Availability and Buying Options in the Emerging SASE Market

By Paula Musich
An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report
February 2021

Sponsored by:

paloalto® NETWORKS

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Availability and Buying Options in the Emerging SASE Market

Table of Contents

Availability and Buying Options in the Emerging SASE Market

Introduction

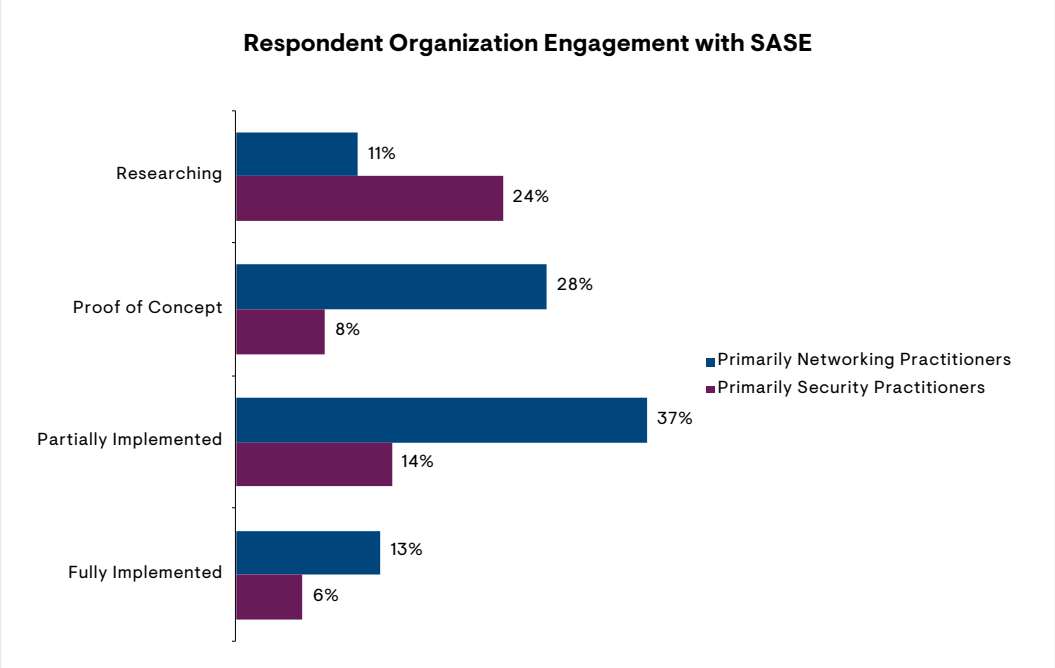
The opportunity described by Gartner analysts as secure access service edge, or SASE, is at this point not so much a market as an aspirational description of where the now-separate networking and security markets need to come together to better serve the needs of the digitally transformed enterprise. The enterprise architectures of the past, based on separate networking and security infrastructures, no longer fit the needs of most enterprises. They were designed to backhaul traffic from remote branch offices and mobile VPN clients to a central location where network traffic is monitored for performance issues, malicious activity, and malware before sending the traffic to its destination, which was often in the same data center. However, the once-centralized applications that end users seek to access no longer universally reside in those concentrated data centers as enterprises more fully embrace cloud services of all kinds. Thanks to the global COVID-19 pandemic and its resulting and rapid shift to work from home operations, digital transformation initiatives have advanced at a much more rapid pace than the industry anticipated.

Having security teams manage a range of discrete security boxes and a growing array of endpoint agents, as well as manage relationships/contracts with too many different security suppliers, is becoming increasingly untenable. Perimeter security, where everything within the DMZ is trusted once authenticated, is a relic of the past. Supporting these old paradigms while struggling to understand what it takes to adequately secure applications, workloads, and data in SaaS, IaaS, and PaaS service provider data centers is too complex and costly for all but the most mature and well-funded security teams. At the same time, the performance bottlenecks introduced by applying old network security architectures to new network traffic patterns cause a poor end-user experience. Those bottlenecks also create an incentive for end users to work around or outside of existing security controls, introducing new risks for their organizations.

With SASE, rather than making the enterprise data center the center of the policy universe, identity becomes that center. Access or privilege levels are determined and policies are applied based on the identity of the user, device, and application. Using that identity information, along with additional context, a range of different networking and security services is applied to each session. Those can include but are not limited to SD-WAN, WAN optimization, routing/path selection, and QOS on the networking side, as well as FWaaS, IDS/IPS, antimalware, recursive DNS, SWG, CASB, and ZTNA on the security side. Although Gartner asserts that all of this should be delivered as a cloud-based service, many of those who claim to participate in the new SASE opportunity offer multiple approaches that include cloud-delivered and hybrid services that distribute a portion of the computing workload to on-premises appliances and client software deployed to remote branch offices. Among those are Cato Networks, Cisco, Fortinet, and Versa Networks. Others, such as VMware, offer both the option to deploy completely from the cloud or deploy on-premises gateways. These suppliers refer to such architectures as *thin branch* and *heavy branch* deployments. Thin branch refers to security delivered from the cloud, while heavy branch executes security tasks locally. In essence, the latter is promoted primarily by legacy hardware-based NGFW providers, such as Fortinet, to protect their existing technology advantage while transitioning to a more cloud-focused delivery of security services.

The SASE Buyer's Journey

Although Gartner only published its SASE paper in the second half of 2019, awareness of the phrase and its basic constructs among IT professionals is already surprisingly high. Enterprise Management Associates found[1] that at least 75% and 78% of respondents in the two different studies are familiar with the term. There were some interesting differences between the survey focused on networking professionals and the survey focused on IT security practitioners around their organizations' engagement with SASE technology. Among those networking professionals familiar with SASE, 37% said their organizations had already partially implemented it, while only 14% of security practitioners familiar with SASE gave a similar answer. At the same time, 28% of networking respondents said their organizations were in the midst of evaluating SASE or engaging in proof of concept activity around it, while only 8% of security practitioners indicated their organizations were conducting a POC. Despite the immaturity of the emerging market and the solutions available to it, 13% of networking respondents said their organizations had fully implemented a SASE solution, while only 6% of security practitioners indicated full SASE deployment. About 10% of networking respondents were split between researching SASE and planning the implementation of a chosen vendor's solution, and only 2% said they had no engagement with it. This suggests that the network operations teams in most enterprises looking to deploy the emerging technology are leading SASE adoption, rather than security operations teams. However, it should be noted that SD-WAN vendors are ahead of security vendors in wrapping their marketing and sales messaging around SASE, and that likely had an impact on networking respondent answers. At the same time, many IT practitioners like to think of themselves as trailblazers in adopting promising new technologies. There is likely a sense of competition among the different groups to claim a leadership role in SASE adoption.



[1] In two separate research projects conducted late in 2020 surveying primarily networking and security practitioners

The Competitive Landscape

The publication of Gartner's paper in late 2019, helped along by the sudden rush to support work from home initiatives in early 2020, opened the floodgates for vendors of all stripes to pursue SASE opportunities. By EMA's count, at least 16 vendors are actively marketing SASE services, and that number will grow quickly as the hype cycle heats up. Not only have SD-WAN vendors rushed into the emerging market, so too have traditional networking vendors, network security vendors—both traditional and those born in the cloud—and content delivery networking vendors. They join existing pure-play SASE startups, such as Cato Networks and Open Systems.

It's tempting to lump the approaches these competitors are taking into two buckets: single-vendor SASE versus multi-vendor SASE. Those that sell a complete set of SASE functions for both networking and security requirements address the complexity of customers having to manage multiple vendor relationships and contracts. Multi-vendor SASE providers give customers a single throat to choke when problems arise and a single management interface to reduce operational complexity. On the other side of the coin, multi-vendor SASE enables the customer to select best-of-breed technologies that can be service-chained together and preserve existing relationships with trusted IT security and/or networking suppliers.

It's more instructive to understand how each competitor arrived at their SASE solution. It can demonstrate where the holes exist in the range of functions their SASE solution includes and illustrate the weaknesses of their approach. The following categorizes the different approaches most vendors identified as SASE providers have taken to date.

Categorizing SASE Vendors

Standalone SASE Specialists	Acquisitions by Large Networking/Security Vendors	Security Vendors Partnering with SD-WAN Providers	CDN Providers Adding SASE Functions
Cato Networks	Cisco/Viptela	Forcepoint	Akamai
Open Systems	Fortinet/OPAQ	McAfee	Cloudflare
Versa Networks	Aruba (HPE) Silver Peak	Netskope	
	Palo Alto Networks/ CloudGenix	Symantec	
	VMware/VeloCloud	zScaler	
		Check Point	

Of those SASE competitors, EMA chose to focus on nine vendors that appear to be furthest along in fleshing out an integrated set of networking and security services necessary to meet the requirements of a digitally transformed enterprise. Those vendors include the following:

- Cato Networks
- Cisco Systems
- Cloudflare
- Fortinet
- Aruba (HPE) Silver Peak
- Palo Alto Networks
- Versa Networks
- VMware
- Zscaler

Illustrating how new and immature the emerging SASE market is, three of the largest competitors that entered the market via acquisition—Cisco, Fortinet, and Palo Alto Networks—planted their flags in the fertile SASE soil in the fall of 2020 by launching their initial integration efforts and packaging plans. Cisco, which acquired Meraki in 2012 and Viptella in 2017, claimed in its launch that it has been working to converge networking and security for years, especially the technologies acquired with OpenDNS in 2015.

Security Functionality

When it comes to security functionality, EMA believes that the same set of security services that protect employees directly connected to the enterprise network needs to be applied to roaming users, branch office users, and the cloud services they seek to access. A true SASE offering at minimum must include SD-WAN, SWG, CASB, ZTNA, FWaaS, the ability to identify sensitive data (including encrypted data) and malware, and consistency in line-rate operations at the network's edge and from the cloud. By that measure, very few (if any) of the vendors featured in this study can claim that mantle. For example, even with a handful of security partners filling in security functionality, Silver Peak still lacks the ability to identify sensitive data and inspect for malware, although it is on the company's roadmap. CASB and ZTNA are currently available as separate offerings from Fortinet as part of its Fortinet Security Fabric. Cloudflare lacks API access to SaaS and plans to add SD-WAN, the ability to identify sensitive data, FWaaS, and network sandboxing soon. VMware won't have SWG, CASB, and FWaaS available until sometime in the second quarter. It's unclear whether Cisco delivers line-rate operations at the edge and from the cloud. Zscaler has the most complete set of integrated networking and security features available in its SASE offering, although it partners with an SD-WAN and WAAP vendor for those functions. This speaks to the maturity level of the market and the long journey ahead for all participants to realize the benefits of the SASE vision.

Beyond those core capabilities, some prospects may also find it compelling to have such functions in their SASE selection as web application and API protection, remote browser isolation, recursive DNS, network sandbox, API-based access to SaaS for data context, and support for managed and unmanaged devices. Among the nine vendors EMA selected, only Cloudflare, Versa Networks, and Zscaler offer WAAP functions, while Fortinet offers WAF only. Palo Alto Networks, Fortinet, and Cato lack RBI support, while Cisco and VMware plan to add RBI. Silver Peak relies on a partner for RBI and Versa Networks just released that capability. Recursive DNS is available from Cisco, Palo Alto Networks, and Versa, while network sandbox capabilities are available from Cisco, Palo Alto Networks, Fortinet, Versa, Zscaler, and from a Silver Peak partner.

Finally, other additional options that some organizations may find attractive include Wi-Fi hotspot protection, network obfuscation, legacy VPN, edge compute protection, and UEBA. Cato Networks and Aruba (HPE) Silver Peak lack those capabilities, while Cisco, Fortinet, Palo Alto Networks, and Versa Networks offer them either directly or through partners. Zscaler lacks legacy VPN, edge compute protection, and UEBA. VMware has edge compute protection on its roadmap.

SASE Architectures

The way competitors have architected their SASE solutions can have an outsized impact not only on performance, but also operational overhead, the cost to deliver the service, and where points of presence can be located. In the case of Palo Alto Networks, for example, its Prisma Access SASE service runs on AWS and GCP, and Palo Alto Networks dedicates a single security processing node for each client. This makes its SASE service more expensive to operate, although it assures good isolation between each client and avoids the performance hit that comes with shared infrastructure. The company asserts that its architecture is cloud-agnostic, but it is limited to deploying only where AWS and GCP have points of presence, which today includes over 100 locations.

In contrast, Fortinet's SASE offering does not intend to have all security functions executed from the cloud. Given its strength as an ASIC-based, high-performance NGFW provider, it has to leverage its competitive advantage. Fortinet will promote the idea of hardening the WAN edge using its on-premises appliances for some security processing. Cato Networks, meanwhile, prides itself on running a single software stack in selected colocation facilities and where it believes it has a cost and flexibility advantage. It is aggressively expanding its own backbone into tertiary markets to expand its geographical presence beyond its 65 points of presence. Cloudflare also leverages its own backbone network, built up over time as a content delivery network provider to encompass 200 data centers around the globe, where Cloudflare performs security and data filtering in a single pass architecture. Each data center runs Cloudflare's single policy engine, and onramps to Cloudflare's edge include GRE tunnels, network interconnects, and Cloudflare's mobile clients. Zscaler is another strictly cloud-based SASE provider, leveraging its extensive cloud infrastructure built up over years as a cloud-based secure web gateway services provider. Its backbone network is made up of 150 points of presence around the globe.

Cisco, for its part, touts direct peering relationships from its 30+ regional data centers with thousands of network operators for high-performance, low-latency access to applications. While its aim is to offer the simplicity of its Meraki solutions with a seamlessly integrated series of security functions, its history of integration is poor. However, Cisco continues to make inroads in integrating its Viptela SD-WAN and Umbrella multifunction cloud security service, with deeper integration coming in March.

Aruba (HPE) Silver Peak's architecture calls for an on-premises, thin-edge appliance that combines SD-WAN, zone-based stateful firewall with advanced segmentation, routing interoperability, WAN optimization, network and application visibility, analytics, and automated integration with cloud-delivered security services from partners. It offers seven different hardware appliance models and a virtual appliance running on industry-standard hypervisors. Its SASE offering relies mostly on an ecosystem of security integration partnerships for most of its security functionality. Aruba (HPE) Silver Peak doesn't have any of its own PoPs, but it relies on its cloud-based security services partners for that connectivity. Specifically, those include Check Point, Netskope, Palo Alto Networks Prisma, and Zscaler. Versa gives its customers the option of running its services from the cloud, in on-premises gateways, or both, using a single operating system and software stack. Its cloud service has 90 points of presence around the globe and the company continues to expand that footprint. VMware takes a similar approach, giving its customers the option to subscribe to cloud-based SASE services and run those services on-premises. It currently has 33 PoPs, with plans to expand that to 50 in the next 12 to 18 months. It is also working with service provider partners to expand the number of PoPs in its arsenal.

Comparing Buying Options

The most common pricing model across the nine vendors covered in this research is a combination of bandwidth plus per-user pricing for SASE offerings that combine networking and security. This is the model employed by Cisco, Palo Alto Networks, Cato Networks, VMware, and to some extent Cloudflare and Versa Networks. Versa's pricing model is based on tiering for the services customers opt to activate and the throughput requirements for each site that is serviced. Fortinet, which has not yet completely solidified its pricing, opted to base its SASE pricing on a per user/per year model. Aruba (HPE) Silver Peak employs a pricing model similar to that of VMware, based on a per-appliance price, bandwidth, and support options. However, customers can also purchase a virtual instance software license based on the bandwidth tier they require. Zscaler's SASE pricing model is per user/per year, although it varies according to the function. For example, VPNs are set up as accounts.

Cato Networks' pricing model employs both bandwidth-based (to the Cato Cloud) and per-user pricing. Depending on their requirements, customers can opt for per-user pricing, bandwidth pricing, or both. Customers can reallocate capacity between sites in the same region without charge, and they can upgrade coverage during the contract period and pay the difference. Downgrades are not allowed, but customers can reallocate capacity to other regions. Deal discounts for customers are handled on a case-by-case basis. Pricing varies between regions based on the cost of service in each region.

Cisco licenses its DNA Premier SASE package based on bandwidth tiers. The customer is entitled to a specific number of end-user licenses based on the bandwidth tier. At the lowest end for a small branch office, a 5 Mbps tier entitles the customer to 10 Umbrella SIG Essentials licenses. For a headquarters location, a 10 Gbps bandwidth tier entitles the customer to 500 Umbrella SIG Essentials licenses. Customers can also purchase additional end-user licenses separately. Cisco has found that most customers who are migrating to Office365 are simultaneously deploying SD-WAN, and the intent is to bring Umbrella SIG Essentials into that mix. Cisco also offers a few different enterprise license agreement options for DNA Premier, and a growing number of components are also available through service provider license agreements (SPLAs). Contract periods include 1-, 3-, and 5-year intervals. The Cisco DNA Premier (DNA-P) software license subscription is sold as a single SKU. Cisco intends to add another SKU that combines networking, security and access—specifically SD-WAN, remote access, VPN, SWG, FWaaS, CASB, and ZTNA—in the future. Other bundles under consideration will address hybrid security options for customers transitioning from on-premises firewalls and SWGs to cloud-based security. Customers can go over the contracted number of users during the contract period, and at the end of the year or contract period, the number is corrected.

Cloudflare employs a flexible licensing scheme that gives customers the option of paying per user/per year and per user/per month. It also offers customers the option to pay as you go or sign up for enterprise license agreements. Pay as you go customers can adjust their subscription up or down based on the number of seats required on a monthly basis as their needs change, and those opting for ELA contracts can work with account managers to adjust contracts at renewal time. Pricing is consistent from one region to another. Cloudflare pricing is per user/per month for most of the components, including Zero Trust Access, Secure Web Gateway, FWaaS, and Remote Browser Isolation, but network-level services are priced according to the number of connections plus a bandwidth charge.

Although Fortinet has only recently finalized their FortiSASE pricing, it is based on the per subscription/per year model, with user tiers available from 25 users to over 10K users. Fortinet's packaging/bundling plans are still preliminary, but the company is considering user tiers at 25, 500, 2,000 and 10,000 users. Fortinet's first SASE bundle, called Secure Internet Access, is focused specifically on secure internet access for work from anywhere capability. A second bundle will extend to enterprises with policies for light branch and heavy branch use cases. A third bundle will focus on microsegmentation and control, which is when ZTNA will come into play. Fortinet intends to offer both ELAs and SPLAs, but those have not yet been finalized. Their pricing will be consistent across regions primarily because they're working with and targeting large multinationals.

The Aruba (HPE) Silver Peak pricing model includes a one-time capital expense for the appropriate appliance, along with a yearly support contract for maintenance and an annual subscription license based on bandwidth tiers. Customers can contract for annual increments of 1, 3, 5, and 7 years. Cloud-delivered security services are bought directly from Silver Peak security partners. Bandwidth tier increments are: 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, and 2 Gbps. Customers can upgrade at any time to a higher bandwidth tier, but only downgrade at renewal time.

Palo Alto Networks' Prisma Access of Networks pricing models are based on total bandwidth used across all sites. Bandwidth pools are divided into amounts each location requires, with a minimum bandwidth pool of 200 Mbps. The Prisma Access for Users license is based on the total number of users, with the bottom tier starting at 200 users. The latter provides broad endpoint support, including MacOs, IoS, Windows, Android, Google Chrome OS, and Linux. All models use an annual subscription. Prisma Access is not available as an enterprise license agreement or in pay as you go pricing. Customers can upgrade their tier or level at any time, but they can only downgrade after a term has expired. Palo Alto Networks does not rent onsite hardware. CloudGenix SD-WAN appliances can be bought via a CAPEX and subscription model, or they can be purchased using an OPEX model.

Versa's pricing model is based on tiering, the services customers opt to activate, and throughput requirements for each site that is serviced. Services linked to individual users are priced based on number of users, while services that are bandwidth and/or performance-based are priced based on throughput and performance requirements (such as Secure SD-WAN). For example, if a customer only selects Versa Secure Access, pricing is based solely on a per-user basis. When customers select multiple services, such as FWaaS, SWG, SA, etc., Versa packages multiple SASE services into a single offering that can include up to 5,000 work-from-anywhere users, up to 250Mbps per branch office, high performance for simultaneous cloud services, and so on. The packages are sold on a subscription basis and customers can select 1-, 2-, or 3-year contracts. Versa also offers enterprise license agreement and service provider license agreement buying programs. Customers can upgrade and downgrade their contract for bandwidth and number of seats.

VMware's SASE offerings are split between bandwidth-based licensing and user-based licensing. For SD-WAN functionality, it offers three subscriptions for standard, enterprise, and premium packages, which entitle the customer to its Orchestrator capabilities and dynamic multi-path optimization, partner gateway support, and a direct tunnel from branch to cloud security services. The enterprise and premium editions add orchestration for firewall edge deployments, advanced networking features, and separate lower bandwidth tiers. The premium edition adds gateways hosted in PoPs. VMware's ZTNA functionality is sold on a per-user basis and treated as an add-on to its Workspace One offering. Customers who want to buy subscriptions in bulk and hardware separately can opt for an ELA. VMware also offers SPLAs for service providers. Customers that contract through ELAs have the option to execute midterm upgrades of software editions.

Zscaler packages its SASE offering into three editions for Zscaler Internet Access. The Professional edition combines traffic forwarding authentication, reporting and updates, URL filtering, file type control, FWaaS, anti-malware, reputation-based threat protection, and cloud application visibility. The Business edition adds SSL inspection, a log streaming service, web access control, bandwidth control, mobile application control, advanced threat protection, cloud application control, DLP, and CASB. The Transformation edition adds advanced FWaaS, IPS, cloud sandbox, and more advanced CASB. The most common pricing model is an annual per-user subscription.

Comparing Support Models

In comparing basic support offerings across the nine vendors, Palo Alto Networks is somewhat limited in its basic support because it is limited to online portal access only. Phone support requires the premium support package, which is 20% of list price. However, Versa and Fortinet are unique among the vendors in offering (premium) onsite support directly. Some Cisco partners offer onsite support as well. Return merchandise authorization times also varied quite a bit, with Fortinet and Palo Alto Networks offering four-hour RMAs for premium support. The lengthiest RMA mentioned was 10 days by Palo Alto. Finally, SLAs also varied across the nine vendors. Aruba (HPE) Silver Peak does not provide an SLA for customers. On the other side, Cato Networks, Cisco, and Fortinet all include SLAs that specify five-nine availability of their cloud services.

Comparing SASE Support Offerings

	Basic	Premium	Onsite Support	Response Window	RMA	SLA
Cato	24x7x365	Dedicated SE	No	1 – 2 hours	Next day	99.999
Cisco	24x7 phone + online	Designated SM	Via partner			99.999 (for Umbrella services)
Cloudflare	24x7	White glove	via partner			100% uptime
Fortinet	24x7	Advanced SE	Yes		4 hours – next day w/ courier	99.999
Aruba (HPE) Silver Peak	24x7x365	Deployment Help	No	30 mins – 24 hours		None
Palo Alto Networks	24x7 online	24x7 phone + guidance			4 hours – 10 days	99.999
Versa	24x7 web + phone	24x7	Yes	1 – 4 hours		99.999
VMware	24x7	Root cause Analysis	Optional	30 mins – *12 hours	4 hours – NBD**	None
Zscaler	24x7	Level 2 Engineer	No	15 mins – 48 hours		99.999

*Business hours
**Next Business Day

Cato Networks provides support for its customers on a 24x7x365 basis worldwide, with the ability to add a dedicated support engineer as a premium option. Cato employs a small but growing customer success team with under seven members. The company provides no onsite support, although it offers remote initial deployment assistance. It provides next-day replacement of RMAs, although it does recommend that clients maintain spare SD-WAN appliances onsite. Its SLA specifies 99.999% availability of its cloud service.

Cisco added a new series of SASE strategic planning services to its security services portfolio, as well as deployment and support services typical of other Cisco security and networking products. Support packages include enhanced support that provides 24x7 phone and online support, along with configuration guidance, and premium support that includes priority technical support and a designated service manager. The Umbrella core services SLA is 99.999% availability. Additional details can be found at https://umbrella/cisco.com/support.

Cloudflare provides its enterprise plan customers with 24x7 support, Tier 1 support, a customer success manager, and a dedicated technical subject matter expert to assist with onboarding. A premium support option provides white glove support. Cloudflare provides no direct onsite support, but it is available from select managed services providers. The company guarantees 100% uptime of its cloud service.

Fortinet's existing FortiCare offering supports FortiSASE. Its global channel and partner networks offer customers the abilities to leverage services and support via Fortinet directly, or via approved service providers and partners. FortiSASE SLAs specify 99.999% availability. Further detail on FortiCare can be found at https://www.fortinet.com/support/support-services/forticare-support.

Aruba (HPE) Silver Peak provides 24x7x365 support with direct access to support engineers. A separate Silver Peak Assist subscription service provides customers with dedicated technical assistance for deployment activities. Aruba (HPE) Silver Peak support teams work with security services partners to ensure deployments succeed. The company also has authorized and certified deployment partners that focus on helping customers design, deploy, and manage their SD-WAN implementations. Component replacements are prioritized by technical support engineers when a new case is submitted into four tiers. Critical issues receive initial support within 30 minutes, major issues receive initial support within one hour, normal issues receive initial support within four hours, and questions/requests for information are answered within 24 hours.

Palo Alto's Prisma Access offers two support levels:

- Standard (included with Prisma Access) offers 24x7 access to the Palo Alto Networks support portal, Knowledge Base and all online documentation, and free online training videos, along with access to LiveCommunity.
- Premium (20% of list price) builds on standard support to add 24x7 telephone support, premium response time, continuous guidance and onboarding oversight, customer success engagement, and optimal posture/best practices guidance.

Both Standard and Premium support contracts include coverage for certified parts and trained technicians. For customers who require advanced RMA options, Palo Alto Networks' support program includes 130 parts depots located strategically around the globe. Replacement options include:

- Return and Repair – Customers return a faulty device and receive a replacement device within 10 business days. This is part of the Standard Support Contract.
- Next Business Day Delivery RMA – Makes reasonable efforts to have a replacement product for a hardware defect delivered by the next business day. This is part of the Premium Support Contract.
- 4-Hour Premium Support RMA – An optional upgrade to make a commercially reasonable best effort to deliver replacement hardware to customers within four hours of issuance of an RMA. It is intended for data center customers who require mission-critical response times. However, it is not available in all geographic locations.

Versa offers basic and premium support subscriptions. Basic support includes 24x7 web and phone support, along with a four-hour first response window and software upgrades and patches. Premium support is offered 24x7 and includes a one-hour first response time window. Optional onsite support is available directly from Versa. The company warrantees its hardware appliances for two years, but customers can purchase extended support options, such as 24x7 return to factory coverage to speed the RTF process and extend such returns beyond the two-year warranty. Faulty hardware is repaired or replaced within four weeks. Customers can also purchase next business day advanced replacement support to bypass the RTF process and have a replacement delivered onsite by a service technician, who also removes the defective unit for repair. Other support options include same business day advance replacement. These services are delivered via a network of global RMAs that span the U.S./Canada, EU and other European countries, APAC/Japan, Australia, the Middle East, and Africa. Versa's SLA for its cloud-based service covers 99.999% uptime.

VMware provides three support packages for its SD-WAN offering, including basic, production, and premier support. Basic support provides global 24x7 access for critical issues, an unlimited number of support requests, one-hour response times for critical (Severity 1) issues, four-hour response times for major (Severity 2) issues, eight-hour response times for minor (Severity 3) issues, and online access to documentation and knowledge base. Production support adds 30-minute response times for critical (Severity 1) issues. Premier support builds on that with 24x7 global access for major (Severity 2) issues, root cause analysis, two-hour response times for major (Severity 2) issues, and four-hour response times for minor (Severity 3) issues.

Zscaler provides three support packages, including a standard support package bundled with its service, an optional premium support package, and an optional premium plus package. All three provide 24x7 access; phone, web portal, and admin UI; online training; user guides; and articles. Standard support provides access to Level 1 support engineers, and an escalation window for Severity 1 issues of 8x5 local time. Premium support provides access to Level 2 support engineers and an escalation window for Severity 1 issues of 24x7. Premium plus layers onto that access to a designated technical account manager and additional engagements with that manager on a weekly, monthly, or quarterly basis. Response windows for tickets submitted to Zscaler's support portal vary across the three packages, and times depend on the issue's severity level, ranging from P1 (most urgent) to P4 (low priority). Response SLAs for P1 issues range from two hours for standard support to 30 minutes for premium and 15 minutes for premium plus.

SASE Go-to-Market Motions

Cato Networks sells through a range of channel partners, including telecom or master agents in the U.S., and in the rest of the world they sell through MSPs, distributors, and VARs. MSPs provide their service on top of Cato's cloud infrastructure. They are in the process of signing up MSPs in the U.S. now. Discounts to channel partners range from 20% for telecom agents, 30% for VARs, and 40% for distributors. In special cases, 15% discounts are offered.

Cisco sells its SASE offering directly to large enterprises as well as through channel partners, including distributors, VARs, and service providers. It is targeting a wide variety of vertical markets, although it does not expect as much demand from financial services and healthcare due to compliance concerns. The verticals it is targeting include state and local government and education (SLED), where it has packages aimed at specific use cases, such as student-based pricing.

Cloudflare sells its SASE offering both directly to enterprise customers and through a range of channel partners. Service provider partners rely on Cloudflare's own infrastructure to deliver its SASE services, which are available in 100 countries around the world. It typically sells to IT and IT security buying centers, although in some cases, networking teams influence the buying decision.

Fortinet has prided itself on being a 100% channel-based company and intends to sell its fledgling SASE offerings through its typical service providers, MSSPs, distributors, and VARs. The company is not targeting specific verticals, but rather sees demand as being very diverse. Still, Fortinet does see the greatest amount of interest from technology, manufacturing, and government verticals. As for active customers or POCs, Fortinet has a couple of POCs with some very large, Tier-1 multinationals based in North America. The company plans to actively pursue customer opportunities first in North America, then expand sales activities and POCs to other parts of the globe in the second half of next year.

Aruba (HPE) Silver Peak goes to market via distributors, VARs, system integrators, service providers, and security technology alliance partners. VARS receive a 33% discount, which remains standard around the globe. To date, through those partners it has delivered over 2,000 production customer deployments of its Unity EdgeConnect SD-WAN edge platform. In the case of a service provider deployment, customers can opt for on-premises Aruba (HPE) Silver Peak hardware appliances or deploy it as a virtual network function running on the service provider's industry-standard CPE hardware. The EdgeConnect VNF can also be deployed alongside a partner's security VNF on different hardware appliances. The service provider manages the customer's deployment using a multi-tenant version of Aruba Orchestrator. The company's largest deployment, serving thousands of sites for a Fortune 50 retailer, was deployed by a service provider partner. Aruba (HPE) Silver Peak targets SLED opportunities with partners that have specific SLED expertise. Thanks to FIPS 140-2 validation testing completed in the first quarter of 2020, Silver Peak also targets federal government opportunities.

Palo Alto Networks sells its Prisma Access and SD-WAN products via service providers, distributors, and VARs. For service provider deployments, Palo Alto Networks hosts Prisma Access for channel partners. The company would not disclose the discounts that it offers to channel partners, nor disclose the number of Prisma Access customers it has, nor the POCs in which it is actively engaged.

Versa goes to market with its SASE service via a global network of partners, including VARs, system integrators, managed service providers, Telcos, resellers, and master agents. If requested, Versa will sell directly to customers. Service providers resell and/or white label Versa's SASE offering. They can host it in their own cloud and use their own networks and PoPs. They can also manage a customer's on-premises equipment and the cloud version as a managed service. Service provider partners include Comcast, Deutsche Telekom, Lumen, Verizon, and NTT Communications. Telecom master agent resellers include Avant, Intelisys, and Telarus. Versa targets a range of vertical markets, including finance, retail, healthcare, high tech, manufacturing, energy, and the public sector, including SLED.

VMware sells its SASE offering directly as well as through a variety of channel partners, including VARs, MSPs, and Telcos. In selling through service providers, deployments can be on-premises, hosted by VMware, and hosted by the service providers themselves. VMware does not target any particular vertical industries for its SASE offering.

Zscaler sells its SASE services directly to enterprises via its regional sales force, as well as through channel partners. Service provider partners resell the product, often using their own brand, but such services are hosted by Zscaler. Although it does not target specific vertical industries, Zscaler has a strong presence in technology, healthcare, financial services, manufacturing, and state and local governments.

Palo Alto Networks Thumbnail

Palo Alto Networks entered the SASE market early in 2019 when it launched its cloud-based Prisma security suite, which included the Prisma Access edge SD-WAN to provide secure access for branch locations. To shore up its SD-WAN capability, in April 2020 the company acquired SD-WAN provider CloudGenix. Palo Alto Networks continues to build on that foundation by integrating the CloudGenix SD-WAN into the Prisma suite and enhancing it by applying machine learning to bandwidth management, extending automation to speed problem resolution, and adding new appliances at the low end for small branch locations and at the high end for large branches, campuses, and data centers. Today, Palo Alto Networks offers four different SASE packages. They include the following:

- Prisma Access Business provides URL filtering and DNS security
- Prisma Access Business Premium provides URL filtering, DNS security, threat prevention, and Wildfire sandbox
- Prisma Access Enterprise provides URL filtering, DNS security, threat prevention, Wildfire, and private application access via service connections (two with Local SKU, five with Worldwide SKU). Optional add-ons for this package include additional service connections, DLP, and interconnect (user to branch and branch to branch access)
- Prisma Access ZTNA: URL filtering, threat prevention, and private application access via service connections (two with Local SKU, five with Worldwide SKU). Optional add-ons include additional service connections and DLP

SASE Supported Functions
Palo Alto Networks

Must Have	Nice to Have	And Then Some
◉ SD-WAN	○ WAAP	◉ Wi-Fi Hotspot Protection
◉ SWG	○ RBI	◉ Network Obfuscation
◉ CASB	◉ Recursive DNS	◉ Legacy VPN
◉ ZTNA	◉ Network Sandbox	◉ Edge Compute Protection
◉ FWaaS	◉ API Access to SaaS	◉ UEBA
◉ ID Sensitive Data/Malware	◉ Managed/Unmanaged Device Support	
◉ Line rate/edge		
◉ Line rate/cloud		

Prisma Access, managed by Palo Alto Networks, was designed as a cloud-agnostic service, although today it relies on AWS, Google Cloud and the subset of points of presence that can accommodate computing capabilities rather than just gateway functionality. Palo Alto Networks claims over 100 PoPs in 76 countries and intends to add another 5-10 over the next 12 to 24 months. The Prisma Access orchestration function is multitenant and leverages cloud-native technologies including containers, serverless, and microservices. Software-based security processing nodes (SPNs) deployed within the cloud infrastructure and based on the company's next-generation firewall technology are dedicated to each customer. While this ensures traffic separation and acceptable performance, it also increases Prisma Access's cost of operation. Palo Alto Networks' single-pass policy engine performs multiple inspections in a single pass, making it highly efficient in enforcing policies informed by contextual information on users, applications, and content. Despite initial integration of the CloudGenix SD-WAN, it is still sold separately from the SASE packages.

Palo Alto Networks' SASE offering is differentiated by the depth and effectiveness of its security functionality, based on its industry-leading NGFW and by the consolidation of at least 10 discrete point tools that it enables. The company lays claim to best-of-breed security and now SD-WAN capabilities, backed by a common policy engine and data model used to augment both security and networking. For existing NGFW customers, Palo Alto Networks provides consolidated management of both NGFW and Prisma Access products to simplify operation. The company also believes the Google Cloud network of data centers, linked via a dedicated fiber network, combined with its low-latency inline security, enables optimal application performance for remote users, backed up by latency SLAs of less than 10ms. Prisma Access competes most directly with Zscaler, and when it wins against that rival, it is most often due to its more robust security, ability to dynamically scale, and ease of management for existing NGFW customers.

Conclusion

Clearly, the SASE capabilities, pricing models, packaging, and integration efforts of these vendors are in their early stages of development and are likely to evolve over time as they build up operational experience. What will be key for early SASE customers and ultimately the solution providers is the level of integration and ease of operation across both networking and security functions, and how easy (or hard) it is to maintain vendor relationships and do business with the solution providers. The more contracts and different pricing SKUs the customer must navigate, the longer the adoption curve will be. For multi-vendor SASE providers working with integration partners, what will also be critical is to minimize finger pointing when issues arise, as they are sure to do. If service chaining is cumbersome and complicated for customers to navigate, that is a recipe for failure.

Beyond those operational issues, sales cycles will depend on the buying center, budget holders, and how well separate teams come together in implementing convergence projects. This market will likely shake out over a longer period of time than typical technology markets take. Combining networking and security into a single market has organizational and cultural implications, especially for larger enterprises, that will take longer to settle than architectural changes. Organizations will have to come to grips with how they are structured, how they approach adoption, and where the budget will come from. They will have to overcome some level of distrust between different IT groups, who will have to put aside their differences to make SASE a success. Executive management will need to create new, more cohesive objectives and incentives to ensure these groups come together in a productive way.

It is still quite early in the buyers' journeys, and most organizations are attempting to chart a new path to get to their ultimate destination: seamless convergence of networking and security in a mobile and cloud-dominated world.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com. You can also follow EMA on Twitter or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com

4068.021221