Angebote und Paketoptionen auf dem neuen SASE-Markt

Von Paula Musich
Ein Forschungsbericht von ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™)
Februar 2021

Gesponsert von:

paloalto® NETWORKS

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

Angebote und Paketoptionen auf dem neuen SASE-Markt

Inhalt

Angebote und Paketoptionen auf dem neuen SASE-Markt

Einleitung

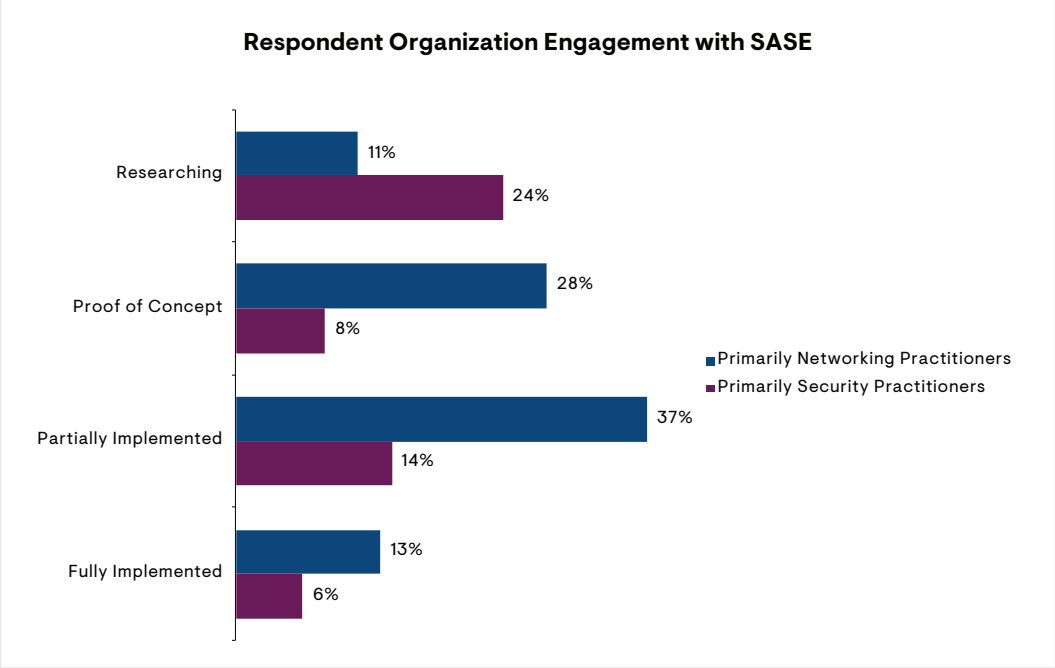
Der Begriff „Secure Access Service Edge“ oder kurz SASE wurde von Gartner-Analysten eingeführt und beschreibt das ehrgeizige Ziel, die separaten Netzwerk- und Sicherheitsmärkte zusammenzuführen, um gemeinsam die Anforderungen digitaler Unternehmen zu erfüllen. Bisher wurden die Netzwerk- und Sicherheitsinfrastrukturen separat verwaltet, doch in den meisten modernen Unternehmen ist das nicht mehr zweckmäßig. In der Vergangenheit musste der Datenverkehr von Zweigstellen und mobilen VPN-Clients an einen zentralen Ort umgeleitet werden, an dem er auf Leistungsprobleme, schädliche Aktivitäten und Malware überprüft und dann an das jeweilige Ziel weitergeleitet wurde, das sich häufig im selben Rechenzentrum befand. Doch inzwischen werden die meisten Anwendungen nicht mehr in zentralen Rechenzentren verwaltet, da immer mehr Unternehmen diverse Cloud-Services in Anspruch nehmen. Aufgrund der COVID-19-Pandemie und dem damit verbundenen Wechsel zur Telearbeit wurde die digitale Transformation viel schneller vorangetrieben, als es die Branche erwartet hatte.

Für Sicherheitsteams ist es fast unmöglich geworden, diverse isolierte Sicherheitslösungen und die zunehmende Zahl an Endpunktagenten sowie die Beziehungen/Verträge mit zahlreichen Sicherheitsanbietern zu verwalten. Perimeterzentrierte Sicherheitskonzepte, bei denen alle authentifizierten Benutzer in der DMZ als vertrauenswürdig gelten, sind längst überholt. Die alten Methoden weiterhin zu unterstützen und gleichzeitig zu verstehen, welche Sicherheitsmaßnahmen für Anwendungen, Workloads und Daten in den Rechenzentren von SaaS-, IaaS- und PaaS-Serviceanbietern angemessen und erforderlich sind, ist eine kaum zu meisternde Aufgabe. Das können sich nur etablierte und finanziell gut aufgestellte Sicherheitsteams leisten. Werden allerdings alte Netzwerksicherheitsarchitekturen für die neuen Datenverkehrsmuster übernommen, entstehen in der Regel Leistungsengpässe und die Benutzererfahrung wird beeinträchtigt. Diese Engpässe können wiederum dazu führen, dass Benutzer Sicherheitsfunktionen umgehen oder deaktivieren, wodurch sich neue Risiken für das Unternehmen ergeben.

Bei SASE steht nicht das Rechenzentrum des Unternehmens, sondern die Identität im Mittelpunkt. In Abhängigkeit von der Identität der Benutzer, Geräte und Anwendungen werden unterschiedliche Zugriffs- und Berechtigungsebenen festgelegt und Richtlinien angewendet. Anhand dieser Identitäts- und Kontextinformationen werden dann für jede Sitzung die relevanten Netzwerk- und Sicherheitsservices ausgewählt. Dazu können beispielsweise SD-WAN, WAN-Optimierung, Routing/Pfadauswahl und QoS für das Netzwerk sowie FWaaS, IDS/IPS, Malwareschutz, rekursives DNS, SWG, CASB und ZTNA für die Sicherheit gehören. Obwohl laut Gartner all diese Funktionen cloudbasiert sein sollten, bieten viele Unternehmen ihre SASE-Lösungen in verschiedenen Modellen an, zum Beispiel als Cloud- oder Hybridservices, bei denen ein Teil der Workloads auf On-Premises-Appliances und Clientsoftware in Zweigstellen ausgelagert wird. Zu diesen Anbietern gehören unter anderem Cato Networks, Cisco, Fortinet und Versa Networks. Andere wie VMware stellen sowohl rein cloudbasierte Lösungen als auch reine On-Premises-Gateways bereit. Diese Ansätze werden *Thin Branch* und *Heavy Branch* genannt. „Thin Branch“ bezieht sich auf die cloudbasierten und „Heavy Branch“ auf die lokal bereitgestellten Sicherheitsfunktionen. Letzteres wird vor allem von älteren hardwarebasierten NGFW-Anbietern wie Fortinet beworben, um bestehende Technologien auch während der Umstellung auf einen überwiegend cloudbasierten Sicherheitsservice weiterhin nutzen zu können.

Käuferinteresse an SASE-Lösungen

Obwohl Gartner das Whitepaper zu SASE erst im zweiten Halbjahr 2019 veröffentlicht hat, kennen viele IT-Fachkräfte bereits den Begriff und das grundlegende Konzept. Enterprise Management Associates hat festgestellt,[1] dass mindestens 75 Prozent bzw. 78 Prozent der Teilnehmer zweier unterschiedlicher Umfragen davon gehört hatten. Bei den Umfrageergebnissen traten allerdings einige interessante Unterschiede zwischen den Netzwerk- und den Sicherheitsexperten zutage. Von den Netzwerkexperten, die SASE kannten, gaben 37 Prozent an, dass ihr Unternehmen das Konzept bereits teilweise implementiert hat. Bei den Sicherheitsexperten waren es nur 14 Prozent. 28 Prozent der Netzwerkexperten sagten aus, dass ihr Unternehmen zum Zeitpunkt der Befragung eine SASE-Evaluierung oder einen Machbarkeitsnachweis (Proof of Concept, PoC) durchführt – im Gegensatz zu nur 8 Prozent der Sicherheitsexperten. Obwohl der Markt noch nicht ausgereift ist und es bisher nur wenige Lösungen gibt, bestätigten 13 Prozent der Netzwerkexperten, dass ihr Unternehmen bereits eine SASE-Lösung implementiert hat. Bei den Sicherheitsexperten waren es nur 6 Prozent. Etwa 10 Prozent der befragten Netzwerkexperten waren an der Auswahl der SASE-Lösung und der Planung der Implementierung beteiligt. Nur 2 Prozent hatten sich überhaupt nicht damit befasst. Das deutet darauf hin, dass sich in den meisten Unternehmen eher die Netzwerkteams als die Sicherheitsexperten mit der neuen Technologie befassen und die SASE-Einführung vorantreiben. Dabei ist zu berücksichtigen, dass die SD-WAN-Anbieter ihre SASE-Lösungen schon wesentlich aktiver bewerben als die Anbieter von Sicherheitslösungen. Dies hatte vermutlich auch einen gewissen Einfluss auf die Antworten der Umfrageteilnehmer. Viele IT-Fachkräfte möchten zu den Ersten gehören, die erfolgsversprechende neue Technologien einführen, daher gibt es unter den einzelnen Gruppen sicher auch einen gewissen Konkurrenzkampf um die Vorreiterrolle bei der SASE-Einführung.

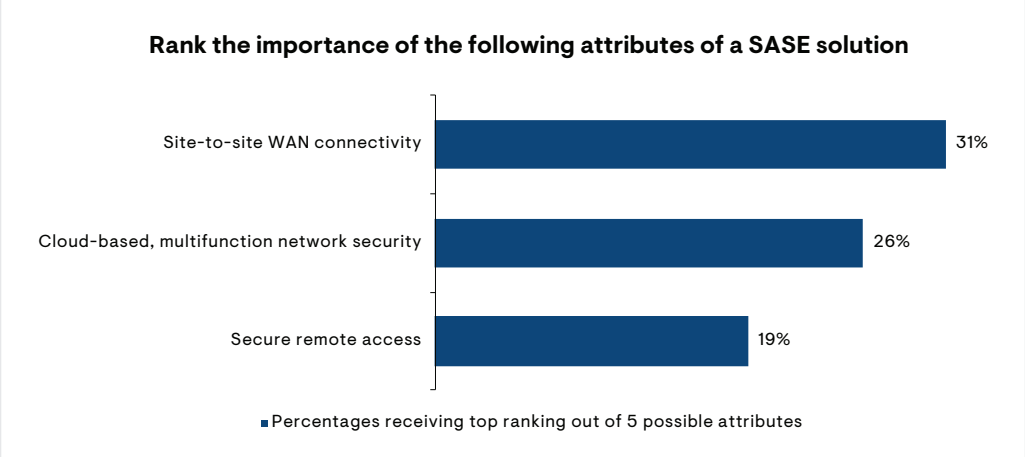


[1] In zwei separaten Forschungsprojekten Ende 2020, bei denen überwiegend Netzwerk- und Sicherheitsfachkräfte befragt wurden

Doch unabhängig davon, wer die Einführung des neuen Konzepts vorantreibt, versuchen immer mehr Unternehmen, die Netzwerk- und Sicherheitsinfrastrukturen zu straffen, um die Benutzererfahrung und die Verwaltbarkeit zu verbessern und die Komplexität zu verringern. SecOps-Teams, die in der Regel zahlreiche Tools für den Schutz der digitalen Ressourcen ihres Unternehmens nutzen, hoffen, dass sich dadurch die Zahl der zu verwaltenden Anbieterbeziehungen und Verträge reduzieren lässt. Das Interesse an SASE ist zwar groß, doch da sich die Marketingbotschaften teilweise stark unterscheiden, ist vielen vermutlich nicht ganz klar, was eine SASE-Lösung tatsächlich ausmacht.

Von den Netzwerkexperten, deren Unternehmen mit der SASE-Implementierung bereits begonnen hatten, gab mindestens die Hälfte an, dass die COVID-19-Pandemie die Einführung beschleunigt hat. Andererseits sagte ein Drittel der Fachkräfte, die ebenfalls bereits mit der SASE-Implementierung beschäftigt waren, dass die Pandemie keinerlei Einfluss auf die Entscheidung gehabt habe. Das lässt vermuten, dass aufgrund der zunehmenden Cloud-Nutzung und der Notwendigkeit, immer mehr externe und mobile Mitarbeiter zu unterstützen, die Konvergenz von Netzwerk und Sicherheit eine natürliche Evolution ist – unabhängig von der plötzlichen Zunahme an Homeoffice-Arbeitsplätzen. Dennoch sind 82 Prozent der Befragten der Meinung, dass SASE zur Geschäftskontinuität während der Pandemie beitragen kann. Von dieser Gruppe gaben 82 Prozent an, dass der Vorteil von SASE in den sicheren Remoteverbindungen besteht. 78 Prozent waren der Meinung, dass die cloudbasierten Sicherheitsservices entscheidend sind, und 68 Prozent sahen den größten Nutzen im Zugriff auf Cloud-Anwendungen und -Services.

Im Rahmen einer Studie zur WAN-Transformation wurden hauptsächlich Netzwerkfachkräfte befragt, die unter anderem einschätzen sollten, auf welche Attribute einer SASE-Lösung potenzielle Käufer den größten Wert legen. Bei der Einstufung fünf unterschiedlicher SASE-Attribute nach ihrer Bedeutung landete die SD-WAN-Konnektivität zwischen Standorten mit 31 Prozent auf Platz 1, gefolgt von funktionsreichen cloudbasierten Netzwerksicherheitslösungen mit 26 Prozent. Einen sicheren Fernzugriff (z. B. Remote-VPN für Telearbeiter und mobile Benutzer) nannten 19 Prozent als das wichtigste und 30 Prozent als das zweitwichtigste Attribut. Als weniger wichtig schätzten die Umfrageteilnehmer den direkten Cloud-Zugriff bzw. die Umstellung auf die Cloud (Onramping) und einen umfassenden Überblick über die Abläufe ein. Angesichts dieser Prozentzahlen verwundert es nicht, dass die meisten Umfrageteilnehmer, die mit der SASE-Implementierung bereits begonnen hatten, eine Kombination aus einer SASE-kompatiblen SD-WAN-Lösung, einer SASE-kompatiblen Netzwerk- und/oder Cloud-Sicherheitslösung sowie einer SASE-kompatiblen Lösung für den sicheren Fernzugriff bevorzugten. 26 Prozent wählten diese Kombination, 24 Prozent bevorzugten hingegen ein SD-WAN, das an die SASE-Anforderungen angepasst wurde. 23 Prozent würden lieber mit einer SASE-kompatiblen Netzwerk- oder Cloud-Sicherheitslösung arbeiten.



Wie bei jeder neuen Technologie werden Unternehmen vermutlich zuerst bestimmte Elemente der SASE-Lösung für kleinere Projekte und spezifische Anwendungsfälle nutzen, zum Beispiel für die Ablösung von MPLS oder den Austausch von Edge-Firewalls oder VPN-Infrastrukturen gegen cloudbasierte Sicherheitsfunktionen. Zu den ersten, die diese neuen Technologien einführen, werden wahrscheinlich noch junge Technologieunternehmen gehören, die vollständig in der Cloud agieren, und kleinere Organisationen, deren Infrastrukturen nicht so umfangreich wie bei großen Konzernen sind. Letztere müssen insbesondere die Trägheit überwinden und sich auf eine längere Schulungs- und Eingewöhnungszeit einstellen.

Markt und Wettbewerb

Die Veröffentlichung des Whitepapers von Gartner Ende 2019 und die Notwendigkeit, Anfang 2020 schnell eine große Zahl an Telearbeitsplätzen einzurichten, haben zahlreiche unterschiedliche Anbieter auf das Potenzial von SASE aufmerksam gemacht. EMAs Schätzungen zufolge vermarkten mindestens 16 Anbieter aktiv SASE-Services und mit jeder Phase des Hype Cycle wird die Zahl schnell steigen. Nicht nur SD-WAN-Anbieter haben den neuen Markt erobert, sondern auch traditionelle Netzwerkanbieter, Netzwerksicherheitsanbieter (sowohl traditionelle als auch cloudbasierte) und Content-Delivery-Network-Anbieter. Hinzu kommen reine SASE-Start-ups wie Cato Networks und Open Systems.

Man wird leicht dazu verleitet, die Angebote auf dem Markt in zwei Kategorien zu unterteilen: SASE-Lösungen, die aus einer Hand stammen, und SASE-Lösungen, für die Angebote mehrerer Anbieter kombiniert werden. Bei Unternehmen, die alle SASE-Funktionen für Netzwerke und Sicherheit selbst bereitstellen, müssen die Kunden nicht mehrere Anbieterbeziehungen und Verträge verwalten. Diese Anbieter stellen ihren Kunden einen zentralen Ansprechpartner bei Problemen und eine übersichtliche Managementkonsole für eine einfachere Verwaltung bereit. Andererseits können Kunden bei SASE-Anbietern mit heterogenen Lösungen die besten Technologien auswählen, die dann in einem Service kombiniert werden, und dadurch bestehende Beziehungen zu vertrauenswürdigen IT-Sicherheits- und/oder Netzwerkanbietern weiterführen.

Aufschlussreicher als dieser Vergleich ist allerdings, sich anzusehen, wie die jeweiligen Anbieter ihre SASE-Lösungen erworben oder entwickelt haben, denn dadurch lassen sich Lücken in den angebotenen SASE-Funktionen und die Schwächen des jeweiligen Ansatzes aufdecken. Nachfolgend werden die verschiedenen Ansätze beschrieben, die die meisten SASE-Anbieter bisher verfolgen.

Kategorisierung der verschiedenen SASE-Anbieter

Unabhängige SASE-Experten	Übernahmen von großen Netzwerk-/ Sicherheitsanbietern	Kooperation von Sicherheits- und SD-WAN-Anbietern	CDN-Anbieter mit SASE-Funktionen
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	

Aus dieser Tabelle hat EMA neun SASE-Anbieter ausgewählt, die integrierte Netzwerk- und Sicherheitsservices schon am besten an die Anforderungen digitaler Unternehmen angepasst zu haben scheinen. Dazu gehören:

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

Der SASE-Markt ist allerdings bei Weitem noch nicht ausgereift: Cisco, Fortinet und Palo Alto Networks, die zu den größten Mitbewerbern gehören und dieses Marktsegment durch Übernahmen erobert haben, positionierten sich erst im Herbst 2020 mit ersten Integrations- und Paketangeboten auf dem wachsenden Markt. Cisco hatte 2012 Meraki und 2017 Viptela übernommen und gab bei der Einführung seiner SASE-Lösung an, dass es schon seit Jahren an der Zusammenführung der Netzwerk- und Sicherheitsbereiche arbeite, insbesondere seit der Übernahme von OpenDNS im Jahr 2015.

Sicherheitsfunktionen

EMA ist der Ansicht, dass die gleichen Sicherheitsfunktionen, die Mitarbeiter bei direkten Verbindungen zum Unternehmensnetzwerk schützen, auch für Roaming, Zweigstellen und Cloud-Services gelten sollten. Eine echte SASE-Lösung muss daher mindestens SD-WAN, SWG, CASB, ZTNA, FWaaS, die Erkennung von Malware und sensiblen Daten (einschließlich verschlüsselter Daten) sowie konsistente Echtzeitverarbeitung am Netzwerkrand und in der Cloud umfassen. Diese Anforderungen kann kaum einer (oder sogar gar keiner) der in dieser Studie genannten Anbieter erfüllen. So kann Silver Peak trotz der Zusammenarbeit mit einigen Sicherheitspartnern bisher keine sensiblen Daten oder Malware identifizieren. Die Einführung einer solchen Funktion ist allerdings in Zukunft geplant. Bei Fortinet sind CASB und ZTNA derzeit als separate Angebote in Kombination mit der Fortinet Security Fabric erhältlich. Cloudflare bietet keinen API-Zugriff auf SaaS, plant aber, in Kürze SD-WAN, die Erkennung sensibler Daten, FWaaS und Netzwerk-Sandboxing einzuführen. VMware wird SWG, CASB und FWaaS erst im zweiten Quartal einführen. Es ist nicht klar, ob Cisco maximale Übertragungsraten am Edge und in der Cloud unterstützt. Die SASE-Lösung von Zscaler verfügt über die bisher umfangreichsten integrierten Netzwerk- und Sicherheitsfunktionen, aber dazu arbeitet das Unternehmen auch mit einem SD-WAN- und WAAP-Anbieter zusammen. Das verdeutlicht, wie unausgereift der Markt zum aktuellen Zeitpunkt ist und welche Hürden die Teilnehmer noch überwinden müssen, damit die SASE-Vision Wirklichkeit wird.

Zusätzlich zu diesen Kernfunktionen könnten potenzielle Käufer auch Angebote wie der Schutz von Webanwendungen und API, Remote-Browser-Isolierung, rekursives DNS, Netzwerk-Sandboxing, API-Zugriff auf SaaS für Datenkontext und die Unterstützung verwalteter und nicht verwalteter Geräte interessieren. Von den neun von EMA ausgewählten Anbietern bieten lediglich Cloudflare, Versa Networks und Zscaler WAAP-Funktionen an und Fortinet nur WAF. Palo Alto Networks, Fortinet und Cato unterstützen keine RBI, während Cisco und VMware die Integration dieser Funktion planen. Silver Peak ist dafür auf Partner angewiesen, während Versa Networks RBI gerade eingeführt hat. Rekursives DNS ist mit den Lösungen von Cisco, Palo Alto Networks und Versa verfügbar, Netzwerk-Sandboxing wiederum bei Cisco, Palo Alto Networks, Fortinet, Versa, Zscaler und einem Silver Peak-Partner.

Zu den weiteren potenziell attraktiven Funktionen gehören der Schutz von WLAN-Hotspots, Netzwerkverschleierung, Unterstützung älterer VPNs, der Schutz von Edge-Computing und UEBA. Den Lösungen von Cato Networks und Aruba (HPE) Silver Peak fehlen diese Funktionen, aber Cisco, Fortinet, Palo Alto Networks und Versa Networks bieten sie entweder direkt oder über Partner an. Zscaler fehlen Funktionen für ältere VPNs, den Schutz von Edge-Computing und UEBA. VMware plant die Einführung des Schutzes von Edge-Computing.

SASE-Architekturen

Die Struktur der SASE-Lösungen kann nicht nur einen erheblichen Einfluss auf die Leistung, sondern auch auf die Betriebskosten, die Kosten für die Servicebereitstellung und die Points-of-Presence-Knoten haben. Prisma Access, der SASE-Service von Palo Alto Networks, wird beispielsweise auf AWS und GCP ausgeführt und Palo Alto Networks weist jedem Client einen eigenen Security Processing Node (SPN) zu. Dadurch fallen zwar höhere Betriebskosten an, aber die Clients sind besser voneinander isoliert und es werden Leistungseinbußen vermieden, die bei einer gemeinsam genutzten Infrastruktur auftreten können. Das Unternehmen betont, dass seine Architektur cloudunabhängig ist, aber es ist auf die Points of Presence von AWS und GCP angewiesen. Diese umfassen derzeit über 100 Standorte.

Fortinet hingegen plant nicht, alle Sicherheitsfunktionen seiner SASE-Lösung in der Cloud anzubieten. Da sich das Unternehmen einen Namen als Anbieter leistungsstarker ASIC-basierter NGFW gemacht hat, muss es diesen Wettbewerbsvorteil für sich nutzen. Es wird für die WAN-Edge-Härtung mithilfe seiner On-Premises-Appliances für bestimmte Sicherheitszwecke werben. Cato Networks wiederum betont, dass es einen einzigen Softwarestack in bestimmten Colocation-Rechenzentren ausführt und dadurch niedrigere Kosten und eine größere Flexibilität erzielt. Das Unternehmen betreibt eine aggressive Expansion seines Backbonenetzwerks in Tertiärmärkte, um die aktuell 65 Points of Presence zu ergänzen. Cloudflare nutzt ebenfalls sein eigenes Backbonenetzwerk, das im Laufe der Zeit auf ein Content-Delivery-Network mit 200 Rechenzentren weltweit angewachsen ist. Dort werden Sicherheitsfunktionen und Datenfilterungen in einer Single-Pass-Architektur ausgeführt. In jedem Rechenzentrum wird die Richtlinienengine von Cloudflare eingesetzt und Verbindungen zum Cloudflare-Edge werden über GRE-Tunnel, Netzwerk-Interconnects und mobile Clients von Cloudflare hergestellt. Zscaler ist ein weiterer rein cloudbasierter SASE-Anbieter, der seine im Laufe der Jahre stark angewachsene Cloud-Infrastruktur für cloudbasierte Secure Web Gateway-Services nutzt. Sein Backbonenetzwerk umfasst 150 Points of Presence weltweit.

Cisco wiederum wirbt mit den direkten Peering-Verbindungen aus seinen über 30 regionalen Rechenzentren mit Tausenden Netzwerkbetreibern, die beim Zugriff auf Anwendungen für hohe Leistung und niedrige Latenz sorgen. Das Unternehmen ist bestrebt, die Benutzerfreundlichkeit seiner Meraki-Lösungen mit nahtlos integrierten Sicherheitsfunktionen zu kombinieren, doch bisher waren die Integrationen nicht sonderlich erfolgreich. Allerdings geht Cisco mit der Einbindung von Viptela SD-WAN und funktionsreicher Umbrella-Cloud-Sicherheitsservices neue Wege. Die umfassende Integration ist für März geplant.

Die Architektur von Aruba (HPE) Silver Peak besteht aus einer On-Premises-Thin-Edge-Appliance, die SD-WAN, eine zonenbasierte Stateful-Firewall mit erweiterter Segmentierung, Routing-Interoperabilität, WAN-Optimierung, Netzwerk- und Anwendungstransparenz, Analysen und die automatisierte Integration cloudbasierter Sicherheitsservices von Partnern umfasst. Das Unternehmen bietet sieben unterschiedliche Hardwaremodelle und virtuelle Appliances auf branchenüblichen Hypervisoren. Für die Sicherheitsfunktionen seiner SASE-Lösung ist es überwiegend auf seine Sicherheitsintegrationspartner angewiesen. Aruba (HPE) Silver Peak hat keine eigenen PoP, sondern nutzt die Verbindungen der cloudbasierten Sicherheitspartner. Dazu gehören Check Point, Netskope, Palo Alto Networks Prisma und Zscaler. Bei Versa können die Kunden zwischen Services in der Cloud, auf On-Premises-Gateways oder einer Kombination aus beidem wählen – unter Nutzung eines einzigen Betriebssystems und eines kompletten Softwarestacks. Der Cloud-Service verfügt über 90 Points of Presence weltweit und das Unternehmen ergänzt diese fortlaufend. VMware verfolgt einen ähnlichen Ansatz und bietet seinen Kunden die Möglichkeit, cloudbasierte SASE-Services zu abonnieren und diese vor Ort auszuführen. Das Unternehmen verfügt über 33 PoP und plant, diese in den nächsten 12 bis 18 Monaten auf 50 auszubauen. Außerdem arbeitet es mit Serviceanbietern zusammen, um mehr PoP zur Verfügung stellen zu können.

Vergleich der Kaufoptionen

Das gängigste SASE-Preismodell der neun im Rahmen dieser Studie untersuchten Anbieter ist eine Kombination aus Bandbreite und Benutzerzahl. Ein solches Modell bieten Cisco, Palo Alto Networks, Cato Networks, VMware und zu einem gewissen Grad auch Cloudflare und Versa Networks an. Das Preismodell von Versa basiert auf Serviceebenen, die die Kunden aktivieren können, und den Durchsatzanforderungen für die jeweiligen Standorte. Fortinet hat seine Preise noch nicht endgültig festgelegt, bietet aber momentan Jahrestarife pro Benutzer an. Aruba (HPE) Silver Peak nutzt ein ähnliches Preismodell wie VMware und rechnet nach Zahl der Appliances, Bandbreite und Supportoptionen ab. Kunden können jedoch auch eine Softwarelizenz für eine virtuelle Instanz mit der benötigten Bandbreite erwerben. Zscaler bietet ebenfalls Jahrestarife pro Benutzer an, aber diese variieren je nach Funktion. VPNs werden beispielsweise als Konten eingerichtet.

Bei dem Preismodell von Cato Networks wird sowohl die Bandbreite (für Verbindungen zur Cato Cloud) als auch die Zahl der Benutzer berücksichtigt. Kunden können ihren Anforderungen entsprechend entweder Tarife pro Benutzer, pro benötigte Bandbreite oder eine Kombination aus beidem wählen. Sie haben die Möglichkeit, Kapazitäten gebührenfrei zwischen Standorten in derselben Region zu verschieben oder während der Vertragslaufzeit zu einem höheren Tarif zu wechseln und nur die Differenz zu zahlen. Downgrades sind nicht zulässig, aber Kunden können ihre Kapazitäten auf andere Regionen übertragen. Rabattoptionen werden im jeweiligen Einzelfall mit dem Kunden besprochen. Die Preise variieren in den verschiedenen Regionen aufgrund der unterschiedlichen Servicekosten.

Cisco lizenziert sein DNA Premier SASE-Paket nach Bandbreite und den Kunden steht dann eine entsprechende Anzahl an Benutzerlizenzen zu. Bei dem günstigsten Tarif für kleine Zweigstellen erhalten Kunden mit 5 Mbit/s zehn Umbrella SIG Essentials-Lizenzen. Für Unternehmenszentralen sind 10 Gbit/s Bandbreite und 500 Umbrella SIG Essentials-Lizenzen verfügbar. Kunden können zudem zusätzliche Endbenutzerlizenzen separat erwerben. Cisco hat festgestellt, dass die meisten Kunden, die zu Office 365 wechseln, auch SD-WAN implementieren, und plant daher, Umbrella SIG Essentials zu diesem Paket hinzuzufügen. Das Unternehmen bietet außerdem einige DNA Premier-Lizenzvertragsoptionen für Unternehmen an und immer mehr Komponenten sind auch über Lizenzverträge für Serviceanbieter verfügbar. Die Vertragslaufzeiten betragen ein, drei oder fünf Jahre. Das Softwarelizenzabonnement für Cisco DNA Premier (DNA-P) wird als eine SKU angeboten. Geplant ist zudem eine weitere SKU, die Netzwerk-, Sicherheits- und Zugangsfunktionen – insbesondere SD-WAN, Fernzugriff, VPN, SWG, FWaaS, CASB und ZTNA – umfasst. Zu den weiteren Plänen für Bundles gehören hybride Sicherheitsfunktionen für Kunden, die von On-Premises-Firewalls und SWGs zu cloudbasierten Sicherheitslösungen wechseln. Kunden können während der Vertragslaufzeit die angegebene Zahl an Benutzern überschreiten und dies dann zum Vertragsende korrigieren.

Cloudflare nutzt ein flexibles Lizenzmodell, bei dem Kunden entweder einen Jahrestarif oder einen Monatstarif pro Benutzer wählen. Außerdem können sie sich für ein nutzungsbasiertes Modell entscheiden oder Unternehmens-Lizenzverträge abschließen. Kunden mit nutzungsbasierten Modellen können bei Bedarf die Zahl der benötigten Lizenzen monatlich anpassen. Vertragskunden haben zum Vertragsende die Möglichkeit, zusammen mit ihrem Account Manager die zukünftigen Anforderungen zu besprechen. Die Preise sind für alle Regionen identisch. Cloudflare bietet für die meisten Komponenten, einschließlich Zero-Trust-Zugriff, Secure Web Gateway, FWaaS und Remote-Browser-Isolierung, Monatstarife pro Benutzer an, aber Netzwerkservices werden basierend auf der Zahl der Verbindungen und einer Bandbreitengebühr berechnet.

Fortinet hat erst kürzlich die FortiSASE-Preise finalisiert, die auf einem Jahresabonnement basieren. Die Benutzeroptionen reichen von 25 bis über 10.000 Benutzer. Die Paket- und Bundle-Preise gelten nur vorläufig, aber das Unternehmen plant, Tarife für 25, 500, 2.000 und 10.000 Benutzer anzubieten. Sein erstes SASE-Bundle „Secure Internet Access“ wurde speziell für einen sicheren Internetzugang für standortunabhängige Arbeitsplätze entwickelt. Ein zweites Bundle ist für Unternehmen geplant und wird Richtlinien für Light-Branch- und Heavy-Branch-Anwendungsbereiche umfassen. Bei dem dritten Bundle wird der Schwerpunkt auf Mikrosegmentierung und Kontrollfunktionen und damit auf ZTNA liegen. Fortinet plant Lizenzverträge für Unternehmen und für Serviceanbieter, die aber momentan noch nicht verfügbar sind. Die Preise werden für alle Regionen identisch sein, weil sie überwiegend für große multinationale Unternehmen konzipiert sind.

Das Preismodell von Aruba (HPE) Silver Peak umfasst einmalige Anschaffungskosten für die erforderliche Appliance, einen Jahresvertrag für den Support und ein Jahresabonnement basierend auf der Bandbreite. Kunden können Verträge für ein, drei, fünf und sieben Jahre abschließen. Cloudbasierte Sicherheitsservices werden direkt von den Silver Peak-Sicherheitspartnern erworben. Die verfügbaren Bandbreitenoptionen umfassen 50 Mbit/s, 100 Mbit/s, 200 Mbit/s, 500 Mbit/s, 1 Gbit/s und 2 Gbit/s. Eine Erhöhung der Bandbreite ist jederzeit, eine Reduzierung allerdings nur bei der Vertragsverlängerung möglich.

Die Preismodelle für die netzwerkspezifische Nutzung von Prisma Access richten sich nach der gesamten Bandbreitennutzung an allen Standorten. Bandbreitenpools werden in die am jeweiligen Standort benötigten Kapazitäten aufgeteilt und der Mindestumfang beträgt 200 Mbit/s. Die benutzerspezifische Lizenz für Prisma Access richtet sich nach der Gesamtzahl der Benutzer. Die Mindestzahl beträgt 200 Benutzer. Bei diesem Angebot werden zudem diverse Endpunkte unterstützt, einschließlich macOS, iOS, Windows, Android, Google Chrome OS und Linux. Für alle Modelle gibt es ein Jahresabonnement. Prisma Access ist weder als Unternehmens-Lizenzvertrag noch als nutzungsbasiertes Preismodell (Pay As You Go) erhältlich. Kunden können jederzeit ein Upgrade anfordern, aber Downgrades sind nur nach Ablauf des Abonnements möglich. Palo Alto Networks vermietet keine Hardware für die lokale Nutzung. CloudGenix SD-WAN-Appliances können im Rahmen eines Investitions- und Abonnementmodels erworben oder als Betriebskosten abgerechnet werden.

Das Preismodell von Versa berücksichtigt verschiedene Serviceebenen, die vom Kunden aktivierten Services und die Durchsatzanforderungen für jeden Standort. Services für Einzelbenutzer werden nach der Zahl der Benutzer abgerechnet, bandbreiten- und/oder leistungsbezogene Services entsprechend nach Durchsatz- und Leistungsanforderungen (z. B. Secure SD-WAN). Wenn ein Kunde beispielsweise nur Versa Secure Access wählt, gilt ein Preis pro Benutzer. Entscheidet sich ein Kunde für mehrere Services wie FWaaS, SWG und SA, kombiniert Versa diese SASE-Services zu einem Angebot, das beispielsweise bis zu 5.000 standortunabhängige Benutzer, bis zu 250 Mbit/s pro Zweigstelle, eine hohe Leistung für simultane Cloud-Services und weitere Funktionen umfassen kann. Diese Pakete werden als Abonnement verkauft und Kunden können Verträge mit einer Laufzeit von ein, zwei oder drei Jahren abschließen. Versa bietet auch Lizenzverträge für Unternehmen und Serviceanbieter an. Es sind Upgrades und Downgrades für die Bandbreite und Zahl der Benutzer möglich.

Die SASE-Angebote von VMware unterscheiden zwischen bandbreiten- und benutzerbasierter Lizenzierung. Für SD-WAN gibt es drei Abonnements für Standard-, Enterprise- und Premium-Pakete, mit denen Kunden Orchestrator-Funktionen und dynamische Multi-Path-Optimierung, Unterstützung für Gateways von Partnern und einen direkten Tunnel von der Zweigstelle zu den Cloud-Sicherheitsservices erhalten. Mit der Enterprise- und der Premium-Version stehen den Kunden auch Orchestrierungsfunktionen für Firewall-Edge-Bereitstellungen, komplexe Netzwerkfunktionen und separate Bandbreitenebenen zur Verfügung. Die Premium-Version umfasst zudem Gateways an den PoP. Die ZTNA-Funktion von VMware wird pro Benutzer angeboten und gilt als Add-on für Workspace One. Kunden, die eine große Menge an Abonnements und separat dazu Hardware erwerben möchten, können einen Unternehmens-Lizenzvertrag abschließen. VMware bietet auch Lizenzverträge für Serviceanbieter an. Kunden mit Unternehmens-Lizenzverträgen haben die Möglichkeit, während der Vertragslaufzeit Softwareupgrades zu erwerben.

Das SASE-Angebot von Zscaler umfasst drei Versionen von Zscaler Internet Access. Die Professional-Version bietet die Authentifizierung bei der Datenverkehrsweiterleitung, Berichterstellung und Updates, URL Filtering, Kontrolle der Dateitypen, FWaaS, Malwareschutz, reputationsbasierte Bedrohungsabwehr und Transparenz für Cloud-Anwendungen. Die Business-Version umfasst zusätzlich SSL-Überprüfung, Log Streaming Service (LSS), Internetzugangskontrolle, Bandbreitenkontrolle, Kontrolle der mobilen Anwendungen, komplexe Bedrohungsabwehr, Kontrolle der Cloud-Anwendungen, DLP und CASB. Die Transformation-Version beinhaltet zudem erweiterte FWaaS, IPS, Cloud-Sandboxing und erweiterte Funktionen für CASB. Das gängigste Preismodell ist ein Jahresabonnement mit Abrechnung pro Benutzer.

Vergleich der Supportmodelle

Bei dem Vergleich der Supportmodelle der neun Anbieter fällt auf, dass der Standardsupport von Palo Alto Networks am stärksten eingeschränkt ist, da Kunden ihn nur über das Onlineportal erreichen. Telefonsupport ist nur mit dem Premium-Paket zu 20 Prozent des Listenpreises erhältlich. Nur Versa und Fortinet bieten (Premium-)Support vor Ort an. Bei einigen Partnern von Cisco ist diese Option ebenfalls verfügbar. Die Bearbeitungszeiten bei einer Reklamation variieren stark. Fortinet und Palo Alto Networks bieten mit vier Stunden beim Premium-Support den schnellsten Warenaustausch. Die längste angegeben Zeitspanne liegt mit zehn Tagen ebenfalls bei Palo Alto Networks. Auch die SLAs unterscheiden sich bei den neun Anbietern stark. Aruba (HPE) Silver Peak bietet Kunden keine SLAs. Cato Networks, Cisco und Fortinet hingegen geben in ihren SLAs ganz konkret eine Verfügbarkeit von 99,999 Prozent für ihre Cloud-Services an.

9

SASE-Supportangebote im Vergleich

	Standard	Premium	Support vor Ort	Antwortzeit	Reklamation/ Warenaustausch	SLA
Cato	Rund um die Uhr	Persönlicher Supporttechniker	Nein	1 bis 2 Stunden	Am nächsten Tag	99,999
Cisco	Rund um die Uhr per Telefon und online	Persönlicher Servicemanager	Über Partner			99,999 (für Umbrella-Services)
Cloudflare	Rund um die Uhr	Premium-Service (White Glove)	Über Partner			100-prozentige Verfügbarkeit
Fortinet	Rund um die Uhr	Advanced SE	Ja		4 Stunden – am nächsten Tag durch einen Kurier	99,999
Aruba (HPE) Silver Peak	Rund um die Uhr	Unterstützung bei der Bereitstellung	Nein	30 Minuten bis 24 Stunden		Keine
Palo Alto Networks	Rund um die Uhr online	Rund um die Uhr per Telefon + Empfehlungen			4 Stunden bis 10 Tage	99,999
Versa	Rund um die Uhr online und per Telefon	Rund um die Uhr	Ja	1 bis 4 Stunden		99,999
VMware	Rund um die Uhr	Ursachenanalyse	Optional	30 Minuten bis *12 Stunden	4 Stunden – NWT**	Keine
Zscaler	Rund um die Uhr	Level-2-Supportmitarbeiter	Nein	15 Minuten bis 48 Stunden		99,999

* Geschäftszeiten

** Am nächsten Werktag

Cato Networks bietet seinen Kunden rund um die Uhr und weltweit Support. Als Premium-Angebot steht auch ein persönlicher Supporttechniker zur Verfügung. Es gibt ein kleines Kundenberatungsteam mit weniger als sieben Mitgliedern, das aber derzeit ausgebaut wird. Das Unternehmen bietet keinen Support vor Ort an, aber Remoteunterstützung bei der Ersteinrichtung. Bei Reklamationen ist ein Austausch am nächsten Tag möglich, es wird jedoch empfohlen, Ersatz-SD-WAN-Appliances vor Ort bereitzuhalten. Im SLA ist die Verfügbarkeit des Cloud-Service mit 99,999 Prozent angegeben.

Cisco bietet für SASE jetzt Beratung zur strategischen Planung und auch die Bereitstellungs- und Supportservices an, die bereits für andere Sicherheits- und Netzwerkprodukte zur Verfügung stehen. Die Angebote umfassen Support rund um die Uhr per Telefon oder online und Unterstützung bei der Konfiguration. Im Premium-Support sind außerdem technischer Support mit einer höheren Priorität und ein persönlicher Servicemanager eingeschlossen. Für die grundlegenden Umbrella-Services ist im SLA eine Verfügbarkeit von 99,999 Prozent angegeben. Weitere Details finden Sie unter https://umbrella/cisco.com/support.

Cloudflare bietet seinen Kunden mit Enterprise-Tarif Support rund um die Uhr, Level-1-Support, einen Kundenberater und einen persönlichen Fachexperten zur Unterstützung bei der Implementierung. Der Premium-Support umfasst Zusatzleistungen (White-Glove-Service). Cloudflare bietet keinen direkten Support vor Ort, aber es können die Dienste bestimmter Managed-Services-Anbieter in Anspruch genommen werden. Das Unternehmen garantiert eine 100-prozentige Verfügbarkeit seines Cloud-Service.

FortiCare-Kunden können FortiSASE nutzen. Aufgrund des großen Vertriebs- und Partnernetzwerks können Kunden Service und Support entweder direkt von Fortinet in Anspruch nehmen oder sich an autorisierte Serviceanbieter und Partner wenden. In den FortiSASE-SLAs ist eine Verfügbarkeit von 99,999 Prozent angegeben. Weitere Details zu FortiCare finden Sie unter https://www.fortinet.com/support/support-services/forticare-support.

Aruba (HPE) Silver Peak bietet Support rund um die Uhr und direkten Kontakt zu Supporttechnikern. Mit einem separaten Silver Peak Assist-Abonnementservice steht Kunden persönliche technische Unterstützung bei der Bereitstellung zur Verfügung. Die Aruba (HPE) Silver Peak-Supportteams arbeiten dazu mit Sicherheitsservicepartnern zusammen. Das Unternehmen hat auch autorisierte und zertifizierte Bereitstellungspartner, die Kunden bei der Planung, der Bereitstellung und der Verwaltung der SD-WAN-Implementierungen unterstützen. Es gibt vier Supportlevel mit verschiedenen Priorisierungsstufen für den Komponentenaustausch: Auf kritische Probleme wird innerhalb von 30 Minuten eine erste Antwort gesendet, bei komplexeren Fällen dauert es eine Stunde. Bei Problemen von normaler Priorität werden Kunden innerhalb von vier Stunden kontaktiert. Allgemeine Fragen und Bitten um Informationen werden innerhalb von 24 Stunden beantwortet.

Prisma Access von Palo Alto Networks umfasst zwei Supportlevel:

- Standard (in Prisma Access enthalten): Kunden erhalten rund um die Uhr Zugriff auf das Supportportal, die Knowledge Base und die gesamte Onlinedokumentation von Palo Alto Networks, kostenlose Onlineschulungsvideos und Zugang zur LIVEcommunity.

- Premium (20 Prozent des Listenpreises): Dieses Level umfasst zusätzlich zum Angebot des Standardpakets Telefonsupport rund um die Uhr, kürzere Antwortzeiten, fortlaufende Unterstützung und Hilfe von Experten beim Onboarding, Kundenberatung sowie Tipps zu Best Practices und zur optimalen Strategie.

Beide Verträge decken zertifizierte Teile und Kontakt zu geschulten Technikern ab. Kunden, die bei Reklamationen einen Vorabaustausch wünschen, stehen im Rahmen des Palo Alto Networks-Supportprogramms 130 Depots weltweit zur Verfügung. Für den Austausch gibt es folgende Optionen:

- Rückgabe und Reparatur: Kunden geben ein fehlerhaftes Gerät zurück und erhalten innerhalb von zehn Werktagen ein Ersatzgerät. Diese Option ist Teil des Standard-Supportvertrags.
- Reklamation mit Geräteaustausch am nächsten Werktag: Das Unternehmen bemüht sich, für fehlerhafte Hardware am nächsten Werktag ein Ersatzgerät zuzustellen. Diese Option ist Teil des Premium-Supportvertrags.
- Reklamation mit 4-Stunden-Premium-Support: Bei diesem optionalen Upgrade wird das Unternehmen alle wirtschaftlich vertretbaren Anstrengungen unternehmen, um dem Kunden innerhalb von vier Stunden nach der Reklamation ein Ersatzgerät zuzustellen. Dieses Angebot ist für Rechenzentrumskunden gedacht, für die eine schnelle Problembehebung geschäftsentscheidend ist. Diese Option ist jedoch nicht in allen Regionen verfügbar.

Versa bietet Standard- und Premium-Supportabonnements. Der Standardsupport umfasst Telefon- und Onlinesupport rund um die Uhr mit einer ersten Antwort innerhalb von vier Stunden sowie Softwareupgrades und -patches. Der Premium-Support ist rund um die Uhr erreichbar und eine erste Antwort geht innerhalb von einer Stunde ein. Optional ist Support vor Ort direkt von Versa erhältlich. Das Unternehmen bietet eine Zweijahresgarantie auf seine Hardwareappliances, aber Kunden können erweiterte Supportoptionen erwerben, zum Beispiel die Rückgabe ans Werk, um den Prozess zu beschleunigen und eine längere Rückgabefrist zu erhalten. Fehlerhafte Hardware wird innerhalb von vier Wochen repariert oder ersetzt. Kunden können auch einen Vorabaustausch am nächsten Werktag wählen, um die Rückgabe ans Werk zu vermeiden. In diesem Fall liefert ein Servicetechniker ein Ersatzgerät an den Kundenstandort und nimmt das defekte Gerät zur Reparatur mit. Zu den weiteren Supportoptionen gehört der Vorabaustausch am gleichen Werktag. Diese Services werden mithilfe eines weltweiten Netzwerks bereitgestellt, das die EU und andere europäische Länder, USA/Kanada, APAC/Japan, Australien, den Nahen Osten und Afrika abdeckt. Im SLA von Versa ist für den Cloud-Service eine Verfügbarkeit von 99,999 Prozent angegeben.

VMware bietet drei Supportpakete für sein SD-WAN: „Basic“, „Production“ und „Premium“. Im Rahmen des Basic-Supportprogramms ist das Supportteam weltweit rund um die Uhr für kritische Probleme erreichbar. Dieser Supportlevel umfasst eine unbegrenzte Anzahl an Supportanfragen, Antworten innerhalb von einer Stunde für kritische Probleme (Schweregrad 1), innerhalb von vier Stunden für dringliche Probleme (Schweregrad 2) und innerhalb von acht Stunden für weniger dringliche Probleme (Schweregrad 3). Außerdem haben Kunden Zugriff auf die Onlinedokumentation und die Knowledge Base. Mit dem Production-Supportpaket werden kritische Probleme (Schweregrad 1) innerhalb von 30 Minuten beantwortet. Der Premium-Support ist zusätzlich weltweit und rund um die Uhr für dringliche Probleme (Schweregrad 2) erreichbar und umfasst eine Ursachenanalyse, Antworten innerhalb von zwei Stunden für dringliche Probleme (Schweregrad 2) und innerhalb von vier Stunden für weniger dringliche Probleme (Schweregrad 3).

Zscaler bietet drei Supportpakete an: Das Standardpaket ist im Service enthalten und es gibt optional ein Premium- und ein Premium Plus-Paket. Alle drei umfassen Support rund um die Uhr per Telefon, Webportal und Administrationsoberfläche, Onlineschulungen, Benutzerleitfäden und Artikel. Der Standardsupport bietet Kontakt zu Level-1-Supportmitarbeitern und einen Eskalationszeitraum für Probleme mit dem Schweregrad 1 zwischen 8 und 17 Uhr (lokale Zeit). Der Premium-Support bietet Kontakt zu Level-2-Supportmitarbeitern und rund um die Uhr die Möglichkeit zur Eskalation von Problemen mit dem Schweregrad 1. Premium Plus umfasst zusätzlich den Kontakt zu einem persönlichen technischen Kundenberater und weitere wöchentliche, monatliche oder vierteljährliche Besprechungen mit dieser Person. Die Antwortzeiten für Tickets, die über das Supportportal von Zscaler eingereicht wurden, variieren je nach Paket und Schweregrad des Problems. Sie reichen von P1 für die dringendsten Fälle bis P4 für Anfragen mit einer niedrigeren Priorität. Die Antwort-SLAs für P1-Probleme liegen bei zwei Stunden für den Standardsupport, 30 Minuten für den Premium- und 15 Minuten für den Premium Plus-Support.

Vermarktung der SASE-Angebote

Cato Networks arbeitet mit diversen Vertriebspartnern zusammen, zum Beispiel Telekommunikationsanbietern und internationalen Distributoren (Master Agents) in den USA sowie MSP (Managed Service Providers), Distributoren und VAR (Value-Added Resellers) in anderen Ländern weltweit. MSP bieten ihre Services in der Cloud-Infrastruktur von Cato an. Momentan werden auch in den USA Partnerschaften mit MSP ausgehandelt. Rabatte für Vertriebspartner reichen von 20 Prozent für Telekommunikationsunternehmen über 30 Prozent für VAR bis 40 Prozent für Distributoren. In bestimmten Fällen werden 15 Prozent Rabatt angeboten.

Cisco bietet seine SASE-Lösung sowohl großen Unternehmen direkt als auch über Vertriebspartner an, einschließlich Distributoren, VAR und Serviceanbietern. Das Angebot ist auf diverse Branchen ausgerichtet, aber das Unternehmen geht davon aus, dass die Nachfrage im Finanz- und Gesundheitswesen aufgrund der strengeren Compliancevorgaben geringer ausfallen wird. Zu den übrigen Branchen gehören Behörden und Bildungseinrichtungen, für die es Pakete zu bestimmten Anwendungsfällen gibt, wie beispielsweise Studententarife.

Cloudflare bietet seine SASE-Lösung sowohl Unternehmenskunden direkt als auch über verschiedene Vertriebspartner an. Serviceanbieter nutzen die Cloudflare-Infrastruktur für die SASE-Services, die in 100 Ländern weltweit verfügbar sind. Cloudfare verkauft seine Produkte in der Regel an Einkäufer aus dem IT- und IT-Sicherheitsbereich, aber in manchen Fällen wird die Kaufentscheidung auch von Netzwerkteams vorangetrieben.

Fortinet arbeitet in der Regel nur mit Vertriebspartnern zusammen und plant, seine neue SASE-Lösung über die üblichen Serviceanbieter, MSSP, Distributoren und VAR zu vertreiben. Das Unternehmen richtet sein Angebot nicht an bestimmte Branchen und verzeichnet Anfragen von unterschiedlichen Stellen. Das größte Interesse zeigen allerdings Technologie- und Fertigungsunternehmen sowie Behörden. Derzeit führt Fortinet einige PoC für sehr große, multinationale Tier-1-Unternehmen in Nordamerika durch. Das Unternehmen plant, zuerst aktiv Verkaufschancen in Nordamerika zu verfolgen und dann in der zweiten Hälfte des nächsten Jahres seine Vertriebsaktivitäten und PoC auf andere Länder auszuweiten.

Aruba (HPE) Silver Peak vertreibt sein Angebot über Distributoren, VAR, Systemintegratoren, Serviceanbieter und Security Technology Alliance-Partner. VAR weltweit erhalten einen Rabatt in Höhe von 33 Prozent. Über diese Partner hat das Unternehmen bisher über 2.000 Bereitstellungen seiner Unity EdgeConnect SD-WAN-Edge-Plattform für Produktionsumgebungen vertrieben. Erfolgt die Bereitstellung über einen Serviceanbieter, können Kunden zwischen Aruba (HPE) Silver Peak On-Premises-Hardwareappliances und einer virtuellen Netzwerkfunktion (VNF) auf der branchenüblichen CPE-Hardware des Serviceanbieters wählen. Die EdgeConnect-VNF kann zusammen mit der Sicherheits-VNF eines Partners auf verschiedenen Hardwareappliances implementiert werden. Der Serviceanbieter verwaltet die Kundenimplementierung mithilfe einer mandantenfähigen Version von Aruba Orchestrator. Die größte Implementierung für Tausende Standorte eines Fortune 50-Einzelhändlers wurde über einen Servicepartner bereitgestellt. Aruba (HPE) Silver Peak ist speziell auf Behörden und Bildungseinrichtungen ausgerichtet und auch seine Partner sind Experten für diese Sektoren. Seit dem Abschluss der Tests für die FIPS-140-2-Validierung im ersten Quartal 2020 sind die Silver Peak-Angebote auch für Bundesbehörden geeignet.

Palo Alto Networks vertreibt seine Prisma Access- und SD-WAN-Produkte über Serviceanbieter, Distributoren und VAR. Für die Bereitstellungen über die Serviceanbieter hostet Palo Alto Networks Prisma Access für Vertriebspartner. Das Unternehmen gab nicht bekannt, welche Rabatte es Vertriebspartnern gewährt, wie viele Prisma Access-Kunden es hat oder wie viele PoC aktiv durchgeführt werden.

Versa vertreibt seinen SASE-Service über ein globales Partnernetzwerk, zu dem unter anderem VAR, Systemintegratoren, Anbieter von Managed Services, Telekommunikationsunternehmen, Wiederverkäufer und Master Agents gehören. Falls erwünscht, verkauft Versa seinen Service auch direkt an Kunden. Serviceanbieter können das SASE-Angebot von Versa weiterverkaufen und/oder als White-Label-Produkt vertreiben. Sie können die SASE-Lösung in ihrer eigenen Cloud hosten und auch die eigenen Netzwerke und PoP nutzen. Außerdem haben sie die Möglichkeit, die On-Premises-Geräte des Kunden und die Cloud-Version als Managed Service zu verwalten. Zu den Serviceanbietern aus dem Partnernetzwerk gehören Comcast, Deutsche Telekom, Lumen, Verizon und NTT Communications. Zu den Master Agents in der Telekommunikationsbranche gehören Avant, Intelisys und Telarus. Versa richtet sein Angebot gezielt auf verschiedene Branchen aus, darunter das Finanz- und Gesundheitswesen, den Einzelhandel, Hightech- und Fertigungsunternehmen, Energieversorger sowie den öffentlichen Sektor, einschließlich Behörden und Bildungseinrichtungen.

VMware vertreibt sein SASE-Angebot sowohl direkt als auch über diverse Vertriebspartner, wie VAR, MSP und Telekommunikationsunternehmen. Lösungen, die über Serviceanbieter verkauft werden, können in On-Premises-Umgebungen implementiert, von VMware gehostet oder auch von den Serviceanbietern selbst gehostet werden. VMware hat sein Angebot nicht auf bestimmte Branchen ausgerichtet.

Zscaler vertreibt seine SASE-Services sowohl über eigene regionale Vertriebsteams direkt an Unternehmen als auch über Vertriebspartner. Servicepartner verkaufen das Produkt häufig unter ihrer eigenen Marke, aber diese Services werden von Zscaler gehostet. Obwohl das Unternehmen seine Lösung nicht auf bestimmte Branchen ausgerichtet hat, ist sie vorrangig im Technologiesektor, Gesundheits- und Finanzwesen, in der Fertigung und in Behörden vertreten.

Kurzer Überblick über die einzelnen SASE-Anbieter

Cato Networks

Das Start-up Cato Networks wurde 2016 mit 332 Millionen US-Dollar Risikokapitalrücklagen gegründet und vermarktet seine Cato Cloud als weltweit erste SASE-Plattform. Das grundlegende SASE-Paket umfasst einen cloudbasierten Service, der SD-WAN, NGFW und SWG sowie die eigene Backbone-Netzwerksoftware beinhaltet und über die Netzwerke verschiedener Anbieter bereitgestellt wird. Zu den optionalen Premium-Add-ons zählen derzeit IPS, erweiterte Funktionen zur Abwehr von Bedrohungen, weltweite Konnektivität und Malwareschutz. Letzterer ist eine OEM-Funktion, die von Cato Networks integriert, verwaltet, bereitgestellt und skaliert wird, um eine nahtlose Benutzererfahrung zu ermöglichen. Für die Zukunft sind als optionale Angebote unter anderem auch DLP, NAC und RBI geplant.

SASE-Funktionen Cato Networks

Unverzichtbar	Empfehlenswert	Optional
◉ SD-WAN	○ WAAP	○ Schutz von WLAN-Hotspots
◉ SWG	Geplant ◉ RBI	○ Netzwerkverschleierung
◉ CASB	○ Rekursives DNS	◉ Unterstützung älterer VPNs
◉ ZTNA	Partner ◉ Netzwerk-Sandboxing	○ Schutz von Edge-Computing
◉ FWaaS	○ API-Zugriff auf SaaS	○ UEBA
◉ Schutz personenbezogener Daten/Malwareschutz	◉ Unterstützung verwalteter/ nicht verwalteter Geräte	
◉ Max. Datenübertragung/Edge		
◉ Max. Datenübertragung/Cloud		

Cato Cloud basiert auf einem einzigen cloudnativen Softwarestack, der SD-WAN- und Sicherheitsfunktionen kombiniert. Die Software ist derzeit an 60 Points of Presence weltweit implementiert und bietet eine zentrale Managementkonsole. Cato erweitert dieses Netzwerk jedes Quartal um drei bis vier neue PoP. Neben den Primärmärkten, in denen sich seine PoP befinden, ist Cato auch in Tertiärmärkte wie Casablanca (Marokko) und Santiago (Chile) eingestiegen. Das Unternehmen kann Multi-Gigabit-Datenverkehr mit maximalen Übertragungsraten verarbeiten und bis zu 2 Gbit/s zur Überprüfung vollständig entschlüsseln. Der gesamte Kundendatenverkehr wird auf einem Cloud-Proxy auf Zugriffsberechtigungen und Bedrohungen überprüft. Die Points of Presence sind symmetrisch, vollständig redundant und mit zwei oder drei Tier-1-Anbietern verknüpft. Die PoP verarbeiten den Internetdatenverkehr und beschleunigen den WAN-Datenverkehr. Sie ermöglichen die Cloud-Optimierung, TCP-Beschleunigung, globale Routenoptimierung, dynamische Anbieterwahl und Ermittlung des besten Pfads für jedes Paket. Als Sicherheitsmaßnahme verwendet die Plattform eine Single-Pass-Architektur mit drei unterschiedlichen Sicherheitsengines, die den Datenverkehr auf Malware überprüfen. Die Plattform ist bereits seit Beginn als mandantenfähige Architektur konzipiert. Die Software wird auf physischen Servern in Colocation-Rechenzentren von Cato Networks ausgeführt. Die meisten verarbeitungsintensiven Funktionen werden in der Cloud ausgeführt, aber Cato Networks nutzt auch eine Thin-Edge-Architektur, für die SD-WAN-Appliances in den Zweigstellen implementiert werden müssen. Außerdem bietet das Unternehmen clientbasierten und clientlosen Zugriff für

Mobilgeräte, wie Desktopcomputer, Laptops und Mobiltelefone. Der clientlose Zugriff erfolgt über interne Webanwendungen, die in einem vom Benutzer konfigurierten Portal bereitgestellt werden.

Die Kunden von Cato Networks haben zwischen 5 und 2.000 Standorte und zwischen 500 und 45.000 Mitarbeiter. Der größte Kunde versorgt mit dem Service 40.000 Mitarbeiter, von denen 20.000 per Fernzugriff arbeiten. Aktuell hat Cato Networks über 750 Kunden weltweit. Zu den typischen Einsatzbereichen gehören die Ablösung von MPLS, von On-Premises-Edge-Firewalls durch cloudbasierte Netzwerksicherheitsfunktionen und von VPNs durch cloudbasierte Sicherheitsfunktionen. Das Alleinstellungsmerkmal von Cato Networks ist der integrierte Softwarestack mit einer zentralen Managementkonsole und nahtlosen Benutzererfahrung. Als direkte Konkurrenzangebote betrachtet Cato Prisma von Palo Alto Networks, Meraki und Umbrella von Cisco, VMware- und Fortinet-Lösungen sowie ZIA und ZPA von Zscaler. Weitere Mitbewerber sind Telekommunikationsanbieter wie British Telecom und CenturyLink.

Cisco Systems SASE

Cisco erklärt, schon vor Jahren mit der Zusammenführung von Netzwerk- und Sicherheitsservices begonnen zu haben, um Benutzern sichere Verbindungen zu Anwendungen bereitzustellen – lange bevor Gartner den Begriff „Secure Access Service Edge" einführte. Cisco positioniert sich als einziger Anbieter, der sowohl ein eigenes SD-WAN als auch eigene Sicherheitsfunktionen entwickelt und bereitstellt. Tatsächlich hat das Unternehmen die proprietären Technologien für sein SASE-Angebot aber durch verschiedene Übernahmen erworben: Meraki and Viptela für SD-WAN und OpenDNS (unter dem neuen Markennamen Umbrella), ScanSafe (Cloud-SWG), CloudLock (CASB) und weitere Sicherheitslösungen. Nur der Threat-Intelligence-Service Talos und das Management- und Orchestrierungs-Framework SecureX wurden von Cisco selbst entwickelt.

Inzwischen bietet das Unternehmen drei Pakete mit SD-WAN, Routing und Sicherheitsservices für drei unterschiedliche Niveaus an: Cisco DNA Essentials, Cisco DNA Advantage und Cisco DNA Premier. DNA Essentials umfasst ein WAN-Overlay, die zentrale Managementkonsole vManage, Unterstützung mehrerer Topologien, Anwendungsrichtlinien, NGFW, Snort-IDS/IPS mit Talos-Threat-Intelligence-Signaturen, DNS-Monitoring und Umbrella-Konnektoren, grundlegende Pfadoptimierung und die Unterstützung von OSPF- und BGP-Routingprotokollen. DNS Advantage bietet zusätzliche unbegrenzte Segmentierung, vAnalytics, Cloud-Onramping für IaaS, URL Filtering, den Malwareschutz Cisco AMP und die Umbrella-Anwendungserkennung. Das exklusivste Paket, DNA Premier, stellt die SASE-Lösung von Cisco dar. Es setzt auf Umbrella SIG Essentials auf und umfasst daher DNS-Sicherheit, SWG, CASB, FWaaS, interaktive Threat Intelligence, SecureX (XDR), den Malwareschutz Secure Endpoint, Secure Malware Analytics-Sandboxing und AnyConnect-Remote-Clients.

SASE-Funktionen
Cisco Systems

Unverzichtbar	Empfehlenswert	Optional
● SD-WAN	○ WAAP	● Schutz von WLAN-Hotspots
● SWG	Geplant ● RBI	● Netzwerkverschleierung
● CASB	● Rekursives DNS	● Unterstützung älterer VPNs
● ZTNA	● Netzwerk-Sandboxing	○ Schutz von Edge-Computing
● FWaaS	● API-Zugriff auf SaaS	● UEBA
● Schutz personenbezogener Daten/Malwareschutz	● Unterstützung verwalteter/nicht verwalteter Geräte	
? Max. Datenübertragung/Edge		
? Max. Datenübertragung/Cloud		

Die SASE-Architektur von Cisco wurde als cloudnativer Service mit Containern und Microservices-Technologie entwickelt. Dadurch sollte die Anwenderfreundlichkeit der Meraki-Produkte auch für die kombinierten Netzwerk- und Sicherheitsservices übernommen werden, die auf den weltweit verteilten Netzwerk-Cloud-Edge-Gateways von Cisco aufsetzen. Die Gateways verfügen über direkte Peering-Verbindungen zu diversen IaaS- und SaaS-Anbietern. Momentan betreibt Cisco über 30 regionale Rechenzentren mit direkten Peering-Verbindungen zu mehr als 1.000 ISP-, CDN- und Saas-Anbietern. Das Unternehmen plant, im nächsten Jahr zehn weitere regionale Rechenzentren hinzuzufügen. Die Umbrella-Richtlinienengine von Cisco ist in die SD-WAN-Funktionen und SecureX integriert, um die automatische Ergreifung von Maßnahmen für die eigenen Netzwerk- und Sicherheitsprodukte sowie für Lösungen von Drittanbietern zu ermöglichen. Für die Integration in vorhandene On-Premises-Firewalls erweitert Cisco seinen Defense Orchestrator, damit Richtlinien von diesen Firewalls auch für den cloudbasierten Service übernommen werden können.

Cisco hat die Implementierung seiner neuen SASE-Lösung vereinfacht, da sie als eine SKU erworben und über automatisierte Tunnel von Cisco SD-WAN zu Umbrella bereitgestellt werden kann. Das SASE-Angebot von Cisco zeichnet sich auch durch das große Funktionsangebot, die effizienten Sicherheitsfunktionen, die umfassende Abdeckung von Netzwerken, Endpunkten und der Cloud sowie durch die langjährige Erfahrung in der Entwicklung und Verwaltung von leistungsfähigen globalen Netzwerken mit hoher Kapazität aus, wie beispielsweise das globale Umbrella-Netzwerk. Die Effektivität der Sicherheitsprodukte und -funktionen von Cisco ist zum Großteil auf seinen Threat-Intelligence-Service Talos zurückzuführen, der über das weltweit größte kommerzielle Threat-Intelligence-Team verfügt. Cisco gibt außerdem an, mit zwei SD-WAN-Angeboten für Unternehmen der weltweit größte SD-WAN-Anbieter zu sein.

Cloudflare One

Cloudflare for Teams ist das neue SASE-Angebot von Cloudflare, das von dem globalen Netzwerk des Unternehmens mit 200 Städten, 100 Ländern und einer Gesamtkapazität von 42 Tbit/s profitiert. Die zugrunde liegende Plattform Cloudflare One setzt auf der großen Netzwerkinfrastruktur des Unternehmens auf und nutzt das Portfolio an Webanwendungen, Zugriffs- und Zero-Trust-Services und Netzwerksicherheitsfunktionen. Es umfasst Netzwerk-Interconnects, IP-Transitverkehr, einen Roaming-Agenten, intelligentes Routing, Beschleunigung des Datenverkehrs, ein Secure Web Gateway, Zero-Trust-Zugriff, Schutz vor DDoS und die Filterung für eingehenden Datenverkehr. Cloudflare for Teams soll auf allen Geräten und an allen Standorten sicheren, schnellen und nahtlosen Zugriff auf alle Anwendungen und das Internet bereitstellen.

Die erste Version von Cloudflare One bietet SWG, ZTNA, Browserisolierung, rekursives DNS mit Unterstützung für verwaltete und nicht verwaltete Geräte, Schutz für WLAN-Hotspots, CASB und Schutz für Edge-Computing. Cloudflare One wird auch im Edge-Netzwerk von Cloudflare ausgeführt und bietet dort maximale Übertragungsraten und Schutz für Edge-Computing. Die Plattform umfasst zudem einen Identitäts-Proxy, der mit mindestens acht Identitätsanbietern kompatibel ist, ein zentrales Dashboard, die einfache Integration in gängige SIEM-Lösungen sowie die Unterstützung von Terraform für das Management und von Integrationen in Azure AD und Tanium für stärkere Gerätesicherheit. Weitere Partner für die Gerätesicherheit sind CrowdStrike, Carbon Black und SentinelOne. In naher Zukunft sollen außerdem ein SD-WAN, verbesserte FWaaS, erweiterte Netzwerkanalysen sowie DLP- und IDS-Funktionen hinzugefügt werden. Cloudflare bietet noch keine kombinierten SKU oder Pakete für seine SASE-Lösung an, aber das Unternehmen gibt an, dass Kunden dank des cloudbasierten, dashboardgestützten Bereitstellungsmodells ganz einfach mehrere SASE-Services gleichzeitig verwalten können. Alle SASE-Services sind integriert und reduzieren daher den Aufwand für die Kunden.

SASE-Funktionen Cloudflare

Unverzichtbar	Empfehlenswert	Optional
Geplant: SD-WAN	WAAP	Schutz von WLAN-Hotspots
SWG	RBI	Netzwerkverschleierung
CASB	Rekursives DNS	Unterstützung älterer VPNs
ZTNA	Geplant: Netzwerk-Sandboxing	Schutz von Edge-Computing
Geplant: FWaaS	API-Zugriff auf SaaS	Geplant: UEBA
Geplant: Schutz personenbezogener Daten/Malwareschutz	Unterstützung verwalteter/nicht verwalteter Geräte	
Max. Datenübertragung/Edge		
Max. Datenübertragung/Cloud		

Cloudflare One nutzt das globale Unternehmensnetzwerk, das Endbenutzer über GRE-Tunnel, Netzwerk-Interconnects oder einen Client für Mobilgeräte verbindet, der einen Tunnel zum nächstgelegenen Rechenzentrum von Cloudflare herstellt. Sicherheitsfunktionen und Datenfilter werden in einer Single-Pass-Architektur ausgeführt. Das SASE-Angebot von Cloudflare zeichnet sich durch das globale leistungsfähige Netzwerk des Unternehmens, die Verfügbarkeit aller Funktionen in den 200 Rechenzentren, die Single-Pass-Architektur für Überprüfungen und die Richtliniendurchsetzung sowie die einfache Bereitstellung und Benutzerfreundlichkeit aus. Als direkte Konkurrenten betrachtet Cloudflare Cisco, Netskope, Palo Alto Networks und Zscaler.

Fortinet SASE

Fortinet hat erst kürzlich – nach der Übernahme von OPAQ Networks im Juli 2020 – seine cloudbasierte SASE-Lösung auf den Markt gebracht. Durch die Kombination der Fortinet- und OPAQ-Technologien ist eine zentrale Managementebene entstanden, über die sich Sicherheitsmaßnahmen und Richtlinien für externe Benutzer verwalten lassen. Die erste Version wurde Ende 2020 veröffentlicht und umfasst SD-WAN, SWG, rekursives DNS, IPS, DLP, Sandboxing, FWaaS, Funktionen zur Erkennung von Malware und sensiblen Daten sowie maximale Übertragungsraten am Edge und in der Cloud. Fortinet prüft und überarbeitet diese erste Version, bei der der Schwerpunkt auf einem sicheren Internetzugang lag, um sicherzustellen, dass sie eine angenehme Benutzererfahrung und nahtlose Integration der OPAQ- und Fortinet-Managementtechnologien bietet. Für das zweite Quartal 2021 sind weitere Integrationen geplant, zum Beispiel von CASB-Funktionen. Außerdem sollen zum Ende desselben Quartals ZTNA-Funktionen in die bestehende FortiGate-Infrastruktur integriert werden. In der Entwicklungsphase befinden sich derzeit unter anderem die Browserisolierung, API-Schutz und vermutlich UEBA-Funktionen. Optional stehen für die SASE-Lösung von Fortinet unter anderem Netzwerk-Sandboxing, Unterstützung für verwaltete und nicht verwaltete Geräte, Schutz von WLAN-Hotspots, Netzwerkverschleierung, Schutz von Edge-Computing und der Einsatz älterer VPNs zur Verfügung.

SASE-Funktionen

Unverzichtbar	Empfehlenswert	Optional
SD-WAN	Nur WAF: WAAP	Schutz von WLAN-Hotspots
SWG	RBI	Netzwerkverschleierung
Geplant: CASB	Rekursives DNS	Unterstützung älterer VPNs
Geplant: ZTNA	Netzwerk-Sandboxing	Schutz von Edge-Computing
FWaaS	API-Zugriff auf SaaS	Add-on: UEBA
Schutz personenbezogener Daten/Malwareschutz	Unterstützung verwalteter/ nicht verwalteter Geräte	
Max. Datenübertragung/ Edge		
Max. Datenübertragung/ Cloud		

Die FortiSASE-Architektur wurde durch die Übernahme von OPAQ Networks gewonnen und speziell als cloudbasierter, mandantenfähiger Service entwickelt, der in das sichere Overlay-Netzwerk von Fortinet integriert wird. Außerdem macht Fortinet gute Fortschritte bei der Bereitstellung einer Richtlinienengine für Netzwerk- und Sicherheitsservices, die derzeit SD-WAN und integrierte Funktionen für FWaaS, IPS, DNS, DLP, SWG und ZTNA unterstützt. Weitere Netzwerkfunktionen für Thin-Edge-Netzwerk-Benutzer sind geplant und werden von der Richtlinienengine unterstützt werden, die mit der neuen Version von FortiSASE im zweiten Quartal 2021 veröffentlicht werden soll. Es ist nicht bekannt, über wie viele Points of Presence Fortinet verfügt, aber 2021 werden vermutlich etwa 30 überwiegend in Nordamerika zur Verfügung stehen. Fortinet ist auf die Peering-Verbindungen von Partnern angewiesen, um die notwendige Konnektivität über deren private Backbonenetzwerke anzubieten, und wird bald vermutlich 30 Partnerbeziehungen abgeschlossen haben. Das Unternehmen vertraut darauf, dass sich damit die Lücke schließen lässt. Fortinet ist sich sicher, dass die beste Architektur durch die Härtung des WAN-Edge und dessen Ausweitung bis zum Cloud-Edge entsteht und dass reine Cloud-Edge-Architekturen langfristig auf dem Markt nicht bestehen werden.

Als direkte Konkurrenten betrachtet Fortinet Cisco Umbrella, Netskope, Cato Networks, Zscaler und Prisma Access von Palo Alto Networks. Um sich davon abzuheben, plant Fortinet, Skalierbarkeit außerhalb des WAN-Edge anzubieten, ohne eine zu hohe Leistung und Latenz zu versprechen. Fortinet stuft Zscaler als Marktführer ein, aber die Lösung bietet keine umfassenden Sicherheitsfunktionen und -services.

Aruba (HPE) Silver Peak

Das Kernstück der SASE-Lösung von Aruba (HPE) ist das Aruba EdgeConnect SD-WAN-Produktportfolio, das im September 2020 übernommen wurde. Die Aruba EdgeConnect WAN-Edge-Plattform umfasst SD-WAN, Routing, WAN-Optimierung und eine zonenbasierte Stateful-Inspection-Firewall mit erweiterten Segmentierungsfunktionen, Anwendungstransparenz und Kontrollelementen. Weitere Sicherheitsfunktionen werden von Partnern bereitgestellt, zum Beispiel Check Point, Forcepoint, McAfee, Netskope, Palo Alto Networks (Prisma), Symantec und Zscaler. Silver Peak verfügt über eine erweiterte automatische Orchestrierung mit Lösungen von Check Point, Zscaler und Netskope. Durch die Integrationen können primäre und sekundäre IPsec-VPN-Tunnel zu den jeweiligen cloudbasierten Sicherheitsservices/-Stacks der Partner im nächstgelegenen PoP und zur nächsten Zweigstelle im SD-WAN erstellt werden. Unternehmen können in der Unity Orchestrator-Benutzeroberfläche per Drag-and-Drop auch eigene Sicherheitsrichtlinien erstellen. Für Silver Peak werden keine speziellen Pakete oder Bundles angeboten.

SASE-Funktionen
Aruba (HPE) Silver Peak

Unverzichtbar	Empfehlenswert	Optional
● SD-WAN	○ WAAP	○ Schutz von WLAN-Hotspots
Partner ● SWG	Partner ● RBI	○ Netzwerkverschleierung
Partner ● CASB	○ Rekursives DNS	○ Unterstützung älterer VPNs
Partner ● ZTNA	Partner ● Netzwerk-Sandboxing	○ Schutz von Edge-Computing
● FWaaS	○ API-Zugriff auf SaaS	○ UEBA
Partner ● Schutz personenbezogener Daten/Malwareschutz	Partner ● Unterstützung verwalteter/nicht verwalteter Geräte	
○ Max. Datenübertragung/Edge		
Partner ● Max. Datenübertragung/Cloud		

Die zonenbasierte Stateful-Inspection-Firewall von Aruba (HPE) Silver Peak wird auf einer physischen oder virtuellen Appliance in den Zweigstellen als Teil der Aruba EdgeConnect-Komponente ausgeführt. Die virtuelle Aruba EdgeConnect-Appliance kann in den Public-Cloud-Instanzen von AWS, Azure, Google oder Oracle implementiert werden. Wenn ein Kunde Firewalls oder andere Sicherheitsservices von Partnern in die Servicekette einbinden möchte, kann EdgeConnect die Abläufe mithilfe der Aruba Orchestrator-Richtlinienengine automatisieren. Netzwerkmanager können spezifische Sicherheitsrichtlinien für Anwendungen oder Anwendungsklassen konfigurieren. Außerdem haben sie die Möglichkeit, in derselben Benutzeroberfläche die automatische Erstellung von primären und sekundären IPsec-Tunneln von jeder Zweigstelle zum nächstgelegenen Cloud-Sicherheits-PoP einzurichten. Für Aruba (HPE) Silver Peak ist auch optional WAN-Optimierung verfügbar, die in inkrementellen Bandbreiten lizenziert wird. Das Unternehmen plant, in Kürze weitere Sicherheitsfunktionen zu integrieren, zum Beispiel IDS/IPS und ClearPass, die agentenlose, rollenbasierte Richtlinienengine für den Netzwerkzugriff von Aruba. Dadurch soll ein umfassender Überblick über die Identitäten und Richtlinien vom Edge bis zur Cloud möglich werden.

Der Aruba Orchestrator wird in On-Premises-Umgebungen, in der Cloud oder als Service von Aruba (HPE) Silver Peak bei den Kunden implementiert. Dadurch können Netzwerkmanager virtuelle Overlays für Anwendungsklassen einrichten und spezifische QoS- und Sicherheitsrichtlinien für das verteilte Unternehmen definieren, konfigurieren und durchsetzen. Das Unternehmen plant zudem, seine Automatisierungsfunktionen für die dynamische Richtlinienanwendungen und die automatische Integration in Partnerlösungen auszubauen.

Zusätzlich zu den Partnerschaften mit führenden Sicherheitsanbietern verfügt Aruba (HPE) Silver Peak auch über automatische Sicherheitsintegrationen für Microsoft für Office 365, Azure und Azure Virtual WAN sowie für AWS über den Transit Gateway Network Manager.

Aruba (HPE) Silver Peak ist ein anerkannter Marktführer im Segment für WAN-Edge-Infrastrukturen. Als SD-WAN-Anbieter zeichnet sich das Unternehmen vor allem durch die Priorisierung geschäftskritischer Anwendungen, eine zuverlässige Anwendungsleistung durch die kontinuierliche Anpassung an die WAN-Bedingungen mithilfe von KI sowie eine einheitliche Plattform aus. Sein SASE-Angebot ist das einzige, bei dem Kunden die besten Sicherheitstechnologien für die Integration in das SD-WAN wählen und dann über die Aruba Orchestrator-Richtlinienengine verwalten können. Auf diese Weise lässt sich eine Anbieterbindung vermeiden. Als direkte Konkurrenten betrachtet das Unternehmen VMware/VeloCloud, Cisco (insbesondere Viptela) und Meraki und geht davon aus, dass es in Zukunft zunehmend mit Fortinet und seit der Übernahme von CloudGenix auch mit Palo Alto Networks konkurrieren wird.

Palo Alto Networks SASE

Palo Alto Networks ist Anfang 2019 mit seiner cloudbasierten Sicherheitssuite Prisma in den SASE-Markt eingestiegen. Dazu gehörte auch Prisma Access Edge-SD-WAN für einen sicheren Zugang in Zweigstellen. Zur Stärkung seiner SD-WAN-Funktionen übernahm das Unternehmen im April 2020 den SD-WAN-Anbieter CloudGenix. Palo Alto Networks hat CloudGenix SD-WAN in die Prisma-Suite integriert und zudem maschinelles Lernen für die Bandbreitenverwaltung und die Automatisierung zur schnelleren Problemhebung hinzugefügt. Außerdem führte das Unternehmen neue Appliances sowohl für kleine Zweigstellen als auch für große Niederlassungen, Campusnetzwerke und Rechenzentren ein. Inzwischen bietet Palo Alto Networks vier verschiedene SASE-Pakete mit folgenden Funktionen an:

- Prisma Access Business umfasst URL Filtering und DNS Security-Services.
- Prisma Access Business Premium beinhaltet URL Filtering, DNS Security-Services, Threat Prevention und WildFire-Sandboxing.
- Prisma Access Enterprise bietet URL Filtering, DNS Security-Services, Threat Prevention, Wildfire und privaten Zugriff auf Anwendungen über Serviceverbindungen (zwei mit lokaler SKU, fünf mit weltweiter SKU). Optional sind für dieses Paket weitere Serviceverbindungen, DLP und Interconnects (zwischen Benutzern und Zweigstellen sowie zwischen Zweigstellen) erhältlich.
- Prisma Access ZTNA umfasst URL Filtering, Threat Prevention und privaten Zugriff auf Anwendungen über Serviceverbindungen (zwei mit lokaler SKU, fünf mit weltweiter SKU). Zu den optionalen Add-ons gehören weitere Serviceverbindungen und DLP.

SASE-Funktionen
Palo Alto Networks

Unverzichtbar	Empfehlenswert	Optional
◉ SD-WAN	○ WAAP	◉ Schutz von WLAN-Hotspots
◉ SWG	○ RBI	◉ Netzwerkverschleierung
◉ CASB	◉ Rekursives DNS	◉ Unterstützung älterer VPNs
◉ ZTNA	◉ Netzwerk-Sandboxing	◉ Schutz von Edge-Computing
◉ FWaaS	◉ API-Zugriff auf SaaS	◉ UEBA
◉ Schutz personenbezogener Daten/Malwareschutz	◉ Unterstützung verwalteter/ nicht verwalteter Geräte	
◉ Max. Datenübertragung/ Edge		
◉ Max. Datenübertragung/ Cloud		

Prisma Access wird von Palo Alto Networks verwaltet und wurde ursprünglich als cloudunabhängiger Service entwickelt. Inzwischen ist er allerdings überwiegend auf AWS, Google Cloud und mehrere Points of Presence angewiesen, die auch Computing- und nicht nur reine Gatewayfunktionen bereitstellen. Palo Alto Networks verfügt über 100 PoPs in 76 Ländern und plant, in den nächsten 12 bis 24 Monaten weitere fünf bis zehn hinzuzufügen. Die Orchestrierungsfunktion von Prisma Access ist mandantenfähig und nutzt cloudnative Technologien wie Container, serverlose Anwendungen und Microservices. Für jeden Kunden werden spezielle softwarebasierte SPN (Security Processing Nodes) in der Cloud-Infrastruktur bereitgestellt, die auf der Next-Generation Firewall-Technologie des Unternehmens basieren. Dadurch werden zwar die Trennung des Datenverkehrs und eine angemessene Leistung sichergestellt, allerdings steigen auch die Betriebskosten für Prisma Access. Die Single-Pass-Richtlinienengine von Palo Alto Networks führt jeweils mehrere Prüfungen durch und ermöglicht dadurch eine äußerst effiziente Richtliniendurchsetzung unter Berücksichtigung von Kontextinformationen zu Benutzern, Anwendungen und anderen Inhalten. Obwohl das CloudGenix SD-WAN ursprünglich integriert wurde, wird es weiterhin separat von den SASE-Paketen vertrieben.

Das SASE-Angebot von Palo Alto Networks zeichnet sich durch seine umfassenden und effektiven Sicherheitsfunktionen aus, die auf seiner branchenführenden NGFW basieren, und durch die Konsolidierung von mindestens zehn individuellen Punktlösungen, die es unterstützt. Das Unternehmen sagt aus, die besten Sicherheits- und jetzt auch SD-WAN-Funktionen anzubieten, die von einer Standard-Richtlinienengine und einem Datenmodell zur Verbesserung des Sicherheits- und Netzwerkstacks unterstützt werden. NGFW-Bestandskunden ermöglicht Palo Alto Networks die zentrale Verwaltung der NGFW- und Prisma Access-Produkte, um den Betrieb zu vereinfachen. Das Unternehmen ist davon überzeugt, dass das Netzwerk aus Google Cloud-Rechenzentren, die über ein spezielles Glasfasernetz verbunden sind, und seine eigenen Inline-Sicherheitsfunktionen mit niedriger Latenz eine optimale Anwendungsleistung für externe Benutzer erzielen und untermauert dies mit Latenz-SLAs von weniger als 10 ms. Die größte Konkurrenz für Prisma Access ist vermutlich die Lösung von Zscaler. Setzt sich Prisma Access gegen diesen Mitbewerber durch, ist dies meist auf seine zuverlässigeren Sicherheitsfunktionen, die dynamische Skalierbarkeit und für NGFW-Bestandskunden zudem die einfache Verwaltung zurückzuführen.

Versa Networks

Versa ist einer der letzten reinen SD-WAN-Anbieter (oder sogar der letzte), der nach einer Reihe von Übernahmen im Jahr 2020 noch unabhängig ist. Versa Networks ist ein Privatunternehmen mit 500 Mitarbeitern und einer Risikokapitalrücklage in Höhe von 196 Millionen US-Dollar. Es wurde vor acht Jahren gegründet und hat dank seiner über 1.000 Enterprise-Kunden und Hundertausenden von Standorten 2020 den Break-even-Point erreicht.

Versa bietet insgesamt sechs verschiedene Pakete an. Die Grundfunktionen sind in allen Paketen enthalten: Netzwerk, Routing, SD-WAN und Mandantenfähigkeit. Das SD-WAN bietet QoS-Maßnahmen, richtlinienbasierte Schadensbehebung zur Verbesserung der Leistung bestimmter Anwendungen, Segmentierung und NGFW. In seinem SASE-Service kombiniert Versa Routing, SD-WAN, dynamische Pfadauswahl, Steuerung des Datenverkehrs und QoS, Anwendungstransparenz und Priorisierung sowie integrierte NGFW, NG-IPS und URL Filtering. SWG und andere erweiterte Sicherheitsservices sind zudem separat erhältlich. Versa unterstützt Homeoffice-Arbeitsplätze mit zwei unterschiedlichen Formfaktoren: einer kleinen Home-Appliance oder Versa Secure Access, einer cloudbasierten Lösung, die auf einem Client mit iOS, Windows und Linux ausgeführt werden kann. Das Premium-SASE-Bundle umfasst nahezu alle unverzichtbaren Sicherheitsfunktionen, neuerdings auch CASB und Browserisolierung. Die verschiedenen Bundles können in Unternehmen nahezu aller Größen, diversen Zweigstellenarten und für beliebig viele Remote-Benutzer verwendet werden.

Versa kann integrierte SASE-Services in On-Premises-Umgebungen, in der Cloud oder in einem Hybridmodell mit demselben Betriebssystem in einem einzigen Softwarestack, dem sogenannten Versa Operating System (VOS), bereitstellen. VOS wird nicht nur als von Versa gehosteter Service angeboten, sondern kann auch in einer privaten Cloud gehostet und dann vom Kunden über sein privates Versa Cloud Gateway betrieben und verwaltet werden. Auch ein Hybridmodell ist möglich, wenn der Kunde an bestimmten Standorten, beispielsweise großen Zweigstellen, eine hohe Leistung benötigt. In diesem Fall werden in der Regel 80 Prozent der Funktionen unternehmensintern und 20 Prozent in der Cloud ausgeführt. Der Cloud-Service von Versa wird über die Versa Cloud Gateways an 90 unterschiedlichen Points of Presence weltweit bereitgestellt. In den nächsten 12 bis 24 Monaten sollen noch zehn weitere PoP hinzugefügt werden. Die PoP befinden sich in Colocation-, öffentlichen und privaten Rechenzentren sowie in Public-Cloud-Umgebungen von AWS, Azure und Google Cloud.

Die SASE-Funktionen von Versa basieren auf der VOS-S3P-Architektur (Single Pass Parallel Processing), in der SD-WAN mit vollem Funktionsumfang, erweiterte Routingfunktionen, Mandantenfähigkeit und Analysen in einem Softwareimage bereitgestellt werden. VOS reduziert die Latenz, verbessert die Leistung und verringert die Zahl der Schwachstellen, die bei der Ausführung mehrerer Softwarestacks, Serviceketten oder Appliances auftreten können. Mit der Managementkonsole Versa Director lassen sich die Erstellung, Automatisierung und Bereitstellung von SASE-Services vereinfachen. Sie kann unternehmensintern oder in der Cloud implementiert werden. Die Orchestrierungsplattform Versa Concerto wurde Mitte 2020 zu Versa Director hinzufügt, um die automatische VOS-Bereitstellung im großen Maßstab zu ermöglichen. Die Plattform automatisiert die Erstellung gängiger Netzwerktopologien und bietet Selbstreparaturfunktionen für Benutzer, Geräte und Zweigstellen sowie optionale Weiterleitungen zu SWG-Drittanbietern.

Angebote und Paketoptionen auf dem neuen SASE-Markt

SASE-Funktionen Versa Networks

Unverzichtbar	Empfehlenswert	Optional
SD-WAN	WAAP	Schutz von WLAN-Hotspots
SWG	RBI	Netzwerkverschleierung
CASB	Rekursives DNS	Unterstützung älterer VPNs
ZTNA	Netzwerk-Sandboxing	Schutz von Edge-Computing
FWaaS	API-Zugriff auf SaaS	UEBA
Schutz personenbezogener Daten/Malwareschutz	Unterstützung verwalteter/ nicht verwalteter Geräte	
Max. Datenübertragung/ Edge		
Max. Datenübertragung/ Cloud		

Laut Versa zeichnet sich sein SASE-Angebot durch drei Punkte aus: Erstens: Es bietet in allen Umgebungen die gleichen Sicherheitsservices, Netzwerkfunktionen und Analyserichtlinien – in der Cloud, in On-Premises-Umgebungen oder in einem Hybridmodell, je nach Anforderungen der Kundenstandorte. Manche Konkurrenten bieten hingegen nur bestimmte SASE-Services in der Cloud an oder gar keine SASE-Services in On-Premises-Umgebungen. Zweitens: VOS bietet mit seiner „Single Pass Parallel Processing"-Architektur einzigartige Vorteile. Dazu gehören eine niedrigere Latenz, bessere Leistung, geringere Risiken und umfassende SASE-Services in einem einzigen Softwareimage. Durch den letzten Punkt entfällt die Notwendigkeit von Serviceketten, Verknüpfungen oder virtuellen Interconnects zwischen verschiedenen SASE-Services. Drittens: Versa gibt an, als einziger SASE-Anbieter seinen Kunden und Partnern die Erstellung eigener privater Services zu ermöglichen, entweder in On-Premises- oder in Private-Cloud-Umgebungen. Auf diese Weise haben sie eine größere Kontrolle als bei anderen SASE-Anbietern. Der größte direkte Konkurrent ist Cisco/Viptela.

VMware SASE

Bei seinem neuen SASE-Angebot hebt VMware insbesondere das marktführende SD-WAN hervor, das es Ende 2017 mit der Übernahme von VeloCloud für 449 Millionen US-Dollar erworben hat. Das Unternehmen stellt auch eine ZTNA-Komponente über VMware Secure Access bereit, das derzeit ein Add-on für Workspace One, seine Plattform für digitale Arbeitsplätze, ist. Sowohl SD-WAN als auch ZTNA sind bewährte Komponenten, die von mehr als 12.000 SD-WAN-Kunden installiert wurden. SD-WAN unterstützt auch die Erkennung von Malware und sensiblen Daten, maximale Übertragungsraten am Edge und in der Cloud, Netzwerkverschleierung und ältere VPNs.

Das Unternehmen arbeitet bereits an weiteren Sicherheitsfunktionen und plant als Nächstes die Einführung integrierter SWG und CASB. Geplant sind außerdem FWaas, Remote-Browser-Isolierung, Netzwerk-Sandboxing mithilfe von Technologien aus der Lastline-Übernahme, API-basierter Zugriff auf SaaS für Datenkontext und Schutz von Edge-Computing. VMware stellt diese Funktionen seinen Kunden direkt und über führende Sicherheitspartner bereit. Aktuell arbeitet das Unternehmen besonders eng mit Zscaler zusammen, aber auch Check Point, Cisco, Fortinet, Menlo Security und Palo Alto Networks gehören zu seinen Partnern.

SASE-Funktionen
VMware

Unverzichtbar	Empfehlenswert	Optional
SD-WAN	WAAP	Schutz von WLAN-Hotspots
Geplant: SWG	Geplant: RBI	Netzwerkverschleierung
Geplant: CASB	Rekursives DNS	Unterstützung älterer VPNs
ZTNA	Geplant: Netzwerk-Sandboxing	Schutz von Edge-Computing
Geplant: FWaaS	Geplant: API-Zugriff auf SaaS	Geplant: UEBA
X-SD-WAN jetzt; SWG geplant: Schutz personenbezogener Daten/Malwareschutz	Unterstützung verwalteter/ nicht verwalteter Geräte	
Max. Datenübertragung/Edge		
Max. Datenübertragung/Cloud		

VMware betont, dass sein SASE-Angebot auf der VeloCloud-Infrastruktur basiert und daher eine reine Cloud-Lösung ist, aber das Unternehmen bietet seinen Kunden auch On-Premises-Implementierungen an. Für Bestandskunden mit SD-WAN oder ZTNA stehen beide Optionen zur Auswahl. Die cloudbasierte Infrastruktur von VMware besteht aus Colocation-Rechenzentren mit Selbstverwaltung für Netzwerk- und Computing-Kapazitäten. Derzeit sind 33 PoP verfügbar und die Zahl soll in den nächsten 12 bis 24 Monaten auf 50 anwachsen. Die Standorte sind über Tier-1-ISP verbunden und haben direkte Peering-Verbindungen zu allen bekannten Cloud-Anbietern. VMware arbeitet auch mit Servicepartnern zusammen, um sein weltweites Netzwerk zu vergrößern, und wird eigenen Angaben zufolge insgesamt 100 PoP zur Verfügung haben, da diese Partner ihre Präsenz ausbauen.

Direkte Konkurrenten für VMware sind Cisco (Meraki and Viptela), Fortinet, Aruba (HPE) Silver Peak und Palo Alto Networks. Laut VMware zeichnet sich seine SASE-Lösung durch die Bereitstellung in der Cloud, führende Multi-Cloud-Unterstützung, zahlreiche Bestandskunden für die WAN-Edge-Infrastruktur und das einheitliche Endpunktmanagement sowie eine ausgezeichnete Benutzererfahrung, einfache Verwaltung und hohe Sicherheit aus.

Zscaler SASE

Zscaler ist vermutlich der bekannteste cloudnative Anbieter, da er schon am längsten cloudbasierte Secure Web Gateway-Services bereitstellt. Das Unternehmen verfügt über 150 PoP weltweit und eine effiziente Single-Pass-Architektur, die Datenverkehr entschlüsselt, auf sensible Daten und Malware überprüft und unter Berücksichtigung der Identität und des Kontexts die angemessenen Richtlinien anwendet. Die mandantenfähige Architektur nutzt einen effizienten Proxy für maximale Übertragungsraten am Edge und in der Cloud.

Der SASE-Service von Zscaler umfasst alle unverzichtbaren Funktionen, allerdings wird das SD-WAN von Partnern bereitgestellt, unter anderem von Aruba (HPE) Silver Peak und VMware. Da die cloudbasierten Sicherheitsservices des Unternehmens schon lange über SWG hinausgehen, unterstützt es bereits komplexere Sicherheitsfunktionen, wie beispielsweise den Schutz von Webanwendungen und API, Remote-Browser-Isolierung, rekursives DNS, Netzwerk-Sandboxing, API-Zugriff auf SaaS-Anwendungen für Datenkontext, die Unterstützung verwalteter und nicht verwalteter Geräte, Schutz von WLAN-Hotspots und die Netzwerkverschleierung. Zweigstellenspezifische Funktionen werden ebenfalls von Partnern bereitgestellt, unter anderem Cisco, Aruba (HPE) Silver Peak und VMware. Zudem gibt es Integrationen für Okta und Ping für die Identitätsprüfung und für CrowdStrike für die Gerätesicherheit. Der SASE-Service wird zusammen mit den Zscaler Internet Access- und Zscaler Private Access-Produkten bereitgestellt, die als Basic- und Advanced-Versionen erhältlich sind.

SASE-Funktionen
Zscaler

Unverzichtbar	Empfehlenswert	Optional
◉ SD-WAN	◉ WAAP	◉ Schutz von WLAN-Hotspots
◉ SWG	◉ RBI	◉ Netzwerkverschleierung
◉ CASB	◉ Rekursives DNS	○ Unterstützung älterer VPNs
◉ ZTNA	◉ Netzwerk-Sandboxing	○ Schutz von Edge-Computing
◉ FWaaS	◉ API-Zugriff auf SaaS	○ UEBA
◉ Schutz personenbezogener Daten/Malwareschutz	◉ Unterstützung verwalteter/ nicht verwalteter Geräte	
◉ Max. Datenübertragung/ Edge		
◉ Max. Datenübertragung/ Cloud		

Ganz im Sinne der Coopetition arbeiten mehrere der in dieser Studie beschriebenen Mitbewerber für bestimmte SASE-Funktionen mit Zscaler zusammen. Als größte Konkurrenten betrachtet das Unternehmen Netskope und Palo Alto Networks. Zu seinen Alleinstellungsmerkmalen zählt Zscaler die cloudnativen Sicherheitsfunktionen, die es in den 150 Rechenzentren bereitstellt, den leistungsfähigen Inline-Proxy, die Thin-Branch-Architektur, die umfassende Prüfung des verschlüsselten Datenverkehrs und die mandantenfähige Architektur in der Cloud.

Fazit

Die SASE-Funktionen, Preismodelle, Paketeinhalte und Integrationen dieser Anbieter stecken noch in den Kinderschuhen und werden im Laufe der Zeit weiterentwickelt werden. Entscheidend wird für die ersten SASE-Kunden – und letztendlich auch die Anbieter – sein, wie reibungslos die Integration und der Betrieb der Netzwerk- und Sicherheitsfunktionen ablaufen und wie einfach (oder schwierig) sich die Beziehung zu den Anbietern gestalten wird. Je mehr Verträge und Preismodelle ein Kunde abschließen und verwalten muss, desto länger wird es dauern, bis sich die Lösungen durchsetzen. Gerade in der Anfangsphase wird es immer wieder Probleme geben. SASE-Anbieter, die mit mehreren Partnern zusammenarbeiten, sollten daher in Bezug auf die Schuldzuweisung Vorsicht walten lassen. Wenn eine Servicekette kompliziert und aufwendig für den Kunden ist, sind die Erfolgsaussichten gering.

Die Vertriebszyklen werden davon abhängen, wer für die Anschaffung und das Budget zuständig ist und wie gut separate Teams gemeinsam Projekte implementieren können. Die Marktbereinigung wird vermutlich länger dauern, als dies sonst bei Technologien der Fall ist. Die Kombination von Netzwerk- und Sicherheitsfunktionen in einem einzigen Markt hat Folgen für die Unternehmensorganisation und -kultur, insbesondere in größeren Unternehmen, in denen Architekturänderungen nicht so schnell umgesetzt werden können. Unternehmen müssen ihre Strukturen analysieren und die Einführung sowie die Finanzierung planen. Es ist wichtig, das Misstrauen zwischen den verschiedenen IT-Gruppen zu zerstreuen, denn nur durch eine effektive Zusammenarbeit lässt sich SASE erfolgreich umsetzen. Führungskräfte müssen neue und umfassendere Ziele setzen und Anreize geben, damit diese Gruppen produktiv zusammenarbeiten.

Das Interesse der Käufer wurde gerade erst geweckt und die meisten Unternehmen suchen noch ihren Weg zum obersten Ziel: der nahtlosen Kombination von Netzwerk- und Sicherheitsfunktionen in einer Welt, in der Mobilität und Cloud-Umgebungen immer größere Priorität erlangen.

Über Enterprise Management Associates, Inc.

Das 1996 gegründete Unternehmen Enterprise Management Associates (EMA) ist ein führender Anbieter von Beratungs- und Analyseleistungen, der detaillierte Einblicke in die gesamte Palette der IT- und Datenmanagementtechnologien bietet. Dank ihrer langjährigen praktischen Erfahrung, Einblicke in die Best Practices der Branche und umfassenden Kenntnisse der aktuellen und geplanten Lösungen verschiedener Anbieter können EMA-Analysten ihre Kunden optimal unterstützen. Weitere Informationen zu den Forschungs-, Analyse- und Beratungsangeboten von EMA für Unternehmenskunden, IT-Fachkräfte und IT-Anbieter finden Sie unter www.enterprisemanagement.com. Sie können EMA auch auf Twitter oder LinkedIn folgen.

Hauptsitz:
1995 North 57th Court, Suite 120
Boulder, CO 80301, USA
Telefon: +1 303 543 9500
www.enterprisemanagement.com

4068.021221