REPORT

SASE: A Journey Toward Network Security

Learn how SASE unifies network access, security and management solutions into a single service offering for the distributed enterprise.

Umesh Lakshman
Head of Solutions Architecture, West, Media and Entertainment, Lumen

LUMEN®
The Platform for Amazing Things℠

Secure Access Service Edge (SASE, commonly pronounced “sassy”) has been gaining momentum since Gartner coined the term in 2019. However, one of the biggest misconceptions about SASE is that it’s a single product you can buy and deploy when really it is an architecture, an ecosystem of technologies and services—including SD-WAN, firewalls, gateways, Zero Trust Network Access (ZTNA) and many others—all working seamlessly together to address networking and security challenges. Various products can deliver these functions depending on which provider you choose to transport you on this journey.

In this report, we will simplify SASE for you while examining the forces driving the need for this architectural model. You’ll also learn about its core components, discover what to look for in a partner and see how the Lumen Platform is well suited to support your SASE needs.

So . . . why SASE?

Depending on where you are in the enterprise cloud adoption race, your organization is either consuming, optimizing, reoptimizing, hybridizing and maybe even looking at edge computing. We are here today learning about SASE because application stacks and use cases have dramatically transformed over the last two decades. This evolution is driving demand for infrastructure and platforms to power next-gen applications, connect and secure disparate branch locations and deliver exceptional and potentially immersive customer and user experiences.

The COVID-19 pandemic magnified gaps in the enterprise application-to-user delivery model, accelerating the need for a location- and application-agnostic, integrated and secure solution that could meet the needs of a growing hybrid workforce. As enterprise network perimeters expanded to accommodate greater numbers of remote workers, access points and devices, businesses experienced heightened security risks and performance challenges. DDoS attacks skyrocketed, critical applications crashed, and many enterprises found their existing resources stretched, tested and in some cases, painfully exposed.

These challenges, combined with the normalization of remote work, underscore the need for a software-defined integrated architecture to enable security across environments, endpoints, locations, devices and users—ideally bundled in a simple, easy-to-manage service wrapper.

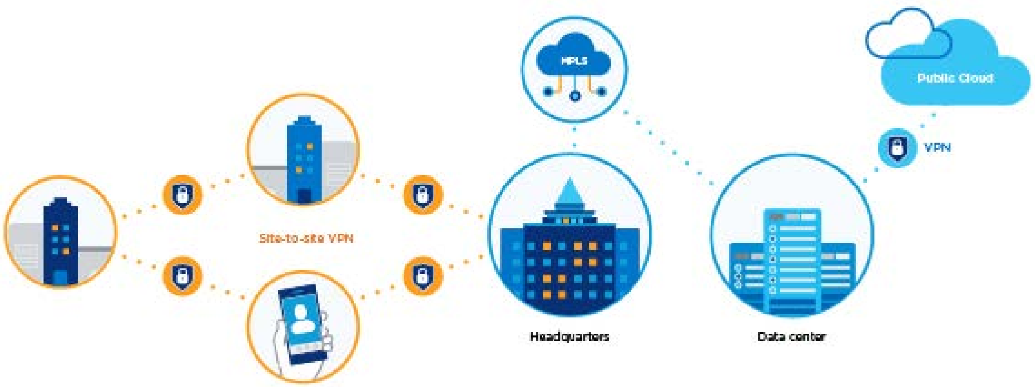
Enter SASE with a red cape. . .

The traditional enterprise data flow is flawed

The promise of SASE is directly related to the historical way of implementing security and access and how traffic flowed from user to application bidirectionally. Enterprises today face three main challenges when managing network traffic and data more efficiently and securely: traffic hairpinning, the explosive growth of SaaS and the proliferation of remote workers and mobile devices within the enterprise.

- **Flaw #1: Hairpinning** – In the traditional architecture, traffic flows from the branch to headquarters, to the data center and on to one or more public clouds. This path, typical in enterprise networks trying to perform all the inspection and security functions in-house or on a specific physical perimeter, is not linear; instead, it takes several sharp turns, which is why it's often called hairpininng. In this scenario, all security functions occur on the headquarters perimeter so network managers can maintain visibility into traffic transiting the network—but this centralized aggregation of traffic and security creates bottlenecks.

F1
Diagram of network traffic data flow resulting in hairpinning



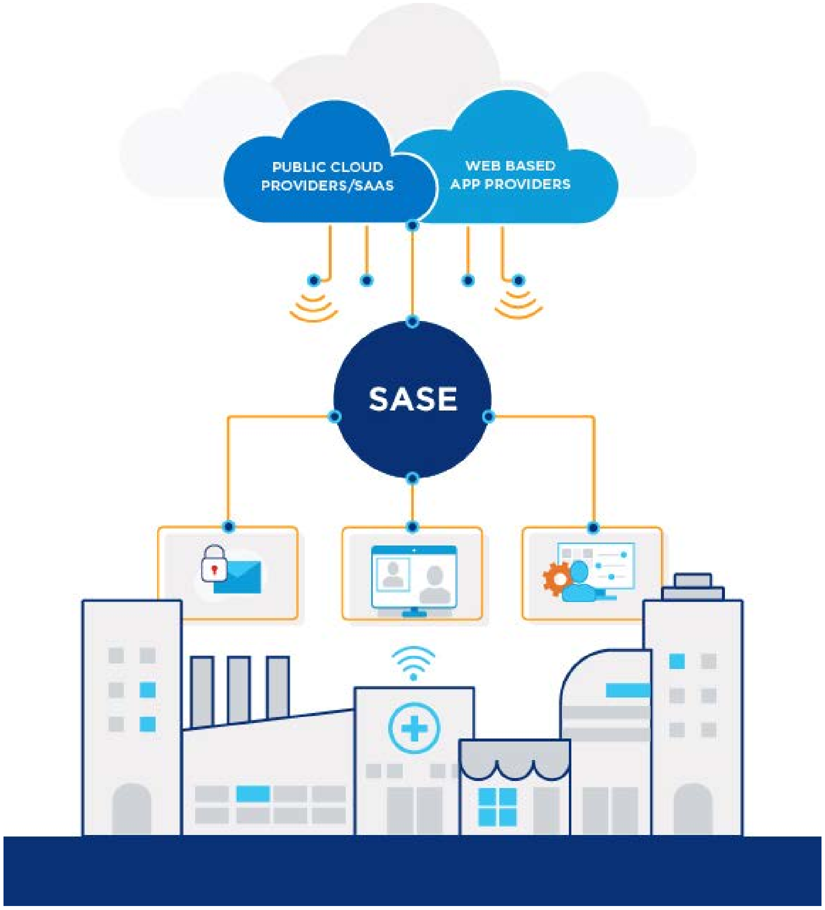
- **Flaw #2: Explosive growth of software-as-a-service (SaaS)** – Over the last decade, SaaS adoption has skyrocketed, with an average enterprise using more than 100 different applications delivered as-a-service. In the traditional model, hairpinning still occurs as traffic flows to a company's headquarters, through a data center, to the cloud containing the SaaS application with Cloud Access Security Broker (CASB) applying specific access policies. Aggregating traffic into a few centralized points also contributes to network congestion.

- **Flaw #3: Proliferation of devices** – The new normal represents a substantial shift towards remote and mobile users or bring-your-own-device models. In the old enterprise model, all the traditional VPN-type functions still happened in one location (headquarters) or a small set of distributed locations. Organizations have also broadened the threat landscape exponentially by letting the same devices access both the enterprise and the open internet.

Bottlenecks like these can result in high latency, poor user experiences, lack of access and application failure. With SASE, we can deliver an enhanced, secure, optimized user experience by creating a simplified architectural framework with all the appropriate security functions regardless of service, device and location—and can be consumed in phases by the enterprise.

The vision of SASE is to deliver network and security as-a-service.

F2
Diagram of SASE connecting clouds, locations and users



In short, the vision of SASE is to deliver network and security as-a-service—enabling organizations to unify disparate security policies, move security functions closer to PoP/Edge locations, lower latency and improve application performance through service chaining.

So . . . who cares?

You should. Or possibly you already do and don't know it. SASE is an architectural journey, and with that journey comes the need for strong collaboration between various organizational groups and entities. No matter how your company is organized, everyday decision-makers include your IT, security and technology leadership. In larger companies, these correspond to the CIO, CISO and CTO. Each of these leaders is responsible for specific areas of focus with some overlap.

- **IT decision-makers** have their eyes on network performance, reliability and capacity, with ubiquitous security interlocked at every function. Their focus is also shifting toward embracing the journey from data to information to action along the road to multi-cloud strategies.
- **CISOs** primarily focus on the end-to-end security of their corporate information assets, applications and devices. Security in this equation is not just a priority but the be-all and end-all, with CISOs taking responsibility for mitigating risk and maintaining security processes and compliance.
- **CTOs** leverage technology to enable and accelerate business model transformation.

SASE sits at the intersection of these domains, whose leaders share four common goals:

- **Improving control and visibility** into security operations and network traffic
- **Performing service upgrades** with minimal to no user impact, adopting new features and patches and ensuring performance and security around new apps and users
- **Improving business productivity** by integrating security and network management and keeping the machinery moving so people can innovate, deliver and do their jobs
- **Enhancing customer experiences** by fine-tuning the performance of critical apps, which helps enhance business outcomes while helping to grow new partnerships, the customer base and revenues

SASE seeks to help achieve these outcomes with a customizable offering, delivering a multi-dimensional solution within a simplified service wrapper. Because the SASE framework encompasses several technologies, potentially from multiple vendors, the successful implementation of a SASE solution is highly dependent on integration and management expertise. Many businesses adopting a SASE strategy will need a partner offering flexible management options that can work in harmony with the expertise and priorities of their current and future IT staff.

How does SASE help transform your business?

You may think that everything you have read so far sounds great, but how does SASE help transform your business? Do you really need to embrace SASE to realize all its benefits? Are you already doing SASE but don't know it yet? So many questions!

In most cases, enterprises are looking at SD-WAN to transform their transport domain while simultaneously focusing on security function. SASE as a framework unifies these parallel (but separate) worlds, creating a confluence where a host of business outcomes are possible through technology:

- **Agility** - Speed to integrate and implement new and differentiated software-based network and security features and functionality
- **Flexibility** - Ability to service chain multiple services as needed to create a differentiated user experience
- **Adaptability** - Single architecture that is agnostic of user location or application venue—thus enabling easy adaptation to multiple use cases, traffic patterns and policies
- **Consistency** - One framework to rule them all and one operational model agnostic of the user, location, device and application
- **Simplicity** - Operational simplicity, consistency and flexibility, all of which help to simplify management, additions, changes and evolution of network and security solutions
- **Enhanced experiences** - Ability to drive higher-order, immersive or optimized user-to-application interactions
- **Cost optimization** – Moving from Capex to OpEx models, streamlining spending and building a foundation for a pay-as-you-grow consumption and usage model

Now let's find out how SASE can deliver these benefits with a single simplified, scalable and performance-driven architecture.

What are the core components of SASE?

At a high level, enterprises have applications that fall into these broad categories:

- SaaS
- Public cloud
- Data center
- Hosted applications
- Pure internet
- Site-specific services

These applications must be securely accessible by any user who could belong to any of the following locations and access methods:

- On-premises
- Mobile
- Bring your own device (BYOD)
- Remote/work-from-home
- Contractor or third party

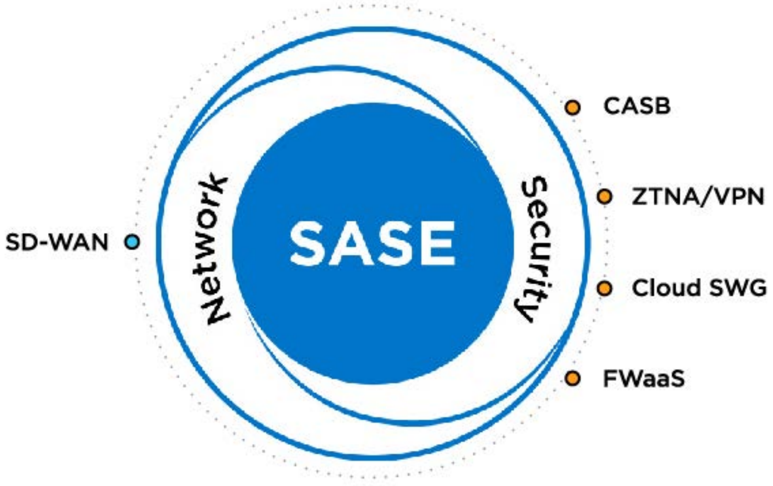
An elegant SASE solution simplifies security and access policies and enables users to access the services they need, depending on their specified privilege levels.

This is a good point to clarify some common misconceptions about SASE:

- **Zero trust is not SASE.** It is a technology and one of the core SASE services.
- **SD-WAN is not SASE.** SD-WAN delivers the streamlined, policy-driven underlay needed to support SASE security functions seamlessly.

SASE is not any one solution. It is an amalgamation of technologies working together under one architecture designed to deliver improved business outcomes. And while the SASE umbrella encompasses many services or functions, we will focus on five core components.

F3
The connected SASE services architecture illustrating the core network and security functions



1. SD-WAN

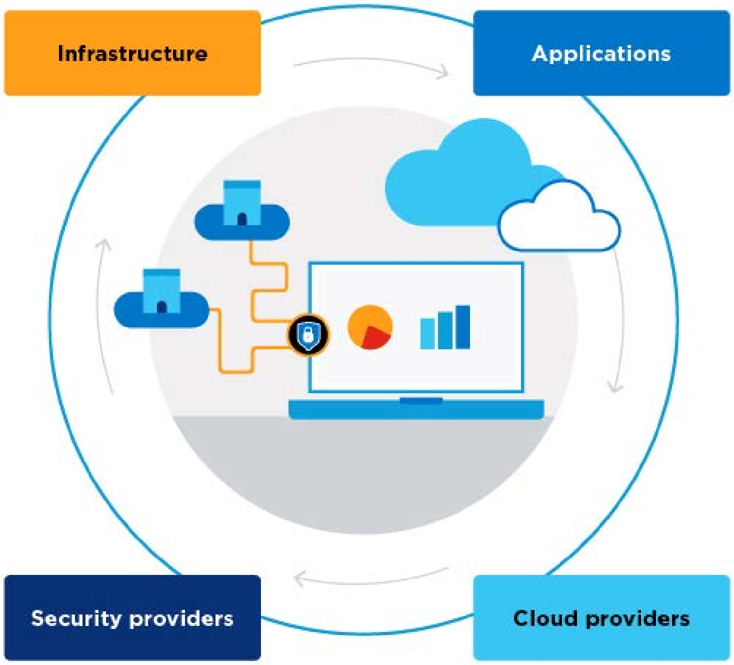
This network approach decouples the type of transport (MPLS, DIA, LTE, Broadband, etc.) by securing and coordinating workloads with centralized visibility and control. With SD-WAN, an enterprise can harness the full power of transport capabilities and enhance the end-user application experience.

Benefits of SD-WAN include:

- **Integrated security:** Offers end-to-end visibility, next-generation firewall capabilities and packet encryption to minimize exposure to threat
- **Adaptability:** Real-time analytics visibility and control to help orchestrate and optimize how the transport is leveraged, increasing productivity and improving cloud and application performance. SD-WAN continuously adapts to changes in the network, mitigating congestion, outages and human errors to deliver an always-on model that keeps users connected to their applications and maximizes uptime
- **Increased network agility:** Coordination of workloads across the full range of connectivity types on a single, automated platform with centralized visibility and control

Enterprises considering an SD-WAN solution or that already have one in place are well on the way to SASE, which integrates SD-WAN with other core services for a holistic and integrated network and security framework.

F4
An enterprise ecosystem



2. Firewall-as-a-Service (FWaaS)

Enterprise firewalls located at company headquarters and branch locations connected by the corporate network perform “perimeter” protection for in-transit traffic sharing. This model comprises multiple firewalls segregated by application domains for SaaS, public cloud, private cloud, public internet, specific sites or VPN use cases such as contractor or remote worker access, resulting in firewalls that spread out geographically and/or virtually.

Over the last several years, the cybersecurity threat landscape has evolved exponentially in terms of the types of attacks, threat actors, and volume and duration of attacks—necessitating enterprises to implement firewalls that can detect threat activity down to the application level. The FWaaS performs firewalling and security functions higher in the OSI/application stack, preventing breaches through these constantly evolving threat vectors.

The primary functions of FWaaS include:

- Intrusion prevention (IPS)
- Intrusion detection (IDS)
- DNS protection
- URL filtering
- Malware protection
- Application-level filtering

FWaaS is vital to SASE because it allows for the flexible delivery of firewall functions at any location without compromising security. It also enables more straightforward integration of all security policies into a single pane of glass view, where they can be managed and orchestrated regardless of the application and its hosted location (SaaS vs. cloud vs. data center).

With the FWaaS service model, organizations will find it easier to implement policies—forgoing the need to log into hundreds of firewalls across the enterprise—and deploy firewalls at scale as the enterprise grows.

3. Secure Web Gateway

As the core service providing next-generation functions, SWG performs constant authentication, URL filtering, data leak protection, malware protection and uniform policy enforcement. Data in different venues (SaaS vs. cloud vs. data center) benefits from uniform policy enforcement, filtering malicious code at the web-based application level and enabling a level of visibility that can be applied directly to the user wherever they are located.

4. Zero Trust Network Access

An important building block of SASE, ZTNA is the policy of trusting no one unless they can be authenticated and regularly revalidated. Often confused with SASE, ZTNA is gaining momentum because users are entering the network from different domains, locations and devices—making them prone to attacks and exposing the enterprise to broader risk.

ZTNA is used for policy compliance and malware protection at the edge. As users move across multiple domains, ZTNA performs constant revalidation. Its primary functions are control of endpoint access, network access, application access and access management.

Like the concept of single sign-on, one-time passwords or authentication tokens, ZTNA verifies access on a zero-trust basis that factors in location, time of day and device as some of the variables. Without ZTNA, these variables might prevent users from accessing the network or expose the network to malicious access. Zero trust minimizes windows of exposure to malicious activity and provides the right access to the right user.

5. Cloud Access Security Broker

This is the final piece of the core SASE service chain. Enterprises no longer store data in a centralized location, like a private cloud or data center. Data has migrated into public clouds, SaaS and site-specific “mini” data centers. In some cases, enterprises have leveraged edge computing to build data lakes closer to the end user, enabling them to deliver differentiated experiences informed by user behavior and application usage.

Users today access data irrespective of venue, location, device and geography. CASB provides an extra layer of protection to minimize the risk introduced by user-owned devices and non-work applications. With CASB in place, a sanctioned employee would be able to use a personal, non-sanctioned device to access company-sanctioned applications (think Salesforce, Office 365, etc.), as well as non-sanctioned applications (Dropbox, Facebook or any other public internet application) without the risk of exposing the company or its data.

CASB also provides full API access into platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS) and SaaS environments, thus simplifying integration into an existing bespoke visibility suite.

In essence, the paradigm shift enabled by SASE when its components work together is the efficient application performance and secure access for any user, from any device, located virtually anywhere.

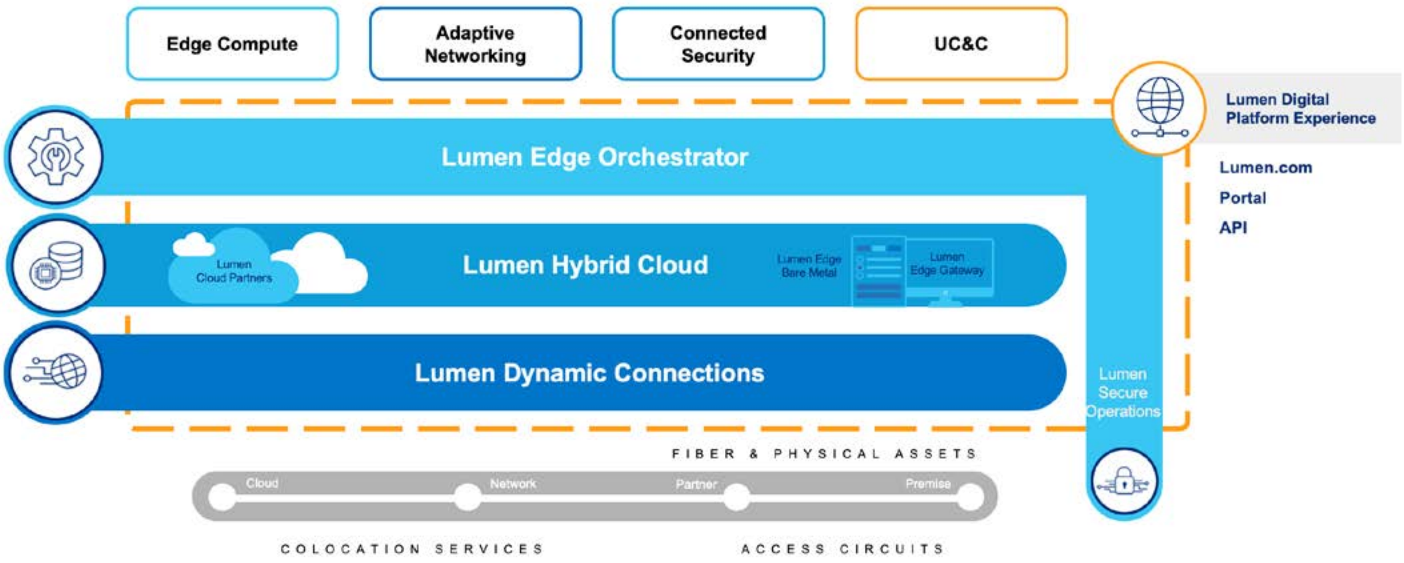
Choosing a SASE partner: Why Lumen?

Now that we’ve covered the five core components of SASE in depth, let’s take a closer look at some key factors to consider when choosing a SASE partner—and how Lumen stacks up in this competitive space.

SASE can be a game changer that accelerates business transformation when adopted, integrated, delivered and operationalized. Network and security as a service enable organizations to service chain multiple functions, simplifying their IT environment while providing a consistent user experience. However, because SASE is not a product but a suite of integrated products and services, it is important to understand how the service wrapper for implementing and managing a SASE solution fits into the bigger picture.

Whether your priority is SD-WAN or security, the right partner is essential for successful outcomes. The Lumen Platform provides a robust, flexible foundation for a comprehensive SASE solution portfolio, leveraging extensive global network infrastructure, high-performing edge cloud services, integrated threat mitigation and response, and a vibrant and open partner ecosystem—all essential components for a unified SASE offering.

Now let’s look at how Lumen can deliver on these criteria.



F5
Diagram of the Lumen Platform with Edge Compute, Adaptive Networking, Connected Security, Unified Communications and Collaboration and global fiber network

Network as a foundation

As a framework, SASE is inherently designed to optimize applications hosted across distributed environments with diverse performance requirements. Any credible SASE provider must be able to build SASE solutions on top of a mix of dynamic cloud, edge and networking infrastructure assets.

Lumen® SASE Solutions are powered by the fastest, most secure platform for next-generation applications and data. Underpinning the Lumen Platform is one of the world's largest and most interconnected networks, enabling low-latency performance via edge nodes that deliver applications and data when and where they are needed (in the public cloud, private cloud, and near or far edge) within milliseconds, protected by integrated security.

With this extensive network as a foundation, the Lumen Platform serves as a unified application delivery solution ideally suited to support the SASE ecosystem.

F6
Core components of the Lumen infrastructure that align with the SASE framework

~400,000
global route miles of fiber

2,200+
connections to public and private data centers globally

Hybrid-cloud
peering with top hyperscalers

6,300+
unique AS interconnects globally[1]

50+
low-latency edge nodes in key metro areas

≤5ms
of latency designed to cover up to 97% of U.S. businesses demand through our Edge assets

#1
peered global network[1]

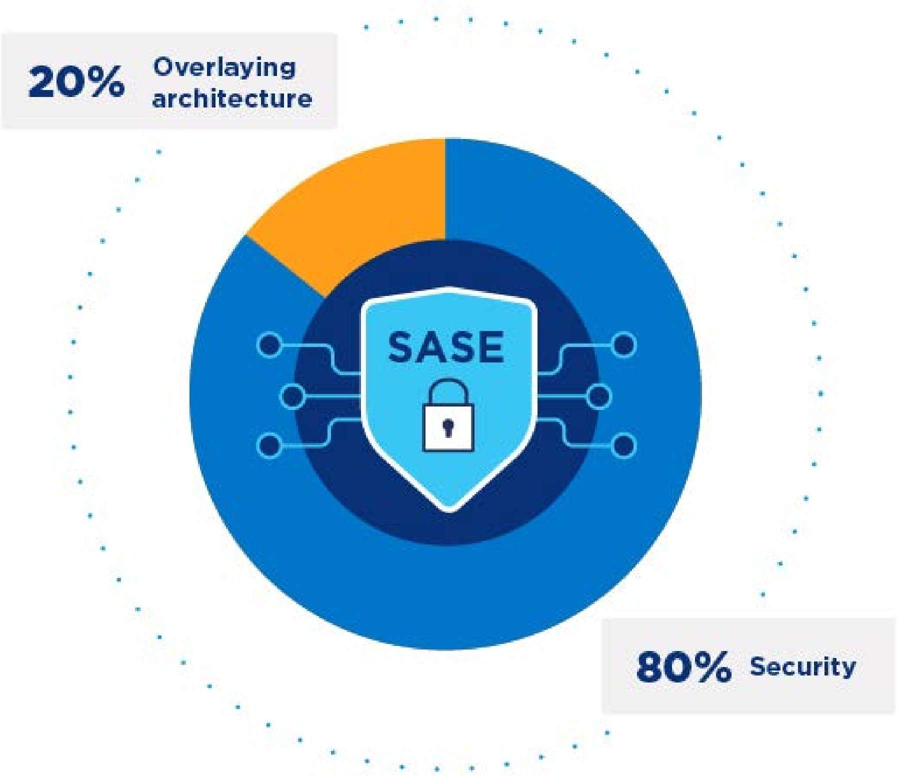
Security is not an afterthought

SASE is 20 percent overlaying architecture and 80 percent security. Ideally architected to support SASE security requirements, the Lumen Platform delivers deep security capabilities with connected security solutions stretching from the core to the edge—embedded all the way down to the fiber in the ground.

Powered by global threat intelligence from Black Lotus Labs®, the Lumen network can identify and eliminate threats earlier—proactively disrupting ~150 C2s (command and control infrastructures) per month through takedowns and notifications. All of this is supported by a multi-tiered scrubbing architecture with more than 170 Tbps of network-based mitigation capacity enacted at 500+ global DDoS scrubbing centers.

This combination of network, cloud integration, low-latency edge performance and a deep roster of security components uniquely positions Lumen to deliver on the promise of SASE.

F7
SASE is 20 percent overlaying architecture and 80 percent security



Service-wrapper simplicity

To make the complex SASE framework deployable and easy to manage, you will also need a partner that offers operational consistency, simplicity at scale and an adaptable architecture with broad geographic reach. Your provider should also be the single point of contact, with responsibility for all aspects of SASE—from support to providing a single bill for service to delivering Network Operations Center (NOC) and Security Operations Center (SOC) resources.

Your SASE service provider should be your single point of contact, with responsibility for all aspects of SASE.

Because different enterprises will have different levels of expertise, management models should be flexible, from self-service to fully managed options. As SASE providers improve their operational proficiency across these foundational areas, they will be better suited to deliver on the unified vision of SASE.

Lumen offers two tiers of SASE service management. Here's how they work:

- **Self-managed:** If you have your own IT resources and expertise to manage a SASE solution and prefer a more in-house, DIY approach, Lumen can help design and implement SASE, providing standard tools and monitoring and APIs for connecting additional services.

- **Pro-managed:** Lovingly called the big "easy button," this option is all-encompassing—from implementation to providing IT staff to ongoing operations management, including software and policy updates, troubleshooting and more. With more than 30 years of network management experience, Lumen has the expertise to complement nearly any enterprise at any point in the SASE transformation.

Vendor-agnostic SASE ecosystem

Each enterprise has unique needs and will begin at a different point on the SASE journey. To tailor the right solution, your SASE service provider needs a robust set of partner relationships to fill out the SASE framework so you can design it to meet your requirements. This may involve different vendors and software choices, each geared toward the best-in-class options for each component.

Lumen has partnered with world-class providers for their expertise in delivering SASE security and network solutions. Lumen SASE is designed with foundational flexibility and adaptability so you can add or change vendors if one solution is not meeting your needs. Unlike single-vendor partnerships, the Lumen portfolio approach lets you quickly switch from one partner to another with much lower operational costs.

The Lumen SASE model isn’t software in a box, but rather a holistic service with diverse product options.

Take the next step in your SASE journey

When Gartner coined the concept of SASE, it intended to promote the vision of networking and security products delivered as a service. And when Lumen built its model for SASE, it was to realize that vision through a platform approach.

Whether you are a large-scale enterprise or a startup, the Lumen business model will help you realize the full benefits of SASE. No matter where you are in the SASE adoption journey, this report provides the foundation to help you understand, assimilate and potentially build a strategy for your SASE adoption while highlighting how Lumen can be your partner, trusted advisor and fellow traveler on this expedition.

Lets go!

Learn how SASE can help your business at lumen.com/sase

[1] The Center for Applied Internet Data Analysis, *AS Rank*, August 2022.

About the author

Umesh Lakshman is the solutions architecture leader for the west region and media and entertainment teams at Lumen. Before joining Lumen, he was a senior sales engineering leader at Cisco, where he built teams that interfaced with some of the world's leading cloud brands.

Professionally, Umesh is committed to driving technical relevancy, strategy and business outcomes through talented people and teams, world-class products and innovative technology, and is the author of four books on security and networking.

He has also written numerous blogs and spoken on diversity, equity and inclusion (DEI), one of his passions. As host of the podcast "Breaking Boundaries," he explores the search for a more diverse and inclusive landscape, both within and outside the workplace.

This content is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. Lumen does not warrant that the information will meet the end user's requirements or that the implementation or usage of this information will result in the desired outcome of the end user. All third-party company and product or service names referenced in this article are for identification purposes only and do not imply endorsement or affiliation with Lumen. This document represents Lumen products and offerings as of the date of issue.

About Lumen

Lumen is guided by our belief that humanity is at its best when technology advances how we live and work. With ~400,000 route fiber miles and serving customers in more than 60 countries, we deliver the fastest, most secure platform for applications and data to help businesses, governments and communities deliver unique experiences.

877-453-8353 | lumen.com | info@lumen.com

LUMEN®

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.