AvidThink

New Faces of Enterprise Connectivity: Convergence and Flexibility

Renewed Focus on Simplicity, Security, and Service-Centricity

RESEARCH BRIEF

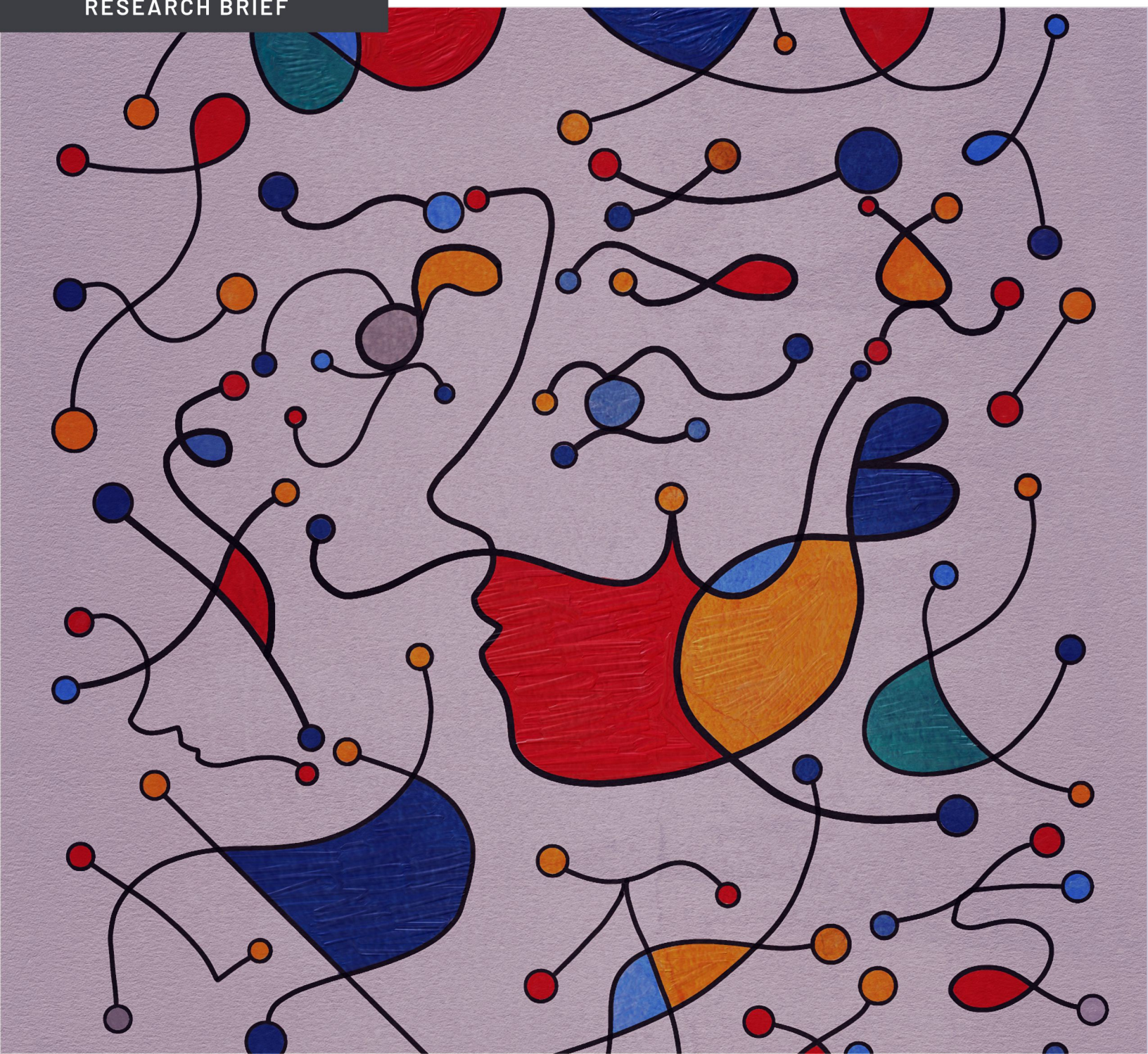


Table of Contents

New Faces of Enterprise Connectivity: Convergence and Flexibility

Renewed Focus on Simplicity, Security, and Service-Centricity

Executive Summary

Enterprises are moving toward next-generation network connectivity convergence, driven by hybrid work, AI workloads, multi-cloud adoption, and increasing cyber threats. Fragmented architectures without unified solutions have resulted in operational inefficiencies. Traditional frameworks relying on separate MPLS, SD-WAN, VPNs, firewalls, Ethernet LANs, Wi-Fi, and isolated security tools are no longer sufficient. Convergence integrates SASE, SD-WAN, ZTNA, Wi-Fi, switching, NaaS, and potentially private 5G into cloud-managed platforms, streamlining operations and strengthening zero-trust security.

AvidThink's recent mid-market enterprise survey in North America highlights key drivers: vendor consolidation, improved visibility and automation, increased compliance requirements, and the need for consistent access across distributed users, devices, clouds, and applications. Convergence offers benefits such as centralized management, enhanced security, lower total cost of ownership through subscriptions and AI-driven operations, and improved hybrid-work performance.

Vendors are evolving rapidly. Networking companies are adding security capabilities (Arista, Cisco, Extreme, HPE/Juniper), while security vendors are expanding into WAN and cloud connectivity, with possible extensions into campus LAN (Aryaka, Palo Alto Networks, Netskope, Zscaler). Campus NaaS startups (Join, Meter, Nile, and others) are also shifting consumption models by offering outcome-based services.

Looking ahead to 2026, AI/ML, Zero Trust, cloud-native architectures, and agentic automation will drive next-generation enterprise network transformation. Enterprises should adopt phased modernization strategies and invest in cross-domain expertise to maximize the benefits of convergence.

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, ZTNA, cloud and AI 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.

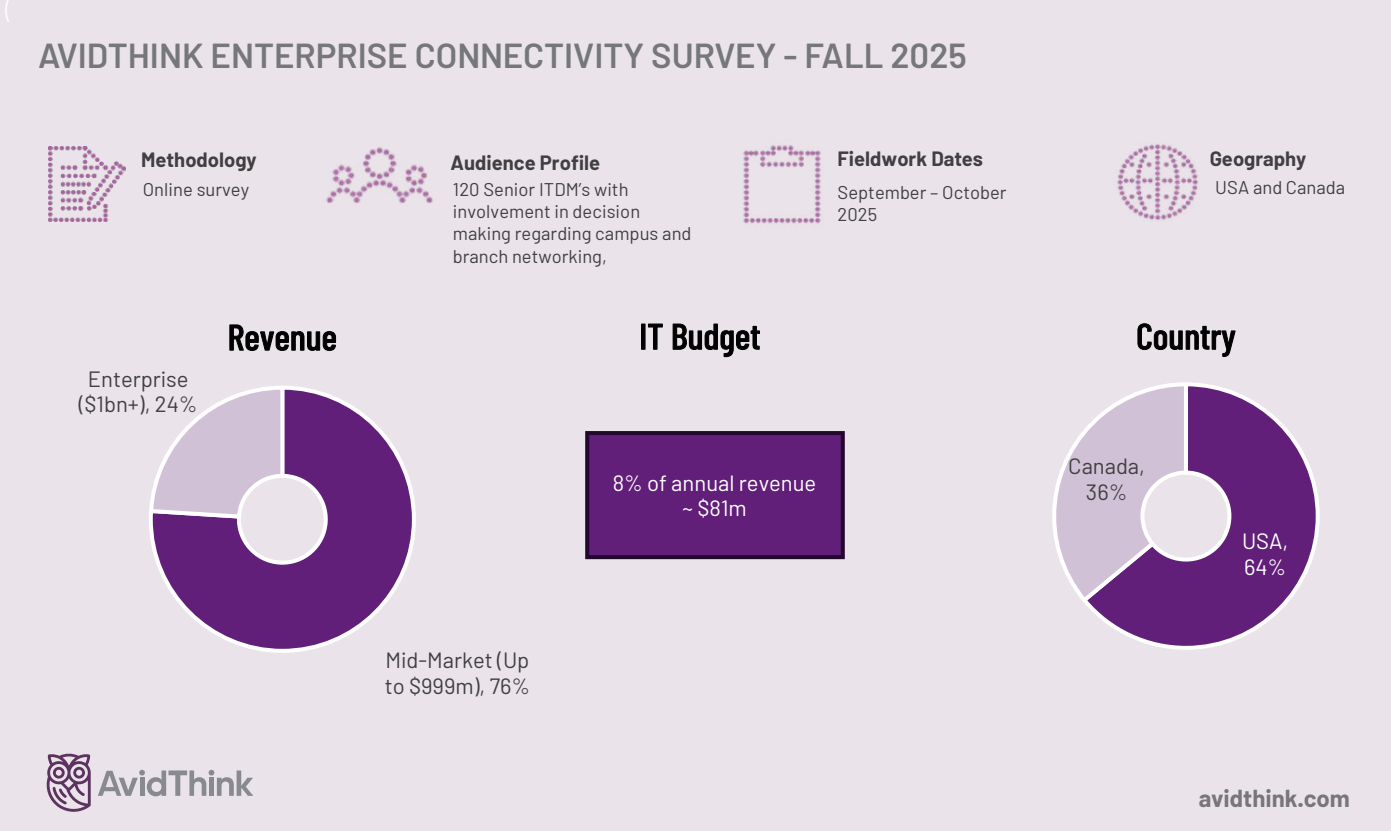
Introduction

Our report examines the convergence of enterprise networking and security solutions across campus and WAN (wide area network) environments. Building on AvidThink's previous research on SASE (secure access service edge) and Campus NaaS (network as a service), it unifies these domains to show how enterprises are planning and implementing next-generation infrastructure as AI-enabled workloads reshape connectivity needs.

We will explore enterprise challenges, adoption patterns, and use cases driving SASE, SD-WAN (software-defined WAN), Wi-Fi, switching, NaaS, ZTNA (zero-trust network access), and private 5G deployments over the next 12 to 18 months. As part of our analysis, we will assess key technology vendors and provide recommendations for enterprises navigating this evolving market.

Methodology

AvidThink surveyed 120 mid-size and large North American enterprises across various industries in Fall 2025. Respondents included IT managers, directors, network and security engineers, architects, CISOs, and CIOs. Over the past three months, AvidThink analysts also conducted vendor briefings and interviews with enterprises and managed service providers to better understand vendor positioning, traction, and current enterprise requirements.



Enterprise Connectivity Challenges

Enterprises advancing towards next-generation connectivity face challenges related to cost, security, talent, operations, and edge expansion. These pressures are accelerating the shift to converged architectures.

- **Cost and Architectural Complexity:** Modern enterprise networks often span multiple service providers across MPLS, SD-WAN, and SASE, resulting in duplicative costs and management overhead. Transitioning from CapEx to OpEx models (NaaS, SASE subscriptions) requires new budgeting and ROI approaches. While single-vendor platforms simplify operations, they raise concerns about long-term flexibility and negotiating leverage.

- **Security Fragmentation**: Security teams commonly operate siloed systems for firewalling, VPNs, CASB, and ZTNA, each with its own policy engines and management consoles. This fragmentation creates inconsistent policy enforcement across on-premises, cloud, and edge environments. Layered compliance requirements (GDPR, HIPAA, PCI-DSS) and country-specific data sovereignty mandates further complicate network and security design.
- **Talent Shortages:** An industry-wide shortage of professionals with blended networking and security expertise constrains enterprise capabilities. Gaps in network automation, cloud security, zero-trust implementation, and threat intelligence make it difficult to fully leverage available tools, even when budgets allow investment.
- **Operational Blind Spots:** Encrypted traffic, SaaS usage, and API calls often go unmonitored. Teams face telemetry overload without correlated, AI-driven prioritization. Root-cause analysis remains difficult when network, application, and security data sit in separate systems, and vendor-specific AIOps tools rarely span multi-vendor environments effectively.
- **Edge and AI Connectivity Demands:** The explosion of IoT, IIoT, and edge devices expands the attack surface while increasing management complexity. Simultaneously, newer AI-driven workloads (especially with the rise of multi-modal models) demand low-latency, high-bandwidth interconnects that legacy WAN architectures struggle to deliver. Standardized security frameworks for edge environments remain immature.

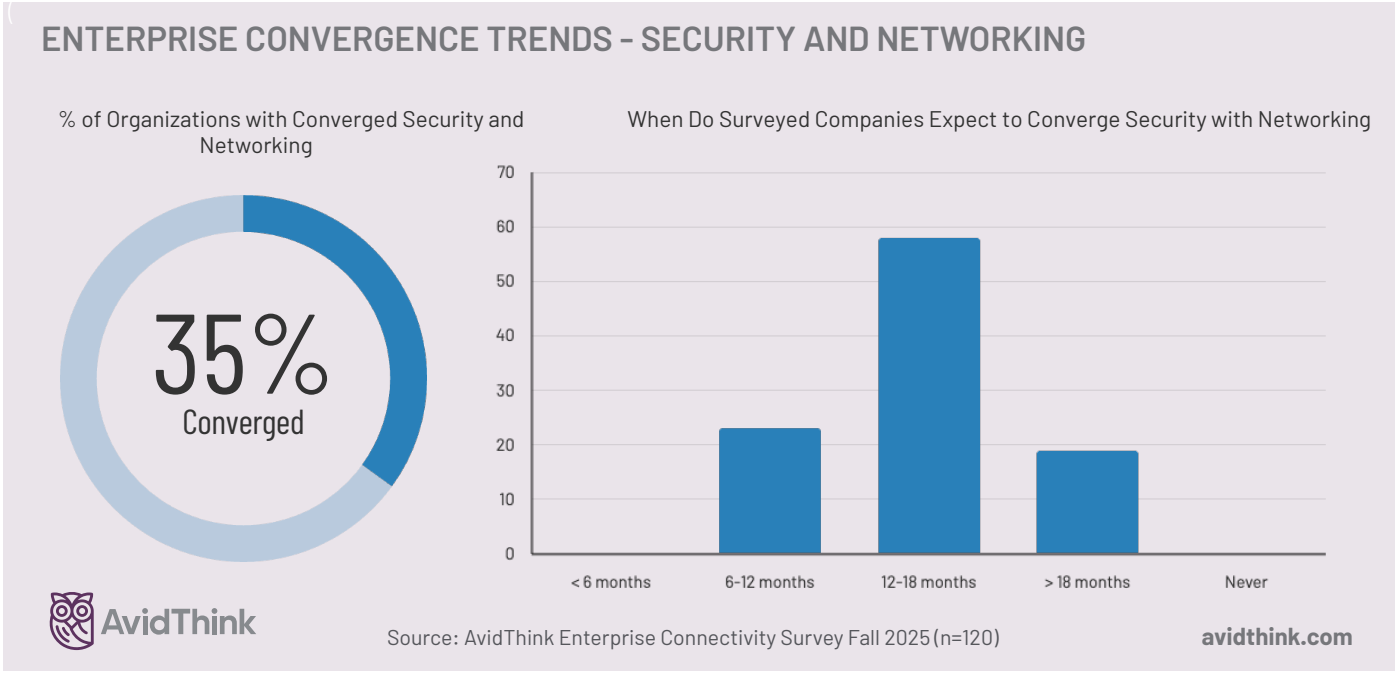
The Case for Convergence

Enterprises are accelerating the convergence of network connectivity and security for compelling business reasons. The drivers are clear; the benefits are measurable.

Distributed Applications and Hybrid Work

Enterprise applications, data, and users are now fundamentally distributed. Organizations rely on hundreds — often thousands — of SaaS and IaaS applications across public clouds and third-party platforms. According to a 2025 survey by virtualization vendor Parallels, 84% of enterprises support hybrid work models[1] combining remote and in-office arrangements.

This reality demands architectures in which security policies follow users, devices, and data dynamically rather than being anchored to physical locations. Legacy perimeter-centric designs cannot consistently enforce policy across the fluid boundaries of modern work.



[1] "Insights on cloud computing | Parallels Cloud Report 2025," Parallels.com, 2025. https://www.parallels.com/products/ras/all-resources/reports/cloud-survey-2025/report/

Escalating Threats and Regulatory Pressure

The threat landscape continues to intensify. Security vendor SentinelOne's 2025 study found ransomware accounted for 35% of enterprise security incidents[2] — an 84% year-over-year increase. AI-enabled attacks, supply-chain compromises, and sophisticated social engineering require continuous verification and automated response capabilities that are difficult to achieve with fragmented security stacks.

Simultaneously, regulatory requirements (GDPR, HIPAA, PCI-DSS, and emerging data sovereignty mandates) raise the bar for consistent policy enforcement and auditability across all network domains. In our AvidThink survey, 59% of respondents ranked compliance among their top three convergence challenges (and drivers).

AvidThink Survey

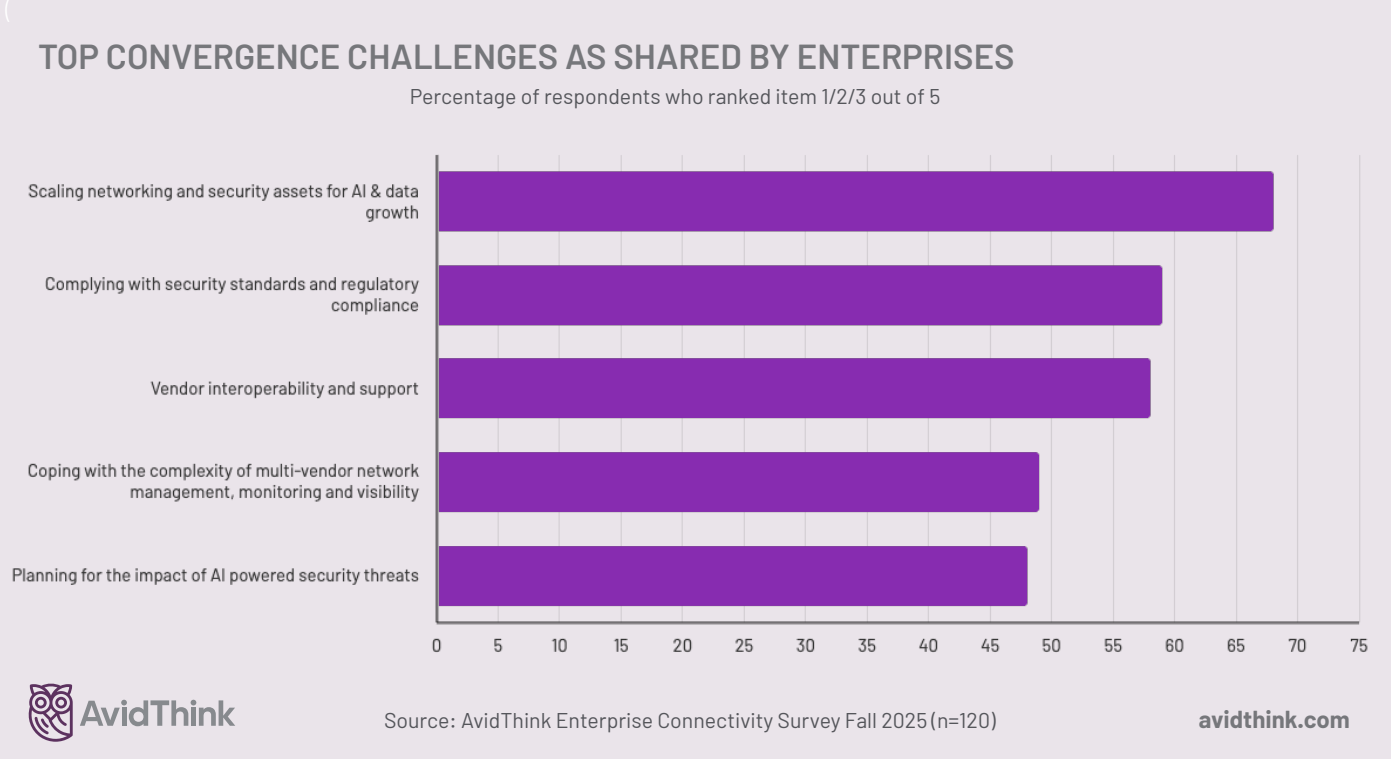
Are you looking for your organization to manage your campus networking (Wi-Fi/switching) and WAN (SD-WAN/SASE) in an integrated way?

Yes: 80%
No: 20%

(n=120)

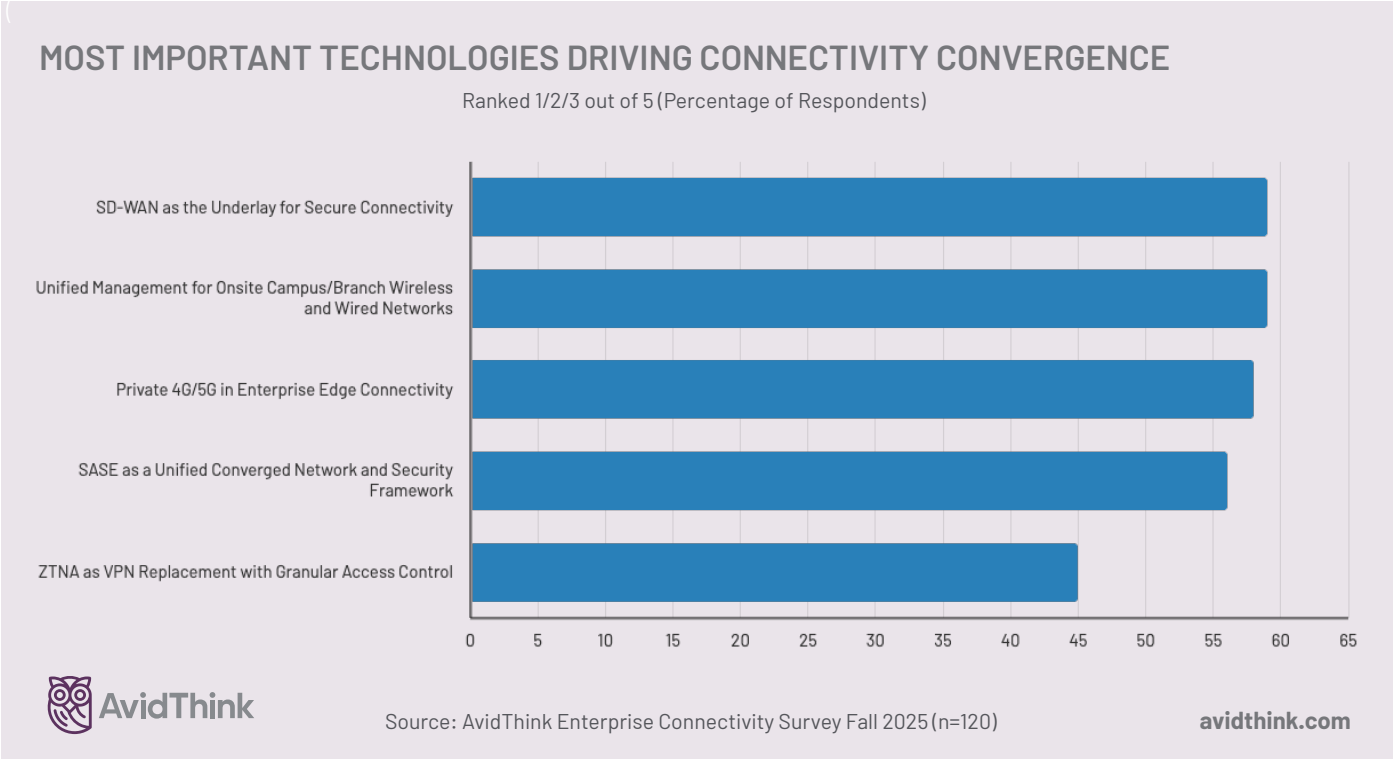
Multi-Cloud Complexity

Multi-cloud is now standard in many enterprises. The 2025 Flexera State of the Cloud report found 86% of enterprises operate in multi-cloud environments[3], with 77% citing security as a top challenge. Applications and data span public clouds, private infrastructure, and SaaS platforms, making consistent visibility and access control increasingly difficult without unified policy engines and shared data models.



[2] SentinelOne, "Key Cyber Security Statistics for 2025," SentinelOne, Updated July 30, 2025. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

[3] "2025 State of the Cloud Report," Flexera.com, 2025. https://info.flexera.com/CM-REPORT-State-of-the-Cloud



Business Benefits

Simplified Operations: The AvidThink survey found 80% of respondents identified a unified management platform as the primary driver for convergence. Centralized control and visibility across campus and WAN eliminates the operational friction of managing multiple product-specific consoles.

Stronger Security Posture: Converged architectures enable Zero Trust enforcement — identity-based access, least-privilege policies, and continuous inspection — consistently across all environments. This is not just an aspirational goal; 59% of AvidThink survey respondents cite security standards and regulatory compliance among their top three challenges.

Cost Efficiency: Convergence can deliver TCO reduction through consolidated hardware, licensing, and maintenance. Cloud and SaaS-like subscription models provide predictable spending. In particular, centralized management with AI-driven automation can reduce operational expenses by 30–60% according to vendor benchmarks. Further, prevention-first security also reduces breach risk, which is critical when average breach costs today top $4.4M per incident (IBM)[4].

Performance and Experience: Integrated architectures minimize interoperability issues and policy inconsistencies. Single-pass SASE architectures — decrypting and inspecting traffic once while processing networking and security in parallel — are typical of newer players or of incumbents that have refactored, eliminating multi-pass inspection latency. And cloud-delivered platforms can optimize resource utilization and reduce backhaul delays.

Agility and Scalability: Cloud-based unified platforms can enable elastic, consumption-based scaling aligned with business growth. Converged policies likely foster collaboration between security and networking teams, helping to break down siloes and enabling faster threat response, plus agile capacity planning.

[4] "Cost of a data breach 2025 | IBM," Ibm.com, 2025. https://www.ibm.com/reports/data-breach

Key Technologies in Focus

Next, we'll touch on technologies at the heart of network connectivity and security convergence and provide an update on SASE, SD-WAN, ZTNA, Wi-Fi, campus Ethernet, NaaS, and private 5G. These are the main technologies cited by our survey takers. The relative importance of private 4G/5G in the survey results was unexpected but speaks to an ongoing demand for complementary wireless capabilities to Wi-Fi, especially in situations where private mobile technologies have an advantage.

SASE

Enterprise SASE adoption accelerated sharply in 2025, driven by hybrid work realities and increasingly sophisticated threats. Single-vendor SASE (SSE + SD-WAN) revenue growth is dramatically outpacing multi-vendor approaches — rising 21% year-over-year in Q1 2025, according to fellow analysts at the Dell'Oro Group[5]. That is consistent with the results of our AvidThink survey, which show that 33% of organizations have already deployed SASE, and an additional 55% have deployments underway.

Several factors made 2025 a breakout year for SASE:

- **Threat intensity:** AI-driven attacks and faster breach timelines demand architectures that adapt in real time

- **Operational pressure:** Enterprises seek cost efficiency, vendor consolidation, and centralized policy control

- **Compliance requirements:** Data protection regulations and supply chain risks push organizations toward unified, auditable security architectures

To achieve a full suite of SASE features, the vendor landscape continues to converge from both directions. Networking-centric vendors are integrating SSE and next-generation firewall capabilities. Meanwhile, security-centric vendors (Zscaler, Netskope, Palo Alto Networks, Fortinet) have integrated SD-WAN and other networking capabilities.

SD-WAN

The global SD-WAN market continues to march forward, driven by the need for cost-effective yet resilient branch connectivity, secure cloud access, and collaboration and AI workloads that require agile WAN performance.

Cloud-first architectures remain a primary driver of growth. Enterprises have shifted 70–80% of workloads to SaaS and public cloud, making SD-WAN the default on-ramp for distributed cloud access. In North America, favorable equipment depreciation rules continue to drive branch CPE-to-SD-WAN refresh cycles, particularly for early 2015–2020 adopters now entering hardware replacement windows.

Key 2025 developments include:

- AI/ML integration across configuration, optimization, and troubleshooting
- Expansion into SASE and SD-Branch for unified security and network management
- Integrated Universal ZTNA connecting users directly to applications
- All-in-one branch appliances combining routing, security, and WAN optimization

We conclude that vanilla SD-WAN has commoditized; differentiation now comes through SASE integration, AI-driven operations, and managed service delivery.

Leading SD-WAN solutions now incorporate IDS/IPS, NGFW, threat detection, and URL filtering — capabilities that were paid add-ons 24 months ago. From this, we conclude that vanilla SD-WAN has commoditized; differentiation comes through SASE integration, app and content awareness and intelligence, AI-driven operations, and managed service delivery. Our survey also shows that, for our mid-market respondents, about half of SD-WAN deployments are now delivered as managed services rather than operated by enterprises.

[5] "Single-Vendor SASE Platforms Propel Revenue to $2.6 B in 1Q 2025, Up 17 Percent Y/Y, According to Dell'Oro Group - Dell'Oro Group," Dell'Oro Group, Jun. 10, 2025. https://www.delloro.com/news/single-vendor-sase-platforms-propel-revenue-to-2-6-b-in-1q-2025-up-17-percent-year-over-year/

ZTNA

Zero Trust Network Access adoption continues to accelerate. A 2025 StrongDM survey found that 81% of enterprises have fully or partially implemented Zero Trust models[6]. Whether this is an overstatement due to the sample population, our conversations with networking and security vendors indicate that Zero Trust is a major initiative across both small and large organizations.

The market is moving toward "Universal ZTNA" — extending security beyond remote users to encompass all devices and users across all network environments. Universal ZTNA provides consistent, identity-based access regardless of location by unifying policies across hybrid environments, reducing attack surface, and simplifying management through a single policy engine.

Market-leading vendors, including Cisco, Fortinet, HPE, Netskope, Palo Alto Networks, Cato Networks, and Zscaler, have adopted Universal ZTNA positioning. As further evidence of the growing importance of a converged networking-security stack, network-centric Ericsson Enterprise Wireless Services (Cradlepoint) extended into this realm with their acquisition of Ericom in 2023 plus with ongoing development. This represents an architectural shift: identity, device posture, and continuous verification become integral to SASE frameworks, replacing not just VPNs but fragmented ZTNA and proxy stacks.

AvidThink believes that enterprises will increasingly prefer Universal ZTNA because it unifies access policies, delivers continuous verification, and integrates natively into SASE platforms. This also lays the groundwork for a broader Zero Trust framework that will eventually span multiple domains: application access, developer environments, cloud platforms, IT infrastructure, and OT environments.

Legacy VPN

Enterprises continue using VPNs for legacy application access and site-to-site connectivity, but most are actively migrating to ZTNA solutions. Legacy VPNs have become attractive ransomware targets, with lateral movement across enterprise networks adding significant breach costs. Larger enterprises typically begin by migrating VPN use cases incrementally to ZTNA as part of broader Zero Trust strategies. VPN-as-a-Service (VPNaaS) offerings from Cisco, Check Point, Palo Alto Networks, and other security vendors provide an interim cloud-delivered alternative with MFA and encryption, though they often lack the granular, identity-based controls that ZTNA delivers.

Campus Wi-Fi

Return-to-office mandates and bandwidth-intensive AI applications drove many enterprises to reevaluate campus wireless capabilities in 2025. Many refreshed legacy access points with Wi-Fi 6 (802.11ax) (with some moving to Wi-Fi 6E) to handle higher device density, increased IoT deployments, and heavier cloud application usage.

Early vendor indications (e.g., from Cisco and HPE Aruba) suggest that Wi-Fi 6E/7 solutions gained traction in late 2025 because they offer future capacity scaling, with awareness of associated challenges: higher power requirements, spectrum-efficiency considerations, and potential backbone switching upgrades.

From a security perspective, WPA3 adoption is increasing, providing stronger encryption and improved authentication. Micro-segmentation is becoming essential — ensuring users, IoT devices, and applications communicate only where explicitly permitted, reducing attack surface and enabling consistent Zero Trust policy enforcement across WAN and LAN.

Key evaluation criteria for Wi-Fi solutions now include:

- AI-driven operations and troubleshooting
- Wi-Fi 7 near-term availability
- Cloud-native management and API programmability
- User experience optimization and location services
- Integration with broader security policy frameworks (with potentially micro-segmentation for IoT/IIoT devices)

[6] M. Todd, "The State of Zero Trust Security in the Cloud Report by StrongDM," Strongdm.com, Jun. 26, 2025. https://www.strongdm.com/blog/state-of-zero-trust-security-cloud

Campus NaaS

Campus NaaS delivers LAN connectivity (Wi-Fi and Ethernet switching) as a managed subscription service, either directly from vendors or through CSP/MSP partners. Demand-side drivers remain consistent from our previous report: overwhelming complexity, IT staff shortages, and preference for OpEx over CapEx. Supply-side enablers include cloud management maturity, AI-driven automation, and the emergence of outcome-based business models.

Incumbent vendors (Cisco with Managed Campus, HPE Aruba Networking, Ruckus) offer Campus NaaS as subscription bundles built on their existing switching portfolios. HPE extends this through GreenLake, bundling networking with storage and compute infrastructure. Startup NaaS vendors (Nile, Meter, Join Digital, Ramen, and Shasta Cloud) have developed different models — with some of them pricing per square foot or user rather than per device, analogous to utility services. Within these startups, some (like Shasta Cloud) provide platforms and tooling that enable MSPs to become NaaS providers while others act as vertically integrated operators who may even design and build their own hardware. Generally, these NaaS offerings have architected cloud-native NOCs on public cloud infrastructure, enabling scalable management and faster deployment. A key differentiator: reducing time-to-service from months to weeks through automated design and deployment processes.

In the past year, startups have emphasized outcome-based pricing with SLA/SLE commitments, including discounts for downtime or service disruptions. This accountability model, combined with deployment speed, is reshaping enterprise expectations. Dell'Oro projects that startups offering Campus NaaS as utility solutions will command approximately one-third of all NaaS revenues by 2028, with the enterprise NaaS sector projected to exceed $940M annually[7].

Private 4G/5G

Private cellular networks rated higher than expected in our enterprise survey, given the perceived headwinds many private 5G vendors face. Yet, private 4G LTE and 5G are gaining traction for secure, high-performance connectivity in environments where conventional Wi-Fi is inadequate (see table below), like manufacturing, logistics, outdoor operations, and industrial sites. Despite early uptake challenges in North America, enterprise adoption is projected to grow at a 42% CAGR over the next five years. As of Q3 2025, the Global mobile Suppliers Association (GSA) identified over 1,904 enterprises globally that have deployed private 4G or 5G networks with contract value exceeding €100K, with manufacturing as the leading vertical[8].

Key requirements driving adoption:

Requirement	Enterprise Need
Data sovereignty	Traffic stays on-premises with enterprise-controlled policies
Performance	Ultra-low latency (<10ms) for real-time control; high throughput (1–10 Gbps)
Scalability	Support for thousands of IoT devices per cell, exceeding Wi-Fi limits
Dedicated capacity	Guaranteed 100% availability via dedicated radio spectrum

Notable deployments include Hyundai and Tesla manufacturing sites, connecting thousands of IoT devices, AGVs, and sensors requiring reliable, real-time, low-latency connectivity. Network-related production shutdowns can cost millions per day, and private 4G/5G mitigates this risk.

Leading vendors include Nokia (despite recent re-organization), Ericsson, Huawei, Celona, HPE (Athonet), Cisco, and Samsung. Network-in-a-box (NIAB) solutions are simplifying deployment by combining 5G core and RAN into plug-and-play units. However, barriers remain: upfront costs, complex spectrum regulation, and integration challenges with existing campus WLAN/LAN infrastructure. Enterprises tell us they are looking for consistent security (zero-trust) policy enforcement across Wi-Fi and cellular domains. AvidThink survey respondents have indicated a strong interest in seeing networking and Wi-Fi/LAN vendors address private 5G integration in their roadmaps. On this front, private wireless startups like Ataya aim to provide a unified observability framework that integrates with incumbents such as Cisco Meraki as part of their private 5G offerings.

[7] "Campus NaaS Startups Poised to Grab Larger Share of the Pie, According to Dell'Oro Group - Dell'Oro Group," Dell'Oro Group, Nov. 06, 2024. https://www.delloro.com/news/campus-naas-startups-poised-to-grab-larger-share-of-the-pie/

[8] "Private Mobile Networks December 2025 | GSA," GSA, 2025. https://gsacom.com/paper/private-mobile-networks-december-2025/

How Convergence Is Playing Out

While the technology building blocks are well understood for convergence, we observe that there are practical realities, including organizational and architectural complexities that enterprise teams must navigate.

Organizational Dynamics Shape Adoption

Our survey confirms that many enterprises maintain discrete networking, security, and IT operations teams with separate decision-making authority. Vendors positioning "Unified SASE" as a single buying decision often overlook these organizational dynamics—purchasing authority remains siloed even when technology converges.

This situation favors a phased adoption approach. Enterprises typically begin with their most pressing challenge, such as SD-WAN refresh, VPN replacement, or cloud security, and then expand incrementally. Convergence is most successful when it fosters collaboration between teams rather than mandating organizational restructuring.

The Underlay Question

SD-WAN was designed as an overlay technology, abstracting and managing across multiple physical underlay options (MPLS, direct internet access, and increasingly fixed 4G/5G wireless access and satellite links). As SD-WAN matures and deployments grow, it's being treated as the underlying fabric for higher-level connectivity abstractions that provide security, encryption, and application-centric optimizations. Regardless, AvidThink believes that AI workloads (including agentic workflows), IoT expansion, and operations in remote or harsh environments will drive enterprises toward hybrid underlays with SD-WAN providing the aggregation, resiliency, intelligence, and SLA management over a portfolio of connectivity options.

Some vendors, notably Cisco, HPE Aruba, and Arista are converging Wi-Fi, switching, VPN, UTM, and SD-WAN into single cloud-managed platforms. This all-in-one branch model appeals to mid-market enterprises with lean IT teams and to MSPs delivering bundled services — though it trades flexibility for simplicity.

Wired and Wireless Integration Challenges

Converging wired and wireless infrastructure is technically straightforward; converging management is not. The two largest enterprise WLAN/LAN vendors — Cisco (Meraki and Catalyst Center) and HPE Aruba Networking (Aruba Central) — provide integrated dashboards, but unified views still lag behind their individual product management stacks. For HPE Aruba Networking, folding in Juniper Mist post-acquisition remains an open issue.

The lack of a truly integrated single pane of glass across WLAN, LAN, SD-WAN, and SSE remains an opportunity for all vendors. Many unified dashboards are aggregation of separate workflows as opposed to true end-to-end integration that encompasses a single set of configuration policies, integrated logging, and licensing and hardware acquisition. Campus NaaS startups hold an advantage here because their single-stack architectures deliver unified management by design rather than through integration.

Cellular and Wi-Fi Policy Alignment

Enterprises deploying private 5G alongside campus Wi-Fi face challenges in integrating policies. Network access and zero-trust enforcement must span both domains consistently, yet security policies optimized for Wi-Fi may degrade performance and increase latency for latency-sensitive IoT or robotic devices on cellular networks. Security vulnerabilities emerge when traffic traverses from private 5G to cloud services or shared networks without consistent policy enforcement.

Simplified deployment models — "5G-as-a-Service" or turnkey NaaS subscriptions incorporating cellular — may accelerate adoption by abstracting these integration challenges as vendors like Meter unify their cellular offerings with their Wi-Fi LAN solutions.

Vendor Offerings and State of the Market

This section will summarize the major networking and security vendors targeting the Americas and European markets that we believe are leading connectivity and security convergence across SASE, Campus NaaS, SSE, WLAN, and SD-WAN. For more detailed descriptions of each vendor and major updates over the last 12 months, please see the Appendix at the end of this report. We will categorize the vendors covered into four major groups: full-stack networking and security, security-led SASE, networking-led, and campus NaaS. We've tried our best to align vendors with respective categories, but in many cases, a vendor may not fall neatly into a single category.

Full-Stack Networking and Security Vendors

These are vendors who have both mature networking and credible network security capabilities. Unsurprisingly, many of these vendors are large corporations.

Key observations on this category:

- These vendors benefit most from installed base gravity, enabling phased convergence rather than rip-and-replace.
- Operational integration, not feature breadth, is now the primary differentiator.
- AI-driven operations are table stakes; policy unification remains the weak point for most.
- Best positioned for large enterprises with complex hybrid estates.

Vendor	Company Background	Convergence Positioning	Key Differentiation	Gaps / Risks	Best Fit
Cisco Systems	Largest enterprise networking vendor globally with dominant routing, switching, WLAN, and WAN presence. Expanded deeply into security and observability.	Broad full-stack convergence across SD-WAN, WLAN, switching, SSE, Zero Trust, and observability.	Scale, ecosystem depth, and channel reach; AgenticOps adds LLM-assisted AIOps for campus/ WLAN.	Fragmented policy and management layers; pricing and integration complexity.	Large enterprises already standardized on Cisco and adopting convergence incrementally.
Fortinet	Security-first vendor expanded into SD-WAN, WLAN, and switching; strong mid-market traction.	Unified SASE built on a single OS, client, and data lake.	Tight security-network integration via Security Fabric; 160+ SASE PoPs.	Campus NaaS is largely partner-led; less traction in very large enterprises.	Mid-market and distributed enterprises seeking vendor consolidation.
HPE Networking (Aruba, Juniper)	Combines HPE Aruba campus leadership with Juniper routing and AI-native ops post-acquisition.	AI-driven end-to-end networking delivered via GreenLake consumption models.	Mist AI strengthens AIOps; Aruba provides campus scale and reach.	Unresolved platform overlap (Mist vs Aruba Central); SSE weaker than security-led peers.	Enterprises prioritizing AI-driven networking with tolerance for integration work.

Security-Led SASE Vendors

Key observations:

- Security-first convergence resonates strongly with CISOs, especially under regulatory pressure.
- Native LAN/WLAN absence remains a structural disadvantage versus full-stack vendors. Expect to see them partner, OEM, or acquire LAN capabilities (especially those with strong zero-trust and micro-segmentation capabilities)
- Architecturally unified platforms outperform "assembled" SASE stacks operationally.
- Increasing relevance in cloud-first and security-led buying centers.

Vendor	Company Background	Convergence Positioning	Key Differentiation	Gaps / Risks	Best Fit
Aryaka Networks	Pioneer of managed SD-WAN evolved into managed Unified SASE provider.	Fully managed SASE over proprietary global backbone.	SLA-backed performance and operational simplicity.	Competes with MSPs; limited self-managed appeal.	Global enterprises preferring managed services.
Cato Networks	Pure-play SASE vendor built natively on a cloud-first architecture.	Unified SASE combining SD-WAN, private backbone, and embedded security.	Single-pass, vertically integrated architecture; ~$300M ARR growing ~45% YoY.	Less modular flexibility for best-of-breed buyers. Fragmentation of portfolio and management systems.	Enterprises replacing legacy WAN + security infrastructure.
Netskope	CASB and data-protection leader expanded into SSE and SASE.	SSE-first convergence extended with SD-WAN and ZTNA.	Strong DLP/SaaS security; single-pass Zero Trust; IPO validation.	LAN/WAN dependence on partners.	Enterprises that are starting to converge on cloud security.
Palo Alto Networks	Leading pure-play enterprise cybersecurity vendor spanning firewalls, cloud security, and SOC platforms.	Security-centric convergence via Prisma SASE and Zero Trust access.	Deep security depth; ~$1.3B SASE ARR in 2025.	No native WLAN or switching; partner dependency for LAN.	Security-led enterprises prioritizing threat prevention who can live with basic integration of controls into their LAN.
Versa Networks	Established SD-WAN vendor with strong MSP footprint.	Universal Secure SASE deployable as cloud, private, or sovereign.	Sovereign and self-managed SASE options.	Limited large-enterprise momentum; weak campus story but strong branch offerings.	Regulated or sovereignty-driven enterprises and MSPs. Enterprises looking for all-in-one solutions and willing to bet on a non-incumbent.

Networking-Led Vendors

Key observations:

- These vendors excel in specific domains (campus, wireless, density) rather than full convergence.
- They usually require partners or complements to address broader security and SASE strategies, though we will likely see them acquiring or building in-house security capabilities over time.
- AI-driven campus operations are becoming a key competitive axis.

Vendor	Company Background	Convergence Positioning	Key Differentiation	Gaps / Risks	Best Fit
Arista Networks	Software-centric networking leader expanding from data center into campus and WAN.	Software-first convergence using a single EOS across campus, DC, and WAN.	Operational consistency and shared telemetry; VeloCloud acquisition strengthens SD-WAN.	No native SSE; relies on partners for full SASE.	Enterprises prioritizing automation and operational uniformity.
Extreme Networks	Campus-focused networking vendor with strengths in switching, WLAN, and cloud management.	Convergence via Platform ONE integrating LAN/WLAN and identity-based access.	Early agentic AI for network policy and operations.	Depends on partners for SASE completeness.	Campus-centric enterprises emphasizing automation.
Ericsson Enterprise Wireless Solutions	Cellular-centric enterprise networking arm of Ericsson (formerly Cradlepoint).	Wireless-first SASE/SD-WAN optimized for LTE/5G WANs.	Clientless ZTNA for WWAN; strong 5G integration.	Limited relevance for wired campuses today. Limited SSE features.	Retail, mobile, IoT-heavy, temporary sites.
RUCKUS Networks	Specialist in high-density WLAN for campuses and venues.	LAN/WLAN convergence with edge security.	Superior RF performance in dense environments.	No SD-WAN or full SSE.	Stadiums, universities, dense campuses.

Campus NaaS Vendors

Key observations:

- Campus NaaS adoption is driven by IT staff shortages and operational fatigue, not only cost.
- Outcome-based SLAs and AI-driven lifecycle ownership are key differentiators.
- Startups are redefining buyer expectations, pressuring incumbents and MSPs.
- Strong initial fit for distributed, low-IT-touch environments.

Vendor	Company Background	Convergence Positioning	Key Differentiation	Gaps / Risks	Best Fit
Join Digital	AI-driven secure networking platform for enterprises and real estate.	NaaS plus virtual-OEM flexibility.	Stream-based observability; hardware flexibility.	Lower large-enterprise brand awareness.	Enterprises/ MSPs needing flexible campus designs.
Meter	Vertically integrated NaaS provider delivering LAN as a utility.	LAN-as-a-Utility with optional SASE integrations.	Full-stack control and in-house hardware enables automation and predictability.	WAN and security rely on partners.	Distributed enterprises prioritizing LAN simplicity.
Nile	Campus NaaS start-up founded by former Cisco executives.	Zero-trust-native campus LAN delivered as a service.	Standardized architecture with self-healing; autonomous lifecycle ops; outcome-based financially-backed SLAs.	Premium positioning might limit SMB reach.	Mid-to-large enterprises seeking a fully managed LAN.
Ramen Networks	Focused on rugged, OT-heavy environments.	NaaS combining Wi-Fi, private 5G, and AI ops.	Strong IT/OT convergence for uncarpeted sites.	Narrow vertical scope.	Industrial and logistics environments.
Shasta Cloud	Technology provider enabling MSPs to build their own MSP-delivered NaaS.	White-label NaaS platform built on open standards.	OpenWi-Fi/ OpenLAN and MSP enablement.	Not enterprise-direct. MSP only.	MSPs delivering differentiated and branded NaaS.

Adoption Challenges for Converged Connectivity

As we look forward into 2026, enterprises pursuing converged connectivity and security will continue to face significant internal barriers beyond technology selection.

- **Legacy Infrastructure Integration:** Integrating new solutions with existing equipment is technically complex, expensive, and time-consuming. A phased migration strategy is more practical than wholesale replacement — though constrained by existing contracts and depreciation schedules. Organizational ambiguity compounds the challenge: it's unclear whether networking or security teams should lead SASE implementation, creating friction before projects begin. For NaaS solutions, pilot deployments replacing a portion of existing campus infrastructure offer a lower-risk entry point. Our conversations with NaaS vendors show that companies will turn over their remote sites to NaaS before transitioning major corporate campuses to the vendor.
- **Talent Gaps:** Survey respondents highlighted skills shortages as the most significant barrier to adoption. Finding professionals with cross-domain expertise in both network engineering and cybersecurity remains difficult; such candidates are rare in a market already short on specialists in either domain. Traditional organizational structures exacerbate the problem. Networking and security teams typically operate independently with separate leadership, budgets, and priorities. This siloed culture — often resistant to change — interferes with the cross-functional collaboration that convergence demands. Upskilling existing staff requires significant time and investment.

- **Compliance Complexity:** Enterprises operating across multiple jurisdictions must navigate overlapping and sometimes conflicting regulations — GDPR, HIPAA, CCPA, PCI-DSS — each with distinct requirements for data handling, access controls, and audit trails. Converged solutions must consistently enforce diverse policies across the entire network. We are increasingly seeing the need to address data sovereignty and privacy in select markets. Some solution vendors have begun offering platforms that can address sovereignty needs while maintaining aspects of managed services and cloud-type flexibility. In addition, mandated security audits require detailed logging and reporting that consolidates data from both networking and security functions — capabilities that integrated platforms are better positioned to deliver.
- **Vendor Lock-in Concerns:** Single-vendor convergence simplifies operations and procurement but creates dependency risks. Proprietary technologies, ecosystems, and APIs can make future vendor transitions technically difficult. Long-term contracts and data stored in proprietary formats further reduce flexibility. This concern intensifies as networking and security technologies evolve at different rates — single-vendor enterprises may miss innovations that emerge outside their chosen platform.
- **Transition Costs:** The financial and operational costs of transitioning to converged solutions, including infrastructure upgrades, training, integration work, and ongoing management changes, can slow adoption. AvidThink recommends enterprises conduct comprehensive TCO analyses that account for both transition costs and long-term operational savings before committing to convergence initiatives.

Future Outlook

SASE Evolution

AvidThink identifies two primary vendor go-to-market strategies emerging in 2025–2026:

- Platform-centric SASE positions unified platforms with single management dashboards that replace incumbent networking or security functions from the outset. Cisco, Palo Alto Networks, Versa Networks, and Fortinet are aggressively pursuing this approach.
- Phased SASE positions modular solutions starting with one core technology (SD-WAN, ZTNA, or CASB), then expanding based on customer use cases. Cato Networks, Netskope, and Zscaler favor this customer acquisition strategy.

The phased approach is generally more accessible for enterprises, as it enables incremental migration. For example, organizations may initially replace VPNs with ZTNA, then expand to CASB, or consolidate legacy NGFWs and SWGs. This strategy also encourages collaboration between networking and security teams and allows vendors to leverage their core strengths when competing with larger incumbents.

Additionally, mid-market SASE adoption is accelerating. Single-vendor solutions appeal to organizations with lean IT teams, preferring managed service delivery. At the recent Mplify Alliance Global NaaS Event, AT&T shared they were seeing increased mid-market demand for managed SASE services in 2025 and expects continued growth through 2026. In contrast, large enterprises who have specialized and diverse needs may continue to adopt a best-of-breed approach with separate SD-WAN and SSE partners.

Deployment flexibility is also expanding. Vendors like Versa Networks now offer cloud-based SASE-as-a-Service, Versa Private SASE, and Versa Sovereign SASE for enterprises deploying on their own infrastructure. This hybrid model appeals to organizations with IT staff capable of managing deployment and operations internally. Other vendors including large incumbents have shared that they are likewise offering to meet customers where needed — whether full-service via an MSP partner, or simply selling solutions for DIY enterprises.

Zero Trust Trajectory

Zero Trust adoption has crossed the mainstream threshold. Looking forward, expect Zero Trust principles to extend beyond network access into application security, developer environments, and OT infrastructure. Enterprises should plan for phased ZT expansion across these domains rather than treating ZTNA as a destination. The key to successful Zero Trust deployment lies in usability and ease of adoption — many ZT solutions tend to be overcomplicated.

SD-WAN Outlook

As we already touched on, standalone or vanilla SD-WAN has commoditized. Differentiation now comes through advanced capabilities in content and app intelligence (including AI workload awareness), AI-assisted visbility and operations, and flexible business models. Enterprises approaching hardware refresh cycles — particularly early 2015–2020 adopters — should evaluate converged SASE solutions rather than like-for-like SD-WAN replacement.

We expect more networking vendors to drive convergence inorganically; for example, Arista Networks' recent acquisition of VeloCloud from Broadcom brought 20K+ enterprise customers onto Arista's cloud-managed platform. Arista had previously acquired security vendor Awake Security. Other networking vendors might likewise expand their portfolio inorganically in 2026.

Campus NaaS Futures

The outcome-based model pioneered by NaaS startups is reshaping enterprise expectations. Pricing tied to SLA/SLE commitments — with discounts for downtime or service disruption — shifts accountability to vendors in ways traditional equipment purchases never did. Nile, Meter, and Join, amongst others, are actively expanding deployment capabilities. AIOps capabilities are proving critical for campus NaaS vendors to lower the cost of delivering fully outsourced LAN services. Enterprises evaluating campus refresh should include these vendors alongside incumbents — the business model innovation may matter more than feature comparisons. Nevertheless, we recognize that not all enterprises are ready to consume their networking or network security like they consume SaaS applications. In the interim, some Campus NaaS vendors have shared that they have had to be flexible in structuring payment plans to accommodate clients still looking for accounting choice (CapEx vs OpEx optimization) in their IT purchases.

The AI Imperative

Every mid-size and large enterprise needs a plan to adopt AI/ML for network and security operations. The data explosion from edge computing, IoT, cloud workloads, and AI applications makes manual management processes untenable. We note two prongs of AI adoption by networking and network security vendors. The first is using AI to drive automation (AIOps), and the second is using AI to improve threat detection.

Network Automation with AI

Capability	Example	Impact
Predictive analytics	Forecast congestion or link failures	Proactive remediation reduces downtime
Intent-based networking	Translate business policies into configurations	Simplifies multi-domain management
Self-healing networks	Detect anomalies, auto-remediate via closed-loop automation	Reduces operational costs and human error
AI-driven assurance	Continuous QoS optimization for apps and users	Improves experience for hybrid work, IoT, edge

Sample vendors supporting these capabilities include Cisco (AI Ops + DNA Center), Juniper (Marvis AI), Arista (CloudVision), and HPE Aruba (Aruba Networking Central/Mist AI/Marvis AI).

AI as Security Engine

Function	AI/ML ROI	Benefit
Threat detection	Anomaly detection, behavioral analytics	Identifies zero-day and insider threats faster
ZTNA & SASE	Adaptive trust scoring, risk-based access	Continuous verification across cloud and edge
SOC automation	Correlation and triage of security events	Reduces MTTR by 50–70%
Generative AI	Summarizes complex threat data	Accelerates analyst decision-making

Example vendors with strong AI security capabilities include Palo Alto (Cortex), Fortinet (FortiAI), Zscaler (AI threat correlation), and Cisco Hypershield. Nevertheless, a key challenge for enterprises is managing interoperability between different vendor AI engines and correlating telemetry across multi-vendor environments.

2026 — Another Year of Agentic AI

Vendors are pivoting development resources toward agentic AI capabilities — autonomous agents that monitor networks, detect anomalies, predict issues, and take corrective action before user impact. Expect security co-pilots and GenAI-assisted workflows in SOC and NOC operations to become mainstream in the next 12-18 months.

AvidThink Recommendations

We'll break our guidance for the market into two categories. One for enterprise IT teams and another for vendors who are interested in converging their networking and network security solutions in response to the trends we've covered in this report.

For Enterprises

- **Assess current state:** Evaluate existing infrastructure, connectivity solutions, and business requirements to identify gaps. Understand where networking and security teams align — and where organizational friction exists.
- **Adopt phased migration:** Implement convergence incrementally, minimizing disruption while building cross-team collaboration. Start with the highest-pain-point use cases (VPN replacement, branch refresh, cloud security gaps).
- **Prioritize Zero Trust:** Ensure security is foundational to next-generation network design, not bolted on. Plan for ZT expansion beyond network access into applications, developer environments, and OT.
- **Evaluate vendor trajectories:** Assess not just current capabilities but long-term roadmaps. Convergence is a multi-year journey; vendor stability and investment direction matter.
- **Address skills strategically:** Invest in cross-domain training for existing staff, or evaluate managed services from MSPs with demonstrated expertise. The build-versus-buy decision for operational capabilities is as important as the technology selection decision.

For Vendors

- **Unify management:** Develop a single management plane integrating networking and security. Swivel-chair administration across multiple consoles undermines the value proposition of convergence.
- **Prioritize interoperability:** Support open standards, RESTful APIs, and modular integration with existing IT ecosystems. Enterprises operate multi-vendor environments; closed platforms limit the addressable market.

- **Embed AI natively:** Build common data lakes across WLAN, SD-WAN, SASE, and switching platforms. Implement AI-powered policy simulation and digital twin modeling. Be open to providing AI-friendly interfaces via MCP (model context protocol) and A2A (agent-to-agent). Bolt-on AI will not compete with AI-native architectures.
- **Deliver consistent Zero Trust:** Provide unified policy enforcement across all connected devices, users, and applications — regardless of domain or location.
- **Simplify consumption:** Outcome-based pricing, SLA-backed commitments, and flexible deployment models (cloud, private, sovereign) are becoming enterprise expectations, not differentiators.

Conclusion

The convergence of networking and security, once considered a forward-looking aspiration, has become an operational imperative driven by distributed workforces, escalating threats, multi-cloud complexity, and AI-intensive workloads. The technology building blocks are now mature. SASE frameworks, Zero Trust architectures, SD-WAN, and cloud-managed campus solutions have progressed beyond early adoption and are now widely deployed in enterprise environments.

Three themes will define success over the next 12–18 months:

- **Organizational alignment matters as much as technology selection.** Convergence initiatives stall when networking and security teams operate in silos with competing priorities. Enterprises that invest in cross-functional collaboration and choose vendors whose solutions bridge rather than bypass organizational boundaries will realize benefits faster.
- **Phased adoption outperforms big-bang transformation.** Starting with the highest-pain-point use case (VPN replacement, branch refresh, cloud security consolidation) builds momentum and demonstrates value incrementally. The vendors gaining traction are those that enable this journey and focus on business outcomes, rather than demand wholesale commitment.
- **AI will separate leaders from laggards.** AI-capable platforms that unify telemetry, automate remediation, and enable predictive operations are moving from differentiation to table stakes. Enterprises and vendors treating AI as a bolt-on capability will find themselves at a structural disadvantage.

The trend toward convergence is irreversible. While we're seeing this first in the mid-market, we expect that as larger enterprises refresh and streamline their IT estates, retiring proprietary systems, they will embrace convergence for its many benefits. Fragmented architectures are unable to provide the agility, security, and operational efficiency required by modern enterprises. CISOs and IT leaders who embrace this transition and address its organizational and technical complexities will position their organizations for resilience in an increasingly demanding environment.

SPONSOR INTERVIEWS SECTION FOLLOWS

Please support our sponsors — check out in-depth interviews with key executives in enterprise connectivity. We encourage you to visit their websites to learn more about their solutions.

ARISTA

Q&A

Jeff Raymond

VP, EOS Software and Services

Enterprise networks have historically been built in silos — data center, campus, branch, WAN — each with different security policies and management tools. How is this changing?

We're seeing a fundamental shift driven by cloud networking principles. The cloud operators building at massive scale aren't thinking about boxes and interface types, they're thinking software-first. This approach, enabled by Ethernet and IP as common transport, allows us to break down those traditional vendor-designed silos. At Arista, we've built a single software train, EOS, that runs across all our networking devices. What this means operationally is profound: you qualify the software once, learn to troubleshoot it once, and can implement consistent policy across your entire network, whether data center, campus, or branch. You don't need five different security policies anymore. You can think about it as one consistent approach, which dramatically lowers the adoption barrier.

Security and networking convergence is a hot topic. What's Arista's strategy here, especially given you're not traditionally known as a security company?

That's exactly the point — we believe security should be integrated into the network, not bolted on as an afterthought. Our Zero Trust Networking pillar includes purpose-built security products: wireless intrusion prevention, CloudVision AGNI for identity management, and our Multi-Domain Segmentation Services (MSS). MSS is powerful because it provides one security policy for group access control across your entire network from data center to campus without proprietary headers or overlays. We can interoperate with existing identity systems like Aruba ClearPass or Cisco ISE in brownfield environments. Additionally, through our Awake Security acquisition, we've embedded Network Detection and Response capabilities directly into EOS, streaming intelligent data to our NDR nucleus for threat detection and automated response through Cloud Vision orchestration.

With the VeloCloud acquisition, how are you balancing integration with maintaining what made VeloCloud successful?

We aim to avoid mistakes the industry has made in the past. The typical playbook is to immediately rewrite every feature in the acquiring vendor's operating system — that's a recipe for three to four years of delivering nothing valuable. VeloCloud is a full-featured product with happy customers and a strong MSP channel that's new to us. Our approach is pragmatic: we're starting with observability, bringing VeloCloud telemetry into our Network Data Lake so CloudVision users can see all their devices. VeloCloud Orchestrator remains the platform for day-to-day operations. Over time, we'll leverage what we've built in EOS, but we're not making religious decisions that don't drive business practicalities. The MSP partners have given us positive feedback — they're pleased with Arista's engagement level.

How is Arista addressing the mid-market, where simplicity and unified operations matter even more?

We have a three-pronged strategy. First is product portfolio expansion — we've introduced smaller footprint products like our 12-port fanless PoE switch, our smallest and most affordable switching product. Second is simplifying operational workflows. Our infrastructure was built for automation, but initially assumed operators were network or software experts. We're now adding layers of abstraction with GUI-driven wizards that let broader enterprise customers solve problems in a few clicks without needing to understand BGP. Third is go-to-market through MSPs, leveraging the VeloCloud channel to expand our entire portfolio's reach. This is a journey; we want to remain excellent in sophisticated data center environments while also excelling across the full spectrum.

Interview with Renuka Nardkani

Chief Product Officer

How has hybrid work changed the way enterprises should think about SASE?

When we talk about SASE, we typically think SD-WAN plus security. But we're living in a hybrid workforce where employees move between office and home, expecting consistent access to applications — whether SaaS-based, privately hosted, or in the public cloud. The challenge is that enterprises usually deploy different solutions for branch security versus remote access, creating inconsistent user experiences and visibility gaps for administrators. This leads to misconfigurations, which remain a leading cause of security breaches. Through 18 months of selling Unified SASE as a Service, we discovered that user experience was often an afterthought. Network design didn't adequately account for remote access use cases or employee experience as decision-making factors.

What does true networking and security convergence look like in practice?

True convergence under SASE must account for both physical locations and remote user experience. That requires rethinking access control policies from the ground up, such as how we create configurations and rules. Aryaka's OnePASS Architecture was built on this principle. It ensures all traffic, whether from users or sites, is processed consistently in a single pass through our Unified SASE platform. The same security policies and visibility apply everywhere, regardless of connection origin. This eliminates the dual-stack problem where different security tools create policy inconsistencies and administrative complexity.

How does Aryaka redefine Zero Trust Access for hybrid and BYOD environments?

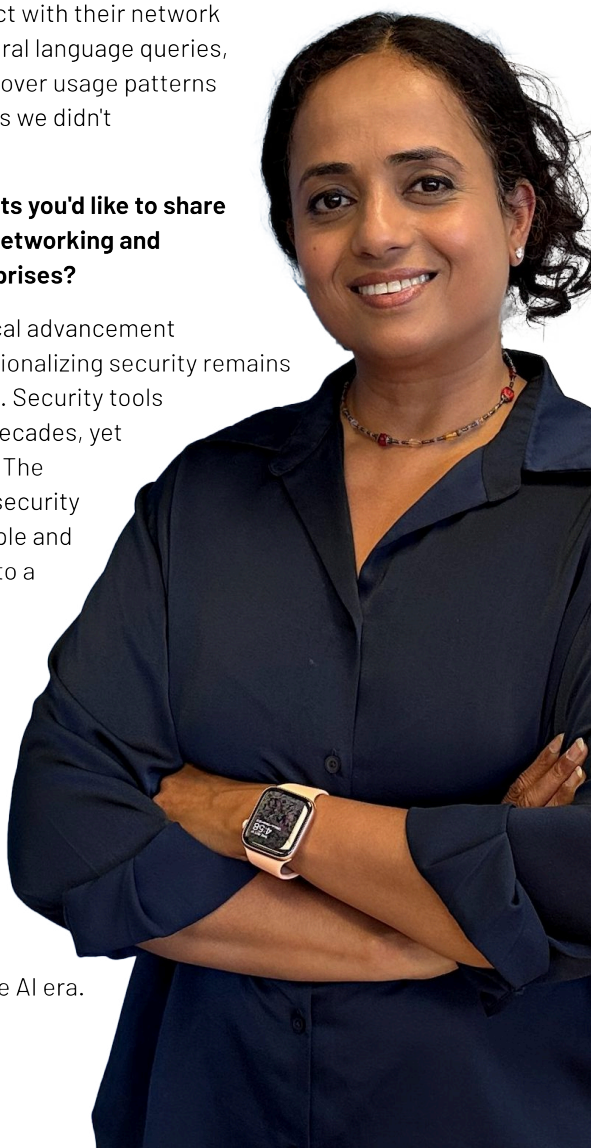
Zero Trust Network Access isn't just about security, it's equally about user experience. Aryaka Universal SASE applies identical policies whether users connect from sites or remotely. We examine all destinations, from private applications, publicly hosted apps, to SaaS applications like Salesforce, then steer and optimize traffic using WAN acceleration technologies like compression and deduplication. We call this LAN-like access over the WAN. Even remote users experience local performance. From a security perspective, administrators gain full visibility and control over all traffic between users and applications, with consistent policy enforcement everywhere.

How do Aryaka's AI capabilities work together to protect and optimize networks?

At Aryaka, AI traffic is just another workload we process, but with unique characteristics. It's distributed, API-driven, and increasingly agentic with bots communicating directly with users. We address this through three capabilities: AIPerform ensures reliable, high-performance connectivity for time-sensitive AI workloads. AIObserve provides visibility into AI traffic, including hidden interactions like chatbots embedded in websites. AISecure delivers access control, threat protection, and data loss prevention tailored to AI protocols and natural-language communication. Traditional DLP tools might miss someone spelling out a credit card number in words to a chatbot. AISecure handles exactly these scenarios. Beyond security, AI transforms how customers interact with their network data through natural language queries, helping them discover usage patterns and exposure risks we didn't anticipate.

Any other thoughts you'd like to share on the future of networking and security at enterprises?

While technological advancement continues, operationalizing security remains the real challenge. Security tools have existed for decades, yet breaches persist. The secret is making security operationally simple and transforming it into a business enabler rather than a barrier. Aryaka is committed to delivering Unified SASE that's easy to use, simple to manage, and powerful enough to secure enterprises for the AI era.



meter

In Conversation with Sunil Varanasi, Co-founder and CTO, Meter

Vertical integration versus best-of-breed has been debated for decades. What's driving Meter's integrated approach, and how does it address real enterprise challenges?

The "best of breed" mindset assumes every vendor you buy is optimal at what it does. But the real challenge isn't individual components, it's organizing and operating the entire network as a single entity. At Meter, we don't compromise on performance, configurability, or management. We deliver enterprise-grade firewalls, switches, access points, PDUs, and cellular — all integrated. Our dashboard provides real-time network statistics that feed our models to make the system continuously smarter. The question isn't whether each component is best in class on its own. It's about whether the system as a whole delivers the performance, reliability, and scale you need.

Tell us about Meter's backend. What automation and self-healing capabilities does it enable?

Meter's backend cloud is extremely powerful — we can automate every component of the network. Take auto-channel or auto-power selection: the devices don't make those decisions. The intelligence lives in the cloud, where we process real-time data and push decisions down to devices. We also learn across customer environments. If two customers have warehouses, we understand warehouse constraints and apply metadata from Warehouse A as a model for Warehouse B. That lets us determine optimal channel selection and placement across our entire customer base. For issue resolution, devices feed data back to our backend. We run validation and automation that can resolve issues and alert customers. If we can't solve it automatically, we work closely with our customer to reach a resolution.

There's significant hype around AI in networking. How is Meter approaching AI differently, and why does determinism matter?

"AI" has become a catch-all term, but in networking, determinism is critical. Network engineers need precise answers, not probabilistic summaries. When you ask "Show me the last time the ISP dipped below 95%," you need an exact answer — "Last week at 9:05 p.m." — not a vague response. We train our own scoped, specific model tightly integrated with our API and virtualization layer to maintain determinism. Our autonomous networks think, learn, and deliver precise solutions.

Network and security convergence has accelerated recently. What's changed, and how does unified policy work at scale?

Multiple trends have been building for years, but what's accelerating convergence now is complexity fatigue. Tools are more complex, pricing is opaque, and customers are tired of IT and network teams fighting with finance over multi-vendor licensing. They want one solution, one management plane, one invoice. With Meter, identity, segmentation, firewall rules, and role-based access control are all cloud-managed in a single dashboard. You can navigate every layer, understand who's on the network, and how policies apply — at scale.

Meter folds in ISP services via Meter Connect. Why take on that complexity?

It's surprising more companies don't think about where the network actually begins—the WAN and ISP. If you don't consider ingress and egress, you can't design a great network. As part of our vertically integrated stack, we procure ISP circuits for customers. In the dashboard, you enter an address, see all available ISPs, and purchase circuits. We know which ISPs deliver high quality at your location, and our SD-WAN supports multi-ISP load balancing and failover. With Meter, customers don't need separate solutions — we provide host monitoring, WAN monitoring, ISP monitoring, application monitoring, and smart routing.

Looking ahead 12-24 months, where is Meter investing?

Customers tell us their IT teams are shrinking while demands grow. Our investment focus is autonomous networks — training models that make networks smarter and reduce IT workload. When you give IT these superpowers, they can do their jobs better and reclaim time for what matters. That's our focus moving forward.

nile

Interview with Pankaj Patel, CEO Shashi Kiran, CMO

The networking industry is facing significant change with AI and economic uncertainty. What's your assessment of where we are right now?

Pankaj: When we started Nile seven years ago, we set out to disrupt an industry where the status quo hadn't changed in decades. Customers believe the way they've built, managed, and deployed networks — and the way they've spent money — will be scrutinized. In the age of AI, everyone is expected to be more efficient and responsive. This shift validates our journey from day one: ruthless automation powered by data, analytics, and our Zero Trust Fabric. We have over 500 deployments, including under challenging verticals such as healthcare and major financial institutions. These proof points demonstrate the value of high-performance, ultra-secure access delivered as a service with total-cost-of-ownership savings.

When customers have historically owned and operated their own aging infrastructure with separate network and security teams, what advice would you give those considering autonomous operations?

Pankaj: I've been in this industry for nearly five decades. Industries change. Skill sets must change. New technologies make you more productive and let you focus on more meaningful work. That's really what AI is teaching us: adopt tools that help you do your job better. With Nile, you don't have to be on call in the middle of the night or on holidays. What I consistently hear from customers is: "Once we deploy Nile, it just works." That's music to my ears.

The industry has long struggled with the separation between networking and security domains. How does Nile address this fragmentation?

Shashi: Legacy architectures rely on discrete boxes with layers of manual operations — like managing spaghetti. Nile brings an entirely new architecture built around unification, radical simplification, and AI-driven operations. We took cloud and data-center best practices: platformization, Zero Trust, and autonomous operations, and applied them to the LAN as a subscription service. Connectivity and security aren't separate domains; they're two sides of the same coin.

Legacy vendors talk about Zero Trust and converged security, but implementation remains challenging. How is Nile's approach fundamentally different?

Shashi: Traditional networks were never built with security in mind — it's bolted on as another appliance, console, and team to coordinate. Gartner notes that over 40% of organizations abandon Zero Trust efforts due to complexity. Nile's architecture is built from the ground up around the Zero Trust Fabric. Security is foundational, and that's why our offering is Secure Network-as-a-Service.

What does a single pane of glass really mean in practice?

Shashi: One unified operational model across the entire lifecycle, from Day 0 through Day 2+. Our cloud-delivered service catalog delivers a rich set of capabilities, including authentication, guest access, and trust and edge services. Whether wired or wireless, campus or branch, network performance or security posture, it's a single interface that lowers costs and shrinks the attack surface.

Where do AI and autonomous operations fit?

Shashi: AI makes convergence operationally viable at scale. We detect network, security, and operational anomalies and handle them across all domains. Our AI reasons across the full stack: Is this a network issue or a security event? Is performance degraded due to configuration drift or an emerging threat? Meanwhile, autonomous operations empower IT staff, preventing burnout and allowing teams to be strategic rather than tactical. Nile helps unburden IT, delivering outcomes without heavy lifting. Customers see 50%+ cost savings with our OPEX-based subscription model while improving both security and performance.

Looking ahead to 2026, what's Nile's vision for converged, autonomous networking?

Shashi: 2026 is a year of scale. We have hundreds of customers and strong proof points across 12 verticals. What's unique is that Nile both innovates the technology and delivers the service. Our goal is to provide what may be the most secure network in the world, fully consumed as a service, with unified operations that eliminate traditional silos between networking and security.

Appendix: Vendor Details

This section contains the detailed descriptions of the vendors we touched on in the main body of the report. The vendor profiles below have been updated from previous reports and some new ones added. As we've indicated, the companies highlighted are a selection of the many hundreds of vendors involved in enterprise connectivity. The companies below are those we've repeatedly encountered over the years and that enterprises and managed service providers have mentioned either in conversations or as part of our recent surveys. If you are a vendor and would like to be included in future editions, reach out to us at research@avidthink.com.

Full-Stack Networking and Security Vendors

Cisco Systems

Cisco maintains market leadership in SD-WAN, WLAN, and SASE, with the most deployed SD-WAN among Fortune 2000 enterprises. Its SASE solution combines their SD-WAN with Cisco Secure Access (SSE), Umbrella cloud security, and ThousandEyes observability — supporting both single-vendor and multi-vendor approaches through integrations with Zscaler, Cloudflare, Netskope, and Palo Alto Networks.

Cisco faces ongoing challenges with customer perceptions of pricing complexity and "Cisco fatigue." Enterprise feedback indicates the SASE solution is perceived as more complex because it comprises integrations of point solutions — Secure Access, Umbrella, Catalyst SD-WAN, Meraki, and ISE — which contribute to operational challenges. The company lacks a unified single security policy layer across SASE components.

In 2025, Cisco launched AgenticOps, an AIOps platform with a proprietary LLM trained on accumulated CCIE expertise and customer network designs. The AI assistant automates workflows and diagnoses network issues, with implementation focused across campus and WLAN products. NaaS is delivered through flexible OpEx subscriptions bundling hardware, software, and lifecycle services, though it remains SKU-based rather than outcome-driven.

Fortinet

Fortinet positions itself as the convergence leader, recognized across SD-WAN, SSE, and WLAN/campus switching. Its single-vendor Unified SASE combines FortiSASE cloud-delivered SSE with SD-WAN, all running on a single operating system, client, and data lake. The solution performs well with mid-market enterprises seeking vendor consolidation with lean IT staff.

In 2025, Fortinet expanded to over 160 PoPs supporting cloud-managed SASE growth. Rather than offering direct campus NaaS, Fortinet enables partners and MSPs to deliver NaaS services using its Security Fabric platform. Key challenges include penetrating large enterprises and potential hardware tariff impacts.

HPE Networking (Aruba and Juniper)

HPE completed its $14 billion acquisition of Juniper Networks in July 2025, creating a comprehensive portfolio spanning campus, data center, service provider, and cloud networking, with AI-native operations. HPE currently maintains both HPE Aruba Networking and HPE Juniper Networking brands.

HPE Aruba positions unified single-vendor SASE solutions integrating SD-WAN, SSE, and network access control, though enterprise feedback indicates SSE capabilities lag specialized vendors in CASB and SWG. The portfolio gains firewall capabilities from Juniper's SRX products. Significant integration challenges remain — deciding whether to merge Juniper's Mist platform with Aruba Central, and rationalizing overlapping campus and branch architectures. On AI capabilities, Juniper's previous advantage has eroded as competitors like Cisco, Extreme, and other networking and security vendors embed agentic AI. NaaS is offered through GreenLake with flexible deployment options (private cloud, VPC, on-premises) using consumption pricing rather than outcome-based models.

Security-Led SASE Vendors

Aryaka Networks

Aryaka pioneered fully managed "Unified SASE as a Service," converging SD-WAN and security (ZTNA, SWG, CASB, DLP, NGFW) into a single cloud-delivered platform on a proprietary Zero Trust WAN infrastructure. The globally distributed private backbone, with nearly 40 points of presence, provides less than 25ms latency through a pseudo-TCP connection architecture with complete traffic encryption, compression, and optimization. Private POPs with dedicated links between locations use owned hardware data centers with top-tier service providers per geography for guaranteed SLAs and five-nines availability.

Aryaka's land-and-expand strategy spans nine solution categories across three buyer personas: network buyers (global connectivity, MPLS migration, last mile), IT buyers (cloud acceleration, SaaS/GenAI acceleration, secure remote access), and security buyers (NGFW, NGFW-SWG, Unified SASE as a Service). The GTM lands with connectivity solutions for new logos, expands through IT-focused upsells, and cross-sells security, requiring established credibility. Customer preferences split distinctly — networking customers prefer a fully managed service, while security customers want self-service via the MyAryaka portal.

The 2025 Unified SASE 2.0 platform added Universal ZTNA, launching mid-November with a two-tier POP architecture: 40+ Tier 1 distributed POPs for backbone connectivity and thousands of Tier 2 POPs via a partner network for user proximity. Once on the backbone, remote users can access any customer site. Additional launches include next-generation DLP with natural language processing and AI security capabilities. Aryaka reports 60% of SD-WAN renewals now include security components, and 120% year-over-year growth in new logo acquisition, with a 95% conversion rate on hosted firewall migrations displacing Palo Alto and Check Point branch firewalls.

Cato Networks

Cato Networks is a leading pure-play SASE vendor with a cloud-native platform purpose-built from the ground up. The value proposition centers on replacing legacy infrastructure with an open, modular architecture that combines SD-WAN, a global private backbone, and embedded, cloud-native security with single-pass processing. With over 3,800 enterprise customers across 190 countries, 55,000+ connected sites, 1.8 million ZTNA users, 1,500 employees, and $300 million+ ARR growing at 45% year-over-year, Cato outpaces the 28% SASE market CAGR.

Strategically, Cato has shifted from platform-first to modularity-first positioning as it moves upmarket from mid-size to the largest enterprises — recognizing that customers may prefer buying specific solutions rather than being forced to adopt a platform wholesale, though platform value compounds over time.

Their September 2025 AIM Security acquisition significantly enhances AI security capabilities. AIM addresses securing AI interactions across three categories: AI You Use (third-party applications such as ChatGPT, Copilot, and IDEs), AI You Build (homegrown applications and agents), and Agentic AI (local and managed agents). AIM integrates into Cato's SASE engine and can coexist with existing SSE or SD-WAN deployments from third-parties, and is sold standalone or as an expansion of existing Cato footprint. Cato is also shifting SSE pricing from bandwidth-based to user-based, aligning with market convention.

Netskope

Netskope excels as an SSE and SASE market leader with its cloud-native Netskope One platform built on robust CASB and DLP foundations. The single-pass Zero Trust architecture integrates SD-WAN, CASB, SWG, ZTNA, DLP, and FWaaS. A key differentiator is NewEdge Private Cloud—dedicated compute infrastructure across 75+ regions globally, with owned hardware data centers (not public cloud-hosted) and top-tier service provider partnerships for guaranteed SLAs and five-nines availability.

Netskope's go-to-market engages both security and networking buyers, with ~75% of deals involving both teams. Entry points vary — CASB for security-led engagements, network modernization for infrastructure-led deals. The company maintains multi-vendor SASE partnerships with Silver Peak and other SD-WAN vendors, extending Digital Experience Monitoring into partner networks rather than forcing single-vendor adoption. Universal ZTNA with Copilot capabilities automatically discovers applications and provides policy recommendations, running locally without cloud traffic for on-premises connections.

Netskope's September 2025 IPO at $7.3 billion valuation validated the SASE market and increased visibility among large enterprises. However, SD-WAN remains a small portion of the business. The company has not announced plans to address the WLAN or NaaS segments, and it continues to partner for campus environments. NAC replacement represents a growth opportunity as customers move away from traditional solutions toward unified ZTNA, providing holistic east-west control.

Palo Alto Networks

Palo Alto Networks leads in converging network security and connectivity through cloud-delivered Prisma SASE, which embeds security into branch networks via Prisma SD-WAN and extends cloud security through Prisma Access. The company recently crossed $1.3 billion in SASE ARR, serving 6,800 customers, and claims the fastest growth among SASE vendors at scale.

Enterprise feedback indicates Palo Alto products are perceived as more complex and higher-priced than competitors. Without native WLAN hardware, the company partners with vendors like Nile and Shasta Cloud for campus networks and maintains SD-WAN partnerships with Arista VeloCloud, HPE Aruba EdgeConnect, and Cisco Catalyst. This reliance on partnerships for networking infrastructure creates a competitive disadvantage compared with full-stack vendors like Cisco, HPE, and Fortinet, particularly in mid-market opportunities.

Versa Networks

Versa Networks offers a comprehensive "Universal Secure SASE" platform with a unified console, policy framework, data lake, and operating system (VOS). Versa has an extensive feature-set that covers all elements of SASE across campus and branch environments. The company has a strong MSP presence, with many global and regional providers building managed SD-WAN services on the platform.

Versa differentiates through both an integrated platform as well as deployment flexibility: shared cloud, Versa Private SASE (dedicated, Versa-managed), and Sovereign SASE (air-gapped, customer-operated). Their approach appeals to enterprises with data sovereignty requirements. The company indicates that it has achieved success with large enterprises where Cisco and Palo Alto Networks historically maintained strong positions. Campus capabilities today (LAN support) are tailored for branch office integration rather than full enterprise deployment.

Networking-Led Vendors

Arista Networks

Arista's enterprise connectivity strategy centers on a software-first approach with a single operating system (EOS) running across all networking devices—campus, data center, and WAN edge. This architectural consistency eliminates operational silos: for example, enterprises qualify software once, learn troubleshooting once, and remediate security advisories uniformly. The CloudVision platform and NetDL (Network Data Lake) serve as the central repository for network state and telemetry, enabling AI-driven automation through AVA (Autonomous Virtual Assist) and unified security policy orchestration across domains.

While not traditionally viewed as a security company, Arista has built purpose-built security capabilities, including CloudVision AGNI (cloud-based NAC), brownfield NAC interoperability (ClearPass, Cisco ISE, and Forescout), Multi-Domain Segmentation Services (MSS) for micro-segmentation without proprietary headers enforced at wire speed in EOS switches, and Network Detection and Response (NDR) via AVA sensors embedded directly in EOS that stream telemetry for threat identification and automated response.

The July 2025 VeloCloud acquisition from Broadcom brings over 20,000 enterprise customers and a mature MSP channel. Rather than forcing immediate EOS integration, Arista is taking a phased approach — VeloCloud Orchestrator remains the day-to-day platform while telemetry integrates into NetDL and CloudVision. For SSE, Arista maintains best-of-breed partnerships with Zscaler, Palo Alto Networks, and Netskope. The company is expanding down-market through new, lower-end products, simplified GUI-driven workflows for mid-market operators, and by leveraging existing Wi-Fi managed service partners and now VeloCloud MSP relationships.

Ericsson Enterprise Wireless Solutions

Ericsson Enterprise Wireless Solutions (formerly Cradlepoint) delivers wireless-first SASE optimized for 5G and LTE environments. The NetCloud SASE platform combines cellular-centric SD-WAN with integrated security capabilities acquired through Ericom, including SWG, RBI, CASB, and ZTNA. In April 2025, Ericsson launched the industry's first clientless ZTNA for Wireless WAN, enabling secure access without VPNs or browser plug-ins — ideal for third-party and BYOD users connecting to IoT/OT devices and corporate applications. The solution leverages built-in application isolation that runs sessions in isolated cloud containers, creating an air gap between corporate resources and unmanaged devices.

NetCloud SASE delivers SD-WAN with intelligent bonding for increased resiliency across multiple WAN connections (wired, cellular, satellite), supporting 5G network slicing for application-specific quality of experience. The platform is managed through NetCloud Manager, providing unified deployment, visibility, and policy enforcement across 5G WWAN, SD-WAN, and security features. Starting August 2025, Ericsson started offering wired and wireless LAN integration capabilities, and in September 2025, Ericsson announced agentic AI updates focused on day-two operations and AIOps for 5G-based networks, providing IT teams with actionable insight into network performance and automated troubleshooting. Ericsson targets enterprises where wireless connectivity is primary — retail stores, branch offices, vehicles, IoT deployments, and temporary sites — positioning itself as the 5G-optimized alternative to wireline-centric SASE vendors.

Extreme Networks

Extreme Networks launched Platform ONE in mid-2025, a converged management platform integrating networking, security, and AI — among the first to incorporate autonomous AI agents for policy, risk, and configuration management. Platform ONE includes Universal ZTNA, unifying cloud NAC and ZTNA under a single identity-based policy engine with integrations for Microsoft Entra ID, Google Workspace, and Okta.

Extreme relies on partnerships rather than offering a fully integrated, native SASE solution. NaaS is primarily a flexible financing and subscription model; in early 2025, Extreme enabled MSPs to leverage Platform ONE for consumption-based billing with pooled licensing.

RUCKUS Networks

RUCKUS Networks leads in high-density campus environments — stadiums, public venues, universities — through proprietary RF technology designed to combat interference and signal degradation. ZTNA capabilities are delivered via the RUCKUS Edge platform, which enables micro-segmentation.

RUCKUS differentiates through deployment flexibility: cloud-managed, on-premises, and controller-less options. However, the company lacks rich SD-WAN and other SSE capabilities, limiting its competitiveness in SASE opportunities that require comprehensive networking and security integration.

Campus NaaS Vendors

Join

Join positions itself as an AI-powered secure network platform company. Originally building custom access points to reduce Wi-Fi AP and LAN switching costs for its NaaS model, the company has evolved to serve two primary segments: commercial real estate (office, multifamily, industrial, retail, hospitality) and Fortune 1000/mid-market enterprise customers. The company maintains operations in North America and Japan (through a joint venture) and a growing presence in Southeast Asia.

Join's Graphite solution platform is containerized, running on-premises or in the cloud, with custom stream processing for continuous observability. The AIOps development combines seven years of historical data with real-time data for its model training. Join presents its hardware cost advantages as significant: whitebox Wi-Fi 7 access points cost almost 10 times less than equivalents from the leading vendors like Cisco and HPE.

The Join business model has evolved from pure NaaS to a virtual OEM model with component flexibility — MSPs and MSSPs can choose managed offerings or operate them themselves, addressing IT staff concerns about displacement. Hardware partnerships span 60+ switch SKUs and 25-30 access point SKUs from Celestica (high-end switching), Foxconn/CyberTAN (mid-range), and Actiontec (best Wi-Fi 7 AP for performance/uptime). Micro-segmentation capabilities provide the foundation for Zero Trust. Their firewall offering focuses on IoT/OT security rather than competing with major vendors like Palo Alto and Fortinet.

Meter

Meter, founded in 2015, recently raised $170 million in a Series C round led by General Catalyst in June 2025, bringing their valuation to over $1 billion. he round included participation from Microsoft, Sequoia Capital, J.P. Morgan, and a roster of Silicon Valley luminaries and founders. Channel partners, including CDW, Microsoft, and WWT, are bringing Meter's solution to a wider customer base. In November 2025, Meter announced a strategic partnership with Lumen Technologies to deliver a unified WAN-to-LAN solution. Available through Meter Connect and soon in the Microsoft Marketplace, the offering enables enterprises to purchase integrated connectivity through a single AI-driven procurement flow.

Meter's positioning centers on vertically integrated infrastructure — controlling the entire stack (hardware, firmware, operating system, cloud management) to deliver superior customer outcomes. Meter's Command, its generative AI provides natural-language troubleshooting, configuration, and custom visualizations. At MeterUp 2025, the company announced that Command now automates network design and configuration end-to-end.

Meter unveiled nine new hardware platforms, including security appliances (dual high-availability 20Gbps and 50Gbps WAN firewall units), multi-gig PoE switches with 25 Gbps backbones, and Wi-Fi 7 access points. A 5G Gateway is standard in all deployments for backup connectivity. The company integrates with third-party SASE providers. Pricing has been streamlined per square foot, with 100% partner fulfillment. Customers like Bridgewater, Lyft, and Reddit rely on Meter across thousands of employees and locations, with target verticals including distributed retail, MDUs, warehouses/logistics, education, and manufacturing. Geographic presence spans the US, Canada, the EU, and the UK, with expansion planned into Europe, the Middle East, Asia, and data centers.

Nile

Nile is redefining secure connectivity for branch and campus networks globally through a Secure Network-as-a-Service (NaaS) approach. CEO Pankaj Patel, a respected ex-Cisco networking veteran, and founder/board member John Chambers (former Cisco CEO and Chairman) lead a team that has raised $300 million to re-invent network security at the edge. Nile's core thesis holds that the LAN security remains the "Wild West" compared to data center and WAN evolution — 90% of enterprise locations have high user and device density, but have no dedicated IT staff.

Nile delivers cloud services to the LAN with autonomous operations built on a Zero Trust fabric foundation. Its Zero Trust Fabric has "built-in" security that unifies wired/wireless convergence, IT/OT integration, and network and network security constructs. Nile features "datacenter-class" capabilities like micro-segmentation, breach prevention, IoT/OT security with a blast radius of 1. A standardized architecture means fixes applied to one deployment are automatically deployed to all. Nile's autonomous operations takes on the entire operations lifecycle from Day 0 to Day 1 through Day N. Furthermore, Nile delivers a suite of secure cloud services to the LAN including wired/wireless access connectivity, DHCP, RADIUS, guest and edge services. Nile

financially guarantees end-to-end performance SLAs for the LAN.

The company aims to solve the long-standing industry problem of security and operational complexity at the edge, where it says $3+ in operations is spent for every $1 invested on technology. Nile's NaaS architecture delivers 30-50% cost savings, with OpEx based subscription offering allowing CxOs to deliver outcomes to their organization built on security, speed, simplicity and cost savings. Operating in 30 countries across 14+ verticals, Nile targets mid-to-large customers with complexity challenges, and has secured hundreds of installations globally, including several in the Fortune 500.

Ramen Networks

Ramen exclusively targets the "uncarpeted enterprise" — warehouses, outdoor work yards, logistics hubs, factories, farms, shipyards, refineries, and higher education campuses where workers, robots, and IoT devices perform mission-critical tasks in rugged environments.

Ramen's NaaS solution combines Wi-Fi 6/7, private 5G/CBRS, and mmWave connectivity with built-in Zero Trust network access and ransomware protection. The platform features agentic AI that automates Cisco, HPE, and white-box network deployment and operations, claiming a 30% reduction in IT workload with ROI in under 12 months. An intelligent agent continuously collects operational data across sites, building live digital twins that highlight root causes and predict issues. A plug-and-play stack with vetted NVIDIA and Qualcomm AI appliances enables computer vision and predictive maintenance deployments.

In April 2025, Ramen announced a strategic partnership with Genians, a Korean ZTNA/NAC leader, to deliver an AI-powered converged network and security platform addressing IT, OT, and cloud environments. Ramen operates through a 100% channel model with 3-5-year contracts priced by area covered and SLA requirements.

Shasta Cloud

Founded in 2022 by ex-Ruckus veterans, Shasta Cloud occupies a distinct competitive position: rather than competing in traditional enterprise bake-offs against NaaS pure-plays like Nile or Meter, the company focuses on winning MSP mindshare by enabling service providers to compete directly with networking vendors and emerging NaaS offerings.

A key architectural differentiator is the company's commitment to open systems and white-box hardware - MSPs and customers can purchase hardware directly from factories at cost, enabling mix-and-match deployments that combine access points from different silicon vendors within the same building. Shasta Cloud actively contributes to and leverages open-source initiatives through the Telecom Infra Project (TIP). The company builds on OpenWi-Fi and OpenLAN Switching standards, focusing engineering investment on MSP enablement, cloud management, and the automation of network design, deployment, and operations.

Target verticals include MDUs, hospitality, retail, and education — mid-market environments where buildings lack dedicated IT departments and rely on MSPs. The current product portfolio includes Wi-Fi access points, switches, and cloud management, with an edge gateway/compute device in development combining firewall and server functionality for on-premises applications. For security, Shasta Cloud maintains a **strategic partnership with Palo Alto Networks**, integrating Prisma SASE capabilities. Pricing follows an all-inclusive per AP or switch subscription. Geographic presence currently spans North America and Australia, with planned expansion into Europe.

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

Rev B