Computacenter

SASE – MODERNE BUSINESS-KONNEKTIVITÄT SCHAFFEN

Was verbirgt sich hinter dem Begriff SASE? Weshalb ist das Thema für Unternehmen aktuell so relevant? Was sind die ersten Schritte, mit denen auch Sie Ihre SASE-Reise starten können? Und welche strategischen Entscheidungen sollten in der Anfangsphase der SASE-Einführung unbedingt berücksichtigt werden?

WAS VERBIRGT SICH HINTER DEM BEGRIFF SASE?

Das Akronym wurde 2019 erstmals von Gartner geprägt und steht für "Secure Access Services Edge". Mit einer Kombination aus Netzwerk- und Security-Komponenten, die in einer einzigen Architektur zusammengeführt sind, erfüllt SASE alle Anforderungen an einen sicheren Zugang für Unternehmen, die am Puls der Zeit arbeiten wollen.

Die Netzwerkkomponenten von SASE umfassen eine ganze Reihe von Bereichen – darunter SD-WAN, Network-as-a-Service und Bandbreitenaggregation. SASE ist der neue Weg, um Ihnen einen schnellen und sicheren Zugang zu cloudorientierten Diensten und SaaS-Angeboten zu ermöglichen. Insgesamt gibt es vielfältige SASE-Angebote, die von Netzbetreibern, Herstellern und Security-Lösungsanbietern teilweise als integrierte Lösungen beworben werden.

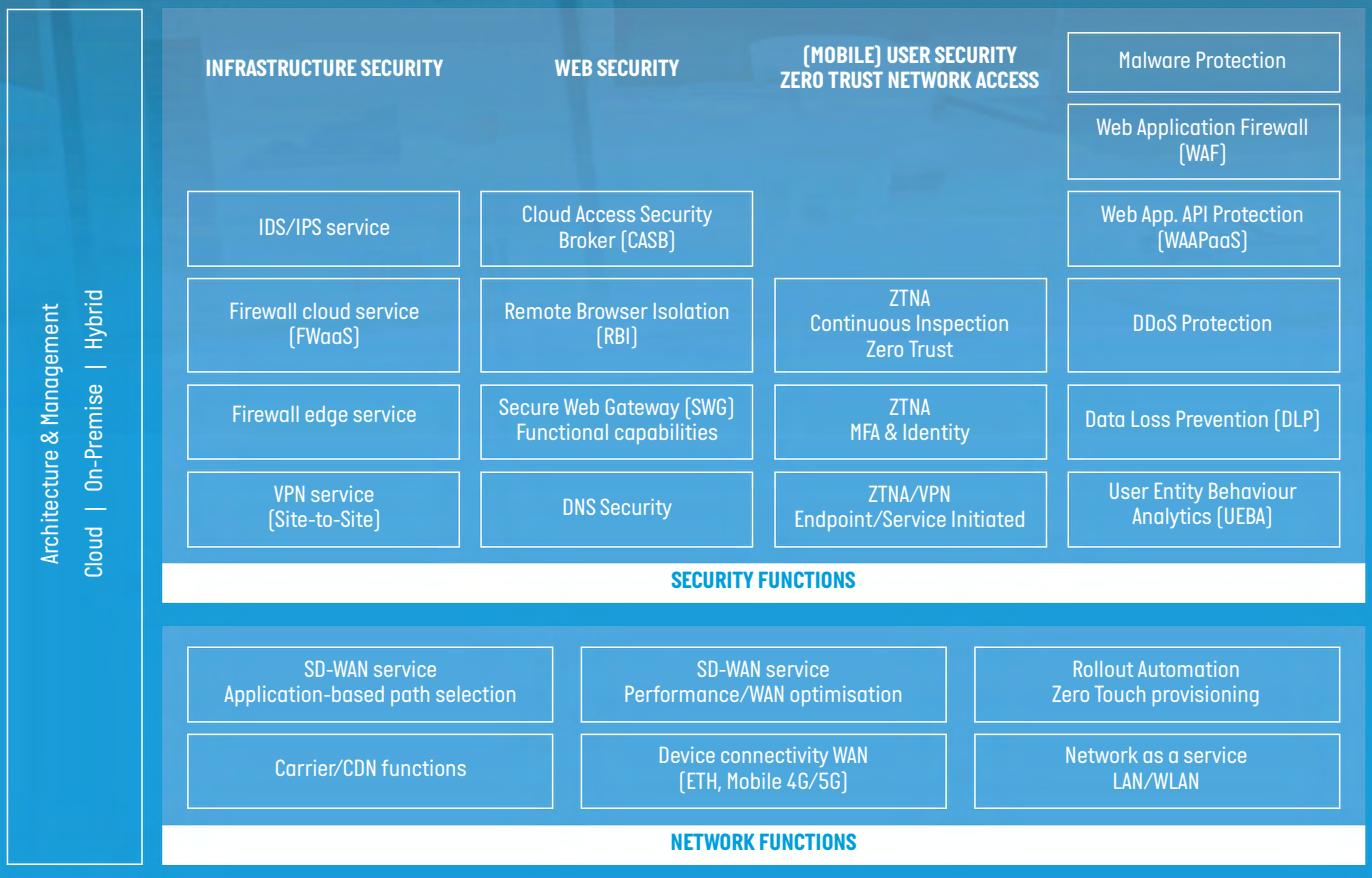
Die Security-Elemente der SASE-Architektur beruhen auf Netzwerk-Security-Funktionen wie VPN, Firewall (as-a-Service), Secure Web Gateway (SWG), Remote Browser Isolation (RBI), Cloud Access Security Broker (CASB) und Malwareschutz.

Um einen stets sicheren Zugang auf Unternehmensressourcen zu ermöglichen, ist Zero Trust Network Access (ZTNA) ein elementarer Bestandteil des SASE-Pakets. Als sinnvolle Ergänzung sind dabei – je nach Anbieterportfolio – zusätzliche Security-Funktionen wie DNS-Security, Web-Application-Firewall/Web Application API Protection-as-a-Service, DDOS-Schutz, Data Loss Prevention (DLP) und User Entity Behaviour Analytics (UEBA) verfügbar.

SASE geht über den reinen Architekturansatz hinaus und stellt sicher, dass Lösungen, die sich an den SASE-Prinzipien orientieren, Folgendes berücksichtigen:

- Die Identität der zugreifenden Entität
- Kontext (z. B. Typ, Zustand und Verhalten des Geräts, wie sensibel die Daten sind, auf die zugegriffen wird)
- Security- und Compliance-Richtlinien
- Eine kontinuierliche Risikobewertung während jeder Sitzung

All diese Funktionen werden gebündelt als ein SASE-Service angeboten – unterstützt durch eine einheitliche Architektur.



Die kombinierten SASE-Funktionen

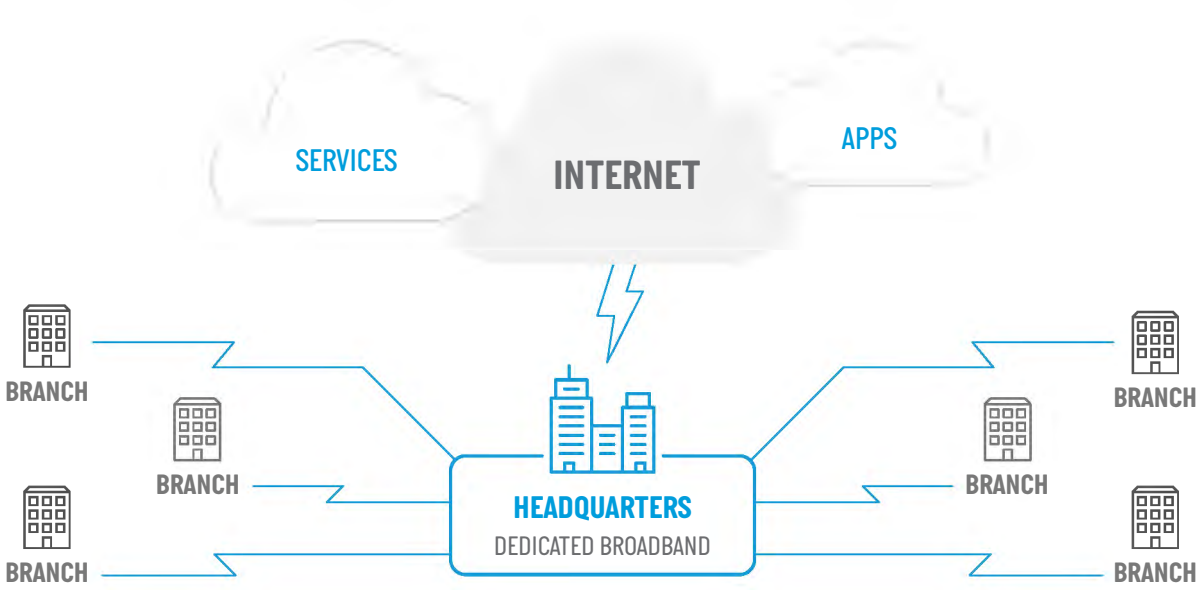
WARUM IST DIESER ANSATZ SO WICHTIG?

Secure Access Service Edge (SASE) beschreibt den neuen, vereinheitlichten Weg zu Netzwerk- und Security-Controls aus der Cloud. Damit verabschiedet sich SASE von der bisherigen Methode, den Netzwerkverkehr immer zwingend durch das zentrale Rechenzentrum zu routen und die Security ausschließlich am Perimeter des Unternehmensnetzwerks zu verwalten.

Stattdessen baut SASE auf SD-WAN-Konnektivität und Konzepte wie Zero Trust Networking auf und stellt damit eine einzige Plattform bereit, die Security-Lösungen für Netzwerke, Webanwendungen, mobiles Arbeiten sowie viele weitere Sicherheitsfunktionen vereint.

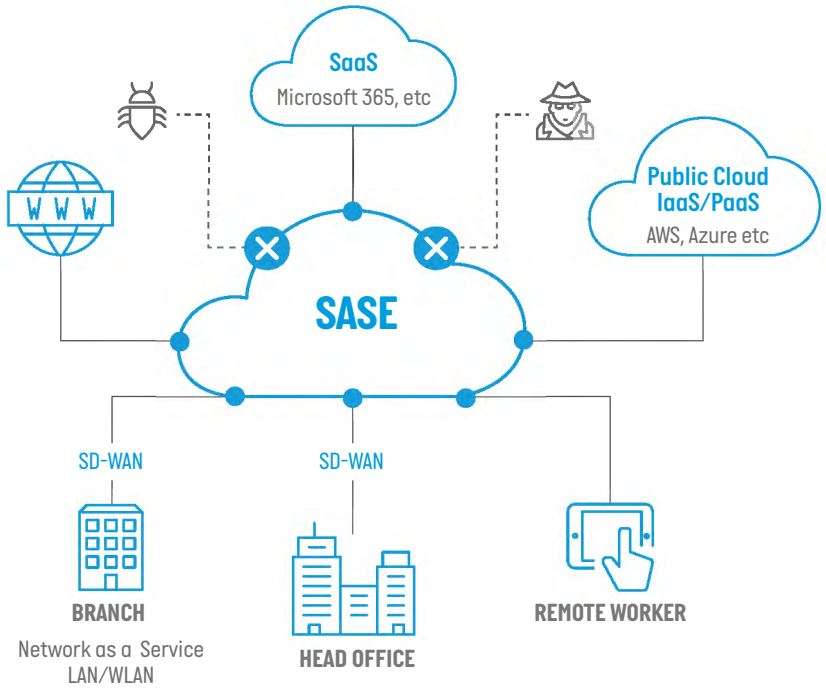
Angetrieben durch die zunehmende Nutzung der Cloud und den rapiden Anstieg mobiler Arbeit ist SASE die zentrale Antwort auf die Frage, wie man den Netzwerk- und Security-Anforderungen eines dezentralen Datenverkehrs bei Konzeption, Aufbau und Management gerecht werden kann – und zwar ohne diesen zwingend zentral durch das Rechenzentrum des Unternehmens zu routen.

Die gestiegene Nachfrage – auch außerhalb der traditionellen Perimeter, Zugriff auf Anwendungen und Daten in der Cloud zu erhalten – hat allerdings nicht nur zu erheblichen Überlastungen und Latenzzeiten im Rechenzentrum geführt, sondern auch zu einer teils unzureichenden User Experience. Dies wurde vor allem zu Beginn der COVID-19-Pandemie deutlich, als Unternehmen ihre Beschäftigten quasi über Nacht ins Homeoffice schicken mussten. Dadurch haben auch Cloud-Zugriffe rapide zugenommen.



Das Schlüsselkonzept hinter SASE sieht vor, elementare Netzwerk- und Security-Funktionalitäten direkt von der Cloud aus verteilt zu etablieren, wodurch diese näher an den Anwendungen und ihren Nutzenden sind. Hierbei erfolgt der Zugriff beispielsweise direkt über nahegelegene Points of Presence (PoP), anstatt sämtliche Verbindungen immer zurück zum zentralen Rechenzentrum zu leiten.

Auf diese Weise verringert das SASE-Modell die hohen Datendurchsatzanforderungen an zentrale Unternehmenszugänge und erlaubt es Unternehmen, die Least-Privilege-Prinzipien einer Zero Trust Architektur anzuwenden.



WER BESTIMMT DERZEIT DEN SASE-MARKT?

Wie eingangs beschrieben, hat Gartner im Jahr 2019 das SASE-Konzept definiert, welches sich stetig weiterentwickelt. Aus diesem Grund gestaltet es sich auch schwierig, die SASE-Services auf einen einzelnen Anbieter oder auf eine einzelne Produktreihe zu beschränken.

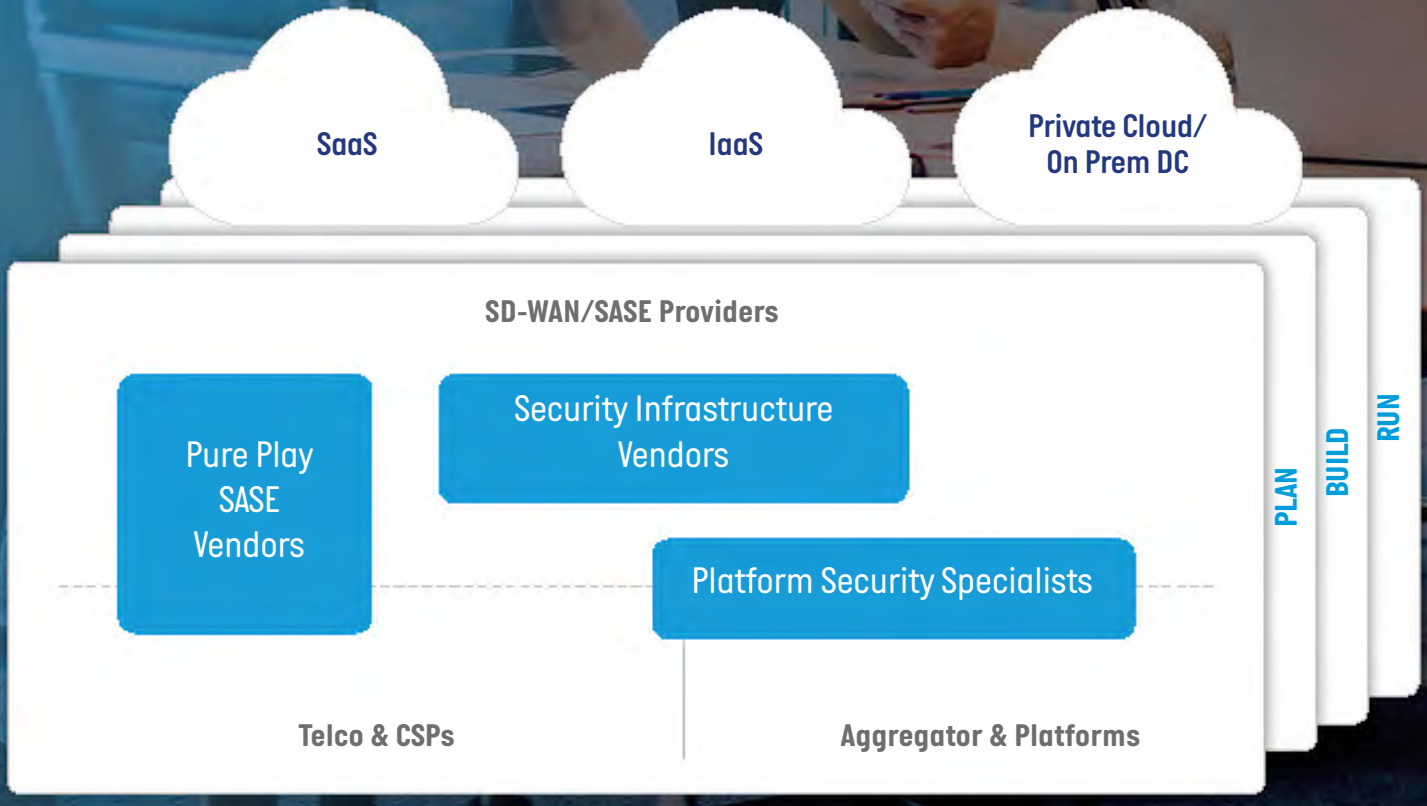
Viele Anbieter behaupten von sich, alle wichtigen Komponenten für eine ganzheitliche SASE-Lösung in ihrem Portfolio mitzubringen. Aus unserer Sicht unterscheiden sich die Anbieter jedoch weiterhin deutlich in ihren Möglichkeiten die gesamten SASE-Funktionen in ihrer Breite und technologischen Tiefe mittels einer zentralen integrierten Plattform gebündelt abzudecken. Insgesamt sehen wir drei relevante Arten von Anbietern am Markt, die aktuell SASE-Funktionen entwickeln – und jeder hat seine eigenen Vor- und Nachteile.

REINE SASE-ANBIETER
Diese Hersteller agieren als reine Softwareanbieter, die sich ausschließlich auf Lösungen im SASE-Stil konzentrieren. Sie bauen nicht auf traditionellem, infrastrukturzentriertem Netzwerk- oder Security-Ansatz auf, sondern haben zumeist einen Cloud-Fokus. Das macht es ihnen leichter, neue Funktionen auf kostengünstige Weise hinzuzufügen.

NETZWERK- UND SECURITY-ANBIETER
Auch Unternehmen, die bislang den Software- und Hardwaremarkt im Bereich Netzwerk -und Security-Infrastruktur bestimmt haben, beschäftigen sich aktuell intensiv damit, ihre bisherigen Plattformen zu transformieren und stetig weiterzuentwickeln. Dies gelingt ihnen, indem sie Produkte bündeln, strategische Akquisitionen angehen und letztlich Hardware- zu Softwareangeboten weiterentwickeln, um die Ergebnisse schließlich als SASE-Lösungen auf den Markt zu bringen. Diese Anbieter verfügen über einen großen Erfahrungsschatz und ein beeindruckendes Lösungsportfolio – dennoch muss weiter an den Portfolios gefeilt werden, da auch diese bisher nicht immer alle Kernkapazitäten von SASE abdecken.

SPEZIALISTEN FÜR SECURITY-PLATTFORMEN
Unternehmen, die bereits Netzwerk- und/oder Security-Funktionen in ihre bestehenden Technologieplattformen integriert haben, ergänzen ihre Plattformen nun auch mit zusätzlichen SASE-Komponenten. Diese Anbieter bergen zwar das Potenzial, sich in der Zukunft als Key Player im SASE-Umfeld zu positionieren, sind aktuell jedoch auch noch nicht am Ziel angelangt. Ein solcher Plattformanbieter kann beispielsweise wesentliche Elemente des SASE-Frameworks abdecken, wie Identity- und Access-Management-Controls, ihm mangelt es dann jedoch an Netzwerkinfrastrukturkomponenten – wie beispielsweise SD-WAN.

Fest steht: Der Markt rund um SASE-Services entwickelt sich rasant. Aus unserer Sicht werden einige Security-Softwareanbieter mit interessanten Alleinstellungsmerkmalen zu Akquisitionskandidaten, um auf deren Basisplattformen neue SASE-Lösungen zu entwickeln und einzuführen.



Wie die verschiedenen Anbieter die SASE-Anforderungen adressieren

VORTEILE VON SASE

Die versprochenen Vorteile einer SASE-Plattform sind umfassend und unterstützen den Übergang zu einer cloudbasierten Security-Lösung für Unternehmen, indem sie Netzwerk- und Security-Funktionen gekonnt kombinieren. Zu den wichtigsten Vorteilen zählen:

- Einfache Skalierbarkeit der Netzwerk- und Security-Funktionen
- Optimale Sicherheit für Anwendungen, die überall eingesetzt werden können
- Zentralisierte, dynamische, rollenbasierte Zugriffskontrollen, die den Betrieb optimieren
- Konsolidierung von Stand-alone-Plattformen
- Vereinfachung komplexer Security-Landschaften mit zahllosen Herstellern und propagierte Kostensenkung durch Konsolidierung und Abschaffung überflüssiger Security-Software und Infrastrukturplattformen
- SASE-Umgebungen sind größtenteils direkt für die Cloud konzipiert. Dies ermöglicht einerseits maximale Flexibilität und hilft darüber hinaus, die Betriebskosten zu minimieren

STOLPERSTEINE BEI SASE

Da der SASE-Ansatz ein sich ständig weiter entwickelndes Konzept ist, gibt es noch kein für alle Belange gültiges Standarddesign, um einen sicheren Unternehmenszugriff über alle User-, Cloud- und Business-Anforderungen hinweg zu managen. Somit gibt es einige Stolpersteine, die beachtet werden sollten:

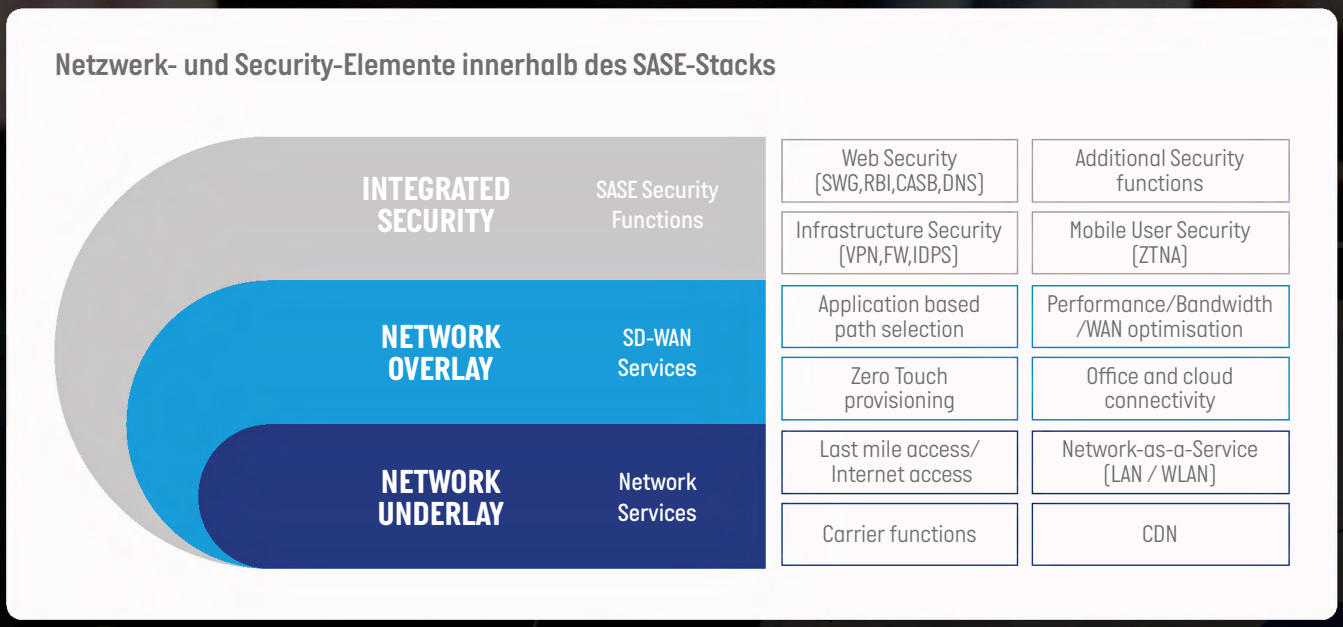
- Generell sollte der Wechsel von einem traditionellen Netzwerk- und Security-Konzept zu einem SASE-Modell nicht unterschätzt werden – vor allem nicht in Organisationen, bei denen sich Netzwerk- und Security-Silos eingeschlichen haben.
- Jedes SASE-Konzept erfordert ein Underlay-Netzwerk (letzte Meile und Backbone), das integriert oder getrennt von der SASE-Lösung bereitgestellt werden muss. Darüber hinaus sollte das Tempo bei der Umstellung auf ein SASE-Modell berücksichtigt werden, denn: Jede Einführung erfordert Integrationen und den Aufbau einer neuen übergreifenden Plattform.
- Darüber hinaus sollte der Einfluss auf den existierenden Security-Betrieb gründlich überprüft werden. Die Prozessabläufe müssen neue und bestehende Datenfeeds von SASE-Lösungskomponenten erfassen, um intelligente Korrelationsregeln für die SIEM-Plattform hervorzubringen. Dadurch wird sichergestellt, dass geschäftskritische Prozesse weiterhin geschützt sind, während das Unternehmen immer weiter auf seiner SASE-Reise voranschreitet.
- Unternehmen werden daher auch in neue Fähigkeiten investieren müssen, um sowohl Management als auch Troubleshooting einer SASE-Umgebung handhaben zu können. Sie sollten daher sicherstellen, dass die SASE-Technologien, in die investiert wird, über angemessene Analyse-Funktionalitäten verfügen.
- Landläufig wird SASE zugeschrieben, dass Lizenz- und Supportkosten deutlich gesenkt werden können, da teure Stand-alone-Security- und Networking-Appliances abgelöst werden. Da jedoch derzeit noch keine übergreifende Plattform am Markt verfügbar ist, die alle Funktionalitäten abbilden kann, hängt der ROI davon ab, wie hoch die Kosten (sowohl Capex als auch Opex) der einzelnen Komponenten sind, beispielsweise eines Cloud Access Security Brokers (CASB). Unternehmen sollten an dieser Stelle genügend Zeit aufwenden, um die erforderliche Due-Diligence-Prüfung durchzuführen. Damit können einzelne Komponenten in die finale Lösung integriert werden. Solange diese Due-Diligence-Prüfung, an der in der Regel mehrere Fachbereiche beteiligt sind, nicht durchgeführt wurde, ist möglicherweise nicht sofort ersichtlich, wo Einsparungen erzielt werden oder wie schnell sie letztlich realisiert werden können.
- Fest steht: Es gibt eine ganze Reihe Hersteller, die SASE-Lösungen anbieten – Tendenz steigend. Obwohl der Markt immer noch relativ jung ist, haben bereits erste Akquisitionen stattgefunden. Daher zeichnet sich bereits jetzt ab, dass es einige Anbieter in Zukunft nicht mehr geben wird. Vor diesem Hintergrund wird es umso wichtiger, auf den richtigen Anbieter zu setzen. Darüber hinaus sollten Unternehmen sicherstellen, dass sie Zugriff auf das benötigte Fachwissen haben – entweder intern oder über einen Partner – um die verschiedenen Lösungen einordnen und bewerten können.

ZUSAMMENFASSENDE ANALYSE DES SASE-MARKTS

Auch Ende des Jahres 2021 steckt der SASE-Markt noch in den Kinderschuhen. Und obwohl mehrere Anbieter bereits andeuten, dass sie zu Man kann zwar sagen, dass der SASE-Markt inzwischen etabliert ist, aber er entwickelt sich auch noch weiter. Und obwohl mehrere Anbieter bereits andeuten, dass sie zu Marktführern werden könnten, sehen wir derzeit keinen eindeutigen Gewinner. Umso entscheidender ist daher, den richtigen Anbieter für die unternehmensspezifischen Anforderungen zu identifizieren. Denn nur wenn die Use Cases auf den Unternehmensbedarf abgestimmt sind, kann das volle geschäftliche und operative Potenzial gehoben werden.

DIE RICHTIGEN ENTSCHEIDUNGEN TREFFEN

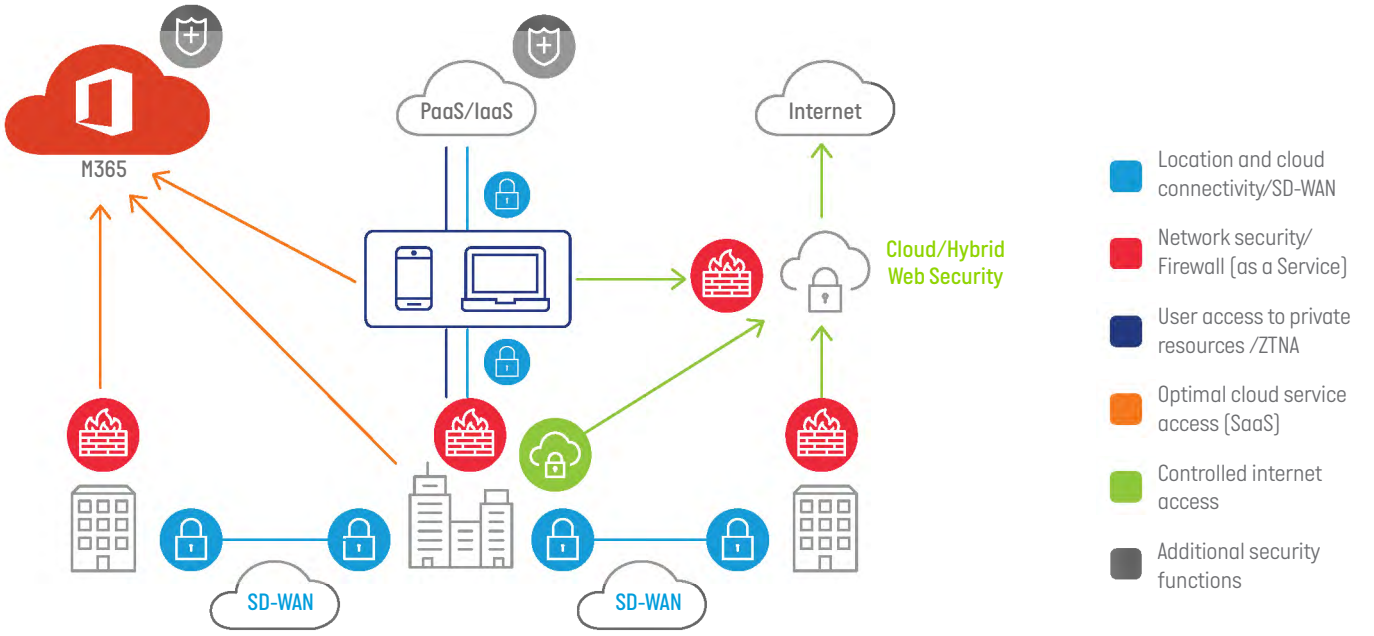
Es ist wichtig, dass Unternehmen den für sie passenden Anbieter auf der Grundlage validierter Use Cases und eines klaren Verständnisses der funktionalen und nicht funktionalen Anforderungen auswählen. Dadurch wird sichergestellt, dass – unabhängig von der gekauften Plattform – ein Mehrwert erzielt wird und dass die Betriebs- und Kostenvorteile wie gewünscht realisiert und die Geschäftsrisiken dabei minimiert werden können.



Darüber hinaus sollte beachtet werden, dass die Produktauswahl nicht auf der Grundlage von Funktionen erfolgt. Dieser Ansatz hat sich als teuer für Unternehmen erwiesen, wenn sie sich versehentlich an nicht benötigte Funktionen gebunden haben, während sie in den dringendsten Bereichen nur unzureichende Funktionen erhalten haben. Letztlich kann die Wahl des richtigen Anbieters Unternehmen auch dabei helfen, eine weniger komplexe Lösung zu realisieren, die sich sogar besser über alle Plattformen hinweg integrieren lässt.

SASE-BAUSTEINE

Für SASE-Lösungen gibt es mehrere architektonische Optionen, die sowohl unterschiedliche organisatorische Anforderungen als auch den Schutzbedarf des Unternehmens widerspiegeln. Aus unserer Sicht gibt es dabei standardisierte Bausteine, die in alle SASE-Designs integriert werden sollten. Damit wird eine solide Grundlage geschaffen, auf der weiter aufgebaut werden kann.



▲ SASE-High-Level-Referenzarchitektur

Standort- und Cloud-Konnektivität/SD-WAN

Das SD-WAN-Overlay stellt die sicheren Verbindungen zwischen Standorten und Cloud-Unternehmensressourcen (IaaS/PaaS) her. In der Regel ist eine SD-WAN-Lösung der flexibelste und effektivste Weg, um Kommunikationsanforderungen von Unternehmen zu erfüllen und bietet darüber hinaus die wesentlichen VPN-Verschlüsselungs- und oftmals auch weitere Basis-Security-Funktionen.

Infrastructure Security/Firewall (as a Service)

Infrastructure Security-Funktionen wie Firewalls dienen der Kommunikationskontrolle und sind ein wichtiger Baustein in der Architektur. Aufgrund ihrer inhärenten Flexibilität können sie auf unterschiedlichste Art und Weise ausgerollt werden. Wird beispielsweise eine Firewall als Edge-Service bereitgestellt, ermöglicht die Architektur, den SASE-Guidelines zu folgen und die Prüffunktionalität zur jeweiligen Session zu verlagern und nicht umgekehrt. Dies gilt für Standorte, an denen der direkte Internetzugang der wichtigste Verbindungsweg ist. Mit Firewall-as-a-Service (FWaaS) wird dieser Prozess in die Cloud verlagert, wodurch die Nutzung einfacher als bei herkömmlichen Firewalls werden kann.

Dank FWaaS können alle Vorteile einer Firewall auch ohne Hardware genutzt werden – und zwar auf und innerhalb der Cloud. Dies ist vor allem für den mobilen Zugriff auf Daten von enormen Vorteil. Eine zentralisierte Verwaltung und Kontrolle der Richtlinien ist dabei eine wichtige Ergänzung für beide Network-Security-Ansätze.

User Access zu privaten Ressourcen/Zero Trust Network Access

Egal ob on-premises oder in der Cloud – der mobile Zugriff auf private Ressourcen erfordert sichere Verbindungen. Bei einer „Zero Trust Network Access"-Lösung erfolgt zunächst eine Authentifizierung zur Validierung der User-/Maschinenidentität – zum Beispiel in Verbindung mit einer Identity-Management-Lösung. Darauf aufbauend erfolgt die Zuweisung der entsprechenden Berechtigungen unter Berücksichtigung von Rolle und Kontext. Im Laufe einer Verbindung sollte eine kontinuierliche Kontrolle erfolgen, um adäquat auf Änderungen im Kontext und automatisiert auf Sicherheitsvorfälle reagieren zu können.

Die Umsetzung eines solchen Zero-Trust-Konzepts, bei dem kein implizites, unqualifiziertes Vertrauen vorgesehen ist, ist eine Kernkomponente von SASE und sollte daher in jedem SASE-Baustein berücksichtigt werden.

Optimaler Cloud Service Access (SaaS)

Ein optimaler Zugang zu Trusted-Cloud-Ressourcen (SaaS), wie beispielsweise Microsoft 365 (M365), ist oftmals einer der Kerntreiber eines SASE-Projekts. Dort bietet zumeist der kürzeste, direkte Weg zwischen dem User und dem nächstmöglichen Office 365-Endpoint die beste Performance. Dabei ist es jedoch wichtig, jene Security-Funktionen zu vermeiden, die den Netzwerkverkehr während der Übertragung unterbrechen und entschlüsseln, da die entschlüsselten Inhalte dabei häufig geändert oder blockiert werden.

Die Anwendung dieser Funktionen auf den M365-User-Traffic führt beispielsweise zu Änderungen an Office 365-Protokollen und -Daten-Traffic (außerhalb der standardmäßigen und dokumentierten APIs). Daher ist ein geeignetes Design, das den Anforderungen der SaaS-Anwendung entspricht und angemessene Sicherheit bietet, unerlässlich.

Kontrollierter Internetzugang

Der kontrollierte Zugriff auf Internet- und Public-Cloud-Ressourcen via Cloud oder Hybrid Web Security erfordert neue Funktionen wie Secure Web Gateways, Remote Browser Isolation und DNS-Sicherheit.

Zusätzliche Security-Funktionen

Zusätzliche Funktionen wie CASB, WAF (Web Application Firewall) und erweiterter Malwareschutz bieten weitere Schutzebenen für die unternehmenskritischen IaaS-, PaaS-, SaaS- und On-Premises-Dienste.

UNSER FAZIT

Fest steht: SASE wird die Integration von Netzwerk- und Security-Services – zusammengefasst in eine ganzheitliche Architektur – maßgeblich vorantreiben und prägen. Dabei glauben wir nicht, dass SASE automatisch das Ende von On-Premises- oder traditionellen Infrastruktur-Security-Herstellern bedeuten wird. Die Gewinner in diesem neuen Markt werden jedoch definitiv die Anbieter mit dem umfassendsten Portfolio sein oder die mit der effektivsten Integration zu Cloud-Ressourcen von Drittanbietern oder zu nativen Providern.

Aktuell gewinnen vor allem zwei Begriffe an Bedeutung, um die verschiedenen Arten von SASE-Ergebnissen zu beschreiben:

Ingress SASE
Diese Maßnahmen ermöglichen den sicheren Zugriff von außen auf interne Anwendungen des Unternehmens – unabhängig davon, wo diese betrieben werden.

Egress SASE
Funktionen, die es ermöglichen, überall sicheren Zugang auf Internetdienste zu haben.

Da sich diese Anwendungsfälle vermehrt in der gesamten Branche durchgesetzt haben, empfehlen wir zu prüfen, ob der ausgewählte Anbieter beide Aspekte abdecken kann oder ob dessen Lösungen nur auf einen bestimmten Bereich ausgerichtet sind. Dies hilft Ihrem Unternehmen, den richtigen Ansatz für den jeweilig gewünschten Business-Outcome zu finden.

Computacenter betrachtet SASE versinnbildlicht als Reise, die in Etappen angetreten wird. Diese beginnt mit einer klaren Definition der Anforderungen bzw. der beabsichtigten Security-Ergebnisse, führt weiter über die Entwicklung eines Soll-Designs und einer Soll-Architektur und der Evaluierung und Validierung der passenden Herstellerlandschaft bis hin zur Identifikation von Optionen für die Konsolidierung oder Integration. Dies ist jedoch nur ein kleiner Ausschnitt von dem, was wir an Maßnahmen in diesem Zusammenhang empfehlen.

SPRECHEN SIE UNS AN!

Wenn auch Sie SASE für Ihr Unternehmen in Betracht ziehen und sich fragen, mit welchen konkreten Schritten Sie Ihre SASE-Reise beginnen sollten, finden Sie bei Computacenter genau die richtigen Ansprechpersonen. Wir geben Ihnen praxistaugliche Anleitungen an die Hand, geben Ihnen einen Überblick zu den unterschiedlichen SASE-Optionen und unterstützen Sie ganzheitlich bei der Definition Ihrer SASE-Strategie und -Architektur. Selbstverständlich beraten wir Sie auch gerne bei der individuellen Anbieterauswahl.

Sprechen Sie einfach Ihr Computacenter Account Management an oder senden Sie uns eine E-Mail an **SecurityEnquiries@computacenter.com**

Über Computacenter

Computacenter ist ein führender, unabhängiger Technologiepartner, dem große Unternehmen und öffentliche Auftraggeber vertrauen. Wir helfen unseren Kunden bei der Beschaffung, der Weiterentwicklung und dem Betrieb ihrer IT-Infrastruktur, um eine digitale Transformation zu ermöglichen, die Menschen und ihr Geschäft erfolgreich macht. Computacenter ist ein an der Londoner Börse notiertes Unternehmen und beschäftigt über 17.000 Mitarbeiter:innen weltweit.

www.computacenter.com

Computacenter