

The Definitive Guide to SASE



Contents

The Traditional Network Is Outdated - pg. 3

Cloud and Mobility: The New Reality - pg. 5

Why You Need to Adopt a SASE Model - pg. 9

The Path to SASE - pg. 19

Find the Right Strategic Partner - pg. 23

Move Confidently Into the Future With SASE - pg. 27

The Traditional Network Is Outdated

The traditional hub-and-spoke wide area network (WAN) architecture is no longer viable.

While this statement may seem premature, two major forces shaping the business world have led to this inescapable conclusion: cloud computing and mobility. The first introduces new and more complicated touchpoints for data across a spectrum of services that include Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The second force encompasses new endpoints, devices, and data and applications being accessed from anywhere.

We live in a world of borderless computing on the far edge, the near edge, in the cloud, *and* in the data center. A traditional hub-and-spoke WAN with all the compute happening in the data center simply can't accommodate this anywhere, anytime, any device reality.



SASE succeeds because it is delivered through a unified, cloud-native platform.

Not surprisingly, all of this ratchets up business and IT complexity, including compliance and security. But it also impacts user experience. Not only is there a need to increase capacity to meet demand, enterprises also must ensure a high level of security without adversely affecting user experience.


This is where Secure Access Service Edge (SASE) enters the picture. It represents the convergence of network-as-a-service and network security-as-a-service. SASE succeeds because it is delivered through a unified, cloud-native platform rather than merely stitching together ad hoc products and services. Simply put: This next-generation networking and security framework produces a sum greater than the individual parts.

But before diving into SASE, let's look at how we got here.

Cloud and Mobility: The New Reality

The ramifications of this changing environment shouldn't be overlooked by enterprise leaders and IT teams. Navigating today's business landscape requires a recognition of just how pervasive and powerful clouds are and how much they change the equation. In a work-everywhere, compute-anywhere world, clouds touch every corner of the enterprise — and extend the network to new people, places, and devices (many unmanaged and even unauthorized). Currently, nearly half (48%) of traffic at branch offices and remote sites can be traced to cloud applications.¹

What's more, over the coming years, the volume of data flowing into and out of clouds will continue to increase. By 2021, it's expected that 94% of workloads and compute instances will be processed by cloud data centers.² A growing array of IoT devices and edge systems are changing the landscape, and additional changes and challenges will emerge as 5G enters the picture.



A legacy WAN architecture and conventional networking model imposes limitations and requires constant attention to ensure that all the components fit together properly and work in harmony. Even then, gaps, glitches, and breakdowns may occur. Although the enterprise data center isn't going away anytime soon, the trend toward placing workloads in the cloud also isn't likely to abate.

In some cases, the enterprise data center will play a less significant role in supporting information technology. In others, it may emerge as a bottleneck, particularly as organizations attempt to manage locations and connect them with software-defined WANs (SD-WANs).

The four walls of the enterprise are gone. Branch offices and mobile workers are the new normal. Sensitive data increasingly resides outside the enterprise data center. By moving from private MPLS networks to the public internet, organizations are confronting increasing security risks and challenges. The possibility — even probability — of devastating attacks across their WAN is growing. This points to a need for a more holistic and comprehensive approach to enterprise security.

This new reality demonstrates that an ad hoc approach to enterprise connectivity, networking, and security is no longer adequate. Enterprises need to connect, secure, and operate an SD-WAN in a better way. To that end, business and IT leaders will benefit by focusing on SASE, the convergence of network-as-a-service and network-security-as-a-service.

Digital Transformation and the WAN



In a traditional WAN, the headquarters is the sun around which all planets orbit. It has a closed MPLS network, applications at the headquarters, and a central internet breakout at the headquarters.



However, digital transformation introduces new requirements for an enterprise. Among them: applications in the cloud, unified collaboration, mobile devices, and the IoT, along with edge infrastructure.



A business-driven SD-WAN infrastructure takes a network to a new level. It revolves around applications in the cloud and provides access to users and devices no matter where they are located. It takes advantage of cloud proximity through local internet breakouts and boosts bandwidth through a mix of MPLS and internet. This approach trims costs, balances traffic over multiple links, and eliminates bottlenecks. It also delivers application visibility and control on the network.

Why You Need to Adopt a SASE Model

It's increasingly clear that enterprise networks are too complex and distributed to manage with limited resources. The ever-increasing complexity of the IoT, decentralized content, APIs, web services, and a proliferation of mobile devices amidst rising quantities and types of security threats have fundamentally changed how computing and IT must be managed.

Traditionally, networking and network security teams have had different motivations: The former aims to make things run as smoothly as possible, while the latter prizes security and compliance above all. Now, these two teams must work together toward the same goal: network connectivity strength *and* security. In addition, most network and network security teams typically deal with a good deal of low-level noise — the operational issues and fires that must be dealt with daily. It can be difficult to find the time to plan strategy, update architecture, and develop new ideas to support new business initiatives.



The move to SASE isn't just a technology transformation, but an organizational change. Joining your networking and network security teams in a shared mission enables them to synergize and better support the organization. And the right SASE partner and service model can reduce your resource strain, helping release staff from some of the day-to-day concerns of running the network and ensuring security so that they have more time to drive innovative projects.

Today, almost no organization starts with a green field. Solutions must be built atop legacy systems — and with the teams you have in place. Consequently, it's time to rethink and, possibly, rewire your enterprise to take advantage of SASE. In reality, SASE is a journey — and it's one that requires a strategic and committed partner that can guide you through the transition process.



Convergence of Networking and Security

SASE facilitates the convergence of network-as-a-service and security-as-a-service based on the movement of digital business away from the enterprise data center. Done right, it creates an umbrella that encompasses critical but discrete networking and security tasks.

Instead of setting policies and controlling access from the center, SASE moves these functions out to the edge, wherever users and devices are. Think of SASE as a worldwide fabric, providing cloud-delivered, policy-based security capabilities on demand.





What an Effective SASE Model Looks Like

The first step in adopting a more sophisticated and streamlined SASE infrastructure is to understand what it is and what it delivers. SASE is a cloud and edge-native platform that delivers a high level of flexibility by supporting identity-based, context-based, and location-aware policies. It skips beyond the technical limitations of configuring IP addresses and aids in managing workloads across physical servers and virtual infrastructures residing in the cloud.

The result is unparalleled agility, flexibility, and scalability. Yet the benefits don't stop there. SASE delivers a single, centralized view and control of network performance and network security. In addition, it provides tools that make it easy to duplicate settings and configurations at branch offices and on distributed devices. Not surprisingly, this approach diminishes complexity and costs as compared to maintaining individual technology stacks at each and every location.



SASE delivers a high level of flexibility by supporting identity-based, context-based, and location-aware policies.

The ability to manage configurations, settings, and permissions across multiple cloud and SaaS providers is transformative. A SASE framework promotes better governance and more consistent security controls. Likewise, it provides powerful tools to integrate networks and security functions more effectively. Using SASE, it's possible to evolve beyond ad hoc point solutions, each with its own lifecycle and total cost of ownership (TCO), and adopt a robust framework that operates holistically.



There are several other key benefits to a SASE framework. These include:

- **A more consistent experience.** SASE establishes a unified user experience across all systems, devices, and geographies.
- **Reduced latency.** With SASE connections reaching the edge and extending to remote locations, end users experience more responsive and secure systems. IT can set policies that route traffic through the most appropriate channels, while necessary security reinforcements are deployed in the most latency-sensitive way.
- **SASE generates additional gains.** The framework aligns with DevOps and DevSecOps initiatives. It also reduces the need for specific skills and dedicated IT staff to administer the network and security.
- **A zero-trust security framework.** Experts agree that SASE represents an initial step toward a more sophisticated continuous adaptive risk assessment throughout the duration of the session.
- **A more consistent experience.** SASE establishes a unified user experience across all systems and devices.
- **Simplified and improved IoT administration and security.** SASE streamlines and consolidates networking, connectivity, and device management within a zero-trust framework.



SASE delivers a better window into processes and optimal workflows.

Ultimately, organizations gain greater understanding of the context of data — including whether data is sensitive or malicious. This, in turn, helps define other crucial tools, solutions, and protections, including the design and use of authentication and encryption. Finally, SASE delivers a better window into processes and optimal workflows, along with more predictable budgeting and OPEX costs. Through predictive analytics, organizations can manage and anticipate data management and security requirements far more effectively. It eliminates potential bottlenecks when changes take place, such as adding new applications. This ultimately leads to a right-sized network.

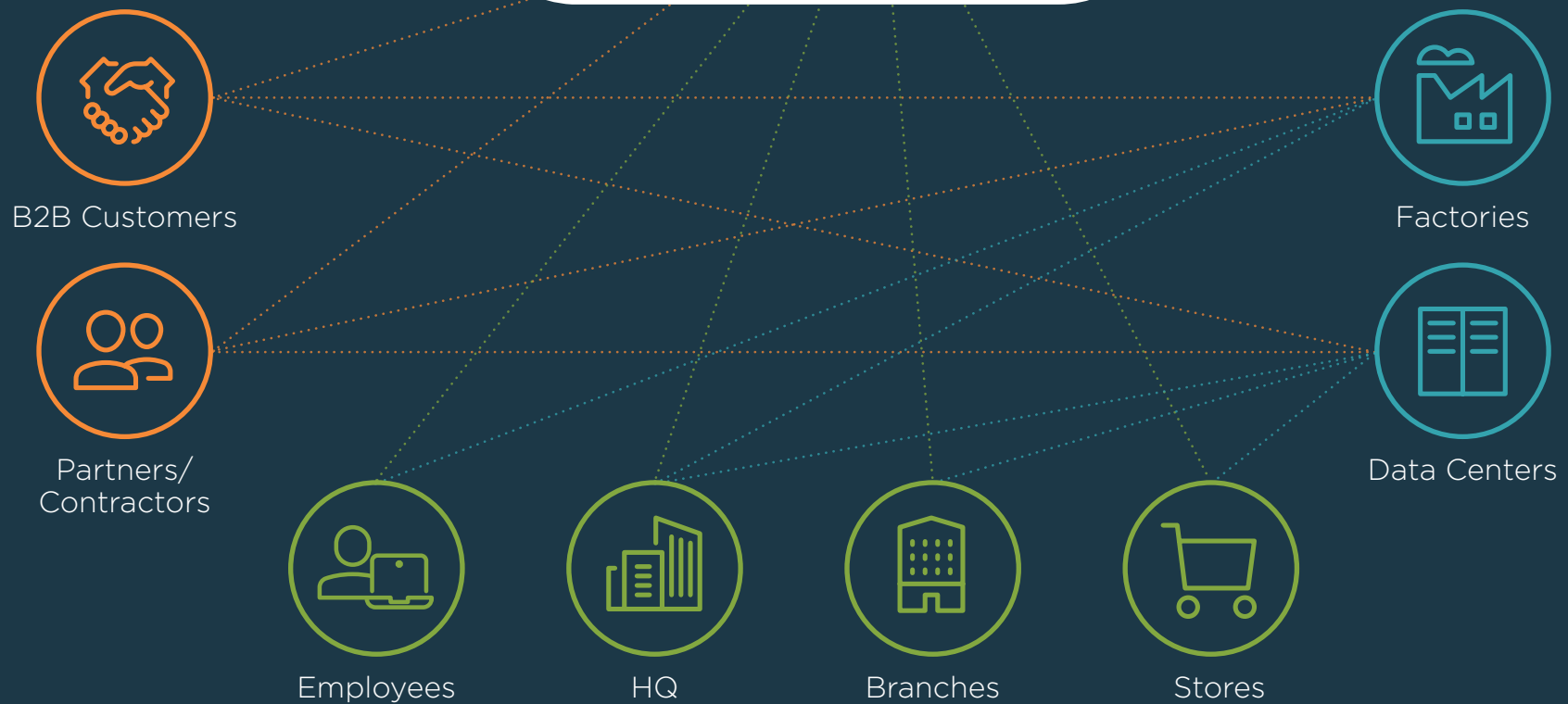


The End of the Classic Security Perimeter

It's not just the cloud that defines today's enterprise. It's a need for a multi-cloud strategy that encompasses hybrid designs (on-premises/cloud), multiple CSPs, and multiple platforms and products, spanning SaaS, PaaS, and IaaS. In addition, it isn't only applications and data that move everywhere. Clients accessing data are more distributed than ever. All these factors render the classic security perimeter — where IT security is primarily enforced in the central data center — irrelevant.

This is why Gartner describes SASE as a more effective way to combine managed services around networks and security.

**Apps, Workloads, and
Sensitive Data *Anywhere***



Managed and Unmanaged Endpoints *Anywhere*

The Path to SASE

A transition to SASE is a longer-term process that requires strategic planning. Because every company has a different starting point — and an entirely different data framework of data, devices, and systems — it's important to proceed at the right pace for each organization. Fortunately, SASE is optimized for such a flexible approach. An enterprise, with the right strategic partner leading the initiative, can move as fast or as slow as necessary, making essential tweaks and improvements as they're needed.

This approach ensures that existing infrastructure remains supported while the transition is taking place. The right strategic approach delivers essential flexibility for central and branch offices, as well as remote users, while supplying maximum bandwidth and quality of service (QoS) for business-critical applications. It also aids in providing secure operations during and after the transition.



There are several key factors to focus on at this stage:

Mapping the network. It's critical to fully map and understand the current network, including what apps are on the network and how much bandwidth they consume, how clouds intersect with the network, where devices and data reside on the edge and with IoT, and how traffic flows through and across the entire infrastructure.

Assessing impact. It's crucial to assess how changes in the network — and security — will impact business processes and practices. This requires a thorough examination of existing data flows, users, and controls. It's important to talk to key managers and others to understand fully where current problems exist and how they might be addressed.

Moving forward while looking back. It's necessary to support both the old and new networks during the transition period. The worst possible scenario is to wind up with systems that won't function correctly or communicate for hours, days, or weeks at a time. This undermines the business and demoralizes a workforce.



Recognizing that the transition period introduces additional challenges and vulnerabilities.

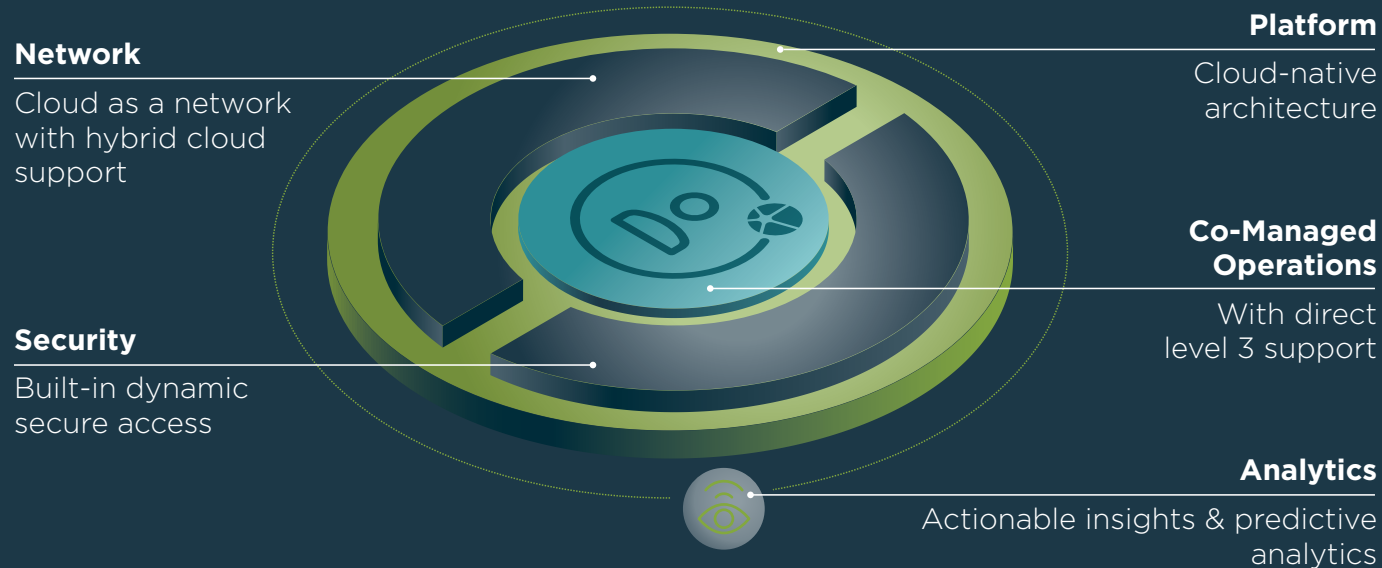
For example, network and security teams must stay in constant contact and work together to address issues as they arise. Traditionally, these teams work separately and often independently, but SASE connects these functions and introduces a common set of goals. This typically requires both cultural and practical adjustments as well as targeted training.

Setting up for the future. Instead of solving the aforementioned challenges with dedicated but disconnected technology, SASE ensures that all the involved components work together seamlessly and provide the right platform for future growth. Moreover, through this holistic lens, you'll get the visibility and insights needed for predictive analysis that informs future business decisions.

To help you successfully assess your current network and needs, transition to SASE, and enjoy the full benefits of the holistic view you'll gain, it's essential to choose the right partner. You need a partner who brings the right technology and experience, asks the right questions, and provides visibility and the level of support your organization needs.

Future-Proof SASE Solutions

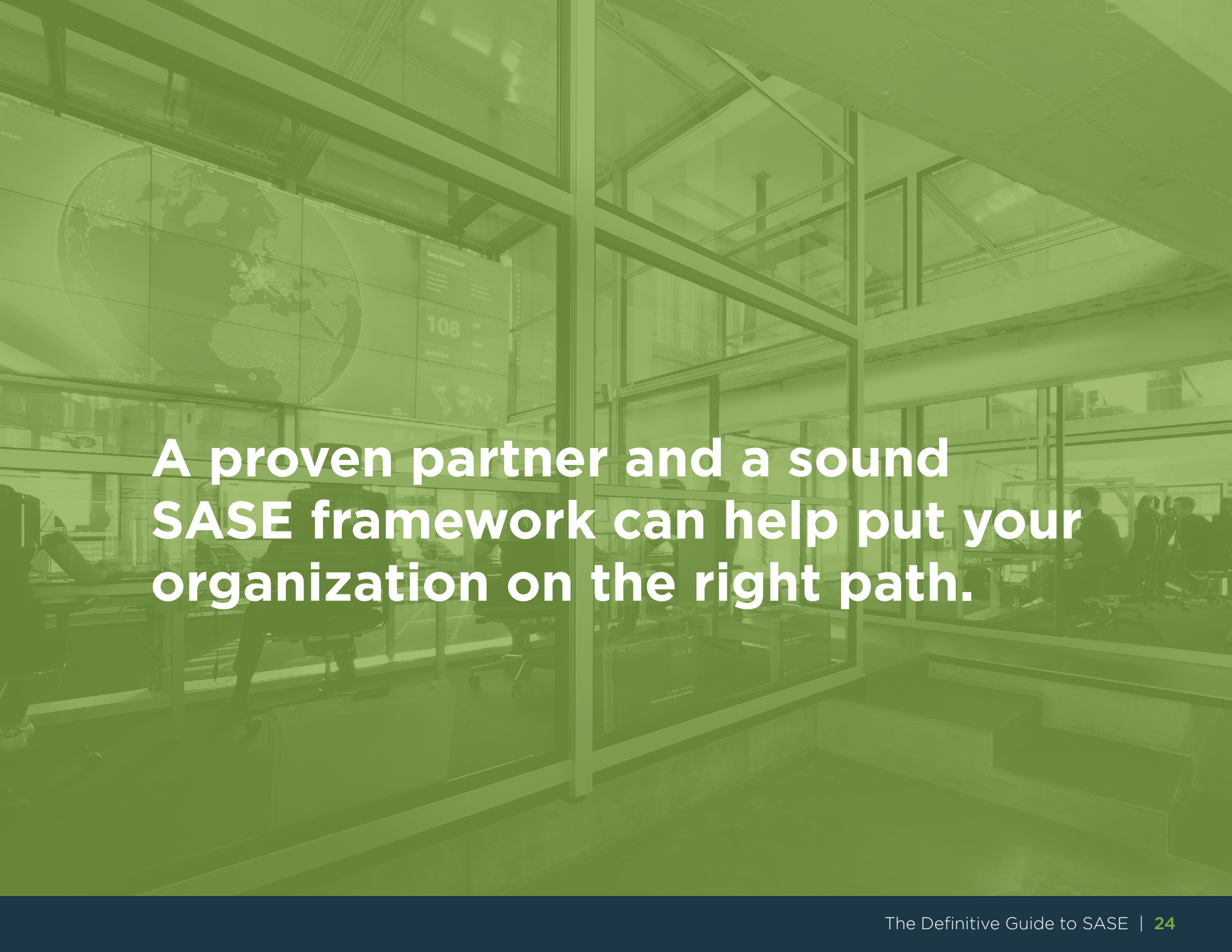
A modern unified SASE assembles all the pieces required to manage an enterprise.



Find the Right Strategic Partner

SASE is receiving growing attention. And it's easy to understand why. Gartner predicts that the SD-WAN service market will grow at an annual rate of 76% annually from 2018 through 2023.³ While security isn't the only factor in this shift to SASE, it's an important consideration. As Gartner puts it: Most enterprises adopting managed SD-WAN services will also need managed security services, which can potentially be sourced from the same service provider.⁴

If there's a takeaway from this it's that with a growing number of players in the SASE space, finding the right vendor is critical. A proven partner and a sound SASE framework can help put your organization on the right path to boost network performance, security, and business results.



**A proven partner and a sound
SASE framework can help put your
organization on the right path.**

Open Systems: A SASE Pioneer

Open Systems is a pioneer in the services that define SASE. It delivers an adaptive, future-proof SASE platform as a service, with 24/7 support to enable network simplicity, intelligent security, and performance.

Open Systems offers:

- Cloud-based, single-pass architecture. Our white-box approach means one platform for monitoring and configuration management, along with one-touch provisioning.
- Hybrid, multi-cloud (SaaS, IaaS, PaaS) support from edge to cloud, including agnostic, any-to-any connectivity and no cloud chaining.
- Secure intelligent edge with built-in, zero-trust, end-to-end security with no service chaining — at the level you need.
- Managed Detection and Response (MDR), an Open Systems technology built on Microsoft Sentinel. It delivers unified security telemetry, robust cloud scaling that eliminates capacity constraints, and expertise provided by highly experienced security analysts.
- Co-managed operations that deliver critical expertise and technical consulting, including support for hardware and software, DevOps and DevSecOps, and governance/compliance. Our experts are your experts. At the same time, you can self-service at the level your organization desires.

- 24/7 follow-the-sun operations management, along with unlimited interactions with L3 engineers.
- State-of-the-art analytics tools that deliver broad and deep visibility across your network, all in a single pane of glass. Improve reporting (via log-forwarding, dashboard, or API, etc.) and get actionable insights for forecasting and proactive decision-making.
- End-to-end lifecycle management — from evaluation and deployment to maintenance and hardware refresh.





Move Confidently Into the Future With SASE

Today's compute-anywhere-and-everywhere world demands more than a conventional approach to SD-WAN and network security. It's critical to have intelligence embedded in systems and to push this intelligence out to clouds and the edge. The right SASE partner can help you transform your network while implementing a more integrated and robust security framework.

Open Systems SASE delivers on the promise of a more sophisticated framework — one that is designed for the digital age and a borderless IT world. Our cloud-native architecture will help you transform your network and security framework into a best-practice model that can take your business to a higher level.

The background image shows a large digital display in a control room. The display is divided into several sections. On the left, there are statistics: 'NUMBER OF NODES' with the value '6449', 'NUMBER OF COUNTRIES' with the value '183', and a small map of Europe. In the center, there is a large, semi-transparent globe showing the world map. On the right, there are more statistics: 'OPEN TICKETS' with the value '40', 'CLIENT RESPONSE' with a star rating, and 'INCIDENT REACTION' with the value '0.6 min'. At the top right, there is a section for 'PRIMARY ENGINEER ON DUTY' with the name 'James Hulka' and a list of other engineers: 'Cedric Zwillingler', 'James Hulka', 'Marc Kuhl', and 'Philipp Mächler'.

Open Systems SASE delivers on the promise of a more sophisticated framework.

Contact us today to **get a free assessment** to learn how you can optimize your network for growth and agility.



Open Systems is a leading global provider of a secure SD-WAN that enables enterprises to grow without compromise. With assured security, AI-assisted automation and expert management that free valuable IT resources, Open Systems delivers the visibility, flexibility and control you really want with the performance, simplicity and security you absolutely need in your network. Learn more at open-systems.com.

¹ EMA, **Wide-Area Network Transformation: How Enterprises Succeed with Software-Defined WAN**, December 2018

² Tech Republic, **"95% of global data center traffic will be from the cloud by 2021,"** February 5, 2018

³ Gartner, **Competitive Landscape: Managed SD-WAN Services**, March 2, 2020

⁴ Ibid.