POINT OF VIEW

Protecting Your Hybrid and Hyperscale Data Centers

Executive Summary

Today's data centers face two distinct challenges when securing critical applications and resources. The first is protecting distributed data centers that leverage a hybrid design of composable and scalable architectures. Hybrid architectures allow distributed branches, campus, and on-premises data centers to seamlessly interconnect with cloud-based data centers that host a variety of essential services. This approach increases operational agility by allowing business-critical applications to be deployed in the cloud while maintaining other applications and data in on-premises data centers to ensure compliance and control. It also better supports your shifting workforce demands, enabling you to provide better access to all applications anytime, anywhere, from any location.

The challenge is ensuring consistent security, visibility, and control when those applications are deployed across different environments. It is especially critical to remember that the on-premises data center must protect those essential applications, data, and workloads that can't be moved to the cloud because of policy or regulatory requirements—but still need to be consumed by employees, customers, and partners from a variety of locations.

And second, a growing number of enterprises are also embracing hyperscale architectures to satisfy growing business demands and the need to optimize user experience through performance, scale, and capacity. But adopting a hyperscale and hyperperformance strategy, especially across a hybrid data center, introduces unique security-related challenges. Legacy security tools that cannot deliver essential services at line rates, such as inspecting encrypted or streaming traffic or elephant flows, can negatively—even severely—affect performance, scale, and user experience, as well as reduce your organization's overall security.

Network security and network performance… can sometimes conflict with each other, as security measures may slow down or disrupt network traffic, and performance optimization may expose the network to vulnerabilities or attacks.[1]

Traditional security solutions struggle to meet today's hybrid data center performance and scale requirements. As a result, too many organizations are forced to choose between accelerating their data and applications and accepting the high costs of protecting such an environment using traditional security tools. In such environments, security can quickly become a bottleneck. And in many cases, maintaining your competitive edge means your need for performance wins out over security. But the resulting security lapses increase the likelihood that attacks like ransomware will result in business disruptions, financial losses, and long-term damage to brand and reputation.

Rethinking Your Data Center Security Strategy

As you revise and expand your data centers, you must ensure that your security solutions can support your new high-performance and highly flexible hybrid architecture. That starts with understanding the core challenges these new environments create and then evaluating providers to find a right-fit security approach designed for hybrid and hyperscale data centers. These issues include:

- **Application access control:** Your hybrid workforce needs to consume applications from any location—both on- and off-premises—and at any time. Once this strategy is implemented, two things become apparent. First, the remote access virtual private network (VPN) remote workers use to access local or cloud-based applications results in excessive trust, allowing criminals to compromise poorly secured home networks and then hijack encrypted tunnels to gain access to the network. That aging technology must be replaced with a zero-trust approach. And second, applications consumed from the cloud come with limited security. To address this issue, many IT teams hairpin traffic back through the on-premises data center for deeper scrutiny, resulting in unnecessary bandwidth use and impacts on performance.

- **Limited visibility:** Hybrid data centers increase operational agility, helping to support new business paradigms, including the shift to work from anywhere. They do this by deploying some resources across multiple clouds while keeping other business-critical applications and data in on-premises data centers for compliance and control. However, your attack surface expands as your data center infrastructure becomes more distributed. And because few legacy security solutions can be deployed everywhere or even work together in those places where they can, blind spots emerge that reduce visibility and increase the potential for breaches and attacks. One critical blind spot results from the inability to inspect encrypted applications and other transactions. Organizations must inspect encrypted flows to detect attacks, especially malware designed to hide in secure channels. This inspection helps prevent ransomware and disrupts command-and-control sessions established through Hypertext Transfer Protocol Secure (HTTPS) Beacons from stealing customer and corporate data. But inspecting encrypted data is the Achilles heel of nearly every legacy next-generation firewall (NGFW), resulting in the significant degradation of application performance and user experience.

- **Shielding vulnerable applications:** Similar to the challenges around inspecting encrypted traffic, consolidating intrusion prevention system (IPS) capabilities into most NGFW solutions creates performance degradation and patch management challenges. However, a standalone IPS's operational and ownership costs are prohibitive for many organizations. This should not be an either-or choice. Your firewall solution should be able to perform such security functions without impacting performance.

- **Hyperscale performance:** New, high-performance innovations—such as elephant flows, edge computing, protection of high-definition television (HDTV) and other rich media traffic, 5G networks, and dynamic core segmentation—require unprecedented performance levels from your NGFW. But most NGFWs use off-the-shelf processors that were simply not designed to provide this level of performance. As a result, most legacy solutions cannot meet today's performance demands, let alone those of tomorrow, without an enormous price tag. And in many cases, not even then.

- **Overall management complexity:** Automation and orchestration at scale across diverse, hybrid IT environments are impossible without simple, centralized management. In addition, configurations can fall out of sync, policies are inconsistently enforced, visibility and control are fractured, and exploitable security gaps invariably begin to be introduced.

Solving the Right Problems

Networking and security leaders have a lot on their plates. Data center evolution, let alone the challenges of securing a hybrid data center environment, can be unwieldy, with issues arising from all sides. But security for hybrid and hyperscale data centers is well within reach. But to achieve this, you should assess these priority considerations when your solution research begins:

- **Take control for a seamless user experience:** Determine who can access which applications and resources—and why. Zero-trust network access (ZTNA) can then convert that assessment into policy, constantly authenticating the user, location, and device and only granting access to specific resources based on policy. This approach removes the excessive level of implicit trust, the weakest element of traditional VPN technology. By creating user-to-application maps that can be consumed and enforced by security tools like NGFW, you can deliver consistent end-to-end security with full compliance controls.
- **Leverage comprehensive visibility to achieve better control:** Most traditional security deployments are riddled with blind spots, often because they operate in silos or have limited capabilities. But they don't need to stay that way. Complete visibility into encrypted flows, such as HTTPS, allows organizations to quickly identify and stop hidden threats. Advanced tools can then actively prevent a wide variety of network, application, and file-based attacks, including ransomware, the theft or corruption of sensitive data, and other sophisticated threats. Consistent security delivered end to end, following applications and workflows across your distributed environment, protects the overall network infrastructure, and ensures that network and business operations remain up and running. Additional tools, such as network segmentation, can further reduce the attack surface, preventing the lateral spread of threats and improving application and transactional compliance (data governance).

"Misconfiguration remains the biggest cloud security risk, according to 59% of cybersecurity professionals. This is closely followed by exfiltration of sensitive data and insecure interfaces/APIs (tied at 51%), and unauthorized access (49%).[2]

- **Keep critical, hard-to-patch legacy systems up to date—virtually:** The potential for vulnerability exploitation or other patch-related issues only increases in large enterprises with legacy systems and aging infrastructure. Intrusion prevention technology can play a crucial role in patch management through "hot patching," where an IPS is positioned to protect vulnerable, hard-to-patch legacy applications. And when IPS is consolidated into a network firewall—built with enough performance power to run both systems instead of as a standalone solution—IT teams can reduce cost and complexity while preserving control across different network and security operations groups. (In fact, prudent consolidation can also reduce the total cost of ownership, including less rack space and lower data center power and cooling costs.)
- **Implement automation:** Networking and security leaders still over-rely on manual operations and an overabundance of tools, often without enough security-skilled staff to manage them. It's a classic problem for network operations center (NOC) and security operations center (SOC) teams. Effectively managing a hybrid data center environment requires reducing the complexity of operations by consolidating the number of point products in place and leveraging automation to improve efficiency. Automation, especially when enhanced with machine learning (ML) and artificial intelligence (AI), can bridge your overall cyber skills gap and ease the burden of your overextended teams. In many cases, an effective AI-based solution can do the work of a dozen or more security analysts—without human error and in a fraction of the time.
- **Deploy a hybrid mesh firewall:** Hybrid mesh firewalls (HMFs) are designed to support today's distributed and highly adaptive networks. They come in a variety of form factors, so they can be deployed natively in any environment. And once deployed, they operate as a unified security platform. Hybrid mesh firewalls unified management and analytics span your entire distributed network, resulting in complete visibility and protection against security threats, simplifying operations, ensuring compliance, enabling end-to-end automation, and reducing complexity to increase operational efficiency. An HFM strategy allows you to support your distributed workforce and compete in today's global marketplace without sacrificing the protections that a coordinated and automated security strategy provides.

Your Hyperscale Architecture Requires Hyperscale Security

You should never have to consider a trade-off between security and performance. But in many organizations, security has become a choke point for traffic entering and exiting most hyperscale data centers (north-south traffic) and traffic moving across and between data centers (east-west traffic). These bottlenecks can adversely affect user experience, slow overall productivity, and impact competitiveness and revenue. They also pressure network administrators to loosen security safeguards so things can speed up. But allowing traffic to flow freely into, out of, and across your network without adequate security dramatically increases the risk of attacks and outages.

What you need is hyperscale security designed to match your hyperscale architecture. That includes avoiding the questionable practice of "implementing" hyperscale security by chaining multiple NGFWs, which is cumbersome, difficult to manage, and needlessly expensive. Such strategies, often touted as an "advanced" clustering feature, are actually the result of vendors that have failed to develop tools designed for today's hyperperformance requirements.

Nearly every other industry today has developed purpose-built, application-specific integrated circuits (ASICs) to optimize specialized processing. Televisions, computer graphics, smartphones, cloud platforms, data center servers and switches, and even smart cars rely on custom, purpose-built processor technology to deliver specialized functions. Security should be no different. But nearly every security vendor continues to rely on off-the-shelf processors to deliver specialized work, which is why they collapse under the strain of encrypted traffic or processor-intensive inspection and analysis.

The Opportunity

The era of hyperscale has arrived—from supporting hybrid data center environments to providing e-commerce application access to enabling organizations to rapidly share large data files across distributed sites to building disaster recovery sites. It allows faster user access, empowers mobile network operators to move from 4G to 5G, and ensures the delivery of broadband internet on wireless devices. And that's just the start. Everything is getting bigger, faster, and more distributed at a breakneck pace.

As a result, everyone needs hyperscale security. Even enterprise organizations not yet tasked with addressing hyperscale productivity still need to implement security designed for a hybrid data center architecture to take advantage of the hybrid model's flexibility and performance benefits.

At the same time, advanced threats targeting the data center core and every network edge are unrelenting. Your security, network engineering, DevOps teams, and operations leaders need to step back from their isolated pieces of the network and look at the big picture to see what is at stake and how to address those challenges with a unified approach. And because the data center is still the heart of your organization, they need to start by addressing hybrid data center performance, bandwidth, and security demands.

This requires the proper consideration of security solutions designed to meet the needs of modern architectures to ensure consistent end-to-end security and an optimal user experience. And that starts with selecting network firewalls designed to work together as a unified system that can be deployed anywhere, scale endlessly, interoperate seamlessly, and perform at the speed of your digital business.

[1] "How do you balance network security and network performance?" Linksys, June 3, 2023.

[2] "2023 Cloud Security Report," Cybersecurity Insiders, 2023.

FORTINET

www.fortinet.com

June 27, 2023 3:58 PM

2240454-0-0-EN