Grow Business with Secure Hybrid and Hyperscale Data Centers

As data center infrastructure evolves, more enterprises, hyperscalers, and service providers are embracing hybrid and hyperscale architectures to satisfy unprecedented demands for user experience, while delivering unparalleled performance, scale, and capacity.

But this trend also creates security-related needs that can negatively, even severely, affect experience, performance, and scale if not properly addressed, and can lead to attacks, disruptions, and long-term damage to brand and reputation.

Organizations should evaluate providers that can offer right-fit security designed for hybrid and hyperscale data centers. That starts with understanding the core challenges hybrid and hyperscale trends create for teams.

- **Limited visibility:** As data center infrastructure becomes more distributed, the attack surface expands, and more blind spots emerge in overall visibility of the environment, the potential for breaches or other forms of disruption increases.
- **Shielding vulnerable applications:** The consolidation of intrusion prevention system (IPS) capabilities instead of standalone IPS devices creates challenges related to performance degradation and patch management, especially keeping up with patches in vulnerable, hard-to-patch legacy applications in multiple management domains.
- **Hyperscale performance:** New, high-performance innovations—such as elephant flows, edge computing, protection of HDTV and other rich media traffic, 5G networks, and dynamic core segmentation—will require unprecedented performance levels from solutions such as next-generation firewalls (NGFWs). But because most NGFWs were not designed with this performance in mind, some solutions will simply be unable to meet these demands of tomorrow without an enormous price tag—and in many cases, not even then.
- **Overall management complexity:** Automation and orchestration at scale is difficult in diverse, hybrid IT environments without simple, centralized management.

Solving the Right Problems

Networking and security leaders have a lot on their plates, and data center evolution can feel like an unwieldy discussion, especially with challenges from all sides.

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

Gain Comprehensive Visibility To Achieve Better Control

Blind spots don't need to stay that way. Through full visibility into unauthorized applications and hidden threats, leaders can protect the overall network infrastructure, keeping the network and business operations running. By including segmentation in the network, teams can also reduce the attack surface, prevent the lateral spread of threats, and consequently achieve better application and compliance (data governance) through defense-in-depth security.

Virtually Patch Critical Hard-to-Patch Legacy Systems

More than 50% of successful security breaches can be traced in some way to poor patch management.[1] And the potential for vulnerability exploitation or another patch-related issue only increases in large enterprises with many legacy systems and aging infrastructure. IPS technology can play a key role in patch management, especially when consolidated into a network firewall instead of as a standalone solution. With the right network firewalls, teams can reduce cost and complexity by running multiple security functions while preserving control among different network and security operations groups. (Prudent consolidation as a whole can reduce total cost of ownership [TCO], including with less rack space in use and by lowering data center power and cooling costs.)

Encourage Automation

It's a classic problem for both the NOC and SOC: Networking and security leaders still rely too much on manual operations, and on too many tools without enough security-skilled staff to manage them. Modernization requires reducing the complexity of operation, not only by consolidating the number of point products required in networks but also leveraging automation to enable improved efficiency. Automation bridges the overall cyber skills gap and eases the burden of overextended human teams like no other operational trend today.

Deliver Not Only Hyperscale Architecture But Also Hyperscale Security

Security and performance can't be a trade-off, but in many organizations, security has become a choke point for traffic entering and exiting most hyperscale data centers, adversely affecting user experience and slowing overall productivity. This in turn puts pressure on network administrators to loosen security safeguards to ensure things can speed up again. But allowing all traffic to flow freely into and out of an organization's network without adequate security greatly increases the risk of attacks and outages. Hyperscale security needs to match hyperscale architecture, and that includes avoiding the questionable practice of "implementing" hyperscale security through multiple NGFWs chained together, which is cumbersome, difficult to manage, and needlessly expensive.

The Opportunity

The era of hyperscale has arrived, from high-velocity e-retail, to the requirements of research organizations sharing large files among distributed sites rapidly, and for mobile network operators for the move from 4G to 5G networks and delivery of broadband internet on wireless devices—everyone needs hyperscale security. But even enterprise organizations that aren't yet tasked with addressing hyperscale productivity need to drive security for hybrid data center architecture so they take advantage of the hybrid model's flexibility and performance benefits.

At the same time, advanced threats at the data center core and at every network "edge" are unrelenting. Security and network engineering and operations leaders must address modern data center performance and bandwidth demands without sacrificing security. Doing so requires the right considerations and then the deliberate selection of security solutions that can meet the needs of a modern architecture.

[1] "Costs and Consequences of Gaps In Vulnerability Response," ServiceNow and Ponemon Institute, April 5, 2018.

FURTINET

www.fortinet.com