WHITE PAPER

aruba
a Hewlett Packard Enterprise company

EINE ERFOLGREICHE WAN- UND SICHERHEITSTRANSFORMATION STÄRKT DAS DIGITALE UNTERNEHMEN

INHALTSVERZEICHNIS

ZUSAMMENFASSUNG 3

SICHERHEIT CLOUDBASIERT BEREITSTELLEN – GENAU WIE ANWENDUNGEN 3

DAS FIRMEN-IOT MIT SD-WAN SCHÜTZEN 5

MIT BRANCHENFÜHRENDEN LÖSUNGEN FÜR GESCHÄFTLICHE AGILITÄT SORGEN 6

DIE WAN-TRANSFORMATION ALS ENTSCHEIDENDEN ERFOLGSFAKTOR FÜR DIE DIGITALE TRANSFORMATION EINBEZIEHEN 6

DIE ANFORDERUNGEN VON ANWENDUNGS-SLAS ERFÜLLEN 7

SCHLUSSFOLGERUNG 7

ZUSAMMENFASSUNG

Unternehmen arbeiten weiterhin an ihrer digitalen Transformation, um Effizienz und Kundenzufriedenheit zu verbessern, neue Marktchancen zu nutzen, die Rentabilität zu steigern und ihren Wettbewerbsvorteil zu sichern. Die Migration von Unternehmensanwendungen in die Cloud ist ein wesentlicher Erfolgsaspekt jeder Initiative zur digitalen Transformation. Warum? Mittlerweile werden mehr Anwendungen in der Cloud als in konventionellen Firmenrechenzentren ausgeführt. Die meisten dieser Anwendungen werden als Software-as-a-Service (SaaS) genutzt. Darüber hinaus müssen Unternehmen in der cloudzentrierten Welt von heute sicherstellen, dass der Anwendungszugriff jederzeit sowie standort- und geräteunabhängig auf direktem, sicherem Weg möglich ist. Daneben soll sichergestellt sein, dass das Netzwerk sowohl für die Mitarbeiter als auch für die Kunden eine konstant hohe Qualität bietet. Schließlich vergrößert die explosionsartige Verbreitung von Mobil- und IoT-Geräten in Unternehmen die Angriffsfläche erheblich, sodass Unternehmen potenziellen Sicherheitsverstößen ausgesetzt sind, die Daten gefährden und zu Netzwerkausfällen führen.

Die bestehenden Firmennetzwerke wurden nicht für die cloudzentrierte Welt von heute konzipiert und sind nicht so agil und sicher, wie es die digitale Transformation verlangt. Unternehmen müssen nicht nur Anwendungen in der Cloud, sondern auch die Nutzer schützen, die über Wide Area Network (WAN) auf diese Anwendungen zugreifen. Zugleich verlangt das wettbewerbsorientierte Geschäftsumfeld von heute, dass Unternehmen ihren Kunden Nutzerfreundlichkeit der Spitzenklasse über ein Netzwerk mit der nötigen Leistung und Verfügbarkeit bieten, um einen optimalen Geschäftsbetrieb zu gewährleisten.

Um das Potenzial der digitalen Transformation voll auszuschöpfen, müssen Unternehmen die WAN- und die Sicherheitsarchitektur gleichermaßen umgestalten – und nicht nur eine von beiden. Unternehmen haben bereits viel in den Wechsel zur Cloud investiert. Jetzt besteht die Herausforderung darin, mit den Cloudinvestitionen einen Multiplikatoreffekt zu erreichen. Der Schlüssel dazu ist die Modernisierung der WAN- und der Sicherheitsarchitektur im Unternehmen. Strategisch ist es daher geboten, ein intelligentes, umfassend automatisiertes, softwaredefiniertes Wide Area Network (SD-WAN) einzuführen, das sich nahtlos in cloudbasierte Sicherheitsdienste integrieren lässt.

Die WAN- und Sicherheitstransformation ist ein Prozess, sodass Unternehmen bei der Modernisierung des WAN oder aber der Sicherheit ansetzen können. Um das Potenzial der Cloudinvestitionen maximal auszuschöpfen, müssen jedoch beide Bereiche modernisiert werden. Ebenso wichtig ist es, sich nicht an einen einzigen Anbieter zu binden und dementsprechend einen Partner für die technologische Lösung zu suchen, der flexibel die freie Wahl lässt. Mit der transformierten Netzwerk- und Sicherheitsarchitektur können Unternehmen dann rasch neue Innovationen einführen und so bei kontrollierten Kosten Produktivität, Umsatzwachstum und Rentabilität steigern.

Um das Potenzial der Cloud und der digitalen Transformation voll auszuschöpfen, müssen Unternehmen die WAN- und die Sicherheitsarchitektur gleichermaßen transformieren – und nicht nur eine von beiden. Unternehmen haben bereits viel in den Wechsel zur Cloud investiert. Jetzt besteht die Herausforderung darin, mit den Cloudinvestitionen einen Multiplikatoreffekt zu erreichen.

SICHERHEIT CLOUDBASIERT BEREITSTELLEN – GENAU WIE ANWENDUNGEN

Herkömmlicherweise wird der gesamte Anwendungsdatenverkehr von externen Standorten zur Sicherheitsinspektion und Überprüfung per Backhaul über private MPLS-Dienste ins Firmenrechenzentrum geleitet (siehe Abbildung 1). Diese Architektur war solange sinnvoll, wie Anwendungen ausschließlich im Firmenrechenzentrum gehostet wurden. Mit der Migration von Anwendungen und Diensten in die Cloud ist diese bisherige Netzwerkarchitektur jedoch nicht mehr geeignet. Sie beeinträchtigt die Anwendungsleistung und ist bei der Nutzerfreundlichkeit unzuverlässig, da der für das Internet bestimmte Datenverkehr über das Rechenzentrum und die Firmen-Firewall geleitet wird, bevor er sein Ziel erreicht.

Auch die konventionelle perimeterbasierte Sicherheit ist angesichts einer steigenden Anzahl an Mitarbeitern, die außerhalb des Firmennetzwerks arbeiten und direkt auf Cloudanwendungen zugreifen, nicht mehr ausreichend. Cloud und SaaS haben Anwendungszugriff und -nutzung ein für alle Mal verändert. Mit der Transformation der WAN- und der Sicherheitsarchitektur stellen Unternehmen den standort- und geräteunabhängigen, sicheren Direktzugriff auf Anwendungen und Dienste für beliebige Multi-Cloud-Umgebungen sicher.

Cloudbasierte Sicherheitslösungen unterstützen ein Spektrum von Netzwerksicherheitsfunktionen, unter anderem Secure Web Gateway (SWG), Firewall-as-a-Service (FWaaS), Cloud Access Security Broker (CASB) und Zero-Trust-Netzwerkarchitekturen (ZTNA). Bisher handelte es sich dabei um dedizierte lokale Einzelfunktionen. Inzwischen lassen sie sich wie in Abbildung 2 gezeigt einheitlich über die Cloud bereitstellen.

Manche Early Adopters cloudbasierter Sicherheitslösungen versäumten es, ein SD-WAN mit adaptivem Internet-Breakout direkt von externen Standorten einzurichten. Entsprechend konnten sie den Datenverkehr von externen Standorten nicht direkt in die Cloud lenken. Ohne die SD-WAN-Komponente lief Datenverkehr für die Cloud weiter per Backhaul über das Rechenzentrum – mit den entsprechenden negativen Folgen für die Anwendungsleistung.

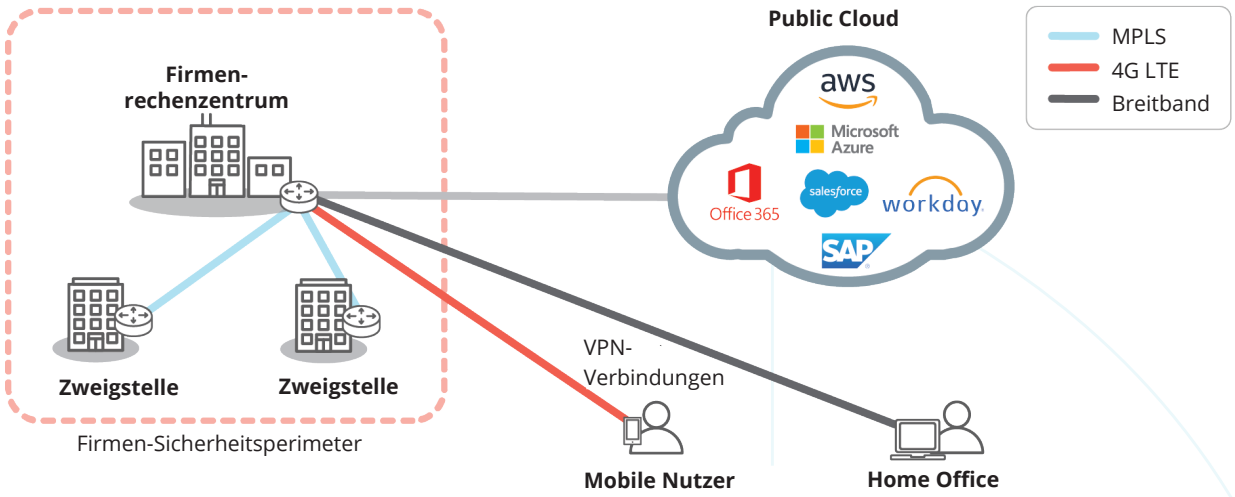

Abbildung 1: Konventionelle WANs und perimeterbasierte Sicherheitslösungen in Unternehmen waren nicht für die Cloud gedacht. Erfolgt für sämtlichen Anwendungsdatenverkehr von externen Standorten ein Backhaul an das Rechenzentrum, leiden Leistung und Nutzerfreundlichkeit.

Die Einführung einer cloudbasierten Sicherheitslösung in Kombination mit SD-WAN vermeidet die Kosten und Komplexitäten, die bei der Verwaltung mehrerer lokaler Firewalls der nächsten Generation entstehen. Das setzt zur Abwehr von Bedrohungen jedoch nach wie vor eine zustandsbehaftete zonenbasierte Firewall für externe Standorte voraus. Wie in Abbildung 3 gezeigt, können Unternehmen mit einer modernen SD-WAN-Lösung per adaptivem Internet-Breakout über Breitbandinternet eine direkte Cloudverbindung herstellen. Die Intelligence zur Erkennung zulässiger Anwendungen erlaubt das lokale Breakout vom externen Standort zum nächsten Point of Presence (PoP). So entfallen Latenzen, während bei SaaS- und Cloudanwendungen wie Microsoft Office 365, 8x8 und RingCentral für höchste Nutzerfreundlichkeit gesorgt ist. Mit der Erkennung von Anwendungen wird es auch möglich, sonstigen Internetdatenverkehr vor der Weiterleitung an einen SaaS-Anbieter zur gründlichen Inspektion zunächst an einen cloudbasierten Sicherheitsanbieter zu senden. In moderne cloudbasierte Sicherheitsdienste integrierte fortschrittliche SD-WAN-Funktionen sorgen für die einheitliche Richtliniendurchsetzung und Zugriffskontrolle für Nutzer, Geräte, Anwendungen und IoT. So können Unternehmen die Compliance gewährleisten, Ausfallzeiten verhindern und das Risiko der Datengefährdung durch Sicherheitsverstöße senken.

DAS FIRMEN-IOT MIT SD-WAN SCHÜTZEN

Die Ausbreitung von IoT-Geräten eröffnet neue Möglichkeiten für Überwachung, Reporting, Meldungen, Automatisierung und Optimierung betrieblicher Prozesse – von Fertigungslinien bis zu Energieeinsparungen durch HLK- und Beleuchtungsautomatisierung. Mit IoT werden Unternehmen durch Automatisierung effizienter – und durch den neuen Komplexitätsgrad zugleich leichter angreifbar. Die IT löst das Sicherheitsproblem, das die wachsende Zahl

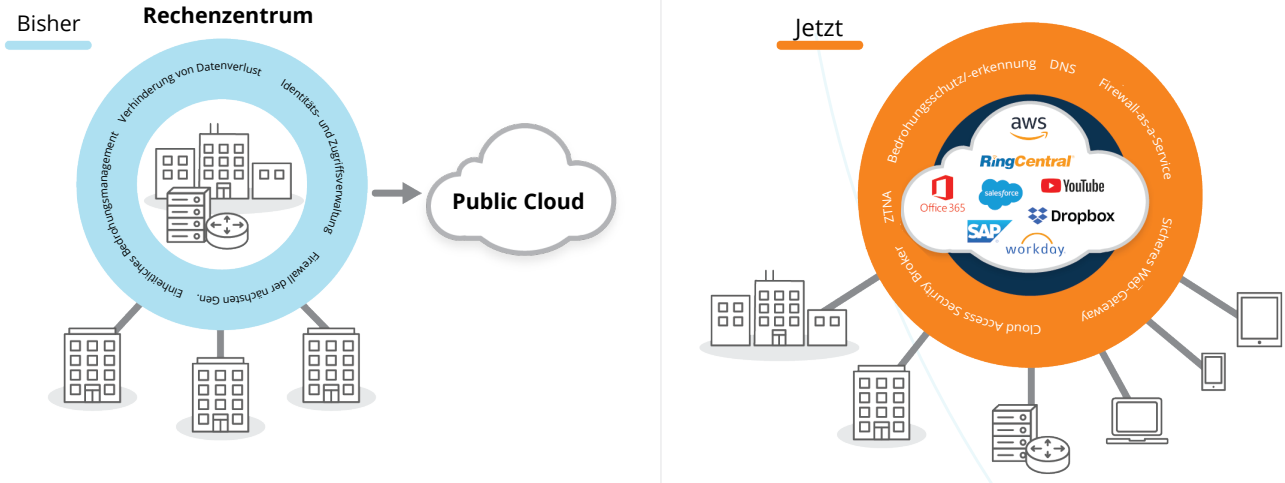

Abbildung 2: Bisher war der Schutz des Rechenzentrums oberste Priorität, in dem Anwendungen ausschließlich gehostet wurden. Seit Anwendungen in die Cloud wechseln und von dort bereitgestellt werden, wird die perimeterbasierte Sicherheit immer ineffektiver. Es ist an der Zeit, umzudenken und die Sicherheit auf die Cloud umzustellen.

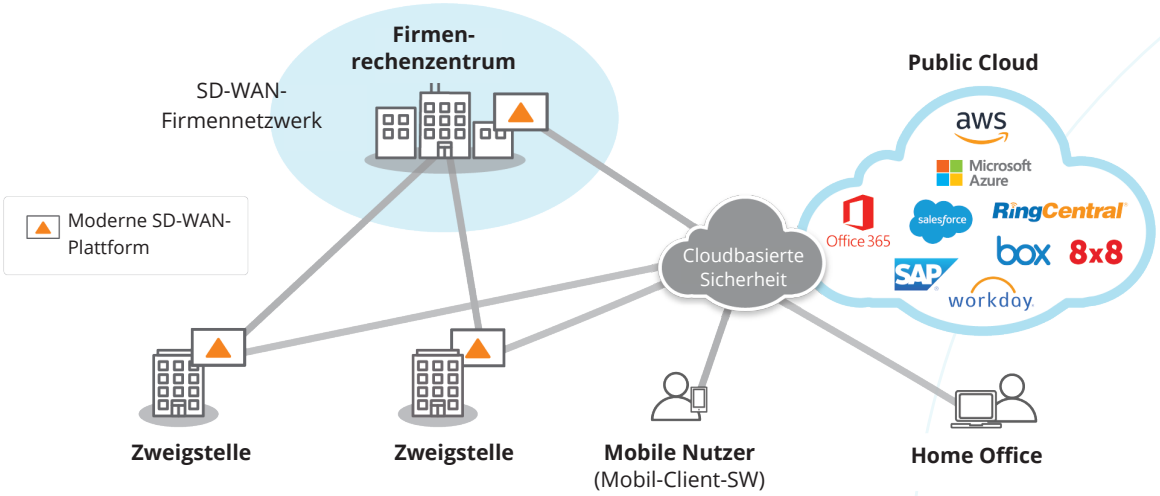

Abbildung 3: Mit einem modernen SD-WAN wechseln Unternehmen sicher in die Cloud. Nutzer an externen Standorten können über Breitbandverbindung mit adaptivem Internet-Breakout direkt auf Cloudanwendungen zugreifen. Zugleich werden Anwendungsleistung und Nutzerfreundlichkeit optimiert. Die Kombination aus modernem SD-WAN und Cloudsicherheit mit richtlinienbasiertem Zero Trust Network Approach (ZTNA) stellt sicher, dass WAN, Benutzer, Geräte und Anwendungen des Unternehmens stets geschützt sind.

an Mobilgeräten mit sich bringt, durch die Bereitstellung von Lösungen für Zero Trust Network Access (ZTNA) auf Basis des Zero-Trust-Modells. Bei einer solchen ZTNA-Lösung wird auf Nutzergeräten wie Laptops, Tablets oder Smartphones ein Endgerätagent installiert. Dieser Softwareagent gewährleistet, dass Datenverkehr vom Gerät vor Erreichen einer SaaS-Anwendung oder eines IaaS-Anbieters an einen cloudbasierten Sicherheitsdienst geleitet wird. Anders als bei Tablets und Smartphones lassen sich ZTNA-Softwareagenten jedoch nicht auf IoT-Geräten installieren, denn diese sind agentenlos und unterstützen die Installation von Softwareagenten von Drittanbietern nicht. Daher benötigen Unternehmen für IoT-Geräte eine andere Sicherheitslösung, um potenzielle Schwachstellen im Firmennetzwerk zu sichern, über die unbefugt ins Netzwerk eingedrungen und der tägliche Betrieb gestört werden kann.

Mit einer modernen, anwendungsbezogenen SD-WAN-Plattform senken Unternehmen das Risiko von Sicherheitsverstößen durch die Bereitstellung von IoT-Geräten. Eine moderne SD-WAN-Plattform identifiziert und klassifiziert den Anwendungsdatenverkehr des ersten Pakets, fängt ihn am Netzwerk-Edge ab, weist ihn dem entsprechenden Segment zu und isoliert ihn vom übrigen Datenverkehr im Netzwerk. Eine moderne SD-WAN-Plattform orchestriert die durchgängige Segmentierung von Firmen-LAN-WAN-LAN bis zu LAN-WAN-Rechenzentrum/Cloud. So ist bei höherer Transparenz für die einheitliche, automatisierte Durchsetzung der Sicherheitsrichtlinien gesorgt. Mit durchgängiger Segmentierung können Unternehmen isolierte Segmente für den Datenverkehr von IoT-Geräten einrichten. Es besteht die Möglichkeit, für jedes Segment eine eigene Sicherheitsrichtlinie zu definieren, die auf den Gerätedatenverkehr angewendet wird. Da der Datenverkehr in den einzelnen Segmenten vom Datenverkehr aller anderen Segmente isoliert ist, wird unbefugter Zugriff verhindert. Sollte eine Bedrohung auftreten, sind ihre Folgen auf das betroffene Segment begrenzt. Mit einer einheitlichen zustandsbehafteten zonenbasierten Firewall schützen Unternehmen zudem per Blockierung externe Standorte und IoT-Geräte vor allen potenziellen Bedrohungen.

Ein Beispiel illustriert das: An einem externen Standort mit installierten agentenlosen IoT-Geräten wie z. B. PoS und HLK-Anlagen (Abbildung 4 unten) erkennt eine moderne SD-WAN-Plattform die jeweilige Anwendung, die von einem bestimmten Gerät exklusiv genutzt wird. Eine Systemrichtlinie fängt PoS-Datenverkehr ab und leitet ihn an das Firmenrechenzentrum weiter, das die Verarbeitung von Kreditkartentransaktionen hostet. In diesem Beispiel kommen im Rechenzentrum bereitgestellte Firewall-Sicherheitsdienste der nächsten Generation zur Anwendung. Demgegenüber segmentieren HLK-Systemrichtlinien den HLK-Datenverkehr und senden diesen vor der Weiterleitung an die in der Public Cloud gehostete IoT-Kontrollzentrale zur zusätzlichen Sicherheitsinspektion an einen cloudbasierten Sicherheitsdienst. Da der IoT-Datenverkehr entsprechend der Unternehmensrichtlinie isoliert wird, stellt ein Verstoß im HLK-Segment keine Gefahr für die Kreditkarteninformationen oder personenbezogenen Daten im PoS-Segment dar. Mit einer Segmentierung können Unternehmen für sie geltende PCI- (und sonstige) Compliance-Anforderungen einfacher erfüllen. Eine umfassende Sicherheitsbereitstellung mit einer modernen SD-WAN-Plattform kann dynamische Unternehmen von heute, die die Vorteile des IoT maximal nutzen möchten, in ihrem Transformationsprozess besser schützen.

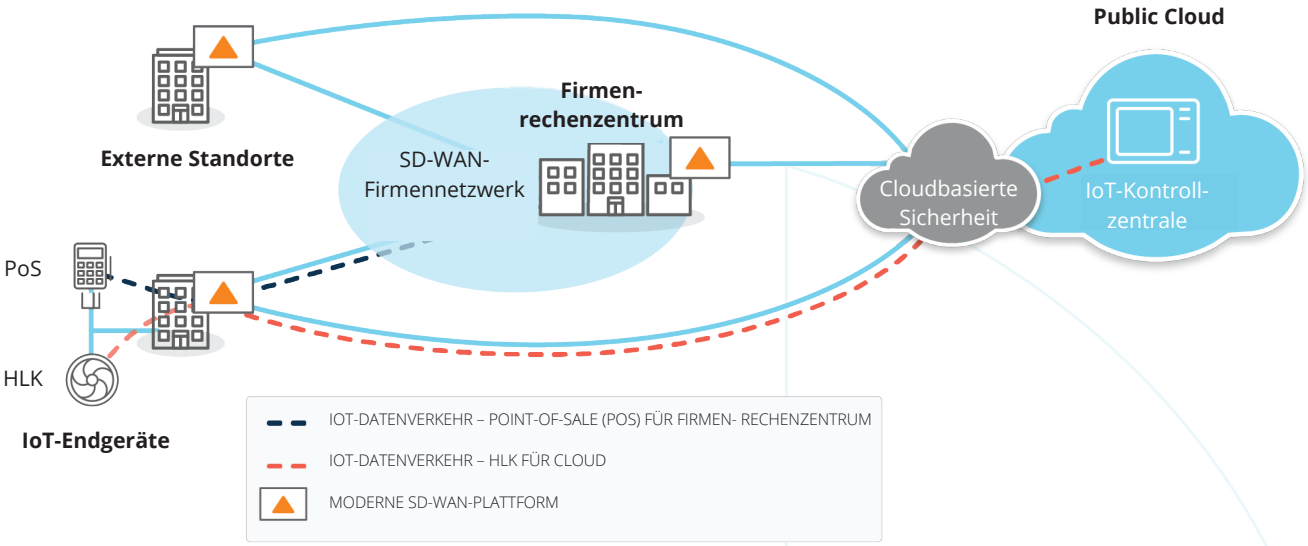

Abbildung 4: Die Zahl der IoT-Endgeräte steigt fortlaufend und vermehrt die Gefahr von Sicherheitsverstößen. Mit einer modernen SD-WAN-Plattform schützen Unternehmen IoT-Geräte hinter der einheitlichen zustandsbehafteten zonenbasierten Firewall. Der Datenverkehr von IoT-Geräten wird dabei dynamisch erkannt, um das Netzwerk unter Anwendung passgenauer Richtlinien differenziert zu segmentieren und so die Compliance-Anforderungen zu erfüllen. Mit einem modernen SD-WAN wird IoT-Datenverkehr am Netzwerk-Edge abgefangen und ohne Kompromisse oder geschäftliches Risiko an das richtige Ziel gesendet, das sich auch in der Cloud befinden kann. Wie in der Abbildung gezeigt, werden sämtliche PoS-Transaktionsdaten vom externen Standort an das Firmenrechenzentrum gesendet. Der HLK-Datenverkehr dagegen geht an eine IoT-Kontrollzentrale in der Cloud.

MIT BRANCHENFÜHRENDEN LÖSUNGEN FÜR GESCHÄFTLICHE AGILITÄT SORGEN

Mit den beständig weiterentwickelten Ansätzen für die Bereitstellung von Netzwerksicherheit und den Herausforderungen, die die Einrichtung komplexer Netzwerklösungen mit sich bringt, gilt es, unbedingt branchenführende Sicherheits- und Netzwerklösungen von Anbietern mit nachweislicher Erfahrung und ausgewiesenem fachlichen Schwerpunkt zu evaluieren. Wahrscheinlich findet sich kein Anbieter, der branchenführende Funktionen für beide Bereiche aus einer Hand bereitstellen kann, und Unternehmen sollten sich nicht mit Basisfunktionen für einen der Bereiche zufriedengeben.

Da Sicherheit angesichts der immer ausgeklügelteren Bedrohungen ein Hauptanliegen ist, müssen Unternehmen flexibel, schnell und kosteneffektiv neue Sicherheitslösungen einführen können, ohne an die Lösung eines einzigen Anbieters gebunden zu sein. Mit einer unabhängigen Netzwerklösung können Unternehmen souverän und ohne Bedenken die Cloudsicherheitslösungen auswählen und bereitstellen, die am besten zu ihren dynamischen Geschäfts- und Sicherheitsanforderungen passen.

Wenn Unternehmen flexibel branchenführende Lösungen wählen können, die SD-WAN und cloudbasierte Sicherheit durch Automatisierung zusammenführen, steigern sie ihre geschäftliche Agilität und Geschwindigkeit. Zugleich bauen sie mit einer einheitlichen Sicherheitsarchitektur, die Cyberangriffe und ihre Folgen abwehrt, Komplexität und Kosten ab. So erzielen Unternehmen unterm Strich einen Multiplikatoreffekt für bereits getätigte und laufende Investitionen in Cloudanwendungen und -dienste.

DIE WAN-TRANSFORMATION ALS ENTSCHEIDENDEN ERFOLGSFAKTOR FÜR DIE DIGITALE TRANSFORMATION EINBEZIEHEN

Neben den vielen Vorteilen der Migration auf eine moderne cloudbasierte Sicherheitsarchitektur bietet auch die WAN-Transformation cloudzentrierten Unternehmen von heute einen enormen Nutzen. Konventionelle routerbasierte WANs waren nie für die Cloud gedacht. Um Cloudanwendungen leistungsfähiger und sicherer zu machen, müssen Unternehmen ihre WAN-Architektur modernisieren und die optimale Netzwerkarchitektur für externe Standorte neu konzipieren. Unternehmen wechseln verstärkt zu SaaS und in die Cloud, insbesondere, um Nutzerfreundlichkeit der Spitzenklasse zu bieten.

Die WAN-Transformation sorgt für einen effizienteren Austausch zwischen Cloud und Nutzern und verbessert die Nutzerfreundlichkeit. Wie bereits erläutert, optimiert adaptives Internet-Breakout zu in der Cloud gehosteten und SaaS-Anwendungen direkt von externen Standorten nicht nur die verfügbare Bandbreite – auch die Latenz, die die Nutzerproduktivität beeinträchtigen kann, wird reduziert.

Viele Organisationen transformieren ihren Netzwerk-Edge und führen SD-WAN ein, um externe Standorte über Breitbandinternetverbindungen zu vernetzen. SD-WAN sorgt ausgehend von zentral definierten Richtlinien für die intelligente anwendungsbasierte Pfadauswahl für eine Reihe von WAN-Links (MPLS, Breitbandinternet, LTE usw.). SD-WAN bietet unter anderem folgende Vorteile:

- kosteneffektive Bereitstellung von Unternehmensanwendungen
- verbesserte Anwendungsleistung, Verfügbarkeit und Nutzerfreundlichkeit
- Erfüllung der Anforderungen moderner externer Standorte
- Einbindung von SaaS- und cloudbasierten Anwendungen und Diensten
- verbesserte IT-Effizienz für externe Standorte durch automatische Dienstbereitstellung

DIE ANFORDERUNGEN VON ANWENDUNGS-SLAS ERFÜLLEN

Diese Strategie führt zu einer direkten Steigerung der Produktivität und Agilität des Unternehmens. Unternehmen benötigen ein Hochleistungsnetzwerk auf einer hochverfügbaren Basis, die geschäftskritische Anwendungen zuverlässig unterstützt. Sicherheit darf niemals nachträglich ergänzt werden. Mit der Möglichkeit zur Unterstützung von Mikrosegmentierungsfunktionen und einer differenzierten Durchsetzung von Richtlinien sind Unternehmen in der Lage, das WAN zu sichern, Compliance-Anforderungen zu erfüllen und Bedrohungen abzuwehren.

Unternehmen müssen neue externe Standorte schnell einrichten und Richtlinien und Sicherheitsregeln dynamisch anpassen können. Die Möglichkeit zur Weitergabe von Richtlinienkontexten ist bei der Automatisierung externer Standorte entscheidend. Damit ist das Konzept einer modernen SD-WAN-Lösung äußerst attraktiv. Statt mehrere Appliances für dedizierte Sicherheitsfunktionen einsetzen zu müssen, vereinfacht und vereinheitlicht bzw. „verschlankt“ dieser Ansatz die WAN-Edge-Architektur für externe Standorte. Mit einer modernen SD-WAN-Edge-Plattform transformieren Unternehmen ihr WAN, indem sie SD-WAN, Routing, WAN-Optimierung, Segmentierung und Sicherheit für externe Standorte in nur einer zentral verwalteten Plattform zusammenführen.

Mit zentralisierter SD-WAN-Orchestrierung und einem anwendungsspezifischen Ansatz ist sichergestellt, dass das Netzwerkverhalten stets den betrieblichen Prioritäten entspricht. Die zentrale Orchestrierung von Netzwerk- und Sicherheitsrichtlinien gewährleistet, dass QoS und Sicherheit für Anwendungen oder Anwendungsklassen einheitlich umgesetzt werden – unabhängig davon, wo oder wie der Zugriff erfolgt. Die Performance und Sicherheit von Anwendungen kann mithilfe von Top-Down-Geschäftsrichtlinien gewährleistet werden, statt durch die Beschränkungen von Bottom-Up-Technologien.

Ein modernes SD-WAN überwacht fortlaufend den Status von Netzwerk und Anwendungen, erkennt veränderte Bedingungen und löst in Echtzeit automatisierte Sofortreaktionen aus, um den Folgen von Brownouts, Blackouts und Sicherheitsvorfällen vorzubeugen. Die Automatisierung der Cloudplattform-Konnektivität durch Integrationen über Anwendungsprogrammierschnittstellen (APIs) vereinfacht zudem den IT-Betrieb, sodass Unternehmen schnell auf cloudbasierte Sicherheitsdienste, IaaS und SaaS zugreifen können.

Moderne Netzwerke setzen lückenlose Transparenz, Programmierbarkeit und Automatisierung voraus, denn nur so lassen sich dynamisch Leistung, Sicherheit und Nutzerfreundlichkeit der Spitzenklasse gewährleisten, die Multi-Cloud-Umgebungen verlangen. Ein intelligentes, mit branchenführendem SD-WAN und cloudbasierten Sicherheitslösungen konzipiertes WAN bringt Initiativen der digitalen Transformation voran und erlaubt es Unternehmen, Innovationen zügig einzuführen und weiterzuentwickeln, ohne Produktivität und Wachstum einzuschränken. Zugleich wird die Gefährdung durch Sicherheitsrisiken minimiert.

SCHLUSSFOLGERUNG

Moderne cloudzentrierte Unternehmen migrieren weiterhin Anwendungen vom Rechenzentrum in die Cloud. Dazu müssen sie WAN und Sicherheit transformieren, denn nur so rentieren sich ihre Cloudinvestitionen wirklich. Gartner hat den Begriff „SASE“ oder „Secure Access Service Edge“ geprägt, der für diese neue Ausrichtung der Branche steht. Wie in Abbildung 5 zu sehen, müssen Unternehmen bei der Konzeption eines Secure Access Service Edge unbedingt sowohl WAN als auch Sicherheit transformieren, um für nahtlose Nutzerfreundlichkeit zu sorgen.

Kein Anbieter ist in der Lage, eine zentrale Plattform bereitzustellen, die branchenführende Technologien sowohl für das Netzwerk als auch für die Sicherheit vereint. Angesichts der immer ausgeklügelteren Bedrohungen müssen Unternehmen flexibel bleiben, um schnell und kosteneffektiv neue Sicherheitslösungen einführen zu können. Unternehmen sollten Plattformen in Erwägung ziehen, bei denen sie branchenführende Netzwerk- und Sicherheitslösungen frei wählbar integrieren können. So vermeiden sie, dass sie an proprietäre Lösungen eines einzigen Anbieters gebunden sind oder sich mit Basisfunktionen zufriedengeben müssen.

Eine moderne SD-WAN-Plattform, die integrierte Anwendungsprogrammierschnittstellen (APIs) unterstützt, eröffnet Unternehmen neue Möglichkeiten zur Automatisierung und damit zur Einbindung verschiedener branchenführender Clouddienste – Sicherheit eingeschlossen. Sie unterstützt grundlegende, unverzichtbare Sicherheitsfunktionen für externe Standorte und ergänzt die Cloudsicherheit, sodass sich Sicherheitsrichtlinien unternehmensweit nahtlos und lückenlos durchsetzen lassen. So können Unternehmen, die noch nicht für die vollständige Transformation von WAN- und Sicherheitsarchitektur bereit sind, in ihrem eigenen Tempo auf eine moderne cloudzentrierte WAN-Architektur umstellen, ohne Kompromisse eingehen zu müssen.

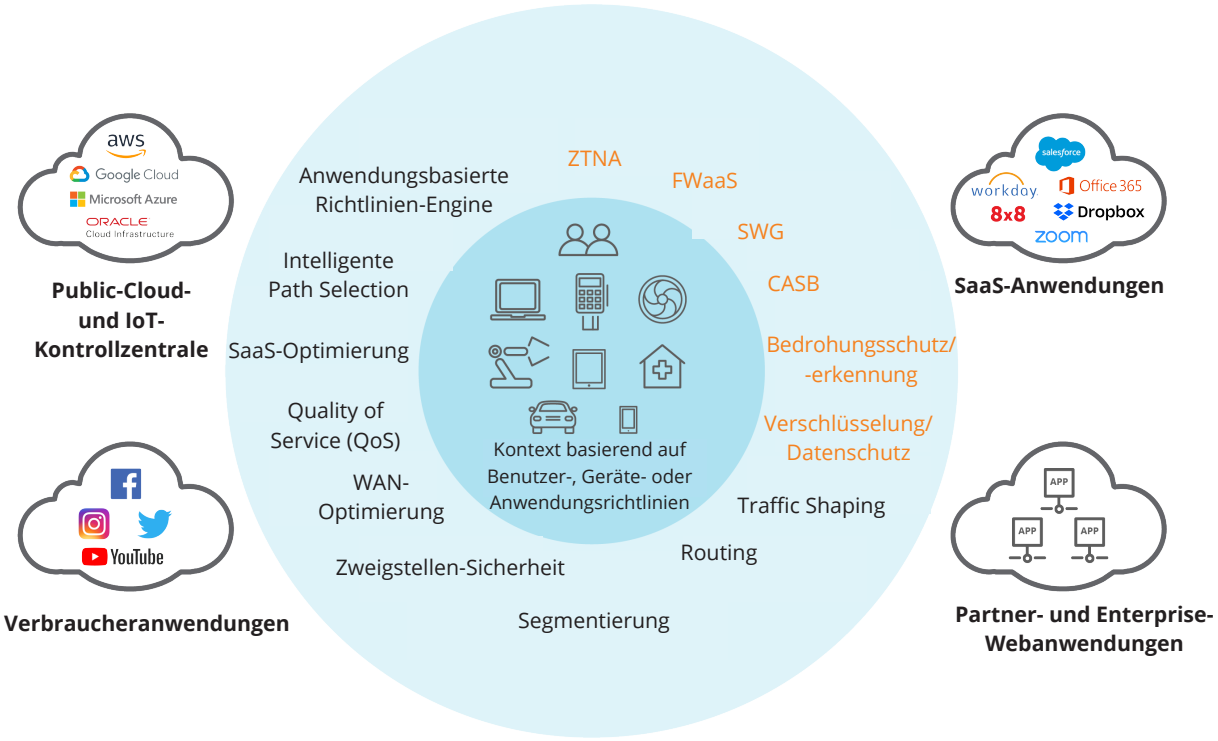

Abbildung 5: Ein sicherer Zugriffsservice wird benötigt, um die digitalen Transformationsinitiativen des Unternehmens zu unterstützen, d.h. die Cloud-first-Strategie und die Mobilitätsanforderungen der Mitarbeiter. In einer robusten SASE-Architektur müssen umfassende WAN-Funktionen mit umfassenden Netzwerksicherheitsfunktionen zusammenarbeiten, um die dynamischen Anforderungen digitaler Unternehmen an einen sicheren Zugriff für Benutzer, Geräte und Anwendungen zu unterstützen.

Unternehmen, die Firewalls für externe Standorte noch nicht außer Betrieb setzen und vollständig auf ein cloudbasiertes Sicherheitsmodell umstellen möchten, sollten unbedingt darauf achten, dass ihre neue SD-WAN-Plattform jede führende Drittanbieter-Softwarelösung für das Unified Threat Management (UTM) uneingeschränkt unterstützt, die als integrierte Lösung für externe Standorte ausgeführt wird. Damit entfallen die zusätzlichen Kosten und Verwaltungskomplexitäten, die dedizierte getrennte Firewalls üblicherweise mit sich bringen. Darüber hinaus können Unternehmen auf diesem Weg flexibel branchenführende Lösungen bereitstellen, die unter dem Strich die nahtlose Migration auf ein cloudbasiertes Sicherheitsmodell erlauben.

Unternehmen investieren weiterhin umfassend in die Cloud mit der Überlegung, dass die Anforderungen für die WAN- und die Sicherheitstransformation es ihnen schließlich ermöglichen, eine Nutzerfreundlichkeit der Spitzenklasse zu bieten, die Produktivität zu steigern und neue Umsatzquellen zu erschließen. Mit einem durchdachten Prozess zur WAN- und Sicherheitstransformation, bei dem keine Abstriche nötig sind, erzielen Unternehmen am Ende einen Multiplikatoreffekt für ihre bestehenden und laufenden Cloudinvestitionen.

aruba
a Hewlett Packard Enterprise company

WP_Successful-WAN-and-Security-Transformation_EM_021621 a00110932enw