WEI INSIGHTS TECH BRIEF

THE FIRST 5 THINGS YOU SHOULD KNOW ABOUT SASE

64% of IT decision makers ranked 'improving data security' as the top IT objective investment, up 22% from the same survey conducted in 2018.[1]

In addition to a wider variety of malicious threats, cybersecurity professionals are adjusting to new and complex networks with unique security needs; namely, those of a decentralized work environment. The normalization of remote work in 2020 and 2021—coupled with wider use of home networks and personal devices for work-related file sharing and behavior—has created an entirely new security paradigm. The traditional wheel-and-spoke security approach will no longer suffice.

As an alternative, Secure Access Service Edge (SASE) security is gaining interest and adoption from leading enterprises. Pronounced "sassy," SASE means cybersecurity no longer needs to operate from a centralized data center, securing WAN in a cloud-native environment instead.

MORE THAN CLOUD-BASED SECURITY

Traditionally, "security, speed and simplicity make an impossible triangle," as Forbes described in December 2020. "It's a tug of war, and if you pull in one direction, you compromise the other two."[2] Fortunately, SASE represents not just cloud-based security but a convergence of security components into a connected, cloud-native environment that streamlines multiple aspects of security without encroaching on the experiences of users. SASE "is therefore a natural solution for managing this new distributed, perimeter-less world," says Forbes.

At a strategic level, SASE represents a solution area for those looking to unify networking and security, reducing cost and risk to the organization while improving everyday operations and collaboration—no matter where workers sit. Gartner predicts that "by 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at the end of 2018."[3]

BEFORE YOU BEGIN: 5 ASPECTS OF THE SASE MODEL TO CONSIDER

SASE is nothing less than a paradigm shift—an entirely new way of approaching network security, combining a cloud-native solution with security functions and a software-defined wide area network (SD-WAN). Here we discuss five aspects of SASE you should consider before committing to adoption.

Cybersecurity professionals are adjusting to new and complex networks with unique security needs; namely, those of a decentralized work environment.

WEI

cisco Premier Partner

1. SASE security is based on identity, not descriptors.

Senior Research Analyst David Holmes at Forrester, who defines SASE as "The Zero Trust Edge (ZTE) model for security and network services," says: "I am an advocate for this model for several reasons... but the primary one is this: The internet was designed without security in mind... [SASE] is a safer on-ramp to the internet for organizations' physical locations and remote workers."[4]

Specifically, SASE routes traffic through a cloud-native security stack rather than through a physical security system in a data center. Authentication is based on the user's identity rather than descriptors, such as IP addresses. Shifting security to the cloud in this way represents a fundamental improvement compared to the classic perimeter-based model that can't keep up with modern user behaviors and business requirements.

2. SASE enables consistency in security and business continuity.

The fragmented approach of using multiple point solutions to enable sufficient network security is no longer required—even as companies add new employees, devices, applications, and business use cases. As Gartner describes, SASE supports "flexible, anywhere, anytime, secure remote access at scale, even from untrusted devices."[3] In this decentralized environment, security teams can deliver consistent protection anywhere—even as the company transforms and workforces become more mobile.

3. There is an impetus for broad SASE adoption at nearly every company today.

Virtually every company today engages in remote networking of some kind, whether that's managing remote workforces or integration with partner systems. As these relationships become more common, there is an urgency among security teams to adapt as legacy models lose their efficacy.

But growing risks and opportunities for improvement aren't just concerns for remote environments. "In the future... organizations will look to put all their network traffic through these [SASE] networks," says Forrester; "that's where the security and network teams will have to work together."[4]

4. SASE is at the cutting edge, just leaving its early stages of development.

Business leaders have a growing interest in SASE, but most are only considering adoption. Even so, SASE is "being actively marketed by the vendor community, with more than a dozen SASE announcements over the past 12 months," Gartner reported in August 2020.[3]

However, many vendors are marketing SASE solutions that don't necessarily abide by core principles of SASE. Business leaders considering SASE must be sure to vet companies, identifying those with software architecture that isn't just cloud-based, but truly cloud-native and authentic.

5. There are best practices when taking your initial approach to SASE.

Although many companies approached SASE first to secure their remote workforces, the seamless and secure connections that SASE supports are desirable no matter where employees sit. As the lines blur between internal teams and those of partners—not to mention IoT devices and remote data sources—streamlined, broad network security assets are growing in appeal as well.

SASE should therefore be a complete business solution, paired with a complete departure from on-premise security architecture. In this way, companies can give all their users—no matter who they are, where they sit, or where those choose to go—a simpler way work.

TAKING YOUR FIRST STEP WITH SASE

As work becomes more distributed and networks overlap, identity must become the central means of authentication if companies are going to succeed. SASE not only accomplishes this core goal—it gives users the freedom to work effectively, and businesses the flexibility to evolve with future security challenges.

Wining SASE solutions are available today. Cisco supports an industry-leading SASE model with their Cisco Umbrella offering, for example, which features SD-WAN, Zero Trust Network Access, and other critical components to modern enterprise distributed networks.

TALK TO WEI TODAY

Talk to the network security experts at WEI today to learn how to leverage Cisco SASE to achieve greater business continuity and help your cloud workforce stay connected and secure.

Sources:

1. IDG Research commissioned by WEI, January 2021.

2. "Four Reasons Why SASE Is The Future Of Network Security." Adi Ruppin, Forbes Technology Council. Dec 16, 2020. https://www.forbes.com/sites/forbestechcouncil/2020/12/16/four-reasons-why-sase-is-the-future-of-network-security/?sh=2f1ca4992a59

3. "Top Actions From Gartner Hype Cycle for Cloud Security, 2020." Susan Moore, Gartner. August 27, 2020. https://www.gartner.com/smarterwithgartner/top-actions-from-gartner-hype-cycle-for-cloud-security-2020/

4. "Take Security To The Zero Trust Edge." David Holmes, Forrester Blog, Feb 16, 2021. https://go.forrester.com/blogs/take-security-to-the-zero-trust-edge/

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 30 years.