PRISMA CLOUD
BY PALO ALTO NETWORKS

Prisma Cloud: Überblick

Public Cloud Security Challenges

Der Bedarf, Anwendungen weltweit schnell zu entwickeln und bereitzustellen, hat zu einem rasanten Vormarsch der Public Cloud geführt. Das Sicherheits- und Compliancemanagement konnte in diesem Ausmaß trotz der Verfügbarkeit zahlreicher Tools und Technologien mit der Entwicklung nicht Schritt halten. Das sind die Gründe:

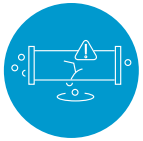
1. Traditionelle Sicherheitstools versagen in einer dynamischen Cloudumgebung, in der IP-Adressen sich ständig ändern. Darüber hinaus funktionieren Produkte auf Agent- oder Proxybasis nicht bei der riesigen Auswahl an API-gesteuerten Tools und Services, die Cloud-Provider bereitstellen.
2. Die Sichtbarkeit von Risiken wird durch punktuelle Lösungen fragmentiert, die Konfigurationsprobleme, Benutzeraktivitäten oder den Datenverkehr im Netzwerk isoliert behandeln. Eine effektive Risikobewertung setzt eine Korrelation über eine Vielzahl unterschiedlicher Datensätze hinweg voraus, um Probleme in ihren Kontext zu stellen. Diese muss durch maschinelles Lernen angetrieben werden.
3. Das Modell der gemeinsamen Verantwortung wird weiterhin schlecht verstanden. Auch wenn die Anbieter von Cloud-Dienstleistungen dafür verantwortlich sind, die physische Infrastruktur der Cloud zu sichern, liegt es in der Verantwortung von Unternehmen, ihre eigenen Netzwerke, Benutzer und Ressourcenkonfigurationen zu sichern. Multi-Cloud-Umgebungen werden zur Regel. Dadurch wird das effektive Sicherheitsmanagement zu einer Last, die sich nicht einfach durch den Einsatz von mehr Menschen lösen lässt.

Multi-Cloud-Sicherheit und Compliancemanagement neu definiert

Prisma™ Cloud (ehemals RedLock) ist ein Sicherheits- und Compliance-Service, der auf dynamische Art und Weise Cloudressourcen und sensible Daten entdeckt. In der Folge ermittelt der Dienst riskante Konfigurationen, Bedrohungen für das Netzwerk, verdächtiges Benutzerverhalten, Malware, Datenverlust und Host-Schwachstellen für GCP™, AWS® und Azure®. Public Cloud verbindet die umfassendste Sammlung regelbasierter Sicherheitsleitlinien mit branchenweit führendem maschinellem Lernen, um Bedrohungen aufzuspüren.

Highlights der Prisma Cloud

Hohe Transparenz von Cloud-Risiken: Einfach navigierbare SaaS-Nutzungs-Dashboards und detaillierte Berichte helfen dabei, Schatten-IT zu begrenzen. Entdecken Sie Risiken auf tieferen Ebenen mit vollständiger Transparenz aller Benutzer-, Ordner- und Dateiaktivitäten in SaaS-Anwendungen. Detaillierte Analysen helfen Ihnen, Richtlinienverstöße in Hinblick auf Datenrisiken oder Compliance rasch zu identifizieren



Datenschutz und Prävention von Datenverlust: Definieren Sie eine detaillierte, kontextsensible Richtlinienkontrolle, um die Durchsetzung zu verbessern sowie Benutzer und Daten bei Verstößen unter Quarantäne stellen zu können. Prisma SaaS kann Ihre Anwendungen durch die Klassifizierung und Überwachung von Daten durch maschinelles Lernen und eine hochentwickelte DLP-Engine schützen.

Detaillierte und adaptive Zugriffskontrolle: Einfach zu verwaltende Richtlinien geben Ihnen detaillierte Kontrolle über den Zugriff auf SaaS-Anwendungen. Sie können bestimmen, welche erlaubt sind und was akzeptables Verhalten innerhalb dieser darstellt. Auf diese Art können Sie den Zugriff für nicht erlaubte Anwendungen blockieren und gleichzeitig die Kontrolle über geduldete Anwendungen behalten.

Daten-Governance und Sicherstellung der Compliance: Sie können schnell und einfach gesetzliche Anforderungen rund um Datenrisiken, beispielsweise für GDPR-, PCI-, PII- oder PHI-Daten, erfüllen und die Vorteile Ihrer cloudbasierten Anwendungen weiter in vollem Umfang nutzen.

Überwachung des Nutzerverhaltens: Die heuristische Überwachung und Meldung des Benutzerverhaltens ermöglicht die Erkennung verdächtiger Verhaltensweisen wie Anmeldungen von unüblichen Standorten, ungewöhnlich umfangreiche Benutzeraktivität oder mehrfach fehlgeschlagene Anmeldungen, die auf den Diebstahl von Anmeldedaten hindeuten können.

Erweiterte Abwehr von Bedrohungen Blockieren Sie bekannte Malware und identifizieren und blockieren Sie unbekannte Malware innerhalb von SaaS-Anwendungen.

PRISMA CLOUD
BY PALO ALTO NETWORKS

Cloud Governance

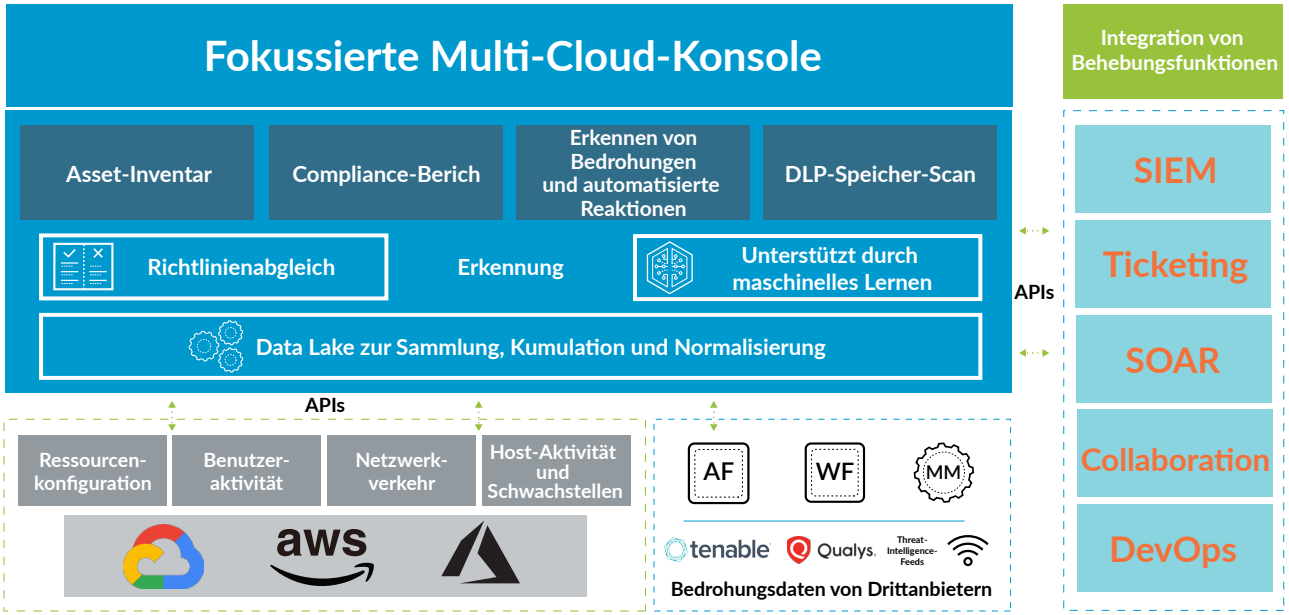
Die Gewährleistung von Compliance inmitten sich stetig wandelnder Cloudumgebungen ist für ohnehin bereits belastete Sicherheitsteams äußerst zeitaufwändig. Die Prisma™ Cloud vereinfacht die Compliance mit der branchenweit vollständigsten Bibliothek an Compliance-Richtlinien deutlich, darunter CIS, NIST, PCI DSS, HIPAA, GDPR, ISO, SOC 2 und weitere. Audit-geeignete Berichte für alle Compliance-Standards können mit nur einem Klick erstellt werden.

Auf moderne SOC ausgelegt

Security Operation Center (SOC) haben oft mit der Eindämmung, Abschwächung und Behebung von Risiken in dynamischen Cloudumgebungen zu tun. Prisma Cloud hilft SOCs durch maschinelles Lernen zur Risikobewertung, ihre Leistung zu steigern, indem Teams entscheiden können, worauf sie ihre Anstrengungen bevorzugt richten. Sie unterstützt auch die automatisierte Behebung, entweder direkt über die Benutzeroberfläche oder über die Integration mit Drittanbieter-Tools wie Angebote zum Security Information and Event Management (SIEM) sowie Security Orchestration, Automation and Response (SOAR).

Wie Prisma Cloud funktioniert

Durch kontinuierlichen Zufluss der Daten hunderter APIs von Cloud-Service-Providern sowie von Threat-Intelligence-Quellen erzeugt Prisma Cloud einen riesigen Data Lake. Sie wendet Analysen auf der Grundlage von Richtlinien und maschinellem Lernen an, um Assets zu entdecken und zu klassifizieren, auf Compliance- und Governance-Verstöße aufmerksam zu machen, verdächtige Aktivitäten zu entdecken und Datenrisiken zu identifizieren. Interaktive Bericht- und Untersuchungsfunktionen ermöglichen die rasche Abklärung von Vorfällen. Schließlich werden Probleme automatisch per API-Integration mit Ihren bevorzugten Tools oder direkt innerhalb der Prisma Cloud-Console behoben.



Für die Zukunft entwickelt

Wo auch immer Sie sich auf Ihrem Weg in die Cloud befinden, Prisma kann helfen:

- Cloud-fähige mobile Belegschaft
- Über die Cloud verbundene Zweigstellen
- Zero Trust Cloud-Sicherheit
- Cloud-Governance und Cloud-Compliance
- Schutz von Daten in der Cloud
- Schutz vor Bedrohungen in der Cloud
- Sichere DevOps