POINT OF VIEW

Hybrid Network Architectures Require Innovative Security Solutions

Executive Summary

The rapid pace of business and the rise of remote work necessitate the convergence of on-premises, virtual, and cloud infrastructures. This hybrid network modernization shifts how data centers are perceived and integrated within the network. As a result, there have been some premature declarations about the demise of data centers and data center security. The fact is, however, that it remains crucial to protect data centers with innovative, high-performance firewalls. The key challenge lies in deploying solutions that scale and adapt to the evolving hybrid landscape, securing critical applications and high-throughput traffic across diverse network environments.

As the enterprise data center landscape changes, I&O leaders are transitioning to a hybrid IT operations model where an on-premises data center is no longer the primary driver for infrastructure decisions.[1]

Outside the Traditional Four Walls of a Data Center

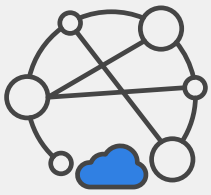
The rise of cloud computing, the accompanying exponential growth of data, and the demand for more responsive applications require data creation and storage to move closer to where data is generated and away from your traditional corporate data center. Likewise, your business applications may live anywhere, from your data centers to multi-cloud to edge compute environments. This distribution of critical resources amplifies your security risks and compounds operational complexity, leading to misconfigurations, inconsistent policy enforcement, and lost visibility as your applications and data traverse the network. Securing the application journey into, within, and across clouds and on-premises locations requires a new approach that natively integrates and extends data center and cloud solutions across your hybrid physical and virtual environments, including all major cloud platforms and technologies.

By adopting a single, cohesive solution instead of trying to separately manage multiple disparate solutions, you can realize consistent policy distribution and enforcement, centralized management, and comprehensive security automation. This will reduce operational complexity, enable greater visibility, and ensure robust security effectiveness across all deployment architectures. By incorporating your infrastructure into a single IT operational model, you can increase network agility, improve security, and quicken response. However, a primary component of such a system remains the data center firewall, provided it can deliver the secure connectivity, network segmentation, and application security you require to protect essential applications, data, and workloads that can't be moved to the cloud but still need to be accessed by employees, customers, and partners.

Defending the Network

Cybercrime is evolving alongside network architecture. Today's expanding attack surface has created an even bigger opportunity for cybercriminals to exploit old and new vulnerabilities. The best defense is to ensure consistent coverage across all attack vectors and tactics, partly because many of today's sophisticated attacks involve a sequence of events. Malicious code enters the network by exploiting vulnerabilities across the attack surface. And once in, it gets to work under the radar, evading detection while expanding its foothold across the network. The trick to thwarting these threats is to have multiple opportunities to stop an attack along its path.

Network and security administrators can begin by implementing a sophisticated approach of their own. The first objective is to protect the network by preventing any threat from breaching edge defenses. However, given the volume of attacks, the sophistication of tools, and the determination of today's attackers, a breach is not a matter of if but when. And when a breach happens, it is essential to have a system designed to detect and minimize business disruptions as quickly as possible. The best way to achieve this is by consolidating technologies and use cases into a simplified, single policy and management framework. This enables organizations to expand visibility and control and reduce risk and cost through early detection and response.



I&O leaders are finding the data center more difficult to design and manage as workloads, infrastructure, and data expand beyond traditional centralized locations. To solve these complex issues, a broader view of data center architecture and operations must be taken into account.[2]

This requires a unified security and management framework that can span all form factors and edges to support hybrid environments in a consistent and coordinated way. This also simplifies operations, helping to address the current IT and security skills shortage. Most IT teams lack people and the financial resources to adequately protect the enterprise. Solving this challenge requires intuitive automation, simplified management, and coordinated response.

Simplifying Operations

Defending your hybrid network starts with a next-generation firewall designed for the data center. But it cannot operate in isolation. To enable an automated security structure that can defend, detect, and respond to today's sophisticated threats, it needs to be part of a centralized security management solution. This enables your NetOps team to observe, correlate, and respond to network anomalies across heterogeneous and distributed networks. It also allows your SecOps team to automatically launch coordinated responses to threats anywhere they are detected, a critical capability for self-healing network operations. By dynamically monitoring across end-to-end domains and coupling that data with advanced machine learning (ML) and artificial intelligence (AI) systems, you can cut through noisy alerts to find and respond to critical issues early in the attack chain before they affect your business.

Centralized management also allows you to deliver consistent and automated security policy across your expanded network ecosystem, essential to building a robust and scalable security posture. It also helps your network and security leaders simplify operations rather than increase complexity. It enables a comprehensive security framework that can span and adapt to your hybrid network to protect all network edges. It also eliminates the manual operations that increase the likelihood of missing critical events because operators cannot hand-correlate data fast enough to detect an attack and launch an effective response.

A single-pane-of-glass network and security management approach is essential for enabling automation and orchestration across the cybersecurity mesh architecture to simplify enterprisewide workflows. It provides your SOC and NOC teams with a unified view across security, networking, and user experience combined with native automation for operation optimization.

Securing the Application Journey

In addition to those applications that, for various reasons, must remain connected to the on-premises data center, most organizations are also building cloud-native applications and leveraging the wide breadth of cloud technologies to gain greater efficiency in delivering application experiences. These applications, deployed in various cloud, hybrid cloud, or virtualized data center platforms, allow users to access them from any location or device.

However, implementing consistent, enterprise-grade security is an afterthought for far too many DevOps teams. The consequence is that applications are often built and deployed without being fully secure—or don't include any security—leaving organizations, their customers, and users at risk.

Implementing a single consistent and optimized security framework experience across hybrid deployments is vital for building, deploying, and running cloud applications and protecting and connecting networks across clouds, data centers, hybrid clouds, and edge compute environments. However, rather than bolting on security after the fact, organizations looking to optimize this journey should focus on the application journey itself, as it is the critical driver in this transformational effort.

Consistently securing every application journey on any cloud empowers organizations to accelerate their digital strategy safely. By ensuring the delivery of consistent policies, centralized management and visibility, and security automation across all clouds and hybrid clouds, organizations can build, deploy, and run business-critical applications and reduce deployment complexity while increasing effective threat detection and response.

Conclusion

As networks embrace hybrid architectures, on-premises data centers retain their importance, and security must evolve. The distributed nature of applications, spanning cloud and edge, demands a comprehensive security strategy. Ad-hoc expansion and outdated firewalls create critical gaps. Modern security solutions are imperative to address the escalating performance demands and complex threat landscape of today's hybrid networks.

In addition, securing today's dynamic applications requires natively integrated data center and cloud security across hybrid and multi-cloud environments. Businesses must deploy next-generation firewalls tailored to modern data center demands, centralized management for networkwide visibility, and simplified operations. This converged approach is essential for defending against sophisticated cyberthreats.

[1] Gartner, How to Evolve Your Physical Data Center to a Modern Operating Model – December 16, 2024 – ID G00816674, Jason Donham, Jonathan Forest

[2] Ibid.

March 28, 2025 4:37 PM / MKTG-1093-0-0-EN