White paper

Thought Leadership

The right approach to SASE

How to secure and optimize your unique network environment

Introduction

While the promise of digital transformation remains a priority, the reality for most enterprise technology teams is that managing and securing an increasingly complex IT environment poses significant challenges.

The traditional IT approach to addressing network congestion and potential security risks is to add more dedicated appliances and specialized systems, but that strategy doesn't work as well in the cloud-native and edge-application distributed world.

The good news is that now there is a better way: secure access service edge (SASE). That sounds like quite a mouthful, but it is really a new way of packaging and delivering security integrated with network services that fits with where and how applications are used in the modern enterprise.

What is SASE?

SASE is an emerging cloud-native security concept introduced by Gartner in 2019. In simple terms, it's a network architecture that merges software-defined WAN (SD WAN) capabilities with comprehensive network security services such as secure gateway, cloud access security broker (CASB), zero-trust network access (ZTNA) and firewall as a service (FWaaS) to create a unified, cloud-delivered service model that supports the dynamic secure access needs of digital enterprises.

> **"The vendors with the competitive edge are those that operate their own global network backbones and have direct connections to cloud services, offer additional security services that can be acquired as a bundle or à la carte, and most important, are easy to acquire and scale as demand changes while also being easy to manage for a large number of users."**
> **—Mike Fratto, 451 Research**[1]

SASE represents a strategic shift in thinking about security by creating a new identity-centric unified networking and security platform that is cloud delivered and universally distributed in a way that ensures that the end users and devices on the network edge—from remote offices and workers to cloud resources to IoT devices—are securely connected. In addition to enhanced security, SASE's cloud-based infrastructure promises to optimize access performance by making it easier to connect to resources wherever they are located, which could drive business benefits like reduced product development time, faster delivery to market and greater agility in response to competitive or operational challenges.

Beyond that general description, just what SASE looks like in detail is a topic of much conversation and debate in the analyst community and tech industry. While Gartner describes SASE as being delivered via a single-pane-of-glass platform, today's reality is that an end-to-end SASE solution requires a combination of vendors, technologies and offerings to be integrated to deliver a customized solution to help achieve an enterprise's goals.

40%

By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.[2]

116%

According to the Dell'Oro Group, "the SASE market will grow at a compound annual growth rate of 116%, attaining a market value of $5.1 billion by 2024."[3]

[1] Mike Fratto, "COVID-19: Secure remote access services in demand as enterprises continue work-from-home strategies," 451 Research, September 10, 2020.

[2] Neil MacDonald, Lawrence Orans, Joe Skorupa, "The Future of Network Security Is in the Cloud," August 30, 2019.

[3] https://www.sdxcentral.com/articles/news/delloro-sase-market-to-hit-5b-by-2024/2020/10/

What is clear is that every letter in the acronym represents an important component in the overall solution. "Secure access" indicates a redefinition of how security is delivered, changing from the traditional location-centric model to an identity-centric one. This makes sense in light of the need to secure end users rather than just the locations where end users may or may not actually be located. "Service edge" highlights the emphasis on cloud-based, as-needed services – a critical component of SASE as companies migrate their core applications to the cloud.

Just what SASE looks like in detail is a topic of much conversation and debate in the analyst community and tech industry.

Why has SASE become a hot topic?

Given the growing need for enhanced security in today's WAN environment, SASE's emergence as the go-to solution has generated significant attention. A number of key factors are driving this trend, including the COVID-19 pandemic, growing online threats, the movement of applications to both cloud and edge, and the increasing use of more dynamic applications. In addition, distributed applications are creating performance and security challenges, such as the need to scale quickly while still being able to optimize network performance and security.

The COVID-19 pandemic

Before 2020, the number of remote and mobile workers had been steadily rising, but the COVID-19 pandemic rapidly accelerated that trend. While we are still working through the fallout from the pandemic, it looks likely that more people will be working from home and other remote locations in some form for the foreseeable future. This has accelerated the migration of business application portfolios into the cloud.

Increased security threats

The proliferation of cloud-based networking, third-party connectivity, an increasing focus on a global presence, IoT devices, remote workers and other trends have pushed a greater portion of business activity, applications and data into the cloud. While this opens up an abundance of new opportunities, these distributed applications and users are making the network more difficult to protect by increasing the attack surface and opening up the potential for new cybersecurity risks. Cybercriminals in particular are looking to exploit potential vulnerabilities created by the number of remote workers that has skyrocketed during the COVID-19 pandemic.

Virtualization and the move to cloud

Over the last several years, enterprises in general have been undergoing a digital transformation, adopting virtualization across their network infrastructure and moving applications, data and workloads (and consequently, traffic) to cloud platforms. The use of dynamic applications that can be deployed, tailored and optimized on the fly is increasing.

Adding more complications and stress on security and networks is the fact that many of these applications are more platform and network intensive, requiring lower latencies and greater throughput for optimized performance and user experience. Some examples of such applications include augmented reality/virtual reality (AR/VR), IoT and video image-capture processing.

A move away from the network appliance box

Increasingly, enterprises are looking to move away from customer premises-based equipment, which has been traditionally referred to as appliances. These fixed assets require significant capital investment and demand an endless cycle of expensive hardware refreshes to keep up with new features, functionalities and software updates.

Sixty-two percent of organizations experienced an increase in information security incidents as a result of the pandemic.[4]

As enterprises become more accustomed to the benefits of cloud and virtualized computing, they are now demanding the same ease of use for their network-based applications that they enjoy with their cloud-based ones. Single-pane-of-glass portals, self-service turn up, and end-to-end integrated security and networking solutions are all elements that are rapidly becoming expectations.

[4] 451 Research Digital Pulse: CORONAVIRUS FLASH SURVEY OCTOBER 2020. https://verizon.northernlight.com/document.php?docid=VK20201016830000071&datasource=VIRNSYND&trans=view&

Vendor consolidation

Technology is always in an endless cycle of expansion and consolidation, sometimes even at the same time. Typically, the early part of a new technology cycle drives increased technology complexity (at least temporarily) and often creates multiple new entrants, meaning organizations must work with many disparate vendors. As a technology matures, substantial vendor consolidation occurs as providers look to round out their offerings through acquisition and consolidation, effectively reducing the number of vendors that enterprises need to engage with over time.

68%

Sixty-eight percent of senior executives say they are rethinking their long-term strategies in the post-pandemic environment.[5]

In order to reduce the risk of technology and vendor mismatches and to avoid a scattershot approach to vendor engagements, many organizations are looking to be more careful about who they work with. They are looking for a select few vendors with broad experience in security, applications and networking (in other words, SASE) that can be trusted to deliver the services they need throughout the technology cycle.

Complexity

There is no doubt that today's enterprise IT environment, with its seemingly ever-expanding stack of multiple vendors and solutions, is hard to manage. Compounding these problems is the fact that internal experts are not always easy to obtain or retain, further handicapping an enterprise's ability to manage the increasing complexity and even decipher vendor noise from reality.

What SASE promises

Unifying network and security addresses enterprise needs for more flexible networking and improved application performance, combined with advanced network security and scalability. With SASE, enterprises will be able to improve business agility while offering their users new ways to secure connectivity to applications or resources, no matter where the end user might actually be connecting from or be located.

Increased agility

At a high level, SASE can enhance agility in a number of ways. It can:

- Reduce systems complexity and integration headaches
- Enable rapid and more secure cloud adoption
- Drive innovative digital business relationships where data, apps, services and more can easily and securely be shared with partners

At a more granular level, with SASE and a cloud-based infrastructure, companies can easily deploy security applications, such as threat detection and prevention, secure gateway, next-generation firewall policies, web filtering, sandboxing, DNS security, and more as needed. These security services can be delivered at the edge closest to the end users wherever they may be and on whatever network transport they are using—fixed and mobile, roaming, small or large branches, etc.

IT infrastructure simplification

When an enterprise takes on a security stack consolidation project, a SASE-based model should be top of mind for consideration. It can simplify IT infrastructure by reducing security-product sprawl and the related management overhead, including the routine but essential maintenance and updating tasks imposed on the often overwhelmed and underskilled IT team. With its ability to offer vendor choices and, eventually, the ability to manage the SASE implementation through a single pane of glass, the advantages are clear.

Network and security function convergence

Another promise of SASE is the ability to converge a number of network and security functions such as application-aware routing and firewalls. SD WAN networks and cloud services are commonplace, but the emergence of cloud-type security functions and applications has highlighted the need to bring the functions together. Being able to manage both from a single control point in the cloud offers a number of benefits, including optimized access performance, reduced operational complexity and an improved security posture.

> **"Customer demands for simplicity, scalability, flexibility, low latency and pervasive security force convergence of the WAN edge and network security markets."**[6]
> **— Gartner**

Improved performance

In addition to all of the benefits that a cloud infrastructure brings, SASE also promises better network performance through the use of a global SD WAN service and built-in optimization to improve network performance. SASE can also reduce latency and improve application performance by converging hybrid networking and cloud security services together, which helps move data inspection closer to the end-user sessions rather than forcing public cloud traffic through the data center.

Superior security

In today's decentralized network environment, the perimeter is not the defensible position it once was. SASE delivers more granular access security decisions based on identity and application, rather than just relying solely on perimeter-focused security to a WAN or VPN segment.

Potential cost savings

Moving your applications to a single, cloud-based, virtualized platform can help you shift away from hardware point products, reducing capex costs and IT resource demand while enhancing scalability and agility. Consolidating down to a single vendor can reduce complexities associated with management and solution integration, and even purchasing and contract negotiations.

[5] The Future of Work, Verizon. https://enterprise.verizon.com/resources/reports/future-of-work-reimagining-business-as-usual.pdf
[6] Gartner, "Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge," 2019.

Getting SASE right: Four critical components

Getting SASE right may be a complex proposition that presents significant challenges. For one thing, it is a still-evolving technology target. However, let's not forget that the major elements that make up SASE have been around in some form or another for at least 10 years. For example, Verizon has been providing IT solutions that comprise SASE for over 20 years.

This extensive experience has given Verizon unique and valuable insights into the challenges and opportunities to applying a SASE approach to network and security services. Based on that real-world expertise, we believe there are four major areas of focus that need to be properly addressed in order to get SASE right.

1. Cross-technology integration

There's no one-size-fits-all SASE solution, which means enterprises will need to be comfortable working with a variety of technologies in order to build an effective implementation that solves a given organization's specific challenges.

Network

Enterprises adopting SASE will need to be able to integrate a broad range of network technologies from physical transport (private IP, MPLS) up through virtualization (SDN layer). The objective, of course, is to build a truly integrated SD WAN capability with traffic routing, prioritization and bandwidth optimization. In addition to SD WAN, organizations can bring in additional network capabilities as a service, such as WAN optimization and routing.

Applications

Since the goal of SASE is to securely connect people and things from anywhere to any application in the clouds, a mix of security solutions will be needed, including ZTNA, secure web gateway (SWG), CASB, FWaaS and more.

Edge computing

Another key ingredient is edge computing, whether it be a content delivery network, multi-access edge computing (MEC) or an IoT gateway. Managing security across these complex and distributed systems will be essential and require a deep understanding of how edge computing fits into the SASE model.

Devices

With the number of mobile devices and apps growing exponentially—and located largely at the network edge—enterprises will need to effectively manage and secure how these devices and operating systems connect to and interact with networks.

2. Orchestration

How the various technology components of SASE come together is critical.

Service chaining

Service chaining is a key component of SASE because it is a way of automating and optimizing the service delivery experience. Service chaining in a virtual network requires expertise in the use of orchestration tools and systems in order to successfully automate delivery and operations of connected services.

Optimization

Since no single entity is currently capable of providing a complete end-to-end SASE solution, organizations will likely need to combine technologies and products to create their desired solutions. Being able to optimize new and already-deployed technology components so each is functioning and contributing at its full potential will be important.

Performance testing

Given the complex multifunctional environment that will characterize SASE, the ability to conduct testing to make sure the system is properly integrated and performing at expected levels will be critical. This requires the proper tools to conduct the integration, performance and stress testing needed to ensure that functions have been deployed in the optimal order and the most efficient configuration.

3. Cross-organization operationalization

While it's true that enterprise network and security teams have been increasingly aligned over the last decade, most are still organized as independent groups. Since SASE by its nature combines these two traditionally separated service components, a rethink of how security and networks are managed in the production environment is required. Not unlike the marriage of networking and telecommunications operations that occurred in the 1990s as those technologies merged, so too will SASE require that security and networking administration and management merge from the organizational perspective.

Because SASE is still very much a work in progress, CIO and CISO groups will need to rethink their respective roles in supporting enterprise infrastructure operations. Proper governance will be key to success as these changes percolate down through the organization, as they will eventually touch the network architects, security architects, application architects and others that need to work together to execute on a company's SASE strategy.

4. Expertise

Broad expertise about networks, SD WAN, virtualized applications, security and devices is a prerequisite to any successful SASE effort. For example, an enterprise will need to have IT experts who have a deep and varied set of skills around anything from MPLS or other network protocols to cloud and security architectures. If this unique skill set isn't available in house, finding a partner that does understand all the nuances of these varied technologies, and how they fit into the SASE model, will be critical.

Leading the way: Verizon's approach to SASE

Verizon has been investing in and providing SASE-like services and technologies for over 10 years. Our multidisciplinary approach, complemented by key partnerships, helps enterprises securely connect a variety of distributed people, data and endpoints from any location to any app or service.

We describe our SASE offering as a "best-of-suite" solution because it brings together proven products from recognized network and security industry leaders–vendors who represent the ideal combination of features, validation, market presence and innovation in solutions and whose technology and services integrate with ours.

With this best-of-suite approach, we can help organizations choose the right network, the right SD WAN policy and the right cloud security provider, and deliver all of those components as one fully managed integrated service.

Leadership across key technologies

Industry-recognized leadership

Verizon's network and security expertise continues to win accolades and is recognized by industry analysts. We've been a Gartner Magic Quadrant for Network Services, Global[7] leader for 14 years running and have been a leader in Managed Security Services, Worldwide for seven consecutive years.[8] For the last three years, we've been the only telecommunications company named a Leader in both Magic Quadrant for Network Services, Global, and Magic Quadrant for Managed Security Services, Worldwide.

Over the last decade, our Data Breach Investigations Report has become the go-to resource for quantifying and assessing evolving cybersecurity trends and continues to be relied on by security professionals, business leaders and organizations in every industry.

Edge computing

As applications move from enterprise data centers both into the cloud and out to the edge, SASE needs to address data security requirements across the distributed network. The Verizon Advanced SASE solution effectively secures both the applications at the edge as well as in the cloud (and in an enterprise data center, for that matter). This means that security is integrated into the network so that as data is processed and moved around the network, it is protected from end to end.

Virtual Network Services

Our leading Virtual Network Services (VNS) offering is a scalable, orchestrated and fully managed platform that turns a physical network into an on-demand virtual network that delivers the cost and agility benefits of software-defined networking (SDN) through key virtualized services such as routing, SD WAN, WAN optimization and more.

Internet of Things

Our deep expertise in IoT continues to be recognized by industry analysts. We've been named a Leader in the Gartner 2020 Managed IoT Connectivity Services, Worldwide report.[9] Verizon's innovative 5G, MEC and IoT professional services help companies achieve blue-sky objectives by building innovative solutions more quickly.

Device management

Integrating and managing the exploding number of network devices (virtual or otherwise) and apps in today's enterprise is critical to a SASE implementation. Our advanced management solutions help IT administrators manage, track and control the devices and services connected to their networks.

[7] Gartner, Magic Quadrant for Network Services, Global. Published: 20 February 2020. Analysts: Neil Rickard | Bjarne Munch | Danellie Young. As a Leader in Magic Quadrant for Network Services, Global 2015–2020; as Leader in Magic Quadrant for Global Network Service Providers in 2011–14; as Verizon Business in Magic Quadrant for Global Network Service Providers 2007, 2009–2010; as Verizon Business in Magic Quadrant for Managed and Professional Network Service Providers, North America in 2008.

[8] Gartner, Magic Quadrant for Managed Security Services. Published: 2 May 2019. Analysts: Toby Bussa | Kelly M. Kavanagh | Sid Deshpande | Pete Shoard.

[9] Gartner, Magic Quadrant for Managed IoT Connectivity Services, Worldwide. Published: 12 December 2019. Analysts: Pablo Arriandiaga | Eric Goodness | Leif-Olof Wallin | Jonathan Davenport.

Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

The right expertise and management experience

We offer interdisciplinary expertise along with unmatched experience working across the key technologies that are required for SASE.

This is critical in today's business world where organizations of all sizes are buying a wide range of cloud, networking and security technologies. These systems and technologies are merging, and many organizations are not ready to integrate and manage this type of complex environment.

Verizon offers a deep bench of senior network and security engineers who span all of these technologies and who have the expertise and knowledge needed to orchestrate, optimize and manage all the key technologies required by SASE.

We provide managed services that simplify SASE deployments and operations, as well as reduce the worry and effort that goes into the securing of organization.

In order to deploy SASE correctly, there are many components that need to be understood, such as the operational environment, performance requirements and security profile—just to name a few.

Because of Verizon's position as a network and security services leader, we bring a collective wisdom that can bring an enterprise a level of expertise and service that would be difficult to find anywhere else. Verizon is bundling proven best-of-breed offerings into a best-of-suite solution that will simplify SASE and reduce the worry by taking that burden off of a business.

We help organizations discover and deploy SASE in the most effective way for each customer's specific needs.

Many companies bringing SASE products to market are technology hardware providers, not managed services providers, and not surprisingly, they're touting a specific, one-size-fits-all solution, whether it's a solution from another technology provider or their own.

The problem with this approach is that in reality, there is no comprehensive technology solution for SASE. What's required is a combination of solutions based on a given enterprise's challenges and objectives. To get SASE right, an enterprise often must work with a provider that is able to bring together best-of-breed technologies and put the entire stack under a single management platform. Verizon is uniquely positioned to do just that.

We have the experience with orchestrating and optimizing that's needed to realize the full potential of SASE.

Today's IT environment is becoming so expansive and complex that many enterprises are finding it increasingly difficult to manage their own network platform, much less keep it secure.

SD WAN, for example, is a sophisticated service that needs to be tuned to an organization's actual set of applications to realize its full potential. That requires a knowledge of applications in general, a knowledge of an enterprise's specific applications, and an understanding of what applications are important and what the business intent is for those applications.

At Verizon, we can leverage the cumulative insights gained through our visibility across multiple organizations and use that to orchestrate and optimize an implementation to realize its full potential.

We offer one point of contact, as well as reporting visibility, across the entire solution.

Right now, most of the vendors talking about SASE are referring to just the core SASE security elements and are either ignoring the connectivity piece or assuming that it is irrelevant. In actuality, the two cannot be separated. Because we can deliver both the network platform and the security components holistically, we gain intrinsic visibility into both network performance and security across all the different connectivity methods.

The right options

We're bundling together a SASE solution in tested, proven approaches—ensuring simplification, optimization and best orchestration for organizations.

One of biggest value propositions of our best-of-suite approach to SASE is that the performance, flexibility and security that it offers can be provided under a single managed-services umbrella, which simplifies the path to SASE and removes the burden (and related worry) of managing individual components from an enterprise.

With a SASE solution that is orchestrated, tested and optimized by Verizon, there is more extensive reporting and visibility, better management, and most importantly, security across the entire distributed enterprise. Based on our experience, we believe the best approach for SASE is to get it from a single provider that can offer greater visibility across the stack, as well as one that possesses the ability to manage and optimize both network and security together.

We're also delivering flexibility with different configurations and point solutions.

For enterprises that have particular requirements for certain vendors or brownfield environments with some embedded services already, we offer industry-leading point solutions that can help fill the gaps and create a full SASE solution. And just like our single-provider option, we have the orchestration and management expertise to make sure that different solutions from different vendors work together seamlessly.

The right mindset

At Verizon, we are already implementing operational changes in order to more fully support our SASE offering. A good example of this is our initiative to bring our Network and Security Operations Centers (NOCs and SOCs) together to align with the broader convergence of network and security driven by SASE.

We also know that service level agreements (SLAs) are critical for adopting a technology like this, so we're putting in place new SLAs that have been specifically created for SASE implementations.

Paving the road to the future

Never has there been a greater need, or a better time, for network and security convergence. Understandably, SASE will disrupt traditional approaches to networking and security, but in doing so, it will give IT professionals an opportunity to fundamentally reimagine how they design their network and security architectures.

In the near term, SASE promises to deliver enhanced security, performance and flexibility across a merging network and security environment. But those same benefits will also accelerate the broader, ongoing initiatives–such as digital business transformation, cloud-native computing and edge computing–that are redefining the future of the enterprise.

Working with a partner that understands the complexity of network and security features that comprise SASE–and that can help you choose and implement the right features to meet your needs–will be critical. Contrary to what some new entrants to the SASE field might claim, network and connectivity matter, and for SASE to work across the full suite of technologies, the network and connectivity must be understood and integrated with the security solutions.

Verizon offers that understanding and expertise. Our collective knowledge and proven leadership across networking, SD WAN, security and devices–combined with our own market-leading solutions and those of our partners–enable us to deliver SASE as an integrated, best-in-suite service.

To find out more about Verizon Advanced SASE, contact your Verizon Business Account Manager, or click here >