HUGHES An EchoStar Company | FORTINET

POINT OF VIEW

Why You Should Invest in Unified SASE Even If You Already Have Secure SD-WAN

Executive Summary

Organizations that have invested in secure SD-WAN have optimized on-premises user experiences, enhanced operational efficiency, and reduced costs. As hybrid work has increased in the last few years, organizations want to extend similar experiences to work-from-anywhere (WFA) users.

The Challenge

Many organizations struggle with maintaining a consistent security approach and a seamless user experience, which is needed to close security gaps and improve productivity for WFA users. The traditional VPN-based approach presents significant challenges for IT teams attempting to enforce consistency across a distributed workforce. VPNs rely on implicit trust, creating significant security risks, including unauthorized access, lateral movement of threats, and increased attack surface exposure.

By 2026, 85% of organizations seeking to secure their web, SaaS, and private applications will obtain the security capabilities from a security service edge offering.[1]

The Case for Adopting Unified SASE

Several factors should be evaluated as organizations consider adopting unified SASE to extend the benefits of existing secure SD-WAN deployment to WFA users. The following are a few key features a robust unified SASE solution will include:

Unification: A SASE solution should have a single console that simplifies configuring and managing security policies along with a single-user agent that reduces complexity and sprawl. Also, it should feature a single data lake that enhances insights and analytics, providing a comprehensive view of an organization's security posture.

Simplification: Transitioning to unified SASE must be easy and completed quickly. Integrating SD-WAN and security service edge (SSE) can be done in minutes to allow remote users to access application steering capabilities from anywhere and get consistent security everywhere.

Performance: A unified SASE solution needs to enable resilient and optimized application performance for remote users. By extending native SD-WAN capabilities to the cloud, SD-WAN policies and rules are applied to connect users on optimal paths to their private applications.

An Easy Way to Onboard SSE to SD-WAN

Existing Fortinet customers who invested in secure SD-WAN or FortiGate Next-Generation Firewalls in the data center or campus want to provide secure and efficient connectivity for hybrid users accessing private applications. Fortinet offers an easy way to onboard SSE to SD-WAN in minutes and provides unified management ideal for organizations looking to improve security and networking for their hybrid workforces.

Organizations can now leverage the Fortinet SSE solution FortiSASE for WFA users to enable secure private access to these private applications and enhance network performance. It will improve user experience by leveraging native SD-WAN integration and comprehensive security inspection over traditional remote access methods.

Conclusion

Many organizations are transitioning to a unified SASE solution to address the security challenges of hybrid work, cloud adoption, and the need for zero-trust security. This approach combines SD-WAN with cloud-delivered security services like Firewall-as-a-Service, zero-trust network access, and cloud access security broker to provide a comprehensive and manageable security solution.

Unified SASE solves challenges related to managing a distributed workforce, securing cloud applications, and transitioning to a zero-trust model by providing centralized security policy management, improved visibility and control, and a better user experience. This results in simplified IT management, reduced security risks, and a stronger security posture for organizations of all sizes.

[1] Charlie Winckless, Thomas Lintemuth, Dale Koeppen, Magic Quadrant for Security Service Edge, ID G00792702, Gartner, April 15, 2024.

March 12, 2025 11:14 AM / MKTG-940-0-0-EN