BUSINESS-DOKUMENT

aruba
a Hewlett Packard Enterprise company

# BEST-OF-BREED SD-WAN UND SASE MIT ZERO-TRUST UNTERSTÜTZEN DAS DIGITALE UNTERNEHMEN

## INHALTSVERZEICHNIS

## ZUSAMMENFASSUNG

Unternehmen setzen weiterhin auf digitale Transformation, um ihre Effizienz zu steigern, die Kundenzufriedenheit zu verbessern, neue Marktchancen zu nutzen, die Rentabilität zu erhöhen und sich einen Wettbewerbsvorteil zu verschaffen. Die Migration von Unternehmensanwendungen in die Cloud ist ein wesentlicher Bestandteil jeder erfolgreichen digitalen Transformationsinitiative. Warum? Heute laufen mehr Anwendungen in der Cloud als in traditionellen Rechenzentren von Unternehmen, und die meisten dieser Anwendungen werden als Software-as-a-Service (SaaS) genutzt. Darüber hinaus müssen Unternehmen in der Cloud-First-Welt sicherstellen, dass Anwendungen jederzeit, von jedem Ort und mit jedem Gerät direkt und sicher zugänglich sind. Sie wollen auch sicherstellen, dass das Netzwerk sowohl den Mitarbeitern als auch den Kunden eine gleichbleibend hohe Erlebnisqualität bietet. Und schließlich hat die explosionsartige Zunahme von Mobil- und IoT-Geräten im Unternehmen die Angriffsfläche dramatisch vergrößert und setzt Unternehmen Sicherheitsverletzungen aus, die Daten gefährden und zu Netzwerkausfällen führen können.

Die heutigen Unternehmensnetzwerke wurden nie für die Cloud-First-Welt konzipiert und reichen nicht aus, um die Herausforderungen im Zusammenhang mit der Cybersicherheit der digitalen Transformation zu bewältigen. Es ist von entscheidender Bedeutung, dass Unternehmen ihre Cloud-Anwendungen nicht nur schützen, sondern auch die Benutzer, die mit diesen Anwendungen über das Wide Area Network (WAN) eine Verbindung herstellen. Gleichzeitig hat die Verbreitung von IoT-Geräten die Angriffsfläche für Unternehmen erheblich vergrößert, so dass sie im Zusammenhang mit der Cybersicherheit zunehmenden Bedrohungen ausgesetzt sind.

Daher besteht die strategische Notwendigkeit, ein intelligenteres, sichereres und hoch automatisiertes Software-definiertes Wide Area Network (SD-WAN) einzuführen, das mit in der Cloud bereitgestellten Sicherheitsdiensten problemlos zu einer branchenführenden Secure Access Service Edge-Architektur (SASE) integriert werden kann. SASE muss durch identitätsbasierte Zero-Trust-Sicherheit erweitert werden, um eine Segmentierung zu erzwingen, sodass Benutzer und IoT-Geräte nur solche Orte im Netzwerk erreichen können, die ihrer Rolle im Unternehmen entsprechen.

Da die WAN- und Sicherheitstransformation ein Prozess ist, kann ein Unternehmen mit der Modernisierung seines WANs oder der Sicherheit beginnen, aber um den wahren Wert von Cloud-Investitionen zu realisieren, müssen beide Aspekte angegangen werden.

Genauso wichtig ist es, die Abhängigkeit von einem bestimmten Anbieter zu vermeiden, indem man sich für Technologiepartner entscheidet, die Flexibilität und Wahlfreiheit bieten. Mit transformierten Netzwerk- und Sicherheitsarchitekturen können Unternehmen neue, zeitgemäße Innovationen einführen, um Produktivität, Umsatzwachstum und Rentabilität zu beschleunigen und gleichzeitig die Kosten zu senken.

**Die heutigen Unternehmensnetzwerke wurden nie für die Cloud-First-Welt konzipiert und reichen nicht aus, um die Herausforderungen im Zusammenhang mit der Cybersicherheit der digitalen Transformation zu bewältigen. Es ist wichtig, dass Unternehmen nicht nur ihre Cloud-Anwendungen schützen, sondern auch die Anwender, die sich mit diesen Anwendungen verbinden. Gleichzeitig hat die Verbreitung von IoT-Geräten die Angriffsfläche der Unternehmen erheblich vergrößert, so dass sie zunehmenden Bedrohungen für die Cybersicherheit ausgesetzt sind.**

## ANWENDUNGEN WERDEN IN DER CLOUD BEREITGESTELLT — SO SOLLTE ES AUCH MIT DER SICHERHEIT SEIN.

Traditionell wurde der gesamte Datenverkehr der Anwendungen von den Zweigstellen über private MPLS-Dienste zwecks Sicherheitsprüfung und -Verifizierung zurück an das Rechenzentrum des Unternehmens geschickt (siehe Abbildung 1). Diese Architektur machte Sinn, als die Anwendungen ausschließlich im Rechenzentrum des Unternehmens gehostet wurden. Mit der Migration von Anwendungen und Diensten in die Cloud wird diese traditionelle Netzwerkarchitektur jedoch unzulänglich, vor allem weil sie die Anwendungsleistung beeinträchtigt und ein inkonsistentes Benutzererlebnis zur Folge hat, da der für das Internet bestimmte Datenverkehr zunächst das Rechenzentrum und die Unternehmensfirewall durchläuft, bevor er sein Ziel erreicht.

Da zudem immer mehr Mitarbeiter außerhalb des Unternehmensnetzwerks arbeiten und direkt auf Cloud-Anwendungen zugreifen, ist die traditionelle perimeterbasierte Sicherheit nicht mehr ausreichend. Die Cloud und SaaS haben die Art und Weise, wie Benutzer sich mit Anwendungen verbinden und mit ihnen interagieren, für immer verändert. Durch die Umstellung ihrer WAN- und Sicherheitsarchitekturen können Unternehmen einen direkten, sicheren Zugang zu Anwendungen und Diensten in Multi-Cloud-Umgebungen gewährleisten, und das unabhängig vom Standort oder den Geräten, die für den Zugriff verwendet werden.

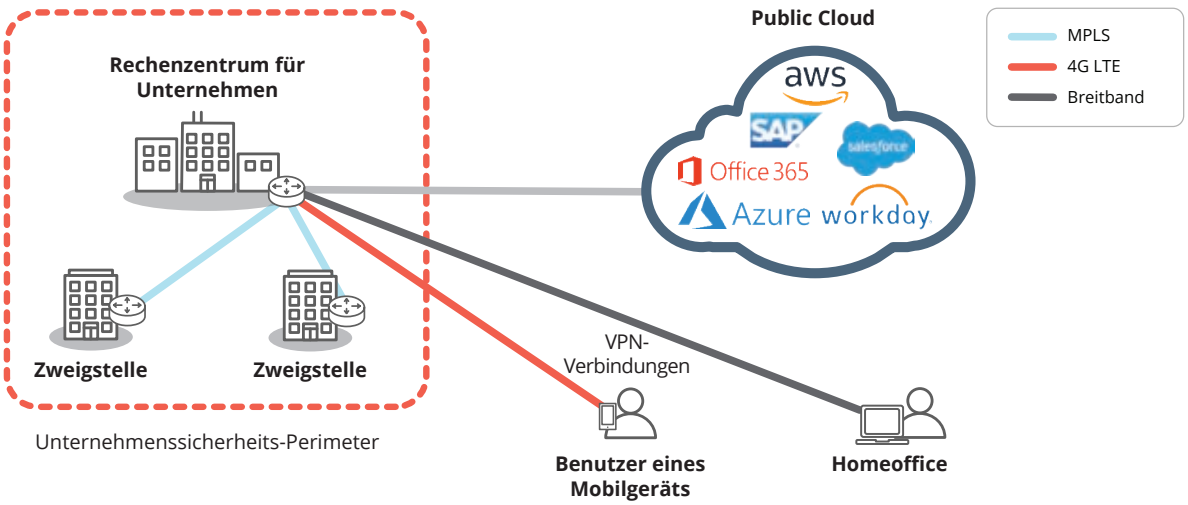


Abbildung 1: Herkömmliche Unternehmens-WANs und perimeterbasierte Sicherheitsansätze wurden nicht für die Cloud konzipiert. Den gesamten Anwendungsdatenverkehr von der Zweigstelle zurückleiten Standorte auf dem Weg zum Rechenzentrum beeinträchtigen die Leistung und führen zu einem inkonsistenten Benutzererlebnis.

2019 prägte Gartner den Begriff SASE (Secure Access Service Edge) für ein Framework, das SD-WAN mit aus der Cloud stammenden Security Service Edge (SSE) Funktionen wie Secure Web Gateway (SWG), Firewall-as-a-Service (FWaaS), Cloud Access Security Broker CASB und Zero Trust Network Access (ZTNA) kombiniert. Bisher waren dies einzelne, dedizierte Funktionen, die nun von der Cloud aus auf einheitliche Weise bereitgestellt werden können, wie in Abbildung 2 dargestellt.

Einige Erstanwender von SSE-Lösungen scheiterten bei der Implementierung eines SD-WAN, das keinen adaptiven Internet-Breakout direkt von den Standorten der Zweigstellen aus vornehmen konnte. Daher konnten sie den Datenverkehr nicht direkt von der Zweigstelle in die Cloud leiten. Ohne die SD-WAN-Komponente wurde der für die Cloud bestimmte Datenverkehr immer noch zum Rechenzentrum zurückgeleitet, was sich auf die Anwendungsleistung negativ auswirkte.

Durch die Einführung von Security Service Edge-Lösungen und SD-WAN entfallen die Kosten und die Komplexität, die mit der Verwaltung mehrerer Firewalls im Unternehmen verbunden sind, aber an den Standorten der Zweigstellen sind nach wie vor Firewall-Funktionen erforderlich, um alle eingehenden Bedrohungen zu blockieren. Wie in Abbildung 3 gezeigt, können sich Unternehmen mit einer fortschrittlichen SD-WAN-Lösung über einen adaptiven Internet-Breakout mit Breitband-Internetverbindungen direkt mit der Cloud verbinden. Die Intelligenz zur Erkennung von Anwendungen auf der Whitelist ermöglicht einen lokalen Breakout von der Zweigstelle zum nächstgelegenen Point of Presence (PoP), wodurch Latenzzeiten beseitigt werden und für vertrauenswürdige SaaS- und Cloud-Anwendungen wie Microsoft Office 365, 8x8 und RingCentral die höchste Erlebnisqualität gewährleistet ist. Durch Application Awareness besteht auch die Möglichkeit, anderen internetgebundenen Datenverkehr zunächst an einen Cloud-Sicherheitsanbieter zur erweiterten Prüfung zu senden, bevor er an einen SaaS-Anbieter weitergeleitet wird. Fortschrittliche SD-WAN-Funktionen, die mit modernen, aus der Cloud zur Verfügung gestellten Sicherheitsdiensten integriert sind, gewährleisten für Benutzer, Geräte, Anwendungen und IoT eine konsistente Durchsetzung der Richtlinien und Zugriffskontrolle. Dadurch können Unternehmen die Compliance durchsetzen, Ausfallzeiten verhindern und das Risiko einer Datenkompromittierung durch eine Sicherheitsverletzung mindern.

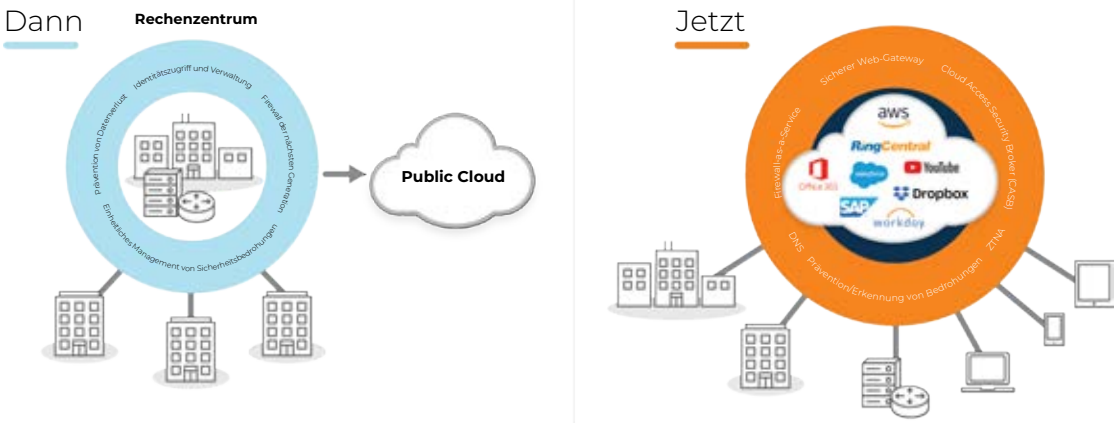


Abbildung 2: In der Vergangenheit ging es vor allem darum, das Rechenzentrum des Unternehmens zu sichern, in dem die Anwendungen ausschließlich gehostet wurden. Seit Anwendungen in die Cloud verlagert wurden und von dort aus bereitgestellt werden, wird die perimeterbasierte Sicherheit von Unternehmen zunehmend ineffektiv. Es muss dringend ein Umdenken erfolgen und die Sicherheit in die Cloud verlagert werden.

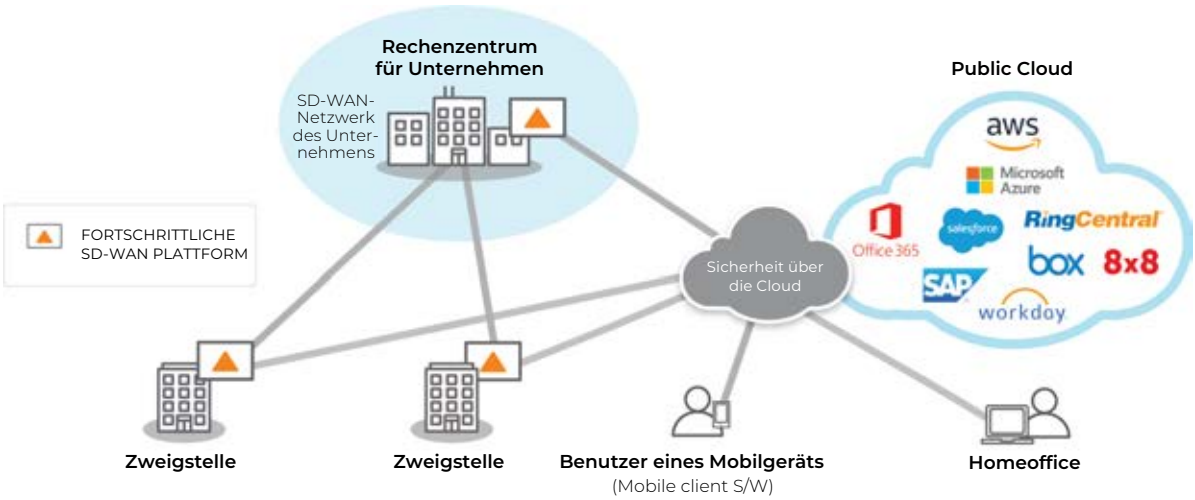


Abbildung 3: Ein fortschrittliches SD-WAN bietet Unternehmen ein sicheres Cloud-On-Ramp. Zweigstellen können Breitbandverbindungen und adaptiven Internet-Breakout nutzen, um Anwender direkt mit Cloud-Anwendungen zu verbinden, und so die Anwendungsleistung und das Benutzererlebnis optimieren. Durch die Kombination von fortschrittlichem SD-WAN und cloudbasierter Sicherheit entsteht ein Secure Access Service Edge (SASE), der sicherstellt, dass Anwender, Geräte und Anwendungen immer sicher sind.

## BEST OF BREED SASE BIETET WAHLFREIHEIT

Aufgrund der sich ständig weiterentwickelnden Ansätze für die Bereitstellung von Netzwerksicherheit und der Komplexität des Aufbaus komplexer Netzwerklösungen ist es wichtig, die klassenbesten Sicherheits- und Netzwerklösungen der Anbieter zu evaluieren, die über nachweisliche Erfahrungen und Kompetenzen verfügen. Es ist unrealistisch, einen einzigen Anbieter zu finden, der branchenführende SASE-Funktionen für beide Bereiche anbietet, und Unternehmen sollten nicht gezwungen sein, bei einem von ihnen Abstriche bei den grundlegenden Funktionen machen zu müssen.

Da die Sicherheit aufgrund der sich ständig weiterentwickelnden Bedrohungen immer wichtiger wird, müssen Unternehmen flexibel genug sein, um neue Sicherheitslösungen schnell und kostengünstig einzuführen, ohne an die Lösungen eines einzigen Anbieters gebunden zu sein. Mit einer unabhängigen Netzwerklösung haben Unternehmen die Gewissheit, die Cloud-Sicherheitslösungen auswählen und einzusetzen zu können, die am besten auf ihre sich entwickelnden Geschäfts- und Sicherheitsanforderungen abgestimmt sind.

Eine fortschrittliche SD-WAN-Lösung lässt sich eng mit mehreren SSE-Anbietern integrieren und ermöglicht die freie Wahl der branchenführenden Anbieterlösungen, die SD-WAN und Sicherheit aus der Cloud durch automatische Orchestrierung vereinen. Mit Best-of-Breed SASE bauen Unternehmen eine konsistente Sicherheitsarchitektur auf, die Auswirkungen von Cyberangriffen abwehrt und gleichzeitig die geschäftliche Agilität erhöht und die Komplexität reduziert. Auf diese Weise können Unternehmen für ihre bestehenden und laufenden Investitionen in Cloud-Anwendungen und -Services letztendlich einen Multiplikatoreffekt erzielen.

## SICHERUNG VON UNTERNEHMENS-IOT MIT EINEM ZERO-TRUST-ANSATZ

Die zunehmende Verbreitung von IoT-Geräten in Unternehmen eröffnet neue Wege, um Geschäftsprozesse zu überwachen, zu dokumentieren, zu melden, zu automatisieren und zu optimieren — von Fertigungsstraßen bis hin zur Automatisierung von HLK und Beleuchtung zur Energieeinsparung. Das IoT macht Unternehmen durch Automatisierung effizienter, aber es vergrößert auch die Angriffsfläche, indem es eine neue Dimension der Komplexität mit sich bringt. Die Art und Weise, wie die IT-Abteilung die wachsenden Sicherheitsherausforderungen für mobile Geräte angeht, besteht darin, eine Zero-Trust Network Access (ZTNA)-Lösung einzusetzen, die auf dem Zero-Trust-Modell basiert. Eine ZTNA-Lösung funktioniert, indem auf einem Anwendergerät wie einem Laptop, Tablet oder Mobiltelefon ein Endpunkt-Agent installiert wird.

Dieser Software-Agent stellt sicher, dass der Datenverkehr vom Gerät an einen in der Cloud verfügbaren Sicherheitsdienst gesendet wird, bevor er an eine SaaS-Anwendung oder einen IaaS-Anbieter weitergeleitet wird. Anders als bei Tablets und Smartphones können ZTNA-Software-Agenten jedoch nicht auf IoT-Geräten installiert werden, da sie agentenlos sind; sie unterstützen nicht die Installation von Software-Agenten von Drittanbietern. Aus diesem Grund benötigen Unternehmen für IoT-Geräte eine andere Sicherheitslösung, um Unternehmensnetzwerke vor potenziellen Bedrohungen zu schützen, die in das Netzwerk eindringen und den täglichen Geschäftsbetrieb stören könnten.

Ein fortschrittliches SD-WAN, das eine Zero-Trust-Architektur unterstützt, segmentiert das Netzwerk dynamisch und wendet die Prinzipien des am wenigsten privilegierten Zugriffs an, sodass Unternehmen das Risiko von Sicherheitsverletzungen beim Einsatz von IoT-Geräten reduzieren können. Es gewährleistet, dass Anwender und Geräte nur mit Zielen kommunizieren, die ihrer jeweiligen Rolle in Bezug auf Identität, Zugriffsrechte und Sicherheitsstatus entsprechen. Es orchestriert eine End-to-End-Segmentierung, die sich über das LAN-WAN-LAN und LAN-WAN-Data Center/Cloud des Unternehmens erstreckt, was mit größerer Transparenz zu einer konsistenten und automatisierten Durchsetzung von Sicherheitsrichtlinien führt. Mit der End-to-End-Segmentierung können Unternehmen isolierte Segmente für den Datenverkehr von IoT-Geräten schaffen. Für jedes Segment kann eine unabhängige Sicherheitsrichtlinie definiert werden, in der die Sicherheitsrichtlinien festgelegt sind, die für den Datenverkehr des Geräts durchgesetzt werden sollen. Da der Datenverkehr in einem Segment vom Datenverkehr in allen anderen Segmenten isoliert ist, wird jeder unbefugte Zugriff verhindert. Selbst wenn eine Bedrohung auftritt, bleiben ihre Auswirkungen auf das Segment begrenzt, in dem sie aufgetreten ist.

Sehen wir uns ein Beispiel an: An einem Remote-Standort, an dem agentenlose IoT-Geräte wie PoS- und HLK-Systeme installiert sind (Abbildung 4 unten), identifiziert eine fortschrittliche SD-WAN-Plattform nur von den Geräten verwendete Anwendungen. Eine Systemrichtlinie fängt den PoS-Datenverkehr ab und leitet ihn an das Rechenzentrum des Unternehmens weiter, in dem die Anwendung zur Kreditkartenverarbeitung gehostet ist. Die vorhandenen Firewall-Services, die in diesem Beispiel im Rechenzentrum eingesetzt werden, werden angewendet. Außerdem segmentieren die Richtlinien für HLK-Systeme den HLK-Datenverkehr und leiten ihn zur zusätzlichen Sicherheitsüberprüfung an den in der Cloud befindlichen Sicherheitsdienst weiter, bevor er das in der Public Cloud gehostete IoT-Kontrollzentrum erreicht. Da der IoT-Datenverkehr gemäß den Unternehmensrichtlinien isoliert wird, stellt ein Verstoß im HLK-Segment kein Risiko für Kreditkarten- und persönliche Daten im PoS-Segment dar. Die Segmentierung hilft Unternehmen auch, PCI- (oder andere) Compliance-Vorgaben für ihr Unternehmen zu erfüllen. Wie in diesem Beispiel gezeigt, kann eine umfassende Sicherheitsimplementierung mit einer fortschrittlichen SD-WAN-Plattform die dynamischen Unternehmen von heute auf ihrem Weg der Transformation besser schützen, während sie die Vorteile des IoT nutzen.

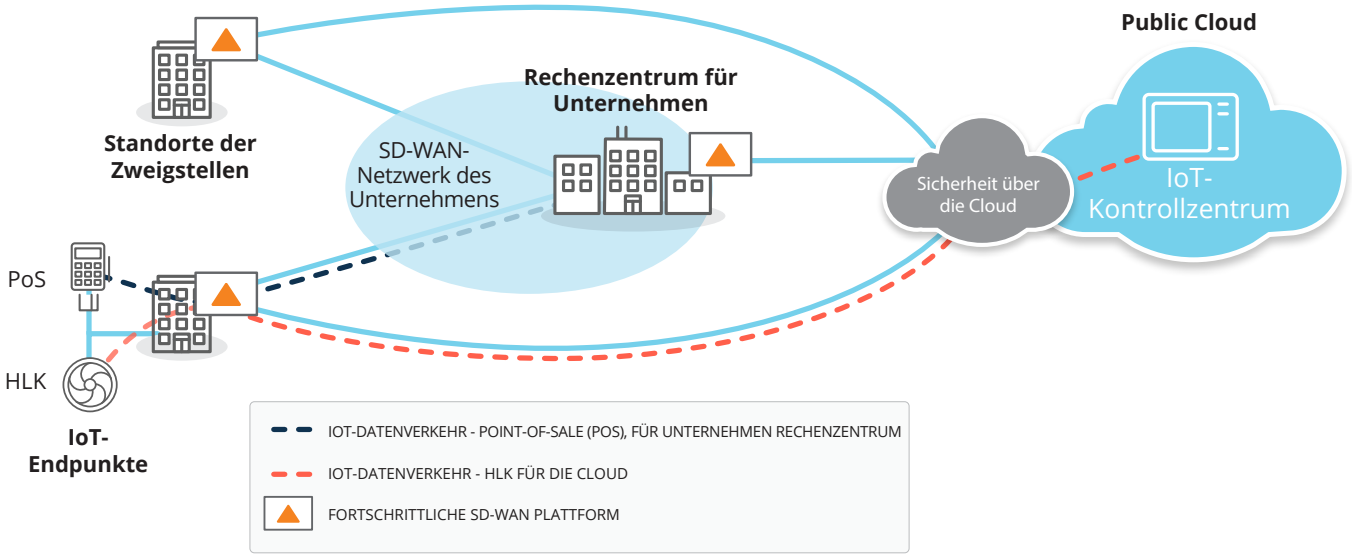


Abbildung 4: IoT-Endgeräte werden immer zahlreicher und bergen neue Risiken für Sicherheitsverletzungen. Mit einer fortschrittlichen SD-WAN-Plattform können Unternehmen IoT-Geräte schützen, indem sie eine Zero-Trust-Architektur implementieren und das Netzwerk dynamisch segmentieren. Wie in der Abbildung gezeigt, werden alle PoS-Transaktionsdaten aus der Zweigstelle an das Rechenzentrum des Unternehmen gesendet, während der HLK-Datenverkehr an ein IoT-Kontrollzentrum in der Cloud weitergeleitet wird.

## SCHUTZ DER ZWEIGSTELLEN VOR ÄUSSEREN BEDROHUNGEN MIT EINEM FORTSCHRITTLICHEN SD-WAN

Mit der Digitalisierung von Unternehmen ist das Risiko von Cyberangriffen in den letzten zehn Jahren erheblich gestiegen. In herkömmlichen Router-basierten Netzwerkumgebungen haben Filialen eine Vielzahl von Netzwerk- und Sicherheitsausrüstungen angehäuft, die sich jedoch nur schwer konfigurieren und warten lassen oder in Bezug auf die neuesten Bedrohungsdaten auf dem Laufenden gehalten werden können. An Remote-Standorten fehlt es außerdem an erfahrenem IT-Personal, wodurch sie potenziellen Sicherheitsverletzungen ausgesetzt sind.

Eine fortschrittliche SD-WAN-Lösung schützt nicht nur den Cloud-Betrieb mit Best-of-Breed-SASE, sondern auch die Filialen vor bösartigen Bedrohungen. Sie verfügt über eine Firewall der nächsten Generation mit Funktionen, die Bedrohungen abwehren, z. B. Angriffserkennung und Prävention (IDS/IPS) und DDoS, um Filialen vor bösartigen Bedrohungen zu schützen.

In der Regel überwacht ein signaturbasiertes IDS-System den Netzwerkverkehr, um Muster zu finden, die einer bestimmten Angriffssignatur entsprechen. Wenn ein Eindringen erkannt wird, sorgt der Sensor für Maßnahmen wie das Verwerfen, Prüfen und Zulassen von Datenverkehr. Systeme zur Verhinderung von unbefugtem Eindringen können entweder im strikten Modus oder im Performance-Modus arbeiten. Im strikten Modus durchläuft der Datenverkehr den Sensor, so dass er sofort blockiert wird, wenn ein Eindringen erfolgt. Im Performance-Modus wird eine Kopie des Datenverkehrs zur Analyse gesendet, was die Netzwerkleistung nicht beeinträchtigt und effizienter ist. Ein Eindringen wird nach seiner Entdeckung blockiert. Je nach Sicherheitsanforderungen können Unternehmen zwischen dem strikten und dem Performance-Modus wählen.

Ein fortschrittliches SD-WAN kann DDoS-Angriffe wie Protokollangriffe, ICMP-Floods, SYN-Floods und IP-Spoofing-Angriffe auch dynamisch erkennen. Nachdem ein anormales Netzwerkverhalten erkannt wurde, begrenzt die Lösung die Anzahl der Anfragen durch Maßnahmen wie Rapid Aging, Drop Excess und Block Source. Außerdem kann sie den Datenverkehr im Falle eines DDoS-Angriffs über nicht betroffene Netzwerkverbindungen leiten und so die Business Continuity sicherstellen.

Wenn Unternehmen fortschrittliche Netzwerk- und Sicherheitsfunktionen wie Routing, WAN-Optimierung und Firewall der nächsten Generation in eine einzige SD-WAN-Lösung integrieren, können sie ihren Netzwerkbetrieb in den Zweigstellen erheblich vereinfachen. Darüber hinaus können Sicherheitsrichtlinien automatisch von einem zentralen Standort aus an die Zweigstellen verteilt werden, was die Konfiguration von Netzwerk- und Sicherheitsrichtlinien erleichtert. Neue Zweigstellen lassen sich schnell und einfach einrichten, und Änderungen der Sicherheitsrichtlinien können innerhalb von Minuten automatisch an Hunderte oder Tausende Zweigstellen verteilt werden, während gleichzeitig die Fehlerquote minimiert wird.

## WAN-TRANSFORMATION IST FÜR DEN ERFOLG DER DIGITALEN TRANSFORMATION ENTSCHEIDEND

Zusätzlich zu all den Vorteilen, die die Migration in eine moderne Cloud-basierte Sicherheitsarchitektur mit sich bringt, ist die Transformation des WAN für die heutigen Cloud-First-Unternehmen von unschätzbarem Wert. Traditionelle routerzentrierte WANs wurden nie für die Cloud konzipiert. Unternehmen müssen ihre WAN-Architektur modernisieren und neu überdenken, wie sie die Netzwerke ihrer Zweigstellen am besten aufbauen, um die Leistung und Sicherheit von Cloud-Anwendungen zu verbessern. Unternehmen nutzen zunehmend Cloud- und SaaS-Lösungen, mit dem Schwerpunkt, den Anwendern die höchste Qualität zu bieten.

Zur WAN-Transformation gehört, zwischen Anwendern und der Cloud einen effizienteren Weg und eine bessere Erfahrung zu bieten. Wie zuvor beschrieben, optimiert die Einführung eines adaptiven Internet-Breakouts für in der Cloud gehostete und SaaS-Anwendungen direkt von den Standorten der Zweigstellen aus nicht nur die verfügbare Bandbreite, sondern verringert auch die Latenz, die sich negativ auf die Produktivität der Benutzer auswirken kann.

Viele Unternehmen sind dabei, ihren Netzwerk-Edge zu transformieren und führen SD-WAN ein, um Zweigstellen über Breitband-Internetverbindungen zu verbinden. SD-WAN bietet auf der Grundlage zentral definierter Richtlinien eine anwendungsgesteuerte intelligente Auswahl von Wegen über mehrere WAN-Verbindungen (MPLS, Breitband-Internet, LTE usw.). Zu den Vorteilen von SD-WAN gehören unter anderem:

- Kostengünstige Bereitstellung von Geschäftsanwendungen
- Verbesserung der Anwendungsleistung, Verfügbarkeit und Erlebnisqualität für den Endbenutzer
- Erfüllen der Anforderungen moderner Zweigstellen/Remote-Standorte oder Standorte
- Anpassung von SaaS- und Cloud-basierten Anwendungen und Services
- Verbesserung der IT-Effizienz in den Zweigstellen durch automatisierte Bereitstellung von Services

## DIE ANFORDERUNGEN DES ANWENDUNGS-SLAS ERFÜLLEN

Dies führt direkt zu einer höheren Unternehmensproduktivität und Geschäftsflexibilität. Unternehmen benötigen ein High-Performance-Netzwerk, das auf einer hochgradig verfügbaren Grundlage aufbaut und geschäftskritische Anwendungen zuverlässig unterstützt. Sicherheit darf nie ein zweitrangiger Aspekt sein. Die Fähigkeit, Funktionen der Mikrosegmentierung und der granularen Durchsetzung von Richtlinien zu unterstützen, bietet Unternehmen die Möglichkeit, ihr WAN zu sichern, Compliance-Anforderungen zu erfüllen und sich gegen Sicherheitsverletzungen zu verteidigen.

Unternehmen brauchen die Flexibilität, neue Zweigstellen zu gründen und Richtlinien und Sicherheitsregeln dynamisch anzupassen. Die Fähigkeit zur Vermittlung von Richtlinienkontexten ist für die Automatisierung von Zweigstellen eine wichtige Voraussetzung. Dies macht das Konzept einer fortschrittlichen SD-WAN-Lösung sehr attraktiv und kann Unternehmen dabei helfen, den Bedarf mehrerer Geräte mit dedizierten Sicherheitsfunktionen überflüssig zu machen und im Gegenzug ihre WAN-Edge-Architektur für Zweigstellen zu vereinfachen und zu konsolidieren — oder „auszudünnen". Eine fortschrittliche SD-WAN-Edge-Plattform ermöglicht es Unternehmen, ihr WAN zu transformieren, indem sie SD-WAN, Routing, WAN-Optimierung, Segmentierung und Sicherheit für Zweigstellen in einer einzigen, zentral verwalteten Plattform vereint.

Die zentralisierte SD-WAN-Orchestrierung und ein anwendungsspezifischer Ansatz gewährleisten, dass sich die Prioritäten des Unternehmens stets im Verhalten des Netzwerks widerspiegeln. Die Vereinheitlichung der Orchestrierung von Netzwerk- und Sicherheitsrichtlinien gewährleistet, dass QoS und Sicherheit konsistent auf Anwendungen – oder Klassen von Anwendungen – angewendet und durchgesetzt werden, unabhängig davon, wie oder von wo aus auf sie zugegriffen wird. Die Anwendungsleistung und -sicherheit kann durch Unternehmensrichtlinien von oben nach unten bestimmt werden, nicht aber durch technologische Einschränkungen von unten nach oben. Ein fortschrittliches SD-WAN überwacht kontinuierlich den Zustand des Netzwerks und der Anwendungen, erkennt veränderte Bedingungen und löst sofortige, automatisierte Echtzeitreaktionen aus, um die Auswirkungen von Spannungsabfällen, Stromausfällen und Sicherheitsbedrohungen zu eliminieren. Darüber hinaus vereinfacht die Automatisierung der Konnektivität von Cloud-Plattformen mit Integrationen über anwendungsprogrammierbare Schnittstellen (APIs) den IT-Betrieb und bietet Unternehmen rechtzeitig die Möglichkeit, Sicherheitsdienste, IaaS und SaaS zu nutzen, die in der Cloud zur Verfügung stehen. Das Netzwerk von heute erfordert End-to-End-Transparenz, Programmierbarkeit und Automatisierung, um die für Multi-Cloud-Umgebungen erforderliche dynamische Leistung, Sicherheit und höchste Erlebnisqualität zu gewährleisten. Ein intelligentes WAN, das mit den branchenführenden SD-WAN- und Cloud-Sicherheitslösungen konzipiert ist, bringt die digitalen Transformationsinitiativen voran und ermöglicht es Unternehmen, sich weiterzuentwickeln und rechtzeitig neue Innovationen einzuführen, ohne ihre Produktivität und ihr Wachstum einzuschränken, während gleichzeitig Sicherheitsrisiken minimiert werden.

## FAZIT

Da moderne Cloud-First-Unternehmen ihre Anwendungen vom Rechenzentrum in die Cloud verlagern, müssen sie die WAN- und Sicherheitstransformation durchführen, um aus ihren Cloud-Investitionen den maximalen Gewinn zu ziehen. SASE, oder Secure Access Service Edge, gibt der Branche eine neue Richtung vor. Wie in Abbildung 5 gezeigt, ist es wichtig, dass Unternehmen sowohl die WAN- als auch die Sicherheitstransformation in Betracht ziehen, wenn sie einen sicheren Zugang zur Service-Edge einrichten, um ein reibungsloses Erlebnis zu ermöglichen.

Eine fortschrittliche SD-WAN-Plattform bietet die Möglichkeit, sich problemlos mit einer Vielzahl von erstklassigen Cloud-Sicherheits-Services zu verbinden und so eine branchenführende SASE-Architektur zu schaffen. Letztlich wird kein einzelner SASE-Anbieter die Möglichkeit haben, über eine einzige Plattform wirklich erstklassige Netzwerk- und Sicherheitstechnologien anzubieten. Angesichts der sich ständig weiterentwickelnden Bedrohungen müssen Unternehmen flexibel genug bleiben, um neue Sicherheitslösungen schnell und kosteneffizient einzuführen. Unternehmen sind gut beraten, wenn sie Plattformen evaluieren, die ihnen die Wahlfreiheit zur Integration des branchenführenden SASE bieten. Dadurch müssen sich Unternehmen nicht auf herstellerspezifische Lösungen eines einzelnen Anbieters festlegen oder sich mit Grundfunktionen und -möglichkeiten zufrieden geben müssen.

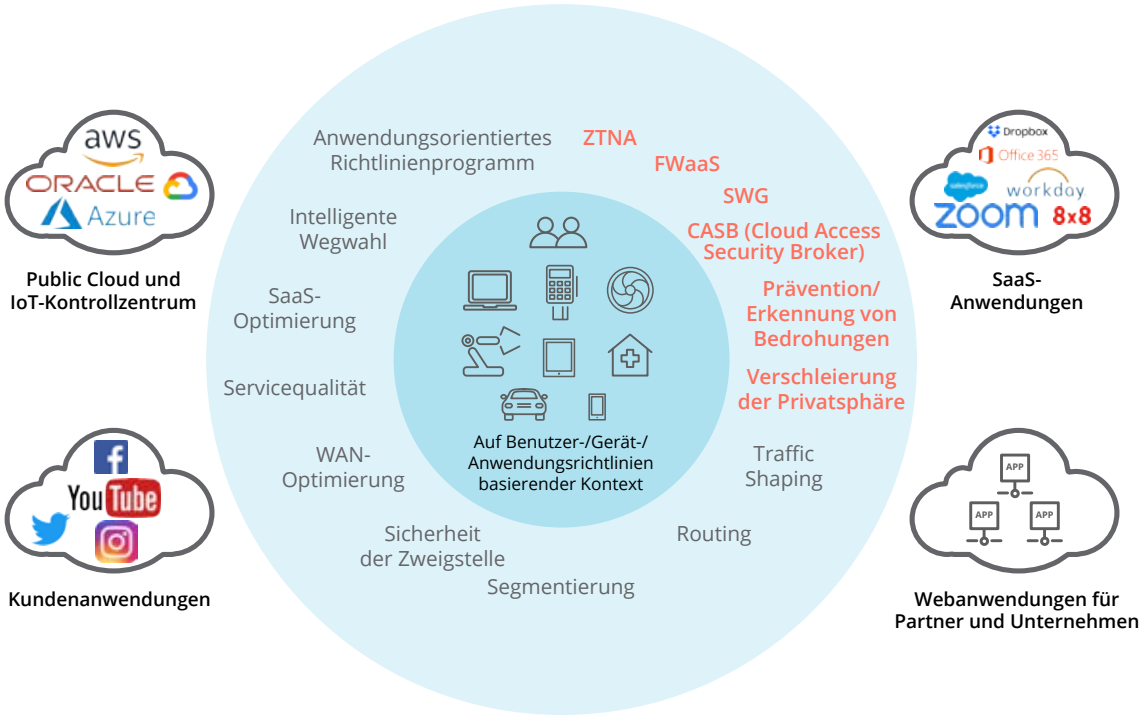


Abbildung 5: Ein sicherer Zugang zum Service-Edge wird benötigt, um die Initiativen des Unternehmens zur digitalen Transformation zu unterstützen, z. B. die Cloud-First-Strategie und die Anforderungen an die Mobilität der Mitarbeiter. In einer robusten SASE-Architektur müssen umfassende WAN-Funktionen mit umfassenden Netzwerksicherheitsfunktionen zusammenarbeiten, um die dynamischen, sicheren Zugriffsanforderungen digitaler Unternehmen für Anwender, Geräte und Anwendungen zu unterstützen.

Außerdem muss angesichts der zunehmenden Verbreitung von IoT-Geräten SASE durch ein Zero-Trust-Sicherheits-Framework ergänzt werden, das auf der Identitätsgrundlage den Datenverkehr dynamisch segmentiert, sodass Anwender und IoT-Geräte nur Netzwerkziele erreichen können, die ihrer Rolle im Unternehmen entsprechen.

Ein fortschrittliches SD-WAN kann die grundlegenden Sicherheitsfunktionen unterstützen, die in der Zweigstelle erforderlich sind, indem es eine Firewall der nächsten Generation mit IDS/IPS-Funktionen integriert und die in der Cloud bereitgestellte Sicherheit ergänzt, um im gesamten Unternehmen eine reibungslose Durchsetzung von Sicherheitsrichtlinien zu gewährleisten. So können Unternehmen ihre Netzwerkinfrastruktur vereinfachen und gleichzeitig in ihrem eigenen Tempo und ohne Kompromisse auf eine moderne, sichere WAN-Architektur umsteigen, bei der die Cloud im Vordergrund steht.

Für Unternehmen, die noch nicht bereit sind, die Firewalls ihrer Zweigstellen abzuschaffen und vollständig auf ein Cloud-basiertes Sicherheitsmodell umzusteigen, ist es schließlich wichtig, eine fortschrittliche SD-WAN-Plattform zu finden, die die Wahlfreiheit zur Unterstützung führender Unified Threat Management (UTM)-Softwarelösungen von Drittanbietern bietet, die als integrierte Lösung in Zweigstellen eingesetzt werden. Dadurch entfallen für Unternehmen nicht nur zusätzliche Kosten und die Komplexität der Verwaltung, die normalerweise bei separaten dedizierten Firewalls anfallen würden. Sie erhalten auch die Flexibilität, branchenführende Lösungen zu implementieren, was letztlich eine reibungslose Migration zu einem Cloud-basierten Sicherheitsmodell ermöglicht.

Da Unternehmen weiterhin erhebliche Investitionen in die Cloud tätigen, werden sie bei Berücksichtigung der Anforderungen an die WAN- und Sicherheitstransformation letztlich auf den Weg gebracht werden, den Anwendern die höchste Qualität zu bieten und gleichzeitig die heutigen Herausforderungen der Cybersicherheit zu bewältigen. Durch eine durchdachte, kompromisslose WAN- und Sicherheitsumstellung können Unternehmen ihre digitalen Ressourcen schützen und aus ihren bestehenden und laufenden Cloud-Investitionen einen Multiplikatoreffekt erzielen.



BP_Successful-WAN-and-Security-Transformation_RVK_080422 a00110932dee

Kontaktieren Sie uns unter www.arubanetworks.com/contact