Networking Handbook

June 2020

SASE model aims to boost network security, performance

TechTarget

In this handbook:

SASE model preps network security for digital transformation

SHARON SHEA, SENIOR SITE EDITOR

Gartner says it's time to get sassy. Not as in being bold or brazen, but *SASE*, as in the acronym for *Secure Access Service Edge*.

Coined by the research firm in late 2019, the term *SASE* refers to a service model that aims to accommodate the needs of cloud-, mobile- and edge-reliant enterprises by creating a converged, centrally controlled fabric of cloud services and security functions.

Andrew Lerner, research vice president at Gartner, wrote in late December 2019 that SASE is "essentially a new package of technologies," including software-defined WAN, secure web gateways, cloud access security brokers, zero-trust network access and firewall as a service "as core capabilities with the ability to identify sensitive data or malware and the ability to decrypt content at line speed, with continuous monitoring of sessions for risk and trust levels."

In a nutshell, the SASE model provides secure access to enterprise data, wherever it may be located.

In this handbook:

Members of the networking and security teams jointly define and control the SASE with other key players, such as mobile and app dev teams and sys admins. As such, SASE is positioned to be a game-changer in the enterprise digital transformation landscape by pulling together cloud applications, mobile employees, and edge and IoT applications, while using identity-driven access management as its core security mechanism.

It's a nascent model, but that hasn't stopped Gartner from predicting that 40% of enterprises will have SASE adoption plans by 2024.

Because of its relative infancy, there is likely much confusion around the Secure Access Service Edge. In this guide, cloud expert Dave Shackleford outlines the service fabric convergence of SASE and how to determine its role in your enterprise. Then analyst John Fruehe discusses the cultural and architectural challenges enterprises may encounter when considering SASE adoption. Finally, Shackleford dives back in to explain the identity-centric nature of SASE and how its policies make organizations more secure.

Digital transformation is a reality facing companies of all shapes and sizes. Is the SASE model the key to putting your enterprise's digital transformation on a secure path?

In this handbook:

Get to know the elements of Secure Access Service Edge

DAVE SHACKLEFORD, PRINCIPAL CONSULTANT, VOODOO SECURITY

The use cases for cloud services continue to expand rapidly, and access scenarios are shifting. Organizations are increasing software-as-a-service use, hybrid cloud infrastructure deployments, and multi-cloud deployment and interconnectivity. Whether oriented toward end-user access to applications and services or traditional data center access to branch offices and other remote locations, the need to make traditional data centers the hub of connectivity is more of a hindrance than ever before.

To address these challenges, Gartner has named a new service model, Secure Access Service Edge, or SASE (pronounced "sassy"). This model combines different elements of cloud services and security into a unified fabric.

ELEMENTS OF SECURE ACCESS SERVICE EDGE

The Secure Access Service Edge model is oriented toward network access, control and architecture. Software-defined networking and security now include

software-defined WAN (SD-WAN). This enables interconnectivity between on-premises environments and cloud provider infrastructure through a singular backbone service or vendor tool. These networking services often provide common networking capabilities, such as routing, bandwidth shaping, and quality-of-service and core content delivery network (CDN) services, that can set priorities on specific content and service access and transmission.

Cloud security as a service is the second convergence category in SASE. This includes services provided by cloud access security brokers (CASBs) -- for example, data loss prevention, content filtering, malware detection and response, cloud provider reputation scoring and user behavior monitoring. Secure Access Service Edge also combines additional security-as-a-service offerings, including VPN replacement technologies, web application firewall (WAF) and traditional firewall filtering, and network intrusion detection and prevention, as well as remote browser isolation.

This emerging cloud networking and security category will prompt some cloud security service providers to change and update their offerings to include new features. The SASE space attempts to take advantage of the cloud brokering model associated with CASB, CDN and even identity as a service. It aims to include more networking capabilities and control, as well as combined security

services in one brokering model that could simplify the current networking and security controls stacks.

BENEFITS AND IMPLICATIONS OF SECURE ACCESS SERVICE EDGE

There are distinct opportunities that may result from Secure Access Service Edge implementation. One architectural advantage is the unification of backbone and edge services that are traditionally broken out into specific vendors and service providers.

Today, core backbone providers, including telecommunications companies, data center and colocation facilities, and core cloud service providers, such as Amazon, Microsoft and Google, are solely responsible for backbone carrier and API capabilities. Secure Access Service Edge would enable one defined backbone to be combined with edge services, like CDNs, CASBs and VPN replacement or edge networking services. A single provider could offer cloud services and internet access to end users, data center services and platforms, and IoT and other distinct devices through a combined networking and security fabric. The fabric would be jointly defined and administered by networking and security teams -- likely with input from mobile, application development and systems administration teams as well.

In this handbook:

For organizations considering Secure Access Service Edge implementation, there are some key considerations. First, decide whether a unified strategy with a single provider for numerous critical services makes sense for the business. The primary benefit would be operational simplification and a smaller list of vendors and providers. The tradeoff could be a massive single point of failure or exposure. Second, scrutinize the capabilities offered. Most SASE vendors originated as SD-WAN, CASB or VPN services and are now bolting on other capabilities through acquisitions or scrambling to develop them quickly -- sometimes with mixed results. Finally, operational and financial costs are a major factor in decision-making.

Secure Access Service Edge is a new category that likely has some significant maturing to do. If an organization already has most or all of the capabilities it needs, it should not rush into this space just yet without a compelling reason. This service fabric convergence is occurring naturally in the cloud space and will come together organically.

Why SASE adoption requires a paradigm shift

JOHN FRUEHE, INDEPENDENT ANALYST

As businesses continue to evolve and move to cloud-based models, IT departments have moved toward delivering more of their capability as a service instead of deploying fixed-function hardware.

Software-defined WAN (SD-WAN) indicated the first major networking change in this shift toward as a service. It virtualized the WAN connection control, opening that service level to other network aspects, like routing, caching, acceleration, quality of service and traffic shaping.

Delivering WAN services to branch offices through a cloud infrastructure also introduced the basis for half of the as-a-service puzzle: network as a service (NaaS). Networking capabilities that were previously delivered by physical appliances can now be provided in a virtual manner through a cloud service, like Microsoft Azure or AWS, under the NaaS moniker.

With NaaS in place, the natural evolution to a service-enabled strategy is to address security as a service -- often called SECaaS. Through SECaaS, the security components used to safeguard network traffic can also be virtualized and delivered through a cloud service. Businesses can consume this service in real

time instead of deploying proprietary hardware platforms with steep upfront capital costs and complex configuration requirements.

WHAT IS SASE?

When combined, NaaS and SECaaS create what Gartner refers to as Secure Access Service Edge (SASE). SASE is a cloud-based architecture that distributes networking and security functions to connected clients, including data centers, IoT sensors and mobile users. Businesses will undertake SASE adoption to connect their branch offices in the future, as their reliance on physical networking gives way to the virtualization and servitization of these functions.

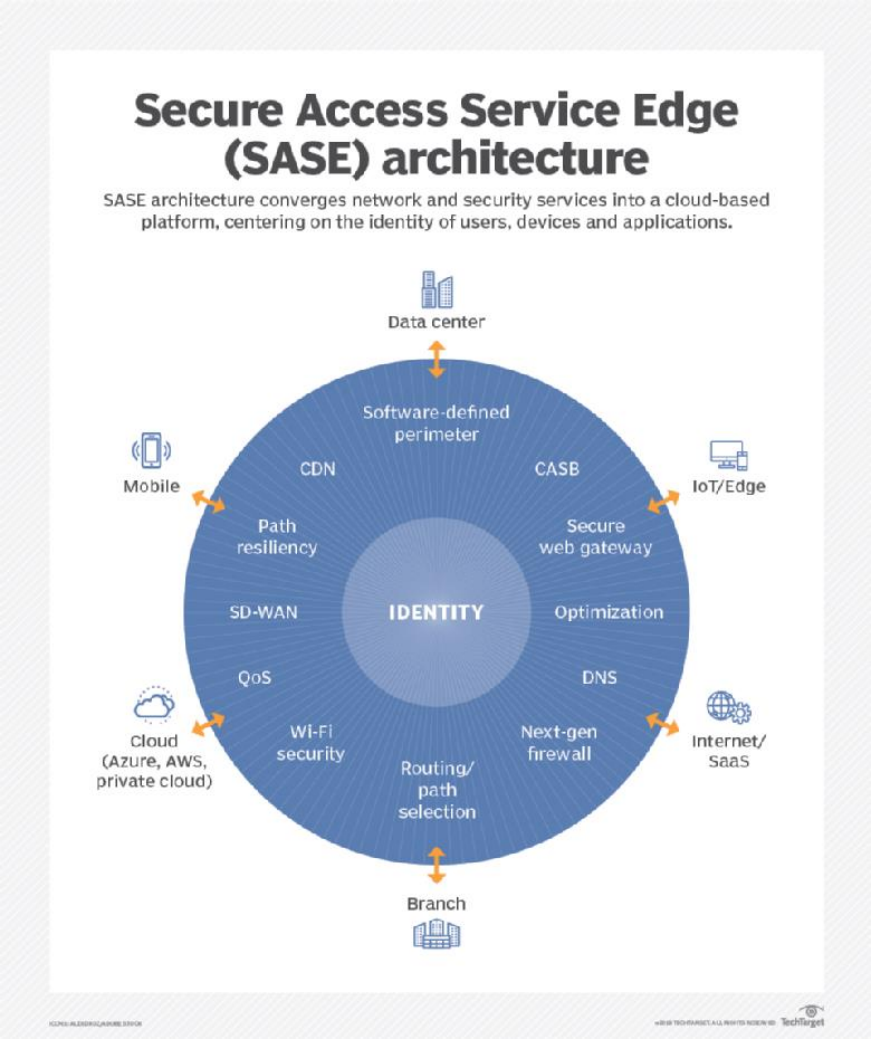
SASE adoption can be challenging, but the payoff will be huge for those companies that are able to make the move.

The key benefits of SASE include the reduction of complexity and cost, the ability to scale up and down to meet business needs, and the ability to rapidly change based on fluctuations in the business environment. The centralized policy

management still enables local enforcement, down to the system or user, and this enforcement is invisible to the branch office.

While these benefits may sound like a nirvana all businesses would clamor to achieve, IT organizations that aren't fully prepared for change may face roadblocks along the way to SASE adoption.

In this handbook:



CULTURAL CHALLENGES FOR SASE ADOPTION

The first challenge with SASE adoption is not technical but organizational. In many companies, networking and security teams are not as intertwined as they should be. Teams in these situations have probably come to a peaceful detente over the years, but a move to services can disrupt both their worlds. It can be a jarring experience that requires teams to relearn the art of cooperation.

As teams overcome this first organizational obstacle, they will also need to resolve three architectural challenges in this new SASE world.

ARCHITECTURE CHALLENGES FOR SASE ADOPTION

1. Nascent markets. The first challenge is the markets for NaaS and SECaaS are both still nascent at this point. The SASE vision is clearly a future state, and while many businesses may start their journey down that path, the road isn't fully paved yet. This expectation needs to be front and center for all adoption discussions, even if it means doing work that may not be fully used in that final state.

2. Vendor selection. The second challenge comes from the selection of SASE vendors. While a single cloud platform provider can deliver NaaS and SECaaS,

the actual underlying networking and security components might not always be optimal for either team. The goal in overcoming this obstacle is to understand which components are the most critical; these are the no-compromise components that are essential in tying everything together. Getting these components right early can keep teams' projects moving forward by not stalling progress.

3. Disparate offerings. The third major challenge is the disparate offerings from vendors. Just because a team has used a vendor for physical load-balancing devices doesn't mean the vendor will also have a service-based cloud component to use. Even if the vendor does, that doesn't mean a cloud provider will offer that component. This is an area where detailed discussions with vendors about both their capabilities and their roadmaps will pay heavy dividends as teams decide how to best move toward a service-based world.

Centralization of IT resources in the headquarters data center is an outdated strategy that creates disadvantages for organizations that aren't adept at change. The business world is increasingly moving to an on-demand model. Companies beginning their transformation toward this more flexible and agile means of operation will see the prominence of SASE increase. SASE adoption can be challenging, but the payoff will be huge for those companies that are able to make the move.

In this handbook:

SASE identity policies enhance security and access control

DAVE SHACKLEFORD, PRINCIPAL CONSULTANT, VOODOO SECURITY

Gartner defined a new cloud-based multifunction architecture service model called Secure Access Service Edge, or SASE, pronounced "sassy," in 2019. SASE offers a wide variety of services, primarily focused on software-defined network access, cloud service access management, VPN replacement and cloud access security broker services. One of the more intriguing capabilities offered with SASE is identity-driven access management, compared to traditional network-based controls and services.

SASE EXPANDS THE DEFINITION OF IDENTITY

The first major shift in the way SASE approaches access management is its definition of what constitutes an identity in the first place. While the more traditional concept of identity still applies -- users, groups and role assignments -- all edge locations and distributed WAN branches and network origins are also considered identities. In a cloud-focused enterprise, secure access decisions

should be centered around the identity of the entity at the source of the connection. This would include users, devices, branch offices, IoT devices and edge computing locations, for example.

HOW SASE INTERPRETATION OF IDENTITY AFFECTS ITS POLICIES

The identity of the users, groups, devices and services in use remains the primary element of SASE identity access policies. Interestingly, SASE identity policies are evolving to include additional relevant sources of identity context that can factor into policy decisions and application. These may include some combination of the identity's location, time of day, device security evaluation or trust validation. The sensitivity of applications and data entities are trying to access may also be considered in SASE identity policies.

These factors can help organizations develop and refine a more progressive least-privilege access strategy that enables strictly enforced access control. The promise of SASE identity policies is that organizations will be able to control interactions with resources based on more varied relevant attributes, including application access, entity identity and the sensitivity of the data being accessed.

HOW SASE FITS INTO A LARGER IDENTITY AND ACCESS EVOLUTION

A shift in the security and identity landscape has been underway for some time. Specifically, zero-trust network access and microsegmentation based on applications and identity affinity policies are evidence of this change. Historically, it has been a largely internal technology shift. However, this has now branched out to a broad access control methodology. This approach facilitates identity-based controls for entire office locations, remote users, IoT devices and more.

The SASE model looks to significantly improve upon the classic access strategies that focus on only network information that may be complex to set up and maintain. For example, complex network information might include IP addresses and ranges or network edge devices with rigid connection methods.

The identity of the users, groups, devices and services in use remains the primary element of SASE identity access policies.

This shift to policies oriented toward application, data, device and user affinity policies may streamline the creation and management of access policy. Once authenticated and authorized to access resources, a SASE service can then act as a VPN-like broker. The SASE model protects the entire entity session, regardless

of where it connects to and originates from. In keeping with the theme of zero trust, SASE systems should have flexible options to apply end-to-end encryption of sessions. Options should also layer in additional web application protection, API inspection and security assessment, content inspection for data loss prevention and any other variety of security services in a brokered access model.

HOW THE SASE MODEL MAKES ORGANIZATIONS MORE SECURE

A variety of attacks are likely to be mitigated with effective application of SASE services in the future. With strong unified policy management, more thorough validation of branch office connections, approved IoT devices, and edge services and locations can be built and maintained. This should help curtail some man-in-the-middle interception attacks, spoofing scenarios and malicious traffic.

End users can also benefit from this model. Leading SASE providers enable the secure encryption of all traffic from remote devices, regardless of location. SASE options will even apply more rigorous inspection policies based on public access, such as at airport and coffee shop networks. Depending on the identity of the user and originating device, privacy controls can be better enforced by routing traffic to points of presence in specific regions as well.

The move to building access models around identity will take time. It will also require a substantial initial effort to move away from tired access models based on IP addresses. But the ends may justify the means, considering how SASE identity policies and benefits will simultaneously make security operations more efficient and attacks more difficult for adversaries.