Leitfaden

SASE: einen Schritt voraus

Wie ein auf Secure Access Service Edge (SASE) basiertes Modell in einer dynamischen Geschäftswelt zum Turbo für Sicherheit und Geschwindigkeit wird.



verizon business

Das Wichtigste in Kürze

- Secure Access Service Edge (SASE) trägt zur Stärkung der Sicherheit bei, indem es Zero-Trust-Prinzipien in alle Aspekte des hybriden Betriebs einbettet. Zudem stärkt es die Resilienz gegenüber Naturkatastrophen, Kabelausfällen und ähnlichen Störungen.
- Durch die sichere Ausführung von Workloads und die Verarbeitung von Daten am Netzwerk-Edge reduziert SASE die Latenz, sodass neue Tools ihr volles Potenzial entfalten können.
- SASE bietet Unternehmen die Flexibilität, in neue Märkte vorzudringen, Richtlinien angemessen anzuwenden und neue Systeme und Nutzerkonten rasch in ihre Infrastrukturen einzufügen.
- Mit den in seine flexible Architektur integrierten Sicherheitsmechanismen reduziert SASE zudem die mit der Nutzung von KI-Tools verbundenen Risiken.

Kontext:

Wir können heutzutage von nahezu überall aus arbeiten. Für Unternehmen bedeutet das, dass sie alle Verbindungen am Rand ihres Unternehmensnetzwerks sichern müssen. Zudem sollten sie die Resilienz stärken – besonders, wenn sie einen Teil ihrer Betriebsprozesse in die Cloud verlagert haben. Das darf jedoch nicht zulasten der Flexibilität gehen, wenn sie in einem schnelllebigen Markt wettbewerbsfähig bleiben möchten.

Lösung:

Ein SASE-Framework mit einem softwaredefinierten Weitverkehrsnetzwerk (SD-WAN), Secure Service Edge und Zero-Trust-Zugriffsmanagement ist ein unverzichtbarer Bestandteil einer modernen Unternehmensinfrastruktur. Wenn die Zugangspunkte am Rand eines Unternehmensnetzwerks gesichert und für eine optimale Leistung konfiguriert sind, können Unternehmen ihren Mitarbeitern mehr Flexibilität dabei bieten, wie und wo sie arbeiten. Zudem sind sie bei der Technologieauswahl weniger eingeschränkt und können ihre Geschäftsziele souveräner verfolgen.





Die Unternehmenssicherung am Edge sollte Priorität haben

Die moderne Geschäftswelt ist schnelllebiger und mobiler als je zuvor. Doch die neuen Technologien, mit denen wir vernetzt und produktiv bleiben, bringen neue Anforderungen an die Sicherheit mit sich.

Inzwischen ist es normal, sich mit einem Laptop an einen beliebigen Ort zu setzen und von dort aus zu arbeiten. Viele von uns denken gar nicht mehr darüber nach, ob sie zuhause, in einem Co-Working-Space oder sogar auf dem Weg zur Arbeit sichere Anwendungen aufrufen sollten oder lieber nicht. Wenn Sie in einem Bereich wie dem Gesundheitswesen oder der Fertigung arbeiten, sind Sie es vermutlich gewohnt, nahezu in Echtzeit auf Daten zum Gesundheitszustand von Patienten oder zum Wartungszustand von Maschinen zuzugreifen.

Viele Mitarbeiter und Kunden in aller Welt nutzen Workloads, die am Netzwerk-Edge ausgeführt werden. Diese Abhängigkeit vom Edge-Computing – also von der Verteilung von Rechenressourcen an den Rand von Unternehmensnetzwerken – ist jedoch eine relativ neue Entwicklung. Die Sicherheitsarchitektur, die zum Schutz von Daten und Menschen am Edge erforderlich ist, wurde erst 2019 formell von Gartner definiert.[1] Damit reagierten die Branchenanalysten auf die steigende Nutzung von Geräten im Internet der Dinge (IoT) und Remote-Arbeit.

Diese inzwischen kritische Architektur wird als SASE bezeichnet.

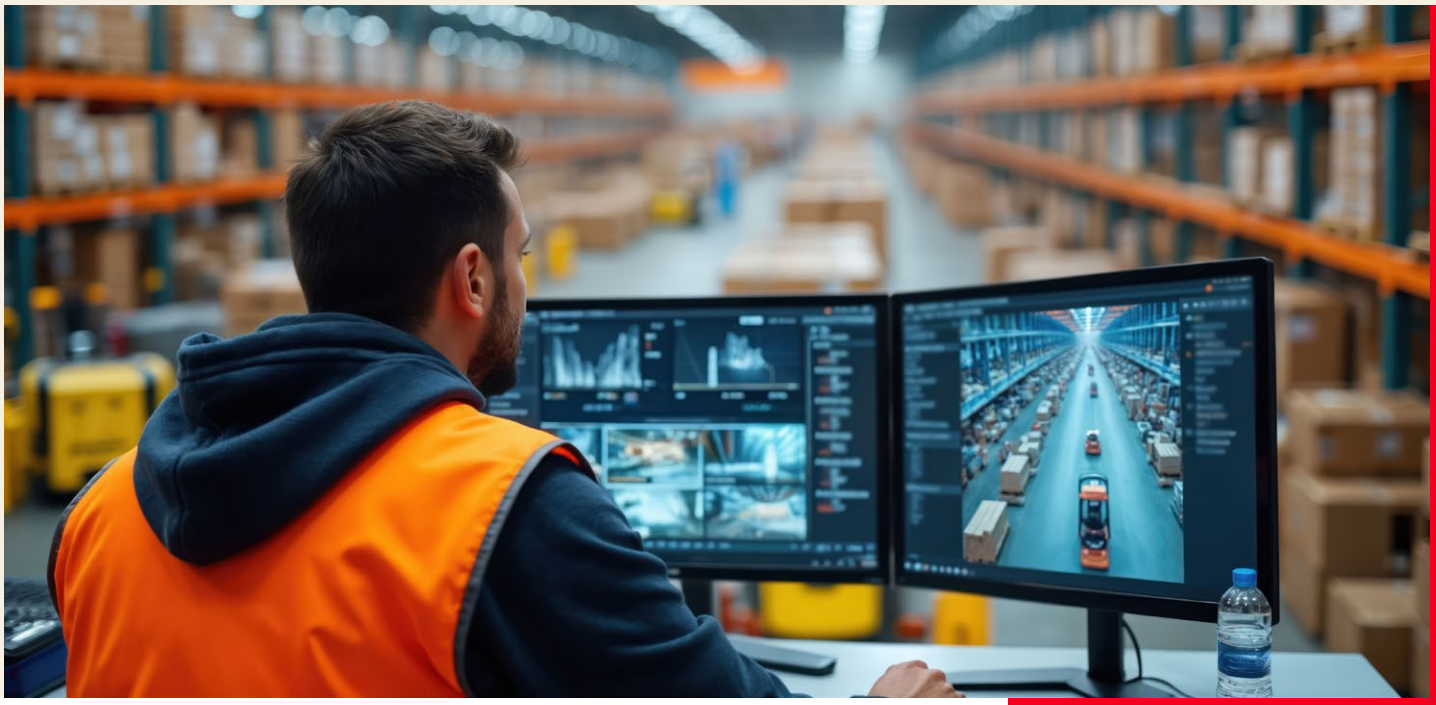
Sie kommen wahrscheinlich täglich mit SASE-Komponenten in Kontakt. In einer verteilten, schnelllebigen und KI-gestützten Geschäftswelt sind diese Sicherheitsmaßnahmen unverzichtbar, denn wenn nicht nur Menschen, sondern auch KI-Tools von überall aus in Echtzeit auf Ihr Unternehmensnetzwerk – den unsichtbaren Motor für so gut wie alle Aspekte der Produktivität – zugreifen können, wären zentralisierte Firewalls oder manuelle Prüfungen viel zu langsam.

Neue agentische KI-Tools, die sofortigen, autonomen Zugang zu Daten verlangen, steigern den Druck auf die Edge-Sicherheit nur noch – Ganz zu schweigen von KI-Algorithmen, die aus ihren kontrollierten Umgebungen entweichen und autonom unerwünschte Dinge tun.[2]

Machen wir uns nichts vor: Inzwischen arbeiten alle Unternehmen in einem Umfeld, das von unerwarteten Störungen, Innovationen und immer neuen Cyberrisiken geprägt ist. Ein sicheres, resilientes Netzwerk, das befugten Nutzern und KI-Tools weiterhin ein ungebremstes und flexibles Arbeiten ermöglicht, ist vor diesem Hintergrund ein echter Wettbewerbsvorteil.

Genau das macht SASE unverzichtbar.

> „Wir leben in einer datengestützten Welt. Die Integrität dieser Daten muss unter allen Umständen gewahrt bleiben."
>
> **Colin Wilson**
> Enterprise Architect,
> Verizon Business



Was genau ist SASE? Und warum ist es so wichtig?

Der Übergang zu einer vorrangig cloudbasierten Arbeitsweise hat die Geschwindigkeit und Effizienz gesteigert, aber auch die herkömmlichen Ansätze für die Unternehmenssicherheit infrage gestellt.

Alistair Neil, Managing Director of Advanced Solutions, International bei Verizon Business, erklärt: „Um 2007 herum begann die Migration in die Cloud. Heute ist die überwältigende Mehrheit der IT-Infrastrukturen cloudbasiert. Unternehmen mussten ihre generell hardwarebasierten Sicherheitsmodelle schnell und grundlegend überarbeiten, um dieser neuen Situation Rechnung zu tragen. [...] SASE ist die Integration von Netzwerk- und Sicherheitsfunktionen, die aus der Cloud für die Cloud bereitgestellt werden."

SASE ist in vielen verschiedenen Branchen im Einsatz und stellt Sicherheitsmechanismen als Cloud-Dienst für Verbindungen am Netzwerk-Edge (statt auf einem zentralen Server) bereit.

Cloud-Nutzern war natürlich bereits bewusst, dass die Datenverarbeitung und -speicherung in der Nähe der Datenquellen die Latenz drastisch reduzieren würde. Ohne SASE wäre diese Arbeitsweise jedoch nicht umsetzbar.

In einem SASE-Modell müssen Nutzer, Geräte und IoT-Hardware in einem Unternehmens-WAN (Weitverkehrsnetzwerk) ihre Identität und Compliance belegen können, bevor sie Zugang erhalten. SASE bietet mehr Unabhängigkeit und schnellere und flexiblere Kontrollen als eine zentrale Firewall, die das gesamte Netzwerk schützen soll.

Ohne sicheres Edge-Computing würden autonome Fahrzeuge auf unseren Straßen Zukunftsmusik bleiben. KI-Assistenten auf Mobilgeräten wären ohne SASE ein zu großes Risiko für die professionelle Nutzung. Sogar die Fernüberwachung von Maschinen und Anlagen wäre ohne SASE sehr viel schwieriger und zeitaufwendiger.

Unsere moderne Welt wäre ohne komplexe Multi-Cloud-Umgebungen undenkbar. SASE trägt dazu bei, sie vor Cyberkriminellen zu schützen, die die Schwachstellen in diesen Umgebungen ausnutzen wollen.

Die Komponenten von SASE

SD-WAN

Das softwaredefinierte (und typischerweise virtualisierte) WAN, in dem Daten durch verschlüsselte Overlay-Tunnel an das Edge übertragen werden.

Secure Service Edge

Ein cloudorientierter Sicherheitsrahmen, der Firewall-as-a-Service, sichere Gateways und Sicherheitsbroker (CASB) umfasst.

Zero-Trust-Zugriff

Das Prinzip „nie blind vertrauen, immer verifizieren" in Aktion, mit der Beschränkung auf die absolut erforderlichen Zugriffsrechte und Authentifizierung an jedem Zugangspunkt.

Wie funktioniert Zero-Trust-Sicherheit im KI-Zeitalter?

Zero Trust ist eine der Kernkomponenten von SASE. Nutzer, Geräte und KI-Tools sollten nicht einfach auf alles in Ihrem Unternehmensnetzwerk zugreifen dürfen. Schließlich lassen Sie auch keine Fremden ungehindert von der Straße in Ihr Büro wandern.

Neil führt aus: „Wie bewegen Sie sich in einer SASE-Umgebung? Identitäten und Zugriffe müssen kontinuierlich überwacht und bei jedem Schritt authentifiziert werden."

„Das ist am besten mit einem Flughafen zu vergleichen. Dort zeigen Sie Ihre Bordkarte und Ihren Pass, gehen durch die Sicherheitskontrolle zu Ihrem Gate und legen Ihre Dokumente dort erneut vor. Die Angestellten vergewissern sich, dass Sie tatsächlich auf ‚Sitz 35A' gebucht sind. Überall, wo Sie hingehen, müssen Sie nachweisen, wer Sie sind, wie Sie dort hingelangt sind und wohin Sie wollen."

Zero-Trust-Sicherheit erfordert, dass alle Nutzer und Dinge, die auf ein Netzwerk zugreifen, ihre eigene Identität haben. Während am Flughafen das Foto im Pass mit dem Gesicht des Passagiers verglichen wird, gleicht ein Zero-Trust-System den Nutzernamen, das Passwort und zum Beispiel Biometriedaten mit dem entsprechenden Eintrag in seiner Datenbank ab. Ein solches System sollte zudem Echtzeit-Kontextinformationen (wie die Uhrzeit und den Standort) nutzen, um die Legitimität der Verbindung zu beurteilen. An unserem Beispielflughafen würden Sie nicht durch die Sicherheitskontrolle kommen, wenn Ihr Flug laut Bordkarte erst am nächsten Tag startet.

Die steigende Nutzung von KI-Tools und -Agenten stellt diese etablierte Methode jedoch auf eine harte Probe.

Neil sagt: „Ich glaube nicht, dass die Konsequenzen in Unternehmen wirklich durchdacht werden. Im Kontext der KI besteht die Sicherheit aus so vielen Ebenen."

Wilson fügt hinzu, dass die Verwaltung der KI-Sicherheit kein rein technisches Problem ist. „Die Herausforderung bei wirklich autonomen Systemen besteht darin, dass keine Menschen da sind, die eingreifen könnten. Sie müssen also von Anfang an strenge Governance-Richtlinien für die Nutzung von Tools durch KI-Agenten einbauen."

Zero-Trust-Prinzipien können auf KI-Tools und autonome Agenten genauso angewendet werden wie auf Nutzer. Voraussetzung ist allerdings, dass Sie jedem KI-Agenten, jedem KI-Browser, jeder autonomen Hardwarekomponente usw. eine eigene Identität zuweisen und dass Ihre Sicherheitsmechanismen den Kontext ihrer Aktivitäten richtig interpretieren können.

KI-Tools, die außerhalb Ihrer Region entwickelt und betrieben werden, können ein erhebliches Risiko darstellen, denn ihre Funktionsweise ist Ihnen möglicherweise unbekannt und erschwert die Rekonstruktion von Datenflüssen. Neil empfiehlt Unternehmen in Branchen wie der Rüstungsindustrie, dem Finanzwesen und dem öffentlichen Sektor, digitale Inseln einzurichten und KI-Tools nur in den dort isolierten Systemen laufen zu lassen.

Ebenso wichtig ist eine sicherheitsbewusste, auf Zero Trust basierte Unternehmenskultur, um die Datenhoheit zu wahren. Um agentische KI wirklich zu verstehen und sicher zu nutzen, müssen Sie nicht nur wissen, wo KI-Agenten im Einsatz sind und worauf sie Zugriff haben, sondern auch deren Aktivitäten kontinuierlich überwachen und die Richtlinien bei der Ausführung rigoros durchsetzen.

Sicherheitsfragen rund um KI

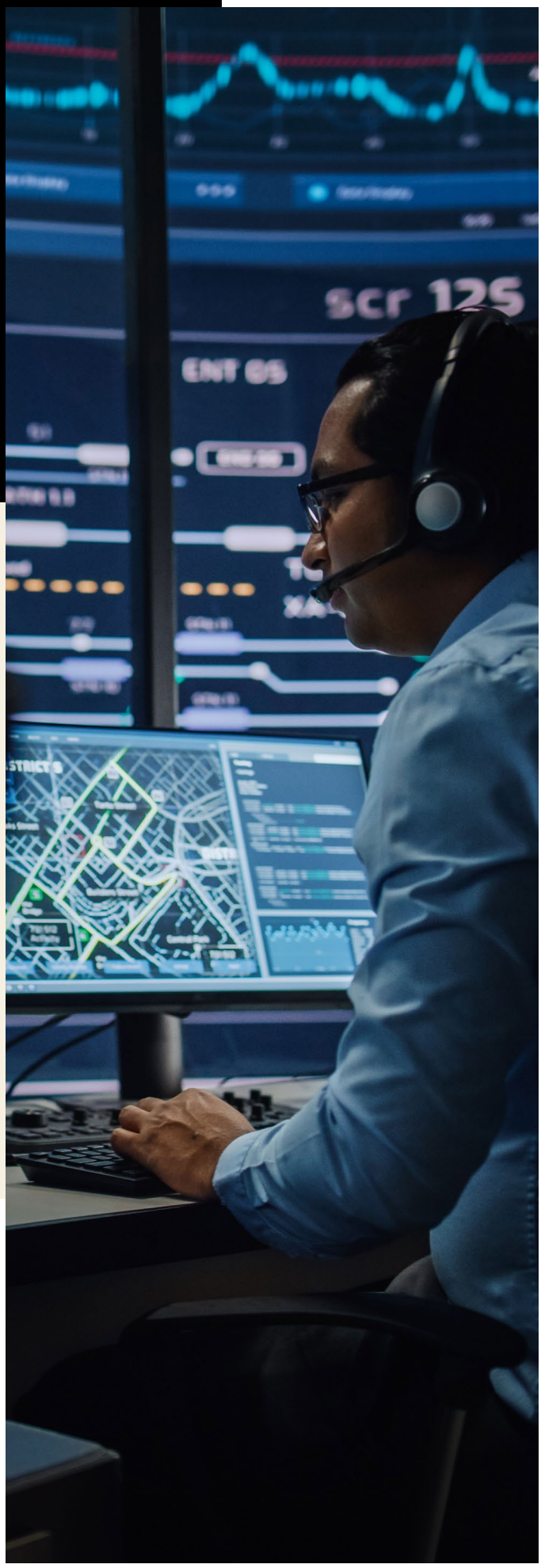
Wie gut sind Daten vor unbefugten Zugriffen durch eigenmächtig handelnde KI und externe Angreifer geschützt?

Ist die Datenhoheit Ihres Unternehmens gegeben? Halten Sie die für Ihre Standorte geltenden Datenhoheitsvorschriften ein?

Könnten Daten unabsichtlich versandt oder ausgeschleust werden?

Ist das Modell selbst sicher und vor Prompt-Injection geschützt?





Dient SASE nur der Sicherheit?

SASE wurde entwickelt, um unbefugte Zugriffe auf Unternehmensnetzwerke zu unterbinden. Das ist jedoch nicht der einzige Grund, es in Ihrem Unternehmen einzusetzen.

Mit SASE können Unternehmen flexibler und resilienter werden und in manchen Fällen sogar Bereiche identifizieren, in denen sie effizienter arbeiten und möglicherweise Kosten einsparen können.

SASE ermöglicht den flexiblen, cloudbasierten Zugriff auf Netzwerkressourcen und Sicherheitsmechanismen und trägt damit zum Erreichen diverser Geschäftsziele bei, stellt aber gleichzeitig sicher, dass Ihr Unternehmen vor bekannten und neuen Bedrohungen geschützt ist. Wenn es von einem Tier-1-Partner wie Verizon Business bereitgestellt wird, der Netzwerksicherheit und Netzwerkleistung in einem Dienstpaket anbieten kann, sind die Vorteile noch größer.

Die SASE-Lösung von Verizon reduziert die Komplexität, die mit der Verwaltung mehrerer Tools in verschiedenen Netzwerken einhergeht, und kann IT-Teams damit wertvolle Zeit einsparen. Wenn Sie weniger Zeit mit der Reaktion auf Vorfälle verbringen und nur einen Vertrag verwalten müssen, können Sie die so gewonnene Zeit und die freigesetzten Finanzmittel und Kapazitäten in Geschäftsbereichen nutzen, die das Unternehmenswachstum vorantreiben.

> „SASE bietet Ihnen sehr viel Flexibilität. Es umfasst ein ganzes Spektrum an Sicherheitsmechanismen, mit denen Sie sich selbst, Ihre Geräte und Ihr Unternehmen schützen können. Zudem kann alles zentral verwaltet werden, was das koordinierte Richtlinien- und Konfigurationsmanagement enorm vereinfacht.“
>
> **Alistair Neil**
> Managing Director, Advanced Solutions International, Verizon Business.



Wie macht SASE unser Unternehmen agiler?

Wenn Unternehmen wachsen, neue Niederlassungen eröffnen und Nutzerkonten und Tools für die Fernarbeit einrichten, stehen die IT-Teams unter Druck, so schnell wie möglich die erforderlichen Richtlinien zu implementieren. Jenseits einer gewissen Größe sind die manuelle Hardware-Konfiguration und die Verwaltung mehrerer Verträge für Sicherheitssysteme nicht mehr tragbar.

Mit SASE können Unternehmen ihr Netzwerk-Edge sichern (sogar, während es wächst), um verteilte Belegschaften und Hybrid-Cloud-Anwendungen nahezu in Echtzeit zu schützen.

Wenn Netzwerkverkehr direkt (d. h. ohne den Umweg über ein zentrales und potenziell weit entferntes Unternehmensrechenzentrum) in die Cloud oder an den nächsten Edge-Node geschickt wird, sinkt die Latenz erheblich. Das verkürzt die Reaktionszeiten von Anwendungen und ermöglicht eine fast unverzügliche Ressourcenbereitstellung per Fernzugriff.

Einfach ausgedrückt können Sie schneller handeln, wenn Sie wissen, dass potenzielle Risiken bereits minimiert wurden.

SASE außerhalb des Büros nutzen

In Branchen wie der Fertigung, der Landwirtschaft und der Logistik spielt Betriebstechnologie (OT) eine entscheidende Rolle für den Routinebetrieb. Wenn diese OT mit der IT verbunden wird – zum Beispiel, weil IoT-Geräte oder smarte Sensoren installiert wurden –, muss sie stärker gesichert werden als dies traditionell der Fall war.

Das neue, breitere Netzwerk-Edge vergrößert die potenzielle Angriffsfläche, kann aber auch neue Möglichkeiten zur Betriebsoptimierung eröffnen, zum Beispiel durch vorausschauende Wartung und ein effizienteres Lieferkettenmanagement. Um diese sicher zu nutzen, sollten Sensoren, IoT-Geräte und andere OT mit demselben Zero-Trust-Ansatz und auf dieselbe Weise behandelt werden wie alle anderen Nutzer.

KI nutzen, aber flexibel bleiben

Der Übergang zu agentischer KI wird vielleicht noch größere Auswirkungen auf alle Aspekte der Netzwerkverwaltung in Unternehmen haben als die Einführung hybrider Arbeitsmodelle. Diese Agenten benötigen unglaublich niedrige Latenzen und eine enorme Bandbreite. Die damit einhergehenden Risiken können durch die Zusammenarbeit mit einem Tier-1-Partner wie Verizon Business minimiert werden, der ein umfassendes SASE-Programm bietet und sogar spezielle KI-Netzwerke unterstützen kann.

Wie kann Verizon Business helfen?

Verizon Business ist direkt mit über 100 Cloud-Anbietern weltweit vernetzt und kann Nutzer, Geräte und Anwendungen daher sicher von Edge zu Edge miteinander verbinden. Unser Tier-1-Internet-Peering senkt die Anzahl der Netzwerk-Hops und steigert die Effizienz. Mit Zusatzoptionen wie Secure Cloud Interconnect und Secure Digital Interconnect können Sie Ihre Kernanwendungen auf hochleistungsfähigen Infrastructure-as-a-Service-Plattformen ausführen.

Wir bieten weltweit Wahlmöglichkeiten für die physische und die virtuelle Konnektivität an. Diese flexiblen Optionen sind auch für unsere LAN- und WLAN-Lösungen verfügbar und können dazu beitragen, Ihr Netzwerk auf die steigenden Anforderungen hinsichtlich der Latenz vorzubereiten, die mit der wachsenden Anzahl von KI- und IoT-Tools am Netzwerk-Edge zu erwarten sind.



Wird SASE Ihren Geschäftsbetrieb resilienter machen?

Seit mehreren Jahren häufen sich schlagzeilenträchtige Cyberangriffe auf bekannte Unternehmen. Ein führender europäischer Autohersteller musste die Produktion für mehrere Monate stoppen und erlitt dadurch massive Verluste. Selbst Cybersicherheitsunternehmen sind nicht immun. Ein Angriff auf einen Softwareanbieter führte zu Ausfällen bei zahlreichen Kundenunternehmen, die Dienste dieses Anbieters nutzten.

Wir können zwar keine Aussagen über die genauen Ursachen dieser Sicherheitsverstöße machen, aber wir können sagen, dass die Angriffsfläche eines Unternehmens desto größer ist, je mehr Verbindungen zu seinem Unternehmensnetzwerk führen und je mehr Tools es nutzt. Durch den Einsatz von KI steigt das Risiko zusätzlich.

Alistair Neil führt aus: „Ganze Branchen müssen sich mit der Tatsache auseinandersetzen, dass Maschinen heute gezielt unbekannte Schwachstellen ausnutzen und Sekunden später Daten ausschleusen können. Die Herausforderung besteht darin, die Architektur so anzupassen, dass Ihre bereits vorhandene Infrastruktur geschützt ist und die Tools, die Sie benötigen, weiterhin genutzt werden können."

KI-Agenten müssen im Namen von Nutzern handeln, APIs aufrufen, Datenbankanfragen stellen und Daten zwischen Clouds übertragen, um die Effizienz zu steigern. Ein Rahmenwerk wie SASE bietet die unverzichtbare Authentifizierung und Governance, die verhindert, dass diese Tools auf Daten zugreifen, auf die sie nicht zugreifen sollten.

SASE kann auch zum Schutz vor der steigenden Menge und Vielfalt anpassungsfähiger Malware und überzeugender automatisierter Phishing-Angriffe beitragen. Mit SASE können Sicherheitsteams Threat-Intelligence-Updates unverzüglich an das Edge weiterleiten, damit Ihre Mitarbeiter informiert und sicher bleiben und das Unternehmen vor Zero-Day-Bedrohungen geschützt ist.

Außerdem entstehen durch die sichere Verteilung von Daten und Workloads an den Netzwerkrand zusätzliche Redundanzebenen, die dem Unternehmen im Bedarfsfall helfen können, sich schneller von unerwarteten Störungen wie Naturkatastrophen und Kabelausfällen zu erholen. Kurz gesagt hilft SASE Unternehmen beim Übergang von einer risikobehafteten zentralisierten zu einer resilienten, flexiblen Infrastruktur.

Wie kann Verizon Business helfen?

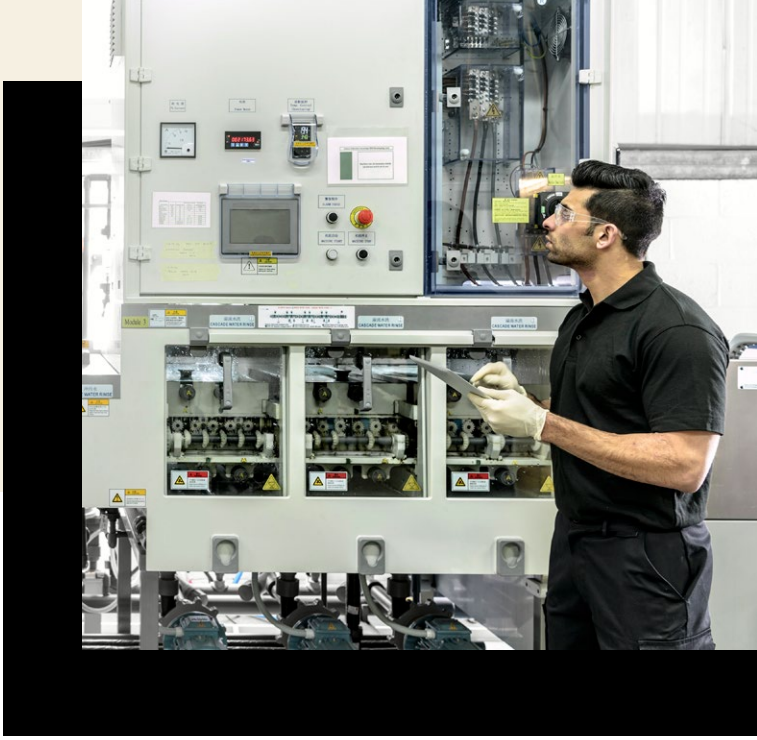
Unser 180 Länder umspannendes Tier-1-Netzwerk enthält redundante Komponenten und Sicherheitsmechanismen, die es skalierbar und stabil genug machen, um die Verfügbarkeit selbst bei Störungen wie durchtrennten Kabeln, Sicherheitsverstößen und Naturkatastrophen aufrechtzuerhalten.

Wir nutzen unsere umfassende Erfahrung im Risiko- und Sicherheitsmanagement, um Ihnen zu helfen, Risiken vorherzusehen und die Produktivität am Edge aufrechtzuerhalten – oder den Geschäftsbetrieb im schlimmsten Fall rasch wieder aufzunehmen. Unsere SASE-Lösung baut auf der belastbaren, sicheren, globalen Netzwerkinfrastruktur von Verizon Business auf und bietet Resilienz vor Ort.

Globale Überwachung für Ihre Sicherheit

Verizon betreibt ein globales Netzwerk, das von Security Operations Centers (SOCs) weltweit rund um die Uhr überwacht wird. Unsere SOC-Teams gehen Milliarden Netzwerkereignissen pro Tag nach, um proaktiv nach Bedrohungen zu suchen und Angriffe auf multinationale Konzerne und Einrichtungen des öffentlichen Sektors abzuwenden.

Wie bleiben wir flexibel, wenn wir SASE nutzen?



Wer die Chancen unserer schnelllebigen Geschäftswelt effektiv nutzen will, muss sowohl Änderungen gegenüber offen als auch gnadenlos effizient sein.

Die Verteilung von Workloads am Netzwerkrand macht den Routinebetrieb flexibler, kann jedoch auch zusätzlichen Aufwand für IT- und Sicherheitsteams verursachen, insbesondere, wenn sie mehrere Verträge und Tools verwalten müssen.

SASE bietet eine einfachere Methode für die zentrale Sicherheitsverwaltung als deren Verteilung auf alle Verbindungen am Edge. Dadurch bleibt eine einheitliche Version aller relevanten Informationen erhalten, die Sie zur konsistenten Durchsetzung von Richtlinien und virtuellen Zugriffsrechten nutzen können.

Neil sagt: „Mit SASE sind sowohl die Ausweitung in neue Märkte als auch Fusionen und Übernahmen einfacher. Wenn Sie neue Partner oder Mitarbeiter in Ihr Netzwerk einbinden möchten, ohne es Risiken auszusetzen, können Sie das auf eine sehr kontrollierte Art tun.“

Kann SASE uns helfen, KI unter Kontrolle zu halten?

Je mehr Autonomie und je weitreichendere Zugriffsrechte KI-Agenten in Unternehmensnetzwerken erhalten, desto wichtiger werden die Einführung und Durchsetzung von Richtlinien und Governance auf der Ausführungsebene.

Eine umfassende SASE-Lösung bietet eine einfache Methode für die Definition und netzwerkweite Durchsetzung von Richtlinien, die die Bandbreitenzuweisung, Netzwerkpriorisierung und sogar Token-Budgets abdecken. So behalten Sie nicht nur die KI und Automatisierung unter Kontrolle, sondern verhindern auch, dass menschliche Nutzer die Nutzungsgrenzen versehentlich überschreiten.

Kann Verizon uns helfen, unser Unternehmensnetzwerk besser zu verwalten?

„Sie können die steigende IT-Komplexität nur mit den richtigen Tools, Automatisierung und KI im Griff behalten. Mitarbeiter allein schaffen das nicht mehr. Wenn Sie ein komplexes Netzwerk verwalten möchten, benötigen Sie den richtigen Partner und eine skalierbare, datenbasierte Plattform.“ meint Wilson.

Edge-Computing in Unternehmen erfordert zweifellos ein hohes Maß an Kontrolle und Überwachung. Ein einheitliches Rahmenwerk aus Richtlinien kann Ihnen helfen, selbst im größten WAN durchweg sichere, konfigurierbare Konnektivität bereitzustellen. Für ein effektives Management benötigen Sie jedoch eine umfassende Übersicht.

Die KI-Betriebstechnologie (AIOps) von Verizon präsentiert Netzwerktelemetriedaten und Anbieterinformationen aus unserer Arbeit in mehr als 200 Märkten auf anschauliche Weise.

Neil erklärt: „Die Entwicklungsgeschwindigkeit wird nur zunehmen. Deshalb unterstützt unsere Plattform die Konfiguration über ein Self-Service-Portal und APIs, damit Sie Tausende von Nutzern und Geräten von einer einzigen Konsole aus und mit einem einzigen Vertrag verwalten können.“

Zusätzliche Vorteile durch MNS

Managed Network Services (MNS) nehmen Ihren Teams die proaktive Verwaltung von Hardware, Routing und Sicherheitsprotokollen ab, damit sie sich auf Ihre strategischen Geschäftsziele konzentrieren können.

Verizon Business MNS nutzen KI zur schnelleren, automatisierten Bearbeitung von Änderungs- und Dienstanfragen, zum Beispiel für die großflächige Bereitstellung von Zugangspunkten, Software-Upgrades und die Datenerfassung. Damit können Sie den Anforderungen einer hybriden Belegschaft besser gerecht werden.

Nahtlose API-basierte Integrationen und ein Self-Service-Portal erleichtern Ihnen die Verwaltung Ihrer Edge-Umgebung und helfen Ihnen, sie unter Kontrolle zu behalten.

Wenn Sie mehr über MNS erfahren oder deren Nutzung mit uns besprechen möchten, besuchen Sie verizon.com/business/de-de/products/networks/managed-network-services/



Alistair Neils Fragen zum Thema SASE im KI-Zeitalter



KI hat die Arbeitswelt und das Management von Unternehmensnetzwerken eindeutig und unumkehrbar verändert. Managing Director Alistair Neil hat diese Entwicklung in Echtzeit miterlebt und seine Erfahrungen bei der Arbeit mit Kunden in aller Welt genutzt, um die drei wichtigsten Fragen zu formulieren, die Entscheider in Unternehmen sich stellen sollten:

1. Welche KI-Tools sollten wir nutzen? Welche könnten gegen uns genutzt werden?
2. Welche Cybersicherheitsvorkehrungen und -kontrollen haben wir bereits? Was benötigen wir außerdem?
3. Wie definieren wir eine angemessene KI-Governance für unser Unternehmen?

Wie kann Verizon Business uns helfen, resilienter, sicherer und flexibler zu werden?

Der Markt für SASE wächst rasant und wird 2030 voraussichtlich mehr als 17 Mrd. USD wert sein.[3] Doch SASE-Lösung ist nicht gleich SASE-Lösung.

Unternehmen, die von der Flexibilität des Edge-Computing profitieren möchten, ohne ihren unsichtbaren Motor – ihr Unternehmensnetzwerk – Risiken auszusetzen, sollten sich für eine strategische Partnerschaft mit Verizon Business entscheiden.

Unsere über 20-jährige Erfahrung beim Konzipieren, Bereitstellen und Verwalten von Netzwerk- und Sicherheitsinfrastrukturen fließt in all unsere Projekte ein.

Wir arbeiten mit branchenführenden Technologiepartnern zusammen, um Ihnen nahtlose Integrationen und die Tools zur Verfügung zu stellen, die Sie zum Schutz und Ausbau Ihres Geschäfts benötigen. Durch diese Kombination aus unserem Tier-1-Netzwerk und Beziehungen zu führenden SASE-Anbietern können wir Lösungen anbieten, die weitaus mehr leisten als die Summe ihrer Komponenten.

Das bedeutet, dass Sie sich in dem Wissen, dass Verizon ununterbrochen nach Cyberbedrohungen Ausschau hält, voll auf Ihr Kerngeschäft konzentrieren können. Unsere Incident-Response-Teams können schnell auf Vorfälle reagieren, angemessene Gegenmaßnahmen auswählen und Sie bei der Ermittlung der Ursache und der Sammlung von Beweisen unterstützen. Zudem bieten wir Simulationen für Führungskräfte an, bei denen wir potenzielle Szenarien verdeutlichen und darauf aufbauend speziell auf Ihr Unternehmen zugeschnittene Schulungen entwickeln, um eine effektive Reaktion auf Cyberbedrohungen zu trainieren.

Unsere SASE-Lösung und unser breiteres MNS-Angebot dienen nicht nur dazu, Dienste auszulagern. Sie bieten zudem proaktive Fehlerdiagnosen, einen auf enger Zusammenarbeit basierten Ansatz sowie zentralisiertes Netzwerk- und Sicherheitsmanagement. All dies hilft Ihnen, die Wirkung von Geschäftsinitiativen zu erhöhen, Ihre Produkte und Dienste schneller auf den Markt zu bringen und Ihre Kunden besser zu bedienen.

Das ist ein Grund dafür, dass wir sowohl im Gartner® Magic Quadrant™ für globale Netzwerkdienste als auch im „IDC MarketScape: Worldwide Managed SD-WAN 2020 Vendor Assessment“ als einen Leader an.

Erste Schritte mit SASE

SASE ist eine komplexe Technologie, die Sie am besten mit einem Partner implementieren sollten, der Sie bei jedem Schritt unterstützen kann. Die Umstellung ist nicht einfach, aber weniger riskant als das Beharren auf älterer Technologie.

Neil sagt: „An dieser Umstellung kommt in der Praxis so gut wie niemand vorbei. Wir unterstützen unsere Partner bei jedem Schritt, um nachhaltige IT-Architekturen zu schaffen statt technische Schulden aufzubauen.“

Unsere Berater-, Transitions- und Projektmanagementteams stehen Ihnen mit der Expertise und den Ressourcen zur Seite, die Sie für den Umstieg von einer risikobehafteten alternden Infrastruktur auf eine moderne cloudbasierte Plattform benötigen. Wenn Sie sich für Verizon Business als Partner entscheiden, erhalten Sie all diese Leistungen im Rahmen eines einzelnen Vertrags und mit einer konsolidierten Rechnung.

SASE mag in erster Linie ein Sicherheits-Framework sein, doch mit Verizon Business trägt es auch zur Steigerung der Flexibilität, Resilienz und Agilität – und damit zum Erhalt Ihrer Wettbewerbsposition in einem schnelllebigen, hart umkämpften Markt – bei.

Wenden Sie sich an unser Enterprise Strategy Team, um zu erörtern, wie Sie diese Vorteile für Ihr Unternehmensnetzwerk nutzen können. Weitere Informationen finden Sie unter verizon.com/business/de-de/solutions/adaptive-networks/



verizon business

1. Gartner, „The Future of Network Security is in the Cloud“, 2019
2. The Guardian, „Sharp rise in incidents of AI escaping users’ control, research finds“, 2026
3. Grand View Research, „Secure Access Service Edge Market (2025 - 2030)“, 2026

© 2026 Verizon. Dieser Inhalt wurde mithilfe künstlicher Intelligenz erstellt und von Menschen geprüft. OGSB1350423