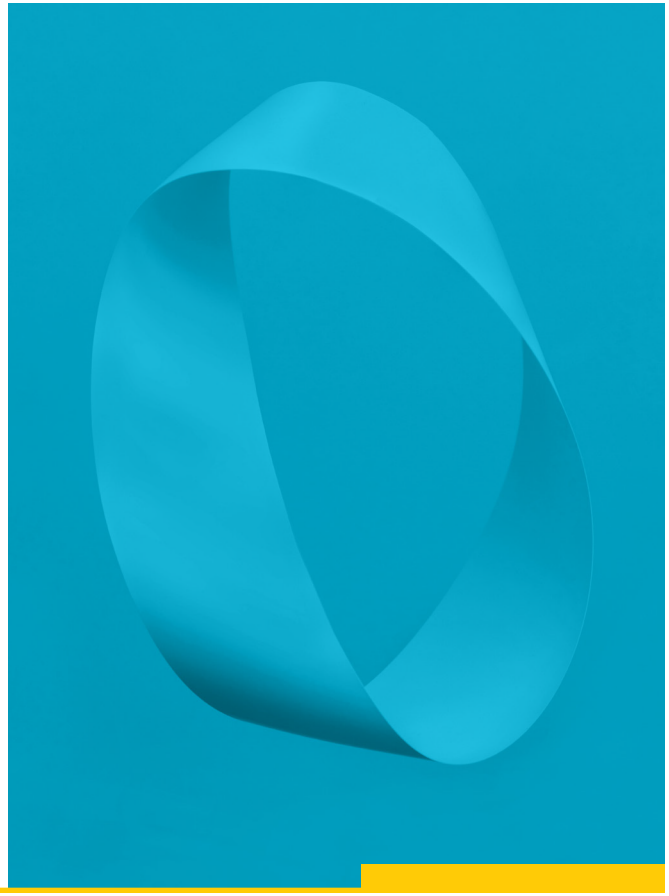
Fünf große Herausforderungen bei der Sicherung privater Clouds

Die ideale Netzwerksicherheitsplattform für eine robuste Zero-Trust-Umgebung

paloalto NETWORKS | STRATA BY PALO ALTO NETWORKS



Inhalt

Die zunehmende Verbreitung privater Clouds

Es gibt zwei Arten von Clouds – öffentliche und private – und sie unterscheiden sich in wesentlichen Punkten, die Unternehmen unbedingt kennen müssen. Anbieter öffentlicher Clouds stellen Ressourcen wie Rechen- und Speicherkapazitäten zu Tarifen auf Pay-As-You-Go-Basis bereit. Die Hard- und Software der Plattform sind nicht sichtbar. Ihr Team sieht nur eine Art Blackbox für die Anwendungen und Daten. Das hat entscheidende Vorteile: Sie benötigen keine Kapitalaufwendungen, vermeiden teure Technologieaktualisierungen und profitieren von nahezu unbegrenzter Skalierbarkeit, hoher Zuverlässigkeit, sicheren Daten-Back-ups und Agilität.

Allerdings verlieren Sie bei der Nutzung einer öffentlichen Cloud auch ein gewisses Maß an Kontrolle, denn Sie teilen sich die Infrastruktur mit anderen Unternehmen, was in sicherheitsbewussten Branchen wie dem Gesundheits- und Finanzwesen für Bedenken sorgen kann. Zudem bereitet die Abstrahierung der Plattform Probleme für Unternehmen in stark regulierten Branchen, in denen jede Systemänderung, die die Arbeitsabläufe, Daten oder die Unternehmenslogik beeinträchtigen könnten, validiert werden muss. Zu den betroffenen Sektoren gehören beispielsweise Hersteller medizinischer Geräte und die Pharmaindustrie. Unter anderem aus diesen Gründen entscheiden sich viele Unternehmen dafür, ihre sensiblen Daten und wichtigsten Geschäftsanwendungen in privaten Clouds bereitzustellen und öffentliche Clouds für die Skalierbarkeit und kundenorientierten Services zu nutzen.

Öffentliche Clouds sind bereits in aller Munde, doch auch private Clouds setzen sich immer stärker durch. Ein durchschnittliches Unternehmen verwendet inzwischen 2,6 öffentliche Clouds und 2,7 private Clouds (siehe Tabelle unten). Mit Blick auf die Zukunft testen Unternehmen jedoch bereits doppelt so viele private Clouds (2,2) wie öffentliche Clouds (1,1). Diese Zahlen unterstreichen die Annahme, dass die meisten Unternehmen von einer Kombination aus öffentlichen und privaten Clouds profitieren – einer sogenannten Hybrid-Cloud-Umgebung.

	Öffentlich	Privat
Aktuell im Einsatz	2,6	2,7
In der Testphase	1,1	2,2
Insgesamt	**3,7**	**4,9**

Anzahl der Clouds, die im Durchschnitt von Unternehmen genutzt werden

Private Clouds bringen spezielle Sicherheitsherausforderungen mit sich, die wir im nächsten Kapitel genauer betrachten.

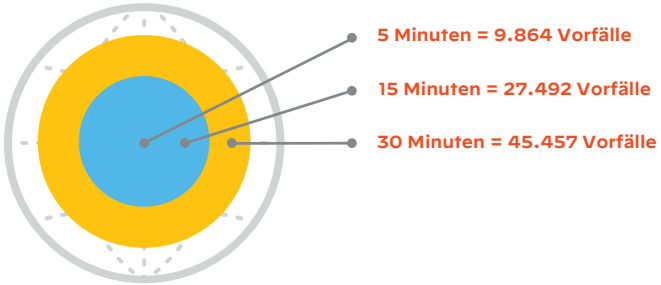
Die wachsenden Herausforderungen bei der Sicherung privater Clouds

Die Implementierung zuverlässiger Sicherheitsmaßnahmen ist generell nicht einfach, aber der Schutz privater Clouds ist eine besonders komplexe Aufgabe, die immer schwieriger wird. Das liegt unter anderem an den folgenden Faktoren:

Wachsende Angriffsfläche: Der Trend zu Homeoffice und mobiler Arbeit schafft mehr potenzielle Einfallstore für Angriffe auf private Clouds. Auch die Erweiterung integrierter Lieferketten birgt weitere Risiken, da Lieferanten und Partner auf ihren Endpunkten eventuell nicht für das erforderliche Maß an Sicherheit sorgen. Inzwischen beginnen sogar vier von zehn Cyberangriffen in der erweiterten Lieferkette und nicht im Unternehmen selbst.

Immer komplexere Bedrohungen: Moderne Bedrohungen umgehen Sicherheitssysteme mit ausgefeilten Techniken, zum Beispiel der Erstellung von Varianten und der Verschlüsselung des Datenverkehrs zwischen der Malware und dem externen Angreifer. Hacker nutzen entweder neue Schwachstellen aus oder verwenden polymorphe Malwarevarianten, die von signaturbasierten Lösungen zur Bedrohungserkennung nicht erfasst werden.

Kürzere Angriffsdauer: Moderne Bedrohungen können nicht nur die Abwehrmaßnahmen besser umgehen, sie richten auch viel schneller Schaden an als in der Vergangenheit. Malware kann bereits wenige Minuten nach dem Eindringen in ein Netzwerk die ersten Daten verschlüsseln. Außerdem können sich Bedrohungen in nicht segmentierten Netzwerken blitzschnell ausbreiten. Das Bedrohungsforschungsteam Unit 42 von Palo Alto Networks hat kürzlich bei einer internen Untersuchung festgestellt, dass sich eine komplexe Bedrohung innerhalb von 30 Minuten auf mehr als 45.000 Instanzen replizieren konnte (siehe Diagramm).



Als Nächstes betrachten wir die Herausforderungen bei der Sicherung privater Clouds – angefangen mit der Verschiebung des Perimeters.

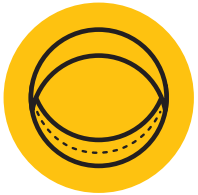
Herausforderung 1: Cloud-Architekturen lassen die Grenzen zwischen interner und externer Umgebung verschwimmen

Traditionelle Sicherheitsmodelle beruhen auf der Annahme, dass es eine klare Grenze zwischen dem Unternehmen und der Außenwelt gibt, den sogenannten Sicherheitsperimeter. Er trennt die vertrauenswürdige Umgebung (innen) von der nicht vertrauenswürdigen Welt (außen). Sofern an allen potenziellen Zugangspunkten effektive Abwehrmaßnahmen implementiert wurden, sind die wertvollen Informationen im Inneren geschützt.

Bei Cloud-Architekturen verschwimmen allerdings die Grenzen zwischen der internen Umgebung und der Außenwelt: In vielen Unternehmen sitzen nicht mehr alle Benutzer im Hauptsitz hinter dem Sicherheitsperimeter, sondern können überall arbeiten. Und wenn eine Anwendung im lokalen Rechenzentrum Daten aus der Cloud abruft, muss auch dieser Datenverkehr den Perimeter fortlaufend überschreiten.

Ein Beispiel zur Verdeutlichung: Ein traditionelles Sicherheitsmodell ist wie ein einfacher Kreis aus einem Papierstreifen. Er hat zwei Seiten – eine Innen- und eine Außenseite –, die deutlich voneinander getrennt sind. Wenn Sie eine Linie über den gesamten Streifen bis zurück zum Ausgangspunkt ziehen, befindet sich diese nur auf einer der beiden Seiten.

Eine Cloud-Architektur hingegen ähnelt einem Möbiusband, also einem Streifen mit einer halben Verdrehung. Im Gegensatz zu dem einfachen Papierstreifen hat ein Möbiusband nur eine Seite. Egal, wo Sie jetzt mit dem Zeichnen der Linie beginnen, wird sie immer über die gesamte Oberfläche verlaufen. Ähnlich wie bei diesem Prinzip unterscheiden cloudbasierte Sicherheitsmaßnahmen nicht zwischen der internen und der externen Umgebung. Sie vertrauen keinem Gerät, keinem Benutzer und keiner Anwendung, bis deren Vertrauenswürdigkeit nachgewiesen wurde.



Das einfache Band hat zwei Seiten: eine Innen- und eine Außenseite.

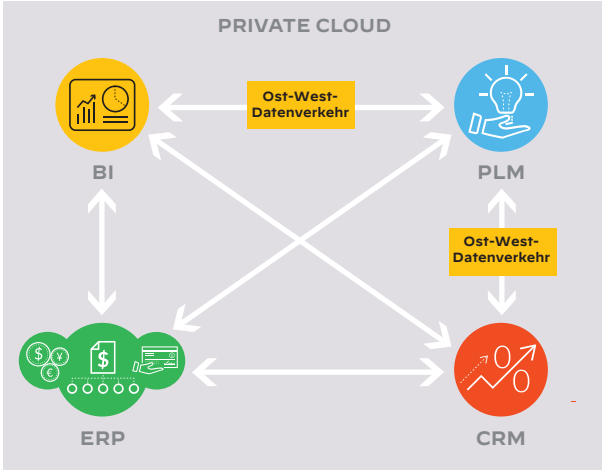
Das Möbiusband hat nur eine Seite: Die Konzepte „innen“ und „außen“ treffen in diesem Fall nicht zu.

Nächstes Kapitel: Integrierte Geschäftsanwendungen erfordern effektivere Sicherheitslösungen für private Clouds.

Herausforderung 2: Integrierte Geschäftsanwendungen überfordern ältere Sicherheitslösungen

Jedes Unternehmen ist ein digitales Unternehmen, da es eine gewisse Anzahl von Geschäftsanwendungen nutzt. Systeme für das Produktlebenszyklus-Management (PLM) dienen der Verwaltung des gesamten Lebenszyklus eines Produkts – vom Entwurf über die Entwicklung und das Design bis zur Herstellung – und sind ein wichtiges Repository für geistiges Eigentum. Mit Lösungen für die Ressourcenplanung (Enterprise Resource Planning, ERP) lassen sich wichtige Finanzprozesse verwalten – von der Beschaffung und Produktionsplanung über die Fertigung der Produkte bis zur Auftragsabwicklung. Vertriebs- und Marketingteams nutzen CRM-(Customer Relationship Management-) und BI-(Business Intelligence-)Lösungen, um potenzielle Neukunden zu identifizieren und mit Bestandskunden zu kommunizieren. Die Liste lässt sich beliebig fortsetzen.

Diese grundlegenden Geschäftsanwendungen werden nicht isoliert ausgeführt. Sie sind in die Infrastruktur integriert, um die Zusammenarbeit zu ermöglichen, die Markteinführung zu beschleunigen und einen Mehrwert aus den riesigen Datenmengen eines Unternehmens zu gewinnen. Diese Integrationen sind für einen Großteil des Datenverkehrs zwischen den Anwendungen verantwortlich (häufig Ost-West-Verkehr genannt), der vor Malware, gezielten Angriffen, Phishingkampagnen und anderen komplexen Exploits geschützt werden muss. Ältere Sicherheitsstrategien sind weder flexibel noch effektiv genug, um diese Herausforderungen zu bewältigen.

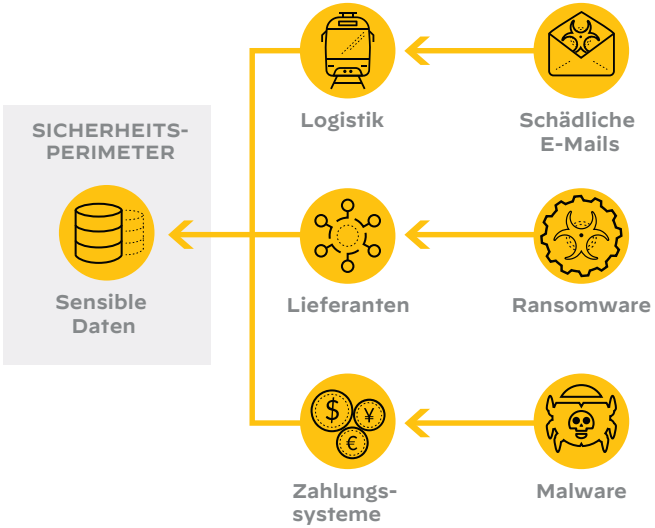


Nächstes Kapitel: Integrierte Lieferketten verursachen Schwachstellen.

Herausforderung 3: Externe Integrationen verursachen Lücken im Perimeter privater Clouds

Um die steigenden Erwartungen der Kunden und Märkte erfüllen zu können, entwickeln sich die traditionellen linearen Lieferketten langsam zu verknüpften Lieferkettennetzwerken. In vielen Fällen haben Lieferanten direkten Zugriff auf bestimmte Bereiche des Unternehmensnetzwerks. Sie selbst verfügen über integrierte Lieferketten, die effektiv eine Erweiterung des Unternehmensnetzwerks sind. Die externen Integrationen sorgen für weitere Schwachstellen, unter anderem in Zahlungssystemen und in der Logistik.

Durch diese Drittanbieterintegrationen steigt die Zahl der Knoten, die gesichert werden müssen, drastisch. Die Angriffsfläche wird enorm vergrößert und die Grenzen der Netzwerke verschwimmen weiter. Dadurch steigt das Risiko von Datenpannen: Laut Accenture beginnen inzwischen vier von zehn Cyberangriffen in der erweiterten Lieferkette und nicht im Unternehmen selbst.

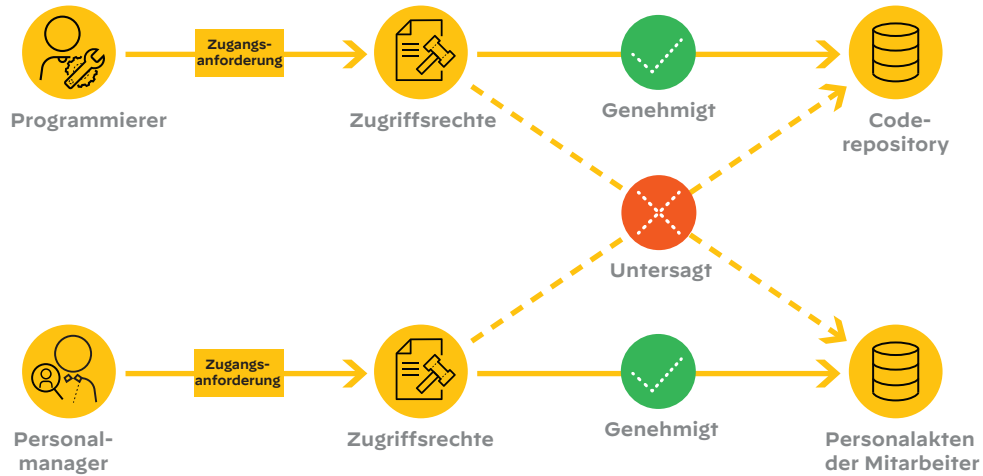


Nächstes Kapitel: Compliance wird in privaten Clouds zur Herausforderung.

Herausforderung 4: Cloud-Umgebungen erschweren die Umsetzung vorhandener Complianceframeworks

Alle börsennotierten Unternehmen sind zur Einhaltung des SOX-Standards verpflichtet, sowohl im Finanz- als auch im IT-Bereich. Unternehmen in stark regulierten Branchen gehen ein hohes Risiko ein, wenn sie die strikten Vorgaben und Standards wie HIPAA[1] im Gesundheitswesen, PCI DSS[2] im Einzelhandel und ACH[3] im Bankwesen nicht einhalten. Werden Anwendungen und Daten vom unternehmensinternen Rechenzentrum in eine private Cloud verlagert, kann dies erhebliche Auswirkungen auf die Compliancestrategien haben.

Eine effektive Compliancestrategie in Cloud-Umgebungen ist nur möglich, wenn das Sicherheitssystem entsprechend angepasst wird. Vorrangig wird dazu ein zentrales Sicherheitsmanagement benötigt, damit Sicherheitsmanager die Richtlinien für die gesamte hybride Umgebung angleichen und durchsetzen können. Eine weitere Herausforderung in Bezug auf die Compliance ist die zunehmende Nutzung von Kubernetes-Containern bei der Entwicklung von Cloud-Anwendungen. Durch diesen Ansatz wird die Effektivität der herkömmlichen Firewalls eingeschränkt, da sie nicht auf die Container zugreifen können. Der letzte Punkt sind Zugangskontrollen. Der Zugang muss durch Richtlinien wie dem Least Privilege-Prinzip und der Multifaktor-Authentifizierung eingeschränkt werden. Beim Least Privilege-Prinzip erhalten Benutzer nur die Berechtigungen, 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.



[1] Health Insurance Portability and Accountability Act

[2] Payment Card Industry Data Security Standard

[3] Automated Clearing House

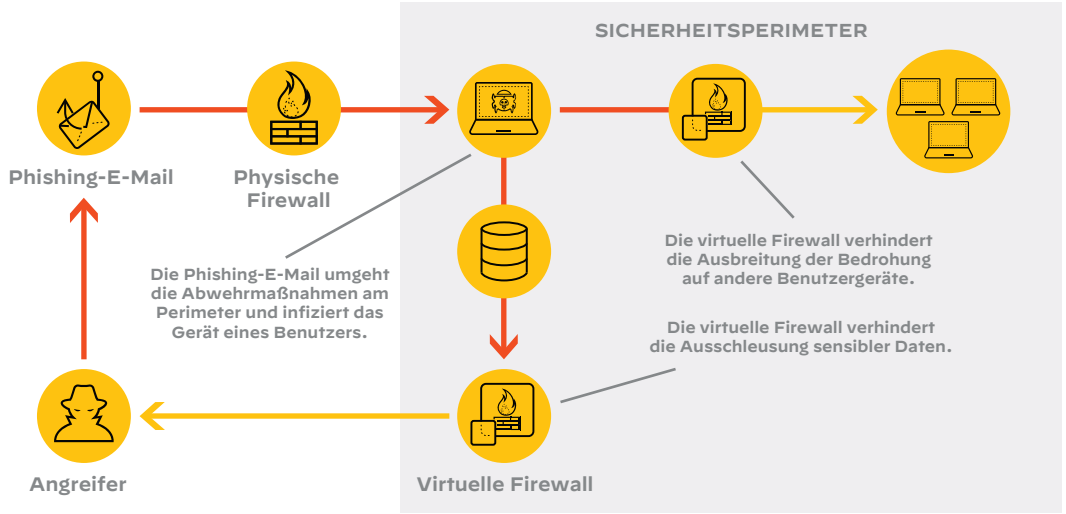
Im nächsten Kapitel wird erläutert, inwiefern moderne virtualisierte Umgebungen für spezielle Herausforderungen in Bezug auf Firewalls sorgen.

Herausforderung 5: Virtualisierte Umgebungen erfordern virtuelle Firewalls

Next-Generation Firewalls (NGFW) sind der Grundpfeiler moderner Netzwerksicherheit. Sie schützen vor Bedrohungen auf der Netzwerk- und Transportebene (Layer 3 und 4 des OSI-Modells) und vor Angriffen auf die Anwendungsebene (Layer 7) wie Distributed Denial of Service (DDoS), HTTP-Floods und SQL-Injektionen. Bis vor Kurzem wurden NGFWs als physische Appliances bereitgestellt, die sich in der Netzwerkarchitektur nicht so einfach verschieben ließen. Dieser Ansatz eignet sich für statische Rechenzentren, doch in den modernen dynamischen virtualisierten Umgebungen stößt er schnell an seine Grenzen.

Abhilfe schaffen virtuelle NGFWs. Diese vielseitigen softwarebasierten Firewalls verfügen über dieselben Funktionen wie die physischen Appliances, können aber außerdem Anwendungen und Workloads automatisch in der virtualisierten Umgebung verfolgen. Der neue Aufbau sieht daher folgendermaßen aus: Physische Firewalls schützen Daten und Anwendungen vor externen Bedrohungen am Sicherheitsperimeter und virtuelle Firewalls sichern den Datenverkehr zwischen Geräten und Workloads innerhalb des Perimeters.

Phishing-E-Mails können beispielsweise häufig die Abwehrmaßnahmen am Perimeter unterwandern und erreichen dann die ahnungslosen Benutzer, die versehentlich die Malware im Anhang starten.

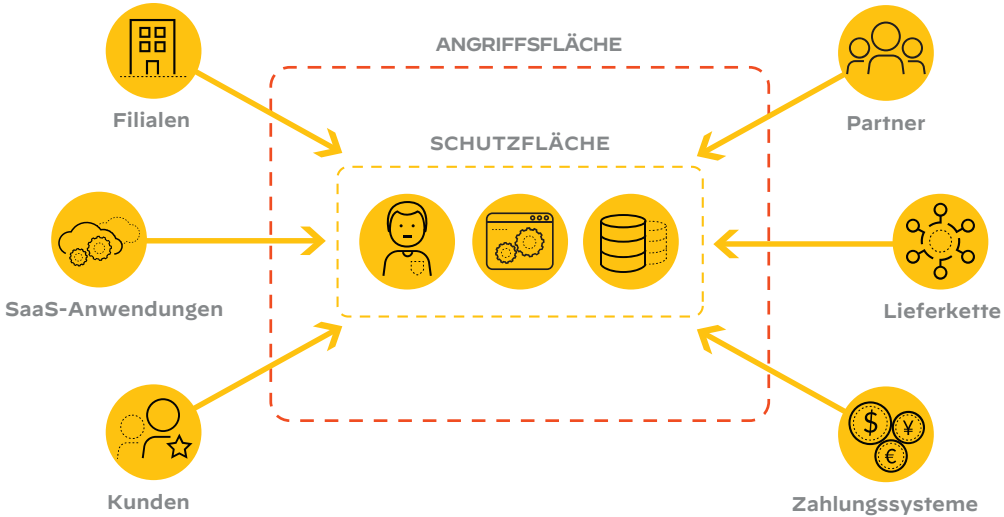


Auf der nächsten Seite erfahren Sie, warum der Schutz privater Clouds einen Zero-Trust-Ansatz erfordert.

Das Zero-Trust-Prinzip: niemandem vertrauen, alles verifizieren

Zero Trust besteht aus verschiedenen Best Practices, die helfen, Datenlecks zu verhindern, indem sie das Konzept der Vertrauenswürdigkeit in virtualisierten Umgebungen eliminieren. Das Grundprinzip lautet „niemandem vertrauen, alles verifizieren“. Eine Zero-Trust-Unternehmensarchitektur nutzt daher zum Schutz der digitalen Umgebungen die Netzwerksegmentierung, um die Ausbreitung von Bedrohungen zu verhindern, die Bedrohungsabwehr auf der Anwendungsebene (Layer 7) zu ermöglichen und detaillierte Zugriffskontrollen für Benutzer zu vereinfachen.

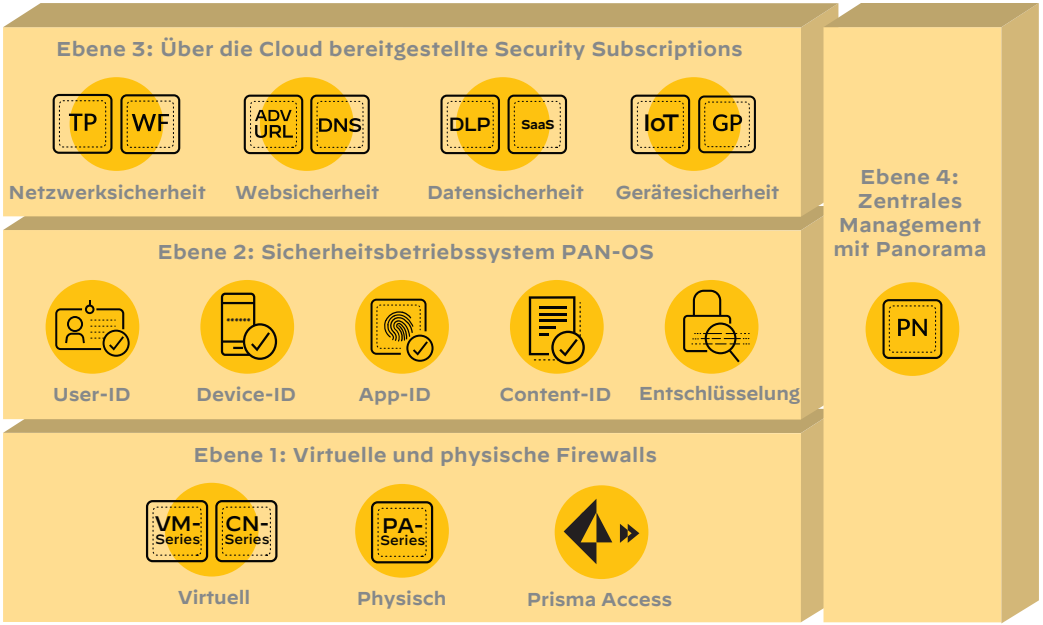
Das Zero-Trust-Prinzip läutet damit einen grundlegenden Paradigmenwechsel ein. Bei älteren Sicherheitslösungen stand die Angriffsfläche im Mittelpunkt, also alle Geräte und Verbindungen, die Hacker potenziell ausnutzen könnten, um die Abwehrmaßnahmen zu umgehen. Das Zero-Trust-Prinzip betrachtet das Problem aus dem entgegengesetzten Blickwinkel und konzentriert sich auf die Schutzfläche, also alle Daten, Anwendungen, Assets und Services, die geschützt werden müssen. Die Schutzfläche ist wesentlich kleiner als die Angriffsfläche und kann in jedem Fall ermittelt und definiert werden.



Nächstes Kapitel: Zur Implementierung des Zero-Trust-Prinzips wird eine Netzwerksicherheitsplattform benötigt.

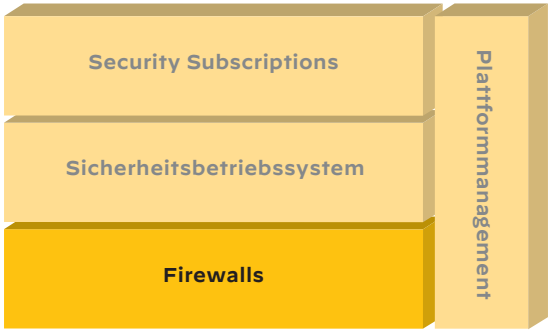
Unsere Netzwerksicherheitsplattform – ideal für Zero-Trust-Umgebungen

Immer mehr Unternehmen entscheiden sich für Hybrid-Cloud-Architekturen und unterstützen verteilte Arbeitsplätze (Filialen, Homeoffice und mobile Benutzer), doch die herkömmlichen Sicherheitssysteme und Punktlösungen sind diesen Anforderungen nicht gewachsen. Für eine Zero-Trust-Architektur benötigen Unternehmen eine integrierte Lösung, die NGFWs, Firewallbetriebssystem, Security Subscriptions und eine zentrale Managementkonsole umfasst. Diese Anforderungen erfüllt Palo Alto Networks mit seiner Netzwerksicherheitsplattform.



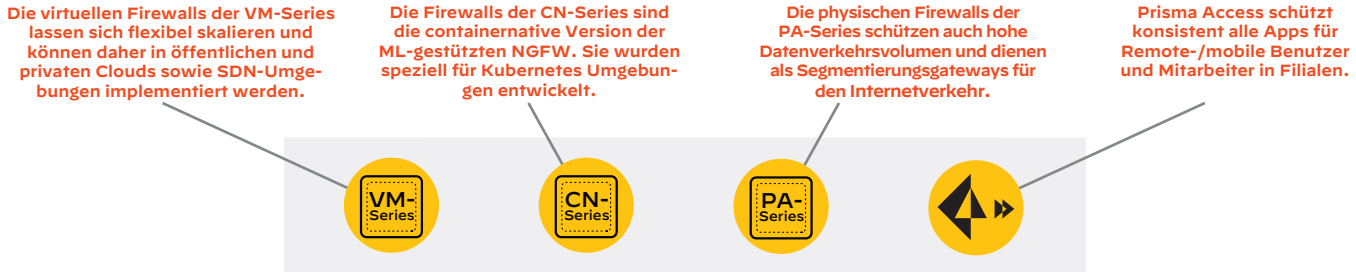
Betrachten wir nun die einzelnen Plattformebenen und beginnen auf der nächsten Seite mit den Firewalls.

Ebene 1: Physische und virtuelle Firewalls



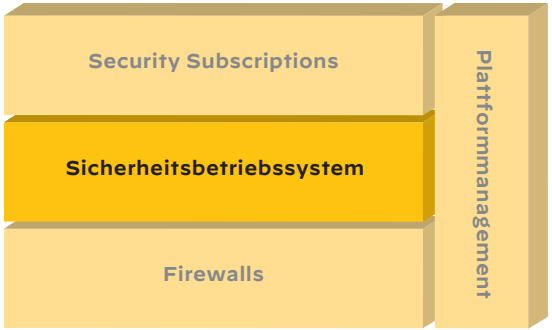
Mit unseren innovativen NGFWs schützen Kunden auf der ganzen Welt ihre Unternehmen bereits erfolgreich vor komplexen modernen Angriffen. Unser Ziel ist es, die Unternehmen unserer Kunden jeden Tag ein bisschen sicherer zu machen. Dazu bieten wir intelligente Netzwerksicherheitslösungen zum Schutz vor neuen Bedrohungen. Wir bieten zuverlässige NGFWs in physischen, virtuellen, containerbasierten und cloudbasierten Formfaktoren.

Aber Sie müssen uns nicht blind vertrauen: Palo Alto Networks wurde zum zehnten Mal in Folge im Gartner® Magic Quadrant™ 2021 für Netzwerkfirewalls als „Leader“ ausgezeichnet und belegte in den Kategorien „Ability to Execute“ und „Completeness of Vision“ den ersten Platz.



Nächstes Kapitel: Das Firewallbetriebssystem spielt eine wichtige Rolle bei der Zero-Trust-Sicherheitsstrategie.

Ebene 2: PAN-OS, das Betriebssystem für Firewalls



PAN-OS ist unser branchenführendes Firewall-betriebssystem, das mithilfe von maschinellem Lernen und Analysen Benutzer, Anwendungen, Geräte und Inhalte eindeutig erkennt und neue Bedrohungen erfasst, die auf Fingerprinting und Signaturen basieren. PAN-OS aktualisiert kontinuierlich die Modelle für das maschinelle Lernen und ist daher beim Aufdecken von Phishing-angriffen besonders effektiv. Außerdem erfasst es Telemetriedaten, empfiehlt Richtlinien- und Konfigurationsänderungen zur Risikominimierung und trägt zur Reduzierung menschlicher Fehler bei. Unten sind die wichtigsten Funktionen von PAN-OS in Bezug auf das Zero-Trust-Prinzip in privaten Clouds beschrieben.

PAN-OS

FUNKTIONEN VON PAN-OS

User-ID

Validiert Benutzer, um mithilfe einer effektiven Authentifizierungsmethode sicherzustellen, ob es sich auch tatsächlich um legitime Anwender handelt.

Device-ID

Stellt die Integrität aller Workloads und Geräte im Netzwerk sicher, einschließlich IoT.

App-ID

Verhindert mithilfe von Least Privilege-Richtlinien den nicht autorisierten Zugriff.

Content-ID

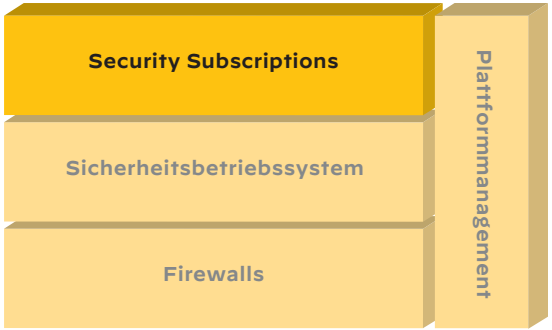
Schränkt die unbefugte Übertragung von Dateien und sensiblen Informationen ein, zum Beispiel Kreditkartendaten und Sozialversicherungsnummern.

Entschlüsselung

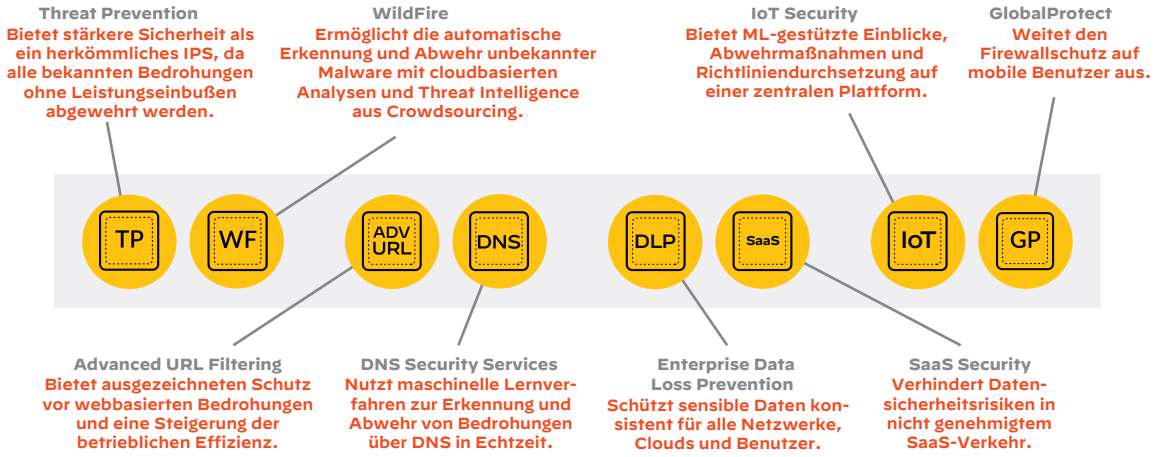
Prüft den gesamten Netzwerkverkehr auf schädliche Aktivitäten und Datendiebstahl.

Nächstes Kapitel: Über die Cloud bereitgestellte Security Services bieten einen flexiblen und kosteneffektiven Sicherheitsansatz.

Ebene 3: Über die Cloud bereitgestellte Security Subscriptions

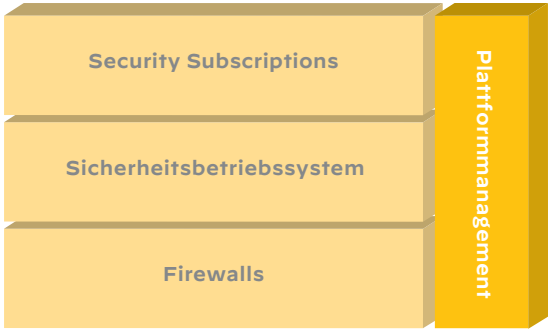


Eine einzigartige und effektive Funktion der virtuellen Software-NGFWs von Palo Alto Networks sind die über die Cloud bereitgestellten Security Services (Cloud-Delivered Security Services; CDSS). Dabei können Sie gezielt die Services auswählen, die Sie benötigen, und diese Auswahl jederzeit an neue Sicherheitsanforderungen anpassen. So haben Sie maximale Kontrolle über das Sicherheitsniveau und profitieren von einer beispiellosen Flexibilität, um auf Änderungen in der Bedrohungslandschaft zu reagieren.



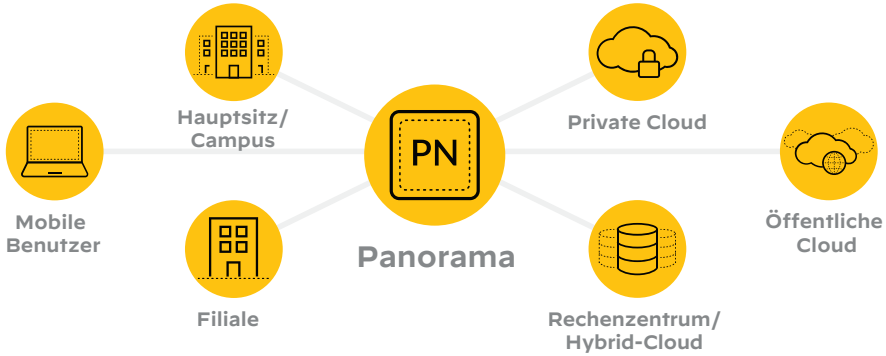
Nächstes Kapitel: Zentrale Managementfunktionen sind eine wichtige Voraussetzung für komplexe moderne Cloud-Architekturen.

Ebene 4: Zentrales Management mit Panorama



Viele große Unternehmen haben mehrere NGFWs in ihren Netzwerken implementiert, was die Verwaltung aufgrund der komplexen Konfigurationen und inkonsistenten Managementkonsolen sehr aufwendig macht. Das führt dazu, dass die Administrationskosten steigen und das Sicherheitsniveau sinkt.

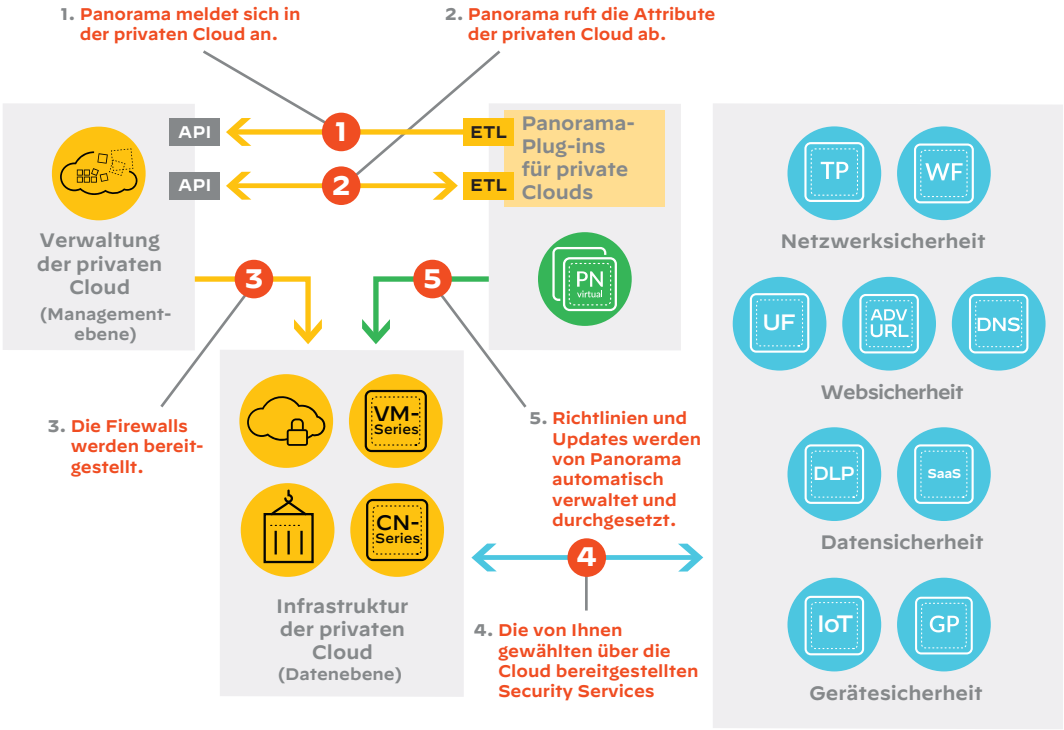
Panorama™ ermöglicht ein zentrales Management und einen umfassenden Überblick über alle Firewalls von Palo Alto Networks, unabhängig von deren Formfaktor oder Standort – von Firewalls am Perimeter und in Filialen bis zu Cloud-Umgebungen und Rechenzentren. Mit Panorama erhalten Administratoren Einblicke in Anwendungen, Benutzer, Geräte und Inhalte für den gesamten Netzwerkverkehr und alle Bedrohungen. Da das Firewallmanagement für das gesamte Netzwerk in einer zentralen Konsole stattfindet, kann zum einen der Zeitaufwand reduziert und zum anderen das Netzwerk effektiver geschützt werden.



Auf der nächsten Seite sehen Sie, wie die Netzwerksicherheitsplattform in der Praxis eingesetzt wird.

Die Plattform in der Praxis

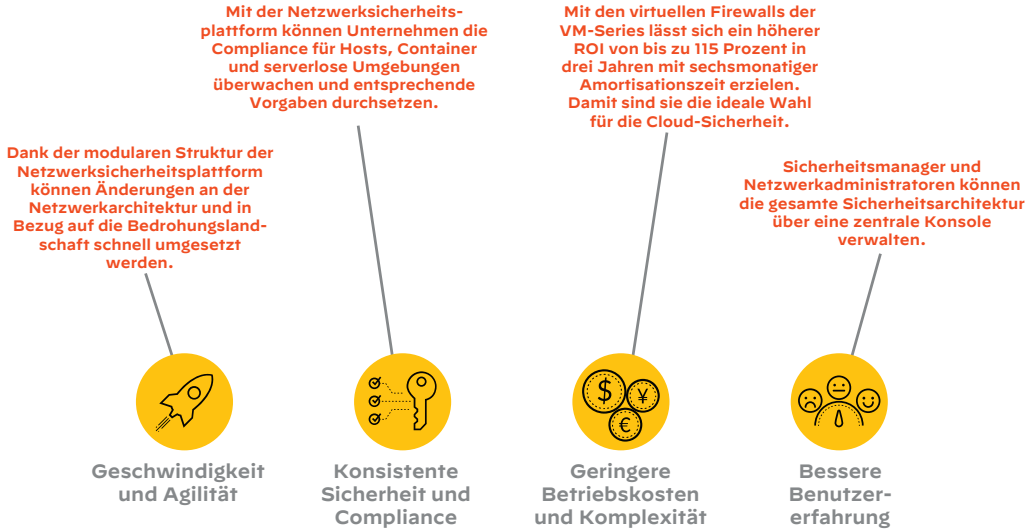
Die virtuellen Firewalls von Palo Alto Networks lassen sich nahtlos in einen Controller für private Clouds oder SDN-Orchestrator integrieren, um die Bereitstellung, Verwaltung und Aktualisierung aller Firewalls der VM-Series und CN-Series zu automatisieren. Dadurch sparen Sie Zeit beim Firewallmanagement und können aktuelle Richtlinien im gesamten Netzwerk konsistent durchsetzen.



Im nächsten Kapitel erfahren Sie mehr über die praxisrelevanten Vorteile der Netzwerksicherheitsplattform.

Die Plattform für einen größeren Mehrwert

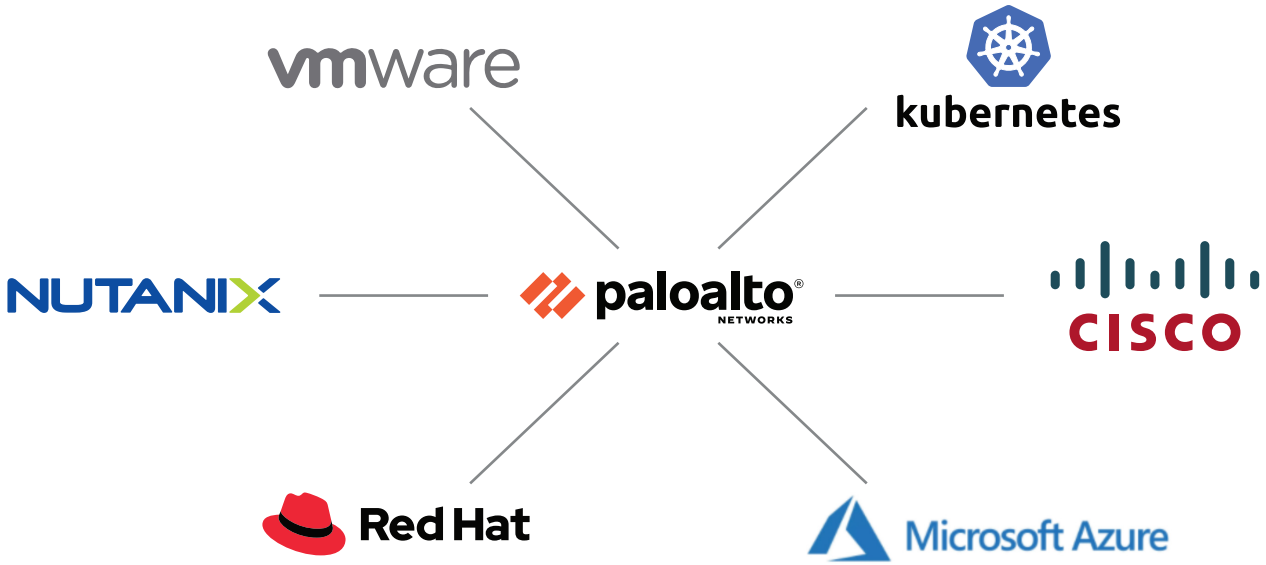
In diesem E-Book haben wir vor allem die Vorteile der Netzwerksicherheitsplattform für *private* Clouds beschrieben, aber sie eignet sich auch für öffentliche und hybride Clouds. Die Netzwerksicherheitsplattform unterstützt zahlreiche Anwendungsfälle in der Cloud und sorgt mit hoher Geschwindigkeit und Agilität für konsistente Sicherheit und Compliance, geringere Kosten und Komplexität sowie eine bessere Benutzererfahrung.



Unsere virtuellen Firewalls unterstützen diverse Virtualisierungssysteme – mehr dazu im nächsten Kapitel.

Integrationen für die wichtigsten Virtualisierungssysteme

Für eine private Cloud ist immer auch eine virtualisierte Umgebung erforderlich. Dazu stehen zahlreiche Virtualisierungssysteme zur Auswahl. Die Netzwerksicherheitsplattform von Palo Alto Networks unterstützt die Virtualisierungslösungen aller großen Anbieter.



Welche Schritte sich als Nächstes anbieten, erfahren Sie auf der folgenden Seite.

Bereiten Sie sich auf die Zukunft vor

Die Bedrohungen für private Clouds werden immer aggressiver, umfangreicher und komplexer. Der traditionelle Ansatz, bei dem ein Sicherheitsperimeter die Welt in vertrauenswürdige und nicht vertrauenswürdige Umgebungen teilt, ist für die modernen Hybrid-Cloud-Architekturen und cloudnativen Entwicklungsstrategien einfach nicht mehr angemessen. Effektive Cloud-Sicherheit lässt sich nur mit mehreren kleinen Perimetern und der Einführung des Zero-Trust-Prinzips erreichen.

Angesichts der Herausforderungen verteilter Architekturen, aggressiverer Bedrohungen und kürzerer Zeitfenster für die Bedrohungserkennung und -abwehr hat Palo Alto Networks die virtuellen NGFWs der VM-Series und die Container-NGFWs der CN-Series entwickelt – innovative Produkte, die effektive Sicherheitsmaßnahmen für private, öffentliche und hybride Clouds ermöglichen. Zusammen mit den physischen Firewalls der PA-Series bilden sie die Grundlage der Netzwerksicherheitsplattform, unseres innovativen und flexiblen Frameworks für die Cloud-Sicherheit.

Informieren Sie sich ganz unverbindlich über die Vorteile der Lösungen von Palo Alto Networks für Ihr Unternehmen – klicken Sie einfach auf die Kästchen unten. Private Clouds werden immer häufiger eingesetzt. Unternehmen, die in puncto Sicherheit bereits vorgesorgt haben, sind damit wettbewerbsfähiger und besser für zukünftige Innovationen gerüstet. Palo Alto Networks möchte Sie dabei als vertrauenswürdiger Sicherheitspartner unterstützen.

Für den Ultimate Test Drive anmelden

Persönliche Demo anfordern

VM-Series 30 Tage kostenlos testen

CN-Series QuikLabs testen

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