Beyond SASE 2.0: The Blueprint for the Future of Connectivity

This indispensable resource demystifies the complex landscape of the Secure Access Service Edge (SASE) architectures, offering a comprehensive overview and practical insights for professionals and organizations navigating the realm of modern networking and security.

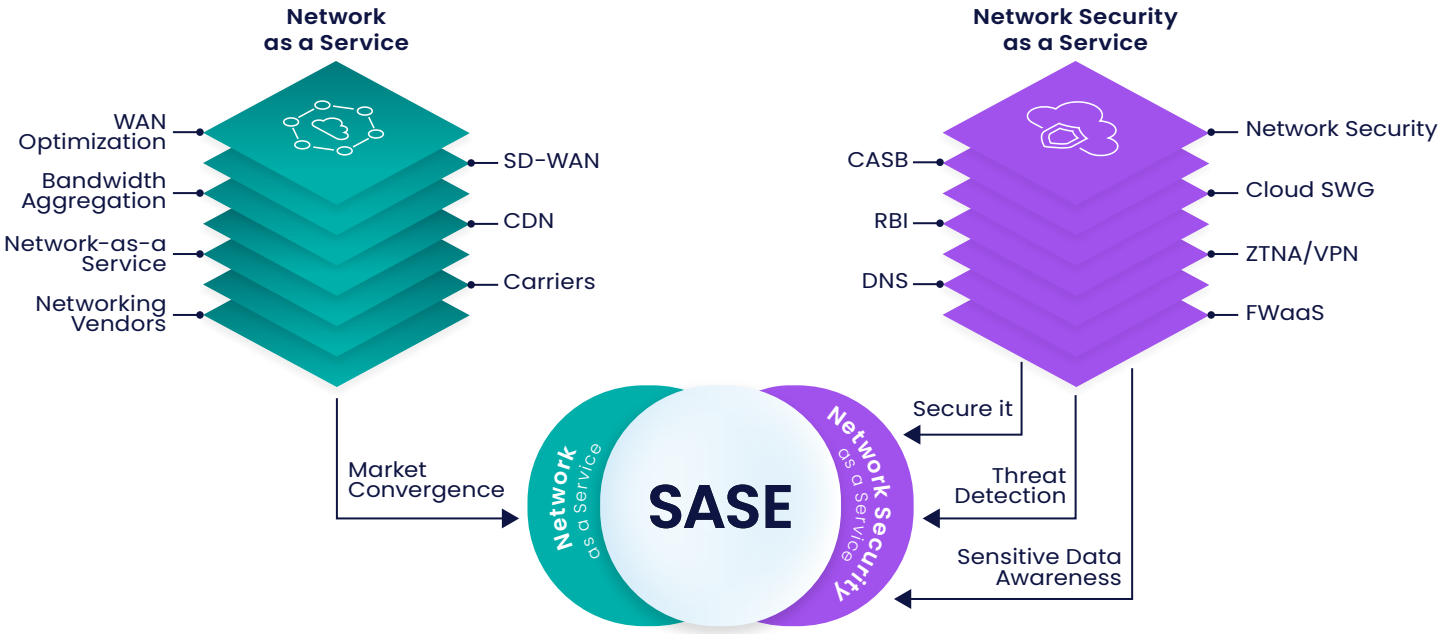
TABLE OF CONTENTS

This guide dives deep into the definition of SASE; why SASE now; plus, the different SASE architectures and things to consider when selecting a vendor. Whether you are just beginning or already deep into your SASE journey, this guide will provide you insights on the convergence of network and security, plus some of the most flexible and cutting-edge methods of implementing SASE such as Unified SASE as a Service.

The Definition of SASE

SASE stands for Secure Access Service Edge. SASE is a technology framework that combines wide-area networking (WAN) and network security solutions and is delivered as a cloud-based service. The analyst firm Gartner coined the term in 2019. Since then, other analysts and organizations have widely adopted the concept. The intent is to deliver these capabilities in a simple, flexible, and agile way and to be part of a secure infrastructure with consistency across the cloud and edge. The business objective is to deliver a consistent user experience with better application performance and reduced security risks, irrespective of users' location and applications or workloads.

As depicted below, the focal point is to deliver both capabilities in an “as-a-service” model. A converged solution of Network as-a-service and Network Security as-a-service is crucial, as SASE is meant to be consumed as cloud-delivered services to meet the demands of modern organizations.



How is SASE different from traditional network security solutions?

The SASE framework is a significant departure from traditional network and network security solutions in its foundational infrastructure. The latter were often deployed on-premises and worked perfectly to keep network and security within the organizational framework. But with the rise of cloud computing and increased use of cloud services overall, SASE's core element of being a cloud-based service makes it more flexible and scalable, as it can adjust quickly to meet the changing business needs of enterprises that have become more hybrid in terms of workforce and workloads. The best part about the core capabilities of SASE is how it combines multiple network and security technologies into a single cloud-based solution. Its integration of security with networking functions and user experience makes it extremely user-friendly for enterprises of all sizes.

How has SASE evolved over the years?

In the early stages, a time period that coincided with the COVID-19 pandemic, many organizations (and vendors) focused on securing network access and corporate resources for a then fully remote workforce. This was done by combining Virtual Private Network (VPN) and Software-Defined Wide Area Network (SD-WAN) with cloud-based security services such as Firewall as a service, URL filtering, Anti-malware, cloud access security broker and intrusion detection and prevention.

That gave rise to terms like single-vendor SASE and multi-vendor SASE where organizations could opt to use technologies from one vendor or multiple vendors.

However, with its evolution, SASE deployments have begun to incorporate more advanced security technologies such as data loss prevention (DLP), enterprise browser isolation and Universal Zero Trust Network Access (UZTNA). UZTNA is achieved by applying the principle of "never trust, always verify." It assumes that all network traffic is untrusted and requires strict user authentication and authorization before allowing access to any resources.

SASE has also begun to incorporate more advanced analytics and artificial intelligence (AI) to better detect and respond to security threats in real-time. With these advancements, many SASE approaches have introduced new complexities with the need to manage multiple point solutions, even if all comes from one vendor and impacts performance. Far from improving agility, these complex approaches often leave Networking and Security teams having to deal with assembling separate parts. A lack of integration is especially true for SASE solutions resulting from multiple acquisitions often require numerous management systems and lack a unified policy management model, resulting in increased costs and time to deploy.

Today CIOs, CISOs, Heads of IT and Directors of Network Security need to ensure secure and performant application and data access to all users across their distributed global network without escalating cost, risk or complexity, or sacrificing user experience. Each stakeholder also has their own specific needs. This is a challenge most SASE vendors have not been able to deliver on.

A unified and comprehensive approach that looks beyond SASE is required to address these challenges comprehensively. An approach that combines a single-pass architecture with unified policy management, a global highly- performant private core network, integrated network, security and observability services and flexible services delivery options. This approach is Unified SASE as a Service.

Beyond SASE: Unified SASE as a Service

Enterprises are confronted by a relentless and seismic shift that makes secure connectivity harder than ever.

Distributed Workforce

50%

Employees work Hybrid

Hybrid Application Deployment

>70 %

Organizations will use Public Cloud by 2027

Increased Security Threats and Attacks

>70 %

Businesses affected by ransomware attacks

Organizations face an increasingly complex IT, security, and networking environment. The constant march of digital transformation, remote work, hybrid compute and workloads across data centers, and multi-cloud environments, increased adoption of AI and automation, proliferating security threats, and the lack of skilled security resources all combine to pressure CISOs and CIOs to deliver a more secure network access without compromising performance and availability. In all that complexity, having organizations integrate all the various security controls adds its own challenge, and no necessarily improvement in security outcomes.

Shortcomings of current SASE Solutions

For decades, enterprises relied on the traditional network set up of a hub-and-spoke network topology, with the central hub as the focal point connecting branch offices and remote users. This topology was no longer effective and posed several challenges as businesses have embraced workforce, edge and cloud transformations.

The current SASE solutions and implementation meant to address these challenges have fallen short in adequately addressing them. The analyst firm Dell'Oro identified four areas of shortcomings:

- **Overemphasis on Security at the Expense of Networking:** Some vendors primarily positioned SASE as a security solution, often neglecting networking functionality. This view limits the scope of SASE, as modern cloud-based network architectures increase IT networking complexity. WAN technologies like SD-WAN play a crucial role in managing this complexity by ensuing network connectivity is always up, ensuring that all traffic is inspected.

- **Insufficient Coupling of Networking and Security:** Most of the SASE market comprises disaggregated solutions, where SD-WAN and SSE (Security Service Edge) components are sourced separately. While this offers flexibility, it lacks the tight integration achievable in unified SASE solutions, where all core network and security technologies come from a single vendor, allowing for better synergy.

- **Neglecting Middle-Mile and Multi-Cloud/Compute Edges:** Current solutions primarily focus on connecting remote users and small branches to Internet-based SaaS applications—a last-mile application of SASE. Neglecting the enterprise middle-mile and multi-cloud/compute edges limits the full potential of SASE. These areas require attention and better support.

- **Challenged Network and Security Workflows:** SASE solutions necessitate a shift in IT teams' network and security operations as they move away from traditional hardware-centric approaches. Workflows, visibility, telemetry, and analytics must adapt to the abstraction from underlying hardware. Some traditional management operations and diagnostic processes become different or even impossible in SASE solutions, leaving administrators seeking more robust capabilities.

Stitched-Together

Multiple point solutions not tightly integrated

Bad End-User Experience

Unacceptable trade-off Security vs. Network when looking for unified outcomes

Operational Complexity

Requires specialized skills and costly consulting services for each of your point products

Prolonged Deployments

Slows down provisioning & configuration

Introducing Unified SASE as a Service

The promise of this approach is to deliver a better user experience while reducing costs and complexity. And to enable enterprises to get it all: performance, agility, simplicity and security without any tradeoffs.

Unified SASE as a Service

A unified single-pass architecture

Enforces policy consistently and without user performance impact across global scale deployments.

A global private network backbone

Delivers security and performance from the first to the middle to the last mile of the network.

A comprehensive and integrated set of services

Including unified policy, network security, SD-WAN, app acceleration, observability, integration services and integrated 3rd party solutions.

Flexible service delivery options

Allow organizations to implement the solution their way, at their pace and to choose from self-managed, co-managed and fully managed service delivery.

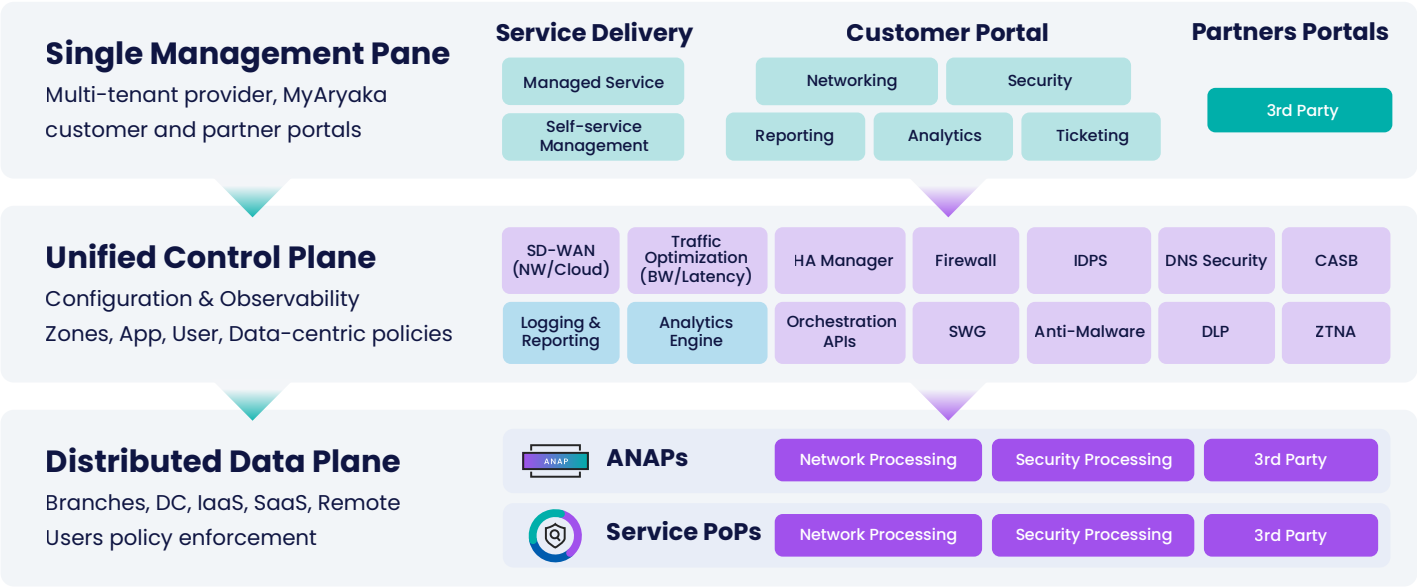
Aryaka Unified SASE as a Service Implementation

Aryaka Unified SASE as a Service provides five compelling business benefits:

- Reduced network attack surface and risk
- World-Class SaaS and multi-cloud application performance
- Improved business and operational agility
- 'As-a-service' flexibility and economics
- Confidence to succeed: enterprises choose their way and pace for their transformation journey

Aryaka OnePASS™ Architecture

A defining feature of the Aryaka Unified SASE as a Service platform is our single-pass architecture which allows enterprises to perform comprehensive inspections and processing, while examining a given data packet only once. The OnePASS architecture ensures that every flow is 'run to completion' for all SASE functions – network services, NGFW, IDPS, SWG, anti-malware and others in the future. It enforces policy consistently and without user performance impact across global scale deployments.



Single Pane Management

A single pane of glass for management, provisioning, and observability for both network and security services. This is the ability to provide visibility into performance characteristics and security aspects of the traffic. As part of the managed services, the NOC/SOC will have visibility across the deployment, with the ability to leverage AI/ML and data analytics for pro-active issue identification and resolution. The enterprise also requires robust role-based customer portal and interfaces with 3rd party portals, for example for traffic log exports in NG-SIEM platforms.

Unified Control Plane

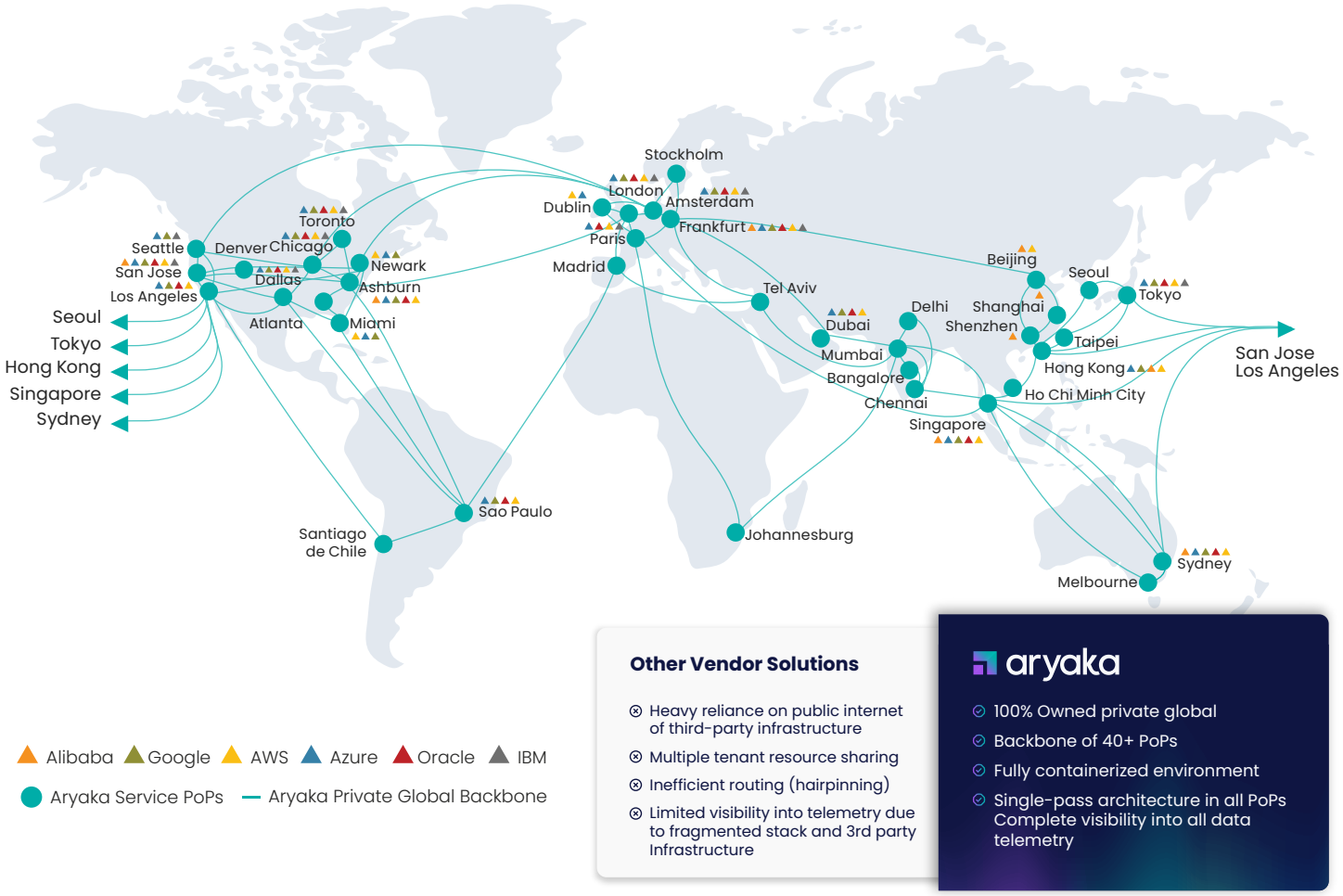
SASE must be centrally orchestrated, a unified control plane that ties these capabilities together in a coherent way to apply policies consistently across hundreds of locations and users to ensure they get applied properly. As we all know, one of the main reasons for security breaches is misconfiguration due to complexity, lack of knowledge, and lack of oversight. Without a unified control plane, it is hard or even impossible to apply security ubiquitously and consistently. Given the as-a-service aspect of SASE, a Unified SASE as a Service provider may effectively offer this control, removing the burden and chance of misconfiguration from the IT department.

Distributed Data Plane

With users and applications anywhere, security enforcement must happen closer to the source. Security controls should be easily enforceable at multiple places and wherever needed — and only once. To address the entire spectrum of the attacks, and provide a better security experience, appropriate security functions need to be able to be applied at any location. This approach requires a distributed policy enforcement with unified security policies enforced closest to where the users are - at the customer premise on the edge appliance or in the PoP/cloud - and closer to the destination where the applications are.

Aryaka Zero Trust WAN

Aryaka's global private network delivers security and performance from the first to the middle to the last mile of the network. The Private core backbone interconnects Aryaka POP locations through redundant and dedicated links. Customers have the option to choose a private core backbone with specific bandwidth allocations for traffic between their offices. Aryaka ensures that the traffic between the offices and the nearest POP locations are connected to leverages the private core. This approach offers benefits such as low jitter, deterministic throughput, and deterministic latency. It also provides enterprises with secure, fast, and reliable cloud and SaaS access from any location in the world.



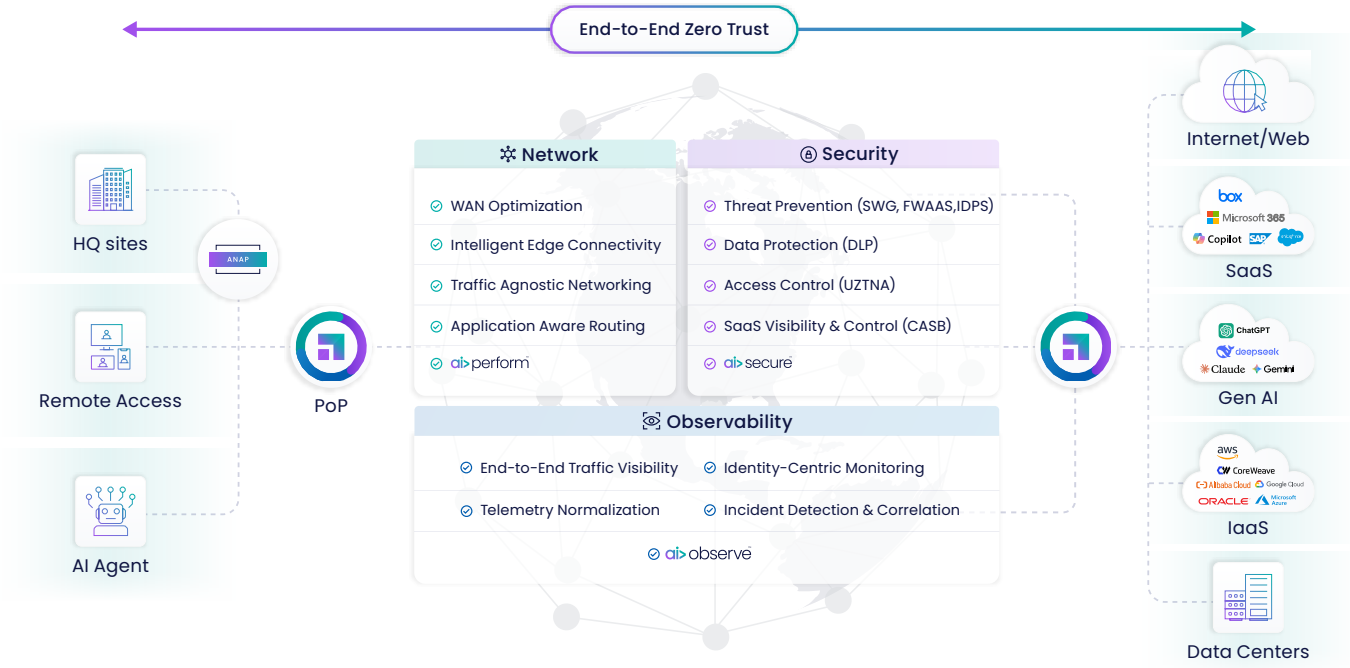
Moreover, leveraging a private backbone not only offers performance advantages but also brings several security benefits into play. Encryption of traffic over the Internet is common among SASE providers and while it may prevent attackers from deciphering the data, they can still gather valuable information. For instance, attackers could discern traffic volume patterns, packet lengths, the source/destination, and other metadata of the traffic. This intelligence can help attackers identify various attacks that they can launch later. Additionally, attackers may be able to inject traffic and launch DoS attacks. As we said before, reducing the attack surface is crucial in mitigating the likelihood of successful attacks. The Aryaka private core network plays a significant role in this by minimizing the attack surface, as it avoids utilizing the Internet backbone across countries for Inter-POP traffic.

Aryaka Unified SASE as a Service: Integrated Services Delivered on a Global Zero Trust WAN

Built on Aryaka's **global private backbone** and delivered through its **OnePASS™ architecture**, Aryaka provides a fully integrated suite of secure networking and observability services that eliminate the complexity of legacy and multi-vendor environments.

Unified SASE Capabilities Include:

- **Zero Trust WAN with Distributed Policy Enforcement:** Delivers consistent, high-performance connectivity and security across branches, remote users, and cloud workloads.
- **Integrated Networking & Security Services:**
  - **SD-WAN as a Service:** Optimized application routing and WAN performance delivered over Aryaka's global Layer 2 core network—replacing MPLS with better agility, performance, and cost-efficiency.
  - **Secure Remote Access:** VPNaaS and UZTNA services connect users securely from anywhere to applications hosted anywhere.
  - **Next-Gen Security Stack:** Unified security for branch and cloud deployments including NGFW, SWG, CASB, DLP, anti-malware, IPS, URL filtering, and geo-blocking.
  - **Multi-Cloud and SaaS Acceleration:** Direct cloud connectivity to hundreds of SaaS, IaaS, and UCaaS platforms with built-in acceleration via Aryaka's SDCI and application optimization technologies.
- **Observability & Insights:** The MyAryaka portal offers real-time insights, alerting, reporting, and policy management across networking and security in a co-managed model.
- **Flexible Delivery Options:**
  - Choose self-managed, co-managed, or Aryaka-managed deployments depending on your operational model and internal capabilities.
  - Integrated support for third-party firewalls and security solutions during transition phases.
- **Professional Services:**
  - Aryaka SmartHands and Day 0 services for installation, activation, and management—including hybrid deployments with 3rd party security infrastructure.
- **Last Mile Services:**
  - Global procurement and monitoring of wireline and wireless connectivity, managed end-to-end by Aryaka with proactive support via a centralized NOC.



Aryaka Flexible Delivery Options

Each transformation journey is different and each organization advances at their own pace. We meet organizations wherever they are on their transformative secure network access journeys. Organizations have varying skills, legacy products, and operational approaches. Our flexible delivery options and ability to integrate 3rd party security products allows us to tailor the journey to each organization's needs. It allows organizations to implement our solution their way, at their pace and to choose from self-managed, co-managed and Aryaka-managed service delivery. We like to say: It's your way, on your SASE journey.

Implementation Choice

- **Self-managed:** Configure, provision, monitor, and manage network and security policies via Aryaka's single web-based portal.
- **Co-managed:** Hand over some aspects to Aryaka or an Aryaka partner and keep others to yourself per your preference.
- **Aryaka-managed:** Leverage Aryaka and we take care as a single point of contact managed services provider.

Delivery Choice

- **Deploy Aryaka Services:** Leverage Aryaka technology and product features for network, security, and observability requirements.
- **Deploy a mix of Aryaka and 3rd party Services:** We meet you where you are for your deployment needs to maximize your existing security footprint investment and experience until you're ready to migrate to Aryaka.

How can I evaluate different providers?

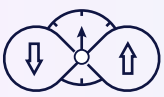
When considering a provider, organizations should evaluate them on several crucial criteria.

Management and monitoring: The provider should provide robust management and monitoring.

Security: The provider should offer a comprehensive security solution that can protect your organization from all types of cyber threats.

Network performance: The provider should have a reliable and fast network that can handle your organization's traffic without causing delays or downtime. Provider should have tools that allow you to monitor the performance and security of your network and make changes as needed.

Ease of deployment: The provider's solution should be easy to deploy and integrate with your existing IT infrastructure, without causing disruptions to your business operations.



Scalability: The provider should be able to scale its solution to meet your organization's growing needs, whether that means adding more users or expanding your network infrastructure quickly and efficiently.

Customer support: The provider should offer excellent customer support, including quick response times and knowledgeable technical support staff who can help you resolve any issues that may arise.

Aryaka Unified SASE as a Service vs Others

	Aryaka Unified SASE as a Service	SASE Technology Vendors	SASE Service Providers
Unified Single-Pass Architecture	OnePASS architecture: Enforce unified policy closet to users via distributed data plane	**Limited** Focus on single-line processing in the cloud for security services.	**Limited** Depends on Technology Vendor solution
Global Private Backbone	Zero Trust WAN with a private core network	**Limited** use of NSPs/CSPs Internet WAN	**Limited** Requires multiple SPs with inconsistent SLAs
Services Network, Security, Observability	Converged services with full control and insights; single data lake.	**Yes** but lack control of underlay network	**Yes** but stitched together Technology Vendor solutions
Flexible Delivery Options	Implementation and delivery choice. Consumption is always as a service.	**Limited** DIY or need SPs support	**No** Managed services focus

Transforming Global Secure Network Access is a Journey

As the network security landscape continues to develop, it is important to understand that the choice between these different SASE approaches is not black and white. Furthermore, SASE is not a one-time event, it is an ongoing journey comprised of a variety decisions impacted by existing investments, available skills and changing business needs.

Organizations must investigate their own unique requirements and strategic objectives to determine the transformation journey that's right for them.

Not every organization starts their journey at the same point. That is why Aryaka meets customers where they are on their journey to modernize, optimize and transform their networking and security environments.

Modernize

- MPLS to SD-WAN Migration
- Global Connectivity
- Secure Remote Access
- Integrated NextGen Firewall

Optimize

- Multi-Cloud & SaaS Acceleration
- AI Acceleration and Security
- Integrated 3rd Party Services

Transform

- Converged Networking and Security

No matter where you are in your global secure network access journey, Aryaka, the leader and first to deliver Unified SASE as a Service can help. Visit www.aryaka.com/products-and-services to learn more about going beyond SASE, and achieve a better experience.

About Aryaka

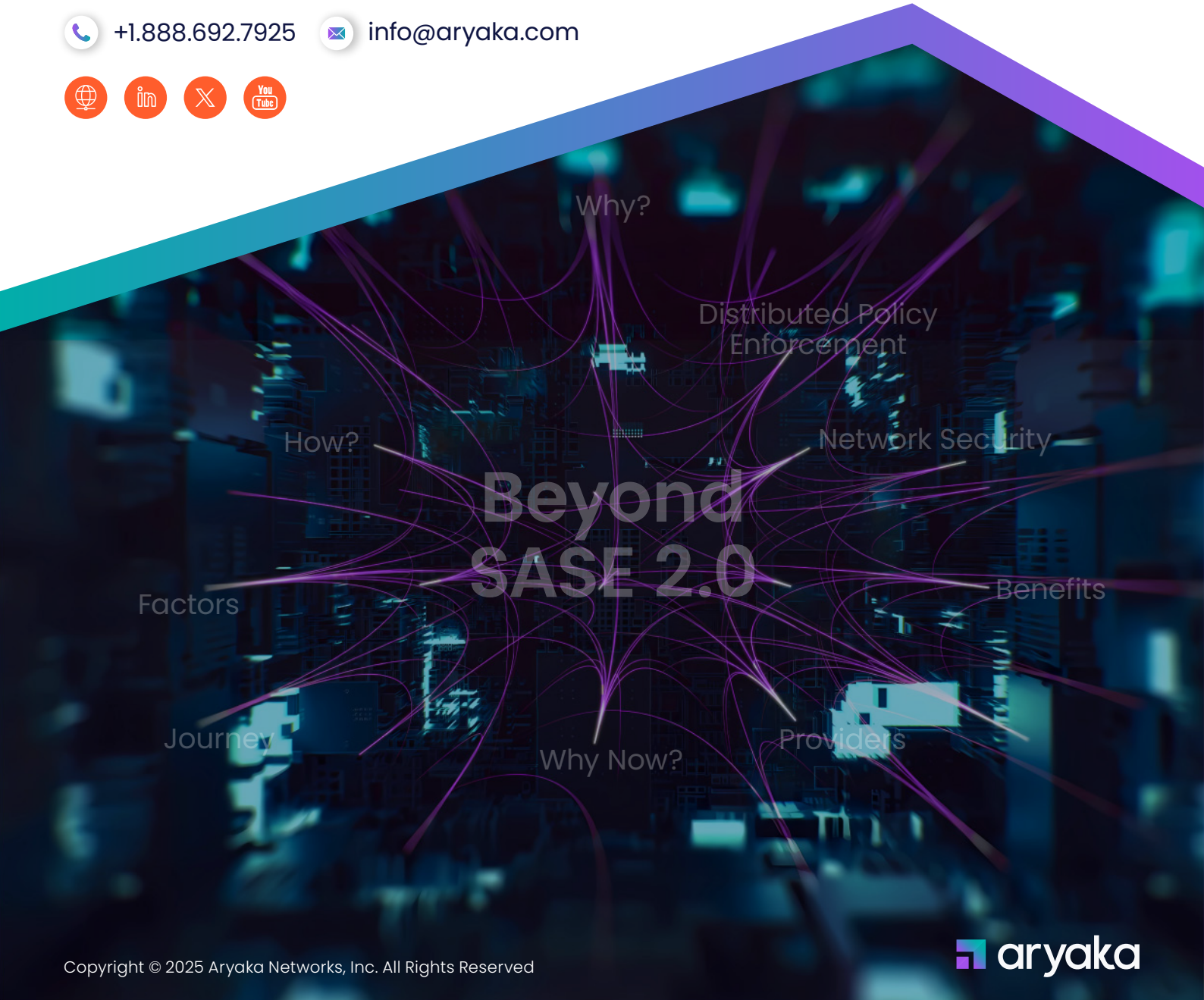
Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions. For more on Aryaka, please visit www.aryaka.com.

Schedule a Free Network Consultation with an Aryaka Expert

See How It Works Live

Contact Us

+1.888.692.7925 info@aryaka.com



aryaka