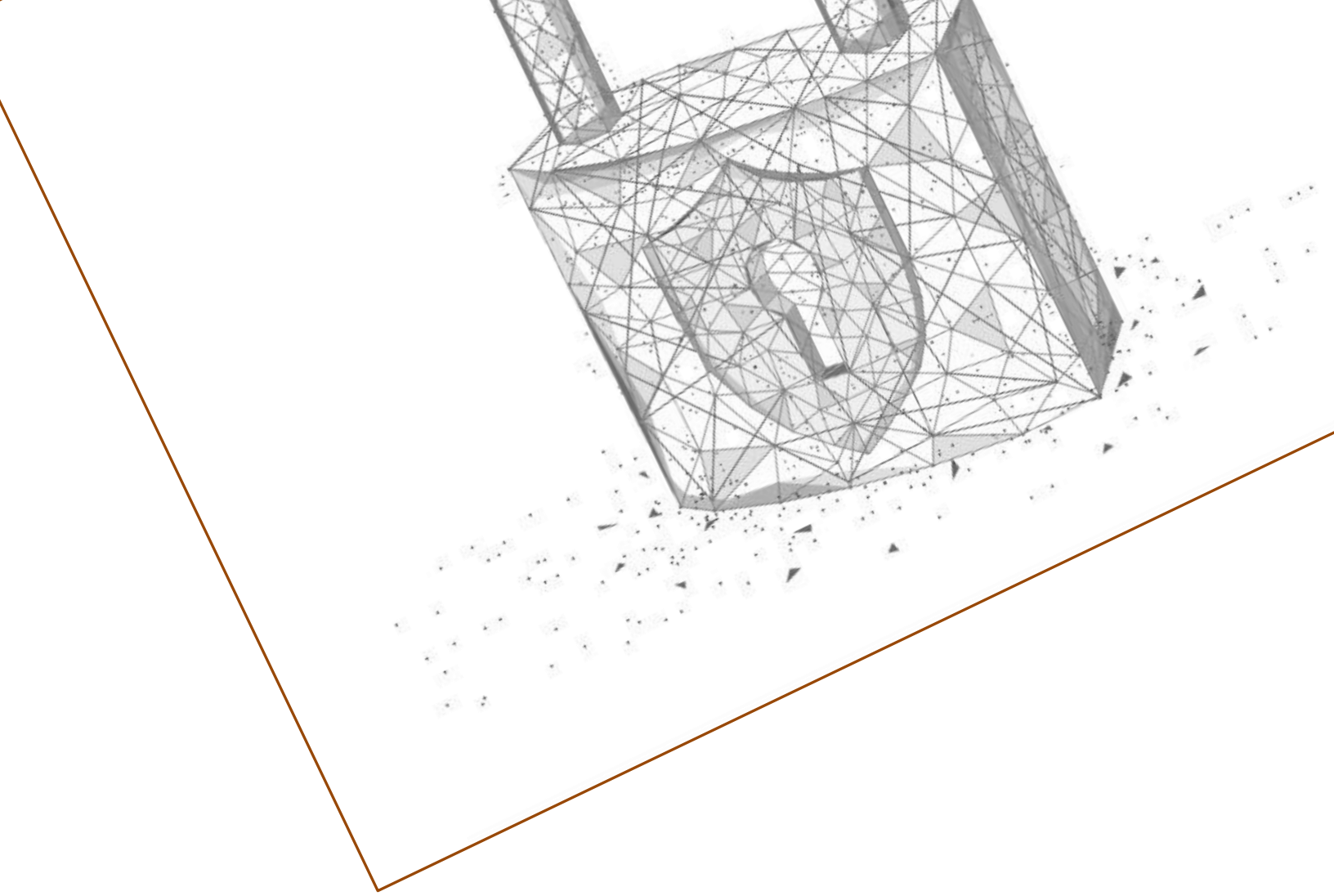


SASE (SECURE ACCESS SERVICE EDGE) PLANNING AND DESIGN GUIDE

WHITEPAPER

Document Date: October 2021
Author: Mauricio Sanchez | Research Director

Dell'Oro Group

Web: https://www.delloro.com

Executive Summary

Enterprise networks are at an inflection point. Three trends that the COVID-19 pandemic accelerated are driving the current moment of change: applications have shifted to the cloud, remote work has increased, and the quality of the digital experience has assumed greater importance. Enterprises realize that legacy networks and security architectures are inadequate, and are unable to provide the necessary security and performance in a user and application environment that has become highly distributed, interactive, and mobile across the Internet.

As a result, enterprises are thinking differently about networking and security. Instead of considering them as separate toolsets to be deployed once and infrequently changed, the problem and solution space is conceptualized along a continuum in the emerging view. Hence, the focus is now on developing a converged platform of connectivity and security services. Furthermore, the need to provision and deliver new services in a matter of hours, rather than in weeks or months, holds as much priority as the ability to reduce the total cost of ownership (TCO).

The vendor community has responded with a new architecture called secure access service edge (SASE) that merges networking and security into a cloud-based service platform that is adaptable, pervasive, and integrated.

Dell'Oro Group previously published a white paper "Enterprise Networks at an Inflection Point: The Motivations for SASE"[1], we described the motivations behind SASE (pronounced "sassy"). In this second paper, whose audience is the IT architect and the operations team, we delve deeper into SASE's technical architecture, the vendor landscape, and emerging areas of vendor differentiation, and we compare and contrast do-it-yourself (DIY) versus a fully managed offering. We close by reviewing critical considerations in selecting a managed SASE service provider.

[1] White paper - Enterprise Networks at an Inflection Point: The Motivations for SASE
https://www.aryaka.com/docs/enterprise-networks-sase-hybrid-workplaces.pdf

Table of Contents

SASE Architecture and Components

In our first paper, titled "Enterprise Networks at an Inflection Point: The Motivations for SASE," we delved into the driving forces behind SASE. We highly suggest reading that first paper before continuing further.

The consensus among leading IT architects and consultants is that enterprises need to embrace a cloud- and mobile-first IT strategy to best address the three accelerating enterprise trends (shift to the cloud, increase in remote work, and focus on digital experience). This shift in strategy has also changed the thinking about connectivity technologies, such as SD-WAN, and network security technologies, such as Secure Web Gateway (SWGs). Instead of regarding them as separate network and security tools to be selected and managed, in the current view, the problem and solution space is viewed as a continuum. Hence, the focus is on developing an integrated platform of connectivity and security services.

SASE is a service-centric, cloud-based solution that provides network connectivity and enforces security between users, devices, and applications. SASEs utilize centrally-controlled, Internet-based networks with built-in advanced networking and security-processing capabilities. By addressing the shortcomings of past network and security architectures and improving recent solutions—in particular, SD-WAN and cloud-based SWGs—SASE brings networking and security into a unified service offering to increase the network's scalability, agility, and security, while reducing overall total cost of ownership (Figure 1).

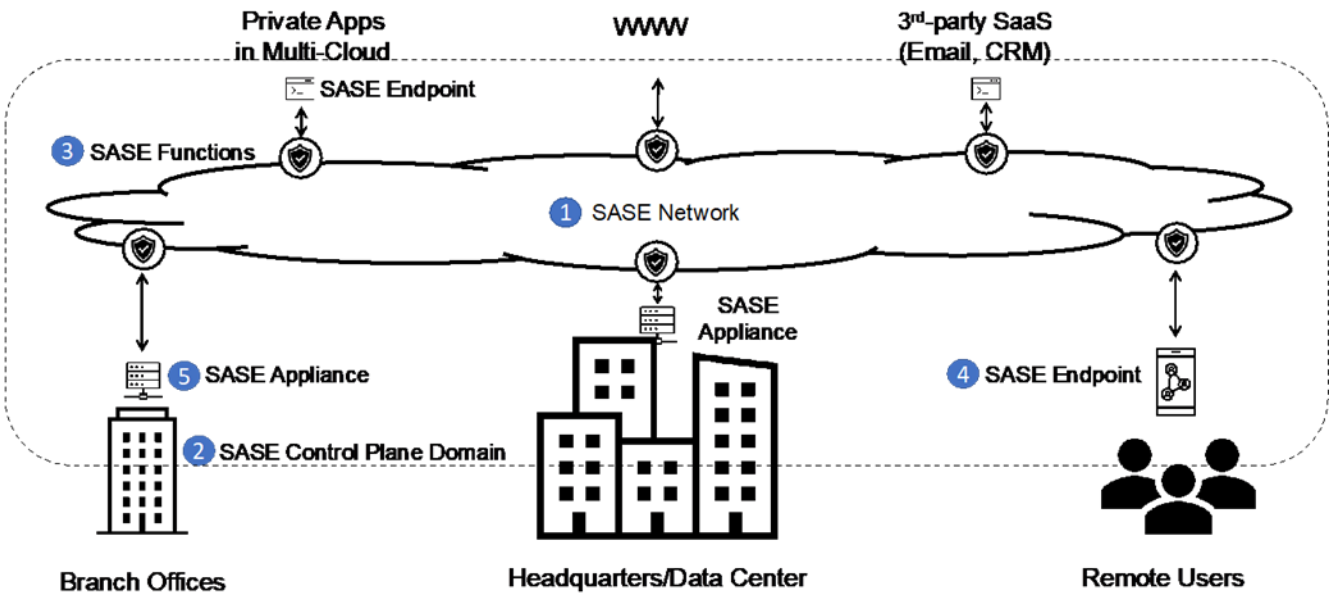


Figure 1 SASE Architecture

As an emerging technology, the definition of SASE is still settling, and inevitable differences in opinion exist. Some in the community characterize SASE as consisting of just cloud-based security services. We believe this view is too limiting and unfairly undercuts the role that networking technologies need to play. The shift toward cloud-based network architectures that rely on general-purpose Internet connections and multi-cloud deployments does not simplify enterprise IT networking. On the contrary, it makes it more complicated. Hence, we believe that WAN technologies that help manage the increased complexity of modern networks, like SD-WAN, are fundamental to the SASE equation.

With SASE rooted in SD-WAN and cloud-based SWG precursors, it shares the same architectural underpinnings and has similar components. SASE consists of five components: the network, control plane software, functions, endpoints, and appliances.

SASE Network

The SASE network is at the heart of the SASE architecture and is designed to connect all SASE endpoints and appliances, and bridge their connectivity to the Internet. It is controlled and managed by the central SASE control plane software. The SASE network lives on the Internet and leverages the ubiquity of the Internet to provide last-mile connectivity to all connected assets. Within the SASE network live the SASE functions to route and secure traffic. Legacy Wide Area Network (WAN) and Virtual Private Network (VPN) are Outmoded in the Agile, Anywhere, and Always Available Era.

SASE Control Plane Software

The SASE control plane software is the brain of a SASE solution. It can set network and security policy at a granular level and secure and direct network traffic by enforcing policies. Key features and capabilities of the SASE control plane software include:

- The ability to set network and security policy at a granular level, and secure and direct network traffic by enforcing policies.
- The option to base network and security policy on user identity, device state, time of day, user/device location, bandwidth, latency, destination, or application. This provides fine-grained security control and increases the efficiency, performance, and security of individual users and applications that traverse the SASE network.
- The ability to deploy and manage network and security services delivered to SASE endpoints, either as a function running on the SASE endpoint or through centrally-delivered, cloud-based, software-based functions.
- Ownership and management by the SASE vendor as a cloud-based, multi-tenant service offering with sufficient administrative control provided to the vendor's customers to manage an instance, that is, the enterprise’s SASE instance.
- The ability to treat multiple WAN connections as a pool of bandwidth resources and dynamically share these resources based on defined criteria, such as cost, performance, and bandwidth.
- Optionally, allows the integration of private MPLS, non-MPLS private, and public Internet connections to create a hybrid network. This integration makes the best use of MPLS security and less-expensive Internet bandwidth based on user and application needs.
- Optionally, integrates with local area network (LAN) access control solutions to enforce network and security policy on the enterprise LAN wired and wireless network edge.
- Optionally, integrates with web application firewalls (WAF) to enforce network and security policy on the application edge.

SASE Functions

Similar to SD-WAN and cloud-based SWGs, SASE leverages Network Function Virtualization (NFV) to run Virtual Network Function (VNFs) in a distributed fashion, nominally in the cloud. VNFs perform either a network function or a security function.

Networking functions include those associated with SD-WAN, and more, such as bandwidth optimization, caching, content delivery network (CDN) services, cost optimization, deduplication, load balancing, path selection and resiliency, quality of service (QoS), routing, and traffic shaping.

Security functions include secure proxying (traditional SWG), cloud application security broker (CASB), data leakage protection (DLP), zero-trust network architecture (ZTNA), firewall as a service, and remote browser isolation (RBI).

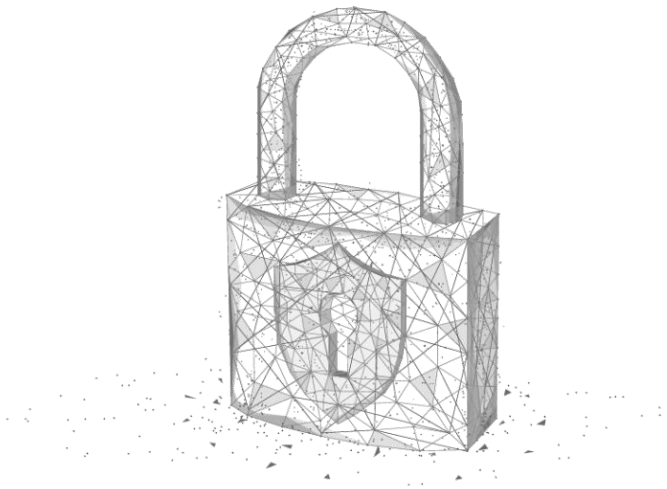
SASE Endpoints

SASE endpoints include all the users, devices, and applications utilizing the secure network connectivity services provided by the SASE solution.

SASE endpoints include logic by which to connect a SASE network. It may be as simple as using web proxy configuration. More typically, the SASE endpoint logic consists of a software agent provided by the SASE vendor. Software agents allow richer interactions with users, devices, and applications. For example, on a device, the software agent can participate in the authentication to the SASE network by providing the user identity and device state, requesting specific services of the SASE network, and encrypting user traffic via SSL/IPsec between the user and SASE network.

SASE Appliances

Under the control of the SASE control plane software, SASE appliances aggregate traffic from users, devices, and applications that cannot connect directly to a SASE network. For example, a SASE appliance may be deployed to provide secure network connectivity to all branch office users, devices, and applications. Like SD-WAN solutions, the three common forms of SASE appliances are access routers, firewalls, and dedicated SASE appliances.



SASE Vendor Landscape and Emerging Differentiators

A vendor typically enters the SASE market with a pedigree as a networking vendor in SD-WAN technologies or as a security vendor in SWG and related security technologies. While we do not believe that every vendor needs all SASE technology components to be successful in the market, several factors may play into their success:

- **Ability to engage the customer in their journey:** We see the enterprise IT security, network, and application teams interested in SASE. In most instances, it is a collaboration between the security and network teams due to many enterprises already considering a security transformation (such as moving to cloud-based SWG) or a network transformation (such as moving to SD-WAN), both of which are fundamental aspects of SASE.

> *Many enterprises are taking an incremental approach toward SASE by first completing either the security or network transformation, and then undertaking the other transformation to manage overall change and risk. We note that SASE does not require that enterprises undertake both transformations concurrently, or complete the security transformation first. For some, the need for network transformation will be more significant, and for those, the path towards SASE will start with networking.*
>
> *Vendors who are flexible and can help their customers irrespective of their starting point and take them through both the network and security transformation will stand out from those who cannot.*

- **Security technology leadership:** Providing robust security is a fundamental value proposition of SASE. Vendors that have superior security technologies or in-house threat intelligence teams will be able to differentiate better.
- **Adequate networking technology:** While some vendors may choose to overlook or minimize the role of networking within SASE, the ability to reliably get traffic from point A to point B remains paramount. Vendors who can demonstrate this to the enterprise networking teams will stand out.
- **Ample cloud service experience:** Fundamentally, a SASE vendor is not in the appliance business, but, rather, in the cloud services business—in particular, the networking and security services hosted in the SASE network. Vendors will need to invest in robust cloud infrastructure and employ strong operational acumen to ensure satisfied customers.
- **Sufficient financial resources:** Vendors will need adequate financial resources to fund SASE solutions and position their businesses to sell their solutions.

The number of vendors marketing SASE has grown to 30 in the two years since the term SASE was first coined. This indicates a low barrier to entry, and we expect an eventual thinning of the vendor landscape, though this will take several years to occur.

Though still a developing market, clear lines of differentiation between SASE vendors have begun to emerge. We discuss five differentiators in the following sections.

Unified versus Disaggregated Implementation

A primary way SASE vendors differentiate themselves is how they implement their solutions, varying from unified to disaggregated.

In the unified implementation, all network and security technologies are offered as a single, integrated platform, whereby just one policy repository spans both the network and security policy. Moreover, all SASE components typically are offered and required to be obtained from a single vendor. This integrated, single-vendor approach usually provides greater ease of use and improved troubleshooting. However, the tradeoff is that it is generally more difficult to integrate other third-party vendor technologies due to the monolithic implementation.

Conversely, the disaggregated implementation consists of separate network and security technologies that have been integrated into a complete SASE solution. As a result, the network and security technologies may come from the same or different SASE vendors. Usually, disaggregated implementations consist of multiple policy repositories–one for each network or security service–and may require manual and sometimes difficult policy reconciliation by administrators that the unified implementations avoid. However, it is generally more straightforward to integrate additional third-party network and security technologies due to the disaggregated nature of implementation.

It is too early to pick the implementation approach that will win in the market. However, early indications point to a co-existence in the market for the next several years, considering the variety of enterprise IT teams making purchasing decisions. Enterprises that have specialized networking and IT teams tend to prefer the multi-vendor, disaggregated SASE approach. This facilitates a best-of-breed SASE deployment that consists of the network and security IT teams' preferred technology vendors. On the other hand, enterprises that lack specialized networking and security IT teams tend to accept single-vendor, unified implementations. The greater simplicity of the unified implementation and only needing to deal with a single vendor, rather than multiple vendors, holds great appeal.

SASE Network: Cloud Service Provider vs. CDN/Edge vs. Custom

Underlying the SASE network is a backbone network. SASE vendors differ in their approach to, and the attributes of, their backbone network. SASE vendors are using one or more of three techniques to implement their SASE network:

1. On top of one or more public cloud service provider(s) (CSP), such as Amazon Web Services, Microsoft Azure, or Google Cloud
2. On top of public content delivery networks (CDN) and edge computing providers
3. Building out a custom cloud network

Public Cloud Service Provider Approach

Global, public CSPs, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, are obvious choices to host a SASE network. The scale of a public CSP's compute, storage, and networking is unmatched.

- **Many Points of Presence**: Public CSPs offer many network entry and exit points spread worldwide that simplify getting traffic into a CSP network.
- **Strong likelihood of application locality**: In some instances, traffic may not even need to exit if the destination application or service is hosted in the same CSP.
- **Economies of scale**: Public CSPs offer opportunities to leverage their massive, elastic compute pools to process traffic and enforce network and security policies.

However, there are various pitfalls when implementing SASE networks in public CSPs:

- **CSPs are oriented to host applications and data, not the network**: The design intention of the majority of public CSPs is to host customer applications and their data. As such, the emphasis is to be a traffic destination, not an intermediate pathway. Moreover, financial hurdles may arise due to the data egress many public CSPs charge as data exits their networks.
- **Black box challenge**: Public CSPs have invested heavily in network capacity tools that facilitate the cloud's abstraction of elasticity. However, these tools are not available to customers, or they are available only in simplified form.
- **Inability to own destiny**: The historical focus of public CSPs has been to maximize the profitability of their total customer workload. This, in turn, leads to design and implementation choices that generally favor the CSP rather than individual customers.

Content Delivery Network (CDN) / Edge Compute Approach

Optimizing Internet-based application performance began over twenty years ago with the first wave of CDN services and, more recently, edge computing providers. A CDN implements a performance-focused network and uses the Internet as the underlying transport. Unlike the best-effort interactions among Tier 1 and Tier 2 network providers composing the general-purpose Internet, a CDN inserts its management and coordination mechanisms to use to improve the Internet selectively. This achieves better results. Edge compute providers extend the concept of CDNs by instantiating distributed compute pools for use by customer applications.

The intense focus on Internet performance bodes well for a SASE network. The end goal of CDNs and edge computing to be the pathway for traffic and not the destination is precisely aligned with the intentions of a SASE network. However, the same black box challenge and inability to own destiny challenges apply. While CDN and edge computing providers are better positioned to address SASE network requirements, they still require effort on behalf of the SASE vendor to adopt.

Custom Approach

Just as CIOs make buy-versus-build decisions for the technology in their enterprises, SASE vendors also have the same choice to make. Vendors can use a CSP or CDN for their SASE network and these two options are analogous to buying technology. The alternative is to build the technology by investing in a custom cloud network.

The advantages offered by the custom cloud approach include:

- **Controlling own destiny:** Being able to make all-important design and implementation decisions, both now and in the future, ensures that a SASE vendor owns their destiny.
- **Overcoming the black box challenge:** Though a SASE vendor may not own and control every last element in their cloud network, they do own enough to avoid falling into the black box trap. The following are essential control points that the custom approach affords the SASE vendor:
  - Coverage: Where to instantiate points of presence
  - Breadth: Ability to ensure that every service is available at every data center
  - Scaling: When to add data center capacity to support a scale-out expansion
  - Capacity: Allocation of network bandwidth per data center
  - Performance: Where to instrument and tune the network to ensure end-to-end visibility and control of latency and roundtrip-times
  - Compliance: Where to place traffic controls to keep traffic in defined zones to comply with government regulations

Though a custom approach has substantial advantages, this option also carries two significant hazards:

- **Skillset and experienced staff**: Having the optimal skill set and team to design, build, and operate a custom cloud is critical. There is no opportunity for trial and error.
- **Upfront and ongoing cost**: A custom cloud means a SASE vendor is alone financially and requires deep pockets. Not only are there up-front costs to open a custom cloud, but ongoing costs will be incurred to expand or refresh.

Irrespective of how the backbone network is implemented, a common goal of all SASE vendors is to provide many points of presence (POPs) on the Internet. With the Internet servicing the last mile between the SASE network and endpoints, SASE vendors aim to reduce the number of public Internet hops for performance and security reasons. SASE vendors may also choose to differentiate by instantiating SASE functions at each POP. Doing so generally improves the performance of the SASE network by virtue of the networking and security decisions being made close to where the traffic originated, rather than being backhauled deeper into the SASE network.

Diversity of Services

With a primary tenet of SASE being the delivery of networking and security as a cloud service, SASE vendors are rapidly innovating and delivering a growing diversity of SASE functions—the features and capabilities—on top of their SASE networks. As a result, the breadth and depth of their SASE functions are a clear point of differentiation between vendors.

The Metro Ethernet Forum (MEF) in 2020 began work on standardizing SASE and, in their MEF SASE Services Framework whitepaper, published a comprehensive set of SASE functions that demonstrates the diversity of service possibilities (Figure 2).

Networking Functions	Security Functions
Routing	Firewall
Path Selection	Threat prevention/detection
QoS	Cloud app discovery
VPN	UEBA/fraud
Cost optimization	DNS protection
Bandwidth optimization	Sensitive data discovery
Deduplication	Obfuscation/privacy
SaaS acceleration	WAF/WAAP
Traffic shaping	Remote browser isolation
Latency optimization	Wifi protection
Caching	SWG
CDN	DLP
Path resiliency	SDP/ZTNA
Redundancy	Network encryption/decryption
Geo restrictions	CASB

Figure 2: Example SASE Networking and Security Functions (reproduced with permission of MEF Forum)

Digital Experience Monitoring and Control

Network and application architects have for many years relied on network and application performance management solutions. These solutions rely on instrumenting networks and applications to provide a real-time view into low-level metrics, such as latency, jitter, and packet loss for networking, along with CPU usage, disk usage, and uptime for applications.

While these low-level metrics are helpful in many instances, they are not usually suitable for describing and understanding users' digital experiences. That is, traditional low-level metrics are in the inside-out perspective on IT performance, but are poor at providing the outside-in realities of what users are experiencing. For example, users may be seeing poor video or slow applications, but these symptoms do not always manifest themselves clearly in the traditional inside-out metrics.

New performance innovations have led to digital experience monitoring (DEM) solutions in the last several years. DEM solutions provide a user-centric view of IT infrastructure performance, assist in helping root cause performance issues, and help identify remediation actions. Underlying DEM solutions are a variety of technologies that in concert help build the big picture, such as synthetic monitoring for application and network path analysis, endpoint agents to monitor user's experience, Javascript injection for browser telemetry, and the same traditional low-level network and performance metrics used by classical network and application management solutions.

Like SASE, DEM is generating great industry interest, and there is a burgeoning set of DEM vendors. While it is too early to tell the direction the DEM vendor ecosystem will take, what is clear is that SASE vendors are embracing DEM as a differentiating feature of their solutions. The architectural requirements for DEM mesh

nicely into the SASE architecture. The SASE network, appliances, and endpoints are all suitable elements to instrument for DEM purposes. In addition, the SASE control plane is a perfect spot to bring DEM insights together.

Some SASE vendors are further ahead and are beginning to introduce artificial intelligence technologies into their DEM and SASE technology base, which opens a new set of possibilities whereby the IT infrastructure does not identify user-centric experience issues, but automatically remediates the problem in real-time.

From DIY to Fully-Managed SASE

Similar to other network and security technologies, SASE can be purchased, deployed, and managed across a spectrum ranging from self-managed (also commonly referred to as do-it-yourself) to fully managed.

In the self-managed or do-it-yourself (DIY) approach, enterprises take complete responsibility for their SASE solution's entire IT lifecycle—its design, selection, deployment, management, and disposition. SASE technology vendors and outside consultants may play a peripheral support role, but all heavy lifting falls on the enterprise IT team.

In contrast, an enterprise delegates the SASE IT lifecycle to an outside provider in the fully-managed approach. The service provider bears the contractual responsibility to achieve agreed-upon service metrics, such as uptime, throughput, latency, average threat detection time, or average threat response time.

In between self-managed and fully-managed is the hybrid approach. In this third approach, an enterprise collaborates with their service provider and shares the SASE IT lifecycle responsibilities. For example, the enterprise team and service provider work together to create the network and applications policies. But then the service provider alone owns the tactical execution and the responsibility for achieving services metrics. In addition, the service provider may provide the enterprise a dashboard to see the real-time status of the network and service as the entry point by which to make change requests to the service provider. This approach balances the ultimate transparency and control of DIY with the full-service nature of the managed approach.

In the following sections, we delve deeper into DIY versus fully-managed SASE and discuss the considerations when choosing a managed service provider.

Considerations for DIY versus Fully-Managed SASE

As enterprises begin to embrace SASE as part of a cloud- and mobile-first IT strategy, they must make the critical decision: go it alone in the DIY approach, bring in an outside provider with a full-service offering, or go in between with a hybrid model? The decision cannot be taken lightly.

There is great diversity in enterprise teams that typically aligns with the size of the enterprise. For example, larger enterprises generally have evolved to have more extensive and more specialized IT teams. As a result, individual members may know a considerable amount about a single topic. Conversely, smaller enterprises typically have IT teams that are smaller in size and consist of generalists. Each individual member knows something about many topics.

Regardless of whether an enterprise is large or small, or consists of specialists or generalists, enterprise teams need to ask the following questions across six categories to help decide whether DIY or fully-managed SASE, or somewhere in between, is the best fit.

Skillset Depth and Breadth

- Do we have a solid grasp of how a cloud- and mobile-first IT strategy impacts the network and security architectures?
- Do we understand the steps necessary in a successful network and security transformation?
- Do we know the implications of public cloud infrastructure versus SaaS?

The questions above are meant to drive discussion within IT teams on whether they understand the network and security ramifications of the cloud- and mobile-first IT strategy. Those who have many years of success with the traditional hub-and-spoke model must be especially careful. They cannot be overconfident and believe that past success with the hub-and-spoke approach guarantees future success. SASE is a journey of network and security transformation away from the hub-and-spoke model in service of the cloud- and mobile-first IT strategy.

While the number of IT professionals that have successfully undertaken network and security transformations is increasing, they are still in short supply. IT teams with such individuals on staff have a great advantage and are better positioned to consider a DIY approach. But the many teams that do not include such individuals may want to consider the service provider path, or at least lean heavily on their consulting capabilities.

Security

- Does the team have the appropriate security skillset? How mature are the security processes in the organization?
- Does the team understand the security ramifications of public SaaS applications?
- Is the team versed in the latest technologies to secure SaaS applications (ZTNA/CASB)?
- Can the team design and monitor a threat detection solution?
- Does the team know how to respond when a threat is detected?

Delivering strong network security is paramount in the implementation of SASE. The long-standing rule of thumb in cybersecurity is that a strong security posture can only be provided by the right combination of people, processes, and technology. Unfortunately, in the security marketplace, people and processes often get overshadowed by the technology discussion—vendors are out to sell technology, after all—but it is critically important that IT teams consider all three.

When it comes to people and processes, enterprise teams need to evaluate their legacy and maturity. For example, if an IT team treats security as a part-time job on top of an existing role, they are unlikely to achieve the level of security they desire. Likewise, if security is treated as an ad-hoc exercise without the constant rigor it demands, again, achieving the desired security posture is doubtful.

Beyond enterprises asking themselves whether they have a strong security culture, they should understand their ability to leverage and adapt to new security technologies. Innovation in the security world runs at a blazingly fast clip, and SASE vendors are proving adept at incorporating new technologies into their solutions. However, without the right people and processes to take advantage of the latest security technologies, the total value of the technology will not be realized.

Like the questions of strategic breadth and depth, IT teams that determine they lack the people and knowledge wherewithal may want to consider the outside expertise available from service providers.

Network

- Can the team design and manage an SD-WAN deployment?
- Does the team understand how to tune cloud applications for maximum performance?
- Can the team handle critical applications that span multiple regions and communication service providers?

Although many SASE vendors focus solely on its security value, the networking facet cannot be overlooked. Getting network traffic reliably and efficiently from point A to point B is crucial in SASE, as is securing the traffic. Therefore, enterprise IT teams need to take stock of their network knowledge and operational capabilities to ensure that the stability and reliability of the network are not jeopardized.

As with security, enterprise teams that are unsure about their ability to craft a contemporary SD-WAN style solution may benefit from the experience and knowledge of a service provider.

Time to Value

- Does managing networking and security provide the best value to the enterprise?
- How quickly can the team onboard enterprise teams and users?
- How often can new features be deployed?

Leading enterprise IT teams run their organizations like businesses. The IT solutions are their products, and the internal enterprise divisions and businesses they service are their clients. Similar to a well-managed business, they focus on providing their customers the best product and service at the lowest investment cost. As a result, they are constantly evaluating which IT products and services they should invest in, and whether to build the solution internally, (a DIY solution), or buy externally, for example, from a service provider.

The questions above are meant to generate IT team discussion about how they should approach their investment decisions. Perhaps the value of managing networking and security in the converged form of SASE is not the best value for the enterprise. If so, outsourcing to an external provider may free up the IT team to focus on more important matters. Likewise, a cost-benefit analysis may show that the level of investment in a DIY SASE would be too high compared to a fully-managed SASE to support the desired schedules for both initial and future feature deployments.

Service Level Agreements (SLAs)

- Does the team have the resourcing required for 24/7/365 coverage?
- How capable is the team of achieving desired uptime? Globally?
- Is the team's time to problem resolution acceptable?

SLAs are agreements based on quantitative metrics that facilitate the grading in an IT service. A successfully executing IT service is generally achieving and exceeding its SLA metrics. For example, if an IT service supposed to deliver five-nines uptime that equates to being fully operational 99.999% of the time—an average of fewer than six minutes of downtime per year.

Our intent is not to describe every SLA metric applicable to SASE, but to highlight that IT teams need to determine which are relevant to them and use the metrics to guide their implementation decision. For example, if an enterprise expects SASE to function 24/7/365 anywhere globally, the IT team will need to determine whether they have the proper staffing in the appropriate locations to support the mandate. They may quickly find out they do not, and to become capable is cost-prohibitive. IT teams may find that service providers can hit more stringent SLAs at a lower cost.

Vendor Management

- Is the team knowledgeable and capable of managing multiple technology vendors?
- Can the team handle working with multiple communication providers throughout the world?

We previously described that SASE implementations exist in two primary flavors, unified and disaggregated. The disaggregated approach generally entails a multi-vendor solution, which depends on the IT team's ability and willingness to manage multiple vendors. It may be easier and desirable to bring in outside help. Good service providers are adept at handling various vendors and driving diligent resolution when problems inevitably arise.

Even when an enterprise chooses the unified SASE approach, which means they usually work with a single SASE technology vendor, they may still need to manage multiple vendors. For example, more extensive, global SASE deployments may need to rely on numerous last-mile communication service providers scattered throughout the world. Every one of these last-mile communication service providers is yet another vendor that needs to be selected, designed, deployed, and maintained. Some enterprises may balk at taking on the work for several reasons, whether resourcing, cost, or skillset. Instead, they may decide to rely on the SASE service provider to manage all last-mile connectivity contracts.

The six areas of consideration for DIY versus fully-managed SASE may lead many enterprises to elect to use a managed SASE service provider. But this leads to another question: how to assess prospective SASE service providers.

Considerations in Choosing a SASE Service Provider

Due to the great interest in SASE, there is a constant stream of new service providers touting managed SASE offerings. But similar to SASE vendors, not all providers are alike. They come with their own areas of strength and weakness that enterprises need to pass judgment on. In this section, we discuss six considerations in choosing SASE service providers.

Extensive Networking and Security Domain Expertise

Similar to SASE technology vendors, SASE service providers are entering the market with a networking or security pedigree. As a result, they possess a deep understanding of either networking or security. But with SASE and its convergence of networking and security still new, only a minority understand both domains well. Therefore, IT teams should not expect that their existing network or security service provider is automatically a good fit to provide SASE services.

While IT teams should leverage the providers they may already have relationships with, they should ensure that any prospective provider can speak to both networking and security, and demonstrate past success in both domains.

Key questions to ask prospective providers include:

- How long have you been providing managed SASE services?
- What are the success stories for customers that looked like us and embraced SASE?
- How many years have you been providing managed network services? Were they customers similar to enterprises like ours?
- What networking certifications does your staff have? What is the average length of tenure?
- How many years have you been providing managed security services?
- What security certifications does your staff have? What is the average length of tenure?
- What experience do you have in undertaking networking transformations (legacy networking to SD-WAN)?
- What experience do you have with cloud-delivered security services such as cloud SWGs?
- What is your experience with WAN/MPLS technologies?
- How do you suggest that our current network and security architecture change?

Technology Options

We previously noted there are now over 30 technology vendors marketing SASE technology solutions and five emerging areas of differentiation between the technology vendors. This means that enterprises must be thoughtful about the SASE technology they embrace through their service provider, and ensure they have picked the one that best fits their needs.

On the other hand, SASE providers need to provide enterprise choice by offering multiple SASE technology vendors, but not to the detriment of maintaining a deep understanding of a vendor's technology or strong support relationships. Enterprises need to be cautious of service providers who attempt to differentiate the number of vendors they claim to support.

Key questions to ask prospective SASE providers regarding their technology options include:

- Which SASE technology vendors do you support?
- How many customers do you have that use the SASE technology vendor you've recommended?
- Is your staff certified by the SASE technology vendor?
- What is the support relationship with the SASE technology vendor? Do you have direct access to vendor's support experts (level 4 support)?
- What is the average time to resolution for critical trouble tickets?

Ease of Migration

For most enterprises, SASE is a journey that will consist of numerous phases spread over time. Therefore, IT teams need to elect service providers that provide flexible deployment options that fit their needs and timeline. In addition, prospective providers should understand the current architecture and recommend the path that incurs the least risk and disruption.

Key questions to ask prospective service providers include:

- Can you support a field trial for a subset of our enterprise?
- What are your recommendations to reduce the disruption to users and applications?
- Can we start first with networking transformation and then security? Or vice versa?
- What will the onramp process be? How long will it take?

Service Flexibility

Traditional networking and security deployments typically employed a set-and-forget mentality. With configuration performed once and then deployed for an extended period without change, enterprise agility suffered. In contrast, SASE aims to make networking and security agile. It is to be expected that SASE deployments will frequently change to respond to current business requirements. SASE needs to complement the cloud's agility by enabling enterprises to deploy applications quickly and retain flexibility.

IT teams need to ensure that their SASE providers are flexible and able to cope with rapid change. Flexibility is not limited to how quickly a SASE provider can make changes, but extends to whether IT teams can make their changes in the provider's infrastructure.

Key questions to ask prospective service providers include:

- How easily and quickly can network capacity be increased or decreased?
- How fast can new network and security services be deployed?
- Can our team directly change security policy (such as firewall, proxy rules, threat sensitivity)? How long will it take? How often can it change?
- Can our team direct change networking policy (such as routing, DNS, IP addressing)? How long will it take? How often can it change?

Operational Excellence

A chain is only as strong as its weakest link. It is no different in enterprise IT. IT teams who pick service providers that lack operational excellence will invariably suffer unexpected outages. With the convergence of networking and security in SASE, the need for operational excellence is even higher.

IT teams need to ensure they vet their prospective candidates by asking questions, such as:

- How many unexpected outages did you experience in the past year? Overall?
- How do you handle worst-case burst traffic situations that may overextend your infrastructure?
- Is all network and security processing done at every point of presence, or do you backhaul traffic to other regions in your network?
- What are your quality assurance processes?
- Do you have a dedicated quality assurance team?

Global Reach

Because users and applications have become highly distributed across the globe, SASE aims to provide secure connectivity anywhere it is needed. Enterprises that have a global footprint need a SASE provider that can match.

Key questions to ask include:

- Can you provide services in all the countries my enterprise is in?
- Do you own your networks in the countries my enterprise is in, or do you have relationships with other communications service providers?
- How many points of presence do you have? How close are they to my key locations?

Conclusion

As we enter the post-pandemic era, enterprises are increasingly embracing a cloud- and mobile-first IT strategy. Traditional approaches relying on legacy hub-and-spoke architecture and assuming a clear network perimeter will no longer work. The new path forward consists of network and security being intertwined with tight integration, adaptable performance, and pervasive security in the style of SASE.

IT architects and operations teams have several vital steps in their SASE journey. They first need to sufficiently understand SASE's architecture and its five core components that we described. Next, with 30 technology vendors vying to win in the marketplace, IT teams need to appreciate the vendor ecosystem and its evolution along with the five areas of differentiation we discussed. IT teams then need to decide on their implementation approach along the spectrum ranging from the DIY to the fully-managed service approach by using the six considerations we examined. Lastly, or for IT teams considering using a service provider for part of an implementation. Lastly, or for the entire implementation, we reviewed six considerations when choosing a SASE service provider.

We hope our paper sheds new light on an increasingly traveled path toward SASE and assists in defining an IT team's potential journey.

About Author

Mauricio Sanchez joined Dell'Oro Group in 2020, and is responsible for Network Security & Data Center Appliance market research program, as well as Security Access and Service Edge (SASE) Advanced Research Report. He brings over 20 years of experience as an executive manager in networking and security technologies, products, and solutions spanning data center, campus, and mobile architectures. Mr. Sanchez helps shape the coverage of next-generation networking architectures and services models. Mr. Sanchez's research and analysis has been widely cited in leading trade and business publications. Mr. Sanchez is a frequent speaker at industry conferences and events.

Email: mauricio@delloro.com

About Dell'Oro Group

Founded in 1995 with headquarters in the heart of Silicon Valley, Dell'Oro Group is an independent market research firm that specializes in strategic competitive analysis in the telecommunications, networks, and data center IT markets. Our firm provides world-class market information with in-depth quantitative data and qualitative analysis to facilitate critical, fact-based business decisions. Visit us at www.delloro.com.

About Dell'Oro Group Research

To effectively make strategic decisions about the future of your firm, you need more than a qualitative discussion – you also need data that accurately shows the direction of market movement. As such, Dell'Oro Group provides detailed quantitative information on revenues, port and/or unit shipments, and average selling prices – in-depth market information to enable you to keep abreast of current market conditions and take advantage of future market trends. Visit us at www.delloro.com/market-research.

Dell'Oro Group
230 Redwood Shore Parkway
Redwood City, CA 94605 USA
Tel: +1 650.622.9400
Email: dgsales@delloro.com
www.delloro.com