Enterprise Strategy Group | Getting to the bigger truth.™

ESG-WHITEPAPER

Die 10 wichtigsten Features eines Next-Generation SD-WAN

Von Bob Laliberte, ESG Senior Analyst, und Leah Matuson, Research Analyst

März 2021

Dieses Whitepaper der ESG wurde von Palo Alto Networks in Auftrag gegeben und wird unter Lizenz der ESG vertrieben.

Inhalt

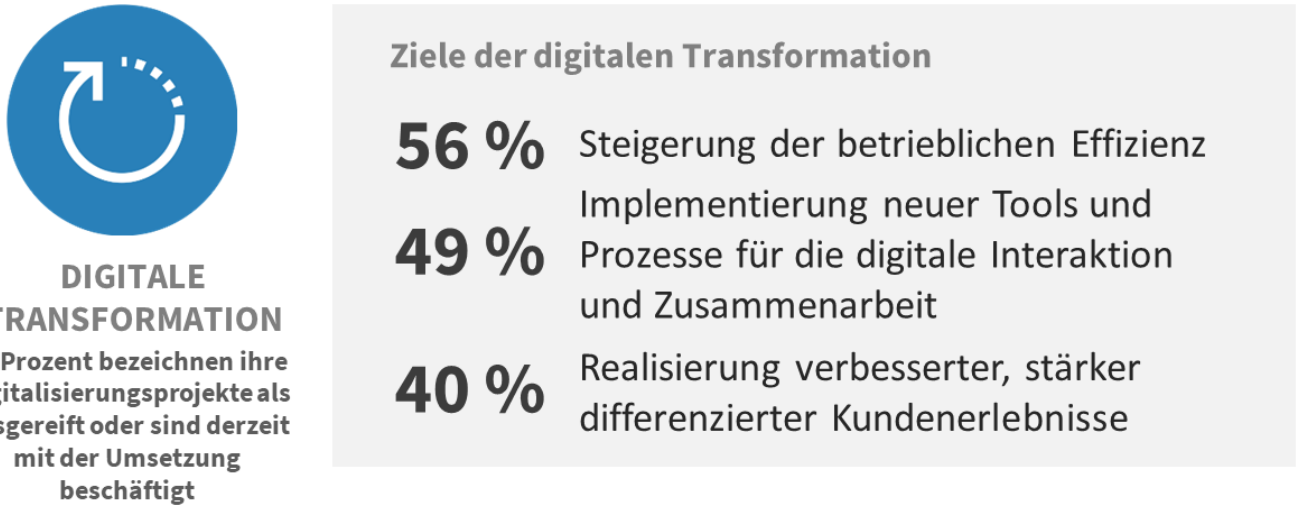
Netzwerklösungen für moderne, verteilte Cloud-Infrastrukturen

Dass moderne Unternehmen immer wieder mit neuen geschäftlichen Rahmenbedingungen konfrontiert sind, ist allgemein bekannt und wenig überraschend. Allerdings hat der Wandel der IT- und Anwendungsinfrastrukturen in letzter Zeit ein derart hohes Tempo erreicht, dass nun in allen Branchen rasche Anpassungen nötig sind. Denn die Pandemie beschleunigt sowohl den flächendeckenden Umstieg auf mobiles Arbeiten als auch die massenhafte Einführung moderner Anwendungen, die auf verteilten Systemen in verschiedenen Rechenzentren, öffentlichen Clouds und an Edge-Standorten gehostet werden. Im Zuge dieser Entwicklung wird die Komplexität der unternehmenseigenen IT-Umgebungen deutlich zunehmen.

Um hier Abhilfe zu schaffen, intensivieren die Verantwortlichen vielerorts ihre Anstrengungen im Bereich digitale Transformation. In einer aktuellen Studie der ESG bezeichnen 22 Prozent der befragten Unternehmensvertreter die eigenen Digitalisierungsinitiativen als ausgereift (weil bereits mehrere einschlägige Modernisierungen umgesetzt und optimiert worden sind), während weitere 50 Prozent von laufenden bzw. in der Umsetzungsphase befindlichen Initiativen berichten.[1] Das ist eine deutliche Zunahme im Vergleich zum Vorjahr, als die entsprechenden Anteile noch bei 19 bzw. 39 Prozent lagen.

Weiteren Aufschluss bietet ein genauerer Blick auf die Gründe, die den Trend zur digitalen Transformation befeuern. In diesem Zusammenhang stellten die Forscher der ESG fest, dass das wichtigste Ziel der erfassten Digitalisierungsinitiativen eine Steigerung der betrieblichen Effizienz ist (56 Prozent), gefolgt von der Einführung neuer Tools und Prozesse für die digitale Interaktion und Zusammenarbeit (49 Prozent) und der Bereitstellung verbesserter und stärker differenzierter Kundenerlebnisse (40 Prozent). Klarerweise handelt es sich dabei sämtlich um Zielsetzungen, die die Anpassung an die oben genannten Veränderungen erleichtern und die Geschäfts- und Unternehmensprozesse krisensicher machen sollen.

Abbildung 1:1 Zahlen und Ergebnisse zur digitalen Transformation



Quelle: Enterprise Strategy Group

Hochgradig verteilte Umgebungen müssen gut vernetzt und gesichert werden

Wie bereits erwähnt, hat die Pandemie nicht nur die Zahl der mobilen Mitarbeiter in die Höhe schnellen lassen, sondern auch die Umstellung auf cloudbasierte Anwendungen beschleunigt. So zeigt die oben erwähnte Studie der ESG, dass COVID-19 in 24 Prozent der erfassten Unternehmen einen dauerhaften Anstieg der Nutzung von Cloud-Anwendungen

[1] Quelle: ESG-Forschungsbericht, *Technology Spending Intentions Survey 2021*, Januar 2021. Alle Verweise auf ESG-Forschungsergebnisse und -Abbildungen beziehen sich auf diesen Forschungsbericht, sofern nicht anders angegeben.

bewirkt hat. Außerdem gibt knapp die Hälfte der Befragten (45 Prozent) an, dass ihr Unternehmen von jetzt an primär cloudnative Anwendungen anschaffen und bereitstellen will. Das ist ein signifikanter Anstieg im Vergleich zum Vorjahr, als dieser Anteil noch bei 38 Prozent lag.

Doch um das volle Potenzial einer verteilten Anwendungsinfrastruktur freisetzen zu können, müssen die Verantwortlichen zunächst für die nötige Konnektivität und effektive Sicherheit sorgen. Wenn geschäftskritische Datenbanken und Apps nicht länger ausschließlich in On-Premises-Rechenzentren gehostet werden und Mitarbeiter ihre Aufgaben überall und über fast jedes Gerät erledigen können, sind effektive, standortunabhängige Sicherheitslösungen erforderlich, die einen dynamisch veränderlichen Perimeter um sämtliche Benutzer und Anwendungen und die gesamte wachsende Angriffsfläche legen. Dementsprechend bezeichnet die relative Mehrheit der von der ESG Befragten (47 Prozent) die Stärkung der Cybersicherheit als wichtigsten Punkt auf ihrer diesjährigen IT-Investitionsagenda (siehe Abbildung 2).

Abbildung 2: Cloud-Migration und Sicherheit als strategische Schwerpunkte

Quelle: Enterprise Strategy Group

Im Einzelnen stehen dabei drei verschiedene Anforderungen im Vordergrund: Zum Schutz von hochgradig verteilten Infrastrukturen sind moderne Netzwerklösungen erforderlich, die erstens über integrierte Sicherheitsfunktionen verfügen, zweitens an jedem Standort die nötige Leistung bieten und drittens erstklassige Kundenerlebnisse unterstützen. Vor diesem Hintergrund will die Mehrheit der Unternehmen (53 Prozent) – laut den Forschungsergebnissen der ESG – verstärkt in langfristige Strategien zum Aufbau von flexiblen IT-Infrastrukturen investieren, um sich gegen künftige Krisen und andere störende Einflüsse auf ihren Geschäftsbetrieb abzusichern. Zugleich lässt sich feststellen, dass die Höhe der IT-Investitionen mit dem Digitalisierungsgrad korreliert. Betriebe mit ausgereifteren Digitalisierungsinitiativen planen durchschnittlich Ausgabensteigerungen von 4,33 Prozent, während Firmen ohne konkrete Digitalisierungsroadmap nur 0,15 Prozent mehr investieren wollen. Infolgedessen wird die Fähigkeit zum Umstieg auf innovative Technologien der nächsten Generation und zur Implementierung von Lösungen für die nahtlose, sichere Anwendungsbereitstellung künftig stark zwischen den beiden Gruppen variieren.

Veraltete Netzwerk- und Sicherheitsinfrastrukturen sind Modernisierungsbremsen

Unter diesen Umständen erweist es sich als gravierender Nachteil, dass die meisten konventionellen Netzwerk- und Sicherheitslösungen nicht für die flächendeckende digitale Transformation der Unternehmensinfrastrukturen ausgelegt sind und architektonische Defizite aufweisen, die die Umsetzung von Innovationen behindern, die Leistung

beeinträchtigen und mit einem hohen Kosten- und Betriebsaufwand verbunden sind. Das gilt insbesondere für Hub-and-Spoke-Netzwerke und auf den Perimeterschutz beschränkte Sicherheitssysteme sowie für einige (ausschließlich paketbasierte) SD-WAN-Lösungen der ersten Generation.

Veraltete Netzwerkinfrastrukturen sind nicht für hochgradig verteilte Umgebungen ausgelegt

Die Defizite von Hub-and-Spoke-Netzwerken

Netzwerke mit einer Speichenarchitektur (Hub-and-Spoke-Netzwerke) wurden ursprünglich für zentralisierte Infrastrukturen entwickelt, in denen alle relevanten geschäftlichen Anwendungen im unternehmenseigenen Rechenzentrum bereitgestellt werden. Sie eignen sich kaum zur Vernetzung der komplexen, hochgradig verteilten Anwendungsumgebungen moderner Unternehmen, weil hier der gesamte von Remote-Standorten ausgehende Netzwerktraffic über das Rechenzentrum fließt, bevor er die gewünschte Cloud-Anwendung oder einen anderen Remote-Standort erreicht. Viele ältere Produkte für den Remote-Zugriff orientieren sich an diesem Modell und nutzen VPNs sowie im Rechenzentrum installierte Konzentratoren und Firewalls für das Routing des Datenverkehrs zwischen Benutzern und Cloud-Anwendungen. Allerdings erweist sich dieser Ansatz zunehmend als Auslaufmodell denn als langfristige Lösung, da er eine Reihe kaum zu bewältigender Herausforderungen mit sich bringt:

- Hohe Kosten: Konventionelle Netzwerklösungen basieren üblicherweise auf teuren und nicht dynamisch anpassbaren Datenleitungen, die von Telekommunikationsanbietern bereitgestellt werden. Das trifft besonders für Hochverfügbarkeits-MPLS-Verbindungen zu, deren Einrichtung zudem oft weitere Ausgaben für den Ausbau lokaler Anschlussnetze nach sich zieht.

- Mangelnde Flexibilität: Aufbau, Ausbau und Verknüpfung kabelgebundener MPLS-Leitungen verschlingen oft viel Zeit. Das erschwert insbesondere die Anwendungsbereitstellung an Edge-Standorten.

- Leistungseinbußen: Beim Festhalten an einer veralteten Netzwerkarchitektur wird das Rechenzentrum mit seinen vielfältigen Sicherheitssystemen schnell zum Nadelöhr, das unnötige Latenzen verursacht und die Anwendungsleistung beeinträchtigt. Außerdem wird hier der gesamte Datenverkehr – vom Gast-WLAN bis zur geschäftskritischen SAP-Anwendung – mit gleicher Priorität übertragen und bei einem Ausfall unterschiedslos auf die Backup-Verbindungen ausgelagert. Erschwerend kommt hinzu, dass die hierfür erforderlichen manuellen Prozesse in vielen Fällen mit einem hohen Zeit- und Arbeitsaufwand verbunden sind.

Weitere Hindernisse durch veraltete SD-WAN-Lösungen

Die Defizite eines konventionellen SD-WAN

Grundsätzlich ist ein SD-WAN deutlich besser für die Anforderungen moderner Unternehmen geeignet als eine herkömmliche Netzwerkinfrastruktur. Trotzdem weisen auch die SD-WAN-Lösungen der ersten Generation gewisse Defizite auf, die den erfolgreichen Umstieg auf verteilte Anwendungsbereitstellungsmodelle erschweren können. Im Vordergrund stehen dabei vor allem die folgenden drei Nachteile:

Rein netzwerkbezogenes Routing und Monitoring: Frühe SD-WAN-Lösungen beschränken sich auf Paketdaten und Analysen des Layer-3-Datenverkehrs und bieten daher nur begrenzte Einblicke in das Geschehen auf der Anwendungsebene. Somit eignen sich diese Produkte in erster Linie zur Durchsetzung netzwerkbezogener Quality-of-Service-Vorgaben, während die Kontrolle der für Cloud- und Edge-Anwendungen geltenden SLAs möglicherweise die Implementierung zusätzlicher Tools erfordert.

Inkonsistente Sicherheitsmaßnahmen: Die Bereitstellung der meisten SD-WAN-Lösungen der ersten Generation erfolgt in Zusammenarbeit mit Sicherheitsanbietern, deren Tools nach der Installation auf die neu eingerichteten Filialinfrastrukturen aufgesetzt werden. Infolgedessen steigt der Zeit- und Arbeitsaufwand für die Einrichtung, Verwaltung und Pflege der Sicherheitsmechanismen. Darüber hinaus birgt dieses Modell das Risiko, dass die an den verschiedenen Remote- und Edge-Standorten eingerichteten Schutzmaßnahmen Diskrepanzen aufweisen, die alle Anstrengungen zur Durchsetzung unternehmensweit einheitlicher Sicherheitsvorgaben aushebeln. Dieses Problem verschärft sich im Zuge des Umstiegs auf mobiles Arbeiten und verteilte Bereitstellungsmodelle noch. Insofern überrascht es nicht, dass die von der ESG Befragten sowohl die Unterstützung der steigenden Zahl mobiler Mitarbeiter als auch die Behebung der aus der Umstellung auf mobile Arbeitsmodelle resultierenden Sicherheitslücken zu den wichtigsten aktuellen Herausforderungen zählten.[2]

Manuelle Prozesse und Abläufe: Wenn Management, Anpassung und Pflege der weitverzweigten, komplexen Netzwerkinfrastruktur überwiegend manuell erfolgen, ist es dem zuständigen IT-Team kaum möglich, ein gutes Benutzererlebnis sicherzustellen. Obwohl hier mittlerweile in den Bereichen Installation und Bereitstellung substantielle Fortschritte zu verzeichnen sind, basieren die Betriebsprozesse und das Lebenszyklusmanagement in vielen Fällen weiterhin auf manuellen Abläufen.

Generell haben fast alle Unternehmen große Mühe, die wachsende Komplexität ihrer Umgebungen für die verteilte Anwendungsbereitstellung und die flächendeckende Unterstützung mobiler Arbeitsmodelle zu bewältigen – unabhängig von der Art der derzeit verwendeten Netzwerklösung. Bei der Umfrage der ESG erklärten 75 Prozent der Teilnehmer, die IT-Infrastruktur ihres Unternehmens sei aktuell komplexer als noch vor zwei Jahren. Zugleich benennt die Studie die fünf wichtigsten Ursachen für diese Entwicklung, die ausnahmslos auf die Herausforderungen rund um die sichere Vernetzung einer hochgradig verteilten Infrastruktur verweisen. Im Einzelnen handelt es sich dabei um die pandemiebedingt steigende Zahl der mobilen Arbeiter (49 Prozent), neue Datensicherheits- und Datenschutzrichtlinien (38 Prozent), wachsende Datenvolumen (38 Prozent), die unbeständige Cybersicherheitslage (35 Prozent) und die zunehmende Zahl und Vielfalt der Endpunkte (32 Prozent).

Checkliste für Ausschreibungen: 10 Vorteile, die Unternehmen auf ihrem Weg in eine erfolgreiche Zukunft benötigen

Bei der Suche nach einer Lösung, die ihrem Unternehmen langfristig sichere Konnektivität für die Anwendungsbereitstellung aus hochgradig verteilten Cloud-Umgebungen und die flächendeckende Einführung mobiler Arbeitsmodelle bietet, können sich die für den IT-Betrieb zuständigen Teams an der nachstehenden Checkliste orientieren.

Dementsprechend sollte das gewählte Next-Generation SD-WAN unbedingt die folgenden zehn Features aufweisen:

1. Anwendungsbezogenes Monitoring und Routing: Im Zuge der fortschreitenden Digitalisierungsinitiativen und der Umstellung auf moderne Bereitstellungsmodelle entstehen hochgradig verteilte Anwendungsinfrastrukturen, die ihrerseits die Implementierung effektiver Tools zur standortunabhängigen Optimierung des Benutzererlebnisses erforderlich machen. Deshalb sollte die von Ihnen gewählte Next-Generation SD-WAN-Lösung unbedingt das anwendungsbezogene Routing und Monitoring unterstützen. Mithilfe der bereitgestellten Layer-7-Daten sollten bei Bedarf für jede Anwendung eigene Richtlinien, SLAs und Übertragungspfade implementiert werden können (statt wie bisher nur für das gesamte Netzwerk). Das erleichtert nicht zuletzt den Umstieg auf die öffentliche Cloud oder Multi-Cloud-Umgebungen, die sich eventuell aus verschiedenen IaaS- und SaaS-Angeboten zusammensetzen.

[2] Quelle: ESG-Forschungsbericht, *The Impact of the COVID-19 Pandemic on Remote Work, 2020 IT Spending, and Future Tech Strategies*, Juni 2020.

2. Komfort und Benutzerfreundlichkeit: Da der Betrieb einer modernen Unternehmensinfrastruktur auch so schon kompliziert genug ist, sollten Sie unbedingt darauf achten, dass sich Ihr neues Next-Generation SD-WAN ohne jahrelange Einarbeitung installieren und bedienen lässt. Insbesondere muss die Lösung rasch und ohne Entsendung von Technikern an allen Remote-Standorten bereitgestellt werden können. Sie benötigen also gewissermaßen ein Plug-and-Play-Produkt, das sofort betriebsbereit ist, wenn es von den vor Ort befindlichen Benutzern mit Strom versorgt und an das Netzwerk angeschlossen wurde. Außerdem sollten Sie sicherstellen, dass Ihr Next-Generation SD-WAN die Zusammenführung von Netzwerk und Sicherheit durch rollenbasierte Zugriffsoptionen für die verschiedenen Teams unterstützt.

3. Hoher Automatisierungsgrad: Die meisten verteilten Unternehmensinfrastrukturen sind mittlerweile so komplex, dass sie mit manuellen Prozessen nicht länger effektiv verwaltet werden können. Um hier die Kontrolle zu behalten, benötigen die für den IT-Betrieb zuständigen Teams eine SD-WAN-Lösung mit intelligenten Automatisierungsfunktionen, die nicht nur die anfängliche Installation erleichtern (Stichwort: Zero-Touch-Bereitstellung), sondern auch die Optimierung und Störungsbehebung der Netzwerkinfrastruktur übernehmen. Beispielsweise kommt es darauf an, dass die Ursachen auftretender Probleme schnell und zielsicher im Netzwerk oder in der Anwendungsinfrastruktur lokalisiert werden können. Hier werden künftig verstärkt Zukunftstechnologien wie künstliche Intelligenz und maschinelles Lernen zum Einsatz kommen.

4. Cloudbasierte Administrations- und Sicherheitsprozesse: Viele Unternehmen haben während der Pandemie auf mobile Arbeitsmodelle umgestellt und müssen nun dafür sorgen, dass sämtliche Mitarbeiter heute und in Zukunft an jedem Standort produktiv arbeiten können. Dieses Ziel lässt sich im IT-Bereich nur mit einer Next-Generation-Lösung mit cloudbasierten Managementfunktionen erreichen. Insbesondere benötigen die für den Netzwerk- und Anwendungsbetrieb zuständigen Teams eine benutzerfreundliche Konsole, die standortunabhängig zugänglich ist, die Implementierung von Anwendungs-, Sicherheits- und Compliance-Richtlinien unterstützt und deren unternehmensweite Durchsetzung ermöglicht. Durch die Entscheidung für eine solche Lösung schaffen Sie nicht nur optimale Voraussetzungen für die Pflege und Anpassung Ihrer Netzwerkinfrastruktur, sondern erleichtern auch die Bereitstellung einheitlicher Schutzmaßnahmen und das automatische Patching. Außerdem kann eine Sicherheitsinfrastruktur mit cloudbasierten Managementfunktionen kontinuierlich (statt wie bisher im Rahmen halbjährlicher oder jährlicher Releases) um neue Features und Sicherheitsupgrades erweitert werden, wenn das von Ihnen gewählte Produkt auf einer modernen Anwendungsarchitektur basiert.

5. Enge Verzahnung von Netzwerk und Sicherheit: Die wachsende Verbreitung des SASE-Frameworks forciert die Zusammenführung der Netzwerk- und Sicherheitsfunktionen (und der dafür zuständigen Teams). Hier kann ein Next-Generation SD-WAN mit sicheren Zugriffsoptionen einen wichtigen Beitrag leisten. Allerdings ergibt sich bei der Einrichtung einer entsprechenden Plattform die Herausforderung, dass alle zusätzlichen Sicherheitssysteme in die SD-WAN-Lösung integriert werden müssen. Hierfür ist eine zentrale, cloudbasierte Managementkonsole erforderlich, die unter anderem die Bereitstellung von Next-Generation Firewalls (NGFW), Lösungen für Zero-Trust-Netzwerkzugang (ZTNA), sicheren Web-Gateways (SWG), Cloud Access Security Brokern (CASB) und RBI-Diensten (Remote Browser Isolation) unterstützt. Darüber hinaus sollte diese Konsole rollenbasierte Zugriffsoptionen bieten, die sich flexibel an die Anforderungen der Netzwerk- und Sicherheitsteams anpassen lassen. Unternehmen stehen also vor der Wahl, entweder den klassischen Best-of-Breed-Ansatz weiter zu verfolgen oder sämtliche Produkte aus einer Hand zu beziehen, um die Integration zu erleichtern.

6. Zuverlässigkeit und Leistung: Next-Generation SD-WAN-Lösungen müssen in der Lage sein, den Datenfluss im Netzwerk unabhängig von der vorhandenen Leitungsinfrastruktur zu optimieren. Das von Ihnen gewählte Produkt sollte also neben MPLS- und Breitbandverbindungen auch gängige Mobilfunknetze wie 4G sowohl für den regulären

Betrieb als auch als Failover-Infrastrukturen unterstützen, um die in puncto Hochverfügbarkeit gestellten Anforderungen erfüllen zu können. Hier eröffnet sich neuerdings mit der flächendeckenden Einführung von 5G die Möglichkeit, eine primär auf Mobilfunknetzen basierende Übertragungsinfrastruktur einzurichten. Doch ganz gleich, ob Sie sich für diese Option entscheiden oder nicht: Die von Ihnen gewählte SD-WAN-Lösung sollte in jedem Fall für eine optimale Bandbreitennutzung sorgen und automatisch in Abhängigkeit der für die betreffende Anwendung festgelegten Priorität den besten Pfad wählen. Dafür müssen sowohl Paketdaten (Layer 3) als auch Daten zu den Anwendungssitzungen (Layer 7) zur Verfügung stehen.

7. Lückenlose Transparenz: Um eine effektive Überwachung und Optimierung des Benutzererlebnisses zu ermöglichen, muss die gewählte Lösung den gesamten Übertragungspfad vom Endgerät bis zum Anwendungsserver lückenlos überwachen. Dabei sollte es keine Rolle spielen, ob es sich bei dem Ersteren um einen unternehmenseigenen IoT-Sensor oder ein privat genutztes Mobilgerät handelt und ob der Letztere im internen Rechenzentrum, an einem Edge-Standort oder in der öffentlichen Cloud implementiert wurde. Wenn Ihr SD-WAN detaillierte Layer-3- und Layer-7-Daten bereitstellt, können Netzwerk- und Anwendungsstörungen schneller lokalisiert und behoben werden. Außerdem erleichtert ein umfassender Überblick über den Netzwerk- und Anwendungsbetrieb die Erstellung von Richtlinien für spezifische Umgebungen.

8. Einsparungen: Bedauerlicherweise wachsen IT-Budgets nicht im gleichen Tempo wie die Komplexität der Unternehmensinfrastrukturen. Daher ist es ein nicht zu unterschätzender Vorteil, dass ein modernes Next-Generation SD-WAN die Ablösung kostenintensiver MPLS-Leitungen durch günstigere Breitbandverbindungen unterstützt. Die hier möglichen Einsparungen fallen besonders deutlich aus, wenn Ihr Unternehmen ein MPLS-basiertes Hub-and-Spoke-Netzwerk betreibt, dessen Hochverfügbarkeitsverbindungen durch dedizierte Failover-Leitungen abgesichert sind. Der Grund: In einem SD-WAN können Hochverfügbarkeits- und Failover-Infrastrukturen durch eine Aktiv/Aktiv-Konfiguration realisiert werden. Zudem ermöglicht eine Next-Generation SD-WAN-Lösung die Konsolidierung des Hardware- und Softwarebestands an den Unternehmensstandorten, wodurch sich unter anderem die Wartungskosten reduzieren.

9. Mehr Flexibilität: Die Möglichkeit zur schnellen Anbindung neuer Standorte hat sich im Zuge der Pandemie als äußerst wichtig erwiesen. Deshalb müssen Next-Generation SD-WAN-Lösungen sowohl die klassische Büroarbeit als auch mobile Arbeitsmodelle unterstützen. Wenn Sie nicht nur kabelgebundene Breitband- und MPLS-Leitungen, sondern auch Mobilfunknetze zur Bereitstellung von Konnektivität nutzen können, profitieren Sie bei der Einführung neuer Technologien von einem Höchstmaß an Flexibilität. Des Weiteren sollten Sie unbedingt darauf achten, dass Ihr Next-Generation SD-WAN mit einem asymmetrischen Bereitstellungsmodell punktet: Hier muss lediglich eine Appliance an jedem Unternehmensstandort installiert werden, damit die dortigen Mitarbeiter direkten Zugriff auf die Cloud erhalten und der Datenfluss in der Netzwerkinfrastruktur optimiert werden kann. (Das ist ein deutlicher Vorteil gegenüber einem symmetrischen Bereitstellungsmodell, bei dem nicht nur in den Zweigstellen, sondern auch in den Zielumgebungen oder in deren unmittelbarer Nähe Appliances eingerichtet werden müssen.)

10. Beschleunigte Innovationsprozesse: Auch dieses letzte Kriterium ist von größter Wichtigkeit, weil sich die Vorteile der Next-Generation SD-WAN-Lösungen keineswegs in einer Senkung der Netzwerkkosten und der Bereitstellung zusätzlicher Bandbreite erschöpfen. Entscheidend ist vielmehr, was Unternehmen mit den zusätzlichen Übertragungskapazitäten anfangen können. Deshalb sind die Verantwortlichen aufgerufen, schon bei der Sichtung entsprechender Produkte auszuloten, wie diese die Verbesserung des Benutzererlebnisses und die Bereitstellung innovativer Serviceangebote (beispielsweise über bandbreitenintensive Video- oder Voice-Apps) unterstützen. Dabei sollte auch berücksichtigt werden, dass Next-Generation SD-WAN-Lösungen zur Konsolidierung verschiedener Dienste am Netzwerk-

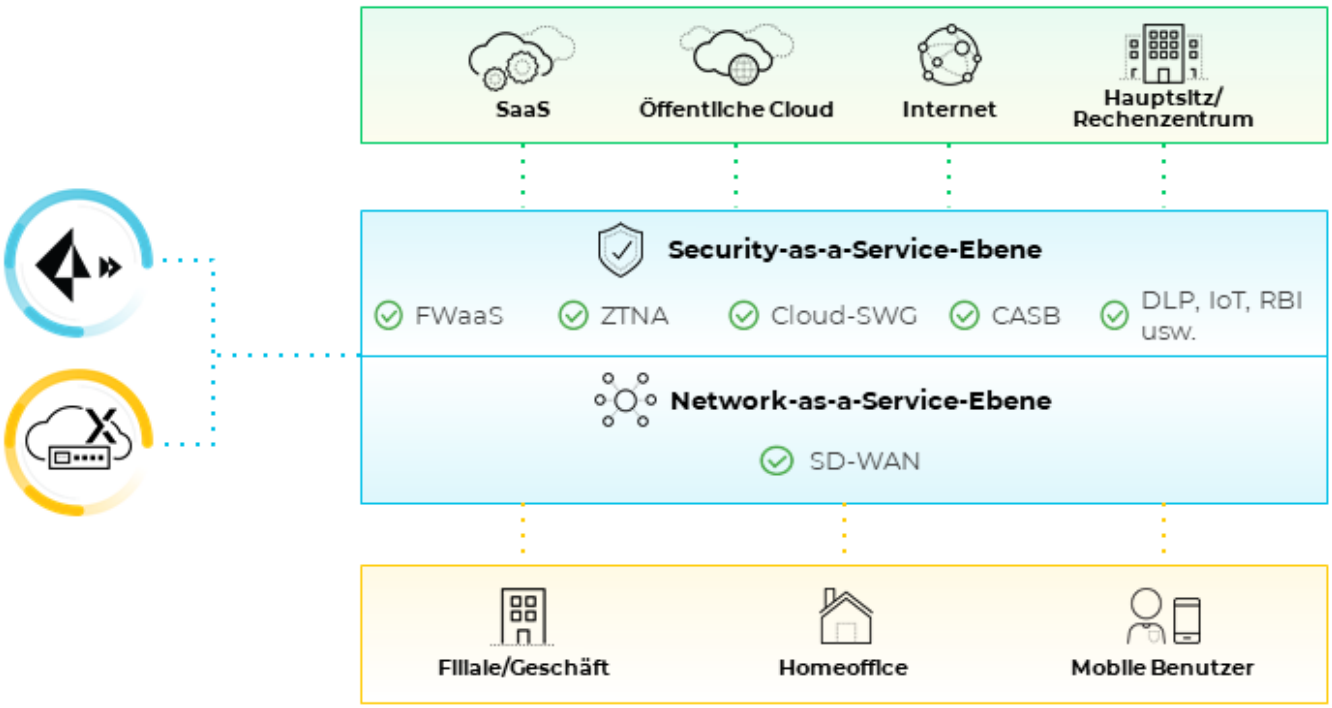
Edge genutzt werden können. Hier bieten sich neben der Einrichtung eines SASE zahlreiche weitere Integrationsmöglichkeiten mit einem beträchtlichen Mehrwertpotenzial.

Das Next-Generation SD-WAN von Palo Alto Networks

Die Sicherheits- und Managementlösung für verteilte Bereitstellungsinfrastrukturen

Da Palo Alto Networks über reiche Erfahrung im Bereich Next-Generation-Technologie verfügt, war es nur konsequent, dass die Prisma-Produktfamilie nach der Übernahme von CloudGenix im April 2020 um eine SD-WAN-Lösung erweitert wurde: Prisma SD-WAN (ehemals CloudGenix SD-WAN). Die bahnbrechende Technologie bietet Kundenunternehmen die Möglichkeit, eine sichere Netzwerkinfrastruktur für alle Büro- und mobile Arbeiter sowie die auf verschiedene Rechenzentren, Cloud-Umgebungen und Edge-Standorte verteilten Anwendungen einzurichten. Außerdem lässt sich Prisma SD-WAN mit Prisma Access zu einer umfassenden SASE-Plattform kombinieren (siehe Abbildung 3).

Abbildung 3: Die umfassende SASE-Lösung von Palo Alto Networks



Quelle: Palo Alto Networks

Prisma SD-WAN von Palo Alto Networks

Prisma SD-WAN von Palo Alto Networks ist eine Next-Generation-Netzwerklösung zur Umsetzung anwendungsspezifischer Konnektivitätsanforderungen. Damit können Unternehmen den Umstieg auf kostengünstige Breitbandverbindungen vorantreiben und das volle Potenzial von 4G- und 5G-basierten Infrastrukturen für Backup-Einsatzszenarien und den Normalbetrieb freisetzen. Darüber hinaus erhalten Kunden durch die Kombination von Prisma SD-WAN mit Prisma Access eine robuste SASE-Plattform. Besonders hervorzuheben sind dabei die folgenden drei Vorteile der Lösung:

Routing und Monitoring auf Anwendungsebene

Prisma SD-WAN nutzt Daten aus der Netzwerk- und Anwendungsüberwachung, um Mitarbeitern an allen Standorten beim Zugriff auf verteilte Anwendungen ein ansprechendes Benutzererlebnis zu bieten. Außerdem erhalten die Verantwortlichen unter anderem detaillierte Angaben zu den erfassten Voice- bzw. Video-Codecs und der (von den Benutzern wahrgenommenen) Übertragungsqualität, damit sie die Einhaltung anwendungsspezifischer SLAs kontrollieren und fundierte Entscheidungen hinsichtlich der Optimierung des Datenflusses treffen können. Davon profitieren nicht zuletzt die Benutzer von Zoom, Teams und anderen Tools für die standortübergreifende digitale Zusammenarbeit. Auch die Störungsbehebung wird drastisch beschleunigt, weil die Ursachen auftretender Probleme rasch in der Netzwerk- und Anwendungsinfrastruktur lokalisiert werden können.

Abgesehen davon zeichnet sich Prisma SD-WAN durch ein hohes Mehrwertpotenzial aus, da zur Realisierung der genannten Vorteile lediglich eine unternehmensseitige Implementierung von Edge-Appliances erforderlich ist. Dieses asymmetrische Bereitstellungsmodell bringt ein deutliches Plus an Flexibilität und verkürzt zudem die Amortisierungszeit.

Leistungsstarke Automatisierungsfunktionen

Prisma SD-WAN wurde speziell zur Realisierung von Effizienzsteigerungen konzipiert und unterstützt daher sowohl automatisierte Installationsprozesse als auch einen automatisierten Netzwerkbetrieb. Zum einen macht die Lösung die Entsendung von Netzwerkexperten an Remote-Standorte überflüssig, da bei der Zero-Touch-Bereitstellung (ZTD) der ION 1000 und anderer Zweigstellen- und Homeoffice-Appliances lediglich der Strom- und Netzwerkanschluss hergestellt werden muss. Wenn dieser einfache Schritt von den Büromitarbeitern vor Ort erledigt wurde, übernimmt die cloudbasierte Managementlösung die richtlinienbasierte Einrichtung der Geräte.

Zum anderen entlastet Prisma SD-WAN die Netzwerkteams der Unternehmen auf vielerlei Weise. Erstens übernimmt die Lösung im Rahmen der automatischen Störungshebung die Konsolidierung der relevanten Ereignisdaten sowie die Identifizierung und Beseitigung der Ursachen des Problems. Zweitens erleichtert Palo Alto Networks durch die Integration von ServiceNow die Übermittlung der relevanten Netzwerk- und Anwendungsdaten, falls ein Vorgang eskaliert werden muss. Drittens unterstützt Prisma SD-WAN die kombinierte Nutzung von Fest- und Funknetzen und erleichtert den Verantwortlichen damit die Umsetzung von Hochverfügbarkeitsvorgaben und die Einrichtung von Backup-Infrastrukturen. Und viertens stellen automatische Optimierungsfunktionen die Einhaltung anwendungsspezifischer SLAs und Richtlinien sicher, indem sie den Datenverkehr jeder App über den jeweils am besten geeigneten Pfad leiten. Dabei haben Kunden auch die Möglichkeit, das cloudnative Backbone-Netzwerk von Palo Alto Networks als Alternative zur Übertragung über das Internet zu nutzen.

Cloudbasiertes Management

Die benutzerfreundliche, cloudbasierte Managementkonsole von Prisma SD-WAN bietet NOC- und SOC-Mitarbeitern im Homeoffice und im Büro rollenbasierten Zugriff auf relevante Informationen und leistungsstarke Funktionen zur Erstellung von Richtlinien. Zugleich senkt die Cloud-Lösung den Hardwarebedarf der Kundenunternehmen und beschleunigt die Betriebs-, Wartungs- und Anpassungsprozesse, da neue Patches und Funktionen nahtlos und ohne vorübergehende Außerbetriebnahme implementiert werden können.

Ein weiteres großes Plus der zentralen Konsole von Prisma SD-WAN ist die Möglichkeit zur sofortigen Durchsetzung der definierten Richtlinien an sämtlichen Edge-Standorten. So lassen sich – bei enger Verzahnung mit Prisma Access – im Handumdrehen einheitliche Sicherheitsmaßnahmen für das gesamte Unternehmen einrichten.

Darüber hinaus ermöglicht Prisma SD-WAN mit der sogenannten CloudBlades-Technologie die API-basierte Edge-Bereitstellung innovativer Sicherheits- und Voice-Services sowie diverser operativer Dienste, ohne dass dafür zusätzliche

Hardware oder Software nötig ist. Hier werden neben Prisma Access auch zahlreiche Drittanbieterdienste wie ServiceNow, Microsoft, Slack, Equinix, Amazon, RingCentral und PagerDuty unterstützt. Außerdem können Unternehmen mit einem speziellen Programm eigene CloudBlades-Integrationen entwickeln.

Prisma Access: die cloudbasierte Sicherheitslösung von Palo Alto Networks

Palo Alto Networks zählt seit Langem zu den führenden Anbietern von Sicherheitslösungen und versetzt moderne Unternehmen mit Prisma Access in die Lage, den Abdeckungsbereich ihrer Sicherheitsinfrastruktur auf Remote-Standorte und mobile Mitarbeiter auszudehnen. Das Produkt besticht durch ein breites Spektrum cloudbasierter Management-, Netzwerk- und Sicherheitsfunktionen, mit denen der Aufbau eines SASE signifikant beschleunigt werden kann. Außerdem ermöglicht es eine lückenlose Überwachung des gesamten Übertragungswegs vom Endgerät (darunter auch IoT-Sensoren) bis zur Cloud-Anwendung.

Zu diesem Zweck stellt Prisma Access die folgenden cloudbasierten Sicherheitsfeatures bereit: Zero-Trust-Netzwerkzugang (ZTNA) zur Zugangskontrolle und Bedrohungsabwehr; Firewall-as-a-service (FWaaS) zum Schutz von Remote-Standorten mit den Erkennungs- und Sicherheitsfunktionen der Next-Generation Firewalls von Palo Alto Networks; Secure Web Gateway (SWG) als Lösung zur ML-gestützten Sperrung schädlicher Websites und zur Verhinderung von Datenverlusten; Cloud Access Security Broker (CASB) zur Durchsetzung der für den Datenaustausch zwischen On-Premises-Geräten und Cloud-Plattformen (IaaS und SaaS) geltenden Sicherheitsrichtlinien; Data Loss Prevention (DLP) zur Stärkung der Datensicherheit und zur Umsetzung geltender Datenschutzrichtlinien; (Remote) Browser Isolation (BI/RBI) zur Minimierung der Angriffsfläche der Endgeräte beim Surfen im Internet; IoT Security zum Schutz vor Angriffen auf vernetzte Geräte und den damit verbundenen Ausfallzeiten, Produktivitätseinbußen und Umsatzverlusten.

Fazit

Um in der modernen Geschäftswelt rund um die Uhr am Ball bleiben zu können, müssen Unternehmen in zukunftsfähige Produkte zur Leistungsoptimierung und Sicherung weitverzweigter Netzwerkinfrastrukturen für mobile Benutzer und verteilte Anwendungen investieren. Das gilt insbesondere im Zuge des von der ESG dokumentierten Trends zur beschleunigten Einführung von Cloud-Anwendungen, die das Benutzererlebnis verbessern und die Produktivität steigern sollen. Denn um die angestrebten Vorteile in der Praxis zu realisieren, ist eine leistungsstarke Konnektivitätslösung mit Hochverfügbarkeitsoptionen und kompromissloser Sicherheit erforderlich.

Dementsprechend sind die Verantwortlichen aufgefordert, die Anwendungsbereitstellung ins Zentrum ihrer Netzwerk- und Sicherheitsstrategie zu rücken. Zum einen empfiehlt sich die Anschaffung von Next-Generation-Technologien für die Überwachung der Anwendungsumgebung. Zum anderen sollte die Zusammenführung von Netzwerk- und Sicherheitsbetrieb (und deren Verzahnung mit anderen IT-Prozessen) durch gezielte Investitionen in innovative Lösungen zur Überwindung der Beschränkungen veralteter Infrastrukturen vorangetrieben werden. Flucht- und Endpunkt dieser Modernisierungsroadmap ist die Einrichtung einer robusten SASE-Plattform. Hier bieten Anbieter wie Palo Alto Networks die Möglichkeit, alle Komponenten aus einer Hand zu beziehen, was neben der Integration der Netzwerk- und Sicherheitstechnologien auch die Supportprozesse und das Troubleshooting vereinfacht.

Durch die Kombination von Prisma SD-WAN und Prisma Access erhalten moderne Unternehmen sämtliche Funktionen und Features, die sie zur Optimierung der Netzwerk- und Anwendungsleistung, zur Sicherung verteilter Bereitstellungsinfrastrukturen, zur Umsetzung mobiler Arbeitsmodelle und zur beschleunigten Einrichtung eines SASE benötigen.

Enterprise Strategy Group ist ein Marktforschungsunternehmen, das IT-Analysen, -Studien und -Validierungen durchführt, IT-Strategien entwickelt und der globalen IT-Community aussagekräftige Erkenntnisse bereitstellt.

www.esg-global.com contact@esg-global.com +1 508 482 0188