WHITE PAPER

Building Tomorrow's Data Center: Your Journey Starts Now

Executive Summary

Digital transformation has fundamentally reshaped how businesses operate, interact with customers, and compete. This transformation is leading to the need for new hybrid network architectures that combine on-premises data centers with hybrid clouds. However, the underlying technologies must be ultra-reliable, energy-efficient, and secure to meet the dynamic performance, scale, and interoperability demands of these hybrid physical, virtual, and cloud infrastructures. Ensuring consistent visibility and control across these hybrid data center architectures comes with many challenges, including the need for a flexible security architecture that can adapt to change to ensure all network components are safe and operating effectively.

On-premises and virtual data centers are vital pieces in today's ever-evolving networking puzzle, with each part playing a critical role in enabling organizations to compete effectively in today's digital marketplace. In this new model, security is essential to protect resources and assets and enable the network to accelerate and adapt without introducing unknown risks that jeopardize the enterprise. The challenge is that few security solutions are designed to meet the demands of these new hybrid environments.

To ensure your security can meet the needs of your evolving data center strategy, you should look for security solutions that can address the issues described below.

Data center functions are no longer centralized in a physical location but rather deployed to meet complex business requirements by utilizing the public cloud, data center, colocation, and edge deployment locations. Therefore, your data center is no longer limited by walls.[1]

The Changing Network Landscape

Data traversing today's networks is growing exponentially. All that data crisscrossing networks across the globe can overwhelm legacy security systems, creating many opportunities for cybercriminals to exploit any vulnerability or temporary weakness in an enterprise data center's security.

A successful cyberattack may damage productivity, consumer confidence, and brand reputation, which may take years to recover from. While CIOs and IT leaders are certainly focused on risk management and protecting data stored on-premises and distributed across the network, the protections in place are often isolated and disjointed, inadvertently adding complexity and risk to the enterprise.

Work is no longer a place; it's an activity

The changing nature of how people work is another factor leading IT teams to embrace a hybrid network architecture that includes on-premises, public cloud, multi-cloud, and private cloud environments. This rise of remote work, coupled with the move toward cloud computing, means the location of some data creation and storage has moved away from the corporate data center. This expands the attack surface, increases complexity, and reduces visibility.

According to Gartner, "Classic data center edge firewall designs are not obsolete and must be maintained in support of traditional inbound data flow patterns and residual outbound connections from internal users that remain on-site in campus environments or at large branches."[2]

A delicate balance must be maintained because the distribution of functions adds increased complexity, security risks, and fragility due to more moving parts and interdependencies.

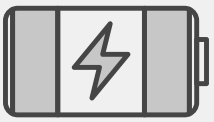
And then there's the environment

In addition to fighting bad actors, data center administrators also worry about environmental sustainability.

With sustainability becoming a requirement for IT infrastructure, the data center's energy usage needs to be greatly reduced. Energy-efficient products can help lower energy costs and reduce the data center's carbon footprint to help adhere to governmental regulations.

Protecting the Dynamic Hybrid Model for Data Centers

Cybercriminals continue to evolve their tactics and use AI to deliver more sophisticated, widespread, and relentless attacks than ever before. The expanding attack surface has created a lucrative opportunity for cybercriminals to exploit old and new vulnerabilities, whether targeting under-secured cloud environments, misconfigured devices, vulnerable IoT, or aging technologies in remote workers' largely unsecured home networks. Ransomware, in particular, is popular among cybercriminals, driven by its low investment and high-profit potential, creating a significant threat to data centers. These facilities, housing vast amounts of valuable data, are prime targets, forcing them to contend with increased risk of attack and the subsequent need for robust and expensive security measures. A successful ransomware incident can lead to devastating consequences, including the encryption of critical data, operational disruptions that cripple services, and severe reputational damage that erodes customer trust. Consequently, data centers must prioritize comprehensive cybersecurity strategies and disaster recovery plans to mitigate the ever-present danger posed by this and other attack methods.



When it comes to data center infrastructure, legacy hardware often is a key contributor to higher carbon footprints and energy waste. By investing in modern solutions, especially those engineered for maximum efficiency, agencies can see immediate results in data center energy bills while lowering an organization's carbon footprint.[3]

Five key elements to protect your hybrid data center

The enterprise data center remains essential for protecting applications, data, and workloads that can't be moved to the cloud but still need to be accessed by employees, customers, and partners. The following components are key:

- **Next-generation firewall (NGFW):** A robust data center protection strategy starts with an NGFW engineered for secure hybrid-cloud connectivity. This NGFW must deliver scalable performance, handling increasing traffic demands with high-speed encryption and decryption to inspect HTTPS traffic. Crucially, it should provide unified security through seamless integration with a security fabric, ensuring consistent policy enforcement across all environments. Finally, granular control through network segmentation and application security is essential to minimize risk and maximize protection.
- **Centralized management:** Because of the distributed nature of hybrid networks, no NGFW solution is complete without centralized security management that provides broad visibility across the entire digital attack surface, on-premises and in multiple clouds. Expanding the infrastructure across a multi-cloud environment inherently widens the attack surface, creating dangerous blind spots due to platform incompatibilities. This reduced visibility significantly elevates the risk of breaches and attacks. To counter this, a robust security management solution must leverage native integrations with major cloud providers, enabling automated and centralized control of your entire security infrastructure through a single, unified interface.
- **Application control:** A third critical element is a solid application access control solution. The evolution to a hybrid workforce means remote workers must be able to consume applications from anywhere at any time. Using virtual private networks (VPNs) to access local or cloud applications results in excessive trust that cybercriminals have been actively exploiting, often by compromising a remote worker's home network and then hijacking their VPN connection to the corporate network. Similarly, SaaS applications consumed in the cloud often have limited security unless traffic goes back to the on-premises data center for deeper scrutiny. Deploying an integrated zero-trust network access (ZTNA) solution enables more secure access to applications, data, and services while delivering a better experience for remote users, whether on or off the network.
- **Intrusion prevention system (IPS):** Patching is a chronic challenge for most organizations, but an NGFW with integrated IPS can help keep critical, hard-to-patch systems up-to-date. By consolidating IPS capabilities into an NGFW, IT teams reduce cost and complexity while preserving control across different network and security operations groups. But as with other extended functions, performance is crucial. An effective IPS-enabled NGFW delivers full security functionality while preserving optimal network performance and user experience.
- **Visibility and automation:** To conquer the security challenges of distributed, hybrid, and multi-cloud environments, organizations must abandon fragmented, legacy approaches. NGFWs must evolve to natively understand cloud architectures, consistently enforce policies, and correlate threat intelligence across all platforms. This cloud-aware approach delivers the unified visibility and automated response capabilities necessary to proactively defend against sophisticated threats and maintain a robust security posture.

Keys to a Future-Proof Framework

The foundation of cybersecurity rests on people: the employees who are the first line of defense and potential vulnerabilities and the experts who craft the solutions organizations rely on. Trust is paramount. Effective security stems from the confidence placed in both the people using the tools and the vendors providing them. Before evaluating any technology, prioritize identifying reputable cybersecurity partners. Seek out those who invest in zero-day research, demonstrate a deep understanding of evolving threats, and engineer a cohesive security ecosystem for your data center. The right vendor empowers your people and strengthens your defenses.

On-premises systems must contribute more flexibility, simplicity, and ease of management than cloud-based systems to remain viable locations for distributed systems.[4]

The best protection for hybrid environments that require agile and adaptive security is to cover all attack vectors and tactics. Today's attacks are a sequence of events requiring a defense-in-depth approach. Once a network is breached, malicious code gets to work under the radar, finding and compromising vulnerable systems, escalating privileges, evading detection, spreading laterally across the network, building backdoors and redundancies, identifying critical data and resources, and then either exfiltrating that data or encrypting it for ransom.

The trick is to deploy an automated security system with multiple opportunities to stop an attack along its path to the data center. That requires a suite of integrated solutions and services designed to operate as a single system, even across a distributed hybrid network. These functions include:

- Advanced sandbox technologies
- Behavioral analytics
- Detection and response systems
- Web filtering
- Antivirus and anti-malware
- AI-based technologies designed to hunt for threats by sifting through mountains of logged data collected from across the network

Ideally, all of these services should be able to run in an advanced security operations center (SOC) environment to detect and respond to indicators of compromise (IOCs) early in the attack cycle.

Finally, look for a provider committed to your success by actively sharing their knowledge and best practices. This can take the form of readiness and response training and services for your SOC teams, enhanced training for novice employees and security professionals alike, playbooks to ensure you're protected and ready in case of a cyber event, and forensic services to get you up and running in the event of a successful breach.

Conclusion

The distributed nature of modern networks, coupled with the rising sophistication of cybercrime, demands a holistic, integrated, and proactive security strategy. This strategy should prioritize robust, cloud-aware NGFWs, centralized management, ZTNA, and intelligent threat detection, all underpinned by a foundation of trust in both technology and the expertise of a reputable vendor. Ultimately, securing the dynamic hybrid model is not merely about deploying advanced technologies. It's about building a resilient security ecosystem that empowers people, anticipates threats, and adapts to change. By embracing a defense-in-depth approach, leveraging automation, and fostering a culture of continuous learning and improvement, organizations can transform security from a reactive burden to a strategic advantage. It is only through this comprehensive and collaborative approach that businesses can confidently navigate the complexities of the digital age and safeguard their critical assets in an increasingly interconnected world.

[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.

[3]Adam Stone, State and Local Governments Benefit from Data Center Sustainability, StateTech, May 13, 2024.

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

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

April 1, 2025 6:34 PM / MKTG-1120-0-0-EN