

DELIVERING SPEED AND SECURITY AT CLOUD-LEVEL ENTERPRISE SCALE

Secure access service edge (SASE) solutions provide a competitive edge by optimizing network protection and performance.

AFTER A RECORD-BREAKING NUMBER OF DATA

breaches, cyberattacks, and ransomware incidents over the past year, nowhere has digital transformation accelerated faster than in the field of network security and performance. To better protect their operations, six in 10 companies anticipate adopting secure access service edge [SASE] solutions by 2025, according to research and advisory firm Gartner. These future-focused tools are quickly becoming the preferred option for safeguarding and supercharging enterprises as they shift to hybrid work, remote devices, and cloud-based apps.

"The pandemic has sparked the work-fromhome era and spiked the demand for cloud-based services. As enterprises face this new normal, many grapple with expensive hardware-based solutions and outdated VPN that hinder user experience," says Abe Ankumah, senior director of product marketing and partnerships for leading cloud-computing security and virtualization technology provider VMware. "Seeking to redesign, upgrade, and safeguard their networks, IT teams across industries are turning to products like cloud-delivered VMware SASE, which affordably combine best-of-breed network connectivity and security to improve user experience and simplify IT operations."

The move to SASE solutions also underscores a major shift in industry thinking. Specifically, IT professionals are recognizing that network security perimeters and data usage needs have grown exponentially and a holistic approach is now required, as organizations today deal with thousands of online interactions from many different devices and apps.

The benefit of SASE is that it is a form of network architecture that combines best practices in data access and privacy with cloud-native security functions (e.g., secure web gateways and firewalls) and zero-trust (multifaceted authentication) principles. It takes both enterprise computing and the fight against cybercrime to the cloud, using a multilayered web of digital connectivity and defense technologies that are interlaced throughout a business's overall IT infrastructure. This speeds up network access and helps protect every high-tech touchpoint and interaction from danger.

TechRadar reports that nine in 10 CEOs say they're already deploying or considering adopting SASE solutions. These sophisticated offerings often consist of numerous parts, such as SD-WAN (seamless multicloud) network architectures, A.I.-based cloud security tools that defend data and applications, and a myriad of network or endpoint entry monitoring programs. But given the scope and scale of such efforts, and the range of high-tech exchanges that need safeguarding, when it comes to successful SASE implementation, there's more to consider than just the underlying technology.

For example, according to VMware, those considering collaborating with SASE providers should look for vendors with extensive experience working with both cloud-based security services and cloud-delivered SD-WAN. A SASE specialist should also be able to support the seamless integration of third-party apps and tools, allowing companies to mix and match solutions to best

"THE PANDEMIC HAS SPARKED THE WORK-EROM-HOME ERA AND SPIKED THE DEMAND FOR CLOUD-BASED SERVICES."

ABE ANKUMAH

SENIOR DIRECTOR, PRODUCT MARKETING AND PARTNERSHIPS, VMWARE support their operations as needed. By efficiently connecting data centers, network touchpoints, and apps—and delivering them to the workforce at lightning speed, thanks to close network proximity—companies can leverage these solutions to build a nimbler, more resilient enterprise.

"The traditional tools used to speed up network access and safeguard connections and data are less applicable once your organization moves to the cloud," says Aaron Cockerill, chief strategy officer for endpoint-to-cloud security provider Lookout. "Users are increasingly accessing your business via their own connections and devices, even as encryption is growing and organizations' level of control over networks and their network visibility continues to shrink. SASE cloud architecture helps businesses improve productivity and security, as well as better adapt to a world of remote devices and hybrid work where more sensitive data is regularly being shared online."

Case in point: Faced with the unexpected rise of COVID-19, in March 2020



one leading health organization needed to quickly transform its business to enable its staff to work remotely. The organization needed to maintain regulatory compliance with the Health Insurance Portability and Accountability Act [HIPAA] and securely maintain patients' privacy. Within just a matter of weeks, Lookout was able to help the organization's operations, and its 25,000 employees, make the shift to cloud-based solutions. Such is the strength and versatility of a SASE implementation, which—in addition to enabling online productivity at scale—helps companies access

applications, networks, and the web with intelligent security protocols and smart analytics technology in place.

By switching to these SASE solutions, companies can provide consistent and reliable access to software programs and data, while minimizing

downtime and latency (network lag). But most important, SASE tools and technologies provide true elasticity at enterprise scale, making it possible to efficiently support both a growing workforce and an array of high-tech hardware options ranging from laptops to mobile devices.

"SASE makes it possible to more effectively protect and defend online operations, while also enabling workforces to achieve greater productivity," says VMware's Ankumah. "Companies can employ the technology not only to help conduct day-to-day operations but also to transform their enterprise."

We protect your data.

You need an integrated approach to keep your business running securely.

The Lookout Security Platform delivers consistent security across all applications and data. We detect and respond to threats in real time while reducing complexity, cost and disruption.



