3 Reasons the Campus Is the Heart of Enterprise Security

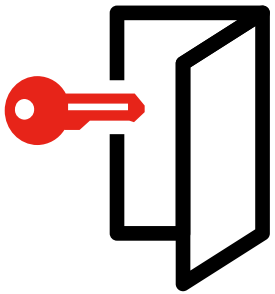
Table of Contents

Executive Summary: Organizations Need a Network Firewall Designed for the Modern Campus

Even as digital acceleration continues to transform businesses, the campus remains the heart of the network. Today, the campus network needs to do much more than simply interconnect the buildings located in the same geographical location. It also needs access to the internet, dispersed data centers, and applications deployed in both the data center and multiple clouds. And it needs to interconnect an increasingly hybrid workforce that needs to collaborate from both within and outside the campus local-area network (LAN).

With the proliferation of both end-user and Internet-of-Things (IoT) devices and the growing adoption of work-from-anywhere (WFA) strategies, the potential attack surface of today's campus continues to increase. Traditional security systems that protect a place in the network are no longer adequate. Today's security must adapt to highly scalable and increasingly hybrid campus environments. And data inspection and policy enforcement must follow users—and the applications they are using—whether they are on-premises, connecting from home, or accessing campus resources while traveling. This shift requires greater visibility and contextual awareness wherever the user goes throughout the campus network.

Rather than being deployed as a static solution at the campus perimeter, campus network security needs to meet users where they are and follow them wherever they go. It can only accomplish this by weaving security directly into the campus network. This deep integration between security and the distributed network ensures the required consistent, seamless, and adaptive experience today's WFA users require, enabling full mobility across the extended campus environment.



According to the Identity Theft Resource Center's 2021 Data Breach Report, the number of reported data breaches jumped 68% last year to 1,862—the highest total ever, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[1]

Reason 1: In the Campus, the User Is the Core of the Network

As the enterprise expands its edges to include campus deployments, the user in many ways becomes the core of the network, moving into, through, and across the campus while accessing applications and other resources. The resulting proliferation of devices, compounded by WFA work models, dramatically increases the attack surface as applications and services follow the user. Modern campus network security needs to meet users where they are and follow them as they perform their jobs. This shift from a static to an active security model requires greater visibility and contextual awareness to ensure consistent policy enforcement wherever the user goes throughout the campus network. The more you can see, the more you can protect. And traditionally isolated security solutions fragment visibility. Broad visibility and integrated solutions enable a consistent and robust security posture throughout the network. Achieving this, however, requires converging networking and security into a single platform to enable proactive protection throughout your network.

Reason 2: The Modern Campus Requires High-performance, Converged Security

As corporate and educational campuses expand to cover multiple buildings, deploying campus security using a network firewall—also known as a next-generation firewall (NGFW)—is increasingly prevalent. Internal network firewalls enable campus locations on the same network to be connected and protected while providing secure access to the internet, remote workers, cloud-based resources, dispersed data centers, and the wide-area network (WAN).

However, rather than providing point security at a fixed perimeter location, successful NGFW deployments must meet users where they are. Integration between systems, including the network, enables them to provide greater visibility and consolidate essential services, such as inspecting encrypted traffic (including TLS 1.3) at line rates while delivering advanced web, video, and Domain Name System (DNS) security.

The perimeter-only protection provided by most traditional firewalls does not address many of the new risks that today's dynamic campus environments encounter. The ability to provide secure segmentation to prevent the lateral spread of internal threats is equally important, as is advanced content security (including intrusion prevention system [IPS] and anti-malware), the ability to ensure trusted access to applications, and centralized risk management. An effective NGFW solution should also support the convergence of security with the network to help unleash the power of LTE/5G to secure critical Industry 4.0 use cases (e.g., virtual reality, robotics, controls, digital twins, etc.). And it should be enhanced with artificial intelligence (AI) and machine learning (ML) to rapidly detect and respond to threats. In addition, it should be enhanced with custom security processors (SPUs)—similar to graphics processors that enable streaming video—to prevent performance degradation while running multiple concurrent services.

Reason 3: Campus Digital Acceleration Enables Automation

Delivering consistent and automated security policy across an expanded network ecosystem is essential to building a strong and scalable security posture. When creating a comprehensive security framework able to adapt to and protect all campus edges, network and security leaders must ensure they simplify operations rather than increase their complexity. The manual operations required to manage and maintain a growing number of isolated security solutions inevitably result in user fatigue errors. They also increase the likelihood of breaches resulting from the inability of operators to hand correlate data fast enough to detect an attack and launch a coordinated response.

NGFWs must also support the implementation of zero-trust network access (ZTNA). Today's businesses run on applications. Allowing users to securely access applications and resources from anywhere, at any time, requires continuous authentication while maintaining effective compliance and security controls. A campus-based NGFW should include a simple and integrated dashboard that enables the coordinated delivery of critical ZTNA mechanisms, such as application controls and identity management.

Speed-to-response is another essential element of any network firewall, enabling the disruption of any attack before it can achieve its malicious goals. Automation working across a truly integrated cybersecurity mesh architecture reduces the time to detect and protect networks from attacks while simplifying device onboarding for large-scale deployments.

And a single-pane-of-glass management approach enables automation and orchestration across the cybersecurity mesh architecture—including support for ecosystem partners—to simplify enterprisewide workflows. An open API approach and cross-environment connectors help simplify and ensure consistent security posture and enforcement, even across multi-cloud environments. However, achieving true operational agility requires that it also learn about and share the ever-changing state of cloud resources.

The hybrid workforce has made the campus increasingly vulnerable, with phishing and ransomware topping the charts. According to the 2021 Verizon Data Breach Investigations Report, 70% of threat actors are financially motivated (ransomware) and 85% of data breaches involve a human counterpart (phishing).[2]

Conclusion: Designing Adaptive Campus Security Requires a New Approach

The campus is the heart of today's enterprise security architecture. In addition to the importance of the people on-site and their high bandwidth and convergence needs, complexities arising from digital acceleration, the proliferation of devices, and an increased reliance on distributed applications require increased automation. Traditional point security solutions that operate in isolation—from each other and the underlying network—cannot address the security requirements of today's campus environments. Today's NGFWs must support the three critical needs of today's campus: the highly mobile WFA user, the need for converged security that can operate at network speeds, and the ability to support automation to quickly detect and respond to threats and adapt to digital acceleration demands.

Most legacy NGFW solutions are no longer able to meet these demands. Organizations need to consider an integrated NGFW platform designed for the way organizations and users do business. They must ensure broad visibility across the campus with secure access to the cloud and remote workforce, complete integration between all security elements and the network, and advanced automation, enhanced with AI and ML, to quickly detect and respond to today's increasingly sophisticated threats.

[1] 2021 Annual Data Breach Report, Identity Theft Resource Center, January 24, 2022.

[2] 2021 Data Breach Investigations Report (DBIR), Verizon, January 18, 2022.

www.fortinet.com

March 29, 2023 6:09 PM

1429374-0-0-EN