Cyberthreats Racing Ahead of Your Defenses? Security-Driven Networking Can Put a Stop to That
# Table of Contents

- Executive Summary ........................................... 3
- Introduction .................................................. 5
- Security-Driven Networking and the Validation of Zero Trust Edge Strategy .......................... 6
- Key Components Required to Achieve Secure Digital Acceleration ........................................ 8
  - Security for Edges and Users ......................... 8
  - Networking Innovations That Drive Digital Acceleration ................................................. 12
  - Simplified NOC Operations for Digital Acceleration ......................................................... 19
- Conclusion: Fortinet’s Unique Approach ............... 22
Executive Summary

Enterprises of all shapes and sizes were deep into the process called digital transformation before the COVID-19 virus hit the world. Digital transformation is “a catchall term for describing the implementation of new technologies, talent, and processes to improve business operations.”¹ Now, on the other side of the pandemic, most organizations are accelerating their digital business initiatives² to meet the demands of the hybrid, work-from-anywhere (WFA) workforce. This new approach is called digital acceleration.

The challenge from digital acceleration is that the addition of new network edges is creating new vulnerabilities, which are outpacing an IT security team’s ability to protect them from cyberthreats. Fortunately, there is a powerful strategy—security-driven networking—that can help fortify organizations so they can be safe and successful in their digital acceleration efforts.
“69% of boards of directors accelerated their digital business initiatives following COVID-19 disruption.”³
Introduction

Today’s hybrid, WFA workforce requires access to distributed applications deployed in data centers, multi-cloud environments, and SaaS locations. At the same time, these employees are bouncing between on-premises locations, interconnected branch offices, home offices, and temporary spots during travel—yet they still need and expect consistent, seamless user experiences. This shift to distributed applications and a WFA workforce means an expanding attack surface that exposes the business to new threats.

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.

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 effective security-driven networking with Zero Trust Edge Strategy will be covered in this eBook.
Security-Driven Networking and the Validation of Zero Trust Edge Strategy

It’s 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, and video streams. Furthermore, when the cybersecurity solutions aren’t integrated and cannot work together to protect against any of the discovered threats, things can get extremely unpleasant for the hybrid workforce.

To solve these issues, security and networking are converging in an approach called security-driven networking. This convergence must be consistently available across all edges to enable better user experience and application control.
We Must Verify Every Attempt

Another necessity that should be part of every security-driven network is a Zero Trust Edge Strategy. A zero-trust access strategy is based on the idea that nothing—no user, no device, no system, no network, no service—operating outside or inside the security perimeter is trusted. Instead, we must verify anything and everything attempting to access the network.

No longer is it acceptable to verify a user or device just once at the perimeter. Now, there is continuous and more dynamic verification of each user, device, application, and transaction. Zero Trust Edge is a strategy that organizations can holistically deploy across edges, users, and applications using consistent convergence of networking and security technologies.
Key Components Required to Achieve Secure Digital Acceleration

Security for Edges and Users

Consistent and coordinated AI/ML-powered protection across all network edges using NGFW

The attack surface is expanding due to the exponential growth of edges in hybrid IT architectures. This is not only a threat to digital acceleration, but automated protection from threats is also needed to keep operations running smoothly. Next-generation firewalls (NGFWs) 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.

In addition, 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 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 decryption including TLS 1.3, and provide automated threat protection. These solutions must be flexible for deployment at any enterprise edge: distributed branch, campus, data center, and cloud.
Encrypted traffic has hit 95%.
Network segmentation for isolation of east-west traffic

For years, network security leaders have responded to cyberattacks by building strong perimeter defenses externally to prevent attacks and segmenting their networks internally for operational controls. But once the perimeter is compromised, the hackers can freely roam around and create havoc by stealing data or shutting down business until a ransom is paid off.

Here’s what is needed:

- On-premises security is needed to protect east-west traffic.
- Because cloud-only-delivered firewall solutions are not enough, consistent convergence of on-premises and cloud-delivered NGFW is key to providing the highest level of protection.
- Organizations need to build dynamic segmentation frameworks that isolate business-critical applications and users.
- Dynamic access control should continuously verify users and devices.
- Applications that are grouped and interconnected with each other following a defense-in-depth strategy that only allows east-west and north-south communication through security inspection and protection through micro-segmentation.
Secure remote users using cloud-delivered SASE

Cloud-delivered secure access service edge (SASE) should provide FWaaS, in-line cloud access security broker (CASB), web filtering, DNS security, antivirus, anti-malware, anti-botnet, SSL inspection, and data loss prevention (DLP) to enable secure remote access. This allows a defense-in-depth strategy with multiple layers of defense, providing full-spectrum protection against known and zero-day threats at scale. This helps remote users achieve a robust web security posture. It supports flexible deployment options from agent-based to agentless, enabling consistent web security across the network, endpoints, and cloud. It also provides simple onboarding with automatic proxy setup and certificate management while offering granular logging and events for efficient troubleshooting and operations.

Key capabilities should include:

- **Secure internet access.** Securely connect all remote users and devices, including headless Internet-of-Things (IoT) devices without the need for installing 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 in-line CASB for comprehensive coverage. Detect, monitor, and control unsanctioned and sanctioned applications.

- **Zero-trust posture check everywhere.** Natively integrated zero-trust network access (ZTNA) lets organizations 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 or even control of off-network devices.
Networking Innovations That Drive Digital Acceleration

**SD-WAN**

Digital acceleration, WFA, and sophisticated cyberattacks are driving changes in the traditional router-centric, hub-and-spoke, and heavily MPLS WAN architecture that creates poor user experience, ineffective security, and complex operations.

A software-defined wide-area networking (SD-WAN) solution must have built-in NGFW security to be efficient and effective. It should also include advanced routing and ZTNA access proxy functions. This all needs to converge into one solution for simplified management. The solution needs to be powerful enough to run all security controls and SD-WAN functions while meeting expected performance.
The core benefits of SD-WAN, NGFW, and advanced routing are the ability to:

- **Deliver superior quality of user experience** at any scale by selecting the most optimum path for key business applications
- **Accelerate network and security convergence**, and simplify WAN architecture
- **Achieve operational efficiencies** through automation, deep analytics, and self-healing, and orchestrate consistent network and security policies
- **Provide better ROI** by migrating from a traditional router-based model to an advanced SD-WAN-based architecture.

The right SD-WAN solution will be able to:

- **Optimize hybrid workforce experience**. Enhance the WFA experience and security posture with consistent security policies and explicit access per application across all edges.
- **Enhance 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.
- **Converge 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.
“By year-end 2023, 60% of enterprises will have implemented SD-WAN, up from less than 20% in 2019, to increase network agility and enhance support for cloud applications.”

---

5
LTE/5G wireless WAN
As enterprises adopt cloud technologies and move away from MPLS networks in their continuing quest for digital acceleration, 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/fiber lines are limited in scope, 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 as network edges multiply.

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 are equipped with the latest LTE/5G technology to transform your branch connectivity no matter its proximity to cable/DSL/fiber.

They also should include dual SIM and dual modem options to provide fast cellular failover and high availability. Out-of-band management ensures business continuity for optimal ROI.
A secure cellular gateway can be used in the following ways:

- **LTE/5G as primary branch WAN link.** This enables reliable direct internet access at branch locations without access to cable/DSL/fiber. It’s ideal for schools, hospitals, or retail shops, industrial locations, and eventually mobile fleets and outdoor environments.

- **LTE/5G failover.** Enhanced broadband reliability can be provided where uptime is critical. Locations range from high-volume retail stores to industrial and utility sites, to hospitals and schools, and entertainment venues.

- **Secure LTE/5G local internet breakouts.** Security can be applied at branches opening to the internet.

**LAN edge solution (secure switches and access points)**

The wired and wireless local-area network (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.

A modern LAN edge solution should converge security with switches and access points (APs) to ensure a secure, seamless user experience. Combining an NGFW with Wi-Fi and Ethernet products lowers network complexity and improves security. A LAN solution must be able to identify what is connected to the network to implement zero-trust access.
A security-driven networking LAN edge solution should deliver:

- **Unified management.** The wired and wireless access layer, along with security controls, should be managed with one interface.

- **Complete scalability.** Stackable 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.

- **Zero-touch provisioning.** Automatic provisioning of equipment with auto discovery, 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 determine their level of privilege or network access.

“By 2024, 80% of enterprises will need to transform their networks and processes to deliver more personalized and interactive online rich media experiences that meet and satisfy customer expectations.”

---

6
Simplified NOC Operations for Digital Acceleration

Automation and centralized management
Manual operations inhibit efficient operational efficiency. They are not only error-prone and slow, but also result in breaches, which defeats the purpose of building a trusted network. Zero-trust edge architecture needs visibility into all locations, users, devices, and applications. Without that visibility, organizations will not have insights or the ability to act on their operations.

A NOC management tool should enable organizations to minimize human errors, automate response to threats, and deliver zero-trust strategy with centralized management. DevSec automation and consistent security policies across hybrid and multi-cloud environments increase operational efficiency and protection.

Look for these abilities in a NOC management tool:

- **Centrally manages.** Controls network and security policies across the network on a single pane of glass.
- **Automates data exchanges.** Supports automatic information transfers between the SOC and existing enterprise applications and services.
- **Automation-driven NOC.** Simplify day-0 operations and optimize day-1 and day-2 troubleshooting with advanced technologies such as AIOps for IT operations.
- **Streamlines operations.** Simplifies the operational workflow across hybrid IT.
Digital experience monitoring (DEM)

Cloud migration, SaaS, and WFA keep the business agile, and employees are distributed, but still digitally connected. Organizations no longer own the infrastructure their traffic transverses, but they are still responsible for the end-to-end user experience. DEM supports modern demands for NetOps teams to shift their focus from traditional performance monitoring to accelerating the delivery of application availability from internal and external networks. Modernizing 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.** Digital transformation has modernized the corporate infrastructure with network and workload edges, while traditional performance monitoring has remained in the core data center. DEM enables end-to-end visibility by monitoring the edges to improve employee productivity.

- **Get employee-to-application visibility of business-critical applications.** Business-driven applications have moved to the cloud, and SaaS adoption is rising. Still, NetOps teams have no visibility into the employee experience. DEMs empower NetOps teams to ensure employees’ digital experience is productive in driving the business.

- **Meet and exceed SLAs.** Ensuring service-level agreements (SLAs) is critical to most businesses, but there are a lot of blind spots in ensuring the user experience. 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.
Fortinet’s Unique Approach

Fortinet has an innovative approach to securing digital acceleration by using Zero Trust Edge Strategy 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 security-driven networking approach—including our unique combination of exclusive purpose-built ASICs, cloud-delivered security solutions, and integrated networking capabilities—enables superior user experience combined with coordinated threat protection for every network edge.

Zero Trust Edge Strategy resolves one of the most enduring challenges facing today’s IT teams: extending enterprise-grade security and granular access control to remote workers. Fortinet's solution provides a unique approach to overcoming user experience, point networking/security technologies, and implicit trust challenges that create obstacles for organizations trying to tackle digital acceleration.


3 Ibid.

