Präsentation des Zero Trust Edge-Modells für Sicherheits- und Netzwerkdienste

Ein Secure Access Services Edge (SASE) ist ein Zero Trust Edge (ZTE)

von David Holmes und Andre Kindness

28. Januar 2021

Warum Sie diesen Bericht lesen sollten

Viele Netzwerkteams haben sich bei der Unternehmensdigitalisierung über die Cloud und das Internet der Dinge (Internet of Things, IoT) für ein SD-WAN entschieden. Ein SD-WAN erfüllt jedoch weder die neuen Sicherheitsanforderungen noch berücksichtigt es, dass Sicherheit und Netzwerke untrennbar miteinander verbunden sein müssen. Sowohl I&O- als auch S&R-Experten sollten diesen Bericht lesen, um Einblick in das noch relativ neue Zero Trust-Konzept zu gewinnen. Es vereint Netzwerk- und Sicherheitsinfrastruktur mit dem Ziel, eine unternehmensweite Netzwerkstruktur zu schaffen.

Die wichtigsten Schlussfolgerungen

Die Sicherheitsaspekte machen ZTE für Unternehmen attraktiv

Bei den meisten Unternehmen, die sich für Zero Trust Edge (ZTE) entscheiden, wird die Priorität darin bestehen, Mitarbeitern im Homeoffice sicheres und reibungsloses Arbeiten zu ermöglichen. Im Zuge dessen werden sie gleichzeitig die lästigen VPNs abschaffen, die in der modernen Industrie für so viel Kopfzerbrechen sorgen.

Das Ziel ist ein am Internet-Edge gehosteter Sicherheits-Stack, aber der Weg dorthin ist noch weit

Aus dem ZTE-Modell soll sich ein allumfassender Cloud- bzw. Edge-gehosteter Sicherheits-Stack entwickeln. Die Technologie ist jedoch aufgrund verschiedener Abhängigkeiten noch nicht ausgereift genug dafür. Solange beispielsweise die Bandbreite in vielen Teilen der Welt noch eingeschränkt ist, müssen einige Elemente lokal gehostet werden.

In puncto Effizienz sollte der intelligente On-Premise-Edge nicht vernachlässigt werden

Es gibt weiterhin gute Gründe für intelligente On-Premise-Entscheidungen am Edge, insbesondere für IoT/OT, Gesundheitswesen und stark vernetzte Umgebungen.

Präsentation des Zero Trust Edge-Modells für Sicherheits- und Netzwerkdienste

Ein Secure Access Services Edge (SASE) ist ein Zero Trust Edge (ZTE)

von David Holmes und Andre Kindness
mit Glenn O'Donnell, Joseph Blankenship, Paul McKay, Renee Taylor und Peggy Dostie

28. Januar 2021

Inhaltsverzeichnis

Zugehörige Forschungsdokumente

Evaluate SDWAN Services Based On Branch Office Goals, Not Hardware Data Sheets (Auswerten von SD-WAN-Diensten auf der Grundlage der Ziele von Zweigstellen anstatt von Hardware-Datenblättern)

Now Tech: Software Defined WAN Hardware/ Software, Q3 2020 (Now Tech: Softwaredefinierte WAN-Hardware/-Software, Q3 2020)

Now Tech: Software-Defined WAN Services, Q3 2020 (Now Tech: Softwaredefinierte WAN-Dienste, Q3 2020)

FORRESTER®

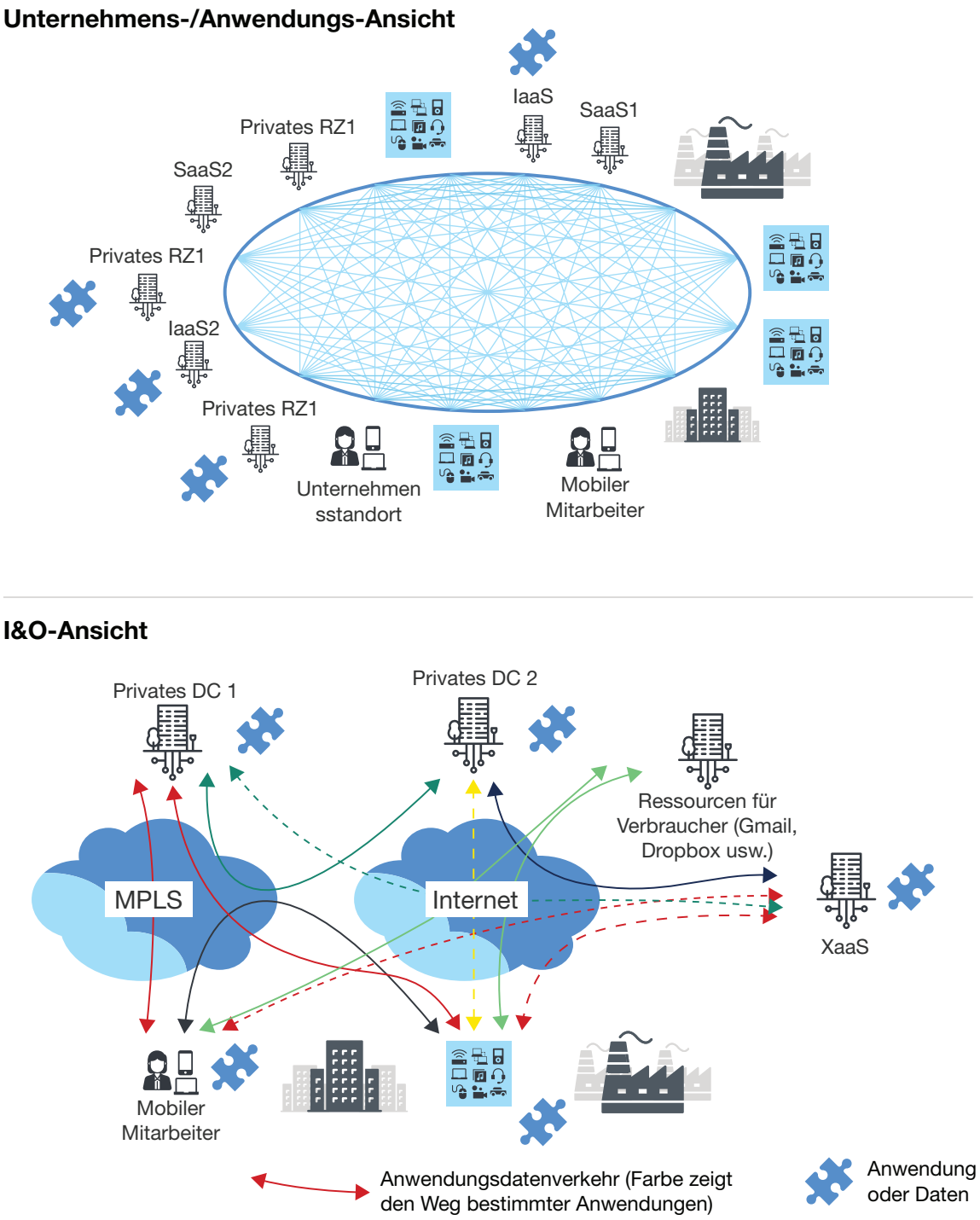
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Sicherheit und Netzwerke müssen heute Hand in Hand gehen

Netzwerke und Sicherheit blicken auf eine lange und komplizierte gemeinsame Geschichte zurück. Ihr Verhältnis lässt sich bestenfalls als höflich und schlimmstenfalls als geradezu feindselig beschreiben. Beide voneinander getrennt zu betrachten, ist jedoch nicht mehr sinnvoll, denn dadurch werden allzu oft die Vorteile digitaler Initiativen zunichte gemacht. Isolierte Netzwerk- und Sicherheitsinfrastrukturen und -betriebsabläufe werden bald der Vergangenheit angehören. Die Gründe:

- **Verteilte Cloud-Anwendungen und -Daten befinden sich außerhalb des Rechenzentrums.** Die Bestandteile der Digitalisierung – Cloud, Edge und IoT – definieren nicht nur den Speicherort von Daten und Anwendungen neu, sondern haben auch das traditionelle Hub-and-Spoke-Netzwerkdesign ins Aus befördert.[1] Mittlerweile verbindet eine unternehmensweite Netzwerkstruktur Unternehmensressourcen, Kunden, Partner und digitale Ressourcen miteinander, um alle Teile des Geschäftsökosystems zu vernetzen (siehe Abbildung 1).[2] Wie der Forrester-Bericht „Build Security Into Your Network's DNA: The Zero Trust Network Architecture“ (Machen Sie die Sicherheit zum festen Bestandteil der DNA Ihres Netzwerks: Die Zero Trust-Netzwerkarchitektur) verdeutlicht, ist dies nur möglich, wenn die Sicherheit in die DNA des Netzwerks integriert ist.
- **Infolge von COVID-19 befinden sich Mitarbeiter jetzt außerhalb der Kontrolle des Unternehmens-LANs.** Viele Unternehmensanwendungen sind mittlerweile cloudbasiert, und es kommen immer mehr hinzu. Auch die Benutzer haben nun die traditionellen Unternehmensgrenzen verlassen. Die Studie von Forrester zu den Erfahrungswerten während der Pandemie ergab, dass 53 % der neuen Telearbeiter auch nach der Krise weiter remote arbeiten möchten.[3] Wenn sich weder die Anwendungen noch die Benutzer weiterhin innerhalb der Unternehmensgrenzen befinden, wird klar, dass die traditionellen, auf diesem Konzept basierenden Sicherheits-Stacks ausgedient haben.

ABBILDUNG 1 Die Verteilung von Anwendungen und Daten über die Unternehmensressourcen hinweg



Traditionelle Sicherheits- und Netzwerkansätze sind für das dezentrale Unternehmen nicht geeignet

Durch die Pandemie im Jahr 2020 wurden Millionen von Mitarbeitern aus der komfortablen Schutzzone innerhalb der Unternehmensgrenzen gerissen und in die Welt der Remote-Arbeit katapultiert. Ein CISO bei einem großen europäischen Versicherungsunternehmen gab an, dass die Remote-Arbeit in seinem Unternehmen vor der Coronakrise 2020 nur 5 % ausmachte. Durch die Pandemie wurde dieser Status quo auf den Kopf gestellt, und 95 % der Mitarbeiter arbeiten nun im Homeoffice. Wie bei vielen anderen Unternehmen konnte die ohnehin schon instabile VPN-Infrastruktur des Versicherungsanbieters diese Last nicht verkraften. Dies deutet daraufhin, dass VPN-Technologie für die Anforderungen moderner Unternehmen einfach nicht mehr geeignet ist. Die neuen Anforderungen, die sich aus der Nutzung von Cloud-Computing und der Unterstützung von Remote-Mitarbeitern ergeben, haben sowohl Netzwerk- als auch Sicherheitsteams vor Herausforderungen gestellt. Der Grund dafür sind veraltete Ansätze, wie beispielsweise:

- **Dedizierte Software- oder Hardware-Appliances vor Ort.** In der Vergangenheit war es so, dass sich ein Technologieproblem in der Regel mit einer bestimmten Art von Lösung beheben ließ. Wenn jedoch über dreißig Jahre hinweg immer wieder Geräte wie WAN-Optimierer oder Firewalls zu einem Netzwerk hinzugefügt werden, hinterlässt dies Spuren: mehr Sicherheitsprobleme, mehr Komplexität, weniger Flexibilität und weniger Effizienz. Mit jedem weiteren neuen Gerät nehmen die Komplexität und die potenziellen Sicherheitsprobleme exponentiell zu.
- **Unzuverlässige On-Premise-Kontrollen und -Richtlinien-Repositorys.** Management-Software vor Ort erfordert spezielle Hardware sowie Mitarbeiter, die jeweils die neuesten Funktionen, Fehlerbehebungen und Sicherheitsverbesserungen aufspielen. Befindet sich die Management-Software in einer privaten Infrastruktur, bedeutet dies nicht nur höhere Kosten für das Unternehmen, sondern auch eine geringere Ausfallsicherheit. Die Migration auf Cloud-Plattformen stand bei der Entwicklung der Software üblicherweise nicht im Vordergrund. Dadurch sind sowohl ihre Effektivität als auch die Disaster-Recovery-Optionen eingeschränkt.
- **Einschränkender hardwareorientierter Ansatz.** Für Flugzeuge, Fahrzeuge und Züge gelten aufgrund von Gewichts- oder Größenauflagen Passform- und Formbeschränkungen. Doch selbst ohne diese Beschränkungen können Technologie-Teams nicht davon ausgehen, dass Hardware für alle Bereiche einer Produktionsstätte, eines Einzelhandelsgeschäfts oder eines Stadions geeignet ist. Es ist also nicht sinnvoll vorauszusetzen, dass Hardware so gebaut werden kann, dass sie beispielsweise zwischen Kunststoff-Extruder und Heizkammer passt oder den Temperaturen in einem elektrischen Umspannwerk in Dubai oder einem Mobilfunkturm im Death Valley standhält.
- **Unzusammenhängende Sicherheits- und Netzwerksilos.** Wenn bestimmte Arten von Hardware und Betriebsabläufen auf bestimmte Gruppen beschränkt werden, erhöht dies die betrieblichen Ineffizienzen weiter, verringert die Ausfallsicherheit der Infrastruktur und führt möglicherweise zu neuen Sicherheitsproblemen. Viele separate Geräte wie Firewalls und Router könnten kombiniert werden, um die Latenz zu reduzieren, indem eine zentrale Tabelle zum Nachschlagen von Regeln für Pakete und zum Anwenden von Sicherheits- und Netzwerkrichtlinien am Port eingesetzt wird.

Die Entstehung von Zero Trust Edge

Aufgrund der Coronakrise waren Mitarbeiter gezwungen, von zu Hause aus zu arbeiten. Dies veranlasste eine zukunftsorientierte Minderheit von Sicherheitsexperten, die VPN-Technologie für ungeeignet hielten, in ZTNA-Lösungen (Zero Trust Network Access) zu investieren, um die Probleme mit VPNs zu umgehen. Einige der ZTNA-Verfechter fragten sich daraufhin, wo sie ZT eventuell noch einsetzen könnten, auch wenn viele Sicherheits- und I&O-Experten Zero Trust in erster Linie für ein Rechenzentrumskonzept hielten (siehe Abbildung 2).[4] Das im Forrester-Bericht „The Zero Trust eXtended (ZTX) Ecosystem“ [Das ZTX-Ökosystem (Zero Trust eXtended)] dargelegte Sicherheits-Framework zeigt jedoch, dass ZT weit mehr als nur ein Rechenzentrumskonzept ist. ZT schützt Unternehmen vor Kunden, Mitarbeitern, Auftragnehmern und Geräten an Remote-Standorten, die über WAN-Strukturen mit einer raueren, offeneren, gefährlicheren und turbulenteren Umgebung verbunden sind (siehe Abbildung 3). Forrester bezeichnet dieses Konzept als Zero Trust Edge (ZTE) und definiert es wie folgt:

> *Eine Zero Trust Edge-Lösung sorgt mit Zero Trust-Zugriffsprinzipien für die sichere Verbindung und Übertragung des an Remote-Standorten ein- und ausgehenden Datenverkehrs. Dabei werden hauptsächlich Cloud-basierte Sicherheits- und Netzwerkdienste genutzt.*

ABBILDUNG 2 Die ersten ZT-Anwender nutzen Sicherheitsmikroperimeter nur im Zusammenhang mit VMs

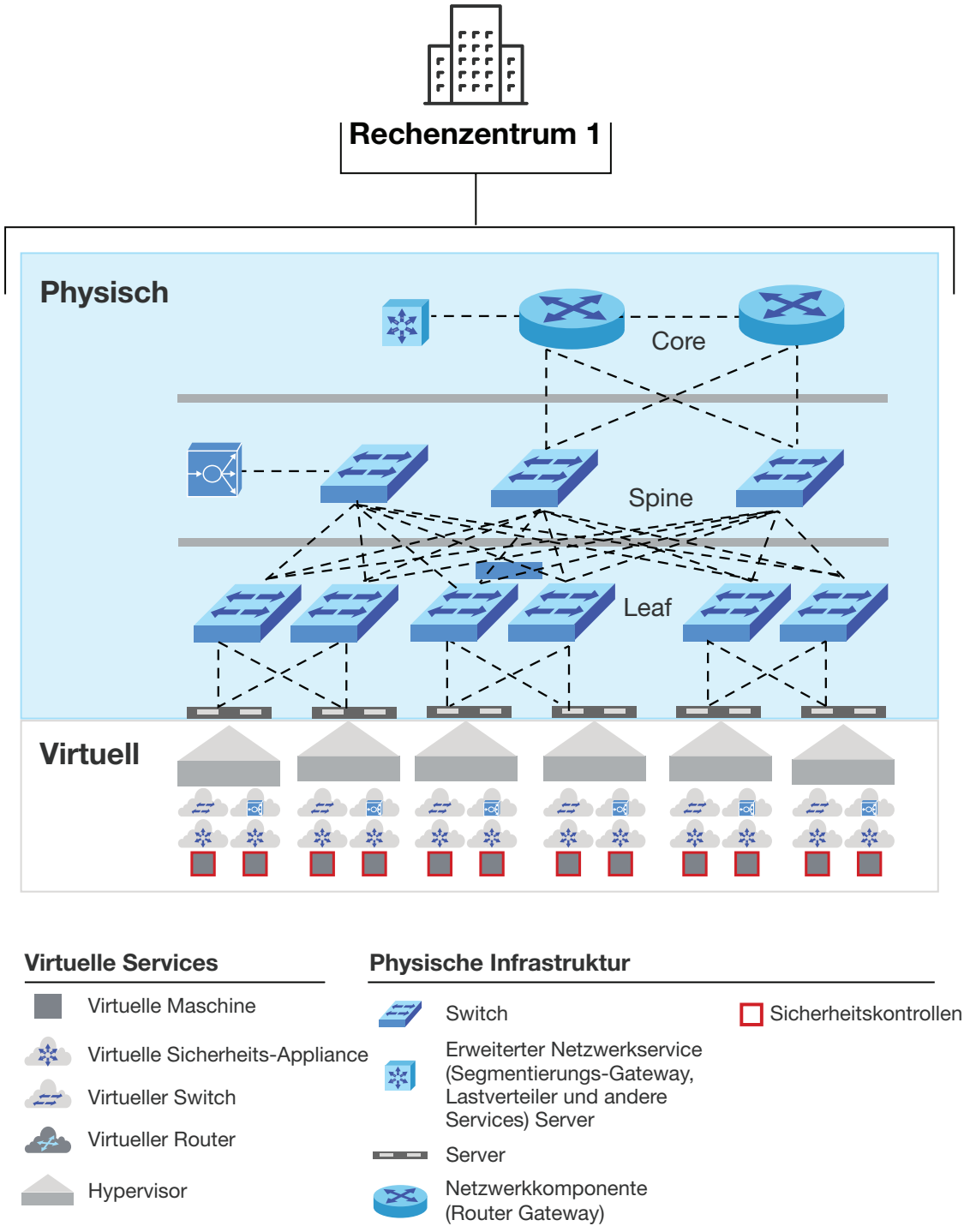
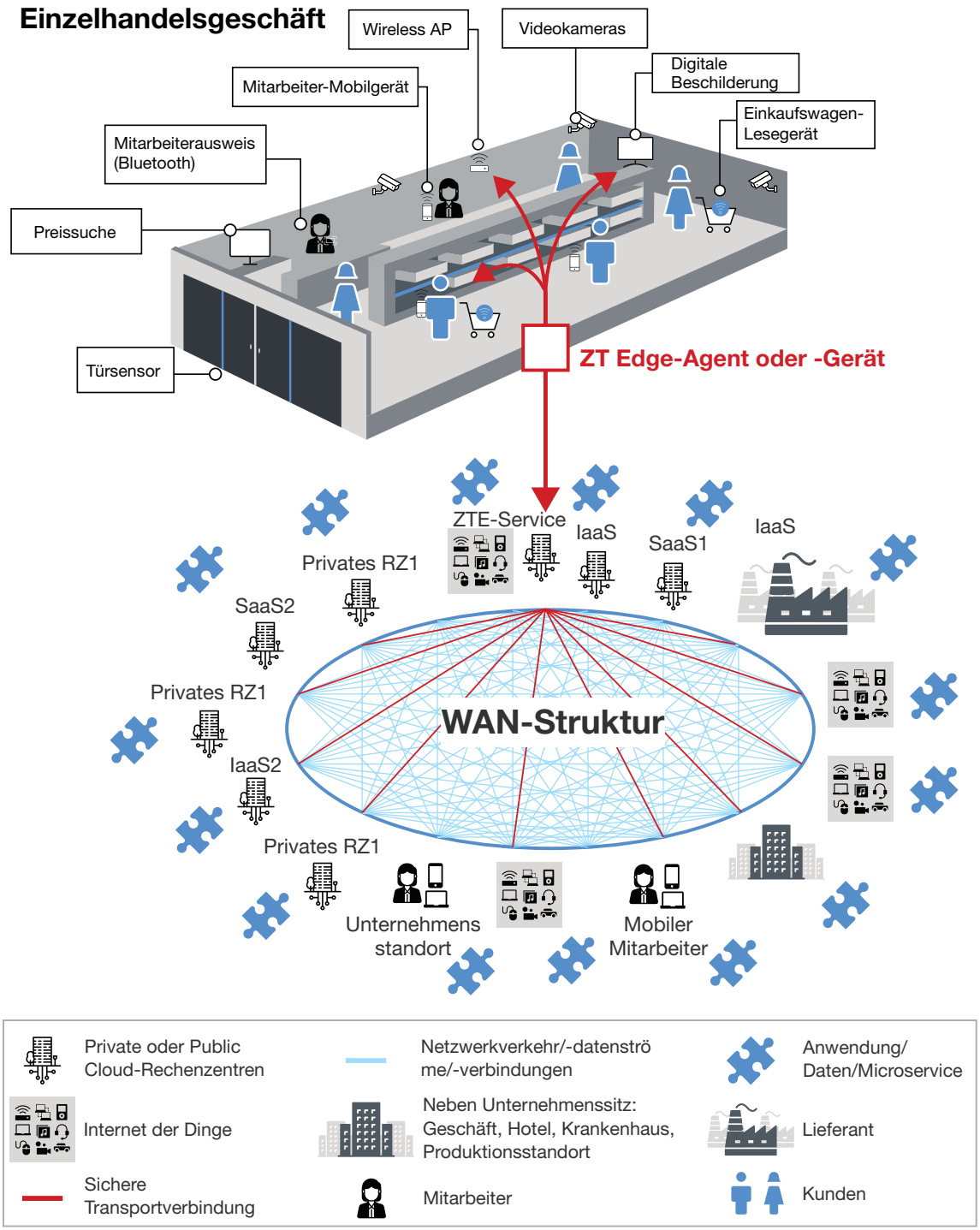


ABBILDUNG 3 ZTE liefert die Sicherheitskontrollen und Netzwerkrichtlinien für den Schutz aller Verbindungen vor Ort



Überraschung! ZTE beginnt in der Cloud

ZTE etabliert das Sicherheits- und Netzwerk-Framework für den Datenverkehr und die Dienste, die von Remote-Standorten aus in Unternehmen eingehen, sowie die Dienste, die an die Standorte oder Benutzer zurückgehen. ZTE ist eine gute Option für dezentrale Unternehmen, setzt aber gleichzeitig voraus, dass die Lösungen, die schnellere und flexiblere Dienste ermöglichen, auf zwei fundamentalen Elementen beruhen:

- **Cloud-basiertes Netzwerk- und Sicherheitsmanagement.** In der Vergangenheit befanden sich Gerätekonfigurationen und Sicherheitsrichtlinien in verschiedenen Tools. Beispielsweise enthielten Netzwerkzugriffskontrollen die Sicherheitsrichtlinien für Benutzer, während Managementlösungen für Firewalls und Netzwerkkomponenten die Gerätekonfigurationen umfassten. Dies erhöht jedoch die Anzahl der Konfigurationsfehler und verringert die betrieblichen Effizienzen, da Mitarbeiter über mehrere Systeme hinweg ähnliche Richtlinien einrichten. Mit Cloud-Management können diese heterogenen Back-End-Systeme zusammengeführt werden. So ist es möglich, Konfigurationen über eine einzige Konfigurationsmanagementlösung zu ändern, hinzuzufügen oder zu löschen.
- **Cloud-basierte Überwachung und Analyse.** Netzwerk- und Sicherheitsüberwachung sind in der Regel voneinander unabhängig und gehören zu den Grundvoraussetzungen für ZTE. Google ist ein gutes Beispiel dafür – es nutzt sein softwaredefiniertes WAN, um eine 100%ige Link-Auslastung zu erreichen. Durch die Überwachung werden Unregelmäßigkeiten im Datenverkehr – häufig Sicherheitsprobleme – bis hin zu den Peering-POPs (Points of Presence) und in großer Entfernung zu den Rechenzentren des Unternehmens identifiziert.[5] Aufgrund der Menge an Daten, die erfasst und synthetisiert werden muss, ist eine Cloud-basierte ZTE-Überwachung erforderlich. Es wird dabei eine solch umfangreiche Rechenplattform benötigt, um eine vollständige Analyse zu ermöglichen.

Einsatz von ZTE zur Bereitstellung von 18 Sicherheits- und Netzwerkdiensten

Unternehmen können die in ZTE-Lösungen enthaltenen Sicherheits- und Netzwerkdienste von überall auf der Welt aus zentral verwalten, überwachen und analysieren (siehe Abbildung 4). Einige der Dienste verbleiben ausschließlich in der Cloud (oder am Cloud-Edge), andere wiederum müssen am Remote-Standort gehostet werden.

ABBILDUNG 4 Art der in einer ZTE-Lösung verfügbaren Dienste

Netzwerk

Bandbreitengarantie	Legt eine minimale Bandbreite für bestimmten Datenverkehr fest
Caching von Inhalten	Stellt lokalisierte Kopien von Daten bereit
Link-Lastausgleich und -Auslastung	Nutzt mehrere Links gleichzeitig, um die Bandbreite des Datenverkehrs und die WAN-Auslastung insgesamt zu erhöhen
Servicequalität	Priorisiert den Netzwerkverkehr
Ausfallsicherheit	Stellt bei Fehlern und Herausforderungen im Normalbetrieb einen akzeptablen Servicelevel bereit und erhält ihn aufrecht
Routing/bester Pfad	Wählt den richtigen Pfad für Layer-3-Transport aus, selbst vom Remote Mitarbeiter zu einer Anwendung in der Cloud
Softwaredefiniertes WAN (SD-WAN)	Wählt die besten Pfade, Links oder Verbindungen basierend auf übergeordneten Metriken aus, wie Jitter, verlorene Pakete und Affinität zu einem Anwendungsprofil
WAN-Verbindung	Stellt die physische Verbindung zu/von einem Standort her
WAN-Optimierung	Bietet Deduplizierung, Paketverschmelzung und andere WAN-Optimierungsfunktionen

ABBILDUNG 4 Art der in einer ZTE-Lösung verfügbaren Dienste (Forts.)

Sicherheit

Einfache Firewall	Bietet einfache Netzwerk-Firewall-Funktionen (Regeln für Layer 3 und 4), die abgetrennt und lokal eingesetzt werden können, um den Datenverkehr von dem Remote-Standort zu reduzieren
Cloud Access Security Broker (CASB)	Kontrolliert und meldet den Zugriff auf Cloud-Anwendungen
Firewall-as-a-Service (FWaaS)	Bietet Cloud-basierte erweiterte Firewall-Merkmale und -Funktionen
Intrusion Detection System/Intrusion Prevention System (IDS/IPS)	Analysiert den Netzwerkverkehr anhand von Signaturen, um bestimmte schädliche Inhalte zu erkennen und abzuwehren
Link-Verschlüsselung	Verschlüsselt und entschlüsselt den gesamten Netzwerkverkehr an jedem Netzwerk-Routing-Punkt
Identitäts- und Zugriffsverwaltung (IAM)	Stellt sicher, dass befugte Mitarbeiter in einem Unternehmen angemessenen Zugriff auf Technologieressourcen erhalten
Secure Web Gateway (SWG)	Verhindert, dass ungesicherter Datenverkehr in ein internes Netzwerk einer Organisation gelangt; URL-Filter müssen ständig aktualisiert werden, und der Trend ging bereits dahin, diese in der Cloud zu konfigurieren, zu hosten und zu warten
Erweiterte Malware-Analyse	Führt Programme in einer geschlossenen Umgebung (Sandbox) aus, um Zero-Day-Malware abzufangen und zu isolieren
Zero Trust Network Access (ZTNA)	Ermöglicht Remote-Mitarbeitern, sich anhand ihrer Identität mit Unternehmensanwendungen zu verbinden, egal wo sich die Mitarbeiter oder die Anwendungen befinden; dies ist der unverzichtbare Signature-Sicherheitsdienst im ZTE.

Die Arten und Standorte von ZTE-Diensten richten sich nach den Anwendungsfällen

Netzwerk- und Sicherheitsarchitekten, die zunehmend auf Zero Trust Edge setzen, müssen den maximalen Nutzen sicherstellen. Welche Arten von Diensten verwendet werden, hängt vom Standort, von den Geräten, den Benutzern und anderen Elementen ab (siehe Abbildung 5). Drei Anwendungsfälle zeigen den Anstieg zwingend notwendiger Funktionen (was bedeutet, dass immer mehr Netzwerk- und Sicherheitsdienste innerhalb der ZTE-Lösung aktiviert werden):

- **Mitarbeitern die sichere Remote-Arbeit ermöglichen.** Durch die Pandemie im Jahr 2020 mussten Millionen von Wissensarbeitern plötzlich vom Büro ins Homeoffice wechseln. Die Bereitstellung des sicheren Zugriffs auf Unternehmensdienste und -anwendungen für diese

Homeoffice-Mitarbeiter ist der erste Anwendungsfall, aus dem sich Unternehmen für Zero Trust Edge entscheiden. Aufgrund vieler der in der Forrester-Studie „Key Considerations For Network And Capacity Management When Operationalizing A Home-Based Workforce“ (Wichtige Überlegungen im Hinblick auf das Netzwerk- und Kapazitätsmanagement bei der Operationalisierung einer Belegschaft im Homeoffice) dargelegten Herausforderungen verzichten die meisten Unternehmen darauf, jedwede Art von Netzwerk-Software oder -Hardware im Homeoffice bereitzustellen. Stattdessen werden Software-Agents auf den Arbeitsgeräten der Mitarbeiter bereitgestellt und ihre Verbindungen mit Cloud-Edge-Sicherheitsdiensten verknüpft (siehe Abbildung 6).

- **Den im Zweigstellen-WAN vorherrschenden Datenverkehr von Geschäftsanwendungen priorisieren.** Die Anzahl der WAN-Verbindungen ist aufgrund der gestiegenen Zahl von Mitarbeitern im Homeoffice in die Höhe geschnellt. Dennoch machen Remote-Büroverbindungen, die hauptsächlich von Mitarbeitern, ihren Anwendungen und unternehmenseigenen Geräten hergestellt werden, den Großteil des WAN-Datenverkehrs in einem Unternehmen aus. Der SaaS-Datenverkehr, wie z. B. O365, hat sich in der letzten Zeit zu einem wichtigen Faktor entwickelt und kann auch einen Teil des Kundenverkehrs beinhalten. SaaS-basierter Anwendungsdatenverkehr erfordert direkte Verbindungen zum Internet, und Kunden müssen möglicherweise eine Verbindung zu LANs von Remote-Büros herstellen. Um diese Herausforderungen zu bewältigen, leiten Unternehmensarchitekten den betreffenden Datenverkehr zunehmend durch Firewall-as-a-Service (FWaaS). Dies geschieht entweder über Router von Remote-Büros und/oder über SD-WAN-Lösungen, die im Forrester-Bericht „Now Tech: Software-Defined WAN Hardware/Software, Q3 2020“ (Now Tech: Softwaredefinierte WAN-Hardware/-Software, Q3 2020) beleuchtet bzw. von einem im Forrester-Bericht „Now Tech: Software-Defined WAN Services, Q3 2020“ (Now Tech: Softwaredefinierte WAN-Dienste, Q3 2020) aufgeführten Dienstanbieter bereitgestellt werden (siehe Abbildung 7). Einige Anbieter, darunter Forcepoint, unterstützen SD-WAN-Funktionen, die in mehrere Sicherheitsdienste integriert sind.
- **Die Sicherheit des Internets aller Dinge gewährleisten.** Neben Homeoffice-Mitarbeitern und generischen Zweigstellen nutzen auch IoT- und Edge-Geräte sowie Geschäftspartner das Netzwerk. Der Architekt des industriellen Steuerungssystems (Industrial Control System, ICS) muss zugehörige Standorte integrieren, wodurch ein noch größeres Augenmerk auf Sicherheits- und Netzwerkrichtlinien gerichtet werden muss. So muss ein Ingenieur in einem Automobilwerk nicht nur den Datenverkehr von Mitarbeitern und Auftragnehmern berücksichtigen, sondern auch den von speicherprogrammierbaren Steuerungen (SPS) von Siemens oder den von Regalgewichten im Rahmen der Bestandsaufnahme von Bosch. Standortbedingt und mangels ausreichender Bandbreite am Standort müssen einige grundlegende Sicherheitselemente zusammen mit allen Netzwerkdiensten vor Ort gehostet werden, um den zu den Cloud-Sicherheitsdiensten geleiteten Datenverkehr zu verringern (siehe Abbildung 8).

ABBILDUNG 5 Bei jedem Anwendungsfall müssen unterschiedliche Sicherheits- und Netzwerkfaktoren berücksichtigt werden

	Remote-Arbeit	Kleines Büro	Heterogener Standort
Ressourcen	Laptop	Desktops, Drucker, Konferenzräume, Webcams	Heterogenes physisches Netzwerk
ZTE-Gateway	Endpoint-Agent	WAN-Gerät mit erforderlichen Netzwerkdiensten vor Ort oder per Agent-Overlay	WAN-Gerät mit erforderlichen Netzwerkdiensten vor Ort
IoT	Nein	Niedrig	Hoch
Edge-Computing	Nein	Niedrig	Hoch
Auftragnehmer	Nein	Nein	Ja
Geschäfts- und Technologieanbieter	Nein	Niedrig	Hoch

ABBILDUNG 6 Mitarbeiter im Homeoffice profitieren von Cloud-basierten ZTE-Sicherheitsdiensten

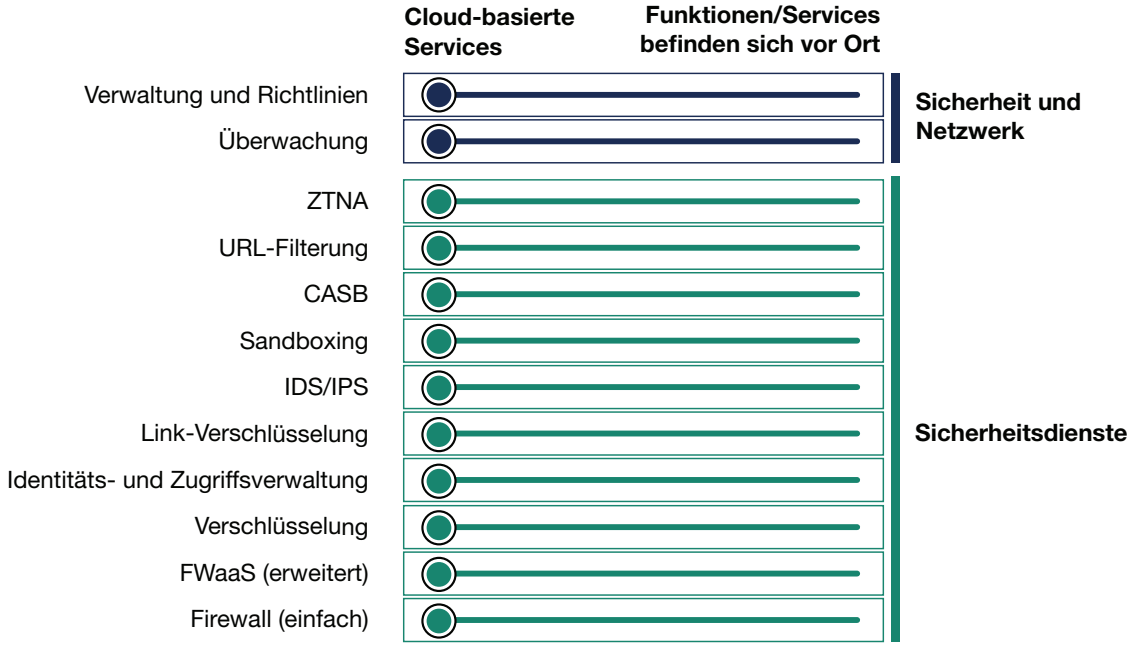


ABBILDUNG 7 Generische Unternehmensstandorte leiten den Datenverkehr zu Cloud-basierten Sicherheitsdiensten

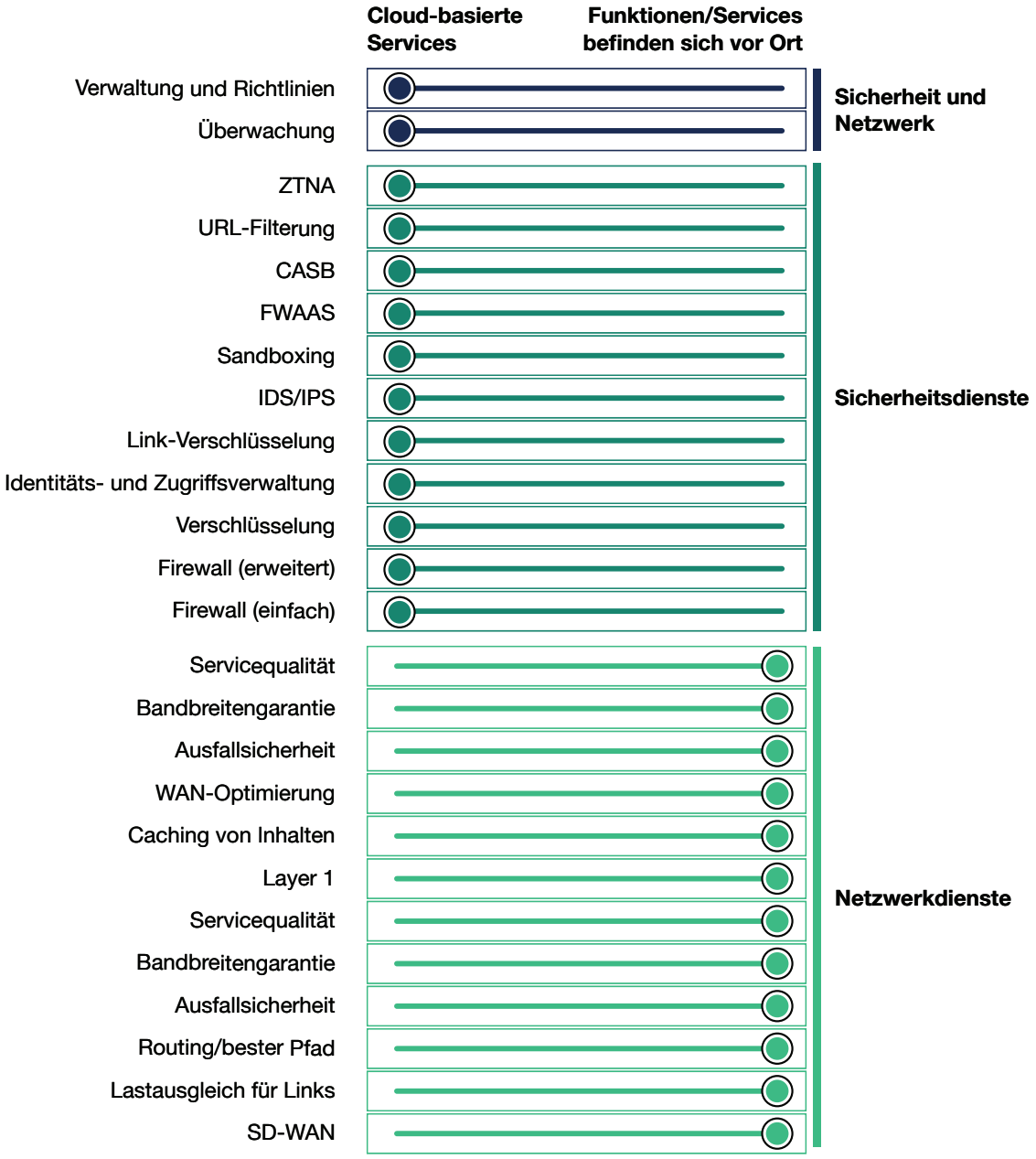
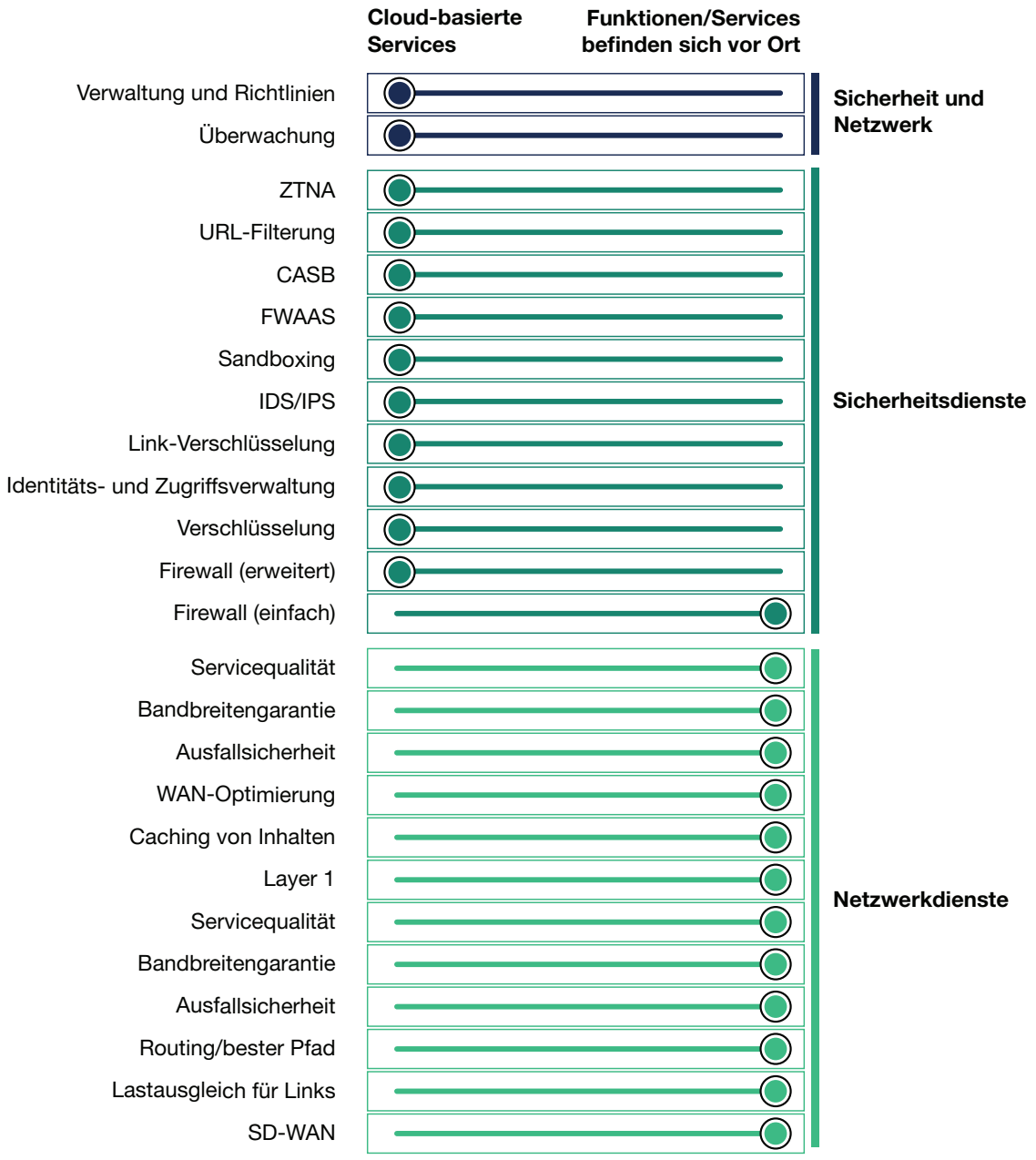


ABBILDUNG 8 Aufgrund komplexer Standorte mit begrenzter WAN-Bandbreite müssen einige Sicherheitsfunktionen lokal gehostet werden



Die verschiedenen Arten von ZTE-Optionen

Technologieexperten stehen drei verschiedene Methoden zur Nutzung von ZTE zur Verfügung:

- **Ein Cloud-basierter Dienst.** Die Cloud-basierten ZTE-Dienste stammen von einem von mehreren relativ neuen Anbietern bereitgestellten Dienst wie Cato Networks und nutzen ein Drittanbieternetzwerk mit Dutzenden – oder in einigen Fällen Hunderten – von POPs, die ZTE-Funktionen am Cloud-Edge bereitstellen. Dieser Ansatz bietet Unternehmen das volle Potenzial von Software-as-a-Service-Lösungen. Allerdings kann kein Unternehmen alle Funktionen bieten, die in den branchenführenden Lösungen zu finden sind. Forrester hat jedoch auch herausgefunden, dass Unternehmen in der Regel nicht alle Funktionen von On-Premise-Lösungen nutzen. Cloud-Lösungen werden häufig den Anforderungen vieler verschiedener Unternehmen gerecht.
- **ZTE-Dienste in Kombination mit einem WAN-Verbindungsdienst.** Andere ziehen einen bestehenden Betreiber von Unternehmensnetzwerken hinzu, der die Kunden direkt mit ZTE-Netzwerken für ausgelagerte Sicherheitsfunktionen verbindet. Comcast Enterprise und Akamai bieten diesen Service bereits. Viele SD-WAN-Hardware- und -Softwareanbieter wie Versa Networks unterhalten Partnerschaften mit Zscaler oder anderen Sicherheitsanbietern. So können Teams die jeweils besten Produkte auswählen, um sicherzustellen, dass sie sowohl Netzwerk- als auch Sicherheitsdienste optimal nutzen. Diese Teams profitieren jedoch nicht von der betrieblichen Agilität oder Effizienz Cloud-basierter Systeme. Ein kombinierter Ansatz aus SD-WAN und ZTE erfordert, dass Technologieteams zusätzliche Schritte durchführen, wie z. B. das Einrichten von Richtlinien für jeden unabhängigen Dienst. Es gibt kein zentrales Management- und Orchestrierungssystem für eine kombinierte Strategie aus SD-WAN und ZTE.
- **Ein Do-it-yourself-Ansatz (DIY).** Ein ausreichend großes und agiles Unternehmen könnte eine eigene ZTE-Plattform mit Cloud-Dienstanbietern als POPs und einem Cloud-gehosteten Service wie der Unternehmens-Firewall von Barracuda als Sicherheitsdienst in der Azure-Cloud von Microsoft einrichten. Dadurch wird sichergestellt, dass die Dienste den Geschäftsanforderungen besser entsprechen. Die Teams müssen in diesem Fall aber auch über das richtige Gespür für die Geschäftsanforderungen und über die erforderlichen Kompetenzen verfügen, um die entsprechende Infrastruktur aufzubauen und zu verwalten. Aus dem Forrester-Bericht „Evaluate SDWAN Services Based On Branch Office Goals, Not Hardware Data Sheets“ (Auswerten von SD-WAN-Diensten auf der Grundlage der Ziele von Zweigstellen anstatt von Hardware-Datenblättern) geht hervor, dass den meisten Teams mindestens eine dieser Voraussetzungen fehlt.

Sicherheits-Stacks: Mehrere Anbieter oder ein einziger Anbieter?

ZTE stellt eine existenzielle Bedrohung für viele On-Premise-Sicherheitslösungen dar, daher ist eine ZTE-Strategie für diese Anbieter jetzt von entscheidender Bedeutung. Ambitionierte Anbieter möchten Ihnen am liebsten das gesamte schlüsselfertige Paket verkaufen (sofern sie eines haben). Für KMU/mittelständische Unternehmen ist die Vorstellung, einen einzigen Anbieter für alle Sicherheitslösungen auf OPEX-Basis zu haben, sehr verlockend. Ihre eigene Entscheidung hängt von der Größe und Komplexität Ihres Unternehmens ab:

- **Größere Unternehmen entscheiden sich auf kurze Sicht eher für einen Ansatz mit mehreren Anbietern.** Sie haben komplexere Anforderungen und heterogenere Dienste. Aufgrund der höheren Anzahl älterer Anwendungen ist die Wahrscheinlichkeit geringer, dass sie sich für einen einzigen

Anbieter entscheiden. Die Befragten dieser Studie waren sich im Hinblick auf diese Analyse weitgehend einig. Bei Unternehmen, die bereits auf Zero Trust Edge setzen, kann ein typischer Ansatz mit mehreren Anbietern so aussehen, dass sie Silver Peak Systems für das SD-WAN und eine Verbindung zu Zscaler für URL-Filterung und ZTNA nutzen. Dies funktioniert beim ersten Anwendungsfall (Mitarbeitern die sichere Remote-Arbeit ermöglichen), aber die Migration anderer Elemente des Sicherheits-Stacks zu einem Stack mit mehreren Anbietern erfordert eine Verkettung von Diensten im großen Maßstab, und die APIs zwischen den Komponenten müssen durchgängig und zuverlässig funktionieren.

- **Kleinere Unternehmen werden eher auf den allumfassenden Sicherheits-Stack setzen.** Forrester geht davon aus, dass kleinere Unternehmen ZTE-Anbieter wie Netskope ausprobieren werden, die einen allumfassenden Stack bieten. In der Regel haben sie geringere Anforderungen und finden es eventuell einfacher, Lösungen aus einer Hand zu beziehen. In der Vergangenheit hat sich gezeigt, dass es bei größeren Technologiekonzernen länger dauert, diese Art von Lösungen einzuführen. Dies war beispielsweise auf dem Wi-Fi-Markt mit Cloud-basierten Lösungen von Aerohive Networks, jetzt Teil von Extreme Networks, und Meraki, jetzt Teil von Cisco, der Fall.

Agent-Overlay oder Gateway ohne Agents: Entscheidend ist die Komplexität

Die Vernetzung aller Benutzer und Anwendungen ist der angestrebte Endzustand des Zero Trust Edge, egal ob sich die Systeme vor Ort, in der Cloud, in einer Private Cloud oder im Remote-Einsatz befinden. Ein komplexes, heterogenes Netzwerk zu vernetzen, ist jedoch einfacher gesagt als getan. Entsprechend werden derzeit zwei Arten von Implementierungen angeboten – eine zur Unterstützung des strategischen Endzustands und eine zur Unterstützung eines taktischen Einstiegs in das Zero Trust Edge-Modell. Einige Anbieter, darunter Zscaler, können beide Modelle gleichzeitig unterstützen, und immer mehr Anbieter ziehen nach.

- **Modell 1: Ein Gateway fungiert als zentraler Sicherheitspunkt.** Dieses Modell wird zu Ihrem einzigen Einstiegspunkt ins Internet. Stellen Sie sich einen SD-WAN-Controller mit einem GRE-Tunnel zu einem vom Anbieter gehosteten Edge-Netzwerk vor. Der gesamte ausgehende Datenverkehr wird anschließend zum Edge-Netzwerk geleitet, das dann dem Datenverkehr dieses Tenants im Netzwerk sofort Sicherheitsrichtlinien zuweisen kann. Die Angriffsfläche des Ausgangspunkts verringert sich drastisch, sodass Angriffe wie DDoS kein Problem mehr darstellen. Diese Option ist zwar die sauberere Lösung, wird aber eher in mittelständischen Unternehmen eingesetzt. Für komplizierte heterogene Umgebungen ist sie möglicherweise auf kurze Sicht nicht umsetzbar.
- **Modell 2: Ein Overlay verteilt die Sicherheit – in der Regel über Agents.** Bei diesem Modell stellen Endpunkte über ein Overlay eine Verbindung mit dem Edge-Netzwerk her. In der Regel wird dies durch einen Endpunkt-Agent ermöglicht, der bestimmt, welche Verbindungen zum ZTE-Netzwerk umgeleitet werden. Das Overlay-Modell kann implementiert werden, ohne das zugrunde liegende Netzwerk zu ändern. Ein erheblicher Nachteil ist jedoch, dass die Installation von Agents aufgrund von Richtlinien in sensiblen Umgebungen wie dem Gesundheitswesen, der Fertigung und der IT/OT gegebenenfalls nicht möglich ist. Axis Security bietet einen innovativen Ansatz, der sich das Overlay-Modell zunutze macht, ohne dass dafür auf den Geräten, die dem Netzwerk beitreten möchten, Agents erforderlich sind. Wir haben einen wichtigen Kunden befragt, der sich aus genau diesem Grund für die Lösung von Axis Security entschieden hat.

Hürden auf dem Weg zum Zero Trust Edge-Modell

Das Zero Trust Edge-Modell verändert oder, besser gesagt, transformiert die Art und Weise, wie Sicherheit und Netzwerke bislang genutzt wurden. Cybersicherheitsfunktionen, die sich ohnehin fortlaufend weiterentwickeln, haben den Sprung zum Zero Trust Edge schneller geschafft. Bei älteren Netzwerken wird die Umstellung deutlich länger dauern. Aufgrund des mit Remote-Mitarbeitern verbundenen Sicherheitsproblems stellen Unternehmen zunehmend auf Zero Trust Edge um. Um jedoch das volle Potenzial dieses Modells nutzen zu können, müssen noch einige Herausforderungen gemeistert werden, darunter:

- **Ältere Anwendungen und Dienste.** Moderne Web-Anwendungen nutzen das Konzept des Identitätsverbunds und sind dadurch (relativ) leicht in einem ZTE zu konfigurieren. Bei Anwendungen, die auf nicht webbasierten Protokollen beruhen, insbesondere RDP/VDI und SIP/VoIP, gestaltet sich das dagegen schon schwieriger. Selbst bei diesen beiden sehr gängigen Arten von Anwendungen gibt es mangels einer standardisierten Methode für ihre Verwendung in der ZTE-Umgebung Probleme.
- **Ältere Netzwerkgeräte.** Sobald die Laptops, Server und Anwendungen mit dem Zero Trust Edge verbunden sind, muss der Architekt Tausende – und in einigen Fällen Hunderttausende – OT- und IoT-Geräte berücksichtigen, auf denen keine Agent-Software installiert werden kann. Diese müssen alle gesammelt mit dem ZTE verbunden werden und dabei gültige Netzwerkprotokolle verwenden. Und genau das ist der Punkt, an dem Sicherheits- und Netzwerkteams zusammenarbeiten müssen.
- **Kapazität und Vertrauen.** Unternehmen können ZTE nutzen, um Probleme wie den sicheren Zugriff für Remote-Worker taktisch zu lösen. Sie sind jedoch noch nicht bereit, Netzwerk- und Sicherheitsdienste von hoher Kapazität zu ersetzen, die die vorderste Front ihrer bestehenden Rechenzentren bilden. Unternehmen mit umfangreichen bestehenden Investitionen in ihre eigenen Rechenzentren warten ein größeres Unterfangen ab – wie etwa die Cloud-Migration ihrer kritischen Anwendungen –, bevor sie diese Services auf Zero Trust Edge umstellen.

Fazit

Sicherheit und Netzwerke endlich vereint im Kampf gegen einen gemeinsamen Feind

Da die Sicherheit in das Netzwerk integriert und damit zu einem Teil seiner DNA wird, sieht Forrester folgende Entwicklung der beiden Organisationen (Sicherheit und Netzwerke) voraus:

1. **Sicherheitsorganisationen legen die Sicherheitsrichtlinien fest und testen sie.** Die Arten des Datenverkehrs und die Dienste, die benötigt werden, um akzeptable Vertrauensstufen zu erreichen, werden vom Sicherheitsteam festgelegt. Mit Überwachungs- und Analysetools stellen die Teams sicher, dass Richtlinien eingehalten werden, und testen und auditieren regelmäßig den Datenverkehr und die Verbindungen – gemeinsam.
2. **Netzwerke nach Sicherheit.** Netzwerkexperten richten das Netzwerk unter Berücksichtigung der vom Sicherheitsteam festgelegten ZTE-Richtlinien ein. Diese Herangehensweise treibt das Zero Trust-Konzept deutlich voran, ist aber gewissermaßen eine Umkehr der letzten 25 Jahre, in denen die Sicherheit auf die Netzwerke aufgesetzt wurde.

3. **Zu guter Letzt: ein sichereres Interneterlebnis.** Wenn man die Entwickler des ursprünglichen Internets auf das Thema Sicherheit anspricht, werden sie offen zugeben, dass sie nie Teil des Designs war. In den 30 Jahren seit seiner Erfindung hat sich das weltweite Internet zu einem gefährlichen Ort entwickelt. Mit Zero Trust Edge gibt es nun endlich einen sichereren Weg durch das Internet.

Zusätzliches Material

Unternehmen, die für diesen Bericht befragt wurden

Wir möchten uns bei den Mitarbeitern der folgenden Unternehmen bedanken, die sich während der Studie großzügig Zeit für diesen Bericht genommen haben.

419 Consulting
Akamai
AT&T
Axis Security
Barracuda
BlackBerry

Cato Networks
Cisco Systems
Citrix
Deutsche Telekom
Edelweiss Financial Services
Famous Supply
Fortinet
Infoblox
IronNet
Jefferies
Juniper
Lightstream
Marriott Vacations Worldwide
Menlo Security
Mentor Graphics
Netskope
Nuspire
Palo Alto Networks
Silver Peak
SKF
VMware
Windstream
Zentera Systems
Zscaler

Fußnoten

[1] Ein privates Rechenzentrum fungiert als Hub für Daten, Anwendungen und Sicherheit mit Remote-Standorten. Restaurants, Akutversorgungszentren und Produktionsstätten, um nur einige zu nennen, verbinden sich mit dem Hub, um auf alle Unternehmensressourcen zuzugreifen.

[2] Siehe Forrester-Bericht „Emerging Technology Spotlight: Businesswide Networking Fabric“ (Neue Technologie im Blickpunkt: Unternehmensweite Netzwerkstruktur).

In einem vernetzten Geschäftsmodell schaffen die an verschiedenen Standorten verteilten Mitglieder des Ökosystems gemeinsam Mehrwert für die Kunden. Siehe Forrester-Bericht „Customer-Obsessed Businesses Need Digital Ecosystems“ (Stark kundenorientierte Unternehmen brauchen digitale Ökosysteme).

[3] In unseren sogenannten PandemicEX-Umfragen zu den Erfahrungswerten während der Pandemie wurden die Teilnehmer Folgendes gefragt: „In welchem Maß unternimmt Ihr Unternehmen/Ihre Organisation diese Schritte, um das mit dem Coronavirus verbundene Risiko zu managen?“ Quelle: Forrester’s Q1 2020 US PandemicEX Survey 1 (3. März bis 6. März 2020), Forrester’s Q1 2020 US PandemicEX Survey 2 (17. März bis 19. März 2020) und Forrester’s Q2 2020 US PandemicEX Survey 1 (1. April bis 3. April 2020).

Siehe Forrester-Bericht „The State Of Remote Work, 2020“ (Stand der Remote-Arbeit, 2020).

[4] In der Anfangsphase von ZT zeigten die Marketingmaterialien von Anbietern nur Lösungen für das private Rechenzentrum auf. Palo Alto beleuchtete beispielsweise in verschiedenen Whitepapers, wie ZT die Ressourcen von Rechenzentren schützen kann. Quelle: „Best Practices – Data Center Security“ (Best Practices: Datenschutz im Rechenzentrum), Palo Alto Networks, 1. Juni 2016 (https://www.paloaltonetworks.de/resources/whitepapers/best-practices-data-center-security).

[5] Quelle: Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, Jonathan Zolla, Urs Hölzle, Stephen Stuart und Amin Vahdat, „B4: Experience with a Globally-Deployed Software Defined WAN“ (B4: Erfahrung mit einem global bereitgestellten softwaredefinierten WAN), Sitzungsbericht der ACM SIGCOMM 2013 Conference, August 2013 (https://storage.googleapis.com/pub-tools-public-publication-data/pdf/41761.pdf).

FORRESTER®

Wir arbeiten mit führenden Technologieunternehmen zusammen, um kundenorientierte Strategien zu entwickeln, die das Wachstum fördern.

PRODUKTE UND LEISTUNGEN

- Zentrale Forschung und Tools
- Daten und Analysen
- Zusammenarbeit mit Kollegen
- Einbeziehung von Analysten
- Beratung
- Ereignisse

Die Forschungsergebnisse und Erkenntnisse von Forrester sind auf Ihre Rolle und wichtige Geschäftsinitiativen zugeschnitten.

RELEVANTE ROLLEN

Marketing- und Strategieexperten

CMO
B2B-Marketing
B2C-Marketing
Kundenerlebnis
Kundenerkenntnisse
E-Business und Channel-Strategie

Experten im Bereich Technologiemanagement

CIO
Anwendungsentwicklung und -bereitstellung
Unternehmensarchitektur
Infrastruktur und Betrieb
- Sicherheit und Risiken

Beschaffung und Anbietermanagement

Experten der Technologiebranche

Analyst Relations

KUNDENSERVICE

Informationen zu gedruckten Exemplaren oder elektronischen Nachdrucken erhalten Sie von der Kundenbetreuung unter +1 866-367-7378, +1 617-613-5730 oder clientsupport@forrester.com. Wir bieten Mengenrabatte und Sonderpreise für akademische und gemeinnützige Einrichtungen.