



Secure Access Service Edge (SASE): 7 Ways Your Business Benefits

The proliferation of new technology has turned business inside out. Operations increasingly exist in a digital framework: employees travel for client meetings or work remotely, retail clerks take orders anywhere in the store, manufacturing and warehouse employees use tablets while on the floor, IoT devices gather data and perform advanced AI functions, and more. All are accessing data and apps that may be located in the cloud. What was once locked away in the data center has broken through the walls. Users — and what they need — can be anywhere.

Demands on IT infrastructure have changed as a result. While mobile work is growing and truly distributed edge computing has become a reality, many companies still depend on relatively centralized hub-and-spoke architectures.

In a hub-and-spoke architecture, the network backhauls traffic to a central hub, where it passes through multiple security devices. Afterward, the traffic moves out to the eventual destination, like a cloud service, for example. Return traffic retraces the same inefficient path. The result is poor user experiences due to data latencies, increased operational complexity from managing multiple point security and management products, longer troubleshooting times, and more difficult change management.

The structure limits a company's operational flexibility, increases costs, makes it difficult to provide unified security, and wastes enormous opportunities.

An emerging approach to infrastructure, called Secure Access Service Edge (SASE, pronounced "sassy"), offers a cohesive yet incremental approach to creating a new context for computing. SASE sits atop software-defined wide area networks (SD-WANs) by integrating security capabilities. The combined services can be managed in cloud implementations and delivered on-premises or via cloud, depending on users' requirements.



SASE sits atop software-defined wide area networks (SD-WANs) by integrating security capabilities. ”

The benefits that SASE offers organizations helps explain why Gartner estimates that **by 2024, at least 40% of enterprises will have SASE adoption strategies**, up from only 1% in 2018.¹

Here are seven reasons you should consider joining the 40%.



1. REDUCES NETWORK-RELATED COMPLEXITY AND COSTS

Companies can solve the trade-off between best-of-breed point solutions and integrated systems. Rather than cobbling together hardware and software from multiple vendors, a business can deal with a single provider for unified management. As a result, companies need fewer appliances and software solutions, and the reduction in complexity delivers costs savings. This unified approach also makes possible more comprehensive monitoring, visibility, and analytics across various services.

2. ENABLES NEW DIGITAL BUSINESS SCENARIOS

The biggest challenge to businesses from current IT infrastructure is its closed-world nature. With cloud-based workloads and applications as the new reality, infrastructure and security must move beyond the premises. Reaching outward is the future of business. Companies need to be able to work seamlessly with remote employees, business partners, contractors, and customers. Instead of relying solely on traditional VPNs that, at best, provide coarse-grained network access, SASE enforces identity and context-aware policies to grant dynamic and granular access for everyone, including business partners. It allows you to open up possibilities without opening the gates to security breaches.

3. IMPROVES PERFORMANCE AND REDUCES LATENCY

In a world where some businesses need nanosecond responses and customers expect immediate action, performance is critical. Voiceover IP (VOIP) telephony, video, collaboration, production control, mission-critical application use, access to business productivity apps, and more all have different performance requirements. Some apps are particularly sensitive to latency while others aren't. IT departments can set policies through SASE that route traffic through the most appropriate channels, whether over a high-bandwidth, low-latency backbone or slower links. That saves more expensive resources for the most important needs.

4. ENHANCES THE USER EXPERIENCE

There are two aspects to user experience. The first is ease of use. Identity-centric policy enforcement can simplify tasks through approaches like a user identity-based single sign-on (SSO) and by providing a consistent experience, no matter the location, device, or application. The second aspect is the perception of application performance. End-to-end latency and similar factors can cause delays that disappoint users. SASE helps prevent performance lag by catching traffic from an endpoint as quickly as possible, applying the required security treatment, and sending the traffic to its destination on the fastest path possible. And when SASE applies the necessary security, it does so by minimizing the number of encryptions and decryptions and eliminating unnecessary chains between security services, providing a latency-sensitive approach.



5. LOWERS OPERATIONAL OVERHEAD

As people and organizations shift more activity to cloud computing and introduce innovative mobile and distributed use cases, change is inherent in computer systems. Traditional hub-and-spoke infrastructures lack flexibility to adapt quickly or simply. Because SASE is cloud-managed and delivered, it can quickly deploy services on premises and in the cloud elastically. Enterprises can scale up or down quickly and easily without needing additional appliances and other hard connections.

6. PROVIDES UNIFIED, ZERO-TRUST SECURITY

SASE takes a zero-trust approach to security, where no endpoint is assumed to be secure. Security is integrated throughout the network, with identity- and context-aware policies being applied centrally to all traffic, even when users are interacting with third-party cloud-based apps or social networks. Tailored decisions can still be made at the local level to address specific needs. With this centralized context-based policy, end-to-end encryption, and protection at all points of entry, SASE helps to ensure corporate and regulatory security needs are met, no matter where users or devices are accessing the network.

¹Gartner, *The Future of Network Security Is in the Cloud*, August 30, 2019

7. INCREASES EFFECTIVENESS OF NETWORK AND SECURITY STAFF

Traditional infrastructures require high staffing levels to manage installation and configuration of the ever-expanding number of devices and applications necessary to keep pace with business. When both network and security operation center services are centralized through a trusted SASE provider with a strong SLA, companies need fewer personnel to manage basic work. Corporations can redirect resources to more complex issues, such as using global capabilities to address nuanced issues of business, regulatory compliance, and application needs. Businesses can have their networks completely managed by a single trusted vendor or maintain as much control as they wish.

OPEN SYSTEMS DELIVERS SASE TODAY

Nearly a decade ago, Open Systems launched an integrated software-defined network and network security platform, delivered as a service. Today, we enable network management simplicity, security, and performance with an edge- and cloud-integrated secure access service edge (SASE) platform to enable enterprises to rapidly adapt their network to the speed of their business.

To learn how SASE can help your business, [contact us for a free assessment.](#)



Open Systems is a leading provider of a cloud-delivered secure access service edge (SASE) platform, provided as a service, that transforms traditional networks into secure, simple-to-manage and cost-effective networks that quickly adapt to the speed of digital business. Managed by world-class experts, the Open Systems platform couples the simplicity, security and performance with the visibility, flexibility and control enterprises absolutely need in their networks. Learn more at www.open-systems.com