

Enterprise Edge and Cloud Networking

Digging into the alphabet soup of SASE, SD-WAN, SSE, ZTNA, MCN, NaaS

RESEARCH BRIEF



Table of Contents

State of Enterprise Connectivity – An Alphabet Soup	1
Market Drivers and Trends	1
What’s Working and What’s Not.....	3
Enterprise WAN and Cloud Connectivity Landscape	6
Why Achieving a Universal Fabric in the Enterprise is Hard	8
Mapping the Space	8
The Managed Services Opportunity	10
CSP Opportunity.....	10
MSP Opportunity	11
Landscape and Select Vendor Examples	11
SD-WAN - Pure Plays	11
SSE - Complementing SD-WAN	12
SASE – The New Holy Grail?.....	12
ZTNA – A Framework Poised to Take Over	12
MCN – Charting a Different Path.....	12
Abstraction Redefinition – Networking and Security	13
NaaS - What Does it Mean?	13
Standardizing SD-WAN and SASE	13
Enterprise Considerations – AvidThink’s Views	14
Security + Networking – Converged or Not?	14
Network and Applications – Converged or Not?	14
Policy and Identity Considerations.....	14
Journey to Unified	15
Conclusion and Final Words.....	15

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, private wireless, edge computing, SD-WAN, SASE, SSE, ZTNA, cloud and containers, SDN, NFV, 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 the Wall Street Journal, Light Reading, Fierce Telecom, Fierce Wireless, Mobile World Live, and other major publications. Visit AvidThink at avidthink.com.

A man with glasses and a beard, wearing a white shirt and tie, is sitting at a desk and smiling. A woman in a light-colored blazer is leaning over his shoulder, also smiling and pointing at the laptop screen. The background shows a bright office with a bulletin board.

Say Goodbye to Network Complexity.

Say Hello to Networking Designed for the **Cloud Era.**

The **Alkira Cloud Network** as a Service:
One Platform for Complete Network
Modernization.

- Build your multi-cloud network in minutes
- Enhance security with integrated firewalls
- Reduce costs without hardware and software

Visit [Alkira.com](https://www.alkira.com) to get started.

Zero Touch Edge Orchestration

Aarna Edge Services
(AES) is here

AES solves the complexity of edge orchestration while supporting multi-cloud use cases across the edge and public clouds — all with user-friendly management from a single pane of glass.

aarnanetworks.com/products/aes



AARNA NETWORKS

AES

Enterprise Edge and Cloud Networking

State of Enterprise Connectivity - An Alphabet Soup

The enterprise connectivity landscape is quickly evolving due to cloud adoption, increased globalization, and evolving workplace dynamics. The transition and decentralization of traditional network infrastructures introduce new challenges and opportunities. As digital transformation pervades all business operations, enterprise connectivity has evolved beyond facilitating corporate communication, becoming a strategic business tool.

The scope of connectivity decisions varies widely, impacting everyone from CIO/CISOs at Fortune 500 companies to small and medium business (SMB) owners with hundreds of employees. Today's connectivity solutions must accommodate a vast range, from home offices, mobile locations, remote offices, factory floors, private data centers, and public clouds to partner sites. The diversity of devices, operating systems, and form factors (bare metal, VM, containers) adds complexity, especially with privacy, security, and compliance needs.

Networking and security vendors and managed service providers (MSPs) promise relief through various solutions with acronyms like SD-WAN, SASE, SSE, ZTNA, and MCN¹. These may include optional security features sporting more acronyms like CASB, DLP, SWG, RBI, FWaaS², and micro-segmentation. To offer a simplified view, some providers present Network-as-a-Service (NaaS) as an umbrella term encompassing these multifaceted solutions. Unfortunately, the term, NaaS, is so diluted – hijacked to mean bandwidth on demand, managed WAN, managed LAN, advanced SD-WAN – that it's unclear whether it will succeed as a category name. Regardless, this veritable **alphabet soup** of acronyms serves to confuse even the most diligent and capable CISOs, especially when vendors continually redefine and reclassify each category to fit their needs.

In this updated edition of our enterprise edge and cloud networking report (originally called SD-WAN/SASE reports), we revisit the market through different lenses, including our previously proposed universal networking fabric (UNF) framework. Despite ongoing changes in terminology, we aim to provide our enterprise and service provider readers with fresh insights and successful strategies amidst fast-paced market evolution, misinformation, and confusion.

Market Drivers and Trends

Several drivers and trends are reshaping the state of enterprise connectivity, pushing organizations to redefine their network infrastructures and strategic approach. Prime among these are work habits changes, workload and topology changes, and ongoing security challenges.

Work Habit and Location Changes

As enterprises figure out their work-from-anywhere strategy to balance flexibility with productivity and collaboration, CISOs are tasked with enabling secure anytime-anywhere connectivity from multiple locations and multiple device types to diverse resources anywhere.

¹SD-WAN: Software-Defined Wide Area Network, SASE: Secure Access Service Edge, SSE: Secure Services Edge, ZTNA: Zero Trust Network Access, MCN: Multi-Cloud Networking. For detailed descriptions of these acronyms, you can download an earlier edition of this report at <https://nextgeninfra.io/sd-wan-sase/>

²CASB: Cloud Access Security Broker, DLP: Data Loss Prevention, SWG: Secure Web Gateway, RBI: Remote Browser Isolation,

As digital transformation pervades all business operations, enterprise connectivity has evolved beyond facilitating corporate communication, becoming a strategic business tool.

Access locations include home offices, remote offices including manufacturing sites, field sites, global offices, and on-the-go places like airports and hotels. Some sites will have local IT resources like printers, file shares, IoT devices like thermostats, coffee machines, or surveillance cameras.

Meanwhile, today's employees expect support for diverse devices, including laptops (Mac, Windows, Chromebooks, Linux), tablets, and phones (iOS, Android).

Finally, the type of resources employees need will depend on the type of organization they work in. Software development, oil and gas, transportation, and logistics firms will have different needs from organizations like primary education, universities, federal, state, and local government, or national defense contractors. The level of security and compliance will be similarly impacted by the organization type.

Workload and Topology Changes

Regardless of organization type, enterprises increasingly adopt cloud-based solutions, resulting in a profound shift from centralized, on-premises workloads to distributed, cloud-based ones.

The emergence of multi-cloud environments and edge computing coupled with ongoing Internet of Things (IoT) adoption are driving the evolution from hub-and-spoke network topologies to complex, distributed ones. This shift requires a new generation of networking solutions that can support the performance, reliability, and agility needed to manage dynamic workloads and topologies.

Traditional VPN functionality that exists as part of edge firewalls, next-generation firewalls (NGFW), branch routers, and even multi-point distributed VPNs are showing their limits. Software-based VPNs, while more flexible in accommodating virtualization and cloud migration, can't scale or adapt to new needs that require on-demand, fine-grained access to resources.

Growing Security Burden

This decentralization of networks has further resulted in a larger attack surface, presenting significant security challenges for enterprises. New workloads being instantiated on shared cloud infrastructure that enterprises can't control add to IT headaches.

This decentralization of networks has resulted in a larger attack surface, presenting significant security challenges for enterprises. New workloads being instantiated on shared cloud infrastructure that enterprises can't control add to IT headaches.

Traditional security measures are proving inadequate in the face of sophisticated threats, forcing organizations to seek security-centric network solutions. Integrating advanced security features directly into network architectures is now a critical requirement. Strong CISO interest in SASE, SSE, and ZTNA is evidence of this sentiment.

Government security frameworks and guidance are evolving to incorporate zero-trust and cloud security topics. For instance, the US National Institute of Standards and Technology (NIST) has begun the process of updating its Cybersecurity Framework (CSF) from 1.0 to 2.0¹ to address emerging topics such as supply chain risk management, zero trust architecture, and cloud security. And in Europe, ENISA, the European Union Agency for Cybersecurity, recognizes the migration to the cloud and recommends the adoption of zero-trust frameworks in their recent ENISA Threat Landscape (ETL) report², an annual report on the status of the cybersecurity threat landscape.

¹NIST CSF 2.0: <https://www.nist.gov/cyberframework/updates/nist-cybersecurity-framework-journey-csf-20>

²ETL 2022: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

Cyber insurance providers that enterprises depend on for funding to recover from breaches and ransomware attacks are raising their security requirements and expected to push for zero-trust, segmentation, and strong identity controls over IT infrastructure, including networks.

This means that many organizations will want security baked in when connectivity to any new or existing enterprise resources is instantiated – in public clouds, private clouds, and anywhere on enterprise premises.

Convergence of IT and OT

Non-IT devices with connectivity have been around for a while. Operational technologies (OT) industrial devices tended to rely on specialized protocols like PROFINET and ModBus. Increasingly, new generations of OT devices, like IoT devices, are using modern connectivity protocols like MQTT, utilizing and providing RESTful APIs, and relying on TLS for encryption. More importantly, these devices are now communicating with services in the cloud for control, software updates, and to upload data for analytics and machine learning. Whether on the factory floor, medical facilities, transportation hubs, or agriculture fields, industrial devices need local and remote connectivity.

Organizations within these vertical industries will invariably want a unified approach that can handle both IT and OT connectivity across sites and cloud applications processing OT and IoT data.

Alignment of DevOps with IT

Many organizations today conduct software development and DevOps activities. Data analytics, custom application development, and in-house application deployment for private data processing require developers to connect to resources in both private and public clouds, from offices, homes, and while on the go. Legacy approaches of standing up software VPN gateways everywhere, relying on VPN clients, or tunneling all traffic over a secure shell (SSH) can't easily scale with development needs. VPNs also expose whole subnets of resources behind the gateways, facilitating lateral movement of cyber-attackers – not ideal from a security vantage point.

Furthermore, with the increasing use of multiple clouds, including hybrid public/private clouds, application components will need cross-component secure connectivity; likewise between the application and private data sets.

Increased emphasis on AI and machine learning workloads (including Large Language Models and Generative AI) will drive more transfers of large data sets and trained AI models between different locations as part of a DevOps or application initiative. Cloud infrastructure teams at organizations that previously handled computing and storage management will have to contend with complex hybrid multi-cloud connectivity.

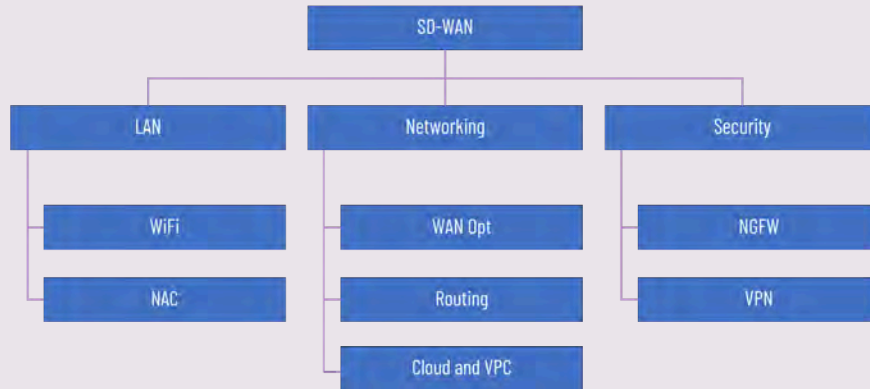
DevOps teams value connectivity tools they can control without bothering IT (or oversight from IT). However, IT and security teams want to ensure that developers and the applications they build conform to enterprise compliance and security standards. This tug-of-war over independence (efficiency) versus security between DevOps and IT security will have to be sorted out.

What's Working and What's Not

Organizations today are grappling with their transition from traditional enterprise networking setups, which consist of:

- **Remote branches and campuses** – Branch routers with limited cloud/central management or NGFW with routing capabilities. Both have VPN gateways that allow remote inbound access. Many enterprises relied on expensive MPLS circuits even as cheaper broadband options became available. Meanwhile, for branch and campus LAN, WiFi and Ethernet switches are managed and treated separately from WAN/edge access though there's increasing adoption of cloud-managed enterprise WiFi routers that provide WAN capabilities with on-site WiFi.
- **Private data centers** – Physical routers or NGFWs protect application resources and allow site-to-site VPN access.
- **Public clouds** – Software or virtual routers/NGFWs that provide VPN gateway or site-to-site VPN access (including from cloud to cloud).
- **Mobile and home locations** – Software VPN clients on mobile and laptops for users to access resources on enterprise premises or private resources in the cloud.

SD-WAN – Many Services Under an Ambiguous Umbrella



avidthink.com

SD-WAN Solves Initial Remote Branch Woes

To address the remote branch management challenges, enterprises have adopted SD-WAN. With its ability to utilize multiple links and actively maintain quality of service (QoS) over cost-effective broadband services, SD-WAN has helped companies worldwide bring secure, reliable, and cost-effective connectivity to dispersed locations while reducing operational complexity.

As a result, the market has seen rapid SD-WAN adoption over the last few years (USD 2-3B in revenue in 2022, depending on analysts), and it continues to gain traction. Many communication service providers (CSPs) and MSPs today offer SD-WAN as a managed overlay service or in concert with basic connectivity. Unified communications (UC) are often bundled with SD-WAN offerings, as is basic enterprise edge security (stateful firewalls, etc).

Stepping up to SASE with SSE

Even as SD-WAN rollouts continue, all leading SD-WAN vendors are upgrading to become SASE solutions, or at least partnering with SSE vendors who can provide SWG, DLP, FWaaS, or RBI capabilities to achieve the same. This is in response to customer demands for protection from an increasing number of cyberattacks, and to further simplify the messy collection of point products across customer remote and campus sites.

As an umbrella term (defined in 2019 by analyst firm Gartner) that includes a kitchen sink of enterprise edge networking and security solutions, SASE is an all-encompassing concept that is hard to achieve in totality. Nevertheless, SASE is poised for rapid growth. Analyst firm Dell'Oro indicated that the SASE market doubled in size from 2021 to 2022 to over USD 6B¹, and it projects SASE revenue will surpass an aggregate of USD 60B from 2022 and 2027, with a 5X growth over that period.

¹Dell'Oro <https://www.delloro.com/news/sase-market-to-exceed-over-60-b-between-2022-and-2027/>

SASE – Throwing the Kitchen Sink at Enterprise Connectivity



avidthink.com

Powered by ZTNA, Cozying up to Applications

Meanwhile, a component of SASE, ZTNA, has emerged as a rising star with its ability to provide fine-grained, identity-based access control to network and server resources and the applications that sit on those servers, significantly improving enterprise security posture.

Zero-trust (ZT), a security philosophy that embraces least privilege, establishment of explicit trust, strict identification of users and devices, and a default deny-all policy, has been embraced by governments, critical industries, and top enterprises worldwide like Google (with BeyondCorp) and Coca-Cola. While ZTNA focuses on applying ZT principles to network access, we believe the overarching ZT access framework will drive the majority of access methodologies over the next decade. Compared to using VPNs for accessing private resources, ZTNA is a targeted approach that exposes the minimal attack surface beyond the application or resource in use.

Unfortunately, ZT is hard to apply comprehensively in practice, which explains poor adoption in the past. Even though the term zero-trust was coined in 2011 by Forrester analysts, the perimeterless security approach had been formalized in the early 2000s and popularized by organizations like the Jericho Forum. It's only in recent years that new vendors and implementations have tried to simplify and streamline ZT deployment for networks and applications.

Despite Progress, Challenges Lay Ahead

Leading SD-WAN solution providers, including Aryaka, Cato Networks, Cisco Viptela/Meraki, Fortinet, HPE Aruba/Silver Peak, VMware, and Versa Networks, all self-identify as SASE vendors today. To be fair to Cato Networks, they were already espousing elements of the SASE architecture years before the SASE umbrella term was coined.

The last few years have seen SASE vendors adding more features: SWG, DLP, IPS, FWaaS, ZTNA, CASB, RBI, and anti-malware to each of their product suites; sometimes through acquisition and other times via organic in-house development. For enterprise CIOs or SMB business owners, sorting through which vendor has which feature and understanding the maturity and usability of each new capability has been messy.

In our conversations with enterprises, we find their decisions are driven less by detailed feature-to-feature comparisons, and more by higher-level forces, including:

- Relying on analyst reports from Gartner, IDC, or Forrester to pick leading vendors (akin to “buying from IBM or Cisco”)
- Recommendations from trusted technology or business peer groups
- Existing IT business relationships – “we’re already a VMware shop,” “we’ve been a Cisco shop forever,” “we use Aruba for most of our networking,” or “we already trust Fortinet for firewalls.”
- Buy-in into a specific solution architecture and vision (e.g., single-vendor SASE versus best-of-breed multi-vendor) – “we believe in Cato’s single-vendor clean-slate architecture because it brings increased efficiency and we’re not bouncing between multiple vendors.”
- MSP or CSP recommendations – “our carrier offers Versa,” or “our MSP says Aryaka’s the right choice for us.”

Only the largest enterprises and select mid-enterprises have the cycles or capacity to run bakeoffs between shortlisted vendors. CSPs and MSPs are more likely to run bakeoffs and evaluate the adequacy of MSP features on the platform (MSP branding support, multi-tenancy, co-manageability). They will focus on profit margins, which lets niche white-label SD-WAN platforms play the cost-effectiveness card. Similarly, open-core/open-source options like flexiWAN have seen interest from CSPs and MSPs hoping to build in their own custom differentiated features, or just to keep costs down.

Even as enterprise-edge locations adopt SD-WAN and embrace SSE or make the full step up to SASE, open questions remain:

- How fast to converge networking and security offerings?
- How to maintain segregation of duties and ownership between security and networking teams in the enterprise? Who’s responsible for what?
- How to solve the multi-cloud networking problem for application stacks? Should MCN be part of the SD-WAN solution?
- How to address work-from-anywhere initiatives across various devices (laptops, tablets, mobile phones)?
- Is the enterprise WiFi router with improved security and WAN link capabilities a viable alternative to SD-WAN?
- How to adopt a ZT framework for connectivity and access? How to converge controls across applications and networks?
- What are the best practices to migrate traditional NGFWs and VPN solutions to SASE? What to do with IPS, DLP, and CASB appliances (virtual or physical) already deployed?

Moreover, the connectivity landscape is evolving to include development team needs, multi-cloud, IoT, and new entrants forcing a rethinking of the networking and security abstraction layer.

Enterprise WAN and Cloud Connectivity Landscape

Modern enterprises face the complexity of securing hybrid environments, with the need to connect various stakeholders to private and public resources. This complexity is compounded by the need to integrate or upgrade legacy branch routers, firewalls, and IPsec VPN setups, escalating the IT workload.

Our interactions with organizations ranging from cutting-edge startups to Fortune 500 companies reveal a universal demand for secure connections across:

- Main offices and campuses
- Remote branches, including temporary co-working spaces
- Home offices
- Mobile locations for traveling staff
- Public and private cloud resources, including VPCs and on-site facilities

Enterprises aim for secure and reliable connections across all these locations but also prioritize manageability, visibility, and consistency across different domains, considering the immense burden on IT staff.

This burden is intensified by the diversity of endpoints, including servers, desktops, laptops, mobile devices, VMs, container instances, and IoT devices. Communication between endpoints now involves more machine-to-machine (M2M) or app-to-app API interactions rather than solely human-to-application. In particular, IDC predicts a global total of 55.7 billion connected devices by 2025, 75% of which will be tied to an IoT platform. Further, these endpoints may not always be under the company's control, a problem accentuated by the rise in remote working, outsourcing, and offshoring, causing increased security risks in order to maintain productivity.

The Quest for a Universal Enterprise Network Fabric

Driven by the need for enhanced agility, performance, and security, enterprises are on a quest for a type of universal network fabric (UNF) - a grand unified theory of an architectural model that seamlessly integrates disparate enterprise resources on networks everywhere, providing a consistent and secure connectivity experience across all endpoints. We've written in the past about this fabric and suggested the capabilities needed for a cross-domain universal solution:

- **Layer 3 Reachability/Identity-Driven** – Ensures end-to-end Layer 3 compatibility while allowing for localized Layer 2 interaction, ensuring compatibility with broadcast and multicast domains. Endpoint identification should focus on the identity rather than IP addressing, with concessions for legacy IP-based controls.
- **Transport Agnosticism** – Compatible with any underlying WAN and LAN connectivity (MPLS, broadband, cellular), including both enterprise-controlled links and those in public clouds with restricted access. Future considerations involve tighter transport integration for improved performance and visibility.
- **Universal Endpoint Platform Support** – Accommodates various applications and components (e.g., microservices in containers) across various hardware types, including desktops, laptops, tablets, and IoT devices, with different strategies for each class.

Enterprise Unified Fabric Requirements - Easy to Say, Hard to Do



L3-based, Identity-driven



Directory Services Integration



Security-Extensible



Transport Agnostic



Policy-Driven/
Intent/Model-Based



Observable



Universal Endpoints (bare metal, containers, VMs, desktops, laptops, mobile)



Fine-Grained Entitlements



Software-Centric/
Hardware-Friendly



Multi-Domain (WAN, LAN, data center)



Privacy-Friendly



avidthink.com

- **Multi-Domain** – Supports end-to-end connections across WAN, LAN, and cloud networks in both private and public settings.
- **Identity and Directory Services Integration** – Integrates with external authentication and identity systems to inform the policy engine on access and privileges based on various attributes.
- **Policy-Driven and Model-Based** – Manages configuration through high-level policies for consistency and scalability, considering multiple factors such as device posture, location, IP reputation, and other contextual details.
- **Fine-Grained and Robust Entitlements** – Supports fine-grained controls to maintain compliance, prevent data leaks, and protect against malicious attacks, based on policy evaluations and presented identities.
- **Privacy** – Supports standard encryption methods with flexibility for cipher suite replacements as needed.
- **Security-Extensible** – Allows for advanced security services to be integrated into the traffic stream, like deep-packet inspection for DLP, IPS, or malware scanning.
- **Observability and Extensive Telemetry** – Offers visibility for easier troubleshooting and rich telemetry for reliable and performant connection monitoring.
- **Software-Centric, Hardware-Friendly** – While the connection components should be software-only, compatibility with hardware accelerators like SmartNICs, DPUs, or extended CPU instruction sets should be maintained for performance.

A fabric that adequately addresses all the elements above across all domains does not yet exist, though different enterprise networking solutions today meet a large number of the criteria, and stitching together different solutions can achieve almost all the above attributes.

Why Achieving a Universal Fabric in the Enterprise is Hard

Creating a single unified network fabric is challenging due to the increasing complexity of enterprise networks. The other reasons are related to enterprise operations:

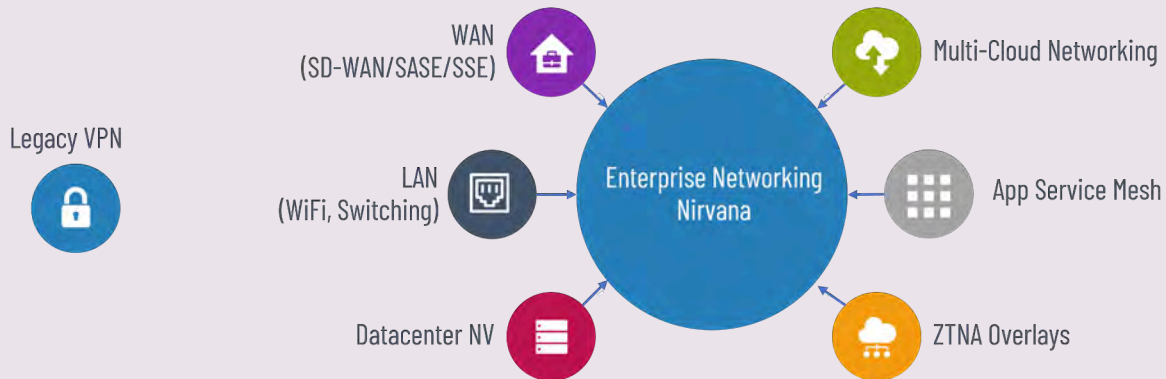
- Limited administrative span of control
- Different priorities across use cases
- Varying timescales of change across domains
- Tight budgets and lack of in-house expertise

Mapping the Space

As hard as achieving UNF nirvana is, it's still valuable to understand the overall landscape of available solutions. Enterprise connectivity solutions encompass a variety of technologies, each addressing different aspects of network performance, security, and management. These solutions stem from different domains, including:

- **WAN (SD-WAN, SSE, SASE)** – We're seeing ongoing migration of MPLS and legacy fixed access to adaptable, multi-transport, and converged connectivity-security links. Diverse SD-WAN solutions are striving to stay on top, evolving into SASE solutions that seek to redefine WAN connectivity through cloud-centric and security-centric frameworks. As we've stated, all these vendors are adding the alphabet soup of acronyms denoting enterprise-edge security capabilities to their solutions. We further see device-specific and enterprise-wide security capabilities like endpoint security XDR (Extended Detection and Response) being integrated into the mix.

Different Paths to Achieving a Unified Converged Networking Solution



avidthink.com

- **LAN (WiFi, Switching)** – It might be unusual to bring LAN technologies into a discussion focused on enterprise edge and cloud networking, which ostensibly covers multi-site versus on-site connectivity. However, cloud-managed LAN solutions like enterprise WiFi and switching have expanded their scope of coverage. Cisco Meraki, HPE Aruba, and Juniper Mist are tying in SD-WAN capabilities into their WiFi branch routers – from handling multiple links to adding smarter networking and security features to converging cloud-based management between WAN and LAN. The converse is also true, with multiple SD-WAN players like Versa Networks expanding into LAN management. Newer managed enterprise campus networking players like Nile (with the backing of Cisco’s former CEO John Chambers) will likely expand their scope beyond LAN to WAN.
- **Datacenter (network virtualization or NV)** – While SDN hype has dwindled, data center NV is still progressing and promising cross-cloud (multi-public-cloud, hybrid private-public cloud) connectivity with vendors like VMware promising bridges between SD-WAN and data center workloads.
- **Cloud and Multi-cloud Networking** – Most large enterprises utilize services from various public cloud providers. IDC indicates multicloud networking will become a major investment focus for 2023¹, with more than 56% of enterprises expected to increase spending. The need to connect across availability zones, cloud regions, and cloud providers to enact data transfers or for cross-component API calls has fueled a range of solutions. SD-WAN/SASE vendors tout virtual gateways, NV solutions propose multi-data center overlay fabrics, and hyperscalers are in the game with container-friendly (and even serverless-compatible) solutions like AWS’s Lattice. A number of multi-cloud specialists, including Alkira, Aviatrix, and Proximo, have each picked a differentiated path to market. Industry heavyweight IBM also recently announced its Hybrid Cloud Mesh, one of the latest entrants into this space.
- **ZTNA and Next-gen VPN** – Many of the above solutions aim to connect disconnected islands of networks (LANs in the data center, LAN at home, LANs on campus, LAN in branch offices) addressing both underlay (physical connectivity) and overlay (virtual connectivity) needs. Both IPsec and OpenVPN-based VPNs have historically played the overlay connectivity game, connecting sites or users/devices to sites. Nonetheless, most organizations recognize the need to move beyond legacy VPNs, and a new generation of ZT-enabled connectivity (ZTNA) has come along, leveraging TLS/mTLS (mutual TLS) or using

¹2022 Future of Connectedness Survey: <https://www.idc.com/getdoc.jsp?containerId=US49727922>

Wireguard (new VPN protocol built into Linux kernel) to enable targeted tunnels between users/devices and remote resources. SASE players like Cato Networks also tout their ZTNA solutions, but pure-play options like Google BeyondCorp, Perimeter 81 and DevOps-focused StrongDM and GoTeleport provide an alternate approach to secure connectivity. Infrastructure software leader, HashiCorp, joined in with their open-source Boundary, which they recently made available as a managed service.

- **Application (service mesh)** – Service meshes, associated with application component-to-component communication, assist with component discovery, performance, security, and visibility. Open-source solutions Istio, Linkerd, Kuma, Consul Connect, Open Service Mesh, Traefik, along with Envoy Proxy have established a foothold side-by-side with container networking stacks like Calico. There's debate over the inclusion of service mesh in our analysis due to the desire of some CIOs to separate the application and network domains. However, given the prominence of M2M communications and the expected growth in inter-application API traffic, we think it's important to start developing models around how application service meshes (and container networking) fits within overall enterprise network connectivity frameworks.

For each of these categories, leading vendors aim to leverage success in their domain to penetrate adjacent markets – SD-WAN growing into SASE, SD-WAN into LAN, SD-WAN to multicloud, or multicloud into SD-WAN/SASE. We'll discuss our view of how we see the space evolving in the next few sections, but before that, let's examine briefly the managed services opportunity for these solutions.

The Managed Services Opportunity

While many of the vendors in each solution category offer a direct-to-enterprise offering, we're seeing an increasing number of large and small enterprises opt for managed connectivity offerings. The ongoing shift towards cloud-based, unified network solutions presents significant opportunities for MSPs and CSPs. And the increasing complexity of managing enterprise networks, coupled with the need for specialized skills to fend off cybersecurity attacks and operate advanced networking technologies, is driving many businesses to consider managed services for their connectivity needs.

CSP Opportunity

Communication Service Providers stand to gain from the transition towards cloud-based networking solutions. The CSPs can evolve traditional connectivity services by incorporating managed SD-WAN and SASE solutions into their network underlay offerings, providing value-added services to their business customers. Another CSP angle is to provide multi-cloud connectivity by leveraging inter-exchange relationships, enabling direct cloud access with strong SLAs.

Furthermore, the move towards 5G allows CSPs to offer high-speed, low-latency mobile services or fixed wireless access integrated with advanced security capabilities. CSPs can similarly apply SASE, SD-WAN, and ZTNA to IoT services, providing security and visibility to devices that benefit substantially from security built into the network.

The one area that has been slower on the uptake is the carrier universal customer premises equipment (uCPE) initiative. We see forward movement on that as being linked to the outcome of enterprise on-premises edge computing strategies. While uCPE initiatives are in play at larger CSPs worldwide, the vision of swappable SD-WAN, SASE, and security services, along with a thriving marketplace of network service apps has not yet materialized. Few virtual network marketplaces exist, though one with traction is Equinix's Network Edge virtual network functions marketplace that's tied to the Equinix Cloud Exchange Fabric.

CSPs who can combine their strength in underlay networking, willingness to provide SLAs, economies of scale, and new security and network service offerings will earn significant new revenue.

In our work with CSPs, we've seen that the key to success in winning a role with enterprises as they evolve WAN and cloud connectivity is to demonstrate an understanding of enterprise workload challenges. Different CSPs have unique assets that can be leveraged in conjunction with these new services – whether a converged wireless and wireline core that provides a common location to run security services, pre-existing relationships with multiple cloud providers for direct connection services (AWS Direct Connect, Azure ExpressRoute, GCP Interconnect), or private APN services that integrate with secure SASE gateways.

CSPs who can combine their strength in underlay networking, willingness to provide SLAs, economies of scale, and new security and network service offerings will earn significant new revenue.

MSP Opportunity

The shift towards unified networking solutions represents a substantial opportunity for Managed Service Providers. MSPs can offer comprehensive network management services encompassing SD-WAN, SASE, ZTNA, and MCN, relieving businesses of the internal complexity of managing these technologies. Many enterprises can't evaluate or understand these services and will depend on external parties to pick and manage on their behalf.

MSPs can provide differentiated services such as network optimization, performance monitoring, and managed security services, making them an attractive option for enterprises looking to ensure optimal network performance and security.

Furthermore, MSPs can provide differentiated services such as network optimization, performance monitoring, and managed security services, making them an attractive option for enterprises looking to ensure optimal network performance and security.

We expect success for vertical-focused MSPs who can tie these new offerings with vertical industry needs – compliance, data privacy and sovereignty, unique workloads, and security.

Likewise, regional MSPs who can address both provisioning physical connectivity (through partnerships with regional, national, and global CSPs) and manage the latest WAN and cloud connectivity services can differentiate themselves against traditional MSPs offering basic managed WAN, NGFW, router, WiFi services.

Landscape and Select Vendor Examples

The enterprise networking space is replete with numerous solutions and vendors. Most major networking and security vendors today have an offering in this converging space for enterprise WAN edge and cloud connectivity – e.g., Check Point, Cisco, Cloudflare, Fortinet, HPE-Aruba, Juniper, Palo Alto Networks, VMware, and Zscaler. Enterprise CIOs or CSPs/MSPs making vendor selections can easily pull a list of vendors from other analyst market reports with quadrants, tables, and other creative depiction of vendors in the SD-WAN, SASE, SSE, ZTNA, and related spaces.

The goal of our report is not to provide a complete list of vendors in each space but to discuss landscape evolution in the context of a few select vendors notable in driving change.

SD-WAN – Pure Plays

Many SD-WAN players that started as pure plays and were acquired by larger entities have broadened into SASE offerings. Examples include VMware SASE (VeloCloud), Cisco Catalyst SD-WAN (Viptela), or Palo Alto Networks Prisma (CloudGenix).

Few SD-WAN pure-plays (i.e., without advanced security capabilities or with no roadmap towards SASE) exist today. The exception would be white-label offerings targeted at MSP solutions for SMBs, vertical-focused SD-WAN solutions from vendors like Mako Networks, and the open-source flexiWAN. For example, Mako targets verticals like quick-serve restaurants and gas stations (Chevron being a notable customer) with a PCI-certified platform – these enterprise purchasers are driven more by vertical-specific and payment-compliant capabilities and less by having the latest SD-WAN or SASE feature built in. Meanwhile, open-source/open-core flexiWAN provides a built-in firewall but integrates with external SSE solutions to provide additional security capabilities.

SSE - Complementing SD-WAN

Secure Service Edge (SSE) vendors are evolving their offerings to integrate more comprehensive security features and provide a broader range of network services. Many are partnering with SD-WAN and other networking vendors to complement existing networking stacks with their edge security solutions. Vendors like Netskope, Zscaler, Palo Alto Networks, Forcepoint, and Skyhigh Security, each with different feature maturity across SWG, CASB, DLP, ZTNA, and RBI, continue to strengthen their offerings while adding endpoint security options or increasing networking capabilities to round out their solution. Even Microsoft has just entered the market with their Entra SSE solution suite, consisting of Entra Internet Access, and (described below) a private access solution.

SASE – The New Holy Grail?

SASE is hailed as the new 'holy grail' of enterprise networking and security. In our conversations with CIOs, it might be better described as the 'holy kitchen sink' in terms of the massive number of features and functions rolled under a single umbrella. Enterprises adopting SASE are finding it hard to configure and manage the rich set of capabilities that comprehensive SASE services offer – especially complex features like DLP or CASB. Meanwhile, SASE vendors continue to build out more features, add more POPs and expand their private network backbones to improve performance and quality of experience. For example, Cato Networks has added DLP, RBI, and improved DNS security, even as they've expanded their POP footprint worldwide. Versa Networks has also built out a veritable menu of security and network features, extending now to campus LAN switches.

Given this cornucopia of potentially confusing SASE offerings, AvidThink recommends starting with use cases and working backward to understand which SASE subsets make the most sense. This is akin to triaging a patient in an emergency room – figure out the top three or four critical enterprise WAN and cloud networking issues, and use that as the evaluation criteria to pick the appropriate SASE vendor(s).

ZTNA – A Framework Poised to Take Over

Vendors in the Zero Trust Network Access (ZTNA) space are expanding their solutions beyond specialized use cases to serve broader enterprise needs. Look for players like Akamai, Cloudflare, Google BeyondCorp, Zscaler, and Perimeter 81 (which also provides other SASE features) to continue innovating and broadening their ZTNA offerings to support a wider range of network environments and use cases. Microsoft is also a player with their recently-announced Entra Private Access ZTNA product which leverages their identity platform (Entra ID, formerly known as Azure AD).

ZTNA is proving a popular alternative to enterprise VPNs due to its ability to limit the scope of remote connections by default. This is different from VPNs that require extensive access control list (ACL) configuration to constrain access by remote users. Many ZTNA solutions also employ reverse proxy approaches that allow secure tunnels to be established without exposing networking ports to on-premises or cloud infrastructure.

ZTNA's tight controls and application centricity (many ZTNA solutions are configured around applications versus networks) allow fine-grained access control that CISOs increasingly favor. The application-centric nature of ZTNA also means a different set of competing solution providers from outside the networking space. DevOps and application security tool players like Hashicorp, with their Boundary product or Tailscale, with their software VPN replacement are popular options. In addition, GoTeleport and StrongDM are other developer-oriented connectivity solutions that provide ZTNA-like capabilities. Beyond this, there's a long list of ZTNA providers, including AppGate, Axis Security, Banyan Security, Cyolo, TwinGate, and even NordLayer from the providers of the popular NordVPN solution.

MCN – Charting a Different Path

Vendors offering Multi-Cloud Networking (MCN) solutions, such as Alkira, Aviatrix, and Proximo, are carving a unique path in the enterprise networking space. They provide seamless connectivity and interoperability across multiple cloud environments, becoming increasingly crucial as enterprises diversify their cloud portfolios. These solutions focus less on providing built-in security features, choosing to partner with other vendors. For example, Alkira provides an easy way to insert security offerings from Cisco, Check Point, Fortinet, and Palo Alto into their cloud networking platform.

MCN capabilities can also be expanded beyond cross-cloud connects. Alkira recently added Extranet-as-a-Service to ease cross-company partner and third-party integration, and demonstrated how its platform could support fast integration during mergers and acquisitions activity.

MCN solutions focus on tying together development with cloud IT environments or facilitating data flow to and from on-premises into the cloud. While MCN solutions don't yet tout branch management, the same control and orchestration infrastructure can be extended to remote offices, and with the appropriate software clients, home and traveling users – this makes them a potential competitor to SD-WAN/SASE players.

Abstraction Redefinition – Networking and Security

Even as the industry appears to converge around the SASE framework, other approaches are forming. For example, we discuss a different approach to enterprise edge and cloud networking in [our recent report introducing the New Middle Mile](#).

Instead of trying to converge security and networking (SASE), companies like Graphiant (founded by a Cisco/Viptela alumnus) are taking an underlay-centric approach. Graphiant focuses on providing private connectivity with SLAs and direct paths to popular clouds and other B2B services via an interexchange capability. It leaves advanced security solutions to partners that run over-the-top services.

How many enterprises prefer a managed WAN with all-in-one security and networking versus a streamlined private connection with the option to run multiple security services over that link is unclear. SD-WAN/SASE momentum is hard to ignore but Graphiant has indicated strong early market interest, including from CSP partners.

NaaS - What Does it Mean?

While we're discussing categories, let's get into one that's been overused over the years and yet could become a new umbrella term that combines SASE with on-demand physical connectivity. The strength and confusion around Network-as-a-Service or NaaS stems from its vagueness. Beyond the fact that it's offered as a "service," there's little agreement on what "network" refers to. In particular, what level of service abstraction we're talking about and whether it's fully- or partially-managed isn't defined.

The standards body, MEF, with its CSP and networking vendor members, is trying to establish a definition. A simple search for NaaS, though, will show multiple networking vendors and CSPs using it to denote services ranging from managed WANs to SD-WAN to variations of SASE and even MCN. The managed secure campus LAN company, Nile, uses NaaS to describe its offerings of managed WiFi and managed switches.

AvidThink will be watching closely to see how the market evolves to embrace one definition over another. We think convergence might take a while.

Standardizing SD-WAN and SASE

While analyst firms like Gartner have attempted to define the high-level capabilities of SD-WAN and SASE, there are no widely-accepted standards for SD-WAN and SASE today.

Many SD-WAN and SASE vendors continue to show limited interest in driving standards during this phase of rapid growth and land grab. Meanwhile, in concert with MEF, large CSPs want to create a common standard for orchestration and management.

Under the MEF 3.0 SD-WAN Services standards (part of the MEF Global Services Framework), MEF members have established MEF 70.1 (updated version of MEF 70) that lays the foundation for MEF services, creating a terminology and framework for evaluating SD-WAN services. Meanwhile, MEF 88, Application Security for SD-WAN Services, aims to define security functions and actions that can be applied to SD-WAN application flows. Other active standards include testing-related SD-WAN efforts in MEF 90.1 and MEF 131.

Other works in progress relating to SASE and beyond include:

- MEF W117 SASE Service Attributes and Service Framework
- MEF W118 Zero Trust Framework and Service Attributes

- MEF W119 Universal SD-WAN Edge Implementation Agreement
- MEF W105 Performance Monitoring and Service Readiness Testing for SD-WAN

We applaud MEF's attempt to bring order to the chaotic space but recognize pragmatically that most vendors are focused on winning market share today. Furthermore, CSP wins are mostly pull-throughs from the enterprise. I.e., if many significant enterprise customers demand the CSP carry a specific vendor, the CSP will do so, regardless of whether the vendor is standards-compliant. There's an uphill battle here but perhaps one worth fighting for if you're a CSP.

Enterprise Considerations – AvidThink's Views

As enterprises navigate the complex landscape of network transformation, they must address several key considerations to ensure successful implementation and alignment with business objectives. These include assessing the convergence of security and networking, evaluating the relationship between network and applications, deciding the right abstraction between underlay and overlay, considering policy and identity aspects, and charting a path towards unified networking.

Security + Networking – Converged or Not?

Converging security and networking into integrated, cloud-native solutions is a significant trend. This approach offers many benefits, such as reduced complexity, consistent security enforcement, and improved network performance. However, it requires a shift in organizational structures and processes, which can present challenges. Businesses must carefully assess their needs and capabilities before deciding if this convergence is the right approach.

The other element to consider is that the vendors may end up doing the convergence on behalf of the enterprise. We anticipate more acquisitions in the market as networking vendors grab security vendors to broaden their offering. In the meantime, enterprises who've chosen to go the managed (MSP) route can leave it to their preferred MSP partner to sort out some of the complexity on their behalf.

Network and Applications – Converged or Not?

The relationship between networks and applications is evolving. Traditional network architectures were not designed to support today's cloud-based, microservices-driven applications. Enterprises can consider converging their network and application strategies, moving towards architectures that provide flexibility, scalability, and performance to support modern applications.

The difficulty here will be the development and DevOps teams' desire for independence and agility – they likely want to pick the access tools that integrate cleanly into their DevOps pipelines. Meanwhile, IT and security want to set templates and frameworks that keep the company safe. We expect ZTNA solutions (and perhaps MCN) to be the first to evolve in this convergence. One possible enterprise-wide architecture is to enact encrypted layer 3 connections across all enterprise sites and end-points and count on an overlay ZT framework for application, development, and network access. This relatively ambitious undertaking will require today's solutions to mature and improve their flexibility in deployment and management-at-scale capabilities.

The difficulty will be the development and DevOps teams' desire for independence and agility – they likely want to pick the network and security access tools that integrate cleanly into their DevOps pipelines.

Policy and Identity Considerations

In the context of network transformation, policy, and identity management play a critical role. Modern network solutions, such as ZTNA, rely on robust identity and policy management to ensure secure access to network resources. Enterprises must consider the implications of these factors on their network strategy, ensuring they have the necessary systems and processes to manage identity and policy. The tie-in between ZTNA and identity is at the heart of Microsoft's recent move to unify their identity and security solutions under the Entra brand and represents an interesting shake-up of the space.

As cyberattacks mount, AvidThink believes that governments worldwide and the industry will have no choice but to wholeheartedly embrace ZT frameworks – ZT access at both the network and application levels will form best practices. NIST standards in the US and ENISA in Europe already recommend ZT principles. In the longer term, we anticipate a re-categorization of the secure access market with ZT as the defining umbrella methodology and network, application, and infrastructure resource access as sub-categories. Regardless of analyst categorization, quadrant, or wave frameworks, the pragmatic reality is that enterprises need to chart their path towards a ZT approach across all IT, OT, and development environments.

Journey to Unified

The journey to a unified network involves several potential paths. Each enterprise's journey will depend on its unique business requirements, existing network architecture, and strategic goals. However, some common paths we have seen in the market include:

- **SD-WAN to SASE (including SD-WAN + SSE):** Many enterprises are finding that a natural first step in network transformation is the adoption of SD-WAN, followed by transitioning towards SASE to integrate advanced security capabilities.
- **MCN standalone or MCN with SD-WAN:** Depending on their cloud strategy, enterprises might choose to implement Multi-Cloud Networking (MCN) separately or in combination with SD-WAN to ensure efficient connectivity across multiple cloud platforms.
- **ZT as overlay followed by ZT as overarching framework:** Enterprises might begin by implementing Zero Trust (ZT) as an overlay on their existing network, then gradually evolve towards a complete ZT framework as they transition from private to public resources.
- **Other Paths:** Other potential paths include adopting edge networking solutions to support IoT and other edge devices or the implementation of AI and machine learning to automate network management and enhance security.

Conclusion and Final Words

The enterprise networking space is undergoing significant transformation, driven by the convergence of networking and security, the rise of cloud computing, and changing work dynamics. Enterprises must navigate this complex landscape carefully, assessing their unique needs, capabilities, and strategic objectives to determine the most appropriate path forward.

Choosing the right solutions and vendors can make the difference between a network that merely supports business operations and actively enables strategic business outcomes. By taking a thoughtful, informed approach to network transformation, enterprises can thrive in the new era of enterprise connectivity.



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

©2023 AvidThink LLC. All Rights Reserved.

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