FORTINET

CHECKLIST

Critical Considerations for Securing Hybrid and Hyperscale Data Centers

Modern hybrid and hyperscale data center architectures must include security that can keep pace. But in many of these data center environments today, traditional network security solutions—especially outmoded traditional firewalls—underperform and underserve, pushing IT teams into dangerous trade-offs between security and performance.

Following are six critical considerations for all enterprise IT teams as they design security for modern data center infrastructure.

☑ Visibility and control.

Managing security risks to high-performance networks means proactively reducing the attack surface. That includes complete visibility and control of the entire environment, the endpoints, network segments, the traffic that is flowing through those segments, applications, and the data that is being accessed. Any device connecting to a data center network is therefore a potential threat vector. But securing a modern data center goes well beyond a traditional on-premises data center. It also requires visibility of all deployed security elements across all the various environments (on-premises, colocations, clouds, etc.), as well as visibility of users, applications, and devices. It further includes intrusion prevention systems (IPS) that check for and help guard against advanced threats by monitoring the network in real time.

☑ Zero-trust principles.

Zero-trust principles are about privileged access and adaptive trust. As a model, zero trust treats every transaction, movement, or iteration of data as suspicious. When properly implemented, a zero-trust system tracks user and network behavior (users-users, user-machines, machine-machine) and data flows in real time and alerts teams or revokes access from accounts when an anomaly or an anomalous behavior is detected.

☑ Segmentation.

Segmenting network traffic implements control points, reduces the potential for attackers to move laterally, and exploit weaknesses in more places in the data center. This means classifying all traffic into different segments, especially at the application and port levels. Segmenting can also be done at the host level and at the network level as well. When successfully implemented, each segment is isolated from all others. Network segmentation helps simplify how organizations enforce security policy by following defense in depth.

☑ Time to service.

Many current data center solutions yield low performance and high latency, meaning organizations can't deliver services with the time, agility, and reliability the hyperscale era demands. Services need to be segmented and interoperate between a massive amount of physical and virtual assets. Modern data center firewalls must be able to offer hardware acceleration for Virtual Extensible LAN (VXLAN) termination and re-origination as well as provide dynamic support for Layer 4 or Layer 7 security. Even a tiny amount of downtime or miniscule service delivery challenge can cost companies millions in lost revenue, trust, and brand reputation.[1]

☑ Capacity.

Many security infrastructures struggle when immense datasets, also known as "elephant flows," are transferred over single connections. But elephant flows are a regular need in the hyperscale era, especially for organizations in industries such as pharmaceuticals, ecommerce, aeronautics, or financial brokerage that require securely encrypting and transferring large datasets using high-throughput flows across data centers or across data centers and multiple clouds. Network firewalls applied to hyperscale data centers must be able to perform at these levels, every day.

[1] Filip Truta, "Downtime Can Cost a Company up to $67 Million Over Two Years, Threatening Brand Reputation," Security Boulevard, February 21, 2019.