Whitepaper
Zukunftsvision

Der richtige Ansatz für den Aufbau eines SASE

Wie Sie Ihre Netzwerkumgebung sichern und optimieren

verizon

Einleitung

Da die digitale Transformation der Geschäftswelt weiterhin rasch voranschreitet, haben immer mehr IT-Teams mit gravierenden Herausforderungen rund um die Verwaltung und Sicherung der zunehmend komplexen Unternehmensinfrastrukturen zu kämpfen.

Konventionelle Ansätze zur Bewältigung steigender Traffic-Volumen und zur Minimierung potenzieller Sicherheitsrisiken basieren auf der Implementierung zusätzlicher dedizierter Appliances und spezialisierter Systeme. Doch im Zeitalter der cloudnativen Apps und auf verschiedene Edge-Systeme verteilten Anwendungen erweisen sich diese Strategien immer häufiger als ungeeignet.

Insofern ist es ein wahrer Glücksfall, dass nun ein besserer Ansatz zu Verfügung steht: das Secure Access Service Edge (SASE). Hinter diesem Wortungetüm verbirgt sich nichts Geringeres als eine neuartige Paketlösung, die Sicherheits- und Netzwerkdienste miteinander kombiniert und daher optimal für die Anwendungsbereitstellungsmodelle moderner Unternehmen ausgelegt ist.

Was ist SASE?

SASE ist ein neues cloudnatives Sicherheitskonzept, das im Jahr 2019 von Gartner eingeführt wurde. Einfach ausgedrückt handelt es sich um eine integrierte Netzwerkarchitektur, die SD-WAN-Funktionen mit vielfältigen Netzwerksicherheitsdiensten wie Secure Gateway, Cloud Access Security Broker (CASB), Zero-Trust Network Access (ZTNA) und Firewall-as-a-Service (FWaaS) kombiniert und in digitalen Unternehmen als zentrale, cloudbasierte und dynamisch anpassbare Infrastruktur für den sicheren Zugriff auf das Internet fungiert.

Dementsprechend markiert die Entwicklung des SASE-Konzepts den Übergang zu einer neuen Strategie, in deren Zentrum eine identitätsbasierte Netzwerk- und Sicherheitsplattform steht, die am Netzwerk-Edge bereitgestellt wird und allen Benutzern an Remote-Standorten sowie sämtlichen IoT-Geräten einen sicheren Zugriff auf cloudbasierte und unternehmensinterne Ressourcen ermöglicht. Dadurch wird nicht nur die Sicherheit, sondern auch die Übertragungsleistung beim standortunabhängigen Ressourcenzugriff verbessert, was sich möglicherweise in geschäftlichen Vorteilen wie einer kürzeren Entwicklungsdauer, beschleunigten Markteinführungsprozessen und einer schnelleren Reaktion auf veränderte Markt- oder Betriebsanforderungen niederschlägt.

Allerdings herrscht in der Branche und der Analysten-Community bisher noch keine Einigkeit darüber, was eine SASE-Lösung über diese allgemeine Beschreibung hinaus im Detail bieten muss. Während die Experten von Gartner hier eine eigenständige Plattform mit einer zentralen Managementkonsole vor Augen hatten, zeichnet sich mittlerweile ab, dass ein modernes SASE auf einer Kombination von Produkten und Technologien verschiedener Anbieter basiert, die miteinander integriert und zu einer genau auf die spezifischen Anforderungen des jeweiligen Unternehmens abgestimmten Lösung zusammengefügt werden.

„Im Wettbewerb haben diejenigen Anbieter die Nase vorn, die eigene globale Backbone-Netzwerke betreiben, Direktverbindungen zu Cloud-Services eingerichtet haben und gebündelte oder beliebig kombinierbare Zusatzdienste bereitstellen, welche sich – was besonders wichtig ist – ganz nach Bedarf zukaufen und skalieren lassen und dabei auch bei großen Nutzerzahlen einfach zu verwalten sind."
— Mike Fratto, 451 Research[1]

40 %

Bis 2024 werden mindestens 40 % der Unternehmen über klare Strategien für den Aufbau eines SASE verfügen. Ende 2018 lag dieser Anteil noch bei unter einem Prozent.[2]

116 %

Laut einer Prognose der Dell'Oro Group „wird der Markt für SASE-Lösungen ein jährliches Wachstum von 116 % verzeichnen und bis 2024 ein Gesamtvolumen von 5,1 Milliarden US-Dollar erreichen".[3]

1. Mike Fratto, „COVID-19: Secure remote access services in demand as enterprises continue work-from-home strategies", 451 Research, 10. September 2020.
2. Neil MacDonald, Lawrence Orans, Joe Skorupa, „The Future of Network Security Is in the Cloud", 30. August 2019.
3. https://www.sdxcentral.com/articles/news/delloro-sase-market-to-hit-5b-by-2024/2020/10/

Angesichts dessen bleibt zur weiteren Klärung des Begriffs vorläufig nur der analytische Blick auf die verschiedenen Bestandteile des Akronyms: „Secure Access“ verweist auf den Übergang vom konventionellen, standortbasierten Bereitstellungsmodell zu einem neuen, identitätsbasierten Sicherheitsansatz, der besser auf den Schutz von mobilen, oft nicht an Unternehmensstandorten befindlichen Mitarbeitern ausgerichtet ist. „Service Edge“ betont, dass es sich um einen cloudbasierten, bedarfsgerecht skalier- und erweiterbaren Dienst handelt, der modernen Unternehmen die Migration geschäftskritischer Anwendungen in die Cloud erleichtert.

Leider herrscht in der Branche und der Analysten-Community bisher noch keine Einigkeit darüber, was eine SASE-Lösung über die allgemeine Definition hinaus im Detail bieten muss.

Warum ist SASE aktuell in aller Munde?

Da der Bedarf an Sicherheitssystemen für moderne WAN-Umgebungen in letzter Zeit stark wächst, hat die Markteinführung geeigneter SASE-Lösungen für beträchtliches Aufsehen und ein gesteigertes Interesse gesorgt. Zusätzlich wird der Trend zum SASE durch die COVID-19-Pandemie, die wachsende Zahl der Online-Bedrohungen, die fortschreitende Migration geschäftskritischer Anwendungen in die Cloud und in Edge-Systeme sowie die Umstellung auf dynamische Apps getragen. Denn im Zuge dieser Entwicklungen sind die Verantwortlichen mit neuen Herausforderungen in Sachen Anwendungsleistung, Netzwerksicherheit und Skalierbarkeit konfrontiert.

Die COVID-19-Pandemie

Obwohl schon vor dem Frühjahr 2020 ein stetiger Anstieg der Zahl der Telearbeiter und mobilen Mitarbeiter zu verzeichnen war, hat der Ausbruch der Pandemie diesen Trend erheblich beschleunigt. Und auch nach der Aufarbeitung der Folgen von COVID-19 werden wahrscheinlich mehr Menschen langfristig von zu Hause und anderen Remote-Standorten aus arbeiten. Das ist eine der Ursachen dafür, dass die Unternehmen immer mehr geschäftlich genutzte Anwendungen in die Cloud migrieren.

Neue Bedrohungen

Zugleich veranlassen aktuelle Trends wie der Umstieg auf cloudbasierte Netzwerkinfrastrukturen und Konnektivitätslösungen von Drittanbietern sowie die wachsende Zahl globaler Online-Angebote, IoT-Geräte und Remote-Mitarbeiter die Unternehmen dazu, immer mehr Geschäftsprozesse, Anwendungen und Daten in die Cloud zu verlagern. Dadurch eröffnet sich den Verantwortlichen einerseits eine Vielzahl neuer Möglichkeiten. Andererseits wird der Schutz des eigenen Netzwerks immer schwieriger, weil die verteilten Anwendungen und Teams die Angriffsfläche und das Sicherheitsrisiko des Unternehmens vergrößern. Immer mehr Cyber-Kriminelle suchen gezielt nach Schwachstellen, die sich aus der im Zuge der COVID-19-Pandemie stark gestiegenen Zahl der Telearbeiter ergeben.

Fortschreitende Virtualisierung und Cloud-Migration

Abgesehen davon hat das Gros der Unternehmen Im Laufe der letzten Jahre mit der digitalen Transformation ihrer IT-Infrastrukturen begonnen und dabei sowohl die eigenen Netzwerkkomponenten virtualisiert als auch immer weitere Funktionen, Datenbestände und Workloads (und den von diesen ausgehenden Netzwerk-Traffic) auf Cloud-Plattformen migriert. Damit einhergehend steigt die Nutzung dynamischer Apps, die nach Belieben bereitgestellt, angepasst und optimiert werden können.

Allerdings nehmen diese modernen Anwendungen mehr Ressourcen und Übertragungskapazitäten in Anspruch, weil sie nur dann eine optimale Leistung und Benutzererfahrung bieten, wenn die Latenzen niedrig und die Durchsatzraten entsprechend hoch sind. Darüber hinaus ist eine umfassende Anpassung und Erweiterung der Sicherheitsinfrastruktur erforderlich. Diese Voraussetzungen müssen insbesondere für Anwendungen aus den Bereichen Augmented Reality (AR), Virtual Reality (VR), IoT und Videoverarbeitung erfüllt sein.

Die Abkehr von Netzwerk-Appliances

Nicht zuletzt deshalb wird in immer mehr Unternehmen nach Alternativen zu den herkömmlichen On-Premises-Geräten gesucht, die gewöhnlich als Appliances bezeichnet werden. Den Verantwortlichen ist bewusst, dass dieses Bereitstellungsmodell umfangreiche Kapitalinvestitionen, regelmäßige Softwareupdates und teure Hardwareupgrades zur Implementierung neuer Features und Funktionen erfordert.

62 Prozent der Unternehmen haben während der Pandemie einen Anstieg der IT-Sicherheitsvorfälle beobachtet.[4]

Zugleich sind die Entscheidungsträger zunehmend von den Vorteilen der Cloud und virtualisierter Umgebungen überzeugt und suchen nun verstärkt nach entsprechenden Lösungen für die Bereitstellung von Netzwerkdiensten und Konnektivität. Besonders gefragt sind zentrale Managementportale, Self-Service-Bereitstellungsfunktionen und miteinander integrierte Sicherheits- und Netzwerksysteme.

4. 451 Research Digital Pulse: CORONAVIRUS FLASH SURVEY OCTOBER 2020. https://verizon.northernlight.com/document.php?docid=VK20201016830000071&datasource=VIRNSYND&trans=view&

Der Trend zur Anbieterkonsolidierung

Im Zuge dieser Umstellung zeigt sich einmal mehr, dass der IT-Bereich von zwei widersprüchlichen, mitunter aber synchron auftretenden Dynamiken geprägt ist: Expansion und Konsolidierung. Üblicherweise wächst in der Frühphase eines neuen Technologiezyklus die Komplexität der angebotenen Produkte (zumindest vorübergehend) sowie die Zahl der Marktteilnehmer, sodass die Unternehmen meist mit mehreren, voneinander unabhängigen Anbietern zusammenarbeiten müssen. Im Zuge der Weiterentwicklung und Reifung der Technologie kommt dann ein Konsolidierungsprozess in Gang, wenn die auf dem Markt präsenten Firmen ihre entsprechenden Angebote durch Übernahmen und die Vereinfachung der eigenen Produktpalette abrunden. Dadurch sinkt allmählich die Zahl der Anbieter, mit denen die Unternehmen interagieren.

68 %

der Manager in gehobenen Positionen beabsichtigen, ihre langfristigen Strategien angesichts der neuen Gegebenheiten nach der Pandemie zu überdenken.[5]

Vor diesem Hintergrund sind die Verantwortlichen vielerorts bestrebt, die Zahl ihrer Partner möglichst klein zu halten, weil sie das von Inkompatibilitätsproblemen und Investitionen nach dem Gießkannenprinzip ausgehende Risiko vermeiden möchten. Sie suchen nach breit aufgestellten Anbietern, die umfangreiche Erfahrung in den Bereichen Sicherheit, Anwendungsbereitstellung und Netzwerke vorweisen und somit alle Phasen des Technologiezyklus mit geeigneten Services abdecken können. Das trifft neuerdings insbesondere auf SASE-Anbieter zu.

Die zunehmende Komplexität moderner IT-Umgebungen

Generell gilt: Je vielfältiger und zahlreicher die Komponenten der IT-Umgebungen moderner Unternehmen werden, desto komplizierter gestaltet sich das Management der darauf basierenden Infrastrukturen. Erschwerend kommt hinzu, dass die dafür nötigen Experten oft nicht zur Verfügung stehen oder auf einfache Weise angeworben und dann im Unternehmen gehalten werden können.

Die Vorteile einer SASE-Lösung

Die Zusammenführung der Netzwerk- und Sicherheitsfunktionen in einer skalierbaren SASE-Lösung eröffnet den Unternehmen die Möglichkeit, die eigene Netzwerkinfrastruktur flexibel an neue geschäftliche Anforderungen anzupassen, die Anwendungsleistung zu verbessern und die Netzwerksicherheit zu stärken. Dadurch erhalten die Benutzer an jedem Standort sicheren Zugriff auf Anwendungen und Ressourcen.

Gesteigerte Flexibilität

Die Implementierung eines SASE kann die Flexibilität des Unternehmens insgesamt steigern, vor allem durch die:

- Beseitigung der Schwierigkeiten, die sich aus der Komplexität und mangelnden Integration der bestehenden Systeme ergeben,
- Schaffung neuer Möglichkeiten für den schnellen und sicheren Umstieg auf die Cloud,
- Unterstützung innovativer geschäftlicher Partnerschaften, die beispielsweise auf der sicheren gemeinsamen Nutzung von Daten, Apps und IT-Diensten basieren.

Darüber hinaus versetzt eine cloudbasierte SASE-Infrastruktur die Verantwortlichen in die Lage, auf einfache Weise neue Erkennungs- und Abwehrsysteme sowie Sicherheitsmaßnahmen wie Secure Gateway, Next-Generation-Firewall-Richtlinien, Webfilter, Sandboxing-Funktionen und DNS-Schutz zu implementieren. Dabei lassen sich alle gewünschten Dienste jeweils über das Edge-System bereitstellen, dessen Standort dem Benutzer am nächsten liegt – und zwar unabhängig davon, ob die Verbindung über eine kabelgebundene Übertragungsinfrastruktur, ein Mobilfunk- oder Roamingnetz oder die Anschlussleitung in einer kleineren oder größeren Unternehmensfiliale hergestellt wird.

Vereinfachte IT-Infrastrukturen

Wenn ein Unternehmen die Konsolidierung der eigenen IT-Infrastruktur und der dort implementierten Sicherheitssysteme plant, sollte der Aufbau eines SASE ganz oben auf der Liste der möglichen Maßnahmen stehen. Denn auf diese Weise lässt sich sowohl die Zahl der eingesetzten Punktlösungen als auch der Arbeitsaufwand für Routine-, Wartungs- und Updateprozesse reduzieren, wodurch die oftmals an der Belastungsgrenze arbeitenden und unzureichend besetzten IT-Teams spürbar entlastet werden. Zudem profitieren die Verantwortlichen von der Möglichkeit, die gesamte Sicherheits- und Netzwerkinfrastruktur über eine zentrale Konsole zu verwalten.

Integrierte Netzwerk- und Sicherheitsfunktionen

Darüber hinaus basiert ein SASE – wie bereits angesprochen – auf der Zusammenführung diverser Netzwerk- und Sicherheitssysteme, sodass beispielsweise die Bereitstellung anwendungsspezifischer Routing- und Firewallfunktionen über eine einheitliche Plattform erfolgt. Damit erscheint das Modell als der logische Schlusspunkt einer Entwicklung, in deren Verlauf die schon länger populären cloudbasierten SD-WAN-Dienste zunehmend um neuartige, cloudnative Sicherheitsmechanismen und -anwendungen ergänzt werden. Das Ergebnis sind straffere, schlankere Betriebsprozesse mit spürbaren Vorteilen für alle Beteiligten: Die zuständigen Teams können Netzwerk und Sicherheit von einer zentralen Konsole aus verwalten, während die Benutzer von leistungsoptimierten Zugriffsoptionen und einem stärkerem Schutz profitieren.

„Die Nachfrage nach nutzerfreundlichen, skalierbaren, flexiblen, latenzarmen und umfassenden Sicherheitslösungen erzwingt die zunehmende Verschmelzung der Marktsegmente für WAN-Edge- und Netzwerksicherheitsprodukte.“[6]
— Gartner

Verbesserte Leistung

Neben den bekannten Vorteilen einer Cloud-Infrastruktur bringt ein modernes SASE außerdem deutliche Verbesserungen in puncto Netzwerkleistung, da hier globale SD-WAN-Dienste und native Optimierungstools zum Einsatz kommen. Zugleich bietet das Modell die Möglichkeit, Latenzen zu minimieren und die Anwendungsleistung zu steigern, da die Systeme zur Prüfung des Cloud-Traffics näher an den Standorten der Endbenutzer bereitgestellt werden können, sodass der betreffende Datenverkehr nicht länger über das unternehmenseigene Rechenzentrum fließen muss.

Starke Sicherheit

In einer modernen dezentralen Netzwerkumgebung ist der Perimeter längst nicht mehr die undurchdringliche Verteidigungslinie, die er einst war. Deshalb lassen sich mithilfe einer SASE-Lösung benutzer-, geräte- und anwendungsspezifische Zugriffs- und Kontrollmechanismen einrichten, die die bestehenden Schutzfunktionen an den Zugangspunkten der WAN-Segmente und VPNs ergänzen oder ablösen.

Potenzielle Einsparungen

Wenn Sie sämtliche Anwendungen auf eine zentrale, cloudbasierte Plattform migrieren, können Sie Ihre hardwarebasierten Punktlösungen durch virtualisierte Komponenten ablösen, um Investitionskosten zu sparen, den wachsenden Bedarf an IT-Ressourcen zu decken und die Skalierbarkeit und Flexibilität Ihrer Infrastruktur zu steigern. Außerdem haben Sie die Möglichkeit, Ihren Teams das Management und die Integration der einzelnen Lösungskomponenten zu vereinfachen und umständliche Anschaffungsprozesse und Vertragsverhandlungen zu vermeiden, indem Sie sich für einen zentralen Anbieter entscheiden und alles aus einer Hand beziehen.

5. Verizon, „The Future of Work“, https://enterprise.verizon.com/resources/de/reports/future-of-work-reimagining-business-as-usual.pdf
6. Gartner, „Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge“, 2019.

Effektive SASE-Lösungen: die vier wichtigsten Merkmale

Der Aufbau eines SASE, das Ihren Anforderungen gerecht wird, ist nicht trivial, zumal sich die Technologie noch in der Entwicklungsphase befindet. Andererseits sollten Sie jedoch bedenken, dass die zentralen Komponenten und Funktionen eines SASE in der einen oder anderen Form schon seit mindestens zehn Jahren verfügbar sind. Beispielsweise hat Verizon bereits seit über zwei Jahrzehnten IT-Lösungen im Angebot, die sich als Fundament einer SASE-Infrastruktur eignen.

Dank dieser umfangreichen Erfahrungen und Einblicke sind unsere Experten genau darüber informiert, wo die zentralen Herausforderungen in Bezug auf die Bereitstellung der für ein SASE erforderlichen Netzwerk- und Sicherheitsdienste liegen und wie sich das volle Potenzial der neuen Technologie freisetzen lässt. Ihre Einsätze in verschiedenen Kundenunternehmen haben sie gelehrt, dass eine erfolgreiche SASE-Lösung sich durch die folgenden vier Merkmale auszeichnet.

1. Integration verschiedener Technologien

Da jedes Unternehmen mit spezifischen Herausforderungen konfrontiert ist, gibt es keine SASE-Lösungen „von der Stange". Dennoch lässt sich feststellen, dass der Aufbau einer entsprechenden Infrastruktur in jedem Fall den versierten Umgang mit diversen Technologien erfordert.

Netzwerk

Bei der Einrichtung eines SASE müssen die Verantwortlichen in der Lage sein, physische Netzwerktechnologien (Private IP, MPLS) und virtuelle Netzwerke (SDN-Overlays) miteinander zu integrieren. Dies dient letztlich der Implementierung von SD-WAN-Funktionen für Routing, Priorisierung und Bandbreitenoptimierung. Ergänzend können die Unternehmen As-a-Service-Angebote rund um die WAN-Optimierung und das WAN-Routing in Anspruch nehmen.

Sicherheit

Da ein SASE als standortunabhängige Infrastruktur für den sicheren Zugriff auf cloudbasierte Anwendungen dient, kann der Schutz der Benutzer und Geräte nur durch eine Kombination verschiedenartiger Sicherheitslösungen gewährleistet werden. Dazu zählen beispielsweise ZTNA-Dienste, sichere Web-Gateways (SWG), Cloud Security Access Broker (CASB) und Firewall-as-a-Service (FWaaS).

Edge-Computing

Eine weitere wichtige Voraussetzung ist die Möglichkeit zur Bereitstellung von Anwendungen und Daten am Netzwerkrand, beispielsweise über ein Content Delivery Network (CDN), eine MEC-Infrastruktur oder ein IoT-Gateway. Allerdings bringt dies nur dann die angestrebten Vorteile, wenn die zuständigen IT-Mitarbeiter über effektive Tools zur Sicherung der komplexen und auf verschiedene Standorte verteilten Edge-Computing-Systeme verfügen und deren Funktionen genau auf die Erfordernisse des SASE-Modells abstimmen können.

Gerätemanagement

Da die Zahl der geschäftlich genutzten Mobilgeräte und mobilen Apps exponentiell wächst und der Netzwerkzugriff immer häufiger über Edge-Standorte erfolgt, sind die Verantwortlichen in den Unternehmen aufgefordert, die einzelnen Geräte und ihre Betriebssysteme effektiv zu kontrollieren und zu sichern.

2. Orchestrierung

Ein reibungsloses Zusammenspiel der verschiedenen Komponenten ist für das Funktionieren des SASE von größter Bedeutung.

Serviceverkettung

Die Möglichkeit zur Serviceverkettung ist eine der wichtigsten Funktionen eines SASE, da sich auf diese Weise die Bereitstellung und das Nutzererlebnis der betreffenden Dienste verbessern und optimieren lassen. In virtuellen Netzwerken ist dafür umfangreiches Wissen über die automatisierte Bereitstellung vernetzter Dienste mithilfe von Orchestrierungstools erforderlich.

Optimierung

Da derzeit kein Anbieter in der Lage ist, eine ausschließlich auf eigenen Produkten basierende SASE-Lösung bereitzustellen, müssen die Unternehmen Technologien und Lösungen verschiedener Anbieter kombinieren, um den gewünschten Funktionsumfang realisieren zu können. In diesem Zusammenhang erweist es sich als Vorteil, wenn die Verantwortlichen in der Lage sind, das Zusammenspiel von neuen und bestehenden Komponenten zu optimieren.

Leistungsprüfung

Um sicherzustellen, dass die Komponenten der komplexen, multifunktionalen SASE-Umgebung nahtlos ineinandergreifen und tatsächlich die gewünschte Leistung bieten, sind umfassende Tests unerlässlich. Daher benötigen IT-Teams moderne Tools, mit denen sie entsprechende Untersuchungen durchführen und das Zusammenwirken und die Konfiguration der bereitgestellten Funktionen auf effiziente Weise überprüfen können.

3. Teamübergreifende Zusammenarbeit

Obwohl die Aufgabenbereiche der Netzwerk- und Sicherheitsteams im Laufe der letzten zehn Jahren immer stärker aufeinander abgestimmt wurden, agieren die meisten weiterhin als voneinander unabhängige Organisationseinheiten. In diesem Fall muss vor dem Aufbau eines SASE das Management der Sicherheitssysteme und Netzwerke in der Produktionsumgebung neu strukturiert werden, um die beiden Bereiche durch die Implementierung einheitlicher Administrationsprozesse näher zusammenzuführen. Diesbezüglich ähnelt die Umstellung auf ein SASE-Modell der Einrichtung kombinierter Netzwerk- und Telekommunikationsinfrastrukturen in den 1990er Jahren.

Abgesehen davon sollten CIO und CISO unbedingt die Aufteilung ihrer jeweiligen Rollen hinsichtlich des Betriebs und Managements der Unternehmensinfrastruktur überdenken. Denn da das SASE-Modell immer noch weiterentwickelt und verfeinert wird, lässt sich nur durch die Schaffung von teamübergreifenden Zuständigkeiten sicherstellen, dass die SASE-Strategie des Unternehmens aktuell und in Zukunft durch ein koordiniertes Vorgehen der Netzwerk-, Sicherheits- und Anwendungsarchitekten und anderer Fachkräfte umgesetzt werden kann.

4. Expertise

Jedes erfolgreiche SASE-Implementierungsprojekt setzt umfangreiches Wissen über Netzwerke, SD-WANs und virtuelle Anwendungen, Sicherheit und Geräte voraus. Dabei müssen die beteiligten IT-Experten insbesondere mit vertieften Kenntnissen rund um Cloud- und Sicherheitsarchitekturen sowie MPLS und andere Netzwerkprotokolle aufwarten können. Falls die entsprechenden Skills nicht im eigenen Unternehmen vorhanden sind, ist es empfehlenswert, die Unterstützung eines Partners zu suchen, der sich bis ins Detail mit den verschiedenen Technologien und ihren spezifischen Funktionen in der SASE-Infrastruktur auskennt.

Verizon als Wegbereiter: unser SASE-Ansatz

Verizon stellt seit über 10 Jahren SASE-ähnliche Dienste bereit und investiert kontinuierlich in diesen Bereich. Zugleich pflegen wir wichtige Partnerschaften zu renommierten Anbietern, die uns in die Lage versetzen, moderne Unternehmen bei der Einrichtung sicherer Zugriffsmöglichkeiten für ihre auf diverse Standorte verteilten Teams, Datenbestände, Endpunkte, Anwendungen und Dienste zu unterstützen.

Deshalb bezeichnen wir unser SASE-Angebot als „Best-of-Suite"-Paketlösung, deren marktgängige Features und Funktionen ideal zusammenpassen und sich nahtlos mit unseren sonstigen Technologien und Services integrieren lassen.

Mit diesem Ansatz können wir Kunden bei der Wahl des richtigen Netzwerks, der richtigen SD-WAN-Richtlinien und des richtigen Cloud-Sicherheitsanbieters beraten und alle erforderlichen Komponenten in Form eines von unseren Experten verwalteten Dienstes bereitstellen.

Verizon als Vorreiter bei wichtigen Schlüsseltechnologien

Anerkennung durch Branchenexperten

Die Netzwerk- und Sicherheitsservices von Verizon stehen bei Branchenanalysten seit Langem hoch im Kurs und haben uns schon viele Auszeichnungen eingebracht. So werden wir seit nunmehr 14 Jahren im „Gartner Magic Quadrant for Network Services, Global"[7] und seit sieben Jahren im „Gartner Magic Quadrat for Managed Security Services, Worldwide"[8] als Leader aufgeführt. Zugleich war Verizon in den letzten drei Jahren der einzige Telekommunikationsanbieter, der sowohl im „Magic Quadrant for Network Services" als auch im „Magic Quadrant for Managed Security Services als Leader" erscheint.

Parallel dazu hat sich unser „Data Breach Investigations Report (DBIR)" mit seinen präzisen Analysen, Zahlen und Fakten zu aktuellen Cyber-Sicherheitstrends in den letzten zehn Jahren zu einer von Sicherheitsexperten, Managern und Unternehmensvertretern aus allen Branchen geschätzten Informationsquelle entwickelt.

Edge-Computing

Da immer mehr Anwendungen aus den unternehmenseigenen Rechenzentren in die Cloud und auf Edge-Systeme verlagert werden, muss eine moderne SASE-Lösung bestehende Datensicherheitsvorgaben auch in verteilten Netzwerken durchsetzen können. Aus diesem Grund sichert Advanced SASE von Verizon neben den unternehmensintern gehosteten Anwendungen auch und vor allem die über Edge-Infrastrukturen und die Cloud bereitgestellten Apps. Konkret bedeutet das, dass in das Netzwerk integrierte Sicherheitsfunktionen die übertragenen Daten vom Anfangs- bis zum Endpunkt der Verbindung umfassend schützen.

Virtual Network Services

Unsere branchenführenden Virtual Network Services (VNS) bieten Unternehmen eine skalierbare Plattform, die über leistungsstarke Orchestrierungsfunktionen verfügt, von unseren Experten verwaltet wird und physische Datenverbindungen in ein virtuelles On-Demand-Netzwerk verwandelt. Dabei profitieren die Kunden nicht nur von den Kostenvorteilen und der gesteigerten Flexibilität einer SDN-Infrastruktur, sondern auch von virtualisierten Routing-, SD-WAN- und WAN-Optimierungsdiensten.

Internet der Dinge

Unsere umfassende Expertise im Bereich IoT findet immer wieder die Anerkennung von Branchenanalysten. Beispielsweise wurden wir im „Gartner Magic Quadrant for Managed Security Services 2020, Worldwide" als Leader eingestuft.[9] Auf diese Weise wird honoriert, dass die professionellen 5G-, MEC- und IoT-Beratungsdienste von Verizon modernen Unternehmen tatkräftige Unterstützung beim Aufbau innovativer Lösungen zur Realisierung visionärer Projekte bieten.

Gerätemanagement

Bei der Einrichtung eines SASE muss eine große Zahl von geschäftlich genutzten Geräten und Anwendungen mitsamt den dafür erforderlichen Managementtools in die neue Infrastruktur integriert werden. In diesem Zusammenhang erweist es sich als Vorteil, dass wir IT-Administratoren leistungsstarke Funktionen für die Verwaltung, Erfassung und Kontrolle aller mit dem Netzwerk verbundenen Geräte und Dienste bereitstellen.

7. Gartner Magic Quadrant for Network Services, Global. Veröffentlicht am: 20. Februar 2020. Analysten: Neil Rickard | Bjarne Munch | Danellie Young. In früheren Jahren erschien Verizon als: Leader im Magic Quadrant for Network Services, Global (2015–2020); Leader im Magic Quadrant for Global Network Service Providers (2011–14); unter dem Namen „Verizon Business" im Magic Quadrant for Global Network Service Providers (2007, 2009–2010); ebenfalls unter dem Namen „Verizon Business" im Magic Quadrant for Managed and Professional Network Service Providers (North America 2008).
8. Gartner Magic Quadrant for Managed Security Services. Veröffentlicht am: 2. Mai 2019. Analysten: Toby Bussa | Kelly M. Kavanagh | Sid Deshpande | Pete Shoard.
9 Gartner Magic Quadrant for Managed Security Services, Worldwide. Veröffentlicht am: 12. Dezember 2019. Analysten: Pablo Arriandiaga | Eric Goodness | Leif-Olof Wallin | Jonathan Davenport.

Umfassende Expertise und Erfahrung

Unsere Expertenteams kennen sich bestens mit den zum Aufbau eines SASE erforderlichen Schlüsseltechnologien aus.

Seit Längerem ist zu beobachten, dass moderne Unternehmen aller Größen vielfältige Cloud-, Netzwerk- und Sicherheitstechnologien anschaffen. Zugleich zeigt sich, dass vielerorts noch nicht die für die Zusammenführung dieser Innovationen erforderlichen Voraussetzungen gegeben sind, weil keine Integrations- und Managementlösungen für derart komplexe Umgebungen zur Verfügung stehen.

Deshalb bieten wir unseren Kunden Unterstützung durch erfahrene Netzwerk- und IT-Sicherheitsexperten, die aufgrund ihrer reichen Erfahrungen und umfassenden Kenntnisse in der Lage sind, die verschiedenen Komponenten eines SASE zu verwalten, zu orchestrieren und zu optimieren.

Unsere Managed Services vereinfachen die Einrichtung und den Betrieb eines SASE und reduzieren dadurch den mit dem Schutz eines modernen Unternehmens verbundenen Arbeits- und Ressourcenaufwand.

Für die erfolgreiche Implementierung eines SASE ist ein detaillierter Überblick über die jeweiligen Betriebsumgebungen, Leistungsanforderungen und Sicherheitsprofile der verschiedenen Komponenten erforderlich.

Insofern ist es ein nicht zu unterschätzender Vorteil, dass Verizon als führender Anbieter von Netzwerk- und Sicherheitsdiensten über umfassende Beratungs- und Unterstützungsmöglichkeiten verfügt, die in der Branche ihresgleichen suchen. Dieses solide Fundament versetzt uns in die Lage, die branchenführenden Produkte verschiedener Anbieter zu einer SASE-Paketlösung zu kombinieren und dadurch die Bereitstellungs- und Betriebsprozesse erheblich zu vereinfachen.

Wir helfen Unternehmen dabei, das SASE-Modell möglichst effektiv vor dem Hintergrund ihrer spezifischen Anforderungen umzusetzen.

Viele SASE-Produkte auf dem Markt stammen nicht von Managed-Services-Spezialisten, sondern von Hardwareanbietern, die (aus naheliegenden Gründen) behaupten, ihre Lösung erfülle alle erdenklichen Anforderungen.

Tatsächlich greifen diese rein technologiebasierten Lösungen „von der Stange“ in der Praxis oft zu kurz, weil sie nicht auf die spezifischen Herausforderungen und Zielsetzungen des Kunden abgestimmt sind. Um wirklich die richtige SASE-Lösung zu finden, empfiehlt sich die Zusammenarbeit mit einem Anbieter, der branchenführende Technologien entsprechend der kundenspezifischen Vorgaben kombinieren kann und eine zentrale Managementplattform für den gesamten Stack zur Verfügung stellt. Verizon ist in dieser Hinsicht bestens positioniert.

Wir verfügen über die nötige Erfahrung in den Bereichen Orchestrierung und Optimierung, um das volle Potenzial des SASE-Ansatzes freisetzen zu können.

Moderne IT-Umgebungen sind so ausgedehnt und komplex, dass die Verantwortlichen vielerorts kaum mehr in der Lage sind, die eigene Netzwerkplattform effektiv zu verwalten und zu schützen.

Das gilt insbesondere für technisch ausgereifte SD-WAN-Dienste, deren volles Potenzial erst dann freigesetzt wird, wenn sie genau auf den Anwendungsbestand des Unternehmens abgestimmt wurden. Hierfür ist nicht nur ein umfassendes Wissen über Anwendungsarchitekturen im Allgemeinen, sondern auch eine genaue Kenntnis der spezifischen Apps und ihrer jeweiligen Rolle und Bedeutung im Geschäftsbetrieb erforderlich.

Bei der Bewältigung dieser Herausforderungen sind die Experten von Verizon klar im Vorteil, weil sie bei der Zusammenarbeit mit einer Vielzahl von Unternehmen reiche Erfahrungen mit der Implementierung, Orchestrierung und Optimierung der verschiedenen SASE-Komponenten gesammelt haben.

Wir stellen jedem Kunden einen zentralen Ansprechpartner sowie einheitliche Überwachungs- und Berichtsfunktionen für die gesamte Lösung zur Verfügung.

Derzeit konzentrieren die meisten Anbieter sich bei der Präsentation ihrer SASE-Lösungen ausschließlich auf die Sicherheitskomponenten und lassen den Konnektivitätsaspekt stillschweigend unter den Tisch fallen. Doch in der Praxis lässt sich das eine nicht vom anderen trennen. Denn um ein lückenloses Bild der Leistung und Sicherheit aller Netzwerkverbindungen zu liefern, müssen die Netzwerkplattform und die Sicherheitskomponenten eng aufeinander abgestimmt sein und im Rahmen eines holistischen Ansatzes bereitgestellt werden. Genau das tut Verizon.

Immer die passende Lösung

Unsere SASE-Lösung basiert auf einem bewährten Ansatz, der jedem Unternehmen das gewünschte Maß an Vereinfachung, Optimierung und Orchestrierung bietet.

Einer der wichtigsten Vorteile unserer umfassenden SASE-Paketlösung ergibt sich aus der Tatsache, dass die vom Kunden erwartete Leistung, Flexibilität und Sicherheit im Rahmen eines ganzheitlichen Managed Service bereitgestellt werden. Das erleichtert die Implementierung des SASE und entlastet das Unternehmen von der Verwaltung einzelner Komponenten.

Außerdem profitieren die IT-Mitarbeiter von ausführlicheren Berichten, einer lückenlosen Überwachung, strafferen Managementprozessen und flächendeckenden Sicherheitsmaßnahmen, da die SASE-Lösung von den Experten von Verizon orchestriert, getestet und optimiert wird. Das bestärkt uns in unserer Überzeugung, dass Kundenunternehmen nach Möglichkeit den gesamten SASE-Stack aus einer Hand beziehen und die Administration und Optimierung ihrer Netzwerk- und Sicherheitsinfrastruktur an einen zentralen Anbieter abgeben sollten.

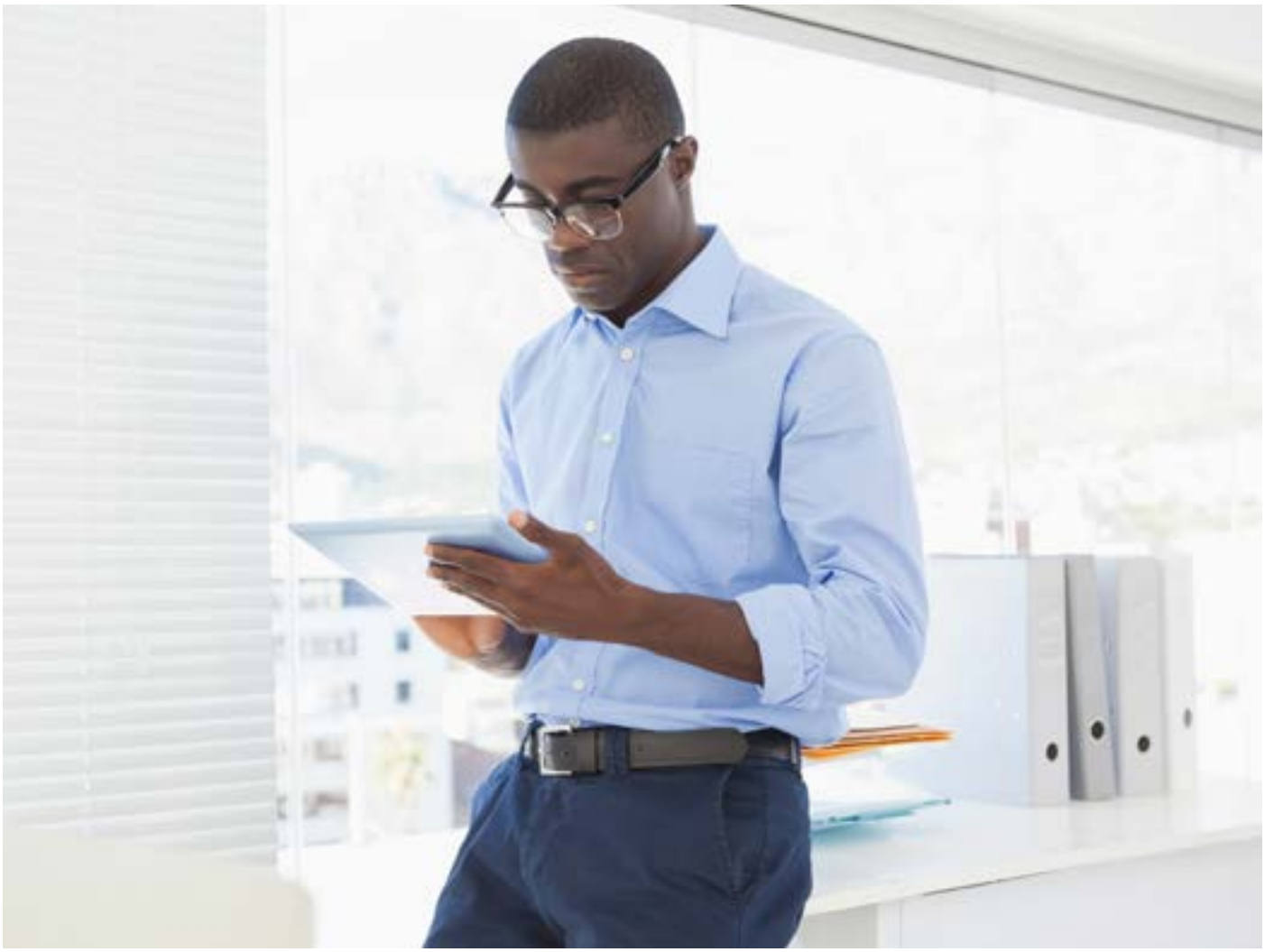
Unser breites Spektrum an Konfigurationsoptionen und Punktlösungen bietet Kundenunternehmen ein Höchstmaß an Flexibilität.

Falls Ihre Firma vertraglich an bestimmte Anbieter gebunden ist oder durch technologische Altlasten und eingebettete Services an der Modernisierung der eigenen IT-Umgebung gehindert wird, finden Sie in unserem Angebot zahlreiche branchenführende Punktlösungen, mit denen Sie vorhandene Lücken schließen und eine SASE-Infrastruktur mit vollem Funktionsumfang einrichten können. Auch in diesem Fall profitieren Sie von unserer reichen Erfahrung in Sachen SASE-Orchestrierung und -Management, sodass jederzeit sichergestellt ist, dass die Lösungen der verschiedenen Anbieter nahtlos ineinandergreifen.

Wir haben noch viel vor

Wir von Verizon sind ständig darum bemüht, unser SASE-Angebot durch die kontinuierliche Optimierung der Bereitstellungsprozesse und zusätzliche Unterstützungsleistungen noch besser zu gestalten. Beispielsweise arbeiten wir derzeit an der Zusammenlegung unserer Network Operations Center (NOC) und Security Operations Center (SOC), um die Verschmelzung von Netzwerk- und Sicherheitsdiensten weiter voranzutreiben.

Und weil wir wissen, wie wichtig strikte Servicelevelvereinbarungen (SLAs) bei komplexen technologischen Umstellungen sind, etablieren wir derzeit neue SLAs, die speziell für die Implementierung und den Betrieb von SASE-Infrastrukturen konzipiert wurden.



Ebnen Sie Ihrem Unternehmen den Weg in die Zukunft

Die Zeit ist reif für die Zusammenführung Ihrer Netzwerk- und Sicherheitsdienste – und die Zeichen standen noch nie so günstig. Zwar lässt sich nicht leugnen, dass der Umstieg auf das SASE-Modell die Abkehr von konventionellen Netzwerk- und Sicherheitsstrategien verlangt. Doch zugleich eröffnet er Ihren IT-Experten die Möglichkeit, bestehende Infrastrukturen von Grund auf neu zu gestalten.

Wenn Sie die Netzwerk- und Sicherheitssysteme Ihres Unternehmens miteinander integrieren, stärken Sie Ihre Cyber-Abwehr und profitieren unmittelbar von spürbaren Vorteilen in puncto Leistung und Flexibilität. Das erleichtert Ihnen nicht zuletzt die Umsetzung längerfristiger, breit angelegter Initiativen zur Umstellung auf digitale Geschäftsmodelle, cloudnative IT-Lösungen, Edge-Computing und andere wegweisende Technologien und Ansätze.

Allerdings benötigen Sie für den erfolgreichen Aufbau einer solchen SASE-Infrastruktur einen Partner, der das komplexe Angebot an einschlägigen Netzwerk- und Sicherheitslösungen jederzeit überblickt und Ihnen bei der Auswahl der für Ihre Anforderungen passenden Features mit Rat und Tat zur Seite steht. Dabei kommt es vor allem auf die Fähigkeit zur Bereitstellung leistungsstarker Netzwerk- und Konnektivitätslösungen sowie zur nahtlosen Integration aller erforderlichen Sicherheitstechnologien an – auch wenn einige Neulinge auf dem SASE-Markt anderes behaupten.

Verizon zählt zu den wenigen Anbietern, die über die dafür nötige Erfahrung und Expertise verfügen. Dank unserer marktführenden Lösungen und der leistungsstarken Produkte unserer zahlreichen Partner sowie aufgrund unserer Vorreiterrolle in den Bereichen Netzwerklösungen, SD-WAN, Sicherheit und Gerätemanagement sind wir bestens positioniert, um Kundenunternehmen integrierte SASE-Dienste aus einer Hand bereitzustellen.

Wenn Sie mehr über Advanced SASE von Verizon erfahren möchten, sprechen Sie mit Ihrem Business Account Manager oder klicken Sie hier >