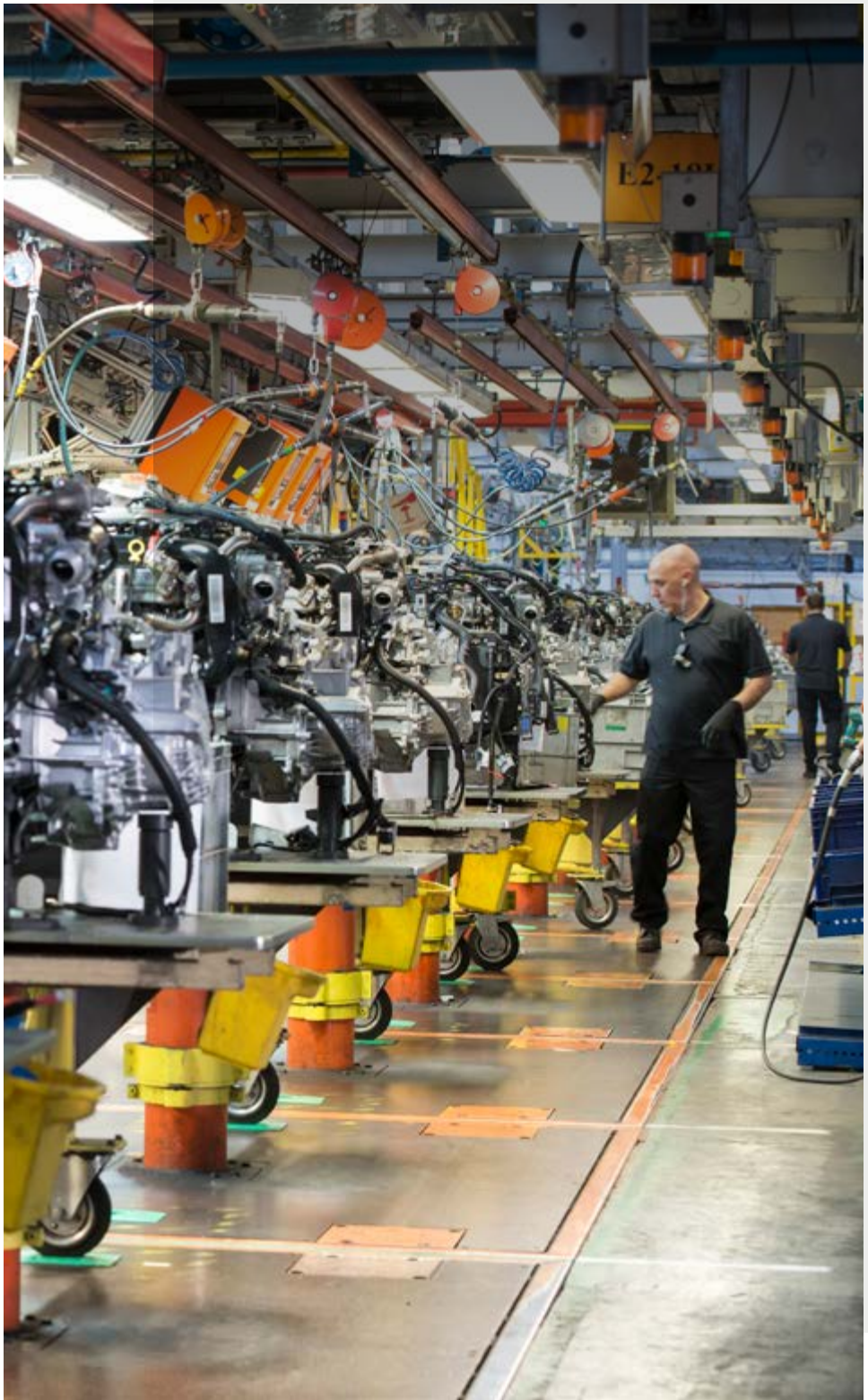
LEITFADEN

DER SASE LEITFADEN **FÜR DIE HERSTELLERBRANCHE**

Inhalt



NETZWERK: ZEIT ZUM UMBDENEKEN

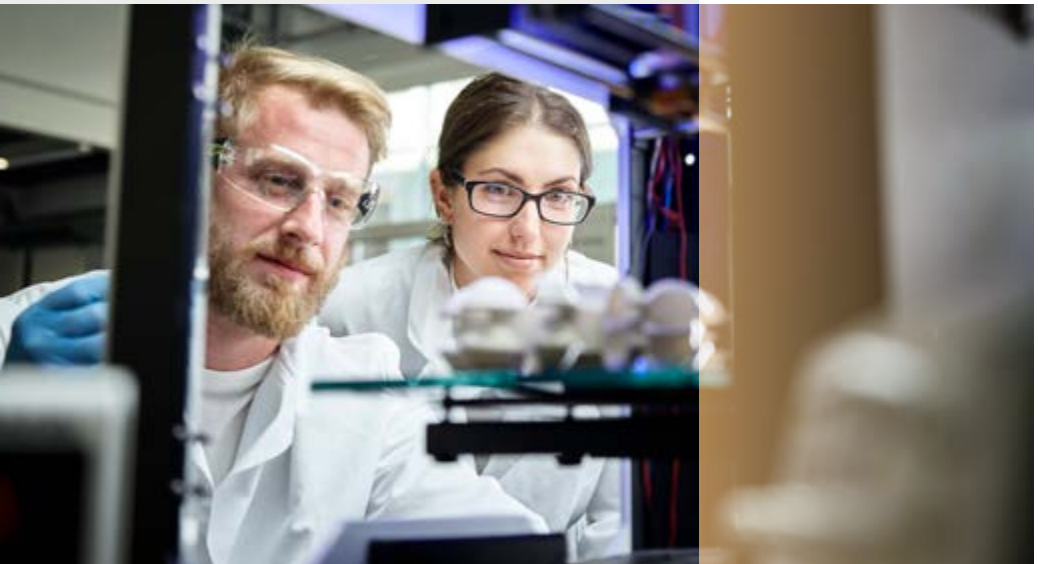
Unternehmen aus der Herstellerbranche stehen vor ganz eigenen Prozess-Herausforderungen. Innovatives Design und Ingenieurwesen erfordern den Zugang zu modernsten digitalen Tools. Dabei muss die Produktion flexibel bleiben, um der Nachfrage schnell gerecht zu werden – vom Lieferkettenmanagement bis hin zur Lagerhaltung und Distribution. Die effektive und effiziente digitale Vernetzung verbindet reibungslos alle Schritte miteinander.

In einem immer enger werdenden globalen Markt ringen führende Hersteller um jeden Wettbewerbsvorteil. Dies beginnt mit der Neudefinition ihrer digitalen Transformationsstrategie (von der Einbindung modernster Fabrikinnovationen aus dem Industrial Internet of Things (IIoT) bis hin zur Einführung von cloudbasierten Datenlösungen) und geht weiter bei der Beseitigung technischer Engpässe und schwerfälliger IT-Silos. Gleichzeitig muss eine 24x7-Betriebszeit bei optimaler Bandbreite gewährleistet werden.

Hinzu kommt das „New Normal“ einer zunehmend dezentralen Belegschaft. Die jetzigen Veränderungen werden den Geschäftsalltag noch lange begleiten. Doch während sich die digitale Vernetzung kontinuierlich weiterentwickelt, ist das Thema Sicherheit allgegenwärtig. Hersteller müssen sich ständig vor einer potentiell hohen Anzahl von Cyberangriffen schützen; bösartiges Hacking, Ransomware, Sabotage oder neu entwickelte Bedrohungen, die man heute noch gar nicht kennt.

Die Speichenarchitektur (Hub-and-Spoke) von gestern, d. h. verstreute Racks mit vor Ort installierter Hardware, ist den technischen Anforderungen der heutigen dezentralen IT-Umgebung eines Unternehmens nicht mehr gewachsen. Das selbe gilt für die Sicherheit, die bereit sein muss, globale Cyberbedrohungen zu bekämpfen und abzuwehren.

Wo können Hersteller eine umfassende, kostenbewusste und unkomplizierte Lösung finden?



SASE ERNEUERT NETZWERKE UND SICHERHEIT

Secure Access Service Edge (SASE) bedeutet den Zusammenschluss der Services für Netzwerk und Netzwerksicherheit. Anstelle einer ad-hoc Sammlung von Geräten und Tools wird Security in die Struktur des Netzwerks eingewoben. Netzwerk und Sicherheit verändert und bewegt sich somit mit dem Unternehmen mit und kann flexibel erweitert und ausgedehnt werden. Der Weg ist geebnet für das Wachstum des Unternehmens.

Mit SASE denken das Netzwerk und die Sicherheit als Einheit und sie entwickeln sich kontinuierlich gemeinsam weiter, sodass Ihr Unternehmen für die Zukunft gut ausgerüstet ist.

CLOUD UND MOBILITÄT: DIE NEUE REALITÄT

Warum brauchen Unternehmen ein so radikal neues Netzwerk- und Sicherheitskonzept? Grund dafür ist die Cloud. Cloud Computing hat die Gleichung in der gesamten Fertigungs-IT verändert. In einer mobilen Welt, in der man überall arbeiten kann, ist auch die Cloud überall im Unternehmen. Derzeit machen Cloud-Anwendungen fast die Hälfte (48 %) des Datenverkehrs an Zweigstellen und erweiterten Standorten aus.[1] Darüber hinaus wird in den kommenden Jahren das Datenvolumen in der Cloud weiter zunehmen. Branchenanalysten sagen voraus, dass Clouds im Jahr 2021 95 % der Workloads verarbeiten werden.[2]

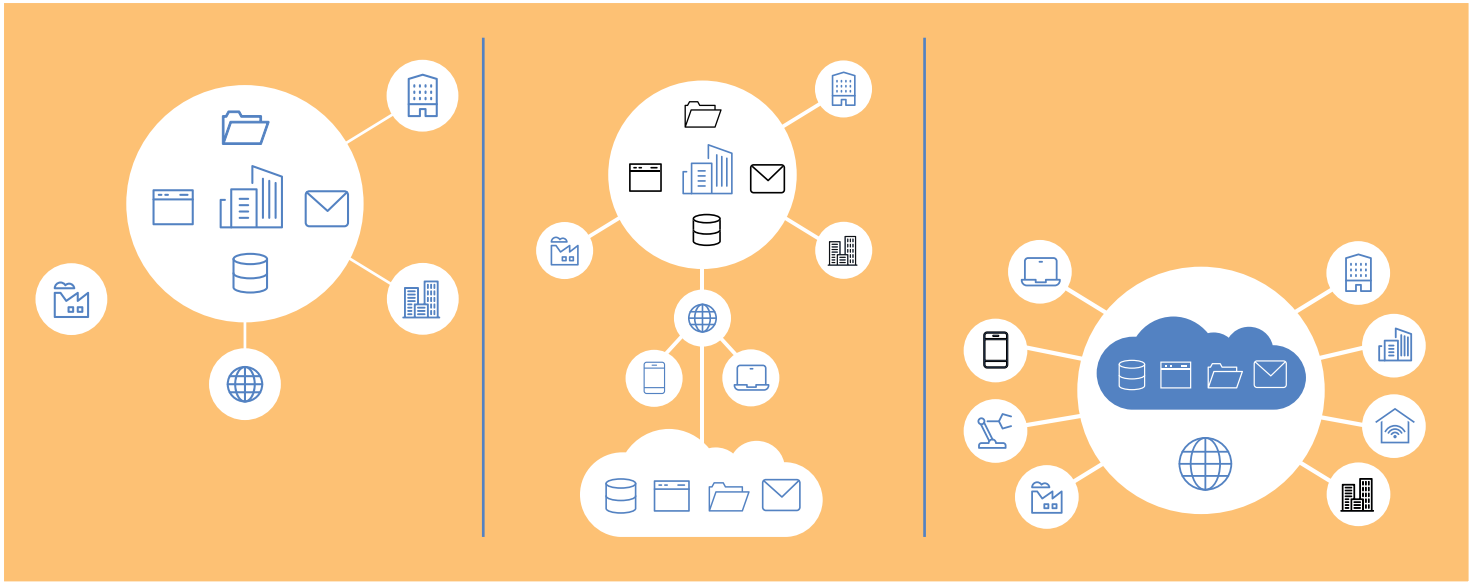
Dieses Wachstum beinhaltet die Unterstützung von Edge Computing. Dabei handelt es sich um ein relativ neues Modell, bei dem die Erfassung, Verarbeitung und Speicherung von Daten in der Nähe des Ortes erfolgt, an dem sie erzeugt werden. Wenn mit der Cloud verbunden, erledigen eine Vielzahl neuer Small-Footprint-Geräte alles, von der Verwaltung der täglichen Produktionsabläufe bis hin zum Versand der fertigen Einheiten. Der Einsatz dieser zahlreichen Geräte – ausserhalb der Reichweite eines physischen Rechenzentrums – birgt jedoch neue Risiken.

Obwohl niemand erwartet, dass lokale Rechenzentren komplett verschwinden werden, ist es dennoch sicher, dass öffentliche, private oder hybride Clouds weiterhin einen grösseren Teil der täglichen Arbeitslast schultern werden. In einigen Fällen wird das Rechenzentrum eine weniger bedeutende Rolle bei der Unterstützung der Informationstechnologie spielen. In anderen Fällen könnten sich die physischen Beschränkungen als lästiger Engpass erweisen, insbesondere wenn wachsende Unternehmen mit der Verwaltung mehrerer Standorte und deren SD-WAN Verbindung zu kämpfen haben.

Da Zweigstellen und mobile Mitarbeiter die Mauern der herkömmlichen Fertigungsunternehmen hinter sich lassen, werden sensible Daten zunehmend ausserhalb des Rechenzentrums gespeichert. Durch den Wechsel von privaten MPLS-Netzwerken zum öffentlichen Internet sehen sich die Hersteller mit zunehmenden Sicherheitsrisiken und Herausforderungen konfrontiert. Die Möglichkeit – oder sogar Wahrscheinlichkeit – von verheerenden Angriffen über das WAN wächst fast täglich. Dieses Risiko macht den holistischen und umfassenderen Ansatz der Unternehmenssicherheit unumgänglich.

Hersteller müssen ein SD-WAN besser vernetzen, sichern und betreiben. Zu diesem Zweck sichern Geschäftsleitung und IT-Teams ihren Wettbewerbsvorteil, indem sie zu SASE wechseln.

DIGITALE TRANSFORMATION UND DAS WAN



In einem traditionellen WAN ist der Hauptsitz die Sonne, um die alle Planeten kreisen. Das System besteht aus einem geschlossenen MPLS-Netz sowie Anwendungen und einem zentralen Internet Breakout am Hauptsitz.

Die digitale Transformation stellt jedoch neue Anforderungen an Herstellerunternehmen. Dazu gehören: Cloud-Anwendungen, vereinheitlichte Zusammenarbeit, mobile Geräte, IoT und Edge Computing.

Eine geschäftsorientierte SD-WAN-Infrastruktur stellt das traditionelle WAN-Konzept auf den Kopf. Sie dreht sich um Anwendungen in der Cloud und bietet Zugang zu Benutzern und Geräten, egal, wo sie sich befinden. Sie nutzt die Nähe zur Cloud durch lokale Internet-Breakouts und steigert die Bandbreite durch eine Mischung aus MPLS und Internet.

Dieser Ansatz senkt die Kosten, gleicht den Verkehr über mehrere Verbindungen aus und beseitigt Engpässe. Zudem wird die Anwendungsübersicht und Kontrolle über das Netzwerk verbessert.

WAS IST SASE?

SASE dezentralisiert die Sicherheit vom Rechenzentrum und dehnt sie auf den Rand des Netzwerks, die Cloud und alles dazwischen aus. SASE definiert auch das veraltete Modell von nicht zusammenpassenden Geräten und starren Verbindungen neu. Stattdessen liefert SASE einen einzigen, intelligenten, automatisierten und dehnbar cloudbasierten Service. Ausserdem sollte ein effektives SASE-Modell alle benötigten Netzwerk- und Sicherheitsfunktionen bereitstellen und gleichzeitig die Flexibilität bieten, neue Funktionen laufend zu übernehmen. Noch wichtiger ist, dass SASE eine schnelle, sichere und konsistente Arbeitsumgebung für die Benutzer sowie den Kern des Cloud-gestützten Edge Computing bietet.

ZWEI WICHTIGE GRÜNDE FÜR DIE EINFÜHRUNG VON SASE

Unternehmensnetzwerke sind zu komplex und zu zerstreut für eine effiziente Verwaltung, insbesondere angesichts des chronischen Mangels an qualifizierten Ressourcen. Gleichzeitig wird die Bedrohung aus dem Netz immer grösser und ausgeklügelter, was Herstellerbetriebe gezwungen hat, ihre Daten- und IT-Handhabung grundlegend zu verändern. Traditionell hatten Netzwerk- und Netzwerksicherheitsteams unterschiedliche Treiber. Erstere zielen darauf ab, dass die Dinge so reibungslos wie möglich laufen, während letztere vor allem Sicherheit und Bedrohungsabwehr im Blick haben. Jetzt müssen diese beiden Teams zusammenarbeiten, um ein gemeinsames Ziel zu erreichen: resiliente Netzwerkverbindung und deren Sicherheit.

WER PROFITIERT VON SASE?

SASE ist eine Cloud- und Edge-basierte Plattform, die dank identitätsbasierter sowie kontext- und standortbezogener Richtlinien ein hohes Mass an Flexibilität bietet. Sie überspringt die technischen Beschränkungen bei der Konfiguration von IP-Adressen und hilft bei der Verwaltung von Workloads über physische Server und virtuelle Infrastrukturen in der Cloud.

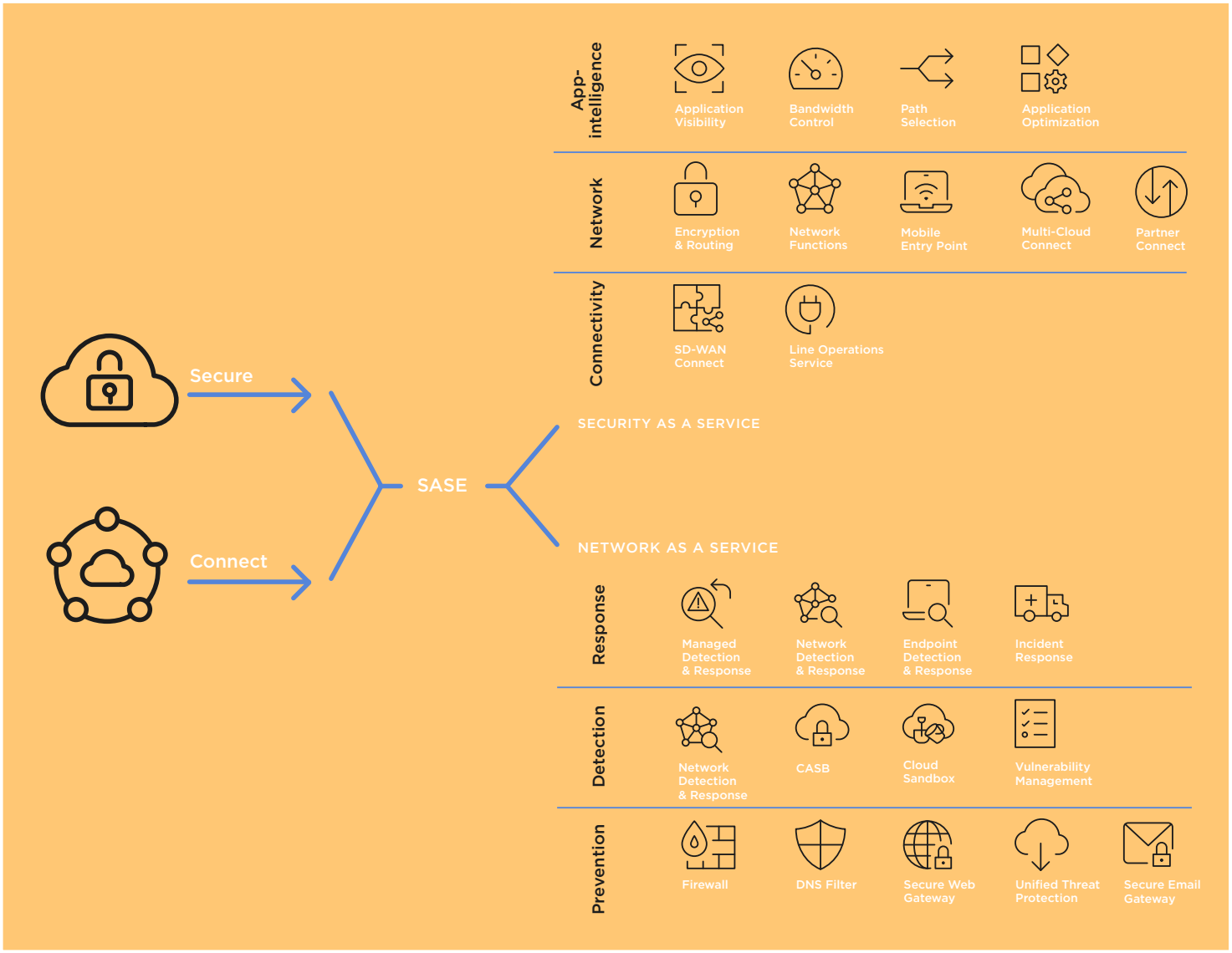
Benutzer profitieren von direkteren Zugriffspunkten und höherer Leistung ihrer cloudbasierten Ressourcen und des Internets. Eine Single-Pass-Architektur, ergänzt durch optimierte Bandbreite, liefert eine benutzer- und anwendungsgerechte Leistung.

Die IT-Abteilung profitiert von der Vereinheitlichung des Netzwerks und der Sicherheit, was den domänenübergreifenden Verwaltungsaufwand reduziert und eine bessere Orchestrierung, Automatisierung und Transparenz mit einer zentralen Kontrolle ermöglicht. SASE bettet ausserdem ein komplettes Set von Sicherheitsfunktionen ein – vom Edge bis zur Cloud und überall dort, wo das Netzwerk hinreicht. SASE verlagert die Verwaltung und Administration von manuellen Schritten auf richtliniengesteuerte autonome Funktionen und Prozesse, wie etwa Zugriffskontrolle, Bandbreitenoptimierung und QoS-Management für Benutzer und Anwendungen.

Eine einheitliche Plattform (Single-Pane-of-Glass-Portal) bietet Einblicke in Echtzeit, während prädiktive Analysen Prognosen liefern. Netzwerk- und Sicherheitsvereinheitlichung, Automatisierung und Orchestrierung bedeuten ausserdem, dass Fertigungsunternehmen Probleme innerhalb von Minuten oder Stunden effektiv lösen können, was früher Tage oder Wochen dauerte. Das modulare Design bedeutet ausserdem, dass Funktionen schnell implementiert und hoch- oder runtergeschraubt werden können, um neue Geschäftsanforderungen zu erfüllen.

NETZWERK UND SICHERHEIT RÜCKEN NÄHER ZUSAMMEN

SASE verschmilzt umfängliche Cybersecurity- und Netzwerkservices zu einem einheitlichen cloudbasierten Service. Richtig gemacht, fördert es die Verlagerung des digitalen Geschäfts weg vom Unternehmensrechenzentrum. Anstatt Richtlinien festzulegen und den Zugriff vom Zentrum aus zu kontrollieren, verlagert SASE diese Funktionen an den Rand des Unternehmens, wo immer sich Benutzer und Geräte befinden. Stellen Sie sich SASE als eine universelle Struktur vor, die bei Bedarf richtlinienbasierte Sicherheitsfunktionen aus der Cloud bereitstellt.



VORTEILE EINER SASE TRANSFORMATION

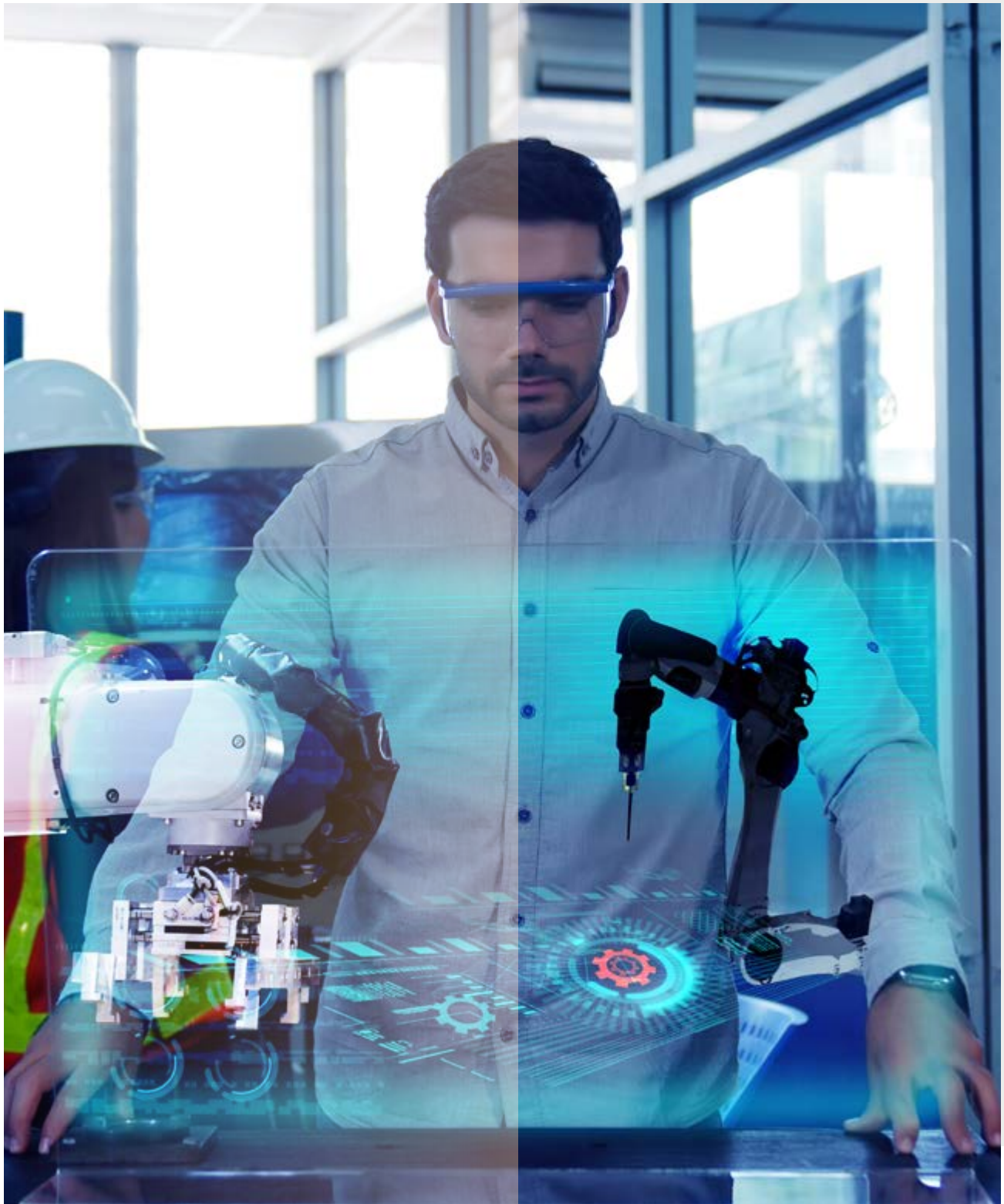
Höhere Leistung
Effiziente Bandbreitenzuweisung steigert Netzwerkleistung und senkt Verzögerungen.

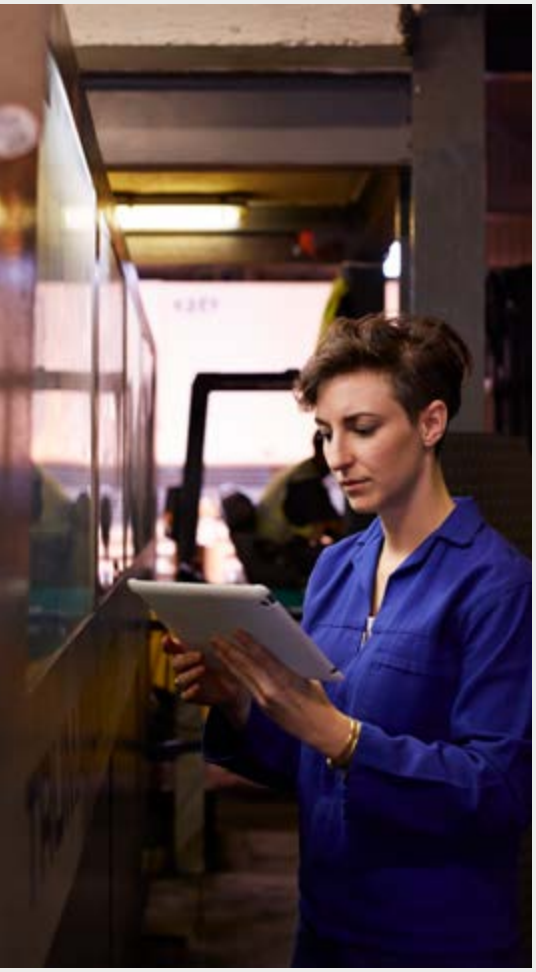
Einfache Verwaltung
Die agile, agnostische und skalierbare Natur von SASE bedeutet, dass die Erweiterung von SASE auf neue Anwendungen einfach und unkompliziert erfolgt.

360° Sichtbarkeit
Mehr Betriebs- und Sicherheitstransparenz über eine einheitliche Plattform mit fundierten Einblicken in Echtzeit.

Bessere Sicherheit
Verbesserte Zugriffskontrollen für cloudbasierte Services und Edge-Implementierungen bei gleichzeitiger Verbesserung des „End-to-End“ Netzwerkschutzes.

Geringere Kosten
Automatische Ressourcenoptimierung, nahtlose Orchestrierung und Prozessautomatisierung vereinfachen den Betrieb und senken die Kosten.





SASE SCHAFFT EIN HOHES MASS AN FLEXIBILITÄT DANK DER UNTERSTÜTZUNG IDENTITÄTS-BASIERTER SOWIE KONTEXT- UND STANDORTBEZOGENER RICHTLINIEN

SASE schafft ein hohes Mass an Flexibilität dank der Unterstützung identitätsbasierter sowie kontext- und standortbezogener Richtlinien. Unternehmen entdecken schnell den Vorteil, dass Konfigurationen, Einstellungen und Berechtigungen über mehrere Cloud- und SaaS-Anbieter hinweg besser verwaltet werden können. Ein SASE Gerüst fördert eine bessere Governance und konsistentere Sicherheitskontrollen.

Darüber hinaus bietet es leistungsstarke Tools, um Netzwerk- und Sicherheitsfunktionen effektiver zu integrieren. Die Implementierung einer SASE Lösung ermöglicht es über ad-hoc Einzelkonfigurationen – jede mit eigenem Lebenszyklus und eigenen Gesamtbetriebskosten (Total Cost of Ownership, kurz TCO) – hinauszuwachsen, zu einem robusten, agilen Gerüst, das ganzheitlich funktioniert.

Das SASE-Framework bietet weitere wichtige Vorteile:

Eine widerspruchsfreie Erfahrung. SASE schafft eine einheitliche Benutzererfahrung über alle Systeme, Geräte und Geografien hinweg.

Geringere Latenz. Mit SASE Verbindungen, die bis zum Edge reichen und sich auch auf entfernte Standorte ausdehnen, erleben Endnutzer schnelle, reaktionsfähige und sicherere Systeme. Die IT-Abteilung kann Richtlinien festlegen, die den Datenverkehr über die am besten geeigneten Kanäle leiten, während notwendige Sicherheitsmassnahmen auf die latenzfreundlichste Weise bereitgestellt werden.

Zusätzliche Gewinne. Das Framework lässt sich mit DevOps- und DevSecOps-Initiativen in Einklang bringen. Es reduziert auch den Bedarf an spezifischen Fähigkeiten und dedizierten IT-Mitarbeitern für die Verwaltung des Netzwerks und der Sicherheit.

Ein Zero Trust Sicherheitsgerüst. SASE ist ein bewährter erster Schritt in Richtung einer differenzierten, kontinuierlichen und adaptiven Risikobewertung während jeder Session.

Vereinfachte und verbesserte IoT-Administration und Sicherheit. SASE optimiert und konsolidiert die Netzwerk-, Konnektivitäts- und Geräteverwaltung innerhalb eines Zero Trust Gerüsts.

SASE ERMÖGLICHT OPTIMALE ARBEITSABLÄUFE

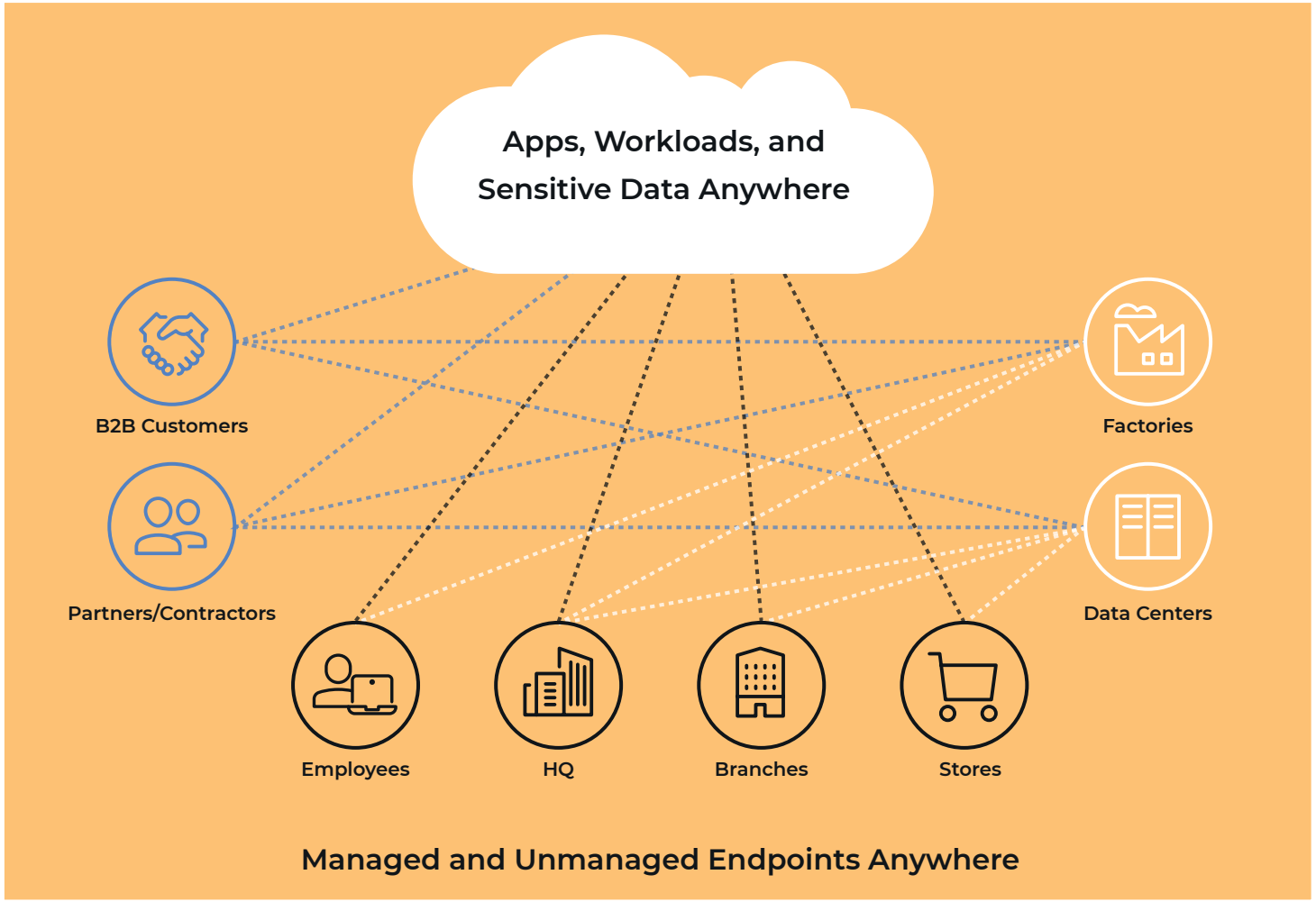
Letztendlich erhalten Hersteller, die SASE einsetzen, ein besseres Verständnis für den Kontext ihrer Daten – einschliesslich der Frage, ob sie heikel oder bösartig sind. Dies wiederum hilft bei der Definition weiterer wichtiger Tools, Lösungen und Schutzmassnahmen, wie z. B. dem Design und der Verwendung von Authentifizierung und Verschlüsselung.

Schliesslich bietet SASE Einblick in Prozesse und ermöglicht optimale Arbeitsabläufe sowie eine bessere Prognose für Budget und OPEX-Kosten. Durch vorhersagende Analysen können IT-Teams in der Fertigung Datenmanagement und Sicherheitsanforderungen viel effektiver verwalten und abschätzen. Ausserdem werden potenzielle Engpässe beseitigt. Diese Fähigkeiten führen letztendlich zu dem optimal passenden Netzwerk.

DAS ENDE DES KLASSISCHEN SICHERHEITSPERIMETERS

Alte Systeme müssen aktualisiert werden, was Hersteller zu Multi Cloud Strategien führt, die hybride Designs (On-Prem und Public Cloud) umfassen. Dazu gehören mehrere CSPs, Plattformen und Produkte wie SaaS, PaaS und IaaS.

Aber es sind nicht nur Anwendungen und Daten, die sich überall hinbewegen. Clients, die auf diese zugreifen, sind dezentraler denn je. Das Wachstum von IoT und Edge Computing bedeutet auch, dass Bereitstellungen, Speicher- und Rechenressourcen zunehmend über Firewalls hinaus verlagert werden. Speziell in der Fertigung umfasst das schnell wachsende Industrial Internet of Things (IIoT) zahlreiche vernetzte Automatisierungssysteme von mehreren Anbietern. All diese Faktoren haben dazu geführt, dass der klassische Sicherheitsperimeter irrelevant geworden ist.



DER WEG ZU SASE

Der Fahrplan für eine erfolgreiche Implementierung von SASE hat folgende erste Stationen:

Abbildung des Netzwerks. Es ist wichtig, Ihr aktuelles Netzwerk vollständig zu erfassen und zu analysieren. Dazu gehört, welche Anwendungen im Netzwerk vorhanden sind und wie viel Bandbreite sie beanspruchen, wie sich Clouds mit dem Netzwerk überschneiden, wo sich Geräte und Daten befinden und wie der Datenverkehr durch die gesamte Infrastruktur fliesst.

Bewertung der Auswirkungen. Als Nächstes müssen Sie bewerten, wie sich Netzwerk- und Sicherheitänderungen auf die Geschäftsprozesse und -praktiken auswirken werden. Dies erfordert eine gründliche Untersuchung der bestehenden Datenflüsse, Benutzer und Kontrollen. Dieser Schritt beinhaltet Gespräche mit Managern und anderen Stakeholdern, um genau zu verstehen, wo aktuelle Probleme bestehen und wie SASE sie lösen kann.

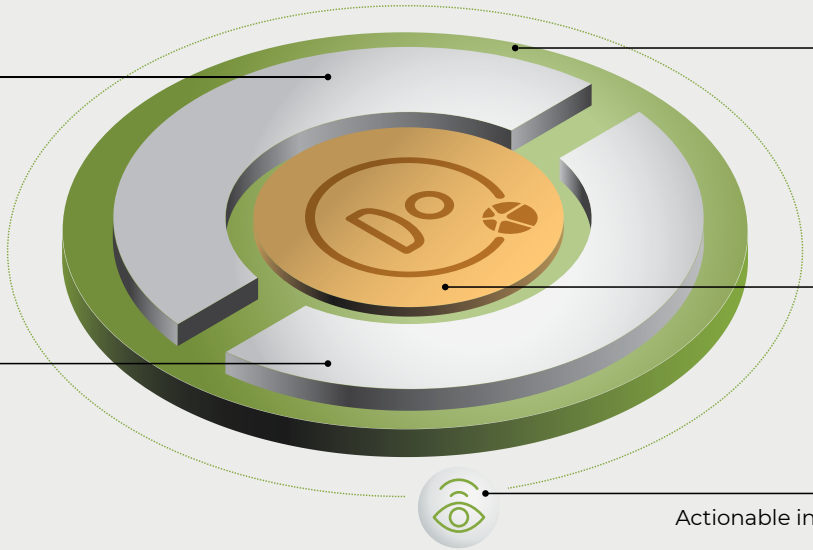
Vorwärts mit Blick in den Rückspiegel. Es ist wichtig, sowohl das alte als auch das neue Netzwerk während der Übergangsphase zu unterstützen. Damit werden Schreckens-Szenarien vermieden, wo Systeme stunden-, tage- oder wochenlang nicht richtig funktionieren oder nicht kommunizieren. Nicht nur das Unternehmen wird geschwächt, sondern auch die Belegschaft bleibt frustriert zurück.

Weitere Herausforderungen und Schwachstellen miteinberechnen. Netzwerk- und Sicherheitsteams müssen in ständigem Kontakt bleiben und zusammenarbeiten, um Probleme zu lösen, sobald sie auftreten. Traditionell haben diese Teams oft innerhalb ihrer eigenen Silos gearbeitet, aber SASE verbindet diese Funktionen und führt eine gemeinsame Zielsetzung ein. Dieser Schritt erfordert in der Regel gezieltes Training aber auch kulturelle und praktische Anpassungen.

Bereit für die Zukunft. SASE hingegen stellt sicher, dass alle beteiligten Komponenten nahtlos zusammenarbeiten. Dieser Ansatz bietet eine optimierte Ausgangslage für Wachstum. Darüber hinaus erhalten Hersteller eine ganzheitliche Sicht und können zukünftige Geschäftsstrategien besser unterstützen, dank eines schnelleren Überblicks, Erkenntnissen und effizienteren Analysen.

SASE FÜR EINE SICHERE ZUKUNFT

Ein modernes und einheitliches SASE-Modell setzt alle Teile zusammen, die für die Verwaltung eines Unternehmens erforderlich sind.



DER PASSENDE STRATEGISCHE PARTNER AN IHRER SEITE

Gartner prognostiziert, dass bis 2024 40 % der Unternehmen SASE einführen werden.[3] Ausserdem wird erwartet, dass IT-Manager „one-stop" Cloud-Lösungen bevorzugen, bei denen sowohl Zuverlässigkeit als auch Sicherheit im Vordergrund steht: Die meisten Unternehmen, die gemanagte SD-WAN Services einführen, werden auch gemanagte Sicherheitsdienste benötigen, die möglicherweise vom selben Service Provider bezogen werden können. - Gartner, 2020[4]

Die grosse Aufmerksamkeit, die SASE in letzter Zeit erhielt, hat viele Player in diesem Bereich hervorgebracht. Der Schlüssel zum Erfolg besteht darin, sich durch all den Lärm und die widersprüchlichen Behauptungen zu kämpfen, um einen bewährten Partner und ein solides SASE Framework zu finden. Die Auswahl des idealen SASE Partners ist entscheidend für die drastische Steigerung der Netzwerkleistung, der Sicherheit und letztendlich den Erfolg für Unternehmen im gesamten Herstellungssektor.

> Der Schlüssel zum Erfolg liegt darin, sich durch all den Lärm und die widersprüchlichen Behauptungen zu kämpfen, um einen bewährten Partner und ein solides SASE Framework zu finden.

OPEN SYSTEMS: EIN SASE PIONIER

Open Systems liefert eine anpassungsfähige, zukunftssichere SASE Plattform als Service. Organisationen rund um den Globus verlassen sich auf ein einfaches Netzwerk, intelligente Sicherheit und Performance sowie einem 24x7 Support – alles aus einer Hand. Dies beinhaltet den Zugang zu mehr als 120 hochqualifizierten und erfahrenen Netzwerk- und Cybersecurity-Experten und DevSecOps-Ingenieuren.

MIT SASE SELBSTBEWUSST IN DIE ZUKUNFT

Die heutige „Compute-anywhere-and-everywhere"-Welt erfordert mehr als herkömmliche Netzwerksicherheit und ein standard SD-WAN. Von Ingenieuren und Managern, die von zu Hause aus zusammenarbeiten, bis hin zu Vertriebsmitarbeitern, die mobile Geräte im Aussendienst nutzen – sensible Daten befinden sich heute überall. Diese neue Cybersicherheitslandschaft erfordert intelligente Systeme und die Erweiterung dieser Intelligenz in die Clouds und den Edge. Der richtige SASE Partner kann Ihnen helfen, Ihr Netzwerk umzubauen und gleichzeitig ein integriertes und robustes Sicherheitsgerüst zu implementieren.

Open Systems SASE löst das Versprechen eines ausgereifteren Frameworks ein – entwickelt für die grenzenlose „next-generation" IT-Welt. Unsere cloudbasierte Architektur hilft Ihnen dabei, Ihr Netzwerk- und Sicherheitsgerüst in ein Best-Practice-Modell umzuwandeln, das die Effizienz, die Sicherheit und den optimalen Workflow Ihres Herstellungsunternehmens erhöht.

Open Systems SASE löst das Versprechen eines ausgereifteren Frameworks ein.

Erfahren Sie mehr darüber, wie SASE von Open Systems Ihr Netzwerk in ein einheitliches Gefüge aus Effizienz, Agilität und Sicherheit verwandeln kann. Kontaktieren Sie uns noch heute für ein kostenloses Assessment.

1 EMA, Wide-Area Network Transformation: How Enterprises Succeed with Software-Defined WAN, Dezember 2018

2 TechRepublic, "95% of global data center traffic will be from the cloud by 2021," 5. Februar 2018

3 Gartner, Competitive Landscape: Managed SD-WAN Services, 2. März 2020

4 Ibid

Wir liefern eine Cybersecurity-Erfahrung, die weit über den Standard hinausgeht. Wir haben eine SASE Lösung entwickelt, die flexibel und skalierbar ist, mit einem echten Zero Trust Ansatz und einem einzigartigen MDR Service, der Störfälle durch präzise Massnahmen minimiert. Unsere Teams überwachen 24x7 mehr als 3 Millionen Endpunkte weltweit. Das verstehen wir unter Cybersecurity, die nicht nur gut, sondern crazy good ist.

Weitere Informationen unter open-systems.com |