

CHECKLIST

Top 6 Recommendations to Improve User Productivity with a Hybrid Architecture

The speed of business is accelerating the data center's journey toward digital transformation, requiring new hybrid network architectures that combine on-premises data centers with hybrid clouds. However, to meet the needs of organizations looking to expand that digital transformation further, the underlying enabling technologies must be more reliable, energy-efficient, and secure than ever.

On-premises and virtual data centers are vital pieces in today's ever-evolving networking puzzle. 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.

Here are six things organizations need to do to position themselves for success.

- ✓

Invest in a Flexible Next-Generation Firewall

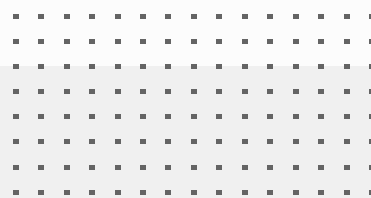
Organizations must invest in a next-generation firewall (NGFW) that includes solutions like SD-WAN, Universal ZTNA, inline sandbox, and SOC-as-a-Service. Such technologies improve WAN connectivity by providing a better user experience with direct internet access, while LAN and WLAN provide faster access to local devices and users. In addition, organizations should consider investing in network firewalls that utilize specialized Application-Specific Integrated Circuits (ASICs) designed for a specific application or purpose beyond what general-purpose CPUs can provide, such as accelerating network security functions.
- ✓

Deploy Unified Networking and Security

Security can't be an afterthought. When security solutions are not well-integrated—with each other or the underlying network—security risks and gaps arise as the attack surface expands and adapts. Such blind spots are vulnerable to sophisticated multi-step attacks and are partly responsible for the dramatic rise in successful ransomware attacks. Because of this, it is essential to implement a unified security framework able to deliver automated and reactive security that can span the entire attack surface. Organizations must also converge their security with networking to protect digital acceleration efforts. NGFWs enhanced with ASIC technology can significantly improve the performance of security functions compared to general-purpose processors. That means they can handle more traffic, perform security inspections at faster speeds, and process packets more quickly, reducing delays in network traffic.
- ✓

Combining Zero-Trust Edge Strategy with Consistent Security and Networking

With new network edges being created on-premises and in the cloud at an unprecedented rate, it is critical that the unified convergence of networking and security be available everywhere—and combined with ZTNA to enable explicit access for applications and continuous verification of users and devices. This convergence is the heart of a zero-trust edge strategy, while flexibility in providing such convergence is vital in securing digital acceleration for rapidly changing hybrid deployments.



✓ **Speed Operations with Centralized and Automated Management**

The exponential growth of network edges, cloud platforms, and tools can significantly increase operational complexity. At the same time, poor network visibility and analytics gaps, as well as manually performed tasks, can degrade the end-to-end digital experience.

These and similar issues can significantly increase the time to configure, manage, and troubleshoot solutions. They also add to operational costs and errors that can cause network outages and reduce flexibility. With centralized and automated management and a dashboard that spans the entire network and security stack, the delivery of network services across their whole life cycle is expedited, while removing manual configuration eliminates a major cause of downtime and security breaches.

✓ **Increase Visibility with End-to-End Digital Experience Monitoring**

Traditional network performance, IT infrastructure, and application performance monitoring limit NOC team visibility. Legacy monitoring systems simply don't provide the insights into critical business application performance that today's organizations require. They also severely hinder the visibility that frontline NOC and help desk teams need to rapidly identify and resolve issues.

A modern digital experience monitoring (DEM) platform gives your NOC team superior visibility. It allows for the end-to-end observation of any application—from the end-user, across the distributed network, and even out to the infrastructure the application is hosted on. A DEM solution can enrich incident management while supplying holistic remediation of performance issues.

✓ **Consolidate and Simplify Operations to Provide Instant ROI**

Organizations adopting modern networking technologies with integrated security achieve better ROI than point products with limited security. Furthermore, it improves employee productivity with better user experience and simplified operations.

Conclusion

Many organizations still use a traditional architecture to connect offices to the data center for application access. However, with users working from anywhere and applications distributed across multi-cloud or SaaS environments, legacy network designs hinder digital acceleration and create user experience challenges. Organizations that want better user productivity and more secure network edges need to invest in a modern hybrid network architecture with integrated security.

Fortinet is the only vendor to offer an NGFW that includes and supports SD-WAN, Universal ZTNA, inline sandbox, and SOC-as-a-Service to protect any edge at any scale. Offering the best convergence of networking and security in the industry, Fortinet empowers organizations to adopt modern networking technologies essential for digital acceleration. Read how Forrester's [Zero Trust Edge Model](#) validates Fortinet's convergence approach. Read how Forrester's [Zero Trust Edge Model](#) validates Fortinet's convergence approach.