Zero Trust für Public-Cloud-Umgebungen

Virtuelle Firewalls als zentrale Komponente einer mehrschichtigen Sicherheitsinfrastruktur

paloalto NETWORKS | STRATA BY PALO ALTO NETWORKS

Inhaltsverzeichnis

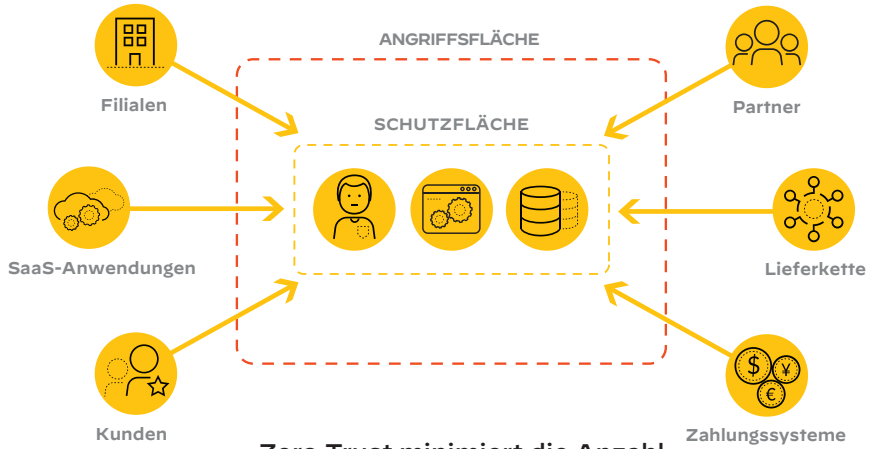
Niemandem vertrauen, alles verifizieren

Das alte Sprichwort „Vertrauen ist gut, Kontrolle ist besser!“ wurde durch den US-Präsidenten Ronald Reagan bekannt, als dieser es im Dezember 1987 anlässlich der Unterzeichnung des Washingtoner Vertrags über nukleare Mittelstreckensysteme in einer Ansprache an Michail Gorbatschow zitierte. Allerdings scheint diese Redensart einen gewissen Widerspruch zu enthalten: Wenn jemand unser Vertrauen verdient, wozu bedarf es da der Kontrolle?

Und tatsächlich basierte das fragliche Vertragswerk eigentlich auf dem Grundsatz „Niemandem vertrauen, alles verifizieren“, der heute das Fundament des Zero-Trust-Ansatzes in der Cybersicherheit bildet. In der Praxis bedeutet das, dass ein Benutzer oder Gerät in einer Zero-Trust-Architektur nicht primär anhand seines Standorts als vertrauenswürdig eingestuft wird. Stattdessen gilt jedes Gerät, jeder Benutzer, jede Anwendung und jeder Datenstrom im Netzwerk bis zur erfolgreichen Authentifizierung und Autorisierung als potenzielle Bedrohung.[1]

Somit stellt das Aufkommen von Zero Trust eine Zäsur im Bereich Cybersicherheit dar. Der Ansatz unterscheidet sich deutlich von älteren Sicherheitsstrategien, bei denen die **Angriffsfläche** im Mittelpunkt stand – also die Gesamtheit aller Geräte und Verbindungen, die Hacker potenziell ausnutzen könnten, um die bestehenden Abwehrmaßnahmen im Netzwerk zu umgehen.

Zero Trust betrachtet das Problem aus dem entgegengesetzten Blickwinkel und konzentriert sich auf die **Schutzfläche**, das heißt auf jene Daten, Anwendungen, Assets und Services, die geschützt werden müssen. Das hat unter anderem den Vorteil, dass die Schutzfläche deutlich einfacher eingegrenzt und bestimmt werden kann, da sie wesentlich kleiner als die Angriffsfläche ist.



Zero Trust minimiert die Anzahl potenzieller Einfallstore für Angreifer

Um nun nachvollziehen zu können, was Zero Trust für die Cloud bedeutet, müssen wir zunächst die drei gängigsten Varianten der Public Cloud unterscheiden.

Die drei wichtigsten Varianten der Public Cloud

Auch wenn wir meist so über die Cloud sprechen, als wäre sie ein klar definiertes Ding, entspricht das bei genauerem Hinsehen nicht der Realität. Denn „Public Cloud“ ist ein Sammelbegriff, der drei verschiedene Modelle umfasst: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS).

Software-as-a-Service (SaaS)

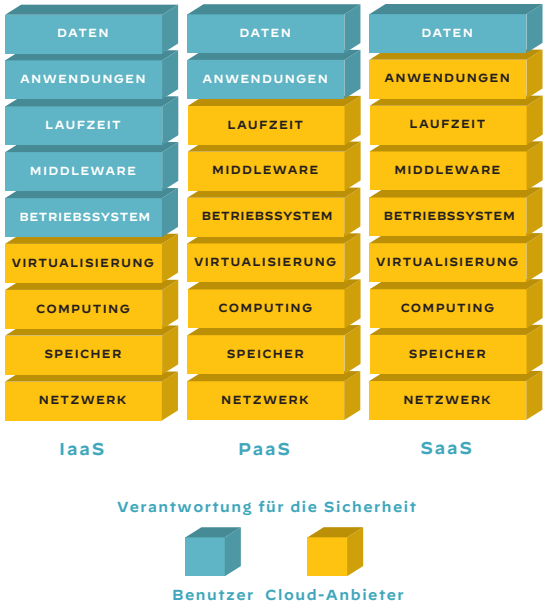
Die meisten Mitarbeiter moderner Unternehmen haben bereits Erfahrung mit der Nutzung von SaaS-Anwendungen wie Salesforce CRM, Adobe Creative Cloud, Google Docs und Microsoft Windows 365. Bei dieser Art von Public-Cloud-Service ist der Kunde Eigentümer der in der Cloud gespeicherten und verarbeiteten Daten, während der Cloud-Serviceanbieter (CSP) für alle anderen Aspekte – von der Netzwerkanbindung bis zur Integrität der bereitgestellten Apps – verantwortlich zeichnet.

Platform-as-a-Service (PaaS)

PaaS wird vor allem von Softwareentwicklern genutzt, weil der Kunde hier Eigentümer der Daten und der Anwendungen ist. Zu den beliebtesten PaaS-Angeboten zählen AWS Elastic Beanstalk, Windows Azure, Google App Engine und Red Hat OpenShift.

Infrastructure-as-a-Service (IaaS)

IaaS ist mittlerweile das bei Weitem gängigste Public-Cloud-Modell, das von Großkonzernen wie AWS, Microsoft Azure, Google Cloud und Alibaba angeboten wird. Hier stellt der Anbieter die Netzwerkanbindung, Speicherkapazitäten und Rechenleistung bereit, während der Kunde die Einrichtung und Pflege des Betriebssystems sowie der Middleware, Laufzeitumgebungen, Anwendungen und Datenbanken übernimmt.



Sicherheitsmodelle für die drei Arten von Public-Cloud-Services

Der Schutz der Public Cloud wird dadurch kompliziert, dass Kunden und Anbieter gemeinsam für die Sicherheit verantwortlich sind – wie im nächsten Abschnitt deutlich wird.

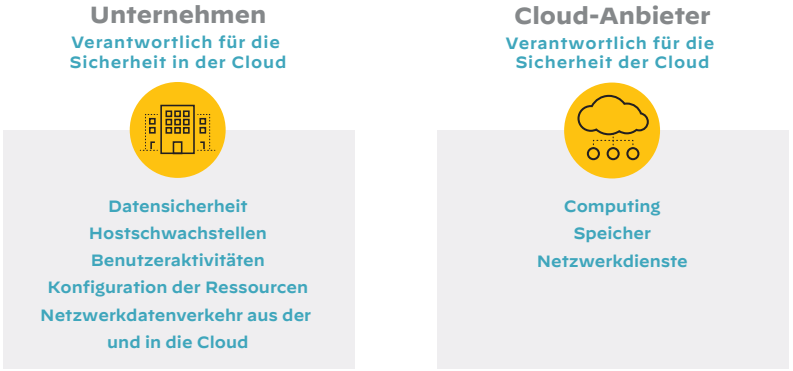
Das Modell der gemeinsamen Verantwortung

Wenn Sie eine private Cloud in ihrer eigenen Infrastruktur bereitstellen, ist Ihr Unternehmen der Eigentümer des gesamten Stacks – von der Hardware bis hin zu den Anwendungen und Daten. Daher gibt es bei diesem Modell auch keine Unklarheiten bezüglich der Sicherheit: Verantwortlich sind ausschließlich Sie und Ihr Team.

Etwas komplizierter gestaltet sich die Sache jedoch in der Public Cloud, wo die sicherheitsbezogenen Zuständigkeiten durch das Modell der gemeinsamen Verantwortung geregelt sind. Hier ist der Cloud-Anbieter für die Sicherung der Plattform verantwortlich, das heißt für sämtliche Hardware- und Softwarekomponenten, die zur Bereitstellung der Netzwerk-, Speicher-, Computing- und Virtualisierungsdienste erforderlich sind – darunter auch verschiedene Standardbetriebssysteme wie Red Hat Enterprise Linux (RHEL) und Windows Server.

Sie als Kunde müssen dagegen die Sicherheit Ihrer Middleware, Laufzeitumgebungen, Anwendungen und Daten gewährleisten und sind außerdem für den Schutz aller nicht standardmäßigen Betriebssysteme zuständig. Kurz: Während der Anbieter die Verantwortung für die **Sicherheit der Cloud an sich** trägt, sorgt Ihr Unternehmen für die **Sicherheit in der Cloud**.

Wie unschwer einzusehen ist, kann dieses Modell nur dann funktionieren, wenn Sie und Ihr CSP in enger Zusammenarbeit alle Sicherheitslücken an den „Nahtstellen“ der beiden Verantwortungsbereiche schließen.



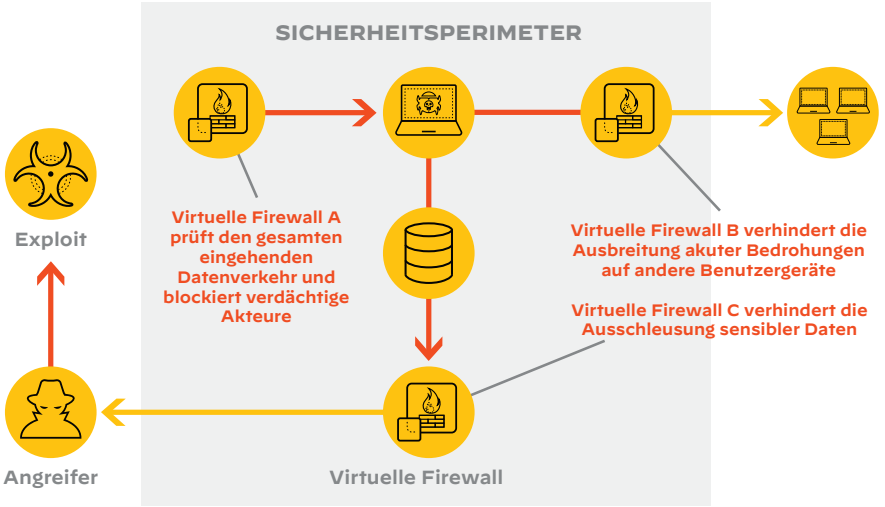
Aufteilung der sicherheitsbezogenen Verantwortungsbereiche in der Public Cloud

Bedenken Sie stets, dass es sich bei Zero Trust nicht um ein bestimmtes Tool oder eine bestimmte Architektur handelt, sondern um ein allgemeines Prinzip. Deshalb geht es im nächsten Abschnitt um virtuelle Firewalls und ihre wichtige Rolle bei der Implementierung einer Zero-Trust-Architektur.

Virtuelle Firewalls: essentieller Schutz für die Public Cloud

Next-Generation Firewalls (NGFWs) sind der Grundpfeiler moderner Netzwerksicherheit, da sie sowohl vor Bedrohungen auf der Netzwerk- und Transportebene (Layer 3 und 4 des OSI-Modells) als auch vor Distributed Denial of Service (DDoS), HTTP-Floods, SQL-Injektionen und anderen Angriffen auf der Anwendungsebene (Layer 7) schützen. Dabei wurden die entsprechenden Systeme bis vor Kurzem ausschließlich als physische, speziell für herkömmliche Client/Server-Anwendungen konzipierte Appliances in konventionellen Rechenzentren bereitgestellt. Allerdings eignet sich dieses hardwarebasierte Bereitstellungsmodell nicht für die dynamischen Multi-Cloud-Umgebungen von heute, weil deren physische Komponenten Eigentum der jeweiligen Cloud-Anbieter sind.

Insofern ist es ein nicht zu unterschätzender Vorteil, dass nun virtuelle Firewalls zur Bewältigung der komplexen Sicherheitsanforderungen der Public Cloud zur Verfügung stehen. Diese softwaredefinierten NGFWs besitzen alle Funktionen physischer Firewallappliances und sind darüber hinaus in der Lage, sich automatisch an jegliche Veränderungen der dynamischen Anwendungen und Workloads in einer virtualisierten Umgebung anzupassen.



Virtuelle Firewalls bieten starken Schutz vor Cyberbedrohungen und unterstützen die Umsetzung einer Defense-in-Depth-Strategie.

Die Verpflichtung zur Umsetzung gesetzlicher Compliancevorschriften gilt für die Public Cloud ebenso wie für On-Premises-Infrastrukturen. Trotzdem ist für Cloud-Umgebungen eine eigene Implementierungsstrategie erforderlich.

Die schwierige Umsetzung von Complianceframeworks in Cloud-Umgebungen

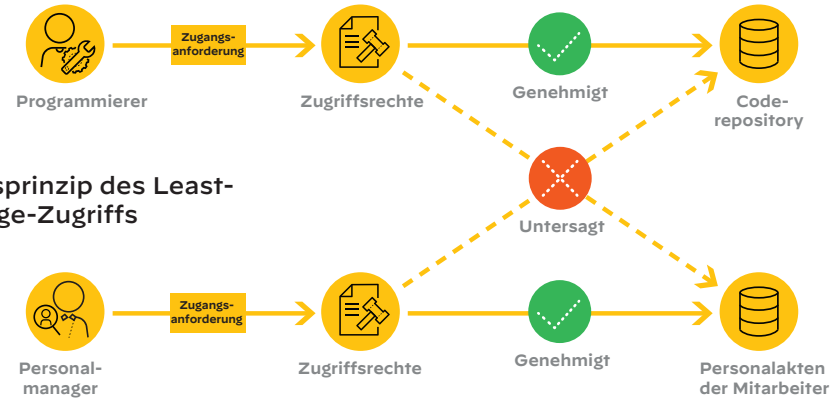
Unternehmen in stark regulierten Branchen gehen ein hohes Risiko ein, wenn sie die strikten Vorgaben und Standards wie HIPAA im Gesundheitswesen, PCI DSS2 im Einzelhandel und ACH3 im Bankwesen nicht einhalten. Werden Anwendungen und Daten vom unternehmensinternen Rechenzentrum in die Public Cloud migriert, kann dies erhebliche Auswirkungen auf die Compliancestrategien haben.

Zum Glück gibt es CSP, die bereit und in der Lage sind, mit dem Complianceprogramm Ihres Unternehmens zusammenzuarbeiten. Zum einen können Sie die Sicherheitsmaßnahmen, die der CSP in seiner eigenen Infrastruktur nutzt, übernehmen, wodurch Ihre eigene Compliance und Ihre Zertifizierungsprogramme gestärkt werden. Die meisten CSP gestatten ihren Kunden die Nutzung ihrer Services zur Aktivitätsüberwachung, um Konfigurationsänderungen und Sicherheitsereignisse in ihrem System aufzuspüren, und verbinden sogar ihre Services mit den vorhandenen Lösungen, um die Erstellung von Complianceberichten zu vereinfachen.

Eine effektive Compliancestrategie in Cloud-Umgebungen ist nur möglich, wenn das Sicherheitssystem entsprechend angepasst wird. Sicherheitsmanager brauchen ein zentralisiertes Sicherheitsmanagement, damit sie Richtlinien in der gesamten Cloud-Umgebung und auch in komplexen Bereitstellungen mit mehreren Clouds harmonisieren können. Zur Erfüllung der Compliancevorschriften müssen Sicherheitsteams die Verwaltung und das Sicherheitsniveau über alle Public-Cloud-Umgebungen hinweg harmonisieren können – etwas, das CSP von ihrer Grundausrichtung her nicht können.

Außerdem müssen Zugangskontrollen durch Maßnahmen wie das Least-Privilege-Prinzip und die Multifaktor-Authentifizierung strenger gefasst werden. Beim Least-Privilege-Prinzip erhalten Benutzer nur für die Anwendungen eine Berechtigung, die sie zur Ausübung ihrer Tätigkeiten und für ihre Position im Unternehmen benötigen. So muss ein Programmierer auf das Coderepository zugreifen können, erhält aber keinen Zugang zu den Personalakten der Mitarbeiter. Für Personalmanager gelten diese Berechtigungen entsprechend umgekehrt.

Das Funktionsprinzip des Least-Privilege-Zugriffs



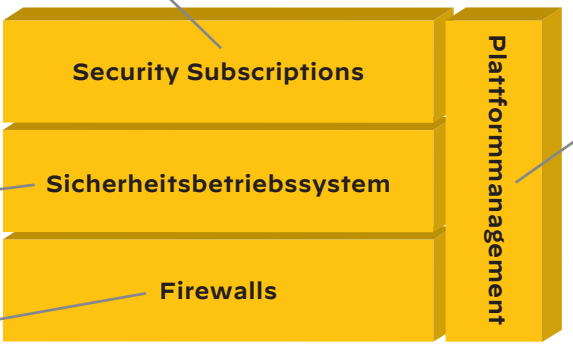
Angesichts so vieler Herausforderungen fragen Sie sich vielleicht, wie Sie Ihre Public Cloud jemals wirkungsvoll schützen können. Diese Frage beantworten wir im nächsten Abschnitt.

Die Architektur der Netzwerksicherheitsplattform

Wenn Sie sich einmal für eine Zero-Trust-Strategie entschieden haben, werden Sie schnell feststellen, dass Ihr gegenwärtiger Mix verschiedener Tools und Sicherheitsansätze nicht ausreicht. Die einzige zuverlässige Möglichkeit zur Sicherung von Public-Cloud-Umgebungen ist eine integrierte Lösung, die virtuelle Firewalls, ein gemeinsames Firewallbetriebssystem, Security Subscriptions und eine zentrale Managementkonsole umfasst. Diese Anforderungen erfüllt Palo Alto Networks mit seiner Netzwerksicherheitsplattform.

Security Subscriptions
Cloud-Delivered Security Services (CDSS) von Palo Alto Networks bietet Ihnen die Möglichkeit, gezielt die aktuell benötigten Services auszuwählen und diese Auswahl jederzeit an neue Sicherheitsanforderungen anpassen.

Plattformmanagement
Panorama™ ermöglicht ein zentrales Management und einen umfassenden Überblick über alle Firewalls von Palo Alto Networks, unabhängig von deren Formfaktor oder Standort – von Firewalls am Perimeter und in Filialen bis zu Cloud-Umgebungen und Rechenzentren.



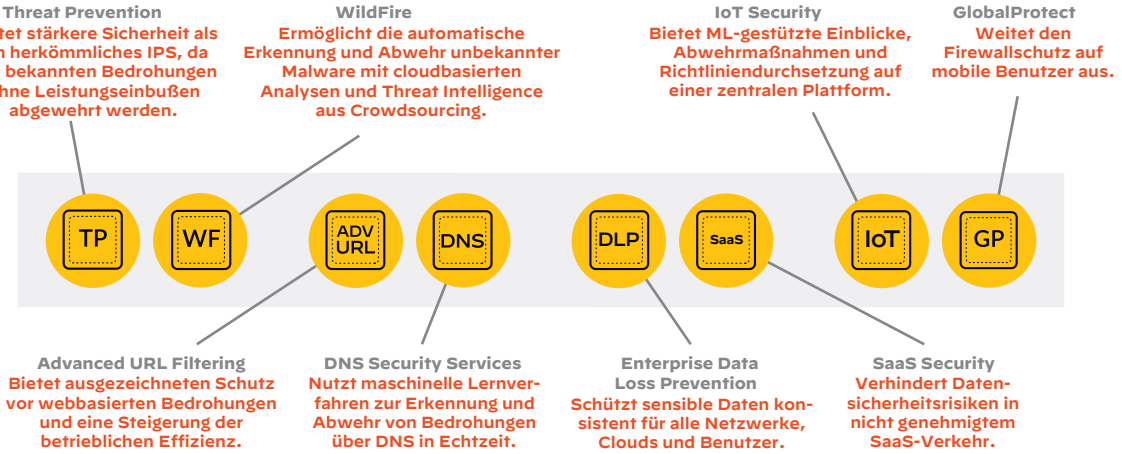
Sicherheitsbetriebssystem
PAN-OS, das branchenführende Firewall-betriebssystem, erkennt mithilfe von maschinellem Lernen und Analysen eindeutig Benutzer, Anwendungen, Geräte und Inhalte und erfasst neue Bedrohungen, die auf Fingerprinting und Signaturen basieren.

Firewalls
Die branchenführenden ML-gestützten NGFWs von Palo Alto Networks bieten konsistente und integrierte Netzwerk-sicherheit mit physischen, virtuellen, containerisierten und cloudbasierten Komponenten.

In dynamischen Cloud-Umgebungen verändern sich die Sicherheitsanforderungen oft. Mit der Netzwerksicherheitsplattform können Sie schnell darauf reagieren, indem Sie im Handumdrehen Sicherheitsservices hinzufügen, wie im nächsten Abschnitt erläutert wird.

Cloud-Delivered Security Services für die Netzwerksicherheitsplattform

Die Netzwerksicherheitsplattform bietet ein umfassendes Angebot an aufeinander abgestimmten Cloud-Delivered Security Services, die sich gegenseitig ergänzen und verstärken, sodass Sie den gesamten Datenverkehr durch Ihre Netzwerke und Clouds zuverlässig schützen können. Während Sie die Lösungen mancher Anbieter nur als Bündel erhalten und somit auch Services kaufen müssen, die Sie eigentlich nicht brauchen, bietet Ihnen die Netzwerksicherheitsplattform absolute Flexibilität. Sie wählen nur die Services aus, die Sie jetzt tatsächlich brauchen, und fügen dann entsprechend weitere Services hinzu – oder kündigen Services –, wenn sich Ihre Sicherheitsanforderungen verändern.

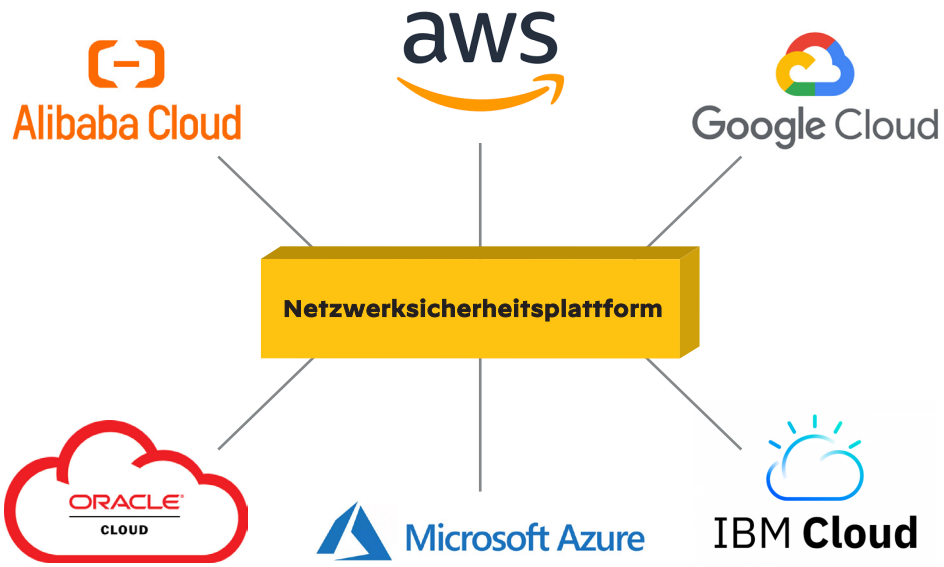


Der Trend hin zu Multi-Cloud-Umgebungen erfordert die Flexibilität, Lösungen unterschiedlicher CSP zu kombinieren, und keine Bindung an einen bestimmten Anbieter. Im nächsten Abschnitt erfahren Sie Näheres.

Von der Netzwerksicherheitsplattform unterstützte CSP

Der Markt für Public Clouds ist extrem vom Wettbewerb geprägt. Kluge Unternehmen können diese Dynamik zu ihrem eigenen Vorteil nutzen, indem sie günstige Vertragsbedingungen aushandeln und zwischen CSP wechseln, um frühzeitig von neuen Technologien zu profitieren.

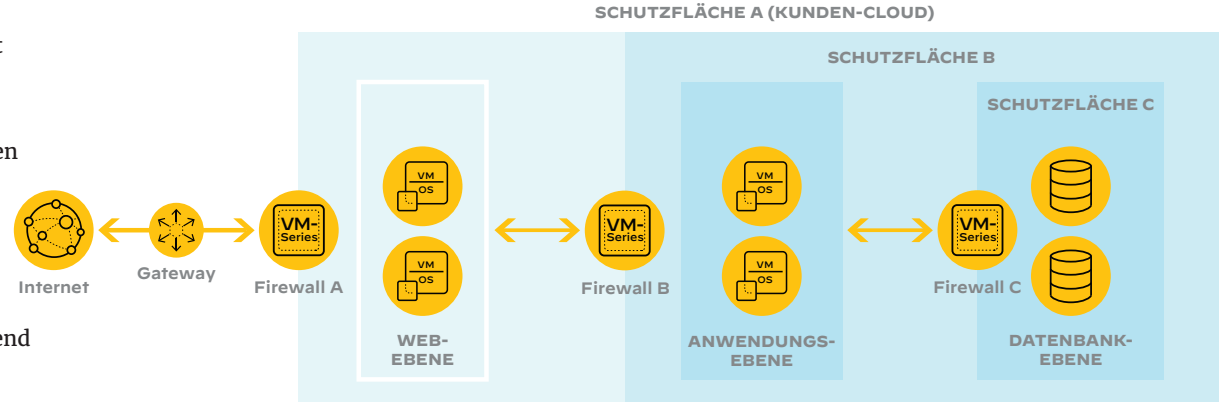
Die Netzwerksicherheitsplattform lässt sich nahtlos mit den Public Clouds aller großen Anbieter einsetzen. Dadurch können Sie sich unbesorgt für den Anbieter (bzw. im Fall von Multi-Cloud-Umgebungen die Anbieter) entscheiden, der Ihren Anforderungen am besten gerecht wird, in dem Wissen, dass Palo Alto Networks Sie dabei unterstützen kann, Ihren Teil der gemeinsamen Verantwortung in jeder Cloud-, Multi-Cloud- oder Hybrid-Cloud-Umgebung zu erfüllen.



Im nächsten Abschnitt sehen wir uns das Gesamtbild an – wie Zero Trust unter realen Bedingungen funktioniert.

Zero-Trust-Sicherheit für Defense-in-Depth

Im ersten Abschnitt dieses E-Books wurde erläutert, wie die Umsetzung von Zero Trust mit einem Perspektivwechsel von der Angriffsfläche zur Schutzfläche einhergeht. In dem rechts dargestellten Beispiel werden zum Schutz einer mehrschichtigen Anwendungsarchitektur mit den drei Ebenen Web, Anwendung und Datenbank drei Firewalls der VM-Series und Cloud-Delivered Security Services (CDSS) genutzt. Jede virtuelle Firewall der VM-Series schafft im Grunde eine klar definierte Schutzfläche. Die Gateway-Firewall untersucht und sichert den ein- und ausgehenden Datenverkehr, während die Firewall der Anwendungsebene den Zugriff auf den privaten Netzwerkbereich kontrolliert, der die Anwendungs- und Datenbankebene umfasst. Der letzte Baustein der Tiefensicherheit besteht aus Mikrosegmentierung, umgesetzt durch eine Firewall, die zwischen der Datenbank und der übrigen Infrastruktur eine zusätzliche Schutzschicht einzieht.



Mehrschichtiger Schutz der Public-Cloud-Anwendungen mit virtuellen Firewalls der VM-Series

Nach diesem kurzen technischen Überblick wenden wir uns nun der Kernfrage zu: wie die Netzwerksicherheitsplattform einen greifbaren geschäftlichen Nutzen und einen beeindruckenden ROI liefert.

Geschäftlicher Nutzen: ROI, Mitarbeiterproduktivität

Unternehmen entscheiden sich für Zero Trust aus Sicherheitsgründen und wegen des geschäftlichen Nutzens. Zu den Vorteilen der Netzwerksicherheitsplattform zählen u. a. die Maximierung der Rendite von Investitionen in die Sicherheit, die Abfederung der Folgen des Fachkräftemangels, die Beschleunigung der Bedrohungsabwehr und die Verbesserung der Benutzererfahrung. Sehen wir uns diese Vorteile der Reihe nach an:

Schneller ROI

In der Vergangenheit konzentrierten sich Sicherheitsfachleute bei Investitionen in die Sicherheit oft auf die Schutzfunktionen und betrachteten finanzielle Aspekte als nachrangig. Heute erwarten Unternehmen mehr und verlangen von CISOs, Lösungen zum Schutz von Daten und anderen nicht greifbaren Werten zu finden, die optimal in ein knappes Sicherheitsbudget passen. Eine aktuelle Untersuchung von Forrester Consulting ergab, dass sich mit den virtuellen Firewalls der VM-Series ein höherer ROI von bis zu 115 Prozent in drei Jahren bei sechsmonatiger Amortisationszeit erzielen lässt.[2] Dieselbe

115 %

ROI
sechsmonatige Amortisationszeit

30 %

Zeitersparnis
bis zur Umsetzung eines zuverlässigen Sicherheitsniveaus

Untersuchung ergab auch eine Verkürzung der Zeit bis zur Erreichung eines zuverlässigen Sicherheitsniveaus um 30 Prozent.

Mit der Migration in die Cloud werden aus Kapitalausgaben (CapEx) Betriebsausgaben (OpEx). Anstatt Hardware und Software selbst anzuschaffen, können Sie diese kostenwirksam von Ihrem CSP leasen. Bereitstellung, Installation, Betrieb und Instandhaltung der Infrastruktur entfallen dadurch auf den CSP, während Ihre Mitarbeiter und Finanzmittel für andere Projekte und Aufgaben zur Verfügung stehen.

Fachkräftemangel in der Cybersicherheit

Die Verwaltung der Netzwerksicherheit war schon immer eine arbeitsintensive Angelegenheit, was angesichts des aktuellen Fachkräftemangels im IT-Bereich und insbesondere in der IT-Sicherheit problematisch ist. Eine aktuelle Umfrage ergab, dass über 2,7 Millionen Positionen nicht besetzt sind und dass die Anzahl der qualifizierten Personen jährlich um 65 Prozent zunehmen müsste, um eine adäquate Personalabdeckung zu erreichen.[3]

Es überrascht nicht, dass Unternehmen nicht mit einem solchen phänomenalen Wachstum rechnen und stattdessen andere Mittel und Wege zur Bewältigung des Fachkräftemangels suchen. Ganz oben auf der Liste stehen technische Lösungen: 38 Prozent der Unternehmen verlagern Arbeitslasten aus dem eigenen Rechenzentrum zu Cloud-Serviceanbietern, um die für den Betrieb, die Instandhaltung und Erneuerung der Infrastruktur benötigten Mitarbeiterstunden zu reduzieren.[4]

Nach dem ROI und der Mitarbeiterproduktivität wenden wir uns im nächsten Abschnitt der Verbesserung der Bedrohungsabwehr und der Benutzererfahrung mit der Netzwerksicherheitsplattform zu.

Geschäftlicher Nutzen: Bedrohungsabwehr, Benutzererfahrung

Effektive Bedrohungsabwehr

Eine der größten Herausforderungen bei der Public-Cloud-Sicherheit ist die große Dynamik der Bedrohungslage. Angreifer ersinnen nicht nur immer wieder neue und raffiniertere Angriffsmethoden, sondern sie modifizieren auch die bekannten, um bestehende Sicherheitsmaßnahmen zu umgehen. Aus diesem Grund ist die Arbeit von Sicherheitsteams nie erledigt.

Die Netzwerksicherheitsplattform nutzt zur Bereitstellung von Sicherheitsdiensten einen modularen, cloudbasierten Ansatz, der es Sicherheitsexperten ermöglicht, schnell und effektiv auf Veränderungen der Bedrohungslage sowie der Unternehmensarchitektur zu reagieren. Stellen Sie sich zum Beispiel vor, Sie erhalten einen Tipp, dass jemand mit einem USB-Laufwerk geheime Daten aus dem Unternehmen schmuggelt. Wenn Sie diese Information für glaubwürdig halten, kann Ihr Team in wenigen Minuten Data Loss Prevention (Schutz vor Datenverlust, DLP) einrichten und Ihr Unternehmen so vor dieser Bedrohung von innen schützen.

Verbesserte Benutzererfahrung

Unternehmen stellen hohe Erwartungen an ihre CIOs und CISOs und keine davon ist wichtiger, als die Infrastruktur auf gleichbleibend hohem Niveau zu halten, damit Mitarbeiter, Lieferanten, Auftragnehmer und andere, deren Arbeit von dem Netzwerk abhängt, diese verrichten können. Alles, was den Zugriff auf wichtige Geschäftsanwendungen und -daten beeinträchtigen könnte, von Verlangsamungen und Ausfällen des Netzwerks über die Ausschleusung von Daten bis hin zu Angriffen mit Ransomware, kann sich negativ auf die Produktivität, Moral und Innovation auswirken.

Daneben gibt es außerhalb des Unternehmens einen weiteren Kosmos mit Benutzern, deren Erfahrungen relevant sind. Wenn Kunden Ihre Website besuchen, erwarten sie, schnell und genau die Informationen und Dienste zu finden, die sie brauchen. Wenn die Website ausgefallen oder auch nur langsam ist, werden sie es wahrscheinlich kein zweites Mal versuchen. Und es kann noch schlimmer kommen! Wenn die Geräte Ihrer Besucher mit Malware infiziert werden oder ihre persönlichen Daten gestohlen werden, weil Ihrerseits die Sicherheit nicht genügt, drohen Ihnen schwere finanzielle Verluste und Strafzahlungen. Der Schaden für Ihre Marke wäre kaum wiedergutzumachen.

Zero Trust ist das perfekte Gegenmittel für diese potenziellen Probleme. Durch die integrierte Netzwerksicherheitsplattform wird die Sicherheitsverwaltung vereinheitlicht und zusammengeführt, wodurch alle Teile der Sicherheitsinfrastruktur ganzheitlich zusammenwirken und so den Schutz maximieren und Störungen minimieren. In den meisten Fällen merken die Benutzer nicht einmal, dass die Plattform überhaupt existiert – das bestmögliche Ergebnis.

Herzlichen Glückwunsch! Sie haben sich in diesem E-Book über die Grundlagen von Zero Trust in Public-Cloud-Umgebungen informiert. Jetzt müssen Taten folgen. Im nächsten Abschnitt erfahren Sie, wie der Einstieg gelingt.

Ihre nächsten Schritte zur Zero-Trust-Sicherheit

Die Migration Ihrer wertvollen Daten und Anwendungen in die Public Cloud führt zu neuen Sicherheitsherausforderungen. Die Lösungen von Palo Alto Networks schaffen hier Abhilfe. Unsere virtuellen Firewalls der VM-Series sind die wesentlichen Bausteine für die Einrichtung einer mehrschichtigen Zero-Trust-Architektur, die Schutz vor Zero-Day-Angriffen und anderen Bedrohungen bietet, die Benutzererfahrung verbessert, einen beeindruckenden ROI liefert und Ausfallzeiten für Benutzer signifikant um bis zu 67 Prozent reduziert.[5]

Die Migration von Anwendungen in die Cloud ist auch mit Risiken verbunden. Mit der Einrichtung einer Zero-Trust-Architektur sollen Risiken reduziert und wichtige geschäftliche Anforderungen und Notwendigkeiten geschützt werden. Lesen Sie unbedingt den gerade erst veröffentlichten Bericht zum Total Economic Impact (TEI) von Forrester Consulting, in dem Sie mehr über den ROI und andere wirtschaftliche Vorteile unserer virtuellen Firewalls erfahren. Oder lassen Sie sich von unserem einfach zu bedienenden ROI-Rechner für virtuelle Firewalls auf der Grundlage der Studie von Forrester Consulting Ihre möglichen Einsparungen berechnen.

Wir unterstützen Sie gern dabei, Ihre Risiken zu mindern. Unsere Sicherheitsexperten stehen gern für eine persönliche Vorführung zur Verfügung und beantworten Ihre Fragen rund um die Sicherheit in Public Clouds. Vereinbaren Sie heute einen Termin für die Vorführung.

1 1. Kapitel: Zero Trust Fundamentals, von Zero Trust Networks.

2 The Total Economic Impact™ of Palo Alto Networks: Virtuelle Firewalls der VM-Series, Forrester Consulting, im Auftrag von Palo Alto Networks, 26. Oktober 2021.

3 A Resilient Cybersecurity Profession Charts the Path Forward, (ISC)2 Cybersecurity Workforce Study, 2021.

4 Ibid.

5 The Total Economic Impact™ of Palo Alto Networks: Virtuelle Firewalls der VM-Series, Forrester Consulting, im Auftrag von Palo Alto Networks, 26. Oktober 2021.

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