Converge! NETWORK DIGEST | AvidThink®

SASEy-WAN - A Kaleidoscopic View

2020 SD-WAN and SASE Report

RESEARCH BRIEF

Table of Contents

aryaka

The Cloud-First WAN Company

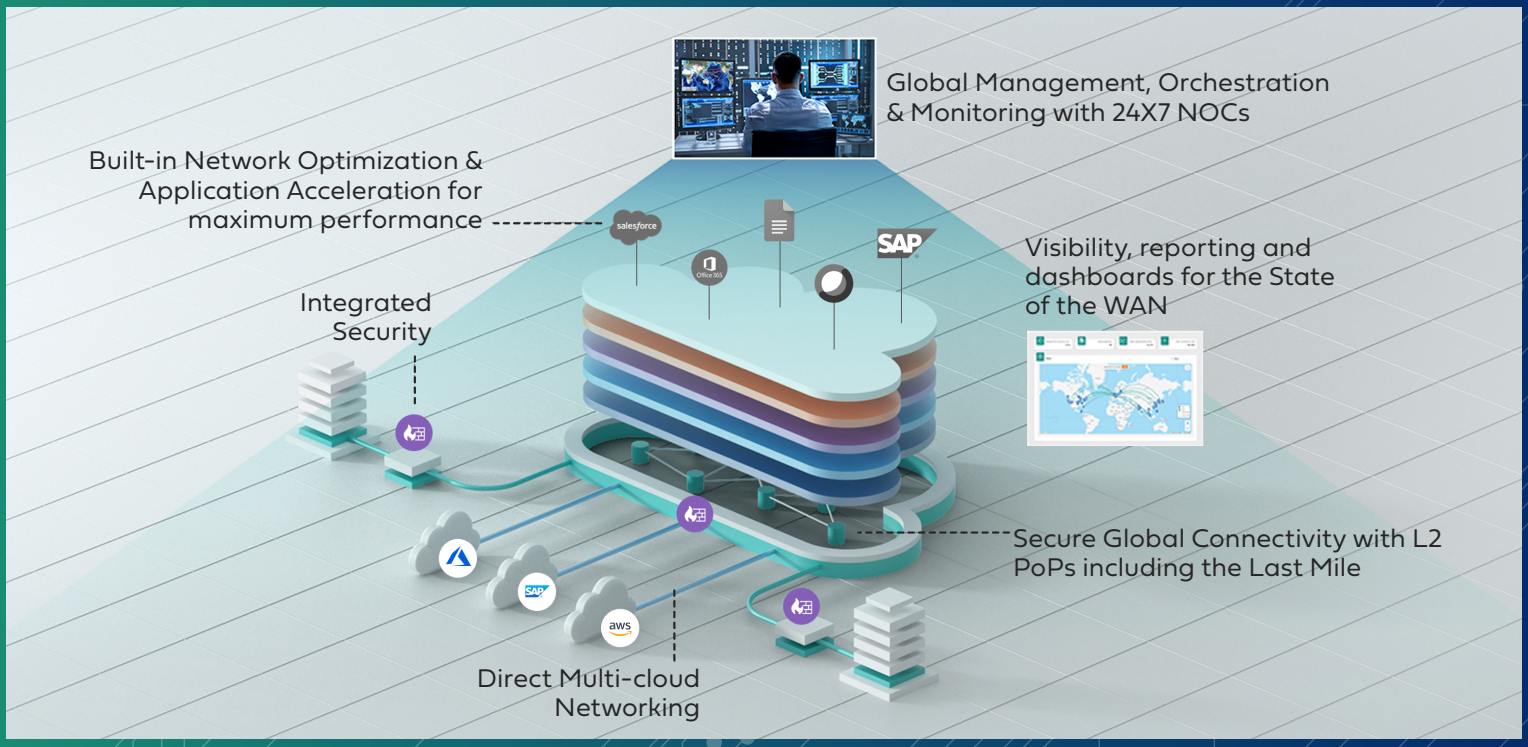
End-to-End Managed SD-WAN Provider for the Cloud-First Enterprise

We Help With

- Digital Transformation
- MPLS Migration
- Multi-Cloud Connectivity
- Paving the Road to SASE
- Application Acceleration
- Operational Simplicity and Flexibility

Why Aryaka?

- Leading TCO - OpEx Only
- Regional and Global
- Private Core, Internet, MPLS
- Gartner Customer Choice for the WAN Edge and Forrester Wave
- Flexible edge and cloud security with Check Point, Palo Alto, and Zscaler



ASAVIE

Now part of Akamai

ENABLING THE SECURE OFFICE ANYWHERE

- Frictionless mobile access to all business resources
- Extend SD-WAN to Mobile & IoT Endpoints
- On-demand Private Mobile Networks

nuagenetworks
From Nokia

Accelerate your Digital Transformation

with the SD-WAN solution that extends business applications from the heart of the cloud to the furthest corner of your organization.

With application-aware visibility and control, SD-WAN extends critical business applications to the **home worker environment**, extending the same policy and security framework used in physical branches.

SD-WAN for **Mobility and IoT** ensures that your business is there, wherever your employees are, seamlessly supporting corporate and BYOD devices without additional software and complexity.

SD-WAN evolution to **SASE** means that security is where you need it, when you need it – in physical branches, on the road, at the home office and in the cloud. It controls access and prevents, detects and responds to threats in real-time.

SASEy-WAN - A Kaleidoscopic View

Introduction — SD-WAN in 2020 goes SASE

Software-defined wide-area networking (SD-WAN) has been the star of the networking world for several years. Still, nothing prepared vendors, service providers, and customers for the explosion in interest and sales that followed the initial wave of pandemic lockdowns. 2020 has been a unique turning point for SD-WAN because of the shift in enterprise networking endpoints from branch to home, but also in SD-WAN's expansion to Secure Access Service Edge (SASE). SD-WAN and the broader category of enterprise end-to-end connectivity are evolving rapidly. This rapid evolution makes it hard for enterprises and service providers to track the trends that matter. Furthermore, SD-WAN and SASE encompass multiple capabilities, and present themselves differently when viewed from a kaleidoscope of angles — hence this year's report title.

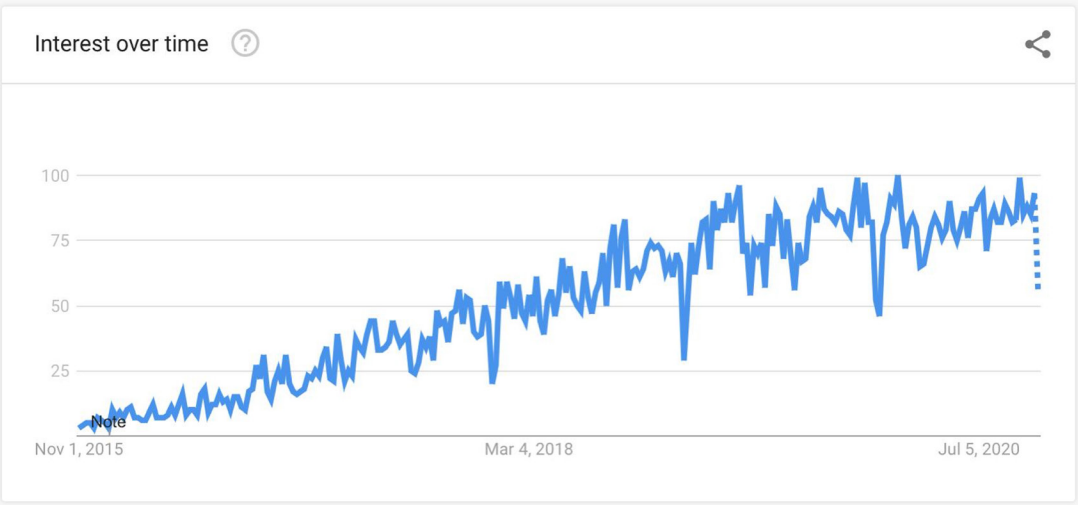
This year's AvidThink report on the topic will provide an update to last year's SD-WAN report: first examining current enterprise viewpoints, followed by delving into service provider trends. We'll then look at the changing vendor ecosystem and provide our observations of the market at large. Finally, we'll look into our crystal kaleidoscope and wrap with recommendations to enterprises on charting a course through the rest of 2020 and into 2021. As always, you can reach out to us at **research@avidthink.com** with questions and feedback!

A Robust Market for Products and Services

Estimates of SD-WAN market size and growth rate vary wildly, as befits a technology segment lacking firm, universally acknowledged boundaries. Nonetheless, every research firm studying the market expects robust growth in the sales of SD-WAN equipment, software, and services.

Gartner, typically a reliable gauge on enterprise IT's thinking and buying patterns, **estimates that enterprise spending on managed SD-WAN services** will hit $5.7 billion in 2023, growing at a phenomenal annual rate of 76.1 percent. Services revenue comes atop already robust purchases of SD-WAN equipment, which, **extrapolating from its 2019 data**, should be nearly $3 billion per year now. Overall, **Gartner sees** enterprise spending on SD-WAN equipment growing at an annual rate of 23 percent in the five years between 2018 and 2023. Much of the growth is due to SD-WAN's rapid penetration into the majority of enterprises. Indeed, Gartner expects that within three years, 60 percent of all new enterprise managed WAN deployments will include SD-WAN.

The SD-WAN sales figures are also reflected in steadily growing consumer interest as reflected in **Google search trends**.



Source: Google Trends; SD-WAN global interest over the past five years.

Remember, all of these projections predate the disruptive events of 2020. Thus, while corporate budgets are tight due to the pandemic-induced recession, IT spending will prioritize items like SD-WAN, SASE and network/cloud services that allow uninterrupted business operations in a world of WFH and e-commerce.

As Gartner's bifurcated revenue estimates indicate, SD-WAN spending spans equipment, software, and services. Indeed, as enterprises gravitate towards subscription services, carriers and other network providers will do more of the equipment spending. Keep these business trends in mind as we look at the technical and product changes that have shaped SD-WAN over the past year and note that some will be more relevant to service providers and others to enterprises operating private SD-WAN infrastructure.

Enterprise Viewpoints

Undoubtedly, the COVID-19 pandemic will have a long-term impact on enterprise IT. With offices emptying overnight, it made extending enterprise networks to remote locations, including the wild west of an employee's home WiFi, a business imperative. Over the intervening months, work-from-home (WFH) requirements have evolved from a temporary necessity to a semi-permanent work environment as offices and schools delayed reopenings.

With return-to-office dates slipping into mid-2021, many organizations discovered the increasing permanence of a world of geographically-distributed project teams, online collaboration, and frequent video conferences. **Facebook CEO Mark Zuckerberg was likely the first** to embrace a permanently remote workforce in May when he said (emphasis added):

> "We're going to be the most forward-leaning company on remote work at our scale. ... I think that it's possible that over the next five to ten years — maybe closer to ten than five, but somewhere in that range —- I think **we could get to about half of the company working remotely permanently.**"

SD-WAN stepped into this maelstrom of change as the way enterprises maintained operations in an online-centric, digitally-transformed economy. As companies digitized operations and increased their dependence on data and advanced analytics to inform decisions, they required a robust, scalable, and secure network fabric connecting even the most remote locations, whether it was an exurban retail store, isolated drilling rig, or foreign call center.

SD-WAN evolved into a financial lever that could finally break the chokehold telecom carriers exerted on enterprise data services by opening the market to competition from more cost-effective carrier ethernet, broadband, and wireless services. SD-WAN also enabled over-the-top (OTT) players like **Aryaka** and **Cato Networks** to provide value-added services without owning wireline or wireless assets. The COVID crisis, combined with the advent of SASE, promises the third phase in the SD-WAN story. Organizations are rapidly adapting enterprise networks to the new reality of the uber-distributed workforce. They are grabbing any available broadband option and relying on a mix of cloud services and on-premises systems. The pandemic, therefore, has catalyzed technology developments propelled by the tailwind of increased sales.

WFH Accelerated Convergence of Network and Security Services

The rush to WFH exposed a festering problem with VPN-based remote access systems: security, which surveys continue to show remains the top networking challenge in large enterprises.

Enterprise remote access systems have used encrypted connections, later VPNs, since the days of dial-up modems, and even early implementations used two-factor authentication (remember those RSA tokens?). These were adequate in the days of client-server applications and moat-and-castle network security when Web browsing was the only reason employees accessed anything outside the corporate network. Unfortunately for legacy security designs, modern IT uses a plethora of cloud software (SaaS), infrastructure (IaaS), business partners, and third-party service providers. These often require new firewall rules, private VPN connections, and user accounts, which together turn the network castle wall into Swiss cheese.

Remote work further exacerbates faulty security designs by creating performance bottlenecks for employees with marginal home Internet circuits. Typical problems include protocol overhead from using obsolete VPN technology, and inferior network design that doesn't support split tunnels, thereby causing unnecessary tromboning of enterprise traffic through enterprise data centers.

Macro Business and Technology Trends Boost Business Need for SD-WAN and SASE

Aside from the sudden, unexpected surge of remote workers, several other business and IT trends have added fuel to the market in 2020, most of which were accelerated by the pandemic disruption. These include:

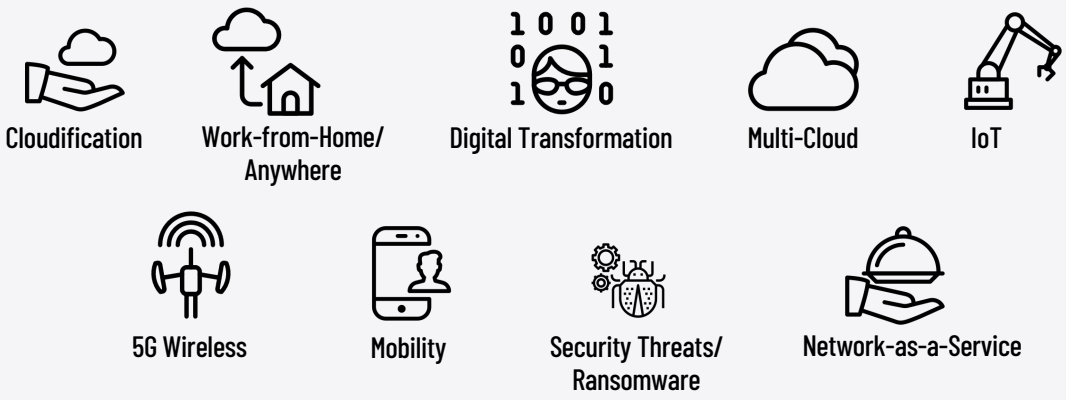
- A shift in business and IT strategy to **consuming cloud services** instead of operating dedicated infrastructure. The cloud-first mindset is hardly universal. Most enterprises won't be abandoning their private data centers anytime soon; however, the financial efficiency and operational flexibility of substituting dynamically-scalable, usage-based OpEx services for fixed CapEx infrastructure are unmistakable. Unfortunately, increased reliance on Internet interconnects subjects application performance, reliability, and security to the vagaries of WAN connectivity and demands a solution like SD-WAN. The migration of workers to home offices exacerbates such network variability by introducing broadband circuits from many providers in various locations with myriad performance characteristics.

SD-WAN also enabled over-the-top (OTT) players like Aryaka and Cato Networks to provide value-added services without owning wireline or wireless assets. The COVID crisis, combined with the advent of SASE, promises the third phase in the SD-WAN story.

- **The digitization of business**, aka digital transformation, is another macro trend that got a pandemic boost as organizations became almost entirely dependent on digital, online processes, process automation, supply chains, and sales. The migration of applications, workflows, and sales channels to outside partners and service providers makes WAN interconnects critical to business operations and increases the criticality of cost-effective, reliable circuits to a broader range of domestic and international locations.
- **The proliferation of multi-cloud IT architectures** with the maturation and evolution of enterprise cloud deployments into a mix of services and infrastructure from several providers. These heterogeneous deployments are in multiple regions per provider and must work with existing privately operated systems. Initially, multi-cloud connections were built and managed as a set of VPCs connected to an organization's central data centers. Unfortunately, this ad hoc approach is operationally inefficient and unscalable. Multi-cloud connectivity and manageability are further complicated by the emergence of hyper-local edge cloud locations such as AWS Wavelength and Azure Edge Zones, along with forthcoming mobile edge infrastructure and services. As organizations build a new generation of **distributed cloud infrastructure**, they turn to software overlays that augment SD-WAN to create a single network fabric that bridges cloud and on-premises connections.
- The proliferation of **intelligent sensors and IoT devices** deployed outside the datacenter spewing enormous amounts of data that is most valuable when analyzed in situ and in real-time. IoT devices have gained enough power, when used with machine learning (ML) technology such as TinyML, to execute sophisticated predictive algorithms on embedded devices. Although these reduce overall data transmission, they don't eliminate the need to ship data to the cloud since the power of IoT entails analyzing data aggregated from many sources across different locations and times. Since IoT and sensors are the quintessential far edge devices, collecting data requires reliable network connections that work across carriers and circuit types. Also, because of the limited footprint on these IoT devices, running a full-fledged VPN or SD-WAN/SASE client might not be feasible. Further, many IoT devices are locked-down, disallowing the loading of additional software. Regardless, enterprises will still demand unified policy and security when it comes to these devices.

- **Increasing shift to mobility** including **emerging 5G-based fixed wireless offerings** that can serve as enterprise-grade WANs by adding the redundancy, security, packet optimization, and QoS features of an SD-WAN. Furthermore, enterprises today continue to shift to mobile-based infrastructures as employees migrate to WFH. Secure mobile access will become a crucial part of future SD-WAN or SASE offerings. A few SD-WAN and SASE vendors have added mobile clients to their product suites to address this requirement, and the rest will follow.
- **Popularity of network-as-a-service (NaaS)** options that bundle SD-WAN and network security features with a globally-distributed fleet of POPs connecting to a private network backbone. CIOs continue to outsource non-core, non-strategic IT functions, and embrace the as-a-service movement. **Several estimates show** the NaaS market growing by at least 30 percent annually over the next several years, reaching $20-50 billion in sales. Since these projections predate this year's disruptive events, they likely understate the growth.
- CIOs are experiencing **increasing security and ransomware attacks** from hackers, which, when combined with an **expanding threat surface** caused by WFH, drives a growing demand for enterprise edge security solutions. The move to SASE is emblematic of the CIO's desires to protect the edge and remote access areas of their network with managed services.

MACRO ENTERPRISE TRENDS IN 2020



AvidThink®

avidthink.com

Service Provider Viewpoints

Unsurprisingly, since communications service providers (CSPs) and managed service providers (MSPs) alike serve the enterprise, their viewpoints will mirror those of the enterprises. Besides, as SPs continue to ram up their managed SD-WAN and SASE services, they will have to contemplate additional service buildout considerations such as orchestration and management.

Regardless, SD-WAN and SASE represent a sizable business opportunity for the service provider markets. Many large SPs we work with view these as multi-hundred to billion-dollar revenue streams for them, assuming they continue to execute well in an increasingly crowded market.

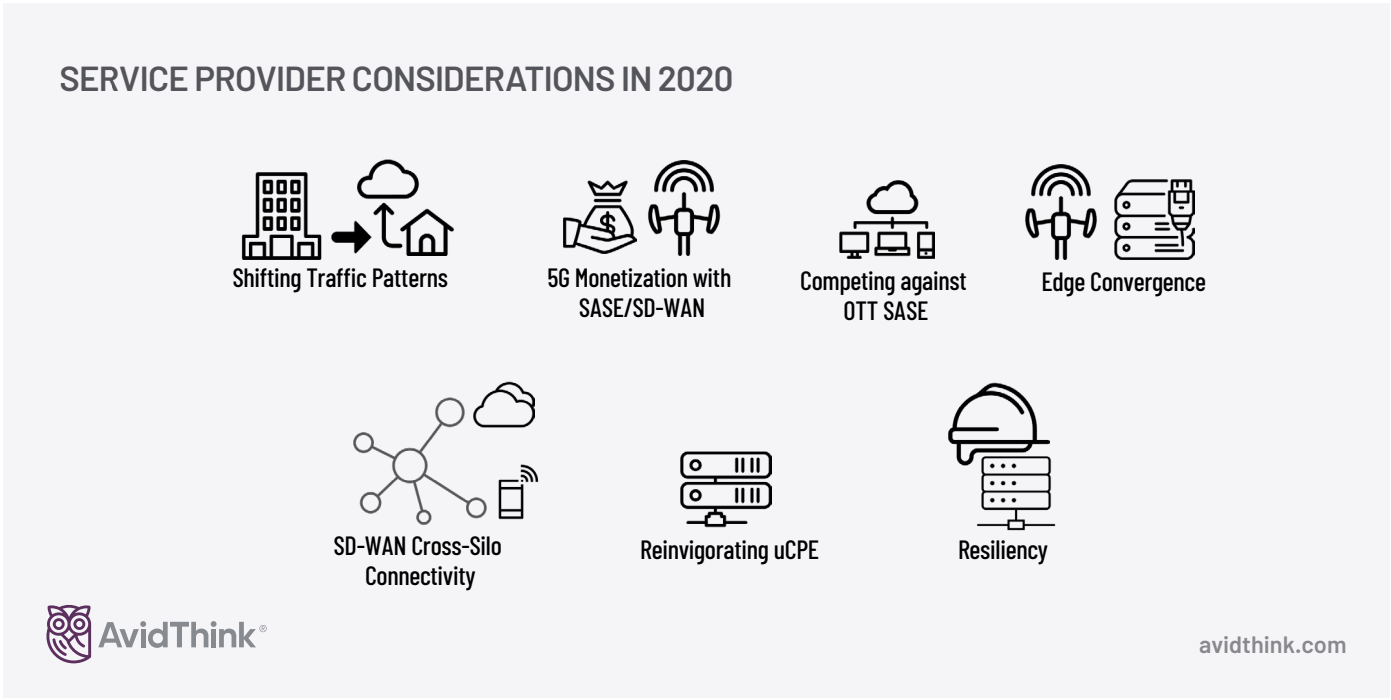
In our conversations with SPs, key considerations from them include:

- **Dealing with rapidly shifting traffic patterns** due to the pandemic. Service providers need to have appropriate carrying capacity at the POPs where the enterprise lines terminate to adequately support enterprise edge services. With the shift from working at enterprise branches to working at home, the traffic load has shifted from metro areas and downtown to the suburbs. Likewise, data traffic has moved from mobile to wireline as home-based workers log onto home WiFi networks that backhaul traffic on broadband connections. Meanwhile, mobile call volume went up during the pandemic since most workers have cut the cord on home phone service. Service providers will need to predict how future hybrid working models will impact their networks and build up accordingly.

Since enterprises today have footprints that span all these different networking silos, SPs have the opportunity to offer a unified fabric that securely connects enterprises across all these domains.

- Examining the use of **SD-WAN and SASE as monetization for 5G**. SPs are looking for ways to monetize their 5G buildout, and providing mobile SD-WAN or mobile SASE on top of 5G (or 4G LTE) can add value to enterprise customers. As companies move to a mobile-first approach for their networking, providing a low-latency converged secure access offering could be compelling. The same protection afforded branches today can be expanded to accommodate mobile devices, fixed-wireless 4G and 5G links (replacing legacy wireline WAN), and mobile IoT devices.
- Finding **differentiators to compete against cloud-based SD-WAN, SASE, and managed security solutions**. SPs recognize that there are multiple providers vying for SD-WAN and SASE dollars at the enterprise. OTT players can effectively play in this space, relegating SPs to play the diminished role of connectivity provider. Some of these OTT players like Aryaka and Cato Networks offer private, high-performance backbones and their own direct public cloud access, further reducing SPs role to mostly last-mile broadband access. SPs, therefore, need to find ways to differentiate their managed SD-WAN and SASE offerings from the OTT and cloud players or find ways to partner with them.
- Leveraging their unique position to add value through **edge convergence** and as a **multi-cloud access provider**. SPs certainly own the last mile, but they also often own the network edge. Control over these strategic edge locations allows SPs to run a converged network access and security stack as close to their enterprise subscribers as possible (short of being on-premises). This enables low-latency and high-performance SASE and SD-WAN offerings. Likewise, they can broker high-speed connections to multiple cloud locations (public, private, SaaS application clouds) to provide the highest-performance links to popular enterprise offerings.

- Looking at how **SD-WAN can unify control over multiple networking silos** that need convergence. Many Tier-1 SPs have multiple connectivity offerings, public mobile networks, home broadband, enterprise MPLS, and carrier ethernet solutions. Some might even venture into private mobile networks on enterprise premises using 4G LTE or 5G technologies. Since enterprises today have footprints that span all these different networking silos, SPs have the opportunity to offer a unified fabric that securely connects enterprises across all these domains.
- Redoubling efforts around **uCPE-based projects to expand beyond SD-WAN/SASE**. Not all SPs who jumped into the universal CPE space early succeeded. Due to virtual network function (VNF) onboarding challenges, orchestration complexity, performance and memory, and compute footprint issues, early uCPE efforts stalled. The state of uCPE orchestration and operating systems have advanced in the last 12-18 months, and today's uCPE efforts are likely to proceed more smoothly. The benefits of uCPE as a multi-solution platform that can host SD-WAN and SASE solutions and as a mini-edge for on-premises applications can be achieved. Further, some SPs are contemplating using these initial uCPE landing points as a platform to offer unified communications services, IoT gateways, and even host parts of a mobile core locally for private enterprise networks.
- Adding **resiliency to deployments** during the pandemic. We've had more conversations with SPs who are rolling out increasingly larger SD-WAN implementations, and the topic of resiliency has come up. As SPs run more services at the edge, the SD-WAN and SASE platforms will need to focus on techniques for adding resilience to these platforms. SPs have shared that it's not always a hardware failure that brings down a remote site, but usually a software-related failure. As SD-WAN and SASE software become more complex, or as uCPE platforms run more services, the likelihood of a failure increases. And especially with travel restrictions due to COVID, SPs realize the importance of resiliency at remote sites. Hence, we see SPs pushing vendors to improve the resiliency of their designs while turning to out-of-band management solutions for critical locations.



Vendor, Technology, and Market Ecosystem Shifts

The SD-WAN market continues to evolve, and one of the most significant changes is the rise of SASE, which is defined as a superset of SD-WAN and other enterprise edge services. In this section, we'll look at a few significant trends that impact this market, including SASE, and spend some time describing adjacencies to this market that we believe are most relevant.

Consolidation of SD-WAN Continues

The SD-WAN market continues to see new entrants while consolidating. In the last year, notable acquisitions include HPE buying **SilverPeak** for $925M, even though HPE already had a WiFi-centric SD-WAN solution in their **Aruba networking division**. HPE is in the process of integrating Aruba with SilverPeak. We also saw Palo Alto Networks grab CloudGenix for $420M, despite already having a firewall-centric SD-WAN solution of its own. **Juniper Networks** also announced their intent to purchase 128 Technology for $450M, combining 128's SD-WAN with their AI technology from their earlier Mist (WiFi) acquisition. **Ericsson** purchased **Cradlepoint**, which was more of a wireless router play but which also had SD-WAN capabilities, for $1.1B.

And in a sign that there's going to be more stars minted in the SASE/SD-WAN market, dark horse SASE-player Cato Networks turned unicorn, achieving **$1B in pre-money valuation** for their latest round of financing in November.

Finally, **Akamai**, the cloud edge giant, gobbled up **Asavie**, a small Irish firm focused on providing secure access to mobile and IoT devices. Asavie's customer base includes Tier 1 SPs like AT&T and Verizon, as well as large enterprises and public sector organizations such as UK's National Health Service. Akamai will likely combine Asavie's technology with their own cloud-edge security products to offer a mobile SASE-type offering. **Nuage Networks** had previously announced a partnership with Asavie, bringing to market an innovative combined mobile, IoT, and SD-WAN solution. It remains to be seen what the Akamai acquisition will mean for the joint offering. The triple combination of Akamai, Asavie and Nuage, bringing together cloud security, mobile and IoT and SD-WAN, could be a comprehensive new offering in the market.

That leaves a few prominent standalone SD-WAN vendors like Versa Networks waiting to be snapped up. Also, with Nokia's recent reorganization and focus on 5G, it's unclear what it means for their leading SD-WAN technology from Nuage Networks — one of the earliest players and one architected for a cross-enterprise deployment from branch to WAN to data center. Will Nokia fold it tighter into a 5G offering, or will it spin it out?

SD-WAN goes SASE-y

SASE builds on an SD-WAN foundation by adding several security features. While the term was recently coined by Gartner, it is widely understood to encompass the following technologies:

- **Secure Web Gateway (SWG)** is an L7 proxy that augments L3 firewalls by inspecting and filtering Web traffic to block malware and content that violates enterprise policies. An SWG also provides detailed usage data to identify unusual traffic or volume and predict capacity needs.
- **Next-generation firewall-as-a-service (FWaaS)** replaces traditional router- or appliance-based firewalls with virtual equivalents that can be inserted anywhere in the network, whether a branch office and employee's home access point or virtual desktop.
- **Cloud Access Security Broker (CASB)** supplements an SWG by enforcing a broader set of enterprise security policies for cloud applications, e.g., SaaS. These include implementing authentication, usage, and data loss policies while providing usage and logging data for SaaS applications.
- **Zero-trust network access (ZTNA)** replaces tunnel-based VPN encryption-authentication, i.e., the moat-and-castle approach to network security, with a granular, distributed set of user- and application-specific controls. ZTNA ensures that access to every application and backend service or file repository is authenticated, authorized, and encrypted.

Of the four above, ZTNA might be the least familiar to our readers. ZTNA encapsulates concepts around a software-defined perimeter that grew out of efforts in the mid-2000s to improve enterprise security. The zero-trust model codified by John Kindervag, while an analyst at Forrester, was subsequently popularized by **Google's BeyondCorp efforts**. ZTNA combines several features into a security platform that uses identity, device postures, context, and the nature of the asset to determine the scope of privileges to allow. It's increasingly important as we move SD-WAN and SASE to include edge locations and IoT devices.

The firm expects the bulk of sales to come from software, where, in the short term, SASE suites are bundled with hardware security appliances.

The SASE concept is barely a year old, so the market is minuscule in size, making explosive growth estimates perfectly normal for a hot IT segment. **A recent projection by Dell'Oro has the SASE market** growing at 116 percent annually over the next five years, a rate that would result in 2024 revenue about 22-times that of 2020. The firm expects the bulk of sales to come from software, where, in the short term, SASE suites are bundled with hardware security appliances. Over time, most buyers, which Dell'Oro projects will be primarily small and medium enterprises looking to simplify their remote network security posture, will gravitate to SaaS products managed by a SASE vendor, carrier, or ISP.

Gartner is more optimistic about broad enterprise adoption, predicting that by 2024, at least 40% of enterprises will have concrete SASE plans and deployments versus single-digit adoption today. Our view is that SASE will span both small and large enterprises, driven by this year's sudden shift to remote work accelerating adoption by all organizations. Large companies with geographically dispersed workforces, many of which will remain permanent WFH employees, stand to benefit the most from SASE adoption. We agree with Gartner that most will procure SASE as a managed service. We also see customers purchasing SASE-type offerings linked to carrier SD-WAN solutions today. The AvidThink view is that SD-WAN was already transforming and consuming adjacent security services and that its eventual evolution would have been some flavor of SASE. The blurring between SD-WAN and SASE will likely continue as vendors battle it out, but the umbrella term will probably be SASE (at least until a universal enterprise fabric emerges).

As befits an immature and evolving concept, there are few fully-integrated SASE products, with incumbent networking vendors spending the past year stitching together a set of security features into a coherent offering. As of Q4 2020, some of the more prominent SASE products are as follows:

- **Aryaka** Managed SD-WAN services including Smart Cloud, Secure, and Insights that work with its globally-distributed POP on-ramps.
- **Barracuda Networks** CloudGen WAN
- **Cato Networks**
- **Cisco SD-WAN** plus Umbrella and Duo Beyond (a ZTNA solution Cisco acquired in 2018)
- **Forcepoint** Dynamic Edge Protection
- **Fortinet** SASE
- **Masergy** SASE
- **Netskope** NewEdge
- **Palo Alto Networks** Prisma Access plus CloudGenix
- **Versa Networks** SASE expands an existing SD-WAN service using its distributed network gateways (POPs)
- **VMware** Secure Access plus Cloud Web Security plus VeloCloud SD-WAN plus NSX Cloud Firewall
- **Zscaler** Cloud Security Platform

We'll note that there's dispute between vendors as to who's really SASE and who's not; however, in our conversations with enterprise customers, the above vendors are accepted as SASE solutions.

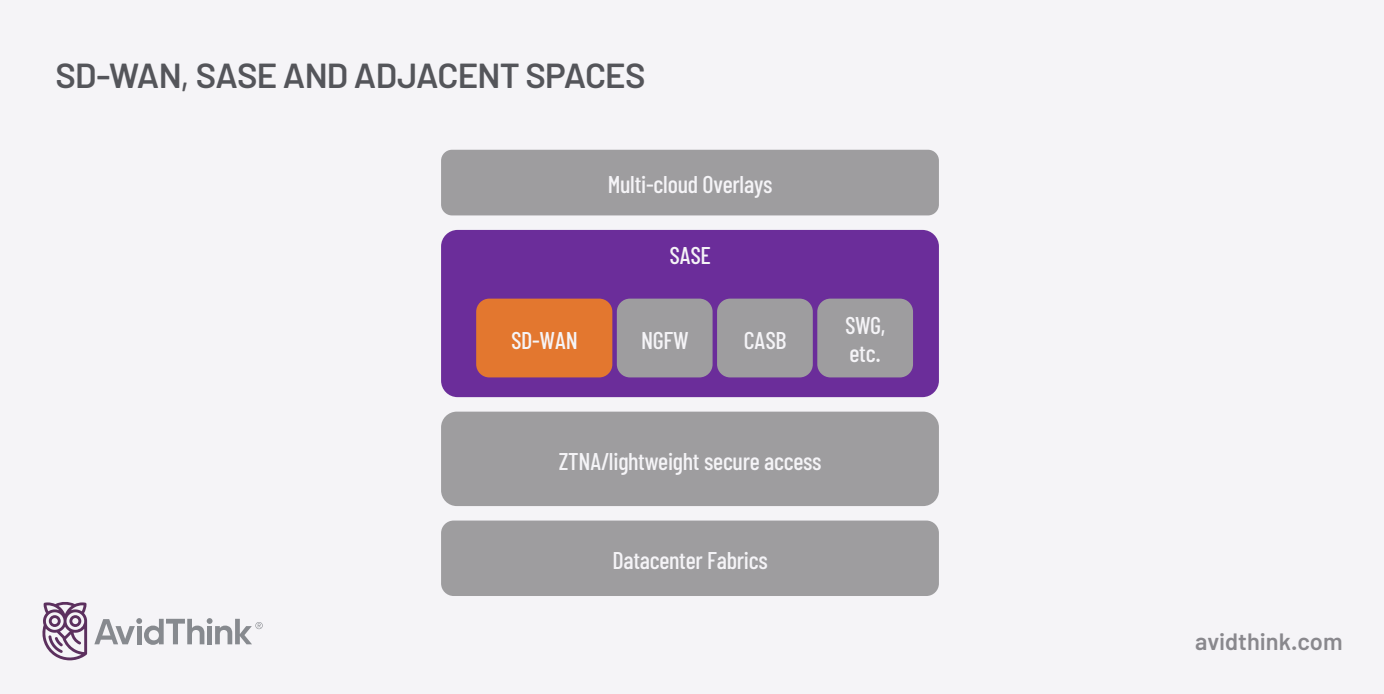
Despite the marketing hype, the newest thing about SASE is the label since it merely describes the unification of a set of network security technologies that have long been separately available. While remote networking is the primary usage scenario and SD-WAN is the foundation, most SASE technologies, for example, zero-trust network access or next-generation firewall, originated to solve broader security problems and are only now being applied to address WFH and branch office security problems.

As a hot new network technology, SASE also suffers from feature-washing, where early products are often little more than a set of existing, discrete offerings that are cobbled together through NFV service chains and lumped under a single management UI. While these look compelling on paper, by lacking architectural unity, they aren't tightly integrated, often suffer from poor and inconsistent performance (particularly latency) and discordant admin interfaces. Therefore, we advise early buyers to dig into the underlying design and integration of SASE products and not just focus on the feature checklist.

We've stated in our past analysis that SASE provides an opportunity to rethink enterprise network security from a cloud-centric viewpoint, building a new security platform that isn't constrained by today's legacy categorization of solutions (NGFW, SWG, CASB, etc.). Likewise, we think that the most exciting developments in SD-WAN come from companies taking a fresh look at remote WANs, redesigning security and building a highly distributed topology with a virtual network control plane.

Ecosystem Expansion and Extensions

SASE is the most considerable shift in the SD-WAN market to date and has redefined the enterprise edge connectivity market to include the security adjacencies we discussed. However, we anticipate further changes in the market from other adjacencies. We've discussed some of these, including cloud-security companies like Akamai and Zscaler, or security companies' cloud offerings such as Palo Alto Networks' Prisma or Cisco's Umbrella. In addition, there are also data center fabrics like VMware's NSX and Cisco's ACI. Nuage's SD-WAN fabric also started out as an SDN data center fabric. While these are primarily intra- and inter-data center focused, we expect an SD-WAN integration or overlap in the near future.



There's also the service mesh, which is an application-centric connectivity technology. Service meshes provide discovery, security, routing, load-balancing for inter-component connectivity between application modules for a cloud service built with a micro-service-based architecture. Again, it's possible they will integrate with SD-WAN/SASE solutions at some point in the future, but for now AvidThink predicts mostly separate evolutionary paths.

Next, we'll delve into two areas that are most likely to overlap with the SD-WAN/SASE world in the near term. First, multi-cloud connectivity solutions, followed by secure fabric offerings (based on ZTNA) that are now popular in the IoT sphere. We'll see that the ultimate goal across these approaches is a NaaS offering that spans all enterprise locations (cloud, branches, homes, mobile), connecting all enterprise devices and users.

Multi-Cloud Overlays

Enterprises today consume multiple cloud technologies. IDC's **2019 Multicloud Management Survey** showed that 81% of enterprises use multiple public clouds and more than one private or dedicated cloud. SD-WAN technology has been used to connect virtual private clouds (VPCs) across these public clouds, as well as from enterprise branches to these VPCs. However, there are significant market entrants focused on multi-cloud connectivity: **Aviatrix** and **Alkira**. Alkira is led by Steve Mullaney, the former CEO of Nicira, which was acquired by VMware, and which pioneered network virtualization with the NSX fabric. Alkira was founded by the Khan brothers (Amir and Atif), who previously founded SD-WAN pioneer Viptela that Cisco acquired in 2017 for $610M.

Both have different approaches to multi-cloud connectivity but essentially stitch network circuits to various cloud providers to create a cohesive, multi-site network with consistent security, traffic management, and access control policies. AvidThink believes that these multi-cloud approaches will expand into multi-site (likely the network edge with the advent of edge computing) and then expand into the areas that SD-WAN today serves.

SD-WAN technology is pivotal to fabrics, given its ability to identify and prioritize different application protocols and packet flows and adjusts route paths, QoS, and other network parameters accordingly regardless of the source or destination. These technologies will prove useful in multi-cloud overlays as well. Multi-cloud fabrics will be critical as larger organizations adopt IT strategies that blend infrastructure (IaaS) and applications (SaaS) from multiple cloud vendors with self-operated IT services delivered from on-premises data centers or colocation facilities.

Secure Enterprise Fabrics

In the past year, the most significant SD-WAN developments focused on security for edge location and remote workers, as well as a shift to mobility. We'll highlight a few notable products and open source projects below that look beyond most SASE/SD-WAN offerings by rethinking the underlying networking and security stack for remote networks. Collectively, these will strengthen the SD-WAN foundation and ultimately displace traditional VPN-based tunnels for edge locations and WFH employees. Many of these technologies are more lightweight than SD-WAN and SASE offerings today. They often also adopt a ZTNA philosophy, and some are taking the IoT route to market because of their low-footprint approach.

The following are some innovative examples of companies rethinking network security for remote and edge networks.

- **Ananda Networks** is a recently-emerged startup with a new type of distributed NaaS that replaces IP-based routing and security with policies based on user identity, i.e., ZTNA. Unfortunately, the company is still secretive about the technical details, but like other NaaS products, it uses a cloud-based network control plane to manage connections and traffic with an identity-based routing algorithm to find and connect users to their destination node. Like SD-WAN, Ananda's control plane uses algorithms to make and optimize connection decisions. However, Ananda goes further by using ML models. It prefers direct links when two nodes are geographically close but will route through an intermediary relay to improve performance and reliability for longer hops. Also, like SD-WAN, Ananda can use multiple WAN paths per virtual connection and end-to-end encryption for each link. The company claims its network performance is significantly faster than SD-WAN and that by integrating identity-based security into the network stack, more secure and easier to manage than SASE add-ons.

- **Dispersive** is another virtual WAN overlay with an SD-WAN alternative that it claims is inherently secure and more efficient at route optimization than conventional approaches. A Dispersive Virtual Network (DVN) splits traffic across multiple links and builds encrypted, multi-hop connections that can dynamically reroute during transmission to avoid congestion or failed links. DVNs are end-to-end connections that use an endpoint application to establish and terminate connections and authenticate users. Dispersive targets industrial, smart city, and energy IoT devices through partnerships.
- **NetFoundry** is a virtual overlay fabric composed of a cloud controller, router nodes, and endpoints connected into a distributed, multi-hop dynamically reconfigurable mesh. Like Ananda and Dispersive, NetFoundry integrates zero-trust security that authenticates users and applications with the controller, enforcing policies that grant endpoints limited access to particular IP addresses, ports, and protocols. NetFoundry encrypts all connections during setup and can separately encrypt data headers to conceal source IPs. NetFoundry is useful to create zero-trust connections to cloud environments, edge IoT networks, and as a VPN replacement for WFH employees.
- **Twingate** is another company that introduced a unique software-defined network platform in the midst of the most significant transition to remote work in history. True to its SDN roots, Twingate segregates network control from data with a design built around five elements: controller, clients, connectors, relays, and an authenticator (IDM). It also uses identity-based connections, i.e., zero-trust, that control who can establish a link and access network resources. Unlike a VPN, Twingate distributes session setup and optimization to the client via an intelligent software-defined proxy. Twingate says its design improves performance, reliability, scalability, and manageability. For example, Twingate links are inherently split tunnels since they don't route traffic through a central VPN hub. Pushing connection set up to the client also eliminates bottlenecks since authorization requests and MFA processing is handled locally and only require access to an external SSO or IDM server, but not the cloud network controller.

Many of these technologies are more lightweight than SD-WAN and SASE offerings today. They often also adopt a ZTNA philosophy, and some are taking the IoT route to market because of their low-footprint approach.

And the following are examples of open-source projects that we view as relevant to the SASE/SD-WAN market:

- **Nebula** is a WAN overlay that Slack developed after realizing that the manageability and performance degradation of its mesh of IPSec-based connections became unacceptable as it increased the number and regional diversity of endpoints. Slack built a new WAN stack based on the Noise Protocol Framework developed by the founder of the secure Signal Messenger. Slack wanted a faster system that provided end-to-end encryption, independent of the underlying transport or service provider, and used certificate-based identity, with identity-based traffic filtering.
- **Noise Protocol Framework** is a development platform for creating crypto protocols based on Diffie-Hellman key agreement that is designed to be more efficient and resilient to DoS attacks, key compromise, and message loss. A Noise protocol starts with two parties exchanging handshake messages, including DH public key exchange and other steps to generate a shared secret key. The handshake allows each side to establish an encrypted connection for sharing messages. Specifications and code are publicly available and include tools for generating, analyzing, and testing handshake patterns; however, some crypto developers complain that the framework is overly complicated and abstruse.
- **Wireguard** is an open-source VPN protocol designed to be faster, simpler, and more efficient than IPSec or OpenVPN. Wireguard can initiate a session in a single round-trip key exchange (using the Noise Protocol Framework). Short pre-shared static keys are used for mutual authentication in the style of OpenSSH. The protocol provides strong perfect

forward secrecy in addition to a high degree of identity hiding. Transport speed is accomplished using a more efficient cipher providing authenticated-encryption for encapsulation of packets in UDP. There are also built-in techniques to mitigate DoS attacks. In benchmarks against OpenVPN and two configurations of IPSec, Wireguard delivered at least 15 percent higher throughput and 20 percent lower latency than the fastest IPSec implementation. Linus Torvalds is a fan, and Wireguard has been incorporated into the Linux kernel as of version 5.6.

It's unclear how these innovative approaches will impact the SD-WAN and SASE market near term, but AvidThink recommends following these companies and projects closely. We believe their low-overhead, ZTNA-centric approach will make them viable alternatives to the existing more heavy-weight approaches to the enterprise connectivity problem.

SD-WAN and SASE Features and Standards

There are no widely-accepted standards for SD-WAN security and SASE features today. Many of the SD-WAN and SASE vendors show little interest in driving standards during this period of rapid growth and land grab. However, service providers are looking to create some commonality so they can orchestrate and integrate multiple SD-WAN and SASE vendors across their deployments (uCPE-based or otherwise). These service providers have joined with the MEF to create standards around both SD-WAN and SASE.

The **MEF 70 standard** lays the foundation for MEF services, creating a nomenclature 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 and is being developed by a consortium of SD-WAN vendors, service providers, and users.

MEF88's draft list of capabilities currently includes:

- Middle-box functions used to decrypt and re-encrypt TLS sessions to allow scanning an application flow to enable security policy enforcement.
- IP port and protocol filtering like that on a traditional L3 firewall.
- Nameserver and DNS filtering to selectively block access to DNS servers and blacklist domains or particular sites.
- URL filtering.
- Malware detection and removal to scan connections and remove harmful content.
- Security event notification to notify users and network administrators about security actions and anomalies.

Additional in-progress work includes:

- Alternatives to IPsec for secure tunnels.
- The storage and transmission of authorization keys.
- Securing administrative traffic.
- Using TPM for credentials.
- Automation and orchestration features.
- Secure zero-touch provisioning.
- Developing standard validation and certification processes.

The MEF expects to have a final draft for MEF88 in the next six months. MEF is also actively working on SASE Services Definition (MEF W117) along with efforts in Zero Trust and SD-WAN and SASE orchestration. Along with these standards, the MEF has embarked on associated certification programs in conjunction with leading test vendors.

It's still unclear whether the market will adopt and adhere to the MEF standards, and whether enough SPs or enterprises will demand compliance. Likewise, it's possible that it's too early in the SD-WAN and SASE product maturity cycle to lock down a standard. Nevertheless, the MEF is meeting an immediate SP need and trying to create a forum and framework for discussion between the key stakeholders.

Conclusion and Recommendations in a SASE World

With so many players in the market, and multiple adjacent players encroaching on the SASE and SD-WAN market, AvidThink anticipates that the market will expand again before consolidating. We expect the CPE/branch-centric solutions will push against the cloud-centric offerings, while we'll see the app- and network-centric solutions evolve independently before integrating or unifying. Likewise, we expect parallel evolution of the different solutions in the various domains: mobile, WAN, IoT, cloud. We anticipate domain-specific players fighting to dominate their segments before expanding into adjacent spaces. How each vendor category sets themselves up for the massive winner-take-all across all domains remains to be seen.

SD-WAN, which was once seen as a cost-control measure to counter often exorbitant prices for enterprise WAN circuits, will evolve into SASE and become a critical enabler for digital business and distributed workforces.

No matter how the overall space evolves, SD-WAN is in the midst of the most rapid, dynamic changes yet as enterprises simultaneously shift to cloud services and remote work. These changes in the way IT procures and delivers applications and services, combined with the new world of WFH that are utterly dependent on cloud storage, collaboration, and video conferencing services, have sparked an explosion in SD-WAN products development and enterprise adoption.

SD-WAN, which was once seen as a cost-control measure to counter often exorbitant prices for enterprise WAN circuits, will evolve into SASE and become a critical enabler for digital business and distributed workforces.

Enterprises face several choices as they plan SASE/SD-WAN strategies:

- **How they procure and deliver** SASE/SD-WAN services, whether from internal infrastructure, a carrier, or as-a-service from an OTT player.
- **How they structure** SASE/SD-WAN projects and service introductions and balance planning rigor and overhead against rapid ROI.

There are two broad strategies:

- The **big bang** of simultaneously attacking problems across business units and solution domains, i.e., cloud, remote access.
- The **tactical attack** of focusing on the most pressing challenges in particular areas.

The right answer varies by the organization; however, we believe it involves a mix of strategic planning and tactical implementation.

For example, it's impossible to implement a multi-cloud fabric without considering an organization's broader network architecture and long-term cloud usage plans. However, once designed and with products selected, a phased implementation is prudent and amenable to modification when problems arise. Likewise, introducing SASE or a new security-centric remote network requires product evaluation and testing that considers pan-organizational business needs and corporate security requirements. Some of the key criteria in selection of the right SD-WAN/SASE products will involve considering their orchestration capabilities, ease-of-integation with existing identity and policy stores, and ease of troubleshooting and overall visibility. Once a solution is selected, it's wise to phase service introduction by focusing on workgroups with the greatest need or that are most amenable to testing new remote access processes.

We'll leave you with the following parting thought: whether the goal is a universal network fabric or an inherently secure remote network, when planning for the next-generation of enterprise SASE/SD-WAN, it's critical to focus on the business needs and not be dazzled by the kaleidoscope of available cool technologies, of which there are numerous.

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

Rev A