



Security der nächsten Generation

Wegweisende Sicherheits- plattform der Enterprise-Klasse für Netzwerk, Cloud und Endpunkte

Überzeugende Argumente

- Industrieweit einzigartige, hoch integrierte Security-Plattform
- Nahtloser Schutz für Netzwerk, Multi-Cloud und Endpunkt
- Physische Appliances mit optimierter Hardware
- Virtual Appliances für Private, Public und Hybrid Clouds
- Single-Pass-Analyse des gesamten Datenstroms – in Echtzeit
- SSL-Decryption und -Encryption
- Offen und skalierbar
- Zentrales Management

Das kalifornische Unternehmen Palo Alto Networks wurde im Jahr 2005 durch den Sicherheitsexperten Nir Zuk gegründet. Palo Alto Networks ist als weltweit führender Anbieter von Cybersicherheitslösungen dafür bekannt, den aktuellen Sicherheitsstand stets zu hinterfragen. Im Mittelpunkt der Entwicklung steht der erfolgreiche Schutz der Anwender vor Cyberattacken im digitalen Zeitalter. Auf die Sicherheitslösungen von Palo Alto Networks vertrauen Zehntausende Unternehmen und deren Kunden, öffentliche Verwaltungen und Organisationen. Die wegweisende Netzwerk-Sicherheits-Plattform schützt Anwender bei der digitalen Transformation durch kontinuierliche Innovation. Sie kombiniert die neuesten Erkenntnisse hinsichtlich Sicherheit, Automatisierung und Analyse unter einem ganzheitlichen Dach. Durch die Bereitstellung einer echten Plattform und die Förderung eines wachsenden Netzwerks von Security-Pionieren profitieren Kunden von hoch effizienten und innovativen Cybersicherheitslösungen für Clouds, Netzwerke und Endpunkte. Dank den innovativen Sicherheitslösungen ist es Palo Alto Networks gelungen, inert weniger Jahre zum schnellstwachsenden Hersteller von Security-Lösungen zu werden. Aktuell setzen über 75 000 Kunden aus unterschiedlichsten Branchen in 150 Ländern auf die Next Generation Security Platform von Palo Alto Networks. Über 85 Prozent der Fortune-100- und mehr als 65 Prozent der Global-2000-Unternehmen vertrauen Palo Alto Networks, wenn es um die Gewährleistung ihrer Cybersicherheit geht.

Umfassende Sicherheit für das ganze Unternehmen

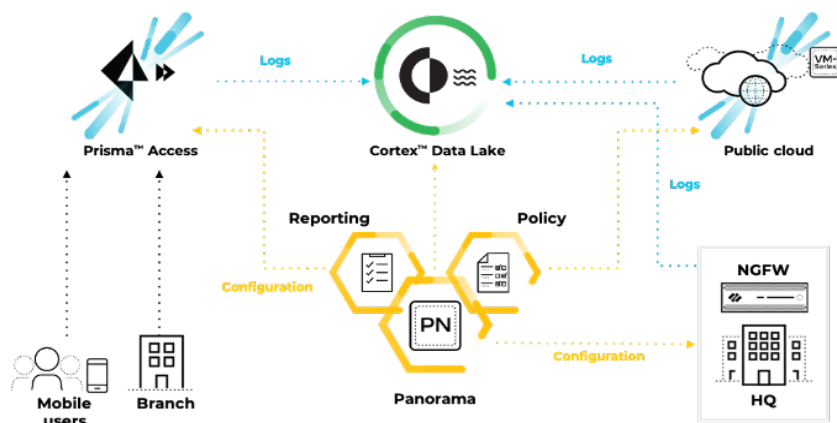
Die Next Generation Security Platform von Palo Alto Networks schützt das Unternehmensnetzwerk sowie sämtliche genutzten Cloud-Dienste – egal ob in der Private, Public oder Hybrid Cloud – und kümmert sich mithilfe von künstlicher Intelligenz automatisch um die Erkennung und Abwehr aller Arten von Cyberattacken

Secure the Enterprise: Strata Next Generation Firewall



Die Next Generation Firewall von Palo Alto Networks wurde von Grund auf neu entwickelt, um der beschränkten Wirksamkeit der alleinigen Kontrolle von IP-Adressen und Port-Nummern (Stateful Inspection) zu entgehen. Mit der Kombination von Benutzererkennung (User-ID), Applikationserkennung (App-ID), Inhaltskontrolle (Content-ID) und der neuen Geräteerkennung (Device-ID) lässt sich der Verkehr detailliert analysieren und regeln. Selbst verschlüsselter Verkehr kann entschlüsselt und überprüft werden, Verschleierungsmethoden werden so erkannt.

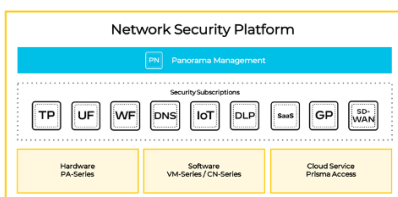
Die Next Generation Firewall steht als Appliance in verschiedenen Leistungsstufen sowie als integrierte Lösung in virtuellen Umgebungen wie VMware zur



Panorama Management ist die zentrale Plattform für Device, Policy und Change Management, Logging und Monitoring.

Verfügung. Alle Funktionen sind für alle Plattformen gleichermaßen verfügbar. Security Subscriptions sind für 1, 3 und 5 Jahre erhältlich. Threat Prevention, URL Filtering, WildFire Sandboxing, GlobalProtect für den Schutz mobiler Geräte, DNS Security, SD-WAN und Enterprise DLP stehen als ergänzende Subscriptions zur Wahl. IoT Security automatisiert die Orchestrierung des IoT Lifecycle und schützt vor Verwundbarkeiten und Bedrohungen.

Bei der VM-Series handelt es sich um eine virtualisierte Variante der Next Generation Firewall, die in vielen privaten und öffentlichen Cloud-Umgebungen eingesetzt werden kann – basierend auf Technologien von VMware, Cisco, KVM, OpenStack, Nutanix, Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud und Alibaba Cloud. Dabei stehen dieselben Security Services wie bei der Next-Generation-Firewall-Hardware zur Verfügung.



Secure the Cloud: Prisma

Prisma Cloud ist eine ganzheitliche, Cloud-native Sicherheitsplattform, die sowohl Funktionen für Cloud Security Posture Management (CSPM) als auch für Cloud Workload Protection (CWP) bietet. Anwendungen und Daten werden während des gesamten Anwendungslebenszyklus in Multi-Cloud- und Hybrid-Cloud-Umgebungen geschützt. Prisma Cloud deckt folgende Funktionsbereiche ab: Visibility, Compliance und Governance, Sicherheit für Host-, Container- und Serverless-Umgebungen, Web Application und API Security, Threat Detection, Identity-based Microsegmentation, IAM und Data Security.

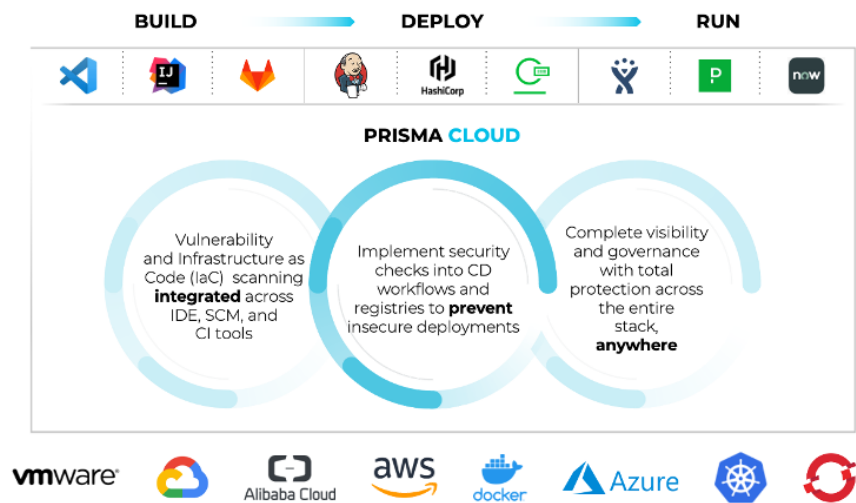
Prisma Access SASE (Secure Access Service Edge) gewährt allen Benutzern einen sicheren Zugang zu Anwendungen in der Cloud, im Rechenzentrum

und im Internet – unabhängig davon, ob der Zugriff aus einer Niederlassung, von unterwegs, vom Home Office oder am Hauptsitz erfolgt.

Mit **CloudGenix** steht ein Cloud-basiertes SD-WAN-Angebot zur Verfügung, das neben den klassischen Kriterien wie

Jitter, Packet Loss etc. auch die Verfügbarkeit der Applikation mit einbezieht.

Prisma SaaS gewährleistet als Cloud-basierter Cloud Access Security Broker (CASB) die sichere Nutzung von Anwendungen und Diensten aus der Cloud.



Secure the Future: Cortex

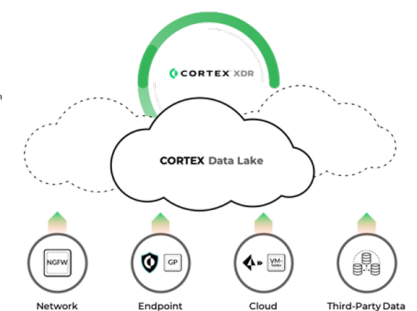
Cortex ist eine Plattform zur Erkennung, Abwehr und Automatisierung. Die Mission von Cortex ist dreiteilig: «Verhindere alles, was möglich ist, erkenne und untersuche schnell, was nicht verhindert werden kann, automatisiere die Reaktion und lerne mit jedem Incident.» Dabei werden modernste Technologien wie Machine Learning und KI eingesetzt.

Cortex XDR Prevent verhindert bekannte und unbekannte Endpunktbedrohungen. Cortex XDR Pro bietet zusätzlich automatisierte Untersuchung, regel- und verhaltensbasierte Analyse sowie integrierte Reaktion auf Sicherheitsvorfälle am Endpunkt.



Cortex XSOAR (Security Orchestration, Automation and Response) orchestriert und automatisiert die Prozesse im Security Operations Center. XSOAR integriert unzählige Datenquellen und nutzt standardisierte, automatisierte Playbooks für eine beschleunigte Analyse und Reaktion. Damit zielt XSOAR auf

die richtige Balance zwischen schneller maschineller Ausführung und abgestufter menschlicher Kontrolle. **Cortex Data Lake** als zentrales Repository sammelt, integriert und normalisiert Sicherheitsdaten aus Palo-Alto-Networks-Lösungen für Netzwerk, Cloud und Endpunkt sowie aus Logs von Drittanbietern.



Cyber Security neu gedacht

Kunden von Palo Alto Networks profitieren von hoch effizienten und innovativen Cybersicherheitslösungen für Clouds, Netzwerke und Endpunkte.

Next-Generation Threat Intelligence

Bedrohungsinformationen von Tausenden Geräten und Millionen Endpunkten, Threat-Feed-Anbietern und weiteren Partnern werden in der Threat Intelligence Cloud automatisch gesammelt, aggregiert und analysiert. Unit 42, das Threat-Research-Team von Palo Alto Networks, lernt aus diesen Daten, wie Angreifer ihre Methoden weiterentwickeln. Mit diesem Wissen werden neue Abwehrmassnahmen erarbeitet und in ert Minuten den Kunden zur Verfügung gestellt. Der hohe Automatisierungsgrad unterstützt Organisationen in der adäquaten Antwort auf moderne Bedrohungen und stoppt Angriffe ohne manuelle Intervention.

Zero Trust Network Access

Palo Alto Networks empfiehlt und unterstützt Zero Trust Network Access. ZTNA ist eine Strategie, die hilft, Datendiebstahl zu verhindern, indem in einer Organisation grundsätzlich kein Zugang ohne vorherige Überprüfung gewährt wird. Basierend auf dem Prinzip «Vertraue nie, prüfe immer» schützt ZTNA vor der Weiterverbreitung von Schadcode in Netzwerken.

Services von Palo Alto Networks

Palo Alto Networks bietet verschiedene Support und Professional Services an. Anwender haben die Wahl zwischen Premium oder Platinum Support, erbracht durch Palo Alto Networks oder durch lokale, autorisierte Support Center (ASC).

Support Services

Wenn jede Minute zählt, ist Verlass auf die schnelle Hilfe der Experten von Palo Alto Networks. Das weltweit verfügbare Supportteam und umfangreiche Ressourcen unterstützen Kunden dabei, Ausfälle zu vermeiden, Risiken zu minimieren und den IT-Betrieb zu optimieren.

Focused Services

Focused Services bieten massgeschneiderten Support durch einen dedizierten Kundenbetreuer. Mit diesen Services erhalten Anwender individuellen, persönlichen Support, wöchentliche Reviews, Ursachenanalyse bei kritischen Vorfällen, Unterstützung bei der Planung von Upgrades sowie quartalsweise Business Reviews.

