specific applications and data flows to enhance security within network segments

Encrypted traffic has hit 95%.[2]

Cloud-delivered SASE for hybrid work security

Over the past several years, organizations have been expanding their multi-edge networking strategies to enable new work-from-anywhere (WFA) realities and support workers as they become increasingly dependent on cloud applications and environments to do their jobs. However, as these networks grow to meet new business demands, the attack surface increases. The result is a growing gap between network functionality and security coverage that inherently exposes organizations to more points of compromise and degrades the user experience of those remote workers who still rely on the conventional, virtual private network (VPN)-only solutions to access the network. This is usually because all their application traffic still needs to be backhauled through the network to receive security protections and access controls. Secure access service edge solutions have been developed to address these issues, enabling organizations to rapidly converge and scale out their security and networking strategies. With SASE, they can securely deliver an expanding and dynamic set of new network edges as well as meet the new demands of a hybrid workforce distributed between on- and off-network users.

An efficient SASE solution provides:

- **A single-vendor SASE architecture:** SASE is designed to deliver secure, cloud-based connectivity. However, very few enterprise networks are cloud-only. Even though many enterprises have a multi-cloud strategy, most still have physical networks. This means that cloud-only security is, by definition, incomplete security. Organizations need to insist on SASE services that are integrated with—or can be deployed as a seamless extension of—the extended network, including SD-WAN security. This is called the single-vendor SASE approach.

- **Enterprise-grade security everywhere:** When assessing any SASE solution, the functionality and performance of its security elements need to be effective. The SASE solution should include components that fully secure all applications and edges and provide secure access to the internet, SaaS applications, and corporate applications, wherever they are located.

- **Seamless convergence between networking and security with unified tools:** Legacy equipment is here to stay. SASE integration with on-premises solutions is essential for streamlined operations and to facilitate change. Seamless integration between on-premises security (SD-WAN and NGFW) and cloud security is key for operations simplification, compliance requirements, and consistent security posture among all users. A SASE solution also extends the convergence of networking and security from the network edge to remote users with unified management, a unified agent, and digital experience monitoring (DEM) for streamlined operations.

Networking Innovations

Software-defined WAN

Digital acceleration, WFA, and sophisticated cyberattacks are driving changes in the traditional router-centric, hub-and-spoke, and heavily multiprotocol label switching (MPLS) WAN architecture. These reactive changes result in poor user experience, ineffective security, and complex operations.

With converged NGFW and software-defined WAN (SD-WAN) capabilities, organizations can deliver superior quality of user experience, achieve operational efficiencies, and provide a better return on investment (ROI).

The right SD-WAN solution provides:

- **Converged WAN and security:** Deliver built-in SD-WAN, NGFW, advanced routing, and ZTNA all in one solution to protect the entire digital attack surface. Furthermore, it integrates DEM to improve employee productivity.

- **Optimized hybrid workforce experience:** Enhance the user experience and security posture with consistent security policies and explicit access per application across all edges.

- **Enhanced hybrid, multi-cloud connectivity:** Enable secure, seamless, faster connectivity to the cloud, within the cloud, and across clouds with a single virtual machine, simplifying management, reducing the footprint, and enabling cloud on-ramp orchestration.

“By 2026, 60% of new SD-WAN purchases will be part of a single-vendor SASE offering, up from 15% in 2022.”[3]

LTE/5G wireless WAN

Challenges arise as enterprises adopt cloud technologies and move away from MPLS networks. For instance, the internet as a corporate connectivity medium is opaque and often unreliable, making it difficult for IT to deliver a high-quality experience to stakeholders. In addition, physical cable, DSL, and fiber lines are limiting, preventing enterprises from deploying edge broadband at every branch. Finally, opening numerous branches to direct internet connectivity presents a multitude of management and security risks for the enterprise.

What's needed is a secure cellular gateway that provides LTE/5G wireless WAN for ultrafast, reliable, widespread edge connectivity to the cloud. These gateways should be equipped with the latest LTE/5G technology to transform your branch connectivity, no matter its proximity to cable, DSL, or fiber.

A secure cellular gateway provides users with:

- **Dual SIM** for fast cellular failover and high availability
- **Out-of-band management** to help ensure business continuity at sites

Secure LAN solution (secure Ethernet switches and Wi-Fi access points)

The wired and wireless LAN forms the backbone of IT, enabling next-generation applications and increasing user productivity. The LAN greatly impacts user experience and is the beginning or end of many security events that occur at the enterprise. The LAN tends to be insecure by nature. Its purpose is to allow people to connect and give access to the deeper network. However, as we have asked these networks to do more and connect more resources, our means to secure them have often not kept up. This leaves the network a prime target for unauthorized entry.

Secure connectivity LAN delivers:

A secure networking LAN edge solution should deliver:

- **Security convergence:** The wired and wireless access layer should be built upon a foundation of security controls to avoid configuration mismatches. Having a common management interface for security and networking reduces the network's risk profile.

- **Complete scalability:** Switching form factors offering 1, 10, and 40 GE access ports with up to 100 GE uplinks should be available to scale from the desktop to the data center. Access points should offer a variety of antenna patterns and physical form factors to ensure coverage regardless of the environment.

- **Zero-touch provisioning:** Automatic provisioning of equipment, global VLAN, security policies, firewall interfaces, and Ethernet ports should be easy.

- **Network access control:** The LAN must be able to identify corporate and IoT devices and automatically determine their level of privilege or network access, then onboard them accordingly.

Simplified Network Operations

Unified and automated management

Manual operations in the network operations center (NOC) inhibit the ability to quickly detect and respond to potential threats to the network. They are not only error-prone and slow but also result in breaches. Secure networking starts with an HMF architecture that unifies all network and security management. It enables consistent security and visibility into all attack surfaces, including locations, users, devices, and applications. Without that visibility, organizations will not have insights or the ability to act on their operations.

Look for these abilities in a NOC management tool:

- **Centrally manages all aspects of network functions:** Simplifies all aspects of network management from deployment to provisioning and from security policy setup to monitoring and response.
- **Scalable and flexible:** Supports mass provisioning and updates while granular enough to configure user-defined rules.
- **Integrates with the SOC:** Aggregates and automates information transfers between the security operations center (SOC) and existing enterprise applications and services.
- **Streamlines and automates:** Simplifies Day 0 operational workflows and optimizes Day 1 and Day 2 troubleshooting with advanced technologies, such as AI for network operations (AIOps).

“Signs that indicate your NOC is outdated: lack of automation, limited visibility, inflexibility, poor integration, lack of security.”[4]

Digital experience monitoring

DEM is essential in any business landscape powered by cloud services and remote work. As companies operate over networks they don't own, DEM ensures they can still oversee and enhance the complete online experience of their users. It pivots NOC teams from just monitoring performance to actively improving application availability and user interactions across all networks. DEM brings all user experience insights into one platform, clarifying user engagement, no matter where they are or where the apps are hosted.

Key benefits of a DEM solution include:

- **Edge monitoring:** DEM offers a panoramic view of the network edge, directly boosting employee efficiency.
- **User-app interaction tracking:** It allows NOC teams to track and optimize how employees interact with critical business applications, ensuring smooth digital operations.
- **SLA management:** DEM tools proactively test and refine the user-app experience globally, aiming to surpass service level agreements and heighten customer satisfaction.

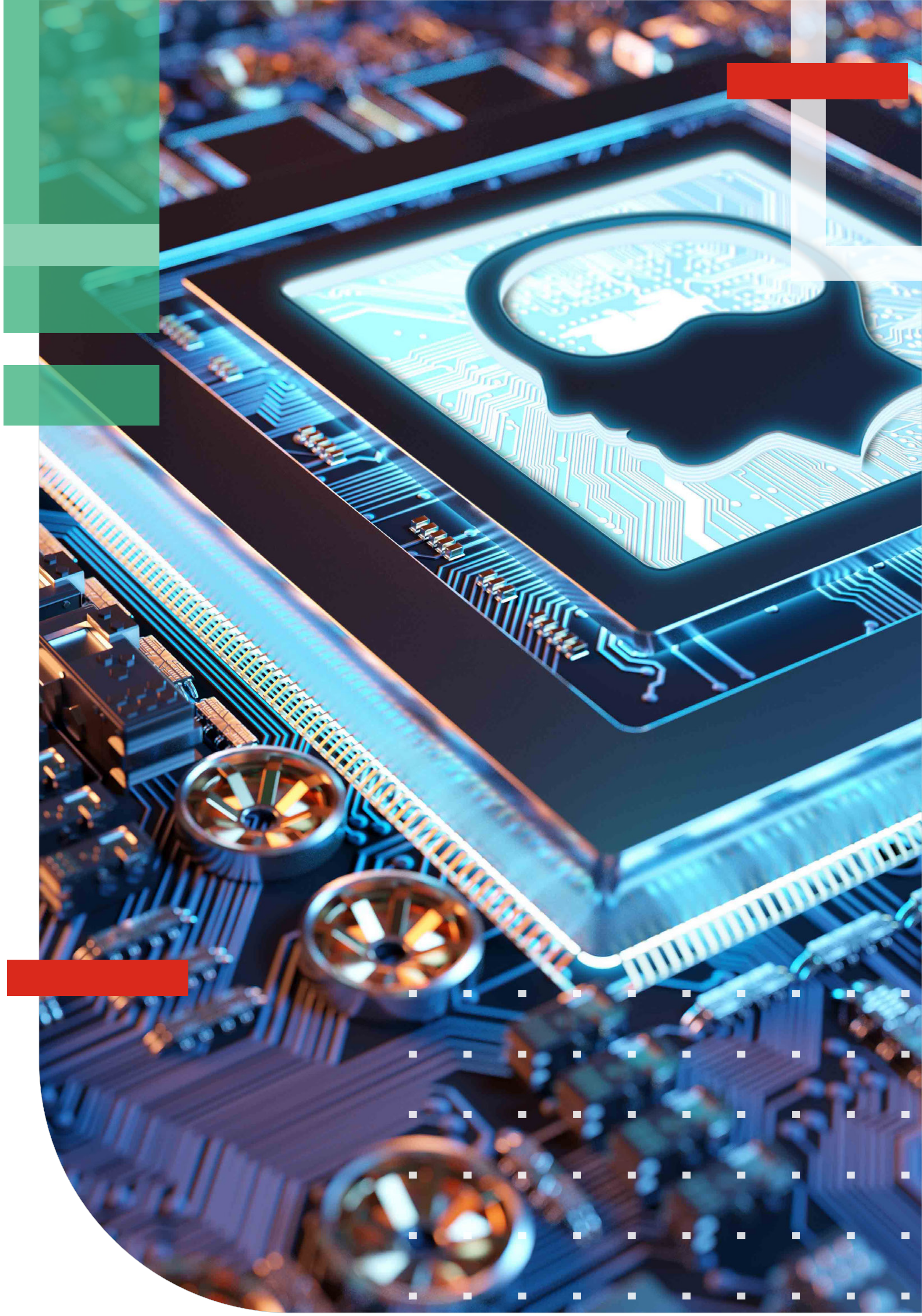
AI network operations

As the modern network gets more complicated, it gets more difficult for IT staff to manually sort through network data and catch poor performance organically. This is compounded by a shrinking pool of highly sophisticated IT talent. This has forced many IT teams into a reactive mode in which they are forced to wait for problems to occur before they try to deal with the issue as best they can. Unfortunately, this approach results in repeated impacts on the users, decreasing the positive business outcomes that digital acceleration tries to achieve.

AI for network operations systems leverages AI with ML algorithms to monitor the network and assist IT in managing the network. With advanced trending and insights gained from processing large amounts of data, an AIOps engine can dramatically shorten the time it takes IT to root cause network issues, including noticing problematic issues and implementing corrective actions before they can impact the end-users.

To ensure optimal network performance, an AIOps system can offer:

- **Low overhead:** The amount of data passing through the network dedicated to AIOps must be minimized to ensure that network bandwidth is preserved for business functions.
- **Trending insights:** AIOps visualizes trends within the network, highlighting where things are deviating from expectations and the historical norm.
- **Assisted resolutions:** AIOps systems provide actionable information and automation to resolve issues in the network far more quickly than humans alone can.



Fortinet Secure Networking

Fortinet has an innovative approach to securing digital acceleration with the convergence of enterprise-class security and networking. This unique platform approach ensures secure access to critical applications and resources, whether users are on-premises or accessing resources remotely. Our secure networking approach, including our unique combination of purpose-built ASICs, a universal operating system (FortiOS), cloud-delivered security solutions, and integrated networking equipment, enables superior user experience combined with coordinated threat protection for every network edge.

With FortiOS at its core, Fortinet Secure Networking tackles one of the most persistent challenges facing today's IT teams: extending enterprise-grade security and granular access control throughout the network and at all levels, from campus to branch to remote workers. Fortinet's solution solves user experience, point networking and security technology, and implicit trust challenges that create obstacles for organizations undergoing digital acceleration.

[1] "Gartner Says 89% of Board Directors Say Digital is Embedded in All Business Growth Strategies," Gartner, October 19, 2023.

[2] "HTTPS encryption on the web," Google Transparency Report, accessed May 22, 2023.

[3] Scott Anderson, "Is Your Network Operations Center Outdated? Here's What You Need to Know," LinkedIn, March 28, 2023

[4] Rahul Awati, "What is a network operations center (NOC)?" TechTarget, accessed January 26, 2023.

FORTINET

January 4, 2024 12:35 PM

1934260-B-0-EN