WHITE PAPER

The Data Center of Tomorrow Starts Today

Deploying a Secure Data Center Across a Hybrid Architecture

Executive Summary

The speed of business is accelerating the data center's journey toward digital transformation, leading to the need for new hybrid network architectures that combine on-premises data centers with hybrid clouds. However, to meet the dynamic performance, scale, and interoperability demands of these hybrid physical, virtual, and cloud infrastructures, the underlying enabling technologies must be more reliable, energy-efficient, and secure than ever. 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.

> "By 2025, individuals and companies around the world will produce an estimated 463 exabytes of data each day—a decade ago, they produced less than three."[1]

Despite the hype that the on-premises data center will soon be extinct, the reality is much more complex. 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—not just to protect resources and assets but to enable the network to accelerate and adapt without introducing unknown risks that can 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 address the needs of your evolving data center strategy, you should look for security solutions that can address the issues described below.

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.

At the same time, the cost of a successful attack continues to rise. According to IBM, the average cost to find and recover from a data breach has reached an all-time high, costing $4.35 million in 2022[2] (in the United States, that cost is $9.44 million per incident). The price of a ransomware attack is even higher. And a destructive attack now takes 233 days to identify and 91 days to contain—a life cycle of nearly a year!

For many organizations, this also means lost productivity, consumer confidence, and brand reputation, which may take years to recover. And while CIOs and IT leaders are certainly focused on risk management and protecting data stored on-premises as well as 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

A recent report from Owl Labs that 62% of businesses worldwide now have a hybrid work arrangement.[3] 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. And 76% of organizations now use two or more clouds to integrate multiple services or for scalability or business continuity reasons.[4]

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. But not all. 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."[5]

And then there's the environment

In addition to fighting back bad actors, data center administrators also worry about environmental sustainability concerns. According to the International Energy Agency (IEA), global data centers consume approximately 200–250 TWh of electricity, contributing to 0.3% of global CO2 emissions yearly.[6] This is more than the national energy consumption of some countries—and around 1% of the global electricity demand.

Protecting the Dynamic Hybrid Model for Data Centers

These market forces have not curtailed cybercrime. In fact, it is more sophisticated, widespread, and relentless than ever before. The expanding attack surface has created a lucrative opportunity for cybercriminals to exploit both old and new vulnerabilities, whether targeting undersecured cloud environments, misconfigured devices, vulnerable IoT, or aging technologies in the largely unsecured home networks of remote workers. Ransomware, in particular, offers a low-investment, high-profit business model that's irresistible to cybercriminals. According to the February 2022 Fortinet Global Threat Landscape report, there are approximately 150,000 ransomware detections per week.[7]

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 consumed by employees, customers, and partners.

1. Protecting any data center starts with a **next-generation firewall (NGFW)** designed to provide secure connectivity, network segmentation, and application security for hybrid-cloud deployments. It must also scale as traffic demands increase, including encrypting and decrypting critical data without impacting data center performance or user experience. And because they must operate in a hybrid environment, data center NGFWs must seamlessly interconnect with security solutions deployed across the network, including data centers, branch offices, cloud systems, and multiple cloud environments that provide or consume essential services. This security fabric approach ensures centralized, consistent security policy enforcement and data protection across the distributed network without compromising performance.
2. 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, both on-premises and in multiple clouds. Deploying resources across a multi-cloud environment inevitably leads to more blind spots as the attack surface expands—especially because clouds run on distinct and largely incompatible platforms. The resulting reduced visibility increases the potential for breaches and attacks. Because of this, an effective security management solution should use native integration with each major cloud provider to enable automated, centralized management of the entire security infrastructure from a single pane of glass.
3. A third critical element is a solid **application access control solution**. The evolution toward a hybrid workforce means remote workers must be able to consume applications from anywhere at any time. Using virtual private networks (VPN) 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 back into the corporate network. Similarly, Software-as-a-Service (SaaS) applications consumed in the cloud often come with limited security unless traffic goes back to the on-premises data center for deeper scrutiny. Deploying a 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.
4. Sixty percent of successful security breaches are traced in some way to poor patch management.[8] Because patching is a chronic challenge for most organizations, NGFWs can help keep critical, hard-to-patch systems up-to-date with an integrated **intrusion prevention system (IPS)**. By consolidating IPS capabilities into a next-generation firewall, 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 IPS-enabled NGFW must be able to perform all of its functions without degrading network performance or impacting user experience.
5. Protecting today's distributed data centers requires a **holistic approach**. Hybrid architectures expand the attack surface, reducing visibility and increasing risks. And security becomes exponentially more complicated when it needs to protect a multi-cloud environment. Many legacy solutions can't be deployed in every cloud environment, can't effectively share or enforce policy, or cannot collect and correlate threat intelligence from across the network to detect sophisticated threats and automatically launch a coordinated response. An NGFW solution must natively understand how clouds function to consistently enforce security policies across different cloud providers. It must also be capable of monitoring the ever-changing state of private and public cloud resources to ensure consistent end-to-end security and a strong and consistent security posture.

Building a Framework for Success

All security starts and ends with people. People deploy what they trust. And the people who build, design, research, and update security products are often the key differentiators between a solution that works and one that doesn't. That's why, before you start evaluating devices, you need to identify credible cybersecurity providers—ones that run their own zero-day research, understand the threat surface and how to defend it, and have created a vital synergy between the various security components that protect the data center.

> "Many enterprises are struggling to adapt and scale security to a new work paradigm driven by digital transformation and the shift to remote work."[9]

You also need defense in depth. Rather than yesterday's cumbersome (and expensive) model of layering duplicate technologies, 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. 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, and artificial intelligence (AI)-based technologies designed to hunt for threats by sifting through mountains of logged data collected from across the network, to name a few. And 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

Network architectures may be changing, but cybercrime does not stop. Your expanding attack surface has created an even bigger opportunity for cybercriminals to exploit old and new vulnerabilities. However, network and security administrators can thwart these efforts with a sophisticated approach of their own. It starts with next-generation firewalls that can be seamlessly deployed in any environment in any form factor, connected by a centralized security management solution that enables an automated security structure that can span and adapt to even the most dynamic network environments. Mixing in application access control and intrusion prevention as part of a holistic approach will ensure the security of your evolving data center strategy.

[1] McKinsey & Company, "Is your organization using data ethically?" October 2022.

[2] IBM, Cost of a Data Breach Report 2022, March 2022.

[3] Owl Labs, State of Remote Work 2022, July 2022.

[4] Cybersecurity Insiders, 2022 Cloud Security Report, May 2022.

[5] Gartner, "How the Shift from Firewall Appliances to Hybrid Cloud Firewalling Will Change Selection Criteria," March 2021.

[6] International Energy Agency, Data Centres and Data Transmission Networks, September 2022.

[7] FortiGuard Labs, Global Threat Landscape Report, 2H 2021, February 2022.

[8] John Emmitt, "Patch Management: Best Practices and Why It's Important," Security Boulevard, March 2021.

[9] Gartner, "How the Shift from Firewall Appliances to Hybrid Cloud Firewalling Will Change Selection Criteria," March 2021.

FORTINET®

www.fortinet.com

January 23, 2023 8:54 AM

1903707-0-0-EN