POINT OF VIEW

Protecting Your Hybrid and Hyperscale Data Centers

Organizations are building hybrid data centers that consist of composable and scalable architectures. Their hybrid design enables distributed branches, campuses, and on-premises data centers to interconnect with data centers hosting a variety of essential services deployed across multiple clouds. This hybrid approach increases operational agility by deploying business-critical applications in the cloud while maintaining other applications and data in on-premises data centers to ensure compliance and control. This distributed model also better supports shifting workforce demands, enabling organizations to provide better access to all applications anytime, anywhere, from any location. But within that cloud model, it is critical to remember that the enterprise on-premises data center[1] remains essential for protecting those applications, data, and workloads that can't be moved to the cloud but still need to be consumed by employees, customers, and partners.

As data center infrastructure evolves, a growing number of enterprises are embracing hyperscale architectures to satisfy demands for optimal user experience while delivering unparalleled performance, scale, and capacity.

But the adoption of hyperscale and hyperperformance across a hybrid data center model can also create security-related challenges that can negatively, even severely, affect user experience, performance, and scale. Traditional security solutions struggle to keep up with hybrid data center performance and scale requirements. Increasingly, organizations are forced to choose between accelerating data and application performance and the high costs of protecting such an environment using traditional security tools. Security can quickly become a bottleneck, and in many cases, maintaining a competitive edge means that the need for high performance wins. But the resulting security lapses can play a critical role in enabling attacks like ransomware that can result in business disruptions, financial losses, and long-term damage to brand and reputation.

Organizations need to rethink their data center security strategy. That starts with understanding the core challenges hybrid and hyperscale trends create for teams and then evaluating providers that can offer right-fit security designed for hybrid and hyperscale data centers. These include:

- **Application access control:** As organizations adopt a full-time hybrid workforce that consumes applications from anywhere and anytime, two things become apparent. First, the remote access virtual private network (VPN) used to access local or cloud-based applications results in excessive trust. And second, applications consumed from the cloud come with limited security unless traffic is hairpinned back to the on-premises data center for deeper scrutiny.

- **Limited visibility:** With the shift to work from anywhere, organizations adopt hybrid data centers to increase operational agility. They do this by deploying resources across multiple clouds while keeping other business-critical applications and data in on-premises data centers for compliance and control. However, as the data center infrastructure becomes more distributed, the attack surface expands. As a result, more blind spots emerge, reducing visibility and increasing the potential for breaches and attacks. One critical blind spot is the result of encrypting applications and other transactions. Organizations need to inspect encrypted flows to detect all types of attacks, especially malware that hides in secure channels. This helps prevent ransomware and to disrupt 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 most traditional firewalls, resulting in the significant degradation of application performance and user experience.
- **Shielding vulnerable applications:** The consolidation of intrusion prevention system (IPS) capabilities into a next-generation firewall (NGFW) solution, rather than using standalone IPS devices, can create performance degradation and patch management challenges. However, the operational and ownership costs of a standalone IPS are prohibitive for many organizations. This should not be an either-or choice.
- **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—will require unprecedented performance levels from solutions such as NGFWs. But because most NGFWs were not designed with this level of performance in mind, some solutions will simply be unable to meet today's 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 are especially difficult in diverse, hybrid IT environments without simple, centralized management. But without it, 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 feel like an unwieldy discussion, with challenges coming from all sides.

But security for hybrid and hyperscale data centers is well within reach. Leaders should evaluate these priority considerations when solution research begins:

Take Control for a Seamless User Experience

Start with determining who can access which applications and resources—and why. Zero-trust network access (ZTNA) can then convert that into practice by constantly authenticating the user, place, and device and only granting access to resources based on policy. This approach removes the excessive level of implicit trust results that is 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 in place.

Leverage Comprehensive Visibility To Achieve Better Control

Most traditional security deployments are riddled with blind spots. 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 protects the overall network infrastructure, ensuring that the network and business operations remain up and running. Additional tools, such as network segmentation, can further reduce the attack surface, prevent the lateral spread of threats, and improve application and transactional compliance (data governance).

Virtually Keep Critical, Hard-to-Patch Legacy Systems Up to Date

60% of successful security breaches can be traced in some way to poor patch management.[2] And the potential for vulnerability exploitation or other patch-related issues only increases in large enterprises with many legacy systems and an aging infrastructure. IPS technology can play a crucial role in patch management, such as with "hot patching," where an IPS is used to protect vulnerable, hard-to-patch legacy applications. And when consolidated into a network firewall designed with enough performance power to run both systems instead of as a standalone solution. IT teams can reduce cost and complexity while preserving control among different network and security operations groups. (In fact, prudent consolidation can reduce the total cost of ownership [TCO], including less rack space and lower data center power and cooling costs.)

Encourage Automation

Networking and security leaders still over-rely on manual operations and on an overabundance of tools without enough security-skilled staff to manage them. It's a classic problem for both the network operations center (NOC) and security operations center (SOC). Effectively managing a hybrid data center environment requires reducing the complexity of operations—not only by consolidating the number of point products in place but by leveraging automation to enable improved efficiency. Automation, especially machine learning (ML) and artificial intelligence (AI), helps bridge the overall cyber skills gap and eases the burden of overextended human 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.

Deliver Not Only Hyperscale Architecture but Also Hyperscale Security

An organization 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). This can adversely affect user experience, slow down overall productivity, and impact competitiveness and revenue. It also puts pressure on network administrators to loosen security safeguards so things can speed up. But allowing all traffic to flow freely into and out of an organization's network without adequate security dramatically increases the risk of attacks and outages.

Organizations need hyperscale security to match their hyperscale architecture. That includes avoiding the questionable practice of "implementing" hyperscale security by chaining multiple NGFWs together, which is cumbersome, difficult to manage, and needlessly expensive. Such strategies result from manufacturers that have failed to develop tools designed for today's hyperperformance requirements. Instead, they still 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. Every other industry has developed purpose-built application-specific integrated circuits (ASICs) designed to optimize specialized processing—televisions and computer graphics, smartphones, cloud platforms, data center servers and switches, and even smart cars all rely on custom, purpose-built processor technology to deliver specialized functions. Security should be no different.

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 that aren't yet tasked with addressing hyperscale productivity still need to implement security designed for a hybrid data center architecture so that they can 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. Security, network engineering, DevOps teams, and operations leaders need to step back from their pieces of the network and look at the big picture to see what is at stake. And because the data center is still the heart of the organization, they need to start by addressing hybrid data center performance, bandwidth, and security demands. If not, they will not be able to support a

distributed workforce and a global marketplace without sacrificing the protections that a coordinated and automated security strategy provides.

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

[1] "What is a Data Center?" Fortinet.

[2] John Emmitt, "Patch Management: Best Practices and Why It's Important," Security Boulevard, March 9, 2021.

July 27, 2021 3:52 AM
1181055-0-0-EN