Partner-Logo hier

ZTNA 2.0: Der neue Standard für die Zugriffssicherung

Schützen Sie Ihre hybride Belegschaft in einer Welt, in der „die Arbeit“ kein Ort, sondern eine Tätigkeit ist.

Table of Contents

Einleitung

Die letzten zwei Jahre haben in jeder Hinsicht radikal verändert, wie und wo wir arbeiten. Bereits begonnene Initiativen zur Unterstützung mobiler Arbeitsweisen, zur intensiveren Nutzung der Cloud und ähnliche mehr wurden plötzlich mit Nachdruck beschleunigt, um den veränderten Umständen Rechnung zu tragen. Inzwischen arbeiten wir in einer Welt, in der wir nicht mehr wie früher „zur Arbeit gehen". Stattdessen ist „die Arbeit" nun eine Tätigkeit, die wir nahezu überall ausüben können.

Dadurch ist die Angriffsfläche exponentiell gewachsen, insbesondere in den zahlreichen Architekturen, die nun Direktverbindungen zu Anwendungen unterstützen, statt den gesamten Datenverkehr über das Rechenzentrum zu leiten.

Ältere Architekturen für den Fernzugriff verkomplizieren die Situation zusätzlich, denn sie gewähren zu umfangreiche Zugriffsrechte und stellen wenig oder keine Funktionalität zur Erkennung von Bedrohungen und Schwachstellen bereit. In einer solchen Umgebung kann ein Hacker sich über ein geknacktes Nutzerkonto Zugang zu zahlreichen vertraulichen Ressourcen verschaffen.

Das ist eine sehr reale Gefahr, denn gleichzeitig ist ein drastischer Anstieg der Zahl und der Raffinesse von Cyberattacken zu beobachten. Ransomwareangreifer waren während der Pandemie besonders aktiv und machten reiche Beute.

Inzwischen besteht kein Zweifel mehr daran, dass die herkömmlichen Ansätze für den sicheren Fernzugriff und veraltete Architekturen wie die ursprüngliche Version von Zero-Trust-Netzwerkzugriff (Zero Trust Network Access, ZTNA) nicht ausreichen, um der Flut immer neuer und immer gefährlicherer Angriffe an allen Punkten der rasant wachsenden Angriffsflächen moderner Unternehmen Einhalt zu gebieten.

Anwendungen, wohin man schaut

80 % der Firmen haben eine Hybrid-Cloud-Strategie.[1]

Firmen nutzen im Schnitt 110 SaaS-Anwendungen.[2]

Die fünf Mängel von ZTNA 1.0

ZTNA-Lösungen der ersten Generation – die wir im Folgenden ZTNA 1.0 nennen werden – wurden vor fast zehn Jahren entwickelt. Seitdem haben sich die Bedrohungslandschaft, Unternehmensnetzwerke und die Art und Weise, wie und wo wir arbeiten, radikal geändert. Infolgedessen sind ZTNA-1.0-Lösungen für die neue Arbeitswelt nicht mehr geeignet und Hacker suchen eifrig nach neuen Methoden, um ihre Unzulänglichkeiten auszunutzen.

Bevor wir die Lücken betrachten, die nun bestehen, sollten wir kurz zurückschauen und uns erinnern, was ursprünglich mit ZTNA 1.0 geschützt werden sollte.

ZTNA 1.0 wurde entwickelt, um die Zahl der von außen erreichbaren Ressourcen – und damit die Angriffsfläche – von Unternehmen zu reduzieren. Es spielt die Rolle eines Zugriffsvermittlers, der die Herstellung einer Verbindung zu einer Anwendung erleichtert. Wenn ein Benutzer auf eine Anwendung zugreifen möchte, prüft dieser Zugriffsvermittler, ob der Zugriff gestattet werden sollte oder nicht. Wenn der Zugriff gestattet wird, gewährt der Zugriffsvermittler ihn und baut eine Verbindung auf.

Und das ist alles. Der Zugriffsvermittler spielt im weiteren Verlauf keine Rolle mehr. Der Benutzer hat uneingeschränkten Zugang zu der Anwendung, ohne zusätzliches Monitoring durch das Sicherheitssystem.

Dies ist das Architekturmodell von ZTNA 1.0. Angesichts der aktuellen Bedrohungslage ist dieses Modell mehr als bedenklich – es ist gefährlich. Im Folgenden betrachten wir fünf Gründe, warum die weitere Nutzung von ZTNA 1.0 mehr Schaden als Nutzen bringen könnte, wenn es um die Abwehr der aktuellen Cyberbedrohungen geht.

Benutzer, wohin man schaut

76 % der Angestellten möchten weiterhin zumindest zeitweise im Homeoffice arbeiten.[3]

1. Verstößt gegen das Least-Privilege-Prinzip

Erstens: ZTNA 1.0 verstößt gegen das Prinzip, nur die unbedingt erforderlichen Zugriffsrechte zu erteilen. Mit „Zero Trust" ist gemeint, dass nichts und niemand als von Haus aus vertrauenswürdig betrachtet wird. Dabei soll das Least-Privilege-Prinzip durchgesetzt werden, indem ein Benutzer mit einer Anwendung – und sonst nichts – verbunden wird.

Tatsächlich sprechen alle Anbieter von ZTNA-1.0-Lösungen sehr überzeugend über genau dieses Prinzip und empfehlen, Zugriff zu einzelnen Anwendungen und nicht zu größeren Netzwerksegmenten zu erteilen. In der Praxis findet das Zugriffsmanagement bei den derzeit verfügbaren ZTNA-1.0-Lösungen jedoch auf den Ebenen 3 und 4 des OSI-Modells – der Netzwerk- und der Transportebene – und ausschließlich aufgrund der Kombination aus IP-Adresse und TCP/UDP-Port statt.

Ein Netzwerk ist nicht dasselbe wie eine Anwendung, aber ZTNA-1.0-Lösungen nutzen Zugriffskontrollen auf Netzwerkebene, um auf Anwendungsebene Zugang zu gewähren. Diese Abhängigkeit von Richtlinien

Ransomware hatte 2021 gravierende Auswirkungen

2021 gab es 518 % mehr Ransomwareangriffe als 2020.[4]

In den USA, Kanada und Europa wurde 171 % mehr Lösegeld gezahlt als 2020.[5]

1. *Flexera 2021 State of the Cloud Report*, 9. März 2021, Flexera, https://www.flexera.com/about-us/press-center/flexera-releases-2021-state-of-the-cloud-report.
2. „Average number of software as a service (SaaS) applications used by organizations worldwide from 2015 to 2021", Statista, 16. Februar 2022, https://www.statista.com/statistics/1233538/average-number-saas-apps-yearly/.
3. *The State of Hybrid Workforce Security 2021*, Palo Alto Networks, 15. August 2021, https://start.paloaltonetworks.com/state-of-hybrid-workforce-security-2021.
4. *Unit 42 Ransomware Threat Report*, Unit 42, 24. März 2022, https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html.
5. Ebd.

auf Ebene 3 und 4 bringt leider eine ganze Reihe von Problemen mit sich. Wenn eine Anwendung beispielsweise dynamische Ports oder IP-Adressen nutzt, müssen Sie ihr Zugang zu einem breiten Spektrum von IP-Adressen und Ports gewähren und Ihre Angriffsfläche damit unnötig vergrößern. Der Zugriff kann auch nicht auf Teile oder einzelne Funktionen von Anwendungen beschränkt, sondern nur für ganze Anwendungen gewährt werden. Zudem kann jede Malware dieselben genehmigten IP-Adressen und Ports nutzen, um ungehindert zu kommunizieren und sich auszubreiten. Fazit: ZTNA 1.0 gewährt weit mehr Zugriff als erforderlich und verstößt damit gegen das Least-Privilege-Prinzip.

2. Folgt dem „Allow-and-Ignore"-Modell

Zweitens: ZTNA-1.0-Lösungen verlassen sich auf das äußerst riskante „Allow-and-Ignore"-Modell.

Warum ist dieses Modell riskant? Nachdem ein Zugriffsvermittler eine Verbindung zwischen einem Benutzer und einer Anwendung hergestellt hat, gilt diese Verbindung bis zum Ende der Sitzung als vertrauenswürdig, ohne dass das Nutzer- oder Geräteverhalten während der Sitzung geprüft wird.

Mit der Annahme, dass die einmal etablierte Vertrauenswürdigkeit nicht wieder geprüft werden muss, sind zukünftige Probleme quasi vorprogrammiert. Nach der Prüfung der Vertrauenswürdigkeit kann viel geschehen. Das Benutzer- oder Anwendungsverhalten kann sich ändern oder Anwendungen können infiltriert werden.

Sicherheitsverstöße sind nur möglich, wenn es jemandem oder etwas erlaubt wird, Verwüstungen oder Schaden anzurichten. Genau deshalb klinken viele aktuelle Cybersicherheitsbedrohungen sich in legitime Aktivitäten ein, um keinen Alarm auszulösen.

3. Keine Sicherheitsprüfungen

ZTNA-1.0-Lösungen vertrauen nicht nur allen und jedem, nachdem ihnen Zugang zum Netzwerk gewährt wurde, sondern verzichten auch darauf, den Anwendungsdatenverkehr zu inspizieren. Sobald eine Verbindung etabliert ist, vertraut ZTNA 1.0 der aktiven Sitzung implizit und prüft ihren Datenverkehr daher nicht. Wenn das Gerät infiltriert und Malware in die Sitzung eingeschleust wird, ist eine ZTNA-1.0-Lösung daher nicht in der Lage, schädlichen oder kompromittierten Datenverkehr zu erkennen und angemessen zu reagieren. Damit wird ZTNA 1.0 zu einem „Security-through-Obscurity-only"-Ansatz, bei dem nur die Unbekanntheit einer Verbindung ein gewisses Maß an Sicherheit bietet. Für Unternehmen bedeutet das, dass ihre Benutzer, Anwendungen und Daten durch Malware, infiltrierte Geräte und schädlichen Datenverkehr gefährdet sind.

4. Keine Datensicherheit

Viertens bieten ZTNA-1.0-Lösungen keinerlei Datensicherheit, insbesondere für Daten in privaten Anwendungen. Infolgedessen kann der größte Teil des Datenverkehrs in Unternehmen potenziell durch böswillige Insider oder externe Angreifer ausgeschleust werden. Um dies zu verhindern und sensible Daten in SaaS-Anwendungen zu schützen, sind separate Lösungen zum Schutz vor Datenverlust (Data Loss Prevention, DLP) erforderlich. ZTNA 1.0 steigert somit die Komplexität und das Risiko, da Unternehmen mehrere Punktlösungen implementieren müssen, um all ihre Daten zu schützen.

5. Schützt nicht alle Anwendungen

Fünftens decken ZTNA-1.0-Lösungen nicht alle Anwendungen ab. Cloudbasierte Anwendungen und andere Anwendungen, die dynamische Ports nutzen, sowie vom Server gestartete Anwendungen werden beispielsweise nicht unterstützt. Das ist für Supportteams relevant, da ihre Help-Desk-Mitarbeiter oft mit Anwendungen arbeiten, die vom Server aufgebaute Verbindungen zu Remotegeräten nutzen. Auch SaaS-Anwendungen werden von ZTNA 1.0 nicht unterstützt.

Moderne cloudnative Anwendungen bestehen aus zahlreichen Containern mit Microservices, die oft dynamische IP-Adressen und Ports nutzen. Damit ist die Katastrophe vorprogrammiert. In Umgebungen dieser Art ist die von ZTNA 1.0 gebotene Zugangskontrolle völlig unzureichend. Anwendungen müssten Zugang zu einem großen Bereich von IP-Adressen und Ports erhalten, womit alle Zero-Trust-Bemühungen zunichte gemacht würden.

Je mehr Unternehmen die Migration in die Cloud vorantreiben und cloudnative Anwendungen nutzen, desto hinfälliger wird ZTNA 1.0.

ZTNA 2.0: ein Neubeginn

Wir haben die digitale Transformation beobachtet, die in Unternehmen im Gange ist, um die Effizienz zu steigern und den Mitarbeitern Zugang zu sämtlichen Tools zu bieten, die sie benötigen – unabhängig davon, wo sie arbeiten.

Am deutlichsten ist diese Transformation in der Art und Weise sichtbar, wie Mitarbeiter auf diese Tools zugreifen, denn sie stellen nun direkte Verbindungen zu den Anwendungen her, die sie zur Erledigung ihrer Aufgaben benötigen. Dabei sollte es keine Rolle spielen, ob sie zu Hause, unterwegs oder in einem Büro sind. Alle Mitarbeiter sollten Zugang zu sämtlichen Anwendungen haben, die sie für ihre Arbeit benötigen, ohne dass die Angriffsfläche des Unternehmens dadurch wächst.

Diese Transformation erfordert einen Paradigmenwechsel in der Cybersicherheit. Dieser Paradigmenwechsel ist ZTNA 2.0.

Die fünf Grundprinzipien von ZTNA 2.0

ZTNA 2.0 beruht auf fünf Grundprinzipien.

1. ZTNA 2.0 setzt das Least-Privilege-Prinzip auf die strengste Art und Weise durch und bietet Zugangskontrollen von der Netzwerkebene (Layer 3) bis hin zur Anwendungsebene (Layer 7).
2. ZTNA 2.0 prüft die Vertrauenswürdigkeit kontinuierlich. Wenn das Verhalten eines Benutzers, einer Anwendung oder eines Geräts sich ändert, kann nur die kontinuierliche Neubewertung des gewährten Vertrauensniveaus dafür sorgen, dass jede Veränderung in Echtzeit erkannt und angemessen berücksichtigt wird.
3. ZTNA 2.0 inspiziert den gesamten Datenverkehr lückenlos, um Unternehmen vor allen Bedrohungen auf allen Angriffsvektoren zu schützen.
4. ZTNA 2.0 schützt alle Daten sämtlicher Anwendungen – von den Daten, die in Anwendungen auf alten Mainframes genutzt werden, bis hin zu den Daten, die in modernen, cloudnativen und Kollaborationsanwendungen gespeichert sind.
5. ZTNA 2.0 schützt und sichert alle Anwendungen in Ihrem gesamten Unternehmen, darunter auch private Apps, Cloud- und SaaS-Anwendungen.

Mit diesen fünf entscheidenden Fähigkeiten überwindet ZTNA 2.0 die Leistungsgrenzen von ZTNA 1.0, stärkt die Sicherheit, unterstützt die digitale Transformation und erfüllt die Anforderungen moderner, hybrider Belegschaften. Sehen wir uns nun jedes der fünf Grundprinzipien im Detail an.

1. Rechtevergabe gemäß dem Least-Privilege-Prinzip

Bei Palo Alto Networks haben wir App-ID™, User-ID™ und Device-ID™ erfunden, die alle reichhaltige Kontextinformationen und eine nuanciertere Zuweisung von Zugriffsrechten zu Anwendungen bieten. Doch ZTNA 2.0 funktioniert nicht nach dem Motto „einmal getan, für immer erledigt“. Wir beschränken uns nicht auf die Prüfung von Benutzer-IDs und deren Interaktionen mit FQDNs oder IP-Adressen und Ports.

ZTNA 2.0 erfordert auch App-ID-Kapazitäten für den statusbehafteten Betrieb. Das bedeutet, dass wir kontinuierlich Informationen über die Transmission-Control-Protocol-(TCP-)Sitzung, die Anwendungs-Handshakes, das Anwendungsverhalten, die statusbehafteten Protokolle und mehr erfassen. Gleichzeitig sammeln die User-ID- und Device-ID-Steuerungen kontinuierlich Daten über Benutzer und deren Geräte.

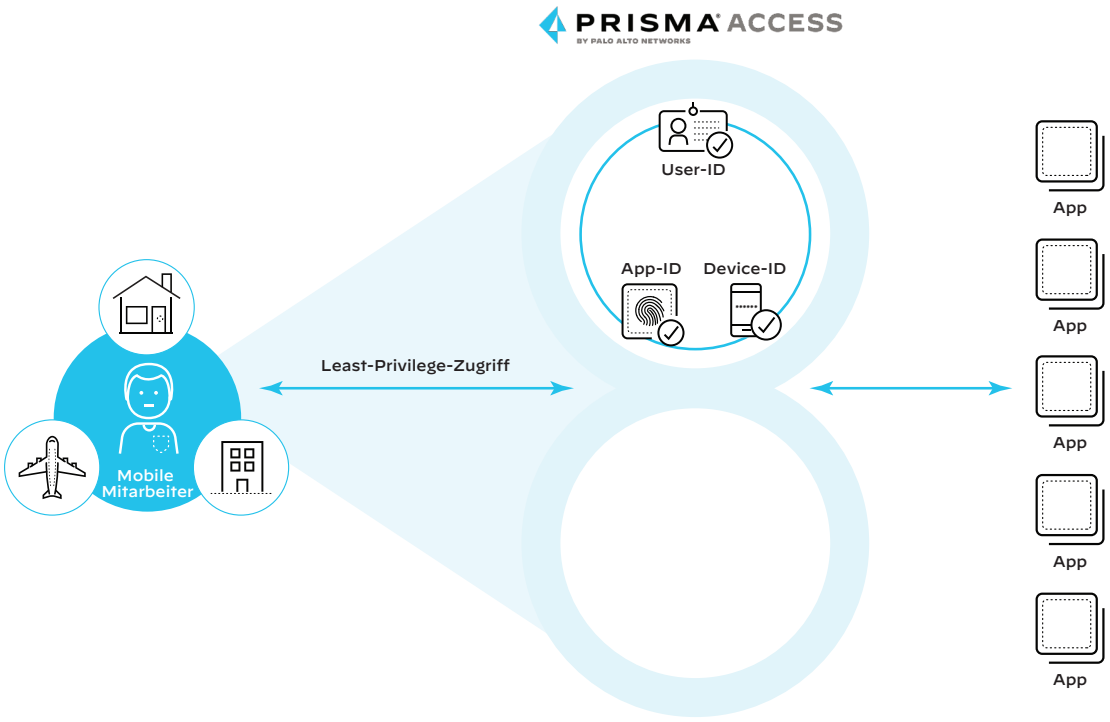

Abbildung 1: Palo Alto Networks nutzt App-ID, User-ID und Device-ID, um die lückenlose Durchsetzung des Least-Privilege-Prinzips zu unterstützen.

Wenn Sie App-ID-, User-ID- und Device-ID-Zugriffskontrollen miteinander kombinieren, gehen Sie über einfache Prüfungen der derzeitigen Vertrauenswürdigkeit hinaus und schaffen eine Umgebung, die reichhaltige Kontextinformationen für eine fundiertere Entscheidungsfindung bietet. Unternehmen können beliebigen Benutzern, die über beliebige Geräte auf eine bestimmte Anwendung zugreifen wollen, Zugang gewähren und kontinuierlich weitere Kontextinformationen sammeln, um in Echtzeit auf etwaige Veränderungen zu reagieren.

2. Kontinuierliche Prüfung der Vertrauenswürdigkeit

Prisma Access prüft die Vertrauenswürdigkeit ununterbrochen weiter, nachdem Zugang zu einer Anwendung gewährt wurde. Die Funktionen zur kontinuierlichen Prüfung der Vertrauenswürdigkeit beobachten und überprüfen nicht nur das Geräte-, sondern auch das Benutzer- und Anwendungsverhalten und alle etwaigen Änderungen darin ununterbrochen, um bei Bedarf in Echtzeit zu reagieren.

Das Kernprinzip von Zero Trust ist, nichts und niemandem implizit zu vertrauen. Wenn die Vertrauenswürdigkeit nicht kontinuierlich überprüft wird, geht man hingegen de facto davon aus, dass das Verhalten von Benutzer und Anwendung stets vertrauenswürdig bleibt, nachdem eine Verbindung zwischen ihnen hergestellt wurde. Doch wir wissen, dass nach der Prüfung der Vertrauenswürdigkeit viel geschehen kann. Benutzer und Anwendungen können ihr Verhalten ändern oder kompromittiert werden.

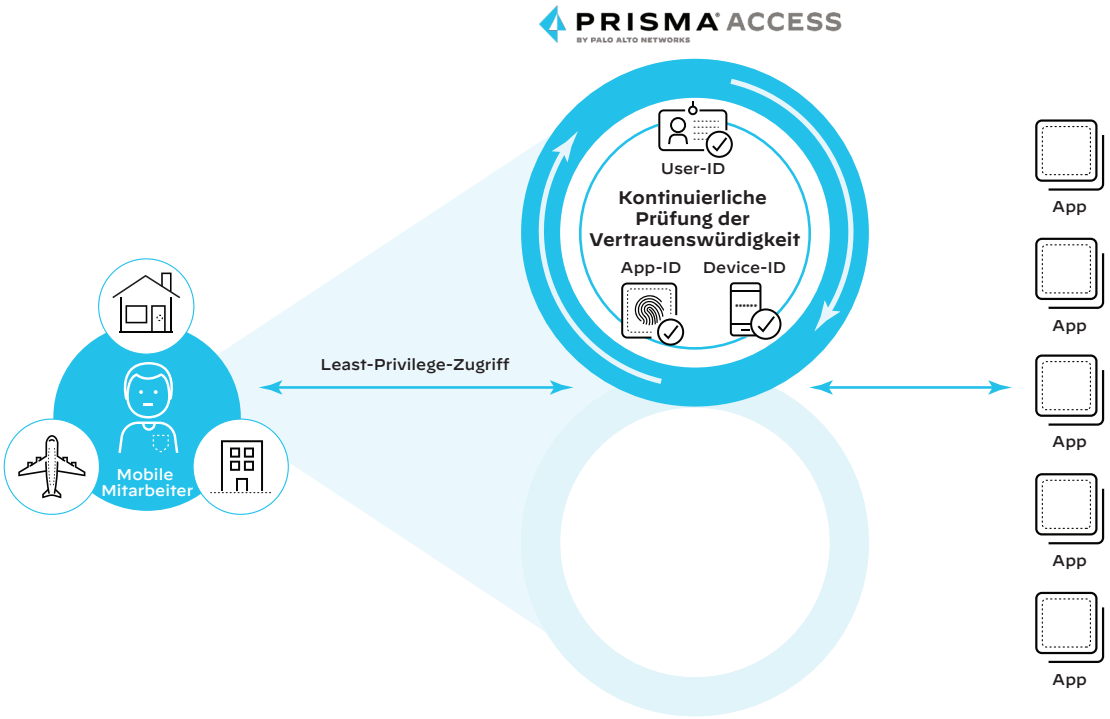

Abbildung 2: Zur kontinuierlichen Prüfung der Vertrauenswürdigkeit werden die Gerätesicherheit sowie das Anwendungs- und Benutzerverhalten ununterbrochen weiter überwacht, auch nachdem einem Benutzer Zugriff zu einer Anwendung gewährt wurde.

3. Kontinuierliche Sicherheitsprüfung

Prisma Access sorgt mit WildFire® und Features wie Advanced URL Filtering, Threat Prevention, SaaS Security und DNS Security für kontinuierliche Sicherheitsprüfungen. Darüber hinaus führen wir tiefgreifende und lückenlose Sicherheitsinspektionen durch, die auch die genehmigten Verbindungen und die Suche nach Zero-Day-Bedrohungen einschließen. Mit unseren KI- und ML-basierten Technologien für die Bedrohungsprävention stoppen wir 95 Prozent der Zero-Day-Bedrohungen inline. Das bedeutet, dass wir nicht warten müssen, bis ein erstes Unternehmen angegriffen oder eine Signatur erstellt wurde, bevor wir Ihre Umgebung schützen können.

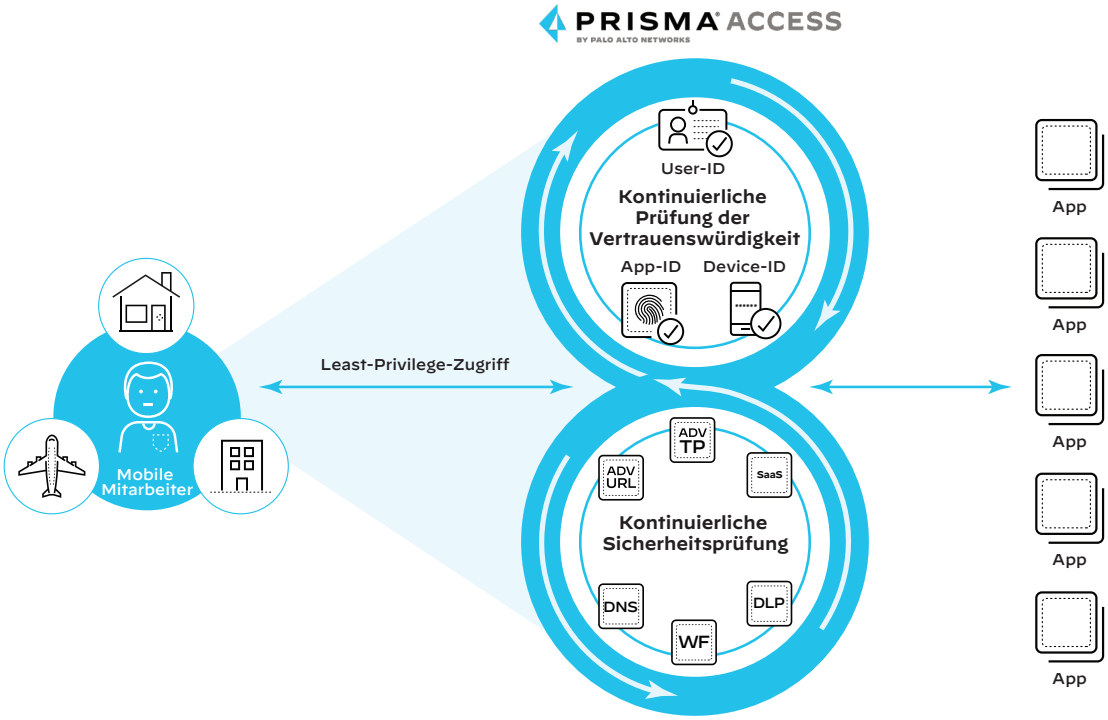

Abbildung 3: Die kontinuierliche Sicherheitsprüfung schützt Ihre Umgebung vor Bedrohungen.

4. Konsistenter Schutz aller Daten

Prisma Access wendet seine modernen DLP-Kapazitäten konsistent auf alle Anwendungsdaten an. Das bedeutet, dass wir dieselben Richtlinien für Daten in privaten und SaaS-Anwendungen durchsetzen und dass Sie nicht raten müssen, welche Anwendungen geschützt und welche Daten sicher sind. Stattdessen können Unternehmen von einer einzigen Lösung aus für starke Datensicherheit und einheitliche Sicherheitsrichtlinien für all ihre Anwendungen sorgen.

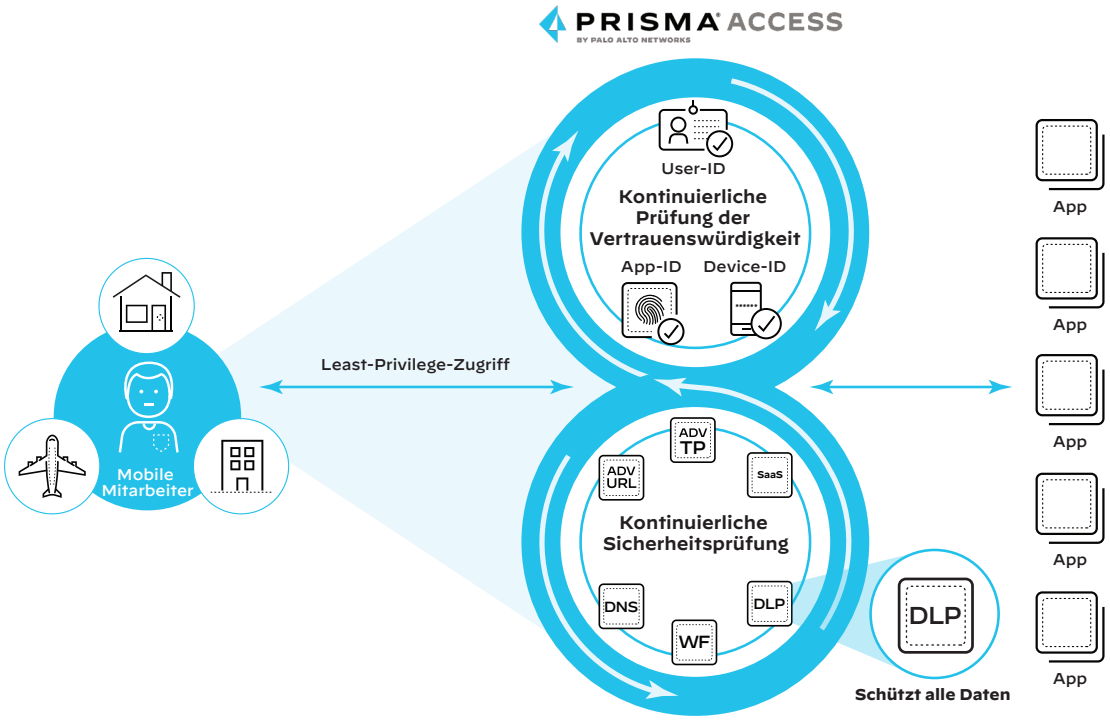

Abbildung 4: Konsistente Datensicherheit sorgt unternehmensweit für einheitlich starke Datensicherheit und Sicherheitsrichtlinien.

5. Konsistente Sicherheit für alle Anwendungen

Prisma Access bietet konsistente Sicherheit für all Ihre Anwendungen, unternehmensweit. Dazu müssen Sie nicht einschränken, welche IP-Adressen und Ports Ihre modernen, cloudnativen, auf Microservices basierten Anwendungen nutzen und SaaS-Anwendungen sind genauso gut geschützt wie konventionelle private oder ältere Anwendungen.

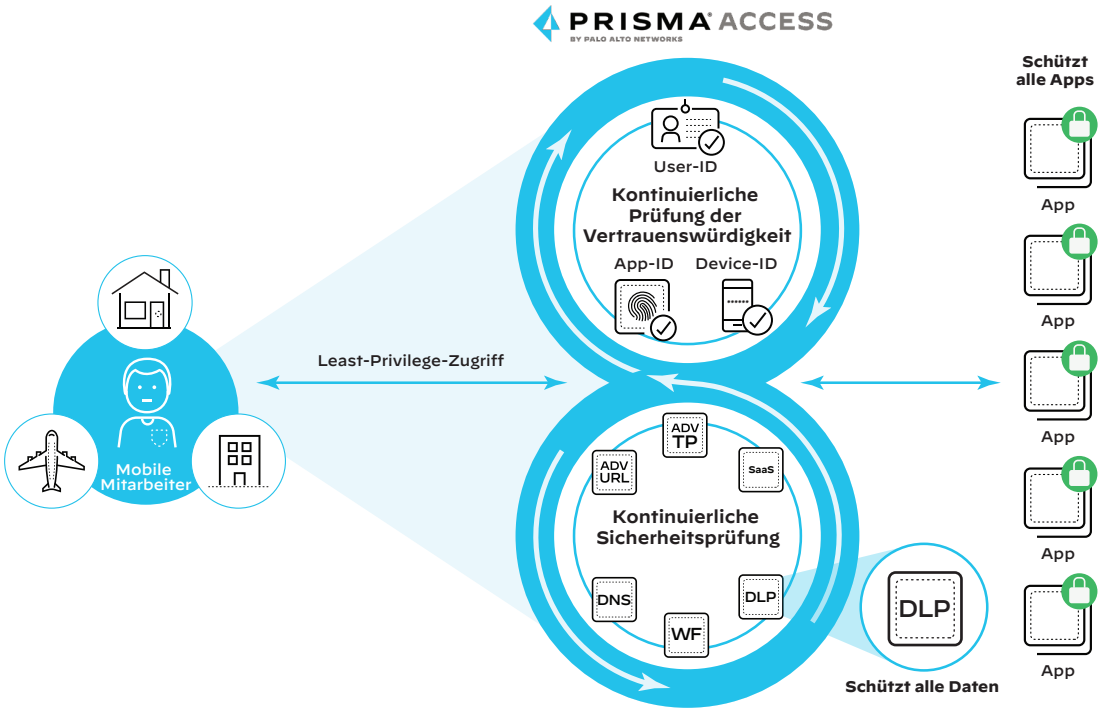

Abbildung 5: Ob herkömmliche, private oder cloudnative Anwendungen – wir bieten dasselbe hohe Sicherheitsniveau für alle.

Prisma Access: die Engine hinter ZTNA 2.0

Prisma® Access stellt die branchenweit erste cloudbasierte ZTNA-2.0-Lösung bereit, die als leicht verwaltbare, einheitliche Sicherheitslösung mit hervorragender Benutzererfahrung entwickelt wurde. Prisma Access vereint als derzeit einziges Produkt branchenführende Features wie ZTNA 2.0, SWG, Next-Generation CASB, FWaaS, DLP und andere mehr in einem cloudnativen globalen Service-Edge, das:

- Alle Benutzer und alle Anwendungen sicher mit **feinkörnigen Zugriffskontrollen** verbindet und so die Angriffsfläche erheblich reduziert
- Die **Vertrauenswürdigkeit verhaltensbasiert kontinuierlich weiter prüft**, wenn die Benutzer mit der Anwendung verbunden sind
- **Tiefgreifende, lückenlose Sicherheitsinspektionen** durchführt, um ohne Beeinträchtigung der Leistung oder der Benutzererfahrung dafür zu sorgen, dass der gesamte Traffic sicher ist
- Mit einer einheitlichen DLP-Richtlinie **sowohl Zugriffe als auch Daten schützt** und dabei für Transparenz sorgt
- Mit einem Produkt **alle Anwendungen ununterbrochen schützt** – On-Premises, im Internet, in älteren Systemen sowie in SaaS- und anderen modernen, cloudnativen Umgebungen

Die einzigartige Architektur von Prisma Access wurde speziell für Cloud-Umgebungen konzipiert und ist daher von Haus aus extrem skalierbar sowie mandantenfähig und isoliert Kunden zuverlässig voneinander.

Prisma Access nutzt die elastische Skalierbarkeit der größten Cloud-Anbieter der Welt und Zugang zu dedizierten Premium-Glasfasernetzen, um branchenführende SLAs für Sicherheitsprozesse und Anwendungsleistung anzubieten.

Gleichzeitig werden potenzielle Probleme durch natives autonomes Management der digitalen Benutzererfahrung proaktiv identifiziert und behoben, bevor die Benutzer sie bemerken. Gemeinsam sorgen diese Features für die **bestmögliche Leistung und Benutzererfahrung**.

Drei Startpunkte für den Wechsel zu ZTNA 2.0 in Ihrem Unternehmen

Der Einstieg in ZTNA 2.0 sollte weder schwierig oder überwältigend sein noch Kompromisse erfordern. Der entscheidende Punkt ist die Ausrichtung – die Abstimmung der Anforderungen auf die wichtigsten Bedenken oder Herausforderungen der meisten Unternehmen, damit diese sich mit der Lösung bewältigen lassen, ohne dass die ganze Architektur umgebaut und/oder der Geschäftsbetrieb gestört werden muss.

Im Folgenden stellen wir drei Beispielprojekte vor, mit denen Sie die Implementierung von ZTNA 2.0 in Ihrem Unternehmen sofort beginnen können:

- **Projekt zur Ablösung von VPN**: Verabschieden Sie sich von VPN-Konzentratoren, leistungsschwachen Architekturen mit zu viel Umleitung, ineffizienten Netzwerkpfaden und anderen Infrastrukturen mit hohem Administrationsaufwand.
- ***Projekt zur Ablösung von SWG***: Gehen Sie von standort- und proxybasierten Architekturen zu einem modernen, cloudbasierten Ansatz über, um Ihren Benutzern sicheren Zugang zu webbasierten und Internettools zu gewähren.
- **Projekt für moderne SaaS-Anwendungssicherheit oder einen Next-Generation CASB**: Modernisieren Sie die Sicherung der explosionsartig steigenden Anzahl genutzter SaaS-Anwendungen und bringen Sie sie – und den Rest der Schatten-IT – unter Kontrolle, reduzieren Sie die Angriffsfläche und stärken Sie den Schutz Ihrer sensiblen Daten.

Startpunkt 1: Projekt zur Ablösung von VPN

Ersetzen Sie veraltete VPN-Technologie für den Netzwerkzugriff Ihrer Remote- und Hybridbelegschaft durch eine modernere ZTNA-2.0-Lösung, die Leistungsengpässe beseitigt und die Verwaltung vereinfacht.

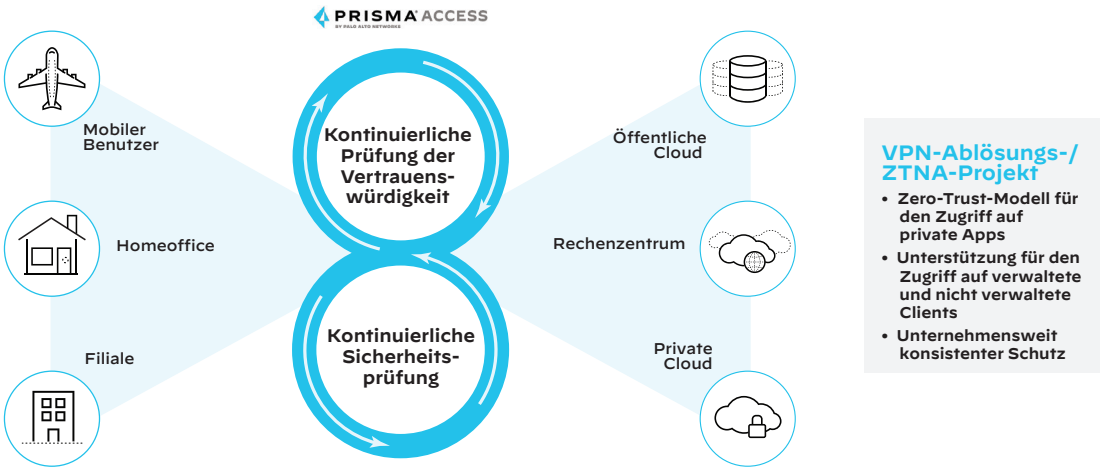

Abbildung 6: ZTNA 2.0 eliminiert die Herausforderungen, die der Schutz von mobilen und Remotearbeitern mithilfe von VPN mit sich bringt.

Projekte zur Ablösung von VPN können durch verschiedene Faktoren ausgelöst werden:

- Anwendungen sollen auf ein echtes Hybridmodell umgestellt werden, um On-Premises-, Cloud- und Multi-Cloud-Umgebungen optimal zu nutzen. Die mangelnde Skalierbarkeit älterer VPN-Technologie, die den Traffic über einen „Konzentrator“ auf dem Firmengelände umleitet oder sogar mehrfach hin- und herschickt, kann die Benutzererfahrung in diesem neuen Modell erheblich beeinträchtigen.
- Die Anforderungen für den Zugriff auf Unternehmensanwendungen haben sich geändert. Früher nutzten Mitarbeiter von Unternehmen verwaltete Geräte, um ihre Arbeit zu erledigen. Heute werden jedoch mehr und mehr nicht verwaltete Geräte mit dem Unternehmensnetzwerk verbunden und zum Zugriff auf Unternehmensanwendungen genutzt.
- Unternehmen streben ein konsistentes Sicherungs- und Sicherheitsmodell an, das alle Anwendungen (und nicht nur die webbasierten oder die älteren Anwendungen) abdeckt.

Es gibt zwar eine Reihe von Lösungen, die einige dieser Anforderungen erfüllen, aber nur ZTNA 2.0 mit Prisma Access bietet die erforderliche Netzwerk- und Sicherheitsfunktionalität zur Unterstützung verwalteter und nicht verwalteter Geräte mit unternehmensweit einheitlicher Sicherheit.

Ablösung von VPN zum Schutz Tausender Mitarbeiter weltweit

Mit Prisma Access stellt dieser Kunde nun konsistente Konnektivität für 350.000 Benutzer in 158 Ländern und direkten Internetzugang für Hunderte von Filialen rund um den Erdball bereit. Darüber hinaus sorgt Prisma Access für zuverlässigen und sicheren Zugriff auf alle Anwendungen, einschließlich der älteren Anwendungen, in über 30 Rechenzentren und Cloud-Umgebungen.

- Hauptsächlich entschied dieses Fortune 100-Beratungsunternehmen sich für Prisma Access, um eine alternde, heterogene und nicht skalierbare VPN-Lösung zu ersetzen, über die Remotearbeiter und -standorte auf Unternehmensressourcen zugriffen.
- Da diese VPN-Lösung aus Komponenten von unterschiedlichen Anbietern zusammengesetzt worden war, war es kaum möglich, ein einheitliches Transparenz- und Sicherheitsniveau für die zahlreichen Mitarbeiter und Standorte in aller Welt zu erreichen.
- Auch die Mitarbeiter waren mit der Lösung unzufrieden, da der Verbindungsaufbau zu lange dauerte, die Leistung stark schwankte und das Benutzererlebnis von Filiale zu Filiale und Ort zu Ort sehr unterschiedlich war.

Startpunkt 2: Ablösung von SWG

Viele Unternehmen wollen die Mitarbeitererfahrung beim Zugriff auf Webanwendungen verbessern. Prisma Access versucht gar nicht erst, die Latenz zu reduzieren, die durch die Umleitung des Webtraffics über ein Unternehmensrechenzentrum vor der Bereitstellung der Inhalte am aktuellen Benutzerstandort entsteht. Stattdessen eliminiert ein Cloud-SWG diese Latenz und stärkt gleichzeitig die Sicherheit.

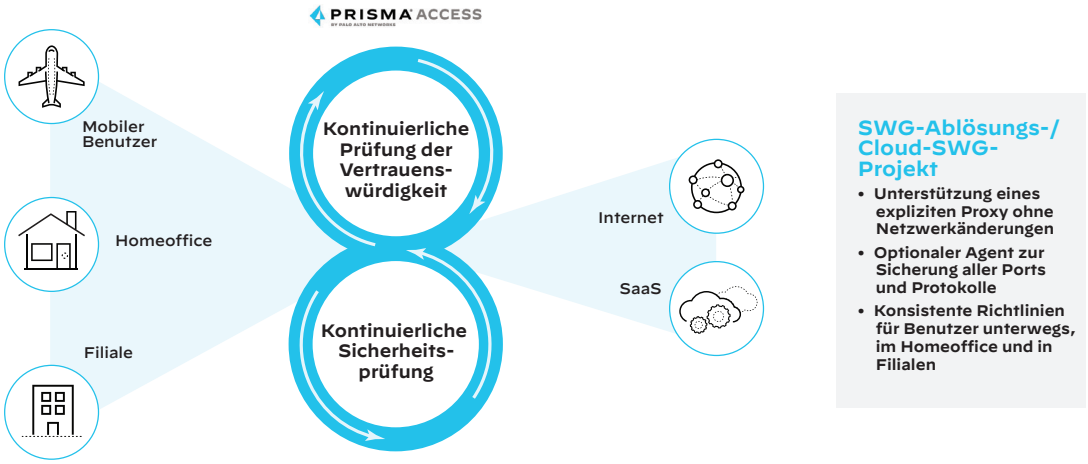

Abbildung 7: ZTNA 2.0 mit Prisma Access eliminiert die Latenz, die Benutzer herkömmlicher SWG-Lösungen so frustrierend finden.

Prisma Access gestaltet die Umstellung zu ZTNA 2.0 zukunftssicher. Ein Unternehmen kann jederzeit Agenten zum Schutz sämtlicher Ports, Protokolle und Anwendungen implementieren. Prisma Access:

- Bietet mehrere Verbindungsmethoden zur Implementierung von SWG für alle hybriden Benutzer und Zweigstellen, darunter explizite Proxys, Agenten und clientlose Varianten.
- Erleichtert Unternehmen den Übergang von herkömmlichen Proxys zu cloudbasiertem sicheren Zugang ohne Netzwerkänderungen, nur mit einer Aktualisierung der vorhandenen PAC-Dateien.
- Kann mit Prisma SD-WAN integriert werden, um einen reibungslosen Einstieg in Prisma Access zu ermöglichen und ein einheitliches Sicherheitsniveau für alle Filialen zu erreichen.

Migration von On-Premises- zu cloudnativer Sicherheit

Als ein immer größerer Teil der Tools und Anwendungen, die die Mitarbeiter für ihre Arbeit benötigten, in die Cloud verlagert wurde, waren die vorhandenen Lösungen immer weniger in der Lage, den reibungslosen Zugriff zu gewährleisten, den die Benutzer erwarteten. Infolgedessen sank die Benutzerzufriedenheit mit diesen Lösungen.

Cloudbasierte Sicherheitsdienste sollten den Umfang der heterogenen On-Premises-Hardwareinfrastruktur dieses Fortune 100-Pharmaunternehmens reduzieren und seine Infrastruktur modernisieren.

Man entschied sich für Prisma Access, um alle 100.000 Benutzer mithilfe der Proxy-Kapazitäten innerhalb von drei Monaten zu migrieren, ohne die Netzwerkarchitektur zu ändern.

Die neue cloudnative Lösung konsolidierte und ersetzte die On-Premises-Proxys und verbesserte das Sicherheitsniveau für alle Benutzer und Standorte. Darüber hinaus implementierte das Unternehmen das native autonome Management der digitalen Benutzererfahrung (ADEM) von Prisma Access, um allen Hybridmitarbeitern eine konsistent hervorragende Benutzererfahrung zu bieten.

Startpunkt 3: Projekt zur zeitgemäßen Sicherung von SaaS-Anwendungen

Die Next-Generation-CASB-Funktionen in Prisma Access sorgen für eine vollständige Abdeckung und Sicherung sämtlicher Anwendungen, On-Premises und in der Cloud. Zudem erhalten Unternehmen eine umfassende Übersicht über ihre „Schatten-IT“ und benutzerfreundliche Arbeitsabläufe für die sichere Nutzung von SaaS-Anwendungen, damit sie mit der explosionsartig steigenden Zahl der genutzten SaaS-Anwendungen Schritt halten können.

Prisma Access bietet die branchenweit größte Abdeckung für den API-basierten Schutz genehmigter SaaS- und Kollaborationsanwendungen.

Mit modernen DLP-Funktionen für private und öffentlich zugängliche Anwendungen bietet Prisma Access Next-Generation CASB dasselbe Datensicherheitsniveau für SaaS-Umgebungen, Netzwerke, Filialen und hybride Belegschaften. Zudem unterstützt es die Problembehebung durch die Benutzer und das Incident-Response-Management.

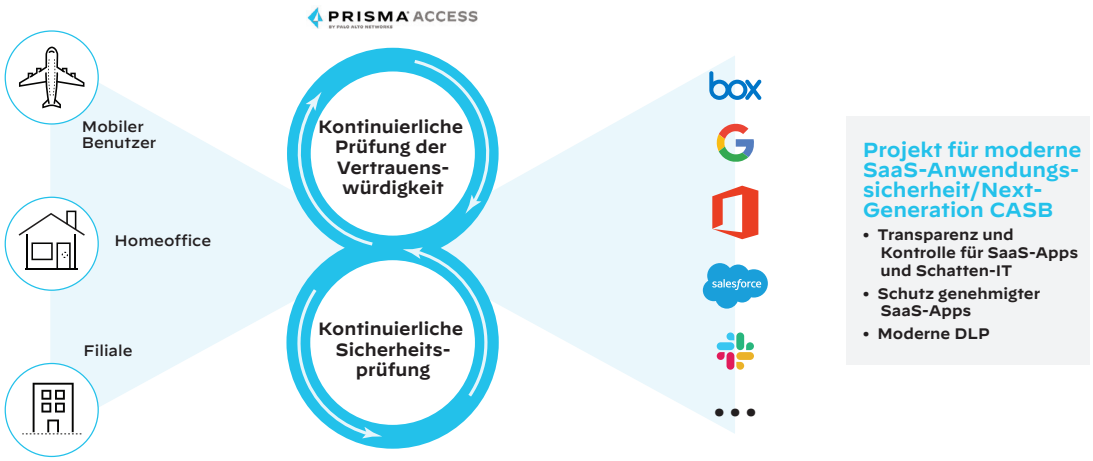

Abbildung 8: Die Next-Generation-CASB-Funktionen in Prisma Access schützen sämtliche Anwendungen, On-Premises und in der Cloud.

Moderne Transparenz, Kontrolle und Datensicherheit für SaaS-Anwendungen

Ein weltweit führender Autohersteller mit über 180.000 Mitarbeitern in 124 Fabriken und 12 großen Technologiezentren weltweit, der in 44 Ländern am Markt präsent ist, nutzte eine stetig steigende Zahl von Cloud-Anwendungen. Das Unternehmen benötigte eine bessere Übersicht und feinkörnigere Kontrolle über seine bekannten und unbekannten SaaS-Anwendungen, ein einheitliches Management für die diversen Produkte verschiedener Anbieter, die im Einsatz waren, sowie Funktionen für die Bedrohungssuche.

Außerdem sollten die Erstellung und Implementierung von Richtlinien vereinfacht werden und ohne Proxys oder Agenten möglich sein. Die Synchronisierung von Risiken, Richtlinien und Zielen in einer eigenen Stackebene sollte ebenfalls abgelöst werden. Dank der Next-Generation-CASB-Funktionen in Prisma Access müssen nun keine Agenten für Inline-Inspektionen und den Schutz nicht verwalteter Endpunkte mehr konfiguriert und aktualisiert werden.

Fazit

Angesichts der fünf erheblichen Mängel von ZTNA 1.0 fragen Sie sich vielleicht, wie dieser Ansatz sich auf dem Markt behaupten konnte. ZTNA 1.0 war eine gute Lösung für die Herausforderungen rund um die Cybersicherheit, mit denen Unternehmen bis vor wenigen Jahren konfrontiert waren. Seitdem hat die Bedrohungslage sich jedoch weiterentwickelt und zugespitzt. Zudem haben hybride Netzwerkumgebungen und die steigende Anzahl der Mitarbeiter, die von außerhalb der gut geschützten Unternehmensgelände auf sie zugreifen, die Angriffsfläche von Unternehmen explosionsartig vergrößert.

Mit ZTNA 2.0 beginnt eine neue Ära des sicheren Zugriffs in einer Welt, in der mit „Arbeit“ nicht wie früher ein Ort, sondern eine Tätigkeit gemeint ist. Prisma Access ist die branchenweit einzige ZTNA-2.0-Sicherheitslösung, die in einem einfachen, einheitlichen Produkt bereitgestellt wird, das speziell für den erfolgreichen Übergang zu ZTNA 2.0 entwickelt wurde.

paloalto NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de

parent_wp_ztna-2.0:-the-new-standard-for-securing-access_051022