GIGAOM

Image credit: Gerd Altmann from Pixabay

David S. Linthicum
Apr 21, 2021

Delivering on the Promise of SASE

A Considerations Guide to Success

Delivering on the Promise of SASE

A Considerations Guide to Success

Table of Contents

1. Summary

"It's where this world is headed and, frankly, if you just step back and think about security as an industry it is incredibly complex, overly so. This is why so many are being constantly challenged, because they have to focus on two separate disciplines, which I believe is fundamentally the wrong approach. Divorcing the two is foolish. By combining them you end up with efficiencies, operational agility, and give your network and security teams time back in their day to focus their energies on other business critical tasks." – Mike Spanbauer, Juniper Networks

Just as technology decision-makers have started to wrap their heads around the idea of a Software-Defined Wide Area Network (SD-WAN), a new reality has emerged. While SD-WANs go a long way towards keeping pace with the evolving requirements of today's digital-first enterprises, they also drive an emerging requirement to combine networking and security.

This basic concept applies equally to the networks that tie our offices to our data centers, to our multiple clouds, and to our remote users and devices. In today's cloud-based environments, you have very little control: every part of your network – the laptops your team uses, the Wi-Fi they use to connect, the applications they connect to – is outside your jurisdiction.

How, in this situation, do you keep all such elements "safe" and secure? The old, zone-based, inside/trusted versus outside/untrusted perimeter firewall paradigm no longer applies. This creates numerous challenges: the architecture of IT has shifted underneath us all, driving a fundamental change in the way we approach security and act to secure our distributed resources and users.

Increasingly, organizations are looking to deploy a Secure Access Service Edge (SASE) architecture as the solution to this challenge. This architecture combines multiple features to reduce complexity and security-related risk, helping organizations prepare for the security challenges of the next 20 years. While the principles behind SASE are sound, it is not a "one size fits all" solution: each deployment is unique and needs to be considered in a way that addresses the needs and practices of the organization concerned.

In this paper we consider what SASE is, how to deploy it, and what lessons can be learned from those already on the journey to better security in a digital-first world, across tools and processes, not least in importance: partnering with the right vendor.

2. The Need for SASE

The modern trends of digital transformation, cloud adoption, remote users and security threats create a set of challenges common to most modern enterprises. When your users are working on devices you don't control, connecting over networks you don't control, to cloud services that are also largely outside of your control, where and how do you insert the needed security?

Once upon a time, this was easy. When all of your users, servers, and data were inside a single office you could just lock the doors and place a firewall on the internet connection. Now that users, data, devices, and workloads are distributed largely outside of the data center, and not even on the corporate network, things have changed, extending the architecture from core to endpoint.

However, cloud infrastructure investment has been growing unremittingly over the past decade, accelerated by recent trends such as the increased move to remote working. This leaves security professionals with the question: how do you secure things over which you have little, or no control? The new goal is a secure and mobile workforce. SASE can help us get there: just as SD-WAN helped us address our connectivity challenges, SASE responds to our new security context, in itself and by enabling an architecture in which data is protected, wherever it may be – what we call a Zero-Trust Architecture.

SASE matters because it is the way organizations will be able to operate anywhere in the world securely and with low latency, aiding efficiency and decreasing the barriers to collaboration and communication. But more importantly, it creates a secure web, no matter where you are. It creates an internet-based architecture that enables security and control at a distance with less complexity for security professionals.

3. Defining SASE

Many organizations today see SASE as a logical step, putting security at the heart of their cloud-native strategy. So, what is it? SASE is an architecture which helps you to move towards a more secure, Zero Trust Architecture by combining a number of existing tools. There are five core characteristics of a SASE architecture, as follows:

1. **Converged network & security:** Combining policy management and availability management, to ensure secure communication in a distributed digital enterprise. The concept is built around removing silos and enabling security-related decisions to be made earlier in the design and delivery pipeline, to achieve a holistic security solution.
2. **Identity-based:** SASE is based on a set of universally-applicable network and security policies built around the identity of the communicating entity (user, device, workload, etc.) and whatever additional information can be utilized (things like security policy but also user and entity behavior analytics (UEBA) and location).
3. **Cloud-native architecture:** SASE demands a cloud-native architecture which distributes inspection and enforcement to provide flexibility, adaptability, and elastic scalability, allowing security professionals to define and defend those enterprise-wide, identity-driven policies that are central to cloud-native success.
4. **All the edges:** SASE extends to all the 'edges' including: headquarters, data centers, branch offices, cloud resources, and mobile users – on both managed and unmanaged devices.
5. **Global reach:** In order to provide the best possible experience, we need to ensure that we don't fall back into that data-center-centric trap of 'tromboning' traffic, which often leads to additional latency and increased bandwidth costs. The converged network and security platform must be available everywhere your organization might operate.

As we can see, SASE is a flexible, comprehensive, and very valuable concept which is moving network security from a set of disparate elements, to a coherent platform. As shown in Figure 1, the 'core' components of a SASE architecture are:

- **Cloud Access Security Broker (CASB)** – Monitors and manages which cloud services can be used, and how they are used.
- **Software-Defined Wide Area Network (SD-WAN)** – Provides reliable WAN connectivity, typically by aggregating multiple Internet connections.
- **Secure Web Gateway (SWG)** – Enforces security policy on all outbound traffic and protects against malicious web traffic.
- **Firewall-as-a-Service (FWaaS)** – Provides the benefits of a next-generation firewall (NGFW) without the need for an on-premises security appliance.
- **Zero-Trust Network Access (ZTNA)** – Uses source identity and the principle of *least privilege* to

minimize potential threats.

But there can be additional aspects of a SASE setup which, depending on your organization's needs and priorities, cover the spectrum of security services. Broadly speaking, these include:

- **Endpoint and user-level services** such as Unified Endpoint Management (UEM), User and Entity Behavior Analytics (UEBA), Remote Browser Isolation (RBI), virtualized applications or desktops, Mobile Device Management (MDM), and Data Loss Prevention (DLP)
- **Application-level services** such as Web Application and API Protection (WAAP), Web Application Firewall (WAF), and Offline edge computing protection
- **Connectivity-based services** such as Content Distribution Network (CDN), Network Sandbox, Wi-Fi hotspot protection, and Network Obfuscation/Dispersion

A resulting downside is that SASE's breadth and its many moving parts can sometimes be daunting, and leave organizations with the impression of a challenge that is beyond their capabilities. So, how do you address this? The reality is SASE can and should be built over time, with careful planning. In addition, the opportunity it provides to implement secure practices and policies across a distributed infrastructure is well worth the investment. We look at these points in the sections below.

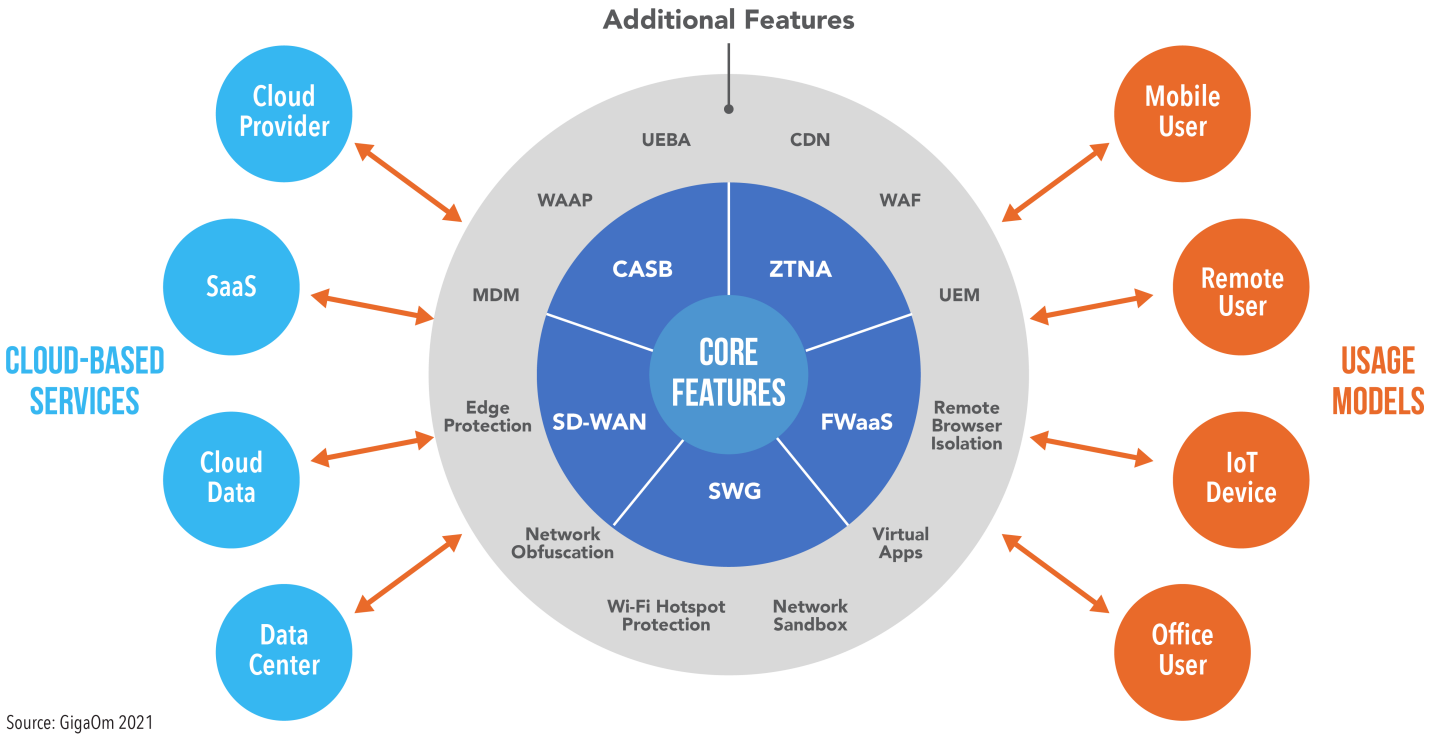

Figure 1. The Core and Additional Capabilities of SASE Solutions

4. Planning for SASE

With SASE, the goal is to connect your organization securely to its resources – whatever the resources, and wherever they are. Modern, cloud-based environments mean all of your infrastructure is distributed and you don't own most, or, indeed, any of it. So, SASE brings to the party the ability to apply security to your resources wherever they are, and manage security from a central location. To get this right, you need to plan the architecture in advance.

The main challenge for those who are looking to implement a SASE architecture is that it is a collection of different technologies combining to create a truly secure infrastructure. Even while the ultimate goal of SASE is a simplification of the role played by security professionals, the process of deploying each of these tools in turn adds to the complexity they face in the short term. This complexity makes the process of designing and creating a SASE infrastructure potentially complicated and fraught with risk: in response, organizations need to consider how they, through their own knowledge and that of partner organizations, deliver a coherent, well-built SASE architecture.

A well-built SASE architecture enables secure access to services residing on-premises and in public and private cloud environments simultaneously, while ensuring consistent security policy through a single management interface to avoid configuration mistakes and visibility gaps. The lists of core and additional capabilities above illustrates the potential scale and breadth of a full SASE architecture – this means deployment cannot be quick, and it most definitely cannot be rushed. Getting this architecture right is about the future of your organization and its long-term security.

The biggest challenge of SASE therefore, is understanding its scope, its long-term implications and anticipating how the needs of your organization, and its data, will be met by these complex components over years, not months.

This means that to implement a SASE architecture, organizations need not only to understand the technology, its demands and requirements, but also to create a transition plan that maps to their needs as they develop and evolve over time.

5. Getting SASE Done

As we have seen, embracing SASE means embracing a fundamental shift in your organization's strategic relationship with securing data, and committing to thinking differently about securing your architecture.

To create a transition plan that allows your company to grow and scale effectively with a SASE setup, you need to examine your data needs. To start this exercise off, for example, ask whether you are outwardly facing application- and customer-centric or internal user-centric as an organization. Are you needing to deliver large volumes of streaming data on a consistent basis, or are your key applications more transaction-based? And so on.

Examining your data needs will help to create your transition plan, by illustrating where your focus needs to be in the initial deployment. If content delivery is your top priority for example, the CDN aspect could be the most important part to secure first. If you want to focus on your users and insider threats, then remote browser isolation and a secure web gateway might become a priority. In other cases, application security must take precedence, making WAAP the first item on your list of day-one must-have features. Each deployment should suit the needs and priorities of your organization.

Take the time to understand your organization's needs and, first and foremost, the needs of those within your organization who are most affected by the possible changes to the security environment. Will these changes affect employees' ability to work, or the operation of customer facing applications? Understanding these ripple effects is the vital first step to be taken before any SASE deployment. To achieve this enlightenment, CISOs can identify the key stakeholders within their organization – and increasingly this task will be led by development teams within specific business units. You can work with these stakeholders to create an architecture that will support their work, not hinder it.

In addition, you can think about the manageability of the SASE deployment. In the process of converging networking and security, IT security teams do not want to add yet more management interfaces to the tool sprawl they've been trying to consolidate for years. Having to provision and manage multiple instances of security policies does nothing to reduce complexity, which is a top aim of SASE projects.

Overall, the process of deploying a SASE architecture requires a long-term investment in tools, training and cultural change. Creating a plan that acknowledges the long-term needs of the organization is a big challenge, but one that can be met by working with the right stakeholders at every stage: this includes partnering with a vendor that matches your needs with its expertise and areas of competence.

6. SASE Dos and Don’ts

In summary then, what considerations can you take into account to avoid pitfalls and assure SASE delivers on its goals? We would make the following recommendations:

Don’t bite off more than you can chew. SASE is complex, with many moving parts which don’t need to be deployed concurrently. So don’t think you have to implement everything all at once. A good place to start is with seamless, consistent policy management.

Start with a business-focused plan. As we’ve stated above, the key is to create a transition plan that takes into account the current needs of your organization and the needs of key stakeholders going forward, including the operational people on the ground who will have to deliver on the strategy. This means that when you are ready to engage with a vendor, you can select the right one for you.

Actively seek vendor alignment. Map your needs now and in the future onto the current offering and roadmap of the vendors you are considering. Is your vendor able to meet you where you are? Will they be able to support your needs at each stage of the journey? This early analysis allows you to start right away and then grow with the support of the right vendor, who will understand your changing needs.

As a final point, note that the architecture of secure networks has already shifted significantly over the last few years, with added acceleration in recent times. This has fundamentally changed the direction of the market – and the ultimate destination is the widespread adoption of Zero Trust Architecture. This means that everything we used to know as true in terms of securing our networks will change – and is changing already. Understand that when you commit to SASE, you are committing to a secure future, and all the change and challenge that entails.

7. Conclusion

The world has changed – the networks, devices and applications organizations are using are out of their control. SASE is a fleet of tools that, when properly combined, secures your data, users and customers, wherever they are situated.

This innovation increases the complexity of deployment significantly. Adopting a SASE architecture is not something that can, or should, happen quickly. As we have recommended, it requires careful planning and steady deployment, starting with the areas of highest risk and value for your organization.

A stepwise approach, starting with policy management, will enable you to start on the right foot. To enable this, it is vital to select a vendor that understands your needs and can join you on the journey to develop the right SASE deployment for your organization – matching the needs of your key stakeholders and customers as you grow and develop.

SASE is a journey – and it's a marathon, not a sprint. The ultimate destination of this journey is a network that is more secure, faster and easier to manage, built around a Zero Trust Architecture. This is a process, and it is worth the investment.

8. About David Linthicum

David Linthicum is a CTO and internationally renowned thought leader in cloud computing. David has spent the last 25 years leading, showing, and teaching large global enterprise organizations across all industries how to use technology resources more productively and constantly innovate.

David has been a CTO five times for both public and private companies, and a CEO two times in the last 25 years. David has published 13 books on computing and his thought leadership has appeared in Wall Street Journal, NPR, Forbes, InfoWorld and Lynda.com. He has expanded the vision of both startups and established corporations as to what is possible and achievable.

All of David's opinions are his own.

9. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

10. Copyright