

POINT OF VIEW

Moving Beyond Fragmented Cloud Security with Unified SASE



Executive Summary

Over the past two decades, organizations have steadily embraced the cloud as a platform for business applications. This shift accelerated during the pandemic with the broad adoption of remote work. Today, many organizations have endorsed a hybrid approach to the workplace with branch office workers, hybrid employees, and on-premises workers leveraging a mix of cloud services and applications, private cloud, and the internet.

The combination of a hybrid workplace and a multi-cloud environment has created a fragmented and complex cloud security infrastructure. Traditional security approaches cannot handle this complexity. A unified approach to cloud security is what's needed to eliminate the silos created by point solutions, to simplify day-to-day management, and to offer fast diagnosis and remediation of problems.

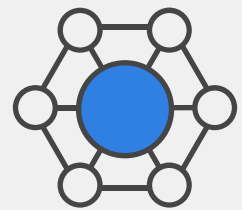
Unified SASE connects users to applications and the web using a unified client. Single-pane-of-glass management ensures consistent network performance and powerful security with built-in intelligence that dynamically adapts to the needs of a hybrid workforce. Adopting a SASE solution that is unified, flexible, and intelligent ensures robust hybrid-work security, more operational efficiency, and a superior digital experience.

Building an Efficient SASE Solution

Today, SASE solutions consolidate a wide variety of networking and security services, including cloud access security broker (CASB), SaaS Security Posture Management (SSPM), secure web gateway (SWG), zero-trust network access (ZTNA), Firewall-as-a-Service (FWaaS), software-defined wide area network (SD-WAN), digital experience monitoring (DEM), and data loss prevention (DLP).

SASE solutions secure a hybrid workforce and multi-cloud workflows and avoid the complexity of traditional security approaches. However, SASE places a substantial burden on administrators who need to master the interfaces of many different tools. Also, the thin edges of the network, including IoT and BYOD, are often unsupported, creating vulnerabilities.

A unified SASE approach addresses these deficiencies, offering consolidated security management from the network edge to the cloud, a variety of deployment options, including on-premises, cloud, and hybrid, sophisticated threat detection and remediation using AI, and the incorporation of generative AI to simplify operations.



“By 2028, 50% of new SASE deployments will be based on a single-vendor SASE Platform offering, up from 30% in 2025.”¹

SASE Must Be Unified

Too often, network and security teams solve issues with seemingly harmless “one-off” point solutions. Unfortunately, this approach can undermine a SASE installation. Examples include deploying a VPN solution for remote access and installing individual point products for each security service edge (SSE) feature, like SWG, CASB, and ZTNA. This leads to inconsistency in corporate security policies and controls and a gap in an organization’s security posture.

One-off actions increase inefficiency and add to network and security complexity, with the corresponding risk of security misconfigurations and troubleshooting issues. That is why unification is the solution.

A unified SASE solution, combining Secure SD-WAN and a cloud-delivered SSE from a single vendor, simplifies security management, enhances visibility, and streamlines operations across an organization’s entire infrastructure, from the network edge to the cloud, resulting in improved user experience, faster onboarding, and reduced costs.



“By 2028, 70% of SD-WAN purchases will be part of a single-vendor SASE Platform offering, up from 25% in 2025.”²

SASE Must Be Flexible

A flexible SASE solution can effectively secure and manage a diverse, distributed network infrastructure by incorporating such features, providing robust support for modern enterprise needs. It also provides adaptable, unified security management across an organization’s entire network infrastructure, regardless of location or device, supporting various deployment scopes and bandwidth requirements to secure users, applications, and devices everywhere.

SASE Must Be Intelligent

In today’s threat landscape, reactive security isn’t enough. A modern SASE solution must leverage AI and GenAI to provide proactive, real-time threat detection and mitigation, streamline operations, and enhance overall security posture and operational efficiency across SD-WAN and SSE environments.

Conclusion

SASE isn’t just a solution, it’s a strategic advantage that empowers organizations to confidently embrace the future of work. To thrive in today’s complex digital world, organizations must prioritize a SASE solution that is unified, flexible, and intelligent. This approach ensures robust security and operational efficiency, empowering organizations to embrace the hybrid workforce and multi-cloud strategy without compromising on security.

By consolidating security functions, offering flexible deployment options, and leveraging AI-driven insights, a comprehensive SASE solution enables businesses to navigate the evolving threat landscape and adapt to the dynamic needs of a distributed workforce. The right SASE solution empowers organizations to embrace the future of work and multi-cloud environments securely and confidently.

¹ Jonathan Forest, Neil MacDonald, Dale Koeppen, Magic Quadrant for SASE Platforms, Gartner, 9 July 2025, <https://www.fortinet.com/resources/analyst-reports/gartner-magic-quadrant-sase>.

² Ibid.

Gartner is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.