HUGHES An EchoStar Company | FORTINET

WHITE PAPER

Unifying Hybrid Workforce Cybersecurity with SASE

A Transformative Approach to Securing Users, Devices, Locations, and Applications

Executive Summary

Organizations must continue to support and secure their work-from-anywhere (WFA) employees who access network resources from varied locations and devices. This is paramount because remote network access introduces complexities and vulnerabilities, requiring robust security solutions to protect against ever-evolving cyberthreats.

The rise of remote work and the proliferation of digital threats necessitate a holistic approach to security, addressing challenges such as consistent policy enforcement, seamless access to cloud resources, and centralized management. Secure access service edge (SASE) solutions offer a transformative approach to unifying hybrid workforce security by integrating networking and security functionalities into a cloud-native platform. SASE protects users, devices, locations, and applications, regardless of their network environment.

73% of executives believe remote workers pose a greater security risk.[1]

SASE goes beyond traditional networking and security solutions by providing cloud-based security service edge (SSE) and on-premises SD-WAN, integrated security services, zero-trust access, and centralized management and monitoring capabilities. This comprehensive solution enables organizations to enhance their security posture, improve operational efficiency, and support a safe and productive working environment for all employees, regardless of location or device. SASE represents the future of hybrid work security, empowering organizations to embrace remote work opportunities while mitigating the associated risks effectively.

Solving Hybrid Workforce Cybersecurity Complexity

With the rise of the hybrid workforce, organizations have had to secure their employees who access the network and applications from on-site and off-site. This WFA shift has significantly expanded the attack surface, encompassing home offices and mobile workers, thereby increasing the complexity of network, application, and resource security.

Organizations dealing with numerous remote offices and WFA employees often encounter difficulties in consistently applying and enforcing security policies and ensuring an optimal work experience for users, regardless of their network location. Securing this WFA environment presents a unique challenge as the changes have occurred organically rather than through a carefully planned strategy.

The rapid proliferation of new network edges and the inclusion of WFA employees, often implemented as independent projects, have created vulnerabilities that cybercriminals eagerly exploit. On top of this, the trend has also led to organizations experiencing poor user, device, and application visibility, resulting in more threats and security gaps.

SASE architecture helps address these challenges by providing secure access and high-performance connectivity to users in large and small branches and remote locations. However, many SASE solutions only solve part of the problem. They either fail to provide consistent enterprise-grade cybersecurity to their hybrid workforce or cannot seamlessly integrate with the range of physical and virtual network and security tools deployed at the network edge. The result is an inability to deliver consistent cybersecurity or optimal user experiences.

Making SASE Unified to Secure Users, Devices, and Locations

SASE represents a transformative approach to network security by unifying disparate security and networking functions into a single, cloud-native platform. One of the core tenets of SASE is its ability to secure users, locations, and applications, regardless of their location or network environment.

Secure users and locations

SASE ensures that users, whether working in the office or remotely, are consistently protected. SASE also extends security protections to any locations where users access network resources, including branch offices and remote sites, whether the user is home, at a coffee shop, or in an airport.

Secure access to applications

In today's digital landscape, applications reside in various environments, including data centers, public clouds, and Software-as-a-Service (SaaS) platforms. SASE ensures that all users who access applications, regardless of their hosting environment, are protected against cyberthreats and data breaches. By integrating features such as cloud access security broker (CASB) functionality, zero-trust network access (ZTNA), and SD-WAN intelligent routing and steering, SASE solutions provide comprehensive protection for SaaS and legacy applications alike.

Unified security platform

At the heart of SASE is a unified security platform that seamlessly integrates various security services, including next-generation firewall (NGFW), secure web gateway (SWG), ZTNA, and secure SD-WAN, among others. This unified approach enables organizations to consolidate their security policies and the number of agents, simplify deployment and management, and reduce the attack surface by eliminating security silos and blind spots.

Scalability and flexibility

SASE solutions are designed to scale dynamically to accommodate the evolving needs of modern enterprises. Whether supporting a small branch office or a globally distributed workforce, SASE platforms offer scalability and flexibility to adapt to changing business requirements. This ensures that organizations maintain a consistent security posture regardless of size, industry, or geographic footprint.

Unfortunately, the shift to remote work has collided with a massive uptick in cybersecurity threats. Such threats include phishing, smishing, and ransomware. The average data breach cost for organizations of 500 employees or fewer is $3.31 million, and the total cost of a breach is never immediately known.[2]

Optimized user experience

With secure SD-WAN, organizations can improve connectivity, operations, and application access by enhancing and securing the WAN on-premises. This transformation results in a significantly better user experience for all. When secure SD-WAN is integrated with SSE, applications are intelligently and dynamically steered over appropriate links, ensuring business productivity and quality of experience, and remote users can leverage the superior user experience to access corporate applications securely and efficiently.

Key Elements of a SASE Solution

While most network solutions have been able to evolve rapidly enough to support the workflows of remote users, offices, and endpoints, most security tools and solutions have not kept pace, failing to offer consistent security and ensure optimal user experience for on-premises and remote users.

In today's evolving WFA landscape, where employees require secure access to applications from various locations and devices, VPNs fail to provide the necessary security and flexibility. SASE has emerged as the modern solution for remote access and hybrid work security, offering a comprehensive approach to security.

An efficient SASE solution combines multiple security capabilities, including NGFW, SWG, ZTNA, CASB, remote browser isolation (RBI), data loss prevention (DLP), end-to-end digital experience monitoring (DEM), together with SD-WAN, into a single, integrated platform. This unified cloud-native architecture allows organizations to consolidate their security stack, simplify management, optimize user experience, get consistent security, and improve visibility across their entire network infrastructure. It also allows for secure access to applications, corporate or SaaS, and to the internet for complete protection against all types of threats.

SASE solutions must also embrace a zero-trust security model, with a single and unified agent, where access to network resources is based on strict authentication, authorization, and continuous verification mechanisms. Organizations can reduce the risk of insider threats, unauthorized access, and lateral movement within their network infrastructure by adopting a zero-trust approach.

SASE solutions incorporate comprehensive AI-powered threat intelligence feeds and analytics to identify and mitigate advanced threats in real time. By leveraging machine learning, behavioral analysis, and threat intelligence sharing, organizations can proactively defend against a wide range of cyberthreats, including malware, ransomware, phishing, and zero-day exploits.

SASE vendors should accompany organizations through their journey and adapt to their architecture and needs. From large branches with SD-WAN to smaller locations with LAN connectivity only to remote locations around the world, SASE needs to secure everyone everywhere to allow for consistent user experience and security.

Conclusion

SASE goes beyond simply addressing the immediate security concerns of the hybrid workforce. It provides scalability, flexibility, and agility to adapt to the evolving needs of modern enterprises. By consolidating security policies, simplifying deployment, and improving visibility, SASE enables IT teams to enhance their security posture and support a safe and productive working environment.

SASE represents the future of hybrid work security, offering organizations a unified platform to secure their network infrastructure, empower their WFA employees, and confidently navigate the complexities of the digital age.

[1] Kathryn Haan, Remote Work Statistics and Trends In 2024, Forbes, June 12, 2023.

[2] Zero Trust Security in the Age of Remote Work, i4DM, September 23, 2023.

March 4, 2024 8:39 AM

2589418-0-0-EN