Resiliente und agile Firmennetze

Warum Software-definierte Netzwerke und SASE zusammengehören.

Erleben, was verbindet.

Firmennetze der Zukunft

Es sind eine Vielzahl an Herausforderungen, mit denen Unternehmen aktuell umgehen müssen. Enormer Kostendruck, Lieferengpässe und politische Unwägbarkeiten erschweren solide Kalkulationen. Hinzu kommen Pandemiefolgen, Cyberkriminalität und Expertenknappheit. Und alle zusammen müssen wir die Transformation zu ökologisch nachhaltigem Wirtschaften stemmen. Wie kann das erfolgreich gelingen? Und was kann IT-Infrastruktur dazu beitragen?

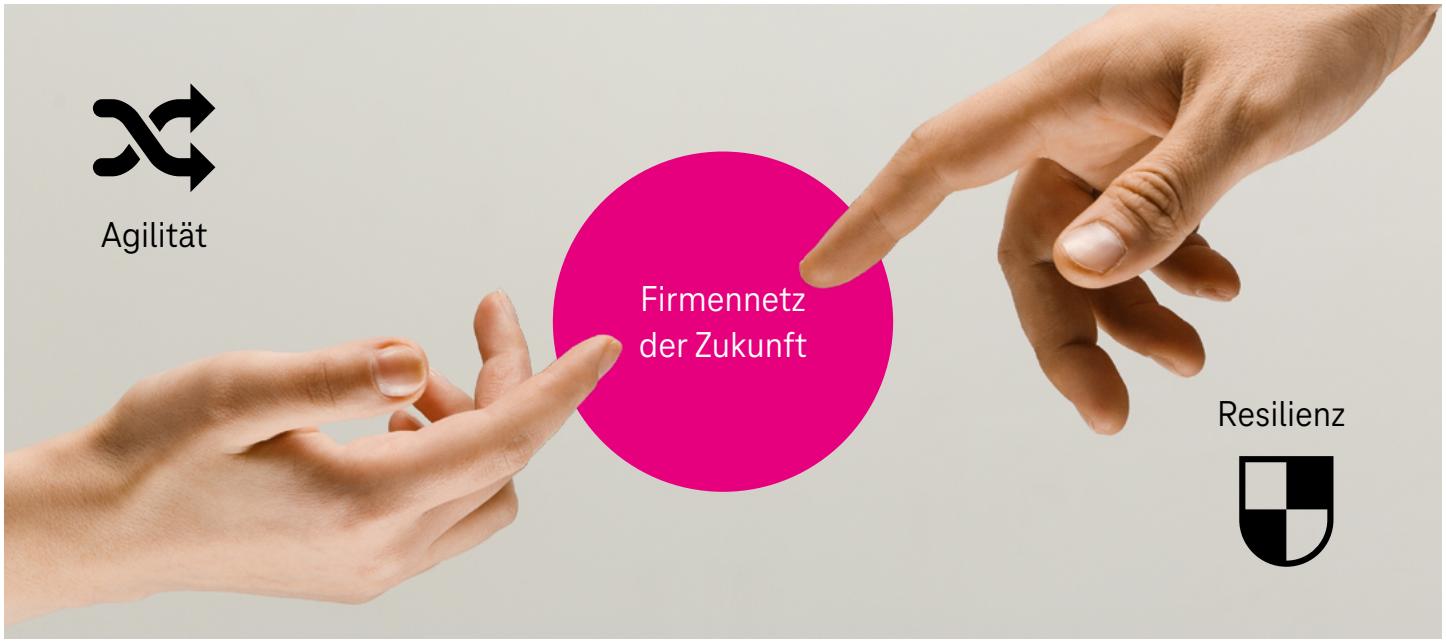
Als Gesellschaft und als Unternehmen geht es momentan darum, möglichst widerstandsfähig und krisenfest zu werden. Eine funktionierende, sichere und zeitgemäße Infrastruktur ist dafür ein wichtiger Baustein. Das gilt auch und insbesondere für IT-Infrastruktur, die ein zentraler und durchaus kritischer Punkt unserer Infrastruktur ist. Aber IT-Infrastruktur kann noch mehr – sie kann Enabler für Innovationen sein – oder diese blockieren.

Netzwerke „alter Schule“ funktionieren nach dem Prinzip Hub and Spoke – englisch für Nabe und Speiche. Die Verbindungen des Netzwerks – meist kabelgebundene Client-Server-Netzwerke – werden über einen zentralen Gateway hergestellt. Spätestens seit Covid 19, als Homeoffice in großem Stil und teils ad hoc umgesetzt wurde, merken Unternehmen, dass sie mit dieser Netzwerk-architektur schnell an Grenzen stoßen. Der zentrale Hub, über den alles läuft, wird zum Flaschenhals – Performanceprobleme an den Netzwerkenden sind die Folge. Neuerungen lassen sich nur unter großem Aufwand umsetzen. Fällt der Hub aus, ist das gesamte Netzwerk betroffen und nichts geht mehr. Die zentrale Netzwerk-architektur ist heutigen und künftigen Herausforderungen nicht mehr gewachsen.

Netzwerk-Architektur muss agiler werden:
Die Zukunft der Netze liegt in der Integriertheit in die IT. Um Geschwindigkeit in der Einführung von neuen Applikationen, Flexibilität in der Nutzung von Anwendungen und New Work zu realisieren, muss die nächste Generation an Daten-Netzen möglichst strukturiert und möglichst automatisiert sein.

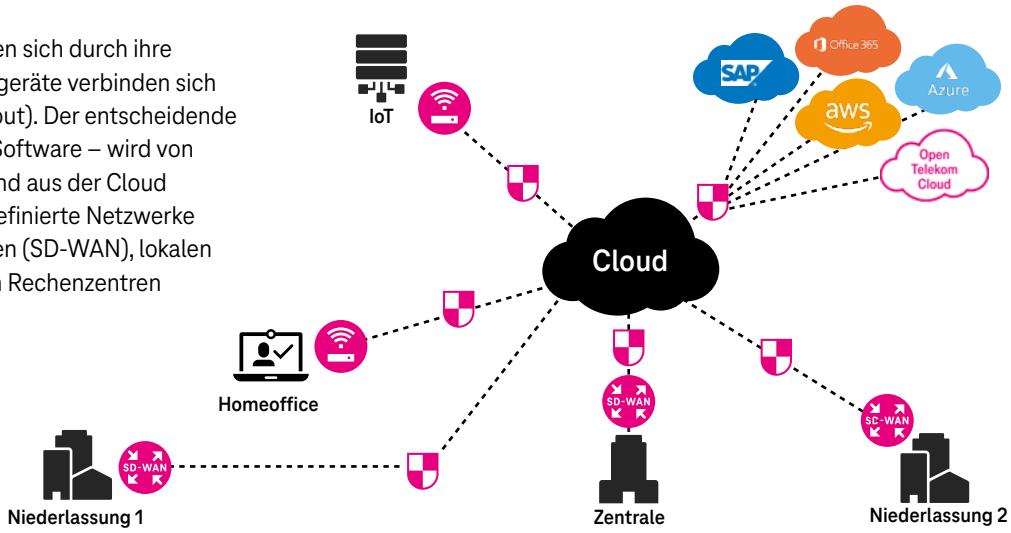
Netzwerk-Architektur muss resilienter werden:
Eine dezentrale Netz-Architektur, die einen direkten Zugang zur Cloud ermöglicht, bedeutet eine stabilere Perfomance an den Netzenden. Zugleich bedarf sie einer neuen Sicherheitsarchitektur, um Sicherheit an allen Enden zu gewährleisten.

Die Zukunft hat schon begonnen: Software-Defined Networks (SDN) lösen die zentrale Hub-and-Spoke-Architektur mehr und mehr ab. Dieses Paper gibt einen Überblick über die Themen Software-definierte Netzwerke und die Sicherheitsarchitektur SASE. In Kombination sorgen sie für agile und resiliente Netzwerke, die den Anforderungen künftiger Entwicklungen gewachsen sind.



Überblick: Software-definierte Netzwerke

Software-Defined Networks (SDN) zeichnen sich durch ihre dezentrale Architektur aus. Sämtliche Endgeräte verbinden sich direkt mit der Cloud (Local Internet Breakout). Der entscheidende Punkt: Die Netzwerkintelligenz – also die Software – wird von Hardware und Transportnetz entkoppelt und aus der Cloud gemanagt. Eingesetzt werden Software-definierte Netzwerke in Weitverkehrsnetzen zwischen Standorten (SD-WAN), lokalen Standortnetzen (SD-(W)LAN) sowie in den Rechenzentren selbst (SD-LAN).



Bestandteile des Software-definierten Netzwerks

SD-WAN
Das Software-Defined Wide Area Network (SD-WAN) kann im Gegensatz zum Wide Area Network (WAN) die Datenübertragungswege standortübergreifend über ein Software-Overlay steuern. So werden die Übertragungswege wie Multiprotocol-Label-Switching (MPLS), Ethernet, LTE oder auch DSL je nach Anwendung oder Dienst automatisch reguliert. Die unterschiedlich kritischen Anwendungen werden flexibel über den besseren und sicheren Kommunikationsweg geleitet. So können auch bandbreitenintensivere Cloud-Services gleichzeitig mit kritisch eingestuften Diensten im SD-WAN genutzt werden. Eine manuelle Konfiguration der Router ist nicht mehr nötig.

SASE
SASE ist eine vollumfängliche Architektur für Ende-zu-Ende-Sicherheit im Netzwerk, die aus der Cloud zur Verfügung gestellt wird. Sie schließt die Sicherheitslücke im Software-definierten Netzwerk, die entsteht, da sämtliche Zweigstellen sich direkt mit dem Internet verbinden. Sie alle mit einzeln zu administrierenden Firewalls auszustatten, wäre zu aufwändig. SASE bietet Sicherheit als Service, der in das Netz integriert und zentral über die Cloud gemanagt wird. Sämtliche Zugriffe und Sitzungen, die Nutzer oder Endgeräte im Netzwerk starten, werden auf diese Weise zuverlässig überwacht. Es sind verschiedene Sicherheitskomponenten, die unter SASE zusammengefasst werden und die je nach Unternehmensanforderungen miteinander kombiniert werden können.

SD-(W)LAN
Auch Wireless Local Area Network (WLAN) und Local Area Network (LAN) lassen sich Software-definiert steuern. Die zentrale Steuerung vereinfacht die Administration erheblich: Die Einrichtung von Gäste-WLANs, das Upgrade von Firmwares, die Konfiguration von Mobilfunk Gateways, die Verbindung von IoT-Sensoren und vieles mehr kann einfach, zentral und sicher überwacht und gesteuert werden. Die lokalen Standortnetze profitieren zudem genau wie die Weiterverkehrsnetzte von den Möglichkeiten, die Software-definiertes Performance-Management bietet: Mindestanforderungen und Bevorzugungen bestimmter Anwendungen können definiert und automatisch durchgesetzt werden.

Transportnetze
Basisinfrastruktur sind und bleiben die Transportnetze. Sie verbinden Mitarbeitende, Standorte und Rechenzentren weltweit und sollten hochsicher, skalierbar und flexibel sein. Für den Datentransport im Software-Defined Network werden in der Regel mindestens zwei Transportnetze genutzt, z. B. Internet und MPLS. Aber auch Mobilfunk wie zum Beispiel 5G und Narrowband kommen zum Einsatz, etwa, um IoT-Sensoren zu vernetzen.

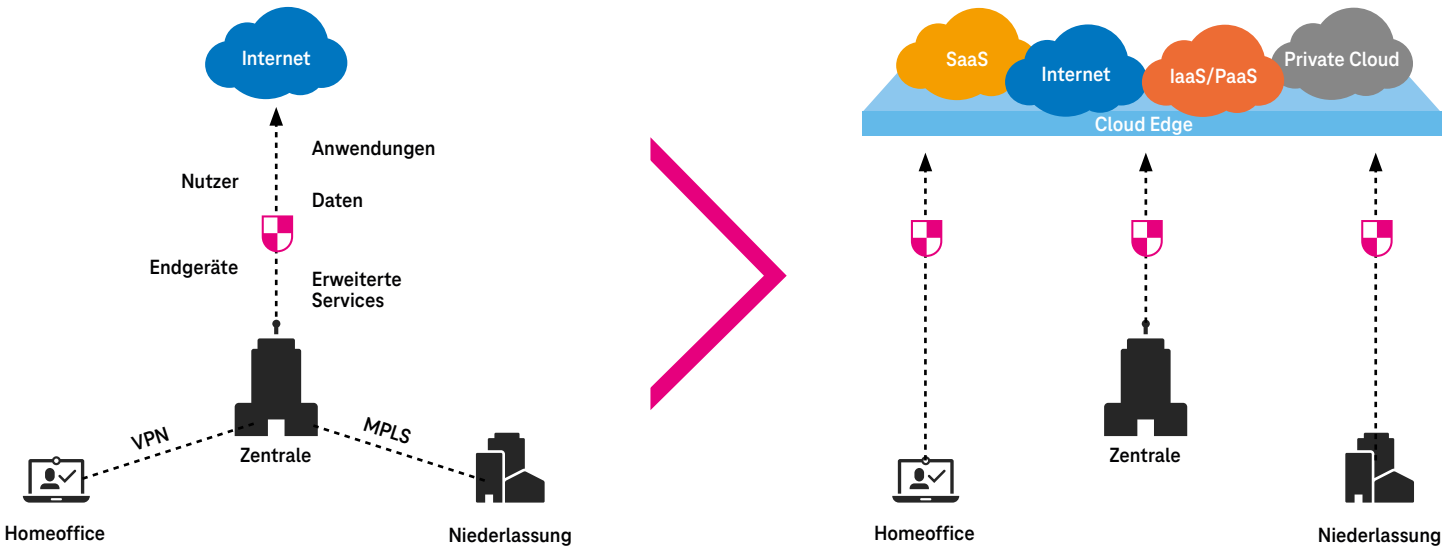
Die Vorteile eines Software-definierten Netzwerks

Höhere Performance und Stabilität ist einer der Vorteile von Software-definierten Netzwerken. Möglich wird die Verbesserung durch das Software-definierte Performance-Management. Der Datenverkehr wird über einen zentralen Controller mit Überblick über das gesamte Netzwerk gelenkt, statt des protokollbasierten Wählens der richtigen Verkehrsroute durch die Steuerungselemente der einzelnen Endgeräte. Auf diese Weise lassen sich Netzwerkressourcen optimal und regelbasiert verteilen. Die Durchsetzung von Mindestanforderungen oder die Bevorzugung bestimmter Anwendungen etwa. Auch Anforderungen an Datendurchsatz, Latenzzeiten, Jitter oder Paketverlust können über individuelle Performance-SLAs oder QoS-Vorgaben geregelt werden. Automatisiertes Performance-Monitoring ermöglicht es außerdem, Performance-Probleme schnell zu erkennen und zu beheben.

Effizienz ist ein weiterer Vorteil Software-definierter Netzwerke. Das Onboarding neuer Endgeräte im Rechenzentrum und den externen WAN-Netzwerken nimmt in traditionellen, hardwarebasierten Netzwerken Tage bis Wochen in Anspruch. Durch die Verlagerung der Steuerungsebene in die Cloud und die damit verbundene Orchestrierung wird das Netzwerkmanagement deutlich vereinfacht. Ob es um das Onboarding neuer Anwendungen, Endgeräte oder ganzer Standorte geht – dank KI und Automatisierung lassen sich diese Prozesse per Mausklick sofort regeln. Software-definierte Netzwerke sind somit gleich in zweifacher Hinsicht effizienter: Mitarbeitende können schneller loslegen, z.B. weil die Home-Office-Anbindung innerhalb von Minuten erledigt ist, und IT-Abteilungen werden durch die zentrale Orchestrierung entlastet.

Innovationsoffenheit ist elementar, um auf neue Situationen reagieren und am Markt von Morgen mitzumischen zu können. Die starke Zunahme mobilen Arbeitens, IoT-Anwendungen und Industrie 4.0 erfordern flexible Umgebungen, die agil auf neue Anforderungen reagieren können. Software-definierte Netzwerke können hier eindeutig punkten. Im Vergleich zu Netzwerkarchitekturen, bei denen die Logik in den Geräten manifestiert ist, lassen sich Netzwerkdienste im Software-definierten Netzwerk schneller entwickeln, testen und verteilen. Sie sind somit eine gute Basis für kommende Innovationen – etwa in den Bereichen IoT, Edge Computing oder AR/VR.

Von zentraler zu dezentraler Netzwerkarchitektur



Sicherheit im Fokus: SASE

Sicherheitsaspekte sind laut einer aktuellen Studie[1] Haupttreiber der aktuellen Netzwerkmodernisierung und -transformation. Das ist kein Wunder, denn die Bedrohungslage wächst exponentiell. Neun von zehn Unternehmen (88 %) waren in den Jahren 2020 und 2021 von Angriffen betroffen, gab der Branchenverband Bitkom[2] im August 2021 bekannt. Die Schäden durch Erpressung und Systemausfall stiegen im Vergleich zu den Jahren 2018 und 2019 sogar um mehr als das Vierfache an.

144 Millionen

neue Varianten von Schadprogrammen

zählte das Bundesamt für Sicherheit in der Informationstechnik (BSI)[3] zwischen Juni 2020 und Mai 2021. Das entspricht einem Schnitt von 394.000 pro Tag.

Schäden durch Erpressung und Systemausfälle in Deutschland seit 2019:

+ 358 Prozent[4]

Wie also steht es mit der Netzwerksicherheit im Software-definierten Netzwerk? Software-definierte Netzwerke sind natürlich nicht per se sicherer. Im Gegenteil: durch den lokalen Cloud-Zugang gibt es auch sehr viel mehr Einfallstore, über die Schadsoftware und Viren eindringen können. Wie kann Netzwerksicherheit im Software-definierten Netzwerk erreicht werden? Bei der Suche nach Antworten auf diese Frage landet man unumstößlich bei vier Buchstaben: SASE.

Was ist SASE? Der Begriff SASE als Akronym für Secure Access Service Edge wurde 2019 vom Marktanalysten Gartner[5] geprägt.

Als die vier Kernelemente von SASE nannten die Analysten folgende Merkmale:

Identitäts-basiert
SASE-Services werden unter Berücksichtigung der Identität der Nutzerinnen und Nutzer eingesetzt. Unabhängig von Ort oder Endgerät können Zugangs- und Sicherheitsberechtigungen so auf einzelne User zugeschnitten werden.

Cloud-nativ
SASE weist wichtige Cloud-Eigenschaften wie Skalierbarkeit, Anpassungsfähigkeit und die Fähigkeit zur Selbstheilung auf. Die Sicherheitsarchitektur ist damit anschlussfähig an zukünftige Entwicklungen.

Alle Endpunkte verbunden
SASE schafft ein einziges Netzwerk für alle Unternehmensressourcen – Rechenzentren, Zweigstellen, Cloud-Ressourcen und mobile Benutzer.

Global verfügbar
Um sicherzustellen, dass sämtliche Netzwerk- und Sicherheitsfunktionen überall verfügbar sind, muss SASE global verfügbar sein.

1) IDC Executive Brief „Network Transformation in Deutschland 2021“ | cisco.com
2) Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr | Bitkom e.V.
3) BSI-Lagebericht 2021: Bedrohungslage angespannt bis kritisch | BSI
4) Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr | Bitkom e.V.
5) Gartner Research: Invest Implications: The Future of Network Security is in the cloud | gartner.com

Bausteine der SASE-Architektur

SASE bündelt mehrere Technologien, um die Sicherheit im gesamten Netzwerk inklusive aller Endpunkte (Edges) jederzeit zu ermöglichen. Je nach Anbieter werden diese unterschiedlich kombiniert. Hier ein Überblick über die vier wichtigsten Komponenten der SASE-Architektur:

Secure Web Gateway (SWG)

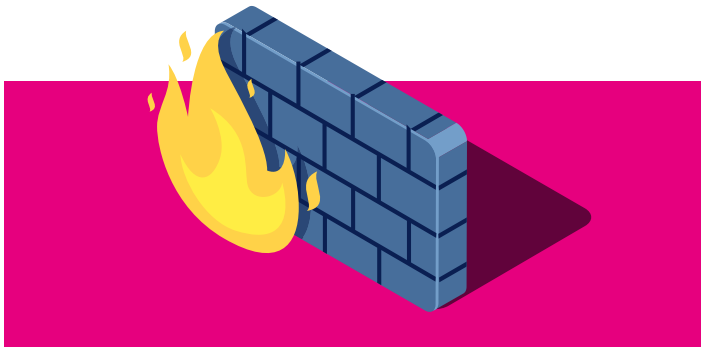
Ein SWG wehrt Bedrohungen aus dem Netz via URL-Filtering und Malware-Schutz ab. Das Gateway blockiert unbefugtes Nutzerverhalten und setzt die unternehmensspezifischen Sicherheitsrichtlinien durch. Die Lösung eignet sich insbesondere, um die Sicherheit von Mitarbeitenden zu gewährleisten, egal ob im Büro oder Remote.

Zero Trust Network Access (ZTNA)

Zero-Trust-Zugriff auf das Netzwerk bedeutet, dass der Zugriff präzise regulierbar ist und anwendungsbezogen vergeben wird. ZTNA-Lösungen beziehen Nutzeridentität, Standort, Endgerät, Tageszeit und die jeweilige Vertraulichkeitsstufe in Echtzeit ein, um eine Risikoberechnung anhand definierbarer Parameter durchzuführen und den Zugriff dementsprechend zu regeln.

Cloud Access Security Broker (CASB)

Ein CASB unterstützt bei der Absicherung von Cloud-Diensten. Er bietet einen Überblick über sämtliche Anwendungen, darunter auch solche, die nicht autorisiert sind (Schatten-IT). Zudem schützt er vor unerlaubten Zugriffen und Datendiebstahl und überwacht die Einhaltung von Datenschutzbestimmungen und Branchenrichtlinien.



Firewall-as-a-Service (FWaaS)

FWaaS sichert den Datenverkehr ab und ist – im Gegensatz zu herkömmlichen, physischen Vorrichtungen – ein Cloud-Dienst. Verschiedene Sicherheitsfunktionen, darunter etwa Malware-Schutz, Intrusion Detection und Sandboxing werden dabei, je nach Anbieter, bereitgestellt. Auch anomaliebasierte Bedrohungserkennung und Standortbestimmung sind mögliche Leistungen der Firewall aus der Cloud.

Was zeichnet SASE aus?

Vergleicht man SASE mit klassischer Security, fällt als erstes die verteilte, dezentrale Sicherheitsarchitektur auf. Während bei Hub-and-Spoke-Architektur ein erfolgreicher Cyber-Angriff auf den zentralen Hub das gesamte Netzwerk lahmlegt, ist es wesentlich schwieriger, das gesamte Netzwerk bei verteilter Sicherheitsarchitektur zu treffen.

Auch in Bezug auf ihre Skalierbarkeit unterscheiden sich die Sicherheitsarchitekturen: Weil die Sicherheit bei SASE als Service aus der Cloud bereitgestellt wird, ist es wesentlich einfacher, sie zu skalieren. Denn das Management von Richtlinien oder Updates erfolgt trotz dezentraler Sicherheitsarchitektur zentral. Bei schnellem Unternehmenswachstum lassen sich Sicherheitsfunktionen so flexibel und unkompliziert erweitern. Auch die Einhaltung von Compliance-Regeln wird deutlich einfacher: Sicherheitsrichtlinien werden einmal definiert und an jedem Punkt des Netzwerkes ausgerollt. Das IT-Team wird durch die Integration von SASE in das Netzwerk entlastet, auch weil es sich nicht mehr um Patches und Updates kümmern muss.

Klassische Security ist Hardware-spezifisch. Sie muss auf sämtliche Endgeräte installiert und einzeln betrieben werden. Das bedeutet viel Aufwand für die Inbetriebnahme, Wartung und Aktualisierung. Kosten für Neuerungen sind schwer zu kalkulieren und ihre Durchsetzung erfolgt immer schrittweise. Sicherheit als Cloud-basierter Service vereinfacht diese Prozesse. Auf einen Klick können sämtliche Netzwerkenden auf den gewünschten Stand gebracht werden. Über ein Dashboard hat die IT stets alles im Blick und kann die frei gewordenen Kapazitäten anderweitig einsetzen. Das bedeutet auch geringere Kosten und eine bessere Planbarkeit.

SASE Services werden identitätsbasiert und kontextbasiert eingesetzt – das heißt, es werden maßgeschneiderte Richtlinien für individuelle Zugriffsrechte vergeben. Beispielsweise würde eine Mitarbeiterin in der Rechtsabteilung einen anderen Zugriff erhalten als ein externer Auftragnehmer, der projektbezogen in der Planungsabteilung arbeitet.

Klassische Security	vs.	SASE
Zentrale Perimeter-Sicherheit		Dezentrale, verteilte Sicherheit
Eingeschränkt skalierbar		Skalierbar
Hardware- und ortsspezifisch		Cloud-, identitäts- und kontextbasiert
Daten hauptsächlich im Unternehmen		Daten hauptsächlich außerhalb des Unternehmens

Zusammenfassung: **Software-definierte Netzwerke und SASE gehören zusammen**

Die zunehmende Nutzung von Cloud-Diensten verursacht hohe Traffic-Mengen, die häufig ineffizient über das Unternehmensnetzwerk geroutet werden. Hub-and-Spoke-Architektur kommt an ihre Grenzen. Unternehmen stellen deshalb auf SD-WAN und SD-(W)LAN um.

Resilienz

Das Software-definierte Netzwerk bietet stabile Performance. SASE ergänzt Sicherheit als Service für das gesamte Software-definierte Netzwerk. Sicherheitsrichtlinien können mit SASE zentral festgelegt und über Cloud-Systeme eingeführt werden, um sie am richtigen Punkt für Benutzer zu gewährleisten. Als Managed Security aus einer Hand reduziert SASE nicht zuletzt Kosten und Komplexität. IT-Infrastruktur wird so widerstandsfähig und krisenfest.

Agilität

Die Netzwerktransformation verlegt den Perimeter von zentraler Hub-and-Spoke-Architektur dezentral in die Cloud. Der Datenverkehr von und zu SaaS und Cloud wird so deutlich direkter geroutet – mit höherer Effizienz. Das bedeutet geringere Latenzen, verbesserte Konnektivität und eine positive Nutzererfahrung.

Dank ihrer Einbindung in die IT wird die Netzwerkarchitektur deutlich agiler. IoT, Industrie 4.0 und künftige Entwicklungen lassen sich flexibel und einfach testen und orchestriert umsetzen.

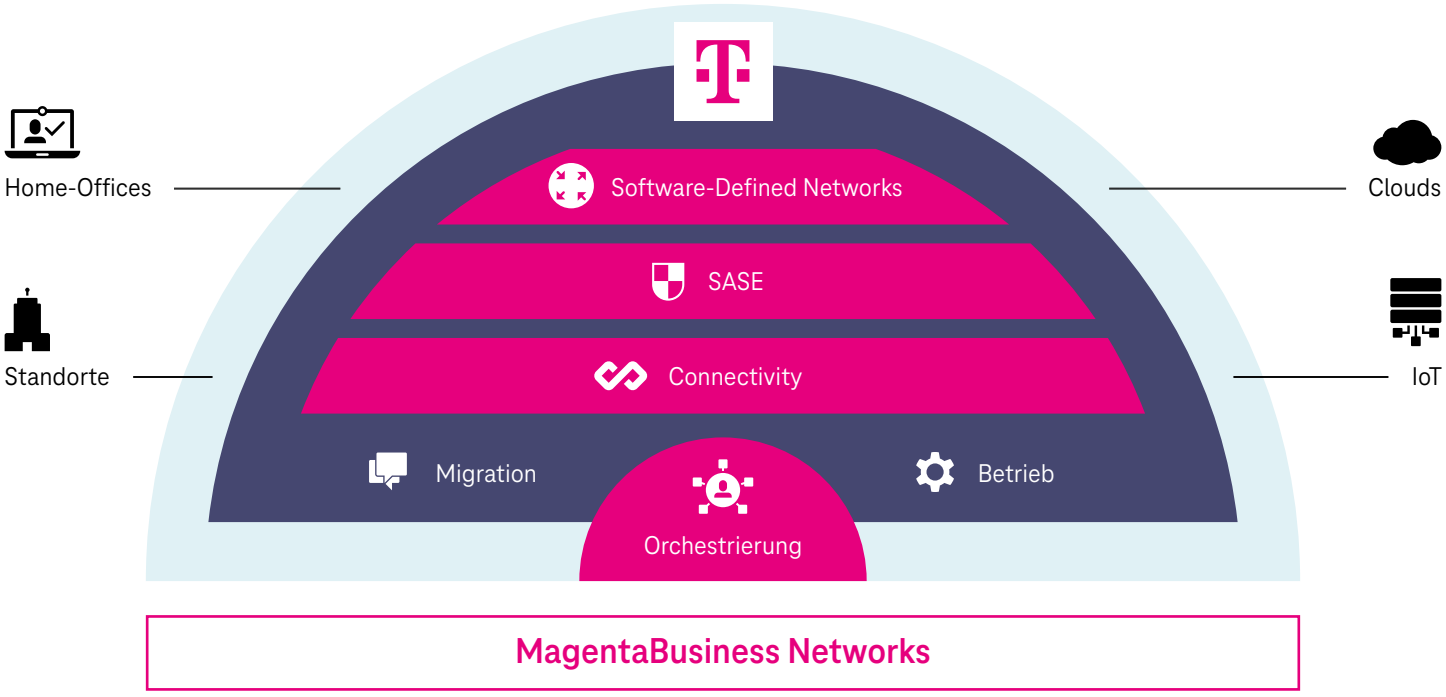
Mit der richtigen Kombination aus Software-definiertem Netzwerk und SASE sind Firmennetze bestens für die Zukunft gerüstet.

Sie wollen Ihr Netzwerk modernisieren?

Die Deutsche Telekom bietet mit MagentaBusiness Networks ein ganzheitliches Netzwerk-Portfolio. Unsere modernen Netze sind auch künftigen Anforderungen gewachsen. Möglich wird dies durch Software-Defined Networks, die die Software-Intelligenz von Hardware und Transportnetzen entkoppeln. Mit unseren SASE-Lösungen wird Sicherheit in die Netzarchitektur integriert. Wir bieten Ihnen umfassenden Service inklusive Migration und Betrieb. Damit Sie sicher und agil in die Zukunft starten können.

Software-definierte Netze der Telekom sind grün:
Seit 2021 surfen alle unserer 291 Millionen Kunden in einem Netz, das sich zu 100 % aus erneuerbaren Energien speist. Durch virtualisierte Services werden Material, Platz und Strom eingespart. Zero Touch Deployment und zentrale Steuerung bedeuten zudem, dass weniger Techniker-Fahrten anfallen. Unser Ziel: Mehr Nachhaltigkeit, mehr Verantwortung, mehr digitale Teilhabe.

#GREEN MAGENTA #GOOD MAGENTA



SD-X: Die Plattform der Telekom für das Netzwerk der Zukunft

Mit SD-X, der Software-Defined Everything Plattform der Telekom, haben Sie den perfekten Überblick über alle Komponenten Ihres Netzwerks: vom SD-WAN über SD-LAN und WIFI bis zu SASE Services und Transportnetzen. Denn die SD-X Plattform automatisiert das Management der technischen UND alle weiteren Prozesse: IT-Service-Management und kommerzielle Prozesse von der Bestellung über die Konfigurationsänderung bis zum Inzidenzmanagement, von Changes und Reportings bis zu Analysen. Als ServiceNow-Plug-In können Sie SD-X in ihre ServiceNow-Umgebung integrieren. Oder Sie greifen auf die in Deutschland gehostete ServiceNow-Plattform der Telekom zurück.

Legen Sie den Grundstein für Ihr Firmennetz der Zukunft!

Noch Fragen?

Wir beraten Sie gerne ausführlich zu den Themen Software-definierte Netzwerke und SASE. Kontaktieren Sie uns.

sd-wan@telekom.de

Oder besuchen Sie unsere Website

Herausgeber
Telekom Deutschland GmbH
53262 Bonn
www.telekom.de

Erleben,
was verbindet.