CHECKLIST

# 9 Critical Considerations for Securing Hybrid and Hyperscale Data Centers

**Today's hybrid and hyperscale data center architectures require security solutions designed to keep up with the pace of business. But too many data center environments still rely on outmoded traditional firewalls that underperform and underserve, pushing IT teams into dangerous trade-offs between security and performance. But because there is so much at stake—and so little guidance—choosing the right solutions can be daunting.**

**Here are nine critical considerations for IT teams to consider as they update the security of their modern data center infrastructure.**

## ☑ Cross-Platform Management and Analytics

Organizations increasingly rely on a mix of on-premises and cloud-based compute platforms. These hybrid architectures are forcing security professionals to view data center security as part of a broader security fabric, one that encompasses both on-premises and multiple cloud platforms. One way to achieve this is by implementing a hybrid mesh firewall (HMF) strategy that leverages unified management and analytics and a common framework to converge security for data center, campus, branch, and cloud platforms into a single, integrated system. This approach ensures that applications and data are protected with consistent security policies and managed by the same tools end to end.

## ☑ Visibility and Control

Managing security risks to high-performance networks means proactively reducing the attack surface. The goal is to ensure that the applications being used, traffic flowing between and through every network segment, and the data being accessed are thoroughly inspected and consistently protected. That requires selecting a solution able to consolidate resources while establishing complete visibility and control across the entire environment. And because every device connecting to a data center network is a potential threat vector, your solution must also support appropriate zero-trust strategies, such as zero-trust network access (ZTNA) and SD-WAN. Your security solution must also seamlessly extend beyond the traditional on-premises data center, providing unified visibility across all environments (on-premises, colocations, clouds, and any combination of those), including users, applications, and devices. And it must also include protections like 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 implementing privileged access and adaptive trust. A zero-trust model treats every transaction, movement, or iteration of data as suspicious. When properly implemented, a zero-trust architecture tracks user and network behavior (users to users, user to machines, machine to machine), and data flows in real-time and alerts teams or revokes access from accounts when anomalous behavior is detected. Security solutions for hybrid and hyperscale data centers must be able to enforce zero-trust policies.

## Segmentation

Segmenting network traffic establishes control points that reduce the ability of attackers to move laterally to detect and exploit weaknesses in different parts of the network, including the data center. Any data center security solution must natively support various segmentation options to actively limit the attack surface. Segmentation starts by classifying traffic into different segments, especially at the application and port levels, but it can also be done at the host and network levels. And many organizations are utilizing zero-trust principles to segment by identity, and your data center security solution should support this option.

## Time to Service

Many legacy data center security solutions deliver low performance and high latency, meaning organizations can't provide services with the time, agility, and reliability that their hyperscale business demands. Even a tiny amount of downtime or minuscule service delivery challenge can cost companies millions in lost revenue, trust, and brand reputation. And to complicate things further, these services must also interoperate between numerous physical and virtual assets. As a result, modern data center firewalls must offer hardware acceleration for Virtual Extensible LAN (VXLAN) termination and re-origination, provide dynamic support for Layer 4 or Layer 7 security, and support physical and virtual environments through a variety of form factors.

## Capacity

Many IT infrastructures struggle when massive datasets, known as "elephant flows," are transferred over single connections. Once limited to specialized use cases, elephant flows are now standard, especially for organizations in industries such as pharmaceuticals, e-commerce, aeronautics, and financial brokerage firms that require securely encrypting and transferring large datasets using high-throughput flows across data centers or between data centers and multiple clouds. Any network firewall being considered for a hyperscale data center environment must be able to perform at these levels every day.

## Scalability

Business needs, and the networks that support them, are constantly evolving and expanding. Scalable network security means that the security solutions can adapt to the changing needs and demands of the network, such as increasing traffic and new devices, threats, network segments, and regulations. It must also deliver processor-intensive functions like inspecting encrypted traffic without compromising performance. Most legacy systems struggle to perform essential encryption functions, let alone things like inspecting streaming video traffic without introducing latency. Scalable network security also means that the security solutions can be deployed and managed efficiently and cost-effectively without compromising the performance or quality of the network. And that's just the beginning. Performance and scalability are table stakes, and network professionals need to future-proof their data centers with security tools able to handle the workloads of today and those anticipated for tomorrow.

## Efficacy and Innovation

Speeds and feeds are just part of the equation. State-of-the-art hardware must also be matched with security services that can deliver valuable intelligence to keep systems tuned to the latest threats. Ideally, these services should be based on a vast network of global sensors and utilize machine learning (ML) and artificial intelligence (AI) to sort through billions of signals to detect critical and emerging threats. The challenge is that these services are more difficult to evaluate. The best way to sort through all the marketing claims around detection is to focus on vendors whose solutions have been independently tested and verified to provide consistently high detection rates. Similarly, innovation is vital if you want to partner with a vendor who can keep your security ahead of today's determined threat actors. Vendors committed to innovation should have a proven track record of security leadership in research, measured in part by zero-day threats detected and innovation, which can be reasonably measured in terms of the number of security patents they have filed.

### A Hybrid Mesh Firewall Infrastructure

No firewall is an island. Network security solutions—whether for data centers, branches, the cloud, or multiple clouds—should work together as part of an integrated hybrid mesh firewall (HMF) framework. Given the complexity of today's networks, the rapid rate of change, and the speed of both business and threats, it isn't enough for security solutions to share logs and events through a security information and even management (SIEM) tool. Security solutions need to be centrally managed, able to correlate information, use AI to detect anomalies, and coordinate behavior with other security solutions so that, for example, both firewalls and endpoint security tools can actively block malicious traffic from an attacking domain. Modern HMFs are essential to this broader security infrastructure strategy.

## Conclusion

Hybrid mesh firewalls enable IT teams to consolidate point solutions, converge management and orchestration, and increase their ability to detect and respond to threats anywhere across today's distributed networks. They play a critical role in protecting these complex, highly adaptive network environments by defending against new threats designed to exploit those networks regardless of where an attack begins or what resources it targets.

However, selecting an effective HMF solution, as with most new solutions, can be challenging—often due to conflicting information from vendors as they compete for market share. Following these nine simple guidelines will help your organization wade through the hype and select and deploy a solution designed to secure your online users, devices, applications, and resources long into the future.

Click here for more details on the value a hybrid mesh firewall strategy can bring to your organization.





June 17, 2023 12:21 PM

2175626-0-0-EN