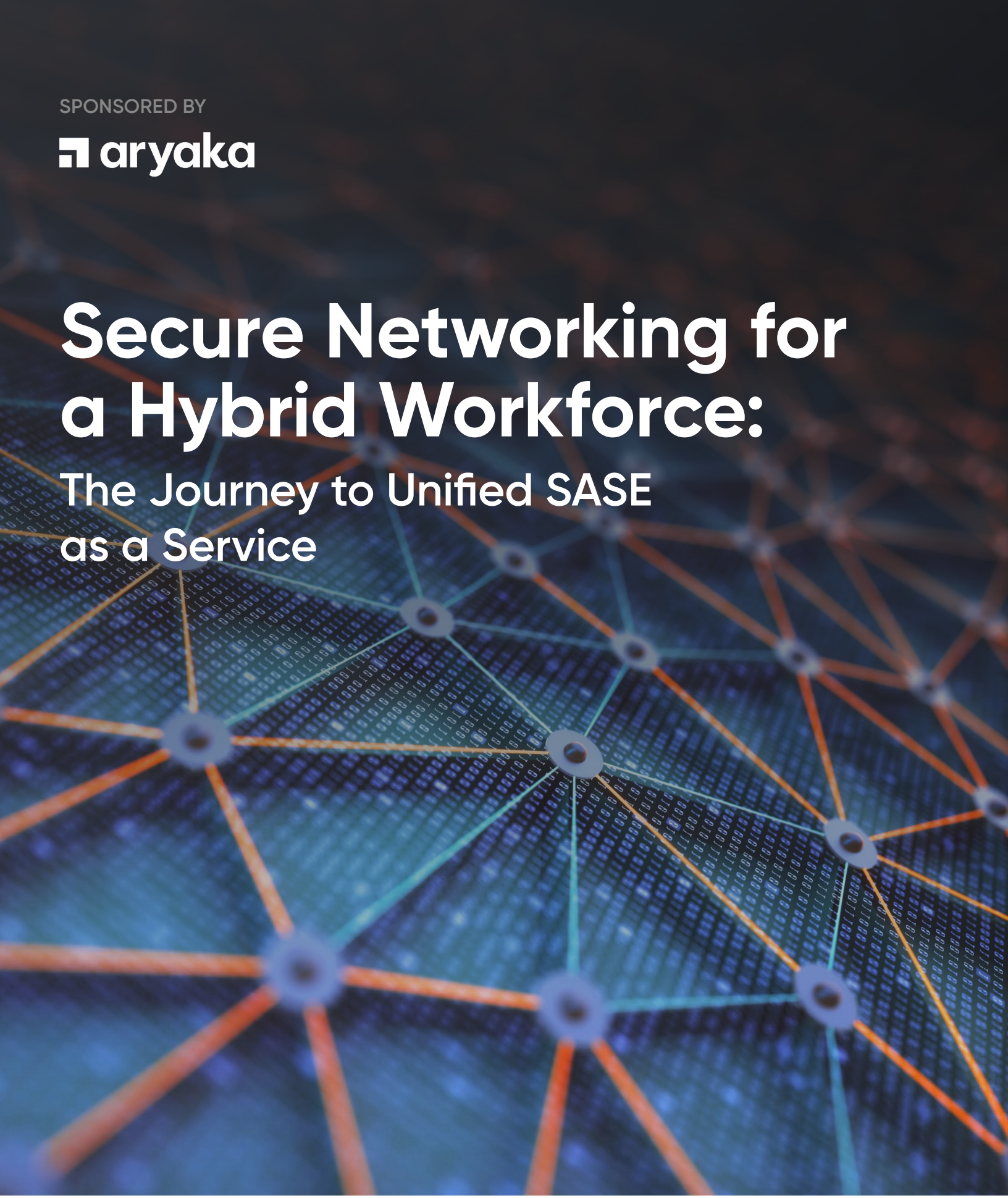
SPONSORED BY

aryaka

Secure Networking for a Hybrid Workforce:

The Journey to Unified SASE as a Service



SC Media

CRA Business Intelligence

ebook
An SC Media publication

Unified SASE as a Service

Security decision makers must ensure secure and performant application and data access to all users across distributed global networks without escalating cost, introducing risk or complexity, or damaging the user experience. The path is littered with potential challenges, including a larger attack surface, increased operational complexity and lack of agility. The key to lowering that risk and ensuring a secure, transparent user experience is Unified SASE as a Service. But where to begin? ***George V. Hulme*** *explains.*

Enterprise business-technology systems have shifted dramatically from on-premises applications to cloud-based applications and computing platforms. That's certainly no secret. What's less understood is how enterprises are getting the most value out of their systems through secure access, data protection, and maximized network management and availability.

"While enterprises are still moving to the cloud, so much of their environment is cloud-based today that the big challenges have changed from how to move to the cloud securely to how to manage and secure everything that's now in the cloud," said Michael Farnum advisory CISO at IT services provider Trace3.

The challenges associated with securing enterprise cloud systems are significant, and those challenges extend far beyond simply the technology. There's the now highly remote workforce that has forever changed how workers connect to enterprise cloud systems and how these cloud systems are networked for access throughout the enterprise, as well as finding the people with the cybersecurity skills necessary to protect these systems. Of course, ever-rising cybersecurity and regulatory risks put enterprise security teams under constant pressure.

Consider the sheer number of cloud applications with which enterprise security teams must contend. According to career site Zippia, the typical employee uses 36 cloud-based services daily, and the average enterprise relies on 1,295 discrete cloud services. That's a 27% increase from 1,022 cloud services used by enterprises in 2016. There's no sign of these trends slowing down. While the trend to moving more applications and data to the cloud is unabating, some will remain on-premises or in co-located data centers, asking IT and CISOs to deal with a hybrid environment. This adds to the complexity of managing and securing a dispersed and distributed enterprise environment.

There's also the fact that traditional security tools were not designed for cloud environments. These legacy tools silo security telemetry and complicate security analytics and threat detection. Additionally, network and security teams already have too many security products they must manage. According to some counts, there are up to 130 security tools within the typical enterprise. That's on top of the historic separation between security and networking teams.

With so many applications and network connections, it's also no longer viable to throw even more toolsets and technologies at cloud and security challenges.

The key to lowering that risk and ensuring a secure, transparent user experience is Unified SASE as a Service. But where to begin?

Using Aryaka's Unified SASE as a Service platform as the example, the following pages will provide details and guidance needed for the journey so organizations can modernize, optimize and transform their environments.

Market snapshot

Mauricio Sanchez, senior director for enterprise network and security research at Dell'Oro Group, said that by baking it into a unified cloud service, SASE promises to simplify IT operations, reduce security and networking complexity, and provide consistent security and performance to distributed workforces and the cloud resources they need to do their jobs.

For those reasons, the SASE market has enjoyed rapid growth. And while precise market estimates vary, projected annual growth rates range from 12% to more than 20% in the next few years. According to Dell'Oro Group, the overall SASE market is projected to grow to more than $16 billion by 2028 — that's an annual growth of 12% from 2019.

5 trends, 4 needs

A recent Aryaka study and report analyzed the key networking and security trends driving the need for Unified SASE as a Service. It includes the results of a survey of 202 C-level, VP, and director-level leaders at organizations in North America, EMEA, and Asia. Respondents were given filter questions to ensure they had a role in planning and managing IT and network services. Five key trends emerged from the research:

1. Networking and security technologies are converging. IT, security, and network professionals understand the benefit of convergence with SASE and SD-WAN to anchor it.
2. SASE and SD-WAN technologies are reaching maturity and they are now seen as legitimate solutions to provide modernized networking and security services.
3. Demand for new cloud services including AI, will drive the need for SASE and SD-WAN. Managed services and Network as-a-service will play a greater role in handling the complexity of cloud networks, AI, and hybrid workforce.
4. Hybrid everything is the future. This includes hybrid work, hybrid infrastructure, and hybrid security deployments.
5. Zero trust security approaches and application-level security will continue to be a key element of network services to support a hybrid everything future.

Respondents pointed to four areas where they need help navigating this environment:

1. Help in dealing with growing network and security complexity.
2. The need to embed and integrate a variety of security functions into a network with full visibility and control.
3. The need for more flexible network architectures to connect many different types of networks, including hybrid cloud infrastructure and remote work.
4. The desire to combine managed services with SD-WAN and SASE strategies to build a comprehensive, integrated secure network transformation. The survey audience sees this as a key strategy for the future, as SASE and SD-WAN technologies are now widely adopted and considered mature.

Trends driving the need for Unified SASE as a Service can be distilled into the following:

- **A hybrid workforce continues to drive cloud adoption**: With remote work and cloud computing, enterprise networks have sprawled. This has driven the appetite for cloud security and networks to converge so that security teams can provide their organizations secure access to data and applications.
- **Increased cyber threats**: The frequency of cyber threats has increased. Converged security and networking capabilities that provide accurate threat detection, precise prevention, and rapid response are essential.
- **Regulatory compliance**: Enterprises must comply with data protection and privacy regulations. Converged security and network technologies that provide data leak prevention, encryption, and granular access controls help enterprises more effectively meet regulatory demands.
- **Operational efficiency**: Converged network and security streamlines operations by consolidating multiple security and networking functions into a unified platform, enabling centralized management, visibility, and reducing complexity.
- **Cost optimization**: By converging networking and security, enterprises can reduce the need for multiple point products, lower capital and operational expenditures while improving overall security posture.

Common-sense security: The case for Unified SASE as a Service

During a recent SC Media panelcast, Sanchez made the case for Unified SASE as a Service along with Renuka Nadkarni, Chief Product Officer at Aryaka, and Reid Kreimeyer, an Aryaka customer and Senior Manager of IT Operations & Infrastructure at The Lauridsen Group, Inc.

“This clearly has been a very fast evolution, with the pace of digital transformation that most customers are doing,” Nadkarni said. “There are a lot of different dimensions to this change — a lot of stitched-together products that customers have in their environment.”

Kreimeyer explained the challenges this has presented for Lauridsen Group, a global manufacturing company with dozens of physical locations across multiple time zones and sometimes hundreds or thousands of miles between the end users that are using the technology and the nearest IT staff member:

“My role as the manager for infrastructure and operations is to architect those solutions and coordinate with other parts of the business that we have spread across the globe,” he said. “We're probably managing close to 2,000 information workers, and we're making technology decisions that are impacting people at the manufacturing plant floor. We're trying to secure for private data centers and AWS and Azure resources.”

Add to that dozens of vendor accounts and third-party integrations that are outside at the edge.

Kreimeyer continued, “In this environment, how do we secure our network from the manufacturing plant floor to the front office of that production facility? And how do we flow data back up to the enterprise? And then the inverse of that as well: How do we get people securely in from the edge, not just to cloud services that they may be using, but also potentially all the way down to the manufacturing floor?”

Kreimeyer ultimately determined that the best way to tame his environment was to invest in Unified SASE as a Service.

“Unified SASE, when it's presented as a service, provides a great way to improve security posture at scale, without having to have a huge investment,” he said.

Four Unified SASE as a Service Essentials

During the panelcast, Nadkarni outlined four core elements that power Aryaka's service:

OnePASS Architecture

A. Allows enterprises to perform comprehensive inspections and processing while examining a given data packet only once.

B. Ensures that every flow is 'run to completion' for all SASE functions – network services, NGFW, IDPS, SWG, anti-malware and others in the future.

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

Zero Trust WAN

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

B. Private Core backbone interconnects Aryaka POP locations through redundant and dedicated links.

C. Customers have the option to choose a private core backbone with specific bandwidth allocations for traffic between their offices.

D. Ensures that the traffic between the offices and the nearest POP locations are connected to leverages the private core.

Services: Networking, security and observability

A. SD-WAN: Deploys on a global core network optimized for cost and performance backed by global SLAs.

B. Multi-Cloud Connectivity: Connect to hundreds of cloud service providers in minutes.

C. SaaS Acceleration: improves the performance of SaaS applications for any user from anywhere in the world without hardware deployment or the overhead.

D. Security Services: Solutions for both branch and cloud deployments to optimally meet distributed enterprises' security requirements.

E. Secure Remote Access:

I. Fully managed VPNaaS for remote and mobile users Next-Gen Firewall–Secure Web Gateway, Anti-Malware and IPS: Unified security policies for both on-premises and remote workers

II. Managed Firewall Services: Integrated management of 3rd party firewalls Last Mile Services: Global procurement and management for wireline and wireless connectivity Professional Services: Aryaka Day 0 services for 3rd party managed Firewalls. Aryaka SmartHands to help with installation and activation of Aryaka Services.

Flexible delivery options

A. Meets organizations wherever they are on their transformative secure network access journeys.

B. Integrates 3rd party security products to tailor the journey to each organization's needs.

Conclusion: The Enterprise Journey to Unified SASE as a Service

For enterprises, there are three keys to succeeding in the move to Unified SASE as a Service, according to Nadkarni: modernization, optimization, and transformation.

Here's how Nadkarni defines each phase:

- **Modernization**: This is the replacing of legacy MPLS networks with a high-performance SD-WAN, combined with secure remote access. Modernization is the first step in evolving from traditional networking to a more agile, cloud-delivered model. "This is where you get everything under one hood, so you can see all of your sites and everything in one place. This is modernizing what you have," Nadkarni says.
- **Optimization**: Optimization refers to unifying all the enterprise cloud assets so that they're integrated well together. "You're using all of these different security vendors, how do you get that functionality and security while making sure your security controls can be enforced? This can include traffic steering, cloud acceleration, as well as any kind of security enforcement for different security capabilities," Nadkarni says.
- **Transformation**: In this step, enterprises fully move to SASE, delivered as a unified service, in the process obtaining networking, security, observability, and application performance into a single cloud-delivered platform. "You have everything now in a single pass architecture," Nadkarni says.

The key to success, experts stress, is for enterprises to move to Unified SASE as a Service based where their current networking and security environments and maturity levels reside, so they can modernize, optimize, and ultimately transform at their own pace.

By utilizing SASE as a service, organizations unify their SD-WAN as well as security through the enterprise next-generation firewall, secure web gateway, cloud access security broker, and zero-trust network access in a way that can be fully managed, co-managed, or self-managed. They can improve network and cloud availability while enabling security teams with the tools they need to secure access across enterprise cloud resources.

In the SC Media panelcast, Nadkarni described Unified SASE as a Service as “the dream come true” for organizations that make up the Aryaka customer base.

“We're trying to solve the problems that come with the pace of digital transformation, trying to (help customers) optimize the business and achieve cost savings without compromising on security.”

If Kreimeyer’s experience is any indication, Unified SASE as a Service has proven to be the right journey.

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, the Official Cyber Security Summit, TECHEXPO Top Secret, and now LaunchTech Communications. To learn more, visit CyberRiskAlliance.com.

SPONSORED BY

Aryaka converges network and security solutions to deliver Unified SASE as a Service, the only solution designed to deliver performance, agility, security and simplicity – without tradeoffs. Aryaka meets customers wherever they are on their secure network access journey, enabling them to seamlessly modernize, optimize and transform their networking and security environments.

Aryaka's flexible delivery options empower enterprises to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for cloud-based software-defined networking and security services.

MASTHEAD

EDITORIAL

SVP OF AUDIENCE CONTENT STRATEGY

Bill Brenner | bill.brenner@cyberriskalliance.com

SALES

CHIEF REVENUE OFFICER

Dave Kaye | dave.kaye@cyberriskalliance.com

DIRECTOR, STRATEGIC ACCOUNTS

Michele Guido | michele.guido@cyberriskalliance.com