

POINT OF VIEW

Protecting Hybrid and Hyperscale Data Centers

Meeting Your Business Needs in a Distributed World



The Hybrid Data Center

Business is no longer confined to a single office; it's spread across clouds, data centers, and edges, demanding a flexible, high-performing, and secure infrastructure. You need to deliver seamless experiences to your employees, customers, and partners, no matter where they are located.

Hybrid data centers help get control over today's networks by blending composable and scalable architectures. They connect distributed branches, campuses, and on-premises data centers with cloud-based services, enhancing operational agility. By deploying business-critical applications in the cloud while retaining sensitive data and applications on-premises, organizations achieve flexibility and control. This distributed model supports a dynamic workforce, providing secure anytime, anywhere access. On-premises data centers remain crucial for safeguarding applications and data that cannot be migrated to the cloud, ensuring seamless access for employees, customers, and partners.

The rise of hyperscale architectures in modern data centers addresses the growing demand for exceptional user experience and unparalleled performance. However, integrating hyperscale and high-performance capabilities within a hybrid environment introduces significant security challenges. Traditional security solutions struggle to match the speed and scale of these architectures, forcing organizations to choose between performance and security. If security is prioritized, it often becomes a bottleneck. If speed is chosen, the organization is not protected, opening the door to potentially devastating cyberattacks.

Overcoming Today's Biggest Data Center Security Challenges

To deliver high-performance security that keeps up with the speed of business, organizations need a comprehensive data center security strategy. That starts with understanding the core challenges hybrid and hyperscale trends create and then evaluating providers that can offer right-fit security designed for hybrid and hyperscale data centers. Key challenges include:

- **Application access control:** As organizations adopt a full-time hybrid workforce that uses applications hosted anywhere, two things become apparent. First, the 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 backhauled to the on-premises data center for deeper scrutiny.

- **Limited visibility:** The need to support remote workers has driven organizations to embrace hybrid data centers, achieving operational agility by distributing resources across multiple clouds while maintaining critical applications and data on-premises for compliance and control. However, this distributed architecture significantly expands the attack surface, creating critical visibility gaps. A particularly concerning blind spot emerges from the widespread use of encryption. While essential for privacy, encryption conceals malicious activity within secure channels. Traditional firewalls struggle with encrypted traffic inspection, resulting in significant performance degradation and impact on user experience.
- **Shielding vulnerable applications:** Consolidating 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 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. Configurations can fall out of sync, policies are inconsistently enforced, visibility and control are fractured, and exploitable security gaps are introduced.

Solving the Right Problems

Networking and security leaders have a lot on their plates. Data center evolution and the difficulties of securing a hybrid data center environment can feel like an unwieldy discussion, with challenges coming from all sides. But, with the right solutions, effective and efficient security for hybrid and hyperscale data centers is well within reach.

The first steps include evaluating firewall offerings to ensure they are powerful enough to handle all security requirements without performance impact, including HTTP inspection, integrating a zero-trust approach, and delivering end-to-end visibility.



www.fortinet.com