

Untangling SASE: Secure Connectivity Without Complexity

What Enterprises and Service Providers Can Expect in 2025

RESEARCH BRIEF

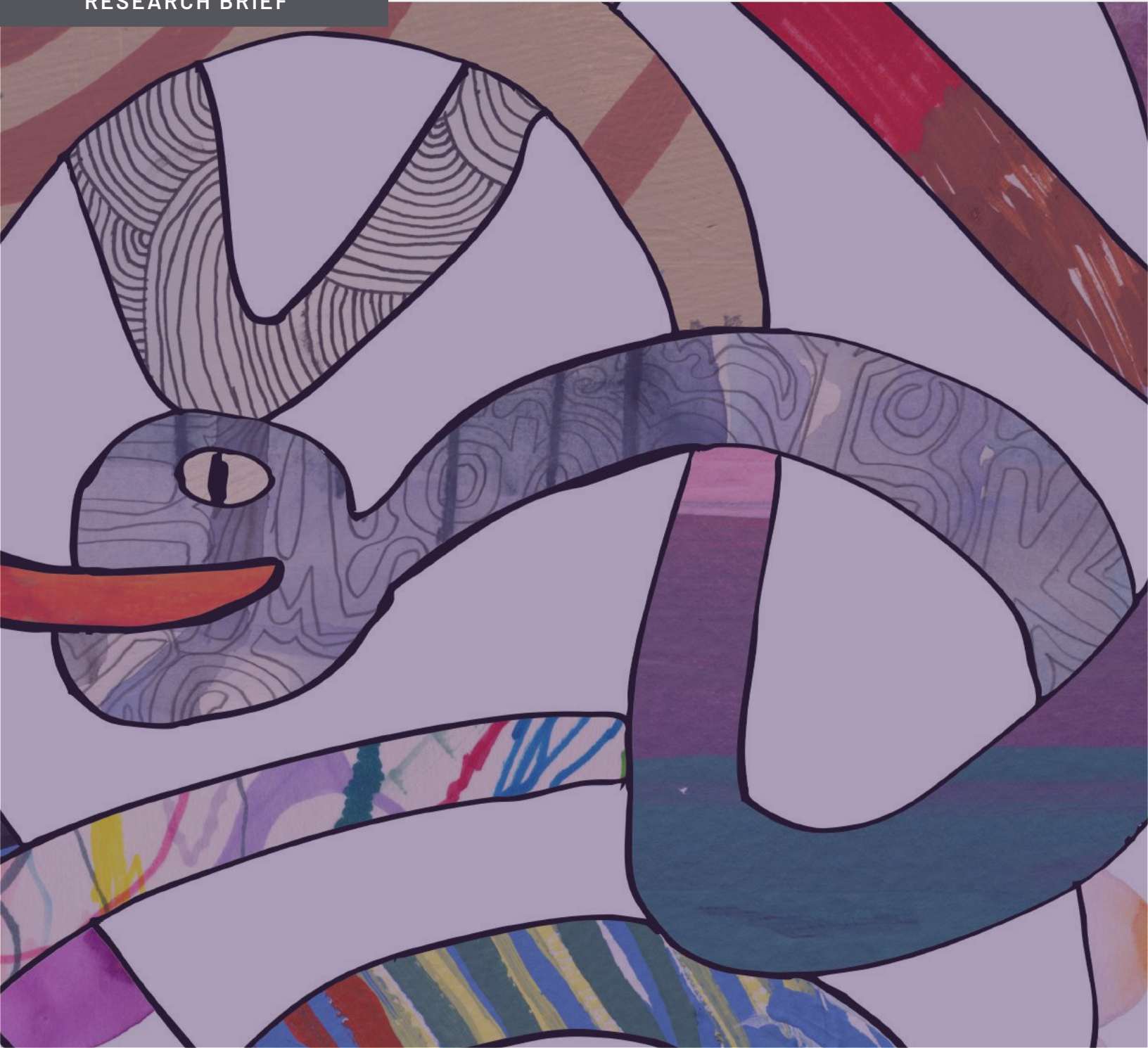


Table of Contents

Executive Summary 1

Introduction – SASE and SDWAN in 2025.....2

 SASE – What's in a Name? Everything.2

Market Drivers and Trends.....2

State of the SASE Market 4

Market Landscape and Select Vendor Examples.....5

 SD-WAN: Migration to SASE5

 SSE: Cloud Drives Rapid Growth with AI on Top.....5

 ZTNA: Gaining Ground but Challenging for Standalone Players.....6

 Multi-Cloud Networking (MCN): Evolving into Table Stakes.....6

 NaaS: The Rise of Service-Based Models6

 Standards for SD-WAN and SASE.....6

Managed Services Opportunity: Connectivity Plus Security7

 CSP SASE Opportunity.....7

 MSP SASE Opportunity7

AvidThink Observations on SASE7

 Playing the SASE Crosswords: Across and Up7

 Ever Evolving: From SASE to SASE 2.0?.....8

 The Transport Game: Overlays and Underlays, Agnostic and Specific.....8

 Zero Avoidance of Zero Trust.....9

 Pick Your Flavor: Single Vendor, Single Platform, Best-of-Breed9

 From Complexity to Simplicity 10

 Impact of AI and GenAI – It's Early Days..... 10

Parting Words..... 11

Untangling SASE: Secure Connectivity Without Complexity

What to Expect in 2025 from SASE, SSE, SD-WAN, and ZTNA

Executive Summary

The Secure Access Service Edge (SASE) market continues its robust growth trajectory, with market forecasts ranging from \$16B to \$25B by 2027-2028. This expansion outpaces traditional network security growth, driven by the persistent evolution of hybrid work models, accelerating cloud adoption, and an increasingly complex threat landscape. As organizations grapple with the challenges of securing distributed workforces and diverse cloud workloads, SASE has emerged as a framework that unifies networking and security capabilities, though the landscape remains complex with an abundance of vendor solutions and overlapping feature sets.

The market is experiencing significant consolidation through strategic acquisitions, with established players like Broadcom (VeloCloud), Cisco, Fortinet, Palo Alto Networks, and Zscaler leading the charge. The SSE (Security Service Edge) component of SASE is growing at twice the rate of SD-WAN, reflecting enterprises' prioritization of security. A notable trend is the increasing integration of AI capabilities, both for operational optimization and for addressing the security challenges posed by generative AI applications. However, this has also led to more sophisticated AI-powered threats, creating a technological arms race between defenders and attackers.

For CXOs navigating this landscape, several key considerations emerge: First, success in SASE implementation requires careful strategic planning before vendor selection, as no single product can address all security and networking needs. Second, while vendors debate the merits of unified platforms versus best-of-breed approaches, the optimal choice depends on each organization's specific requirements and existing infrastructure. Finally, while AI and automation promise to reduce complexity, they should be viewed as amplifiers of existing security practices rather than panaceas. Given the persistent talent shortage in networking and security, many organizations may benefit from considering managed services, though proper oversight and auditability remain crucial.

Research Briefs are independent content created by analysts working for AvidThink LLC. These reports are made possible through the sponsorship of our commercial supporters. Sponsors do not have any editorial control over the report content, and the views represented herein are solely those of AvidThink LLC. For more information about report sponsorship, please reach out to us at research@avidthink.com.

About AvidThink

AvidThink is a research and analysis firm focused on providing cutting-edge insights into the latest in infrastructure technologies. Formerly SDxCentral's research group, AvidThink launched as an independent company in October 2018. AvidThink's coverage includes 5G infrastructure, enterprise networks, private wireless, edge computing, SD-WAN, SASE, SSE, ZTNA, cloud infrastructure, and infrastructure security. Our clients range from Fortune 500 enterprises and hyperscalers to tier-1 communications service providers, fast-growing unicorns, and innovative startups. AvidThink's research has been quoted by Forbes, the Wall Street Journal, Light Reading, Fierce Networks, Mobile World Live, and other major publications. Visit AvidThink at avidthink.com.

Introduction – SASE and SDWAN in 2025

The Secure Access Service Edge (SASE) framework is a strategic move by a leading analyst firm to identify, name, and brand a collection of well-established but aging product categories in enterprise connectivity and network security. Readers of past reports will recall our observation that this veritable **alphabet soup** of acronyms can confuse even well-informed CISOs.

What SASE accurately captures is the ongoing convergence of network connectivity and security. As enterprise networking and cybersecurity needs evolve in response to today's business needs, the legacy product categories of past decades are in transition. SASE is a high-level framework encompassing many of these categories.

SASE – What's in a Name? Everything.

Unfortunately, this "kitchen sink" approach to consolidating a collection of services under two major umbrellas has created challenges. CISOs today face a diverse array of vendors (and managed service providers) advertising a growing and messy list of checkbox capabilities under the two sub-umbrellas of SASE – namely SD-WAN and SSE – that include ZTNA, IPS, DLP, NGFW, WAN Optimization, CASB, SWG, RBI, FWaaS, and other three- and four-letter acronyms¹.

Adding to the confusion, vendors are redefining these categories (declaring theirs as versions 2.0, 3.0, and 4.0) while bundling in new capabilities like multi-cloud networking (MCN) and extended detection and response (XDR), local area network (LAN) features like Wi-Fi protection and network access control (NAC), and internet of things (IoT) device protection (including internet of medical things – IoMT and industrial internet of things – IIoT). These marketing-led redefinitions create more headaches for CISOs as they sort through the spaghetti of solutions.

Even if they successfully navigate the acronym alphabet soup, CISOs still have to contend with deploying and managing these solutions. Current SASE implementations include extensive lists of security and networking features, but lack streamlined management capabilities, forcing operators to flip through multiple user interfaces instead of using a single management console ("swivel tab management").

Within these ongoing developments, this updated report continues our efforts to help enterprise and service provider readers untangle the complex topics of SASE, SD-WAN, SSE, and ZTNA. We examine current market trends and provide an updated landscape to help IT decision-makers navigate this evolving market. Feedback is welcome at research@avidthink.com.

Market Drivers and Trends

There are two fundamental drivers for SASE: (1) reliable, high-quality connectivity to support productivity and (2) robust security to protect the integrity of data communications and enterprise IP. The key components of SASE are designed to overcome the limitations of underlay networks (MPLS, direct internet, wireless WAN, satellite) and secure traffic against cyberattacks. For the many years we've tracked SD-WAN and SASE, one number consistently increases: the number of breaches (and the number of cyberattacks on corporations). For 2024, the 17th edition of Verizon's venerable Data Breach Investigations Report (DBIR)² shows a record-high 10K+ breaches impacting victims in 94 countries. This ongoing cat-and-mouse game between cyber attackers and defenders ensures that security-focused IT spending will remain a significant portion of corporate spending.

Beyond cyberattack trends, we've previously covered the business, technology, geopolitical, societal, and lifestyle trends that impact how enterprises connect people (employees, contractors, and partners) to company applications and data resources. Instead of rehashing content from past reports, much of which remains relevant, we'll summarize the key trends and highlight any changes in the past year:

¹SD-WAN: Software-Defined Wide Area Network, SSE: Secure Services Edge, ZTNA: Zero-Trust Network Access, CASB: Cloud Access Security Broker, DLP: Data Loss Prevention, SWG: Secure Web Gateway, RBI: Remote Browser Isolation, FWaaS: Firewall as a Service, IPS: Intrusion Prevention System, NGFW: Next-Generation Firewall

²"2024 Data Breach Investigations Report," Verizon Business, 2024.

Even if they successfully navigate the acronym alphabet soup, CISOs still have to contend with deploying and managing these solutions. Current SASE implementations include extensive lists of security and networking features, but lack streamlined management capabilities.

- **Work Habit and Location Changes:** The hybrid work model has matured beyond its pandemic origins, creating persistent security challenges. Return-to-office (RTO) mandates from leading companies like Amazon and Apple and financial institutions like Barclays, Citigroup, and JP Morgan Chase complicate cybersecurity enforcement. Three to four workdays in the office combined with one to two WFH days increase the complexity of enabling consistent access controls. Organizations continue to manage a complex matrix of access scenarios, with employees connecting from diverse locations — including home offices, manufacturing sites, and temporary locations — using an increasingly varied device ecosystem. This shift continues to pressure networking and security teams to refactor their access control strategies in favor of zero-trust-based approaches.
- **Workload and Topology Changes:** Enterprise workloads continue their migration toward SaaS and distributed architectures, with multi-cloud and hybrid deployments becoming standard practice. Increasing AI and generative AI (GenAI) workloads drive hybrid infrastructure architectures as enterprises consume managed AI services while seeking spare GPU cycles to rent. Traditional hub-and-spoke network designs are inadequate for these new patterns. Likewise, whether hardware- or software-based, legacy VPN solutions struggle to scale with these emerging requirements, driving strong enterprise interest in SASE and zero-trust architectures.
- **Cybersecurity Regulation and Insurance:** The expanding attack surface created by network decentralization has caught the attention of regulators and insurers. NIST's updated Cybersecurity Framework reflects this concern, emphasizing zero-trust architectures and cloud security. Similarly, the European Union's NIS2 Directive (2022/2555) introduces key requirements for essential and vital entities to comply with by Oct. 17, 2024, or face significant penalties. Even small and medium enterprises (SMEs) in critical sectors must comply. Meanwhile, cyber insurance providers are raising their security requirements, mandating stronger controls and network segmentation. Organizations are increasingly required to demonstrate comprehensive security measures before obtaining or renewing coverage.
- **Convergence of IT and OT:** Operational technology continues to evolve as industrial devices adopt standard internet protocols and APIs. This convergence of IT and operational technology (OT) systems presents unique security challenges, particularly in manufacturing, healthcare, and transportation. Organizations seek unified security approaches that protect traditional IT assets and industrial systems without compromising operational efficiency. SASE vendors like Cato Networks³ have started adding IoT/OT capabilities to their solutions, and private wireless vendors like Ericsson are beginning to converge their zero-trust solutions (with ZTNA and RBI capabilities) with their private 5G capabilities.
- **Convergence of Dev and IT:** The proliferation of in-house software development and AI initiatives creates new security requirements. Organizations must secure complex hybrid cloud deployments while enabling efficient data transfer for AI workloads. Traditional developer access and application security approaches are insufficient for these modern workflows. While SASE evolved from a network security foundation, we're seeing the ZT, CASB, and RBI elements converge with privileged access management (PAM) and privileged identity management (PIM) platforms for application and developer use cases.
- **AI, AI, and AI:** The AI hype, particularly around GenAI, impacts the SASE market in two ways. Previously, AI and machine learning (ML) were used to optimize SD-WAN networks and detect malicious activity in SSE products. Those capabilities continue to evolve and improve with the arrival of transformer models and GenAI. New ML models and GenAI can improve troubleshooting and incident handling. AI is also being applied across all stages of the networking and security product deployment and management lifecycle. For more information on this, we recommend our [recent AI in Networking report](#). The other major impact of AI on SASE, especially for vendors with DLP and CASB capabilities, is enforcing enterprise policies on using GenAI services — controlling access to services and the type of data uploads allowed.

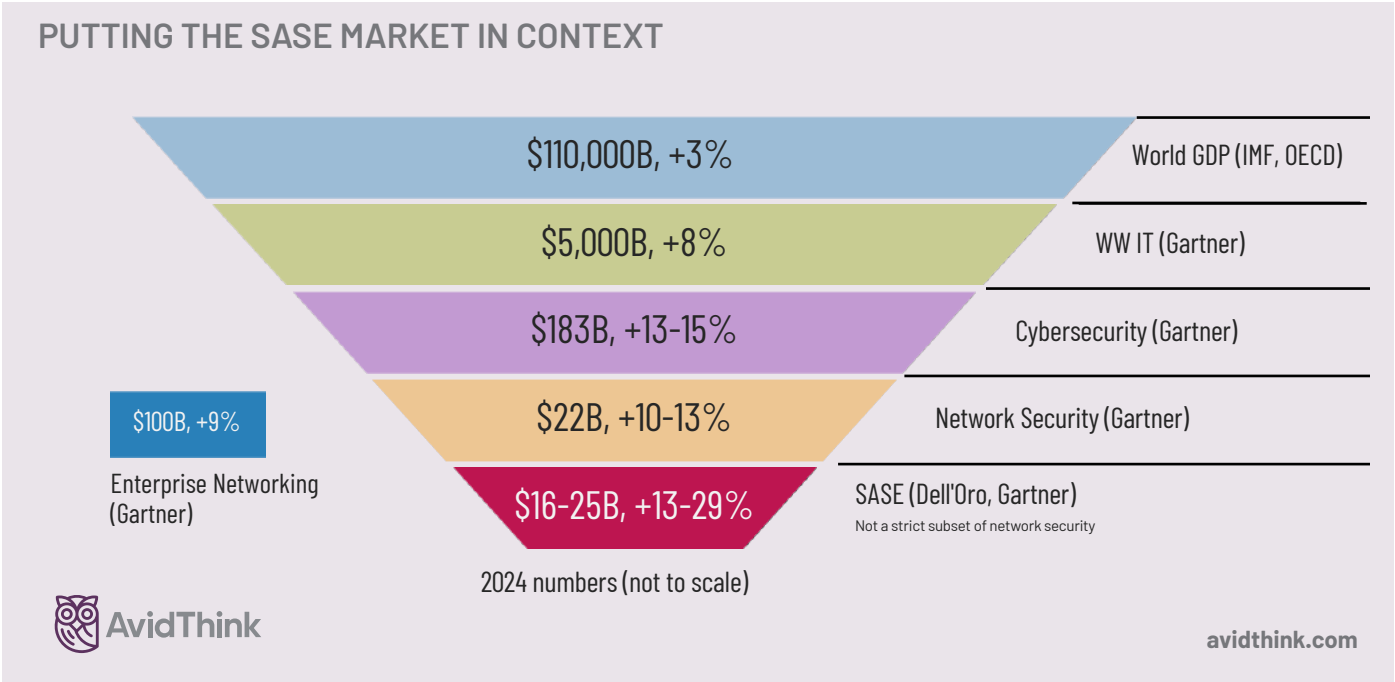
These trends provide a clear direction: enterprises are moving beyond traditional perimeter-based security toward integrated architectures with security controls embedded throughout the network fabric. All major SASE vendors have incorporated zero-trust principles and ZTNA features into their products, and we expect this trend to continue.

³Cato Networks Introduces Industry's First SASE-native IoT/OT Security Solution," Cato Networks, Dec. 10, 2024

State of the SASE Market

The SASE market continues to grow, with fellow analyst firms pegging the market size for SASE at between USD 16B by 2028 (13% CAGR)⁴ and USD 25B by 2027 (29% CAGR)⁵. Other estimates include a market size of USD 24B by 2029⁶, though these figures may underestimate the total value and growth rate of the SASE market.

To put the SASE market in context, let's look at other related markets. The network security market was about USD 22B (10-13% CAGR) in 2024⁷, while the enterprise networking market is at USD 100B (9% CAGR)⁸. Cybersecurity is at USD 180B (13-15% CAGR)⁷,



SASE is projected to grow more rapidly than network security, which is unsurprising since it's consuming existing categories and becoming the top-level aggregation of all enterprise edge and WAN security, plus it's subsuming enterprise networking elements.

The SSE component of SASE, which encompasses ZTNA, CASB, SWG, and RBI, will grow faster than the SD-WAN component (analyst firm Dell'Oro indicates more than 2X). This is expected since much of the initial boom in SD-WAN during the pandemic years has subsided, and there are more RTO efforts than a drive to WFH.

As networking and network security vendors continue to jump on the SASE bandwagon – for lack of a better category – the revenues attributed to SASE will keep growing. We anticipate this will continue until another re-categorization of the space occurs.

At this point, there's no leading candidate to replace SASE as an umbrella framework. However, AvidThink believes that any new top-level category that emerges will likely be built on the foundations of zero trust since that's the framework governments use to assess enterprise and public sector security implementations.

⁴"SASE Growth Diverging: SSE to Outpace SD-WAN Revenue Nearly Two to One," Dell'Oro Group, Aug. 05, 2024

⁵"Forecast Analysis: Secure Access Service Edge, Worldwide," Gartner, 2023.

⁶SD-WAN and SASE: worldwide forecast 2024-2029," Analysys Mason, Oct. 21, 2024.

⁷"Gartner Forecasts Global Information Security Spending to Grow 15% in 2025," Gartner, 2025.

⁸"Forecast: Enterprise Network Equipment by Market Segment, Worldwide, 2022-2028, 2Q24 Update," Gartner, 2024

⁹Gartner Forecasts Worldwide IT Spending to Grow 7.5% in 2024," Gartner, 2024.

¹⁰"World Economic Outlook Update, July 2024: The Global Economy in a Sticky Spot," IMF, Jul. 16, 2024

Market Landscape and Select Vendor Examples

The past year saw consolidation in the market, with leading network security vendors continuing to establish their dominance. For instance, Broadcom (which already owned security firm Symantec) closed on its VMware acquisition but now markets its VeloCloud SD-WAN and SASE products under the VeloCloud brand. Other major players in SASE (SD-WAN + SSE) include cloud-security firm Zscaler, IPO candidate Netskope (which crossed \$500M in annual subscription revenue in 2024 and was last valued at \$7.5B in a 2021 funding round), and security leaders Cisco, Palo Alto Networks, and Fortinet. To expand its ZT offerings and reach in OT, Zscaler bought OT zero-trust specialist Airgap in April 2024. Meanwhile, Fortinet purchased Next DLP in August 2024 to bolster its Unified SASE platform.

Other established security firms, like Check Point and SonicWall, have initiated M&A transactions to expand their reach in SASE. For instance, Check Point has been integrating Perimeter 81, acquired in August 2023, as its Check Point SASE solution. SonicWall bought ZTNA company Banyan Security in January 2024 to bolster its ZT offerings. Cloud security firm Cloudflare acquired BastionZero in May 2024 to add zero-trust infrastructure controls (developer-focused) to its SASE network.

We expect M&A activity to continue into 2025 as product lines converge to meet the requirements of enterprises looking for streamlined and unified offerings. This will drive ongoing market consolidation and likely continued "platformization" of SASE (and cybersecurity). Palo Alto Networks CEO Nikesh Arora's public bet on platformization¹¹ — a unified approach that favors a bundled, integrated solution — ignited a debate within the cybersecurity community in 2024 around best-of-breed versus unified single-vendor solutions. We'll discuss this later in our discussion of single-vendor, single-platform, and best-of-breed approaches to SASE.

Next, we'll cover the trends in each major SASE sub-category.

SD-WAN: Migration to SASE

The SD-WAN market is experiencing a shift as pure-play vendors lose ground to integrated SASE solutions. When leading SD-WAN vendors like VeloCloud, Cisco, and Fortinet push top-level SASE messages, and carrier-centric companies like Ericsson talk about their NetCloud SASE and Zero Trust solutions, there's no debate about future directions.

Case in point, VeloCloud by Broadcom (previously VMware VeloCloud SASE and SD-WAN) is a market leader from the SD-WAN space that transitioned into SASE, now with security capabilities from Broadcom's Symantec division (providing SSE, ZTNA, and more). Over the years, VeloCloud has evolved by adding new edge hardware devices, security features, improved orchestration, better application recognition capabilities, and embracing 5G as a natively supported transport. More recently, VeloCloud introduced its VeloRAIN (Robust AI Networking) architecture. With VeloRAIN, VeloCloud SD-WAN leverages AI and ML to detect AI applications and provide improved controls and quality of service. As part of this, VeloCloud features Dynamic Application-Based Slicing (DABS), which provides QoS regardless of the underlying transport that may span multiple networks.

As another example, Aryaka started as a network-centric company but has evolved since its founding in 2009. Previously a focused SD-WAN solution provider, Aryaka has grown organically and through acquisitions. It differentiates its offering with a converged platform offered as a service, termed "Unified SASE as a Service." Incorporating built-in security features like an NGFW, IPS, CASB, and SWG, and adding zero-trust capabilities, Aryaka is on track to add more controls, smarter detection, and threat protection over the next 12 months while expanding the list of applications it can protect (e.g., AI applications). As with other vendors, it's adding AI-enabled operations to reduce OpEx overhead for its customers.

Mid-market SD-WAN specialists exist, but many offer joint SD-WAN with managed connectivity solutions, sometimes as a white-label offering under an MSP or CSP.

SSE: Cloud Drives Rapid Growth with AI on Top

SSE adoption is accelerating as enterprises prioritize securing their cloud environments. Vendors like Zscaler, Netskope, and Palo Alto Networks lead the charge by offering robust SSE solutions that integrate with existing SD-WAN deployments. Vendors without robust SSE initially integrate into these partner offerings from their SD-WAN platforms but may later offer their own versions of SSE to capture margins.

¹¹"Palo Alto Networks CEO: 'We Firmly Believe' Dramatic Shift In Growth Strategy Will Pay Off," CRN.com, 2024.

As we mentioned earlier, in the last 18 months, SSE providers have jumped on the AI bandwagon, adding fine-grained controls to allow or disallow GenAI-as-a-service providers like OpenAI ChatGPT, Anthropic Claude, and Google Gemini as part of CASB controls. They are applying their DLP logic to control the type of sensitive data that can and cannot be submitted to these services. Some also provide controls over access to private GenAI implementations, protecting enterprise private language model services with a network security layer.

ZTNA: Gaining Ground but Challenging for Standalone Players

ZTNA is gaining prominence as a critical component of SASE. We're most bullish about the growth of ZT (of which ZTNA is a subset) applied across multiple domains: application access, developer environments, cloud platforms, IT infrastructure and services, and OT infrastructure.

Standalone startups in this space have yet to see significant traction. In past years, we've covered Perimeter 81 (acquired), Banyan Security (acquired), Tailscale, Appgate, TwinGate, and more recent startups like CloudBrink (with the added benefit of end-to-end optimization, which it claims dramatically improves throughput). None have achieved breakout success to date, and they continue to battle ZTNA solutions from incumbents, including Zscaler and Cloudflare, which leverages its enormous worldwide edge footprint. Also in the mix is Cato Networks, which offers ZTNA as part of its SASE offering, and Versa Networks, an early SD-WAN player that has added a breadth of SASE features, including ZTNA.

By enforcing identity-based (generalizable to attribute-based) access control, ZTNA minimizes the risk of unauthorized access. However, implementing ZTNA or any ZT framework requires significant changes to enterprise processes and infrastructure, presenting a barrier to adoption.

Multi-Cloud Networking (MCN): Evolving into Table Stakes

Vendors like Alkira and Aviatrix have pioneered multi-cloud networking (MCN) solutions that simplify connectivity across diverse cloud environments. While MCN does not inherently include security features, it complements SASE by enabling secure, scalable multi-cloud architectures. More recently, SASE vendors are touting multi-cloud capabilities as part of their ZT and SD-WAN offerings.

Some leverage virtual proxies installed in cloud environments to facilitate secure overlay-based connectivity across hybrid clouds (public and private data centers). However, without visibility into or orchestration of the underlying networks (network underlay), the multi-cloud capabilities of general SASE solutions are limited to data protection, without the ability for optimization or fine-grained routing controls. Likewise, networking performance in throughput, latency, and loss may lag in generic offerings. Nonetheless, not all enterprises need the control or performance these specialists provide.

NaaS: The Rise of Service-Based Models

Separate from SASE, there's growing momentum in the Network-as-a-Service (NaaS) business model. Initially focused on campus LAN Wi-Fi and switching, we're seeing SASE components (including SD-WAN and SSE subsets, including ZTNA) integrated into these Campus NaaS offerings. Vendors seek to provide a managed (full or partial) unified platform that addresses networking and security needs. For more information on the enterprise uptake of this fledgling business model, [check out our Campus NaaS report](#).

Standards for SD-WAN and SASE

The SASE market is like the Wild West, with many product categories and diverse vendors. Feature definitions are fluid, with different vendors interpreting category capabilities slightly differently. While analyst firms have tried to dictate minimum feature sets or capabilities, vendors have much room for interpretation. Nonetheless, the market's chaotic nature hasn't dampened SASE's growth. Perhaps it has, and growth rates would be higher otherwise, but it's impossible to predict the counterfactual.

The MEF, a global industry association representing network, cloud, and technology providers, has been working on standardizing SD-WAN and SASE to help streamline adoption and ensure interoperability. Initiatives like MEF 70.1, 117, and 118 standards define key attributes for SD-WAN, SASE services, and a zero-trust framework, offering a roadmap for vendors and enterprises. The SASE initiative has early momentum, with vendors like VeloCloud (Broadcom), Fortinet, Versa Networks, and Palo Alto Networks certifying their products. The long-term success of MEF's initiatives will depend on its service provider members requiring their security and networking vendors to conform.

Managed Services Opportunity: Connectivity Plus Security

The ongoing evolution of the market presents mixed opportunities for CSPs and MSPs. All the vendors mentioned provide direct-to-enterprise offerings but also leverage indirect channels to market. With the Campus NaaS movement, we could see more vendors take on managed services themselves to preserve margins and obtain direct learnings from working with customers (particularly to gain security intelligence). At the same time, even SASE vendors previously hostile to CSPs, like Cato Networks, have embraced CSPs in the past few years as part of a wider go-to-market initiative. Most SASE vendors recognize that CSPs (and MSPs) have trusted relationships with enterprise customers (especially SMEs) and can play a vital role in market expansion.

By leveraging existing relationships with enterprises and their expertise in underlay networking, CSPs can provide value-added services that align with SASE principles.

Regardless, the expansion of capabilities in SASE offerings means that CSPs and MSPs who want to continue to add value will need to improve their in-house security capabilities and expertise. Cybersecurity know-how will be the primary reason SMEs (or large enterprises) rely on MSPs and managed services at CSPs.

CSP SASE Opportunity

CSPs are uniquely positioned to capitalize on the SASE market by integrating security features into their connectivity offerings. By leveraging existing relationships with enterprises and their expertise in underlay networking, CSPs can provide value-added services that align with SASE principles. We believe the fastest monetization opportunity on top of connectivity offerings – wireline or wireless (mobile and FWA) – is a security feature add-on for managed SASE (or a subset).

MSP SASE Opportunity

Managed service providers (MSPs) can continue differentiating by offering tailored, converged SASE solutions that address specific industry needs. Vertically focused MSPs, for instance, can integrate compliance and data sovereignty requirements into their offerings, appealing to regulated industries like healthcare and finance. As ZT capabilities in these products expand, we anticipate that MSPs will be relied on to implement vertical-related controls in different industry environments (factories, hospitals, clinics, etc.) that improve security across IT and OT while maintaining compliance.

AvidThink Observations on SASE

Over the last decade, we've tracked the emergence of SD-WAN through its extension into branch and campus networks (SD-LAN, SD-Branch), the move to SASE, the SSE split, and now the ZT movement. We've consulted for networking and security vendors, tier-1 SPs, and MSPs. We've learned a few things throughout this evolution and will share our updated observations on this market.

Playing the SASE Crosswords: Across and Up

Three domains are relevant to SASE: IT, OT, and developers (Dev). We've seen SASE solutions span across IT and OT domains, addressing standard IT resources like servers, laptops, and mobile phones, but also OT devices like robots and AGVs on factory floors, security cameras in warehouses, or infusion pumps at hospitals. The next reach-over will likely be the Dev domain. As ZT frameworks become more prevalent and we see increased convergence between network and application controls, developers

will leverage ZTNA solutions to access private and public cloud resources and remote servers and devices. This upward convergence between network and applications will result in more ZTNA solutions that integrate with enterprise identity services and policy solutions, and integration with PIM and PAM systems more common with application and operating system access control.

Ever Evolving: From SASE to SASE 2.0?

Related to the cross-domain and application stack expansion above, we expect existing vendors to expand their offerings even as the market consolidates through M&A (and unsuccessful vendors shut down). The typical journey starts with SD-WAN, and then NGFW and other essential SSE services like SWG and DNS security are added. Following are content security features, including DLP, CASB, and RBI. Beyond that, we see ZTNA and endpoint protection features added, at which point IoT and OT support are folded in. A quick follow-up is building or integrating with XDR, SIM, and SOAR capabilities.

After this, we expect ZTNA to start converging with application access control systems like PIM/PAM, followed by cloud workload controls and cloud micro-segmentation as possible additions. When vendors reach this level of comprehensiveness, we'll be hard-pressed to call this SASE, no matter what version number we append to it. However, we anticipate this will take a few years, by which time some leading analyst firms will create a new category.

The Transport Game: Overlays and Underlays, Agnostic and Specific

One of the selling points for SD-WAN was its transport agnosticism — regardless of MPLS, direct internet over a fiber link, 4G LTE/5G, or satellite, the overlay solution was guaranteed to work. Vendors then added more visibility and controls to the underlay to improve troubleshooting and QoS — link bonding, forward error correction, WAN optimization, and transport-specific optimizations (particularly for wireless access).

However, with government standards mandating zero trust and increasing threats across all attack surfaces (including GenAI-enabled deepfakes and personalized social engineering attacks at scale), enterprises have little choice but to embrace ZT.

As a vendor example, Ericsson Enterprise Wireless Solutions, which continues to use the well-recognized Cradlepoint branding in its product lines, seeks to differentiate its solutions with unique wireless-centric capabilities. Ericsson's NetCloud SASE provides cellular-centric SD-WAN with increasing security and zero-trust capabilities (seeded with cloud security, RBI, and ZT capabilities from their Ericom acquisition).

With fixed wireless access and mobility becoming more important to enterprises, we anticipate this positioning will gain traction. Furthermore, Ericsson's enterprise-centric private wireless and neutral host coverage extension solutions are available through its Ericsson Enterprise 5G suite and are part of an enterprise-focused GTM, providing joint capabilities into converged OT and IT environments in specific enterprise verticals (manufacturing, logistics, etc.). This unification of the different enterprise connectivity offerings and the establishment of a zero-trust foundation align with our market observations.

Other vendors have embraced the importance of visibility into the underlay.

VeloCloud also touts 5G wireless awareness and recently introduced DABS for improved QoS controls. Meanwhile, Cisco has integrated ThousandEyes for visibility into its Cisco Meraki Secure Connect SASE platform.

Similar optimizations abound in the multi-cloud connectivity space, leveraging private backbones and points-of-presence (persistent and on-demand) to improve performance and reduce egress costs.

Moving forward, we anticipate increased use of underlying telemetry in conjunction with AI/ML algorithms to improve QoS and security over underlying transports — transport agnosticism for capacity, reliability, and resilience, but with underlay intelligence for QoS, including latency.

Zero Avoidance of Zero Trust

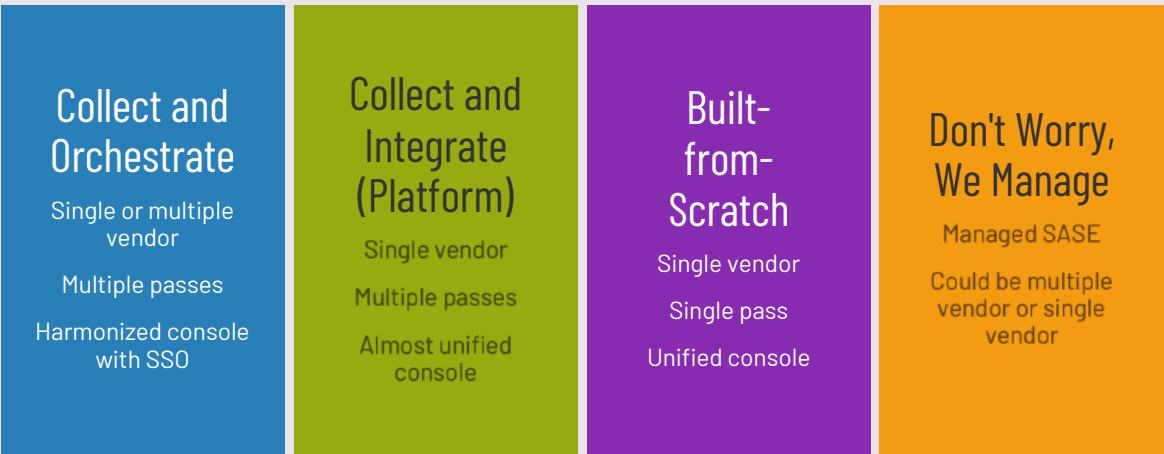
Implementation of zero trust can be difficult, even painful. It can be a huge challenge to identify roles, identity stores, sources of policy, and pools of telemetry and analytics and try to tie it all together in a normalized and standardized fashion. However, with government standards mandating zero trust and increasing threats across all attack surfaces (including GenAI-enabled deepfakes and personalized social engineering attacks at scale), enterprises have little choice but to embrace ZT. There's an opportunity for vendors and CSPs/MSPs to step in and help reduce the barriers to ZT adoption. The more automation, intelligence, and guidance built into products, the better for vendors and enterprise customers. We see plenty of fertile ground here for innovative companies to step in and take ZT to the next step. For enterprises, ZT doesn't have to be rolled out across all domains in a day – triaging and prioritizing where ZT can add the most value allows a staged rollout that can improve cyber-resilience at each milestone.

Pick Your Flavor: Single Vendor, Single Platform, Best-of-Breed

We expect the ongoing positioning battle between vendors (and service providers) about which approach is "best" to continue into 2025 and beyond. The arguments are self-serving, justifying how they arrived at their respective solutions, and buying themselves time to build their ultimate solution (with the architecture they aspire to reach). The basic factions are:

- **Collect and Orchestrate:** Whether single or multiple vendor solutions, this collection of "best-of-breed" products is loosely integrated with a harmonized console (single sign-on for convenience). Traffic goes through multiple passes, which isn't ideal, but because each individual component in the chain is "best-in-class," the results may be acceptable as long as latency is not an issue.
- **Collect and Integrate:** This is the "platform" approach, where a single vendor (usually large) has integrated multiple product lines (in-house or acquired) into a single unified console (with quirks that need ironing out and siloed features) to ease configuration. Traffic may still take multiple passes under the hood.
- **Built-from-Scratch:** These come from less established upstarts who've built their new single-vendor platforms from the ground up with single-pass architectures and a unified console. Many are working hard to round up the networking and security capabilities while trying to avoid the trap of increasing complexity as they enrich functionality.

ONGOING DEBATE: SINGLE VENDOR, SINGLE PLATFORM, BEST-OF-BREED

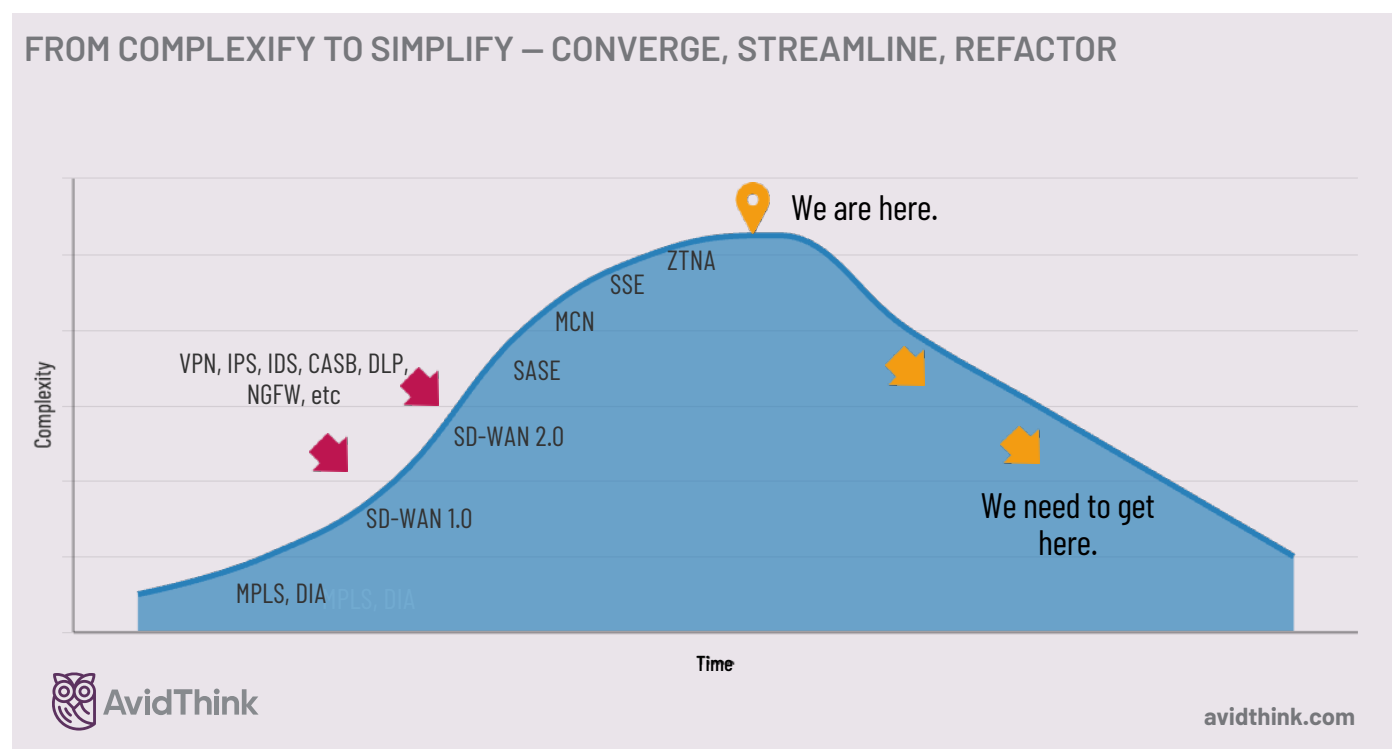


- **Don't Worry, We Manage:** Managed providers (either vendor-managed as a service or MSPs) can absorb the complexity that enterprises face by managing or co-managing SASE services on behalf of customers. Whether single or multiple vendors, single-pass or multiple-pass are less relevant (except for performance and costs) to the end customer. The purchasing evaluation here will be based on different KPIs.

From the end customer's perspective, there's no single "best" approach or vendor. Some enterprises have existing vendor relationships and may choose to evolve with their incumbent "collect and orchestrate" or "collect and integrate" provider. Others with greenfield opportunities may decide to take their chances with a built-from-scratch vendor with innovative and high-performance architectures. Yet others may go the managed route. We view SASE as a diverse market for vendors and end customers with different needs and considerations.

From Complexity to Simplicity

The initial stage of our journey to SASE has been one of "complexification," where vendors keep adding more acronyms (and associated capabilities) to their platforms. This has resulted in complicated UIs, many with navigation bars with acronyms stacked on each other so unsuspecting enterprise users can click into each tab to configure their RBI service, SWG, NGFW, or other relevant service.



Fortunately, we see forward-thinking vendors converging and refactoring their UIs into a higher level of abstraction with objects around users, devices, identity and roles, resources, and policies, with added features for troubleshooting, monitoring, and reporting. Vendors with an integrated platform will be better positioned to execute this stage-two journey to simplicity.

Impact of AI and GenAI – It's Early Days

For the AI drumbeaters, we'd like to point out that AI/ML has been widely used in cybersecurity. However, new ML techniques and the scaling up of computing resources can improve the accuracy and performance of our security systems. GenAI can improve user interaction and help explain security alerts.

Likewise, GenAI represents a significant step toward intent-based security. The language understanding and early reasoning capabilities look promising. This could be applied to help improve enterprises' time to security and reduce user complexity. As we pointed out above, it's early, but given all the hype and investment dollars, we expect rapid advancement on this front.

We have two cautionary notes to wrap up our AI discussion. One, GenAI isn't a panacea; there are computing costs, energy use, and increased response latency. We recommend applying it judiciously to areas of the highest impact. Two, AI and GenAI are double-edged swords. Attackers and defenders can both use them, and we're seeing an improvement in the quality of phishing and social engineering attacks, with personalized attacks and realistic deepfakes. We can confidently predict that 2025 will see increased spending on GenAI by both attackers and defenders.

Parting Words

SASE represents the next step in the evolution of enterprise networking and security, offering a unified framework to address the complexities of modern IT environments. By embracing SASE and zero-trust principles and leveraging the right vendor solutions, enterprises can enhance their security posture, streamline operations, and enable strategic growth. However, we'd like to remind our readers:

- A security strategy requires upfront thinking and planning; picking a SASE vendor isn't the first step.
- No one vendor is perfect, and no single product can or will solve all your needs.
- Vendor selection isn't your last step either; the hard work comes after that decision.
- GenAI and automation are amplifiers; you can automate your way to security excellence or mediocrity, so focus on verification, validation, and performance monitoring.
- Talent recruitment and retention issues in networks and security will not disappear; consider managed services as an alternative.
- With managed services, delegation is not abdication — ensure you have auditability and that you can monitor your watchers.

As the SASE market continues to evolve, we recommend enterprises stay agile and educated and strive to make informed decisions about their SASE vendor selection. The market will consolidate over the few next years even as it morphs into yet another wave of enterprise network security services — we'll be watching carefully as the shift happens. In the meantime, we're open to feedback on our report and happy to answer any questions. You can reach us at research@avidthink.com.

SPONSOR AND VIP INTERVIEW SECTION FOLLOWS

Please support our sponsors. Check out in-depth interviews with their SASE thought leaders and experts. We encourage you to visit their websites to learn more about their solutions.

Interview with Sanjay Uppal

VP and GM, VeloCloud Division at Broadcom

Can you provide an overview of the evolution of SD-WAN and its transition into the AI networking phase?

SD-WAN initially addressed the challenge of enterprises shifting their applications to the cloud. This was phase 1 – introducing simplified, secure, and optimized networks leveraging the Internet. Telecom operators capitalized on this by integrating SD-WAN into their services.

Phase 2 introduced Secure Access Service Edge (SASE), which addresses security concerns by combining SD-WAN with advanced security capabilities. Now, we're entering the third phase: AI networking. This phase focuses on how generative AI (GenAI) transforms enterprise and telecom networks. Unlike traditional workloads, GenAI introduces asymmetrical traffic flows and demands new networking paradigms to handle multimodal upstream data and ensure real-time, secure interactions.

Can you elaborate more on these traffic pattern changes from using GenAI?

We're seeing almost a complete reversal of traditional asymmetric patterns. While web applications typically have minimal upstream traffic and larger downstream responses, GenAI workloads can show up to 100:1 ratios in the opposite direction. The traffic pattern is driven by multimodal inputs – video, voice, and text – sent upstream to large language models, with relatively concise responses coming back downstream.

How are enterprise networks being impacted by AI-related developments like RAG (Retrieval Augmented Generation) and Agentic AI?

Two major shifts are happening. First, RAG drives significant upstream traffic as enterprises must upload their proprietary information to fine-tune or contextualize large language models. Second, and more crucially, Agentic AI introduces complex peer-to-peer interactions between large and small language models distributed across public and private networks. This creates new demands around latency and traffic patterns that traditional networks weren't designed to handle.

What real-world examples illustrate the potential impact of AI on network use?

Consider augmented reality in retail. Imagine a shopper wearing smart glasses that streams real-time video to an AI backend, which analyzes products and provides audio feedback. This interaction creates substantial upstream traffic for processing video and delivering actionable insights.

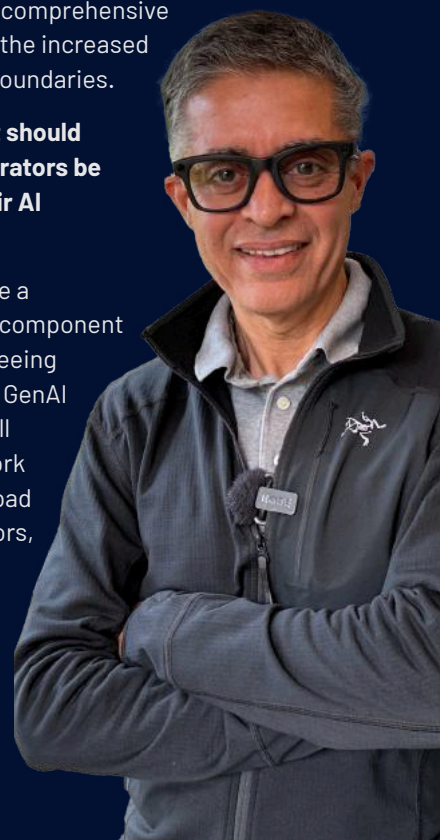
These use cases highlight the need for networks to support high upstream bandwidth, low latency, and robust security. It's not just about functionality; it's about enabling new experiences while ensuring seamless, secure operations. Such capabilities define the future of AI-driven networks.

What's VeloCloud's approach to addressing these new AI networking challenges?

We've developed our VeloRAIN (VeloCloud Robust AI Networking) architecture that addresses several critical aspects. It starts with AI-powered application identification, even with encrypted traffic. We then perform channel estimation to understand the behavior of variable underlays like 5G or satellite. This enables what we call Dynamic Application-Based Slicing (DABs), which provides application-specific quality of service guarantees. Additionally, we've integrated comprehensive security measures to protect the increased data flow leaving enterprise boundaries.

Looking ahead to 2025, what should enterprises and telecom operators be thinking about regarding their AI initiatives?

Every GenAI project must have a corresponding AI networking component in the budget. We're already seeing enterprises launch numerous GenAI projects, but their success will depend on whether the network can support these new workload patterns. For telecom operators, there's an opportunity to monetize application-based slicing tied to specific use cases and quality of experience requirements rather than traditional physical network constraints.



[Click here to learn more about VeloCloud and VeloRAIN](#)

velocloud[™]
by Broadcom



Interview with Renuka Nadkarni, Chief Product Officer



Renuka, can you give us a high-level overview of the key trends driving the evolution of networking and security architectures today?

Absolutely. The world has changed dramatically in the past decade. Users are no longer confined to office spaces, and applications have moved out of on-premises data centers into the public cloud. With hybrid work environments and distributed applications, the traditional point-to-point connectivity models and perimeter-based security approaches simply don't work anymore. We're hearing from customers that they need to modernize their network architectures to meet these challenges.

Aryaka has been focused on providing high-performance connectivity for business-critical applications. How has the change in customer needs impacted your approach?

The evolution of SASE has reinforced our belief in the importance of integrated networking and security. At Aryaka, we started with a vision of providing seamless, high-performance connectivity. Over time, our customers began asking for more security features, like access control, anti-malware, and intrusion prevention. We responded by integrating these security capabilities directly into our global private network, creating a unified SASE solution. This allows us to provide a solution where both networking and security are handled simultaneously, optimizing performance and enhancing security posture.

How does your unified approach address today's enterprise challenges?

Aryaka's Unified SASE (Secure Access Service Edge) as a Service combines networking and security capabilities into a single, integrated solution. It's designed to handle the agility and digital transformation demands that customers are navigating. At Aryaka, we've built our offering around this concept, delivering it as a service so customers don't need to manage complex appliances or fragmented tools.

Our OnePASS architecture processes both networking and security at the same layer, providing performance, simplicity, and scalability. This unification is key for modern enterprises dealing with dispersed users and dynamic cloud environments.


Aryaka has built its own global backbone for connectivity. Can you explain why this approach is significant for customers?

Our global backbone is like having a dedicated lane on a busy highway during rush hour. The internet is rife with variabilities — DDoS attacks, fiber cuts, and oversubscription, to name a few. These can severely impact performance, leading to latency and poor user experiences. Our dedicated underlay network provides 100% redundant capacity, ensuring consistent performance even during disruptions. This foundational design eliminates many limitations of traditional architectures and internet-based overlays, giving our customers reliable, high-performance connectivity.

There's been a lot of buzz about AI in the last 2 years. What role does AI play in networking, and how does Aryaka address its associated challenges?

AI adoption brings both opportunities and challenges to networking. It drives significant data transfers, which strain network infrastructure and demand reliable connections. AI also creates new attack surfaces, bypassing secure web gateways via tools like ChatGPT. Additionally, many organizations lack visibility into AI-enabled traffic, raising concerns about data leakage and intellectual property risks. At Aryaka, we tackle these challenges head-on by ensuring robust, secure networking for AI workloads. We also provide comprehensive visibility and observability, giving customers control over how AI traffic moves through their network.

To learn more about Aryaka and Unified SASE as a Service, visit www.aryaka.com



Interview with Archana Khetan

SVP, Product Management and Technical Marketing

Ericsson Enterprise Wireless Solutions



With increasing numbers of enterprises embracing wireless WAN connectivity, what advice do you have for evaluating SASE vendors?

As organizations increasingly adopt wireless WAN, it's crucial to evaluate solutions based on their ability to address the unique challenges of these networks. Look for capabilities that optimize wireless connectivity, integrate Zero Trust principles, and provide a seamless deployment experience.

What makes NetCloud SASE stand out in an increasingly crowded SASE market?

What truly differentiates NetCloud SASE is that it's the industry's only single-vendor unified SASE solution optimized specifically for wireless WAN. Our solution is built on three core pillars: wireless WAN optimization, zero-trust architecture, and simplified deployment. With wireless WAN projected for double-digit growth over the next five years - driven by 5G advancements and emerging Edge AI requirements - having a SASE solution that understands the unique challenges of wireless connectivity is crucial.

You mentioned wireless WAN optimization. How does NetCloud SASE address the unique challenges of wireless connectivity?

The key difference lies in understanding that wireless networks present fundamentally different challenges than fixed connections. Consider an emergency vehicle like an ambulance - its network profile changes as it moves across a city, yet the transmission remains mission-critical. We've developed features like cellular intelligence to incorporate deeper cellular insights into decision-making, and advanced link bonding that enables flexible traffic distribution across multiple links based on connection quality and traffic type. We've also included support for SA-mode network slicing, all working together to deliver reliable, consistent, high-bandwidth user experiences over wireless WANs.

Zero-trust architecture is often mentioned in SASE solutions. How does your implementation differ?

Many SASE solutions claim zero-trust capabilities, but they're often retrofitted onto existing architectures. Our approach embeds zero-trust principles into the fundamental network creation process, establishing a "deny-all-by-default" foundation. The solution obscures all IP addresses and blocks East-West traffic, crucial for minimizing attack surfaces and preventing lateral movement as networks scale. This built-in rather than bolted-on approach makes a significant difference in security effectiveness.

How have you addressed the deployment complexity that often comes with SASE solutions?

We've taken a ground-up approach with single-pass architecture, delivering one platform, one policy engine, and a consistent provisioning experience across both WAN and LAN services, particularly for private 5G deployments. We've also integrated an LLM-based AI agent model called AI-based NetCloud Assistant ("ANA"), which provides straightforward assistance throughout deployment. This starkly contrasts with solutions that claim to be single-vendor but are, in reality, multiple disjointed products cobbled together.

[Click here to learn more about NetCloud SASE from Ericsson Enterprise Wireless](#)

ERICSSON 



AvidThink, LLC
1900 Camden Ave
San Jose, California 95124 USA
avidthink.com

©2024 AvidThink LLC. All Rights Reserved.
This material may not be copied, reproduced, or modified in whole or in part for any purpose except with express written permission from an authorized representative of AvidThink LLC. In addition to such written permission to copy, reproduce, or modify this document in whole or part, an acknowledgment of the authors of the document and all applicable portions of the copyright notice must be clearly referenced.