FORTINET

Cyberthreats Racing Ahead of Your Defenses? Secure Networking Can Put a Stop to That

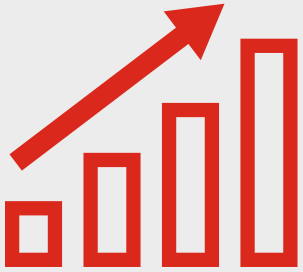
Table of Contents

Executive Overview

While digital acceleration delivers a number of benefits such as reduced costs, faster growth, and better user experience, it has also led to a rapid expansion of attack surfaces and the creation of 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 the addition of these new network edges is creating 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. Because most traditional network architectures were built using disparate and statically deployed point products that provide implicit access to all applications, the result has been disastrous. 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 application, 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 at scale. The key security, networking, and operations tools and integrations that are required to implement secure networking are covered in this ebook.

Key Components Required to Achieve Secure Digital Acceleration

A modern enterprise network needs solutions spanning three areas to achieve robust secure networking: powerful network operations center (NOC) solutions to centralize and unify management of the overall footprint, security solutions for edges and users, enhanced networking equipment.

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 interconnected, east-west traffic has increased, allowing a successful breach in one part of the network to spread to others quickly. 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) combine the ability to deploy critical next-generation firewall (NGFW) functions anywhere across your network—campus, data center, public clouds, private cloud, and Firewall-as-a-Service (FWaaS) and secure access service edge (SASE) environments—with centralized and unified management. This creates a single, integrated platform that can span, scale, and adapt 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

The attack surface is expanding due to the exponential growth of edges in modern enterprise architectures. Because this presents a threat to digital acceleration, automated threat protection is needed to keep operations running smoothly. Next-generation firewalls need threat intelligence that leverages artificial intelligence (AI) and machine learning (ML) to act as a force multiplier to speed threat prevention, detection, and response for known, zero-day, and unknown attacks.

Furthermore, with almost all internet traffic now encrypted, malicious actors can find their way in or out of a network by hiding in encryption. Organizations can no longer turn off secure sockets layer (SSL) inspection to avoid performance degradation. A solution is required that is powerful enough to provide full high-fidelity visibility into all secured paths, detect threats with SSL/Transport Layer Security (TLS 1.3) decryption, and provide automated threat protection. These solutions must be flexible for deployment at any enterprise edge for an HMF architecture: distributed branch, campus, data center, and cloud.

In addition to proven security controls, a modern NGFW should include:

- Unified management: On-premises and cloud-delivered protection deployed within the same framework of an HMF architecture
- Dynamic segmentation: The ability to dynamically build frameworks that isolate business-critical applications and users
- Embedded access control: Dynamic access control that continuously verifies users and devices
- Microsegmentation: Security inspection and protection through granular control over applications and workloads

Cloud-delivered secure access service edge

Cloud-delivered secure access service edge enables remote users to seamlessly access private applications in a data center or multi-cloud environment. It allows organizations to continue to leverage existing investments to secure a hybrid workforce and avoid adding point products. This helps remote users achieve a robust web security posture. Secure access service edge supports flexible deployment options from agent-based to agentless, enabling consistent web security across the network, endpoints, and cloud. A SASE solution should also provide simple onboarding with automatic proxy setup and certificate management while offering granular logging and events. This enables efficient troubleshooting and operations.

Encrypted traffic has hit 95%.[2]

Key SASE capabilities should include:

- Secure internet access: Securely connect all remote users and devices, including headless Internet-of-Things (IoT) devices without the need to install agents. This enables comprehensive web security for real-time protection against previously unknown threats.
- Detection and protection of sensitive data: Avoid shadow IT and data exfiltration with inline cloud access security broker (CASB) for comprehensive coverage. Detect, monitor, and control unsanctioned and sanctioned applications.
- Zero-trust posture check everywhere: Natively integrate zero-trust network access (ZTNA) to shift from implicit trust to per-application explicit access based on identity and context with continuous validation. This enables effective control of who and what is on the network and the control of off-network devices.

Networking Innovations

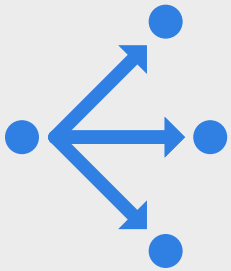
Software-defined WAN

Digital acceleration, work-from-anywhere (WFA), and sophisticated cyberattacks are driving changes in the traditional router-centric, hub-and-spoke, and heavily multiprotocol label switching (MPLS) WAN architecture. The results of these reactive changes are 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 access proxy in one solution to protect the entire digital attack surface.
- 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 (VM), simplifying management, reducing the footprint, and enabling cloud on-ramp orchestration.



“...enterprises have realized that having SD-WAN is more important than ever due to increasingly distributed and complex network infrastructure and the new normal of having to support hybrid or remote work; SD-WAN provides the centralized management, security, and performance required for today’s work-from-anywhere, cloud-first business environment.”[3]

LTE/5G wireless WAN

As enterprises adopt cloud technologies and move away from MPLS networks, challenges arise. 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 should provide users:

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

LAN edge 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, in many cases our means to secure them have not kept up. This leaves the network a prime target for unauthorized entry.

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 both security and networking reduces the risk profile of the network.
- 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 pattern sand 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 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 needs to enable 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 network aspects: Unifies and automates network and security policies across the network on a single pane of glass.
- Automates data exchanges: Supports automatic information transfers between the security operations center (SOC) and existing enterprise applications and services.
- Enables an automation-driven NOC: Simplifies day-0 operations and optimizes day-1 and day-2 troubleshooting with advanced technologies such as AI for network operations (AIOps) for IT operations.
- Streamlines operations: Simplifies the operational workflow across the HMF environment.

“From a security perspective, the NOC functions as the first line of defense that enables the organization to monitor network security and recognize and address any attacks or disruptions to the network.”[4]

Digital experience monitoring

Cloud migration, Software-as-a-Service (SaaS), and remote workers keep the business agile, and employees are distributed, but still digitally connected. Organizations no longer own the infrastructure that their traffic transverses, but they are still responsible for the end-to-end user experience. Digital experience monitoring (DEM) supports modern demands for NOC teams to shift their focus from traditional performance monitoring to accelerating the delivery of application availability from internal and external networks. Moving siloed performance-monitoring tools to a comprehensive DEM platform enables end-to-end visibility into the overall user experience no matter where the user resides or where the application is hosted.

A DEM solution lets organizations:

- Monitor at the edge: DEM enables end-to-end visibility by monitoring the edges to improve employee productivity.
- Get employee-to-application visibility of business-critical applications: DEM empowers NOC teams to ensure employees' digital experience is productive in driving the business.
- Meet and exceed SLAs: A DEM can continuously test users with an application experience across the globe to not only meet but exceed SLAs while improving customer satisfaction ratings.

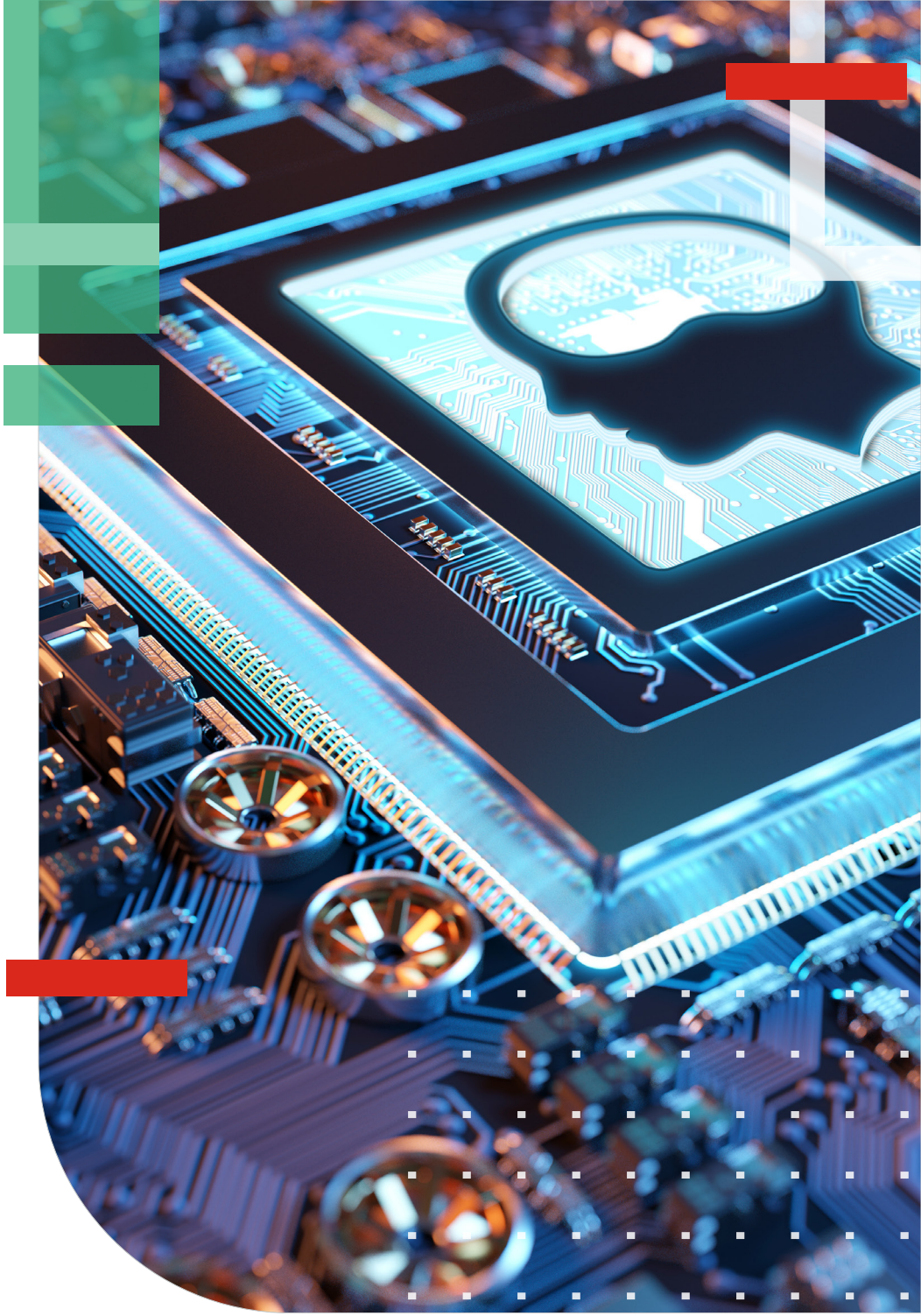
Artificial intelligence network operations

As the modern network gets more complicated, the ability for IT staff to manually sort through network data and catch poor performance organically has diminished. This has forced many IT teams into a reactive mode in which they wait for trouble tickets to be filed and then try to deal with the issue as best they can. Unfortunately, this approach results in repeated impact to the users, which works against everything that digital acceleration is trying to achieve.

Artificial intelligence 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 amount of time it takes IT to root cause network issues, including noticing problematic issues and implementing corrective actions before it can impact the end-users.

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

- Low overhead: The amount of data passing through the network for AIOps must be minimized to ensure that network bandwidth is preserved for business functions.
- Trending insights: AIOps should visualize the trends within the network, highlighting where things are not going as expected.
- Assisted resolutions: AIOps systems should provide actionable information on how to resolve issues in the network far more quickly than a human can.



Fortinet Secure Networking

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

Fortinet Secure Networking resolves one of the most enduring 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] Sarah Lispet, "Wondering how to take your SD-WAN to the next level? From security to automation, here are the top SD-WAN trends for 2022," Megaport, February 9, 2022.

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

FORTINET

www.fortinet.com

June 13, 2023 10:59 AM

1934260-A-0-EN