Security

"Hi, it's SASE!" "SASE who?"

Secure Access Service Edge is the SASE (pronounced as “sassy”) kid on the security block – but how do you make it work for your organization? Here are a few tips.

Author: Dheeraj Rawal

When the world witnessed some of the largest cyberattacks in the last two or three years – including SolarWinds, Colonial Pipeline, and more – it became loud and clear that the security landscape is evolving exponentially.

In view of the increased threat from cyberspace, companies are asking themselves whether their security solutions are still adequate. Because one thing is certain: corporate networks today are more vulnerable than ever. Soaring interconnectivity, remote accesses, Internet of Things, and edge computing create more entry points and widen the attack surface.

As if this weren’t enough, the pandemic drove users off company premises. Employees now access business apps from anywhere (homes, maybe even cafes and trains) and sometimes even via their personal devices too. All in all, IT teams are struggling to keep data and apps protected, with complexities piling up. Secure Access Service Edge (SASE) is a promising solution to master these challenges.

How it all began

Sometime in 2019, Gartner coined the term SASE, and ever since then, the acronym has turned out to be more than just a buzzword. It has taken the network security industry by storm. The reason for this is that, as more and more employees accessed corporate networks and data from different places, traditional perimeter-based network security became less relevant. This is because traditional network topologies direct network traffic through a corporate data center, where it is checked and forwarded to the respective user.

Why does it matter to businesses?

With SASE being cloud-based, the traffic backhauling process to the data center is bypassed and directly routed through the nearest point of presence. This unburdens the data center and brings one remarkable advantage for the users: if they access business apps like Microsoft 365, their user experience improves considerably thanks to the faster app response.

But this rapid response doesn’t come at the cost of security. SASE allows businesses to distribute networking and security services to endpoints. In simple terms, regardless of where the user is situated, services like URL filtering, SD-WAN, and secure web gateways are still executed. Moreover, zero-trust policies ensure that the access to data and apps is context-based.

What do businesses have to gain with this approach?

Essentially, SASE tackles the latency and security problems together by converging network and security. It offers not just speed (this is a win-win situation for businesses looking to marry network and security happily). Additionally, SASE reduces complexity and introduces more efficiency, visibility, and control over security architectures.

All these advantages bundled together make SASE a lucrative option for businesses. It is gaining ground faster than expected. SASE adoption by enterprises in 2018 was about one percent – but Gartner predicts that about 40 percent of them will develop strategies with SASE factored in by 2024.

The pandemic and the distributed workforce

As a matter of fact, the pandemic has been an accelerating force for the growth of SASE. With many of the employees working from home, the number of devices connected to the corporate networks has risen manifold.

Before the pandemic, IT departments would typically see a “distributed workforce” as a synonym for branch premises spread across the globe. But with the pandemic setting in, each of the employees working from home is a branch in themselves.

The chaos of connectivity

When the reality of the pandemic hit, businesses saw tens of thousands of employees suddenly working from home. And they wanted access to apps like Zoom and MS Teams. The most common

SASE tackles latency and security problems together by converging network and security.

The shift from traditional networking concepts to SASE is the first step in implementing real zero-trust-based models. Perimeter-based network security no longer serves the purpose of the distributed workforce and cloud workloads.

Thomas Tschersich, CSO, Deutsche Telekom

problem was network congestion. Solutions centered around SASE solved this problem effortlessly, but those relying on a traditional VPN setup had to go through considerable turmoil.

This “hyper-distributed” workforce is not going to fade away soon. On the contrary: it will become a normal way of working with companies now adopting hybrid work, and some even offering a permanent remote work option to their employees.

With SASE, companies have better visibility of network performance and can easily diagnose/troubleshoot security and performance problems. The most important factor, of course, is that CISOs don’t have to trade off security for performance and productivity if they opt for SASE.

Cyberattacks cause damages in the billions

In the wake of a growing number of attacks, cybersecurity is an overriding concern for organizations. According to a report by cybersecurity ventures, global cybercrime costs in 2015 stood at USD 3 trillion, whereas by 2025, the figure is set to reach USD 10.5 trillion.

It is expected that such trends will drive enterprises even more strongly to adopt SASE. The Gartner report on SASE convergence 2021 stressed the fact that security architecture must undergo changes so that security could be delivered through the cloud.

Similar thoughts are echoed by Deutsche Telekom CSO, Thomas Tschersich: “The shift from traditional networking concepts to SASE is the first step in implementing real zero-trust-based models. Perimeter-based network security no longer serves the purpose of the distributed workforce and cloud workloads.”

What enterprises should consider when developing their SASE strategy

Many vendors that previously offered SD-WAN solutions have started to sell SASE solutions to cater to the growing market demand. So enterprises that want to introduce SASE should use a structured catalog of requirements to evaluate their provider(s). Furthermore, they should avoid quick-fix deployments. These will just end up piling on more complexities that increase efforts and costs in the long run.

Therefore, SASE should be deployed as one cloud service, ensuring that SD-WAN and security capabilities are covered in what vendors are offering.

Enterprises should even consider a quick proof of concept before doing a fully-fledged deployment. In other words, for a successful SASE deployment, enterprises need to ask the right questions (also to themselves) to find the right vendor. Here are some of the key considerations one should account for before kickstarting one’s SASE journey:

1 Understand your users and apps

Who are your users? What are their demands? Identifying your users allows you to configure your SASE appropriately. Have you thoroughly assessed your IT environment, its use cases, the migration plan, access controls, and timelines?

2 Understand security policies

How do you ensure that you comply with General Data Protection Regulation and the California Consumer Privacy Act, which is considered the strictest privacy law in the U.S.? Does the provider’s SASE solution allow the configuration of Zero Trust Network Access (ZTNA) & Software-Defined Perimeter (SDP) policies?

3 Buy-in from all stakeholders

Do you have the commitment of all parties for removing legacy-based architecture/apps? Migrating to the cloud is a fundamental decision with importance for the entire enterprise. This usually requires a buy-in from key stakeholders in the IT and security teams, along with consultants, C-level executives, the Board, etc.

4 SASE solutions must facilitate hybrid work

As users switch from office to home and vice versa in the hybrid work model, the SASE solution should also be able to switch intelligently and without creating any hurdles for the end-user. Can the provider cover that?

5 Know how your traffic will be handled

Does the SASE solution offer global service with several points of presence? Understanding how traffic will be handled will help you to know whether performance issues might arise.

6 Check for resilience

Which service levels does the provider offer? How do they ensure availability for their service? Outages and downtimes can cause pains – make provisions for this as best as you can.

7 Look for a complete solution

What is the degree of integration of the solution? If a vendor integrates too many separate services, there is a high probability that you will have to manage all of those services with different consoles, configurations, and policies (maybe even more hardware and software too). Not only management but investigating and troubleshooting a problem during downtime could thus become difficult. Make sure you choose a unified SASE solution that is simple. Ideally, it should have a single pane of glass to manage.

8 Don’t rush into it!

SASE adoption needs to take into account the existing IT environments, current legacy systems, and business needs. You don’t have to phase out legacy systems in one go. There is a good chance that you will have to adopt SASE in bits and pieces and take an evolutionary approach. Do it incrementally: dip your toes in the water before you take a dive. Keep in mind that you might need to customize the solution. ■

Better choose an integrated approach

Going with several providers often increases the complexity of the resulting landscape – and the multi-vendor approach may not constitute a full SASE solution anyway. Choose one or two providers and carefully evaluate them on the above points. Enterprises must also gauge the vendor’s capability to innovate and adapt to market changes.

A user-friendly SASE networking and security solution delivered from the cloud should deliver several advantages. Enterprises that plan their SASE with a perspective on scalability, flexibility, visibility, simplicity, and performance pave the way for the future.

Interested in SASE? If you want to plan your next steps, read our SASE self-check white paper on our website.