PRISMA CLOUD
BY PALO ALTO NETWORKS

Prisma Cloud für Amazon Web Services

Schützen Sie alle Ressourcen in Ihrer AWS-Umgebung mit Prisma Cloud

Vorteile von Prisma Cloud für AWS

- Visualisierung aller verbundenen Ressourcen in Ihrer gesamten AWS-Umgebung
- Sicherstellung andauernder Compliance und einfache Erstellung von Berichten in Ihrer AWS-Umgebung.
- Sichere DevOps durch Aufstellen von Sicherheitsmaßnahmen mit Echtzeitüberwachung, um Bedrohungen, wie zum Beispiel bedenkliche Konfigurationen, vertrauliche Benutzeraktivitäten, unbefugten Netzzugang und Host-Schwachstellen zu finden.
- Verwendung von Funktionen zum Auffinden von Anomalien, um die Beeinträchtigung von Accounts und Insider-Bedrohungen zu verhindern
- Untersuchung von aktuellen Bedrohungen oder früheren Vorfällen und schnelle Bestimmung der Grundursachen
- Kontextbezogene Benachrichtigungen, sodass Ihr Team Vorfälle priorisieren und schnell reagieren kann
- Nahtlose Integration mit Amazon GuardDuty.

Prisma Cloud vereinfacht die Gefahrenabwehr in der Cloud für AWS

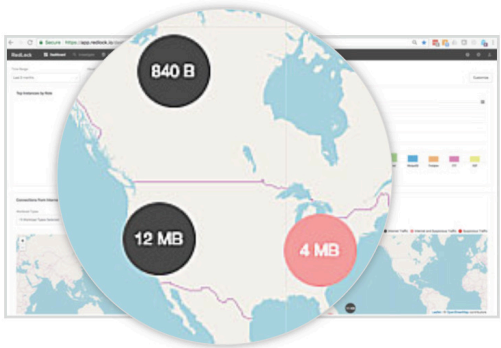
Die Anzahl der Einsätze beim Public Cloud Computing übersteigt mittlerweile die Cybersicherheitsabwehr. Das Fehlen einer physischen Netzwerkgrenze zum Internet, das Risiko versehentlicher Veröffentlichungen durch unerfahrene Benutzer, die dezentrale Sichtbarkeit und die dynamische Beschaffenheit der Cloud vergrößern die vorhandene Angriffsfläche deutlich. Auch wenn man mit einzelnen Sicherheitslösungen bestimmte Herausforderungen bewältigen kann, bieten diese dennoch keinen ganzheitlichen Schutz in einer Umgebung, in der die Ressourcen sich ständig ändern, wie dies bei Amazon Web Services der Fall ist.

Prisma™ Cloud (ehemals RedLock) ist ein Cloudsicherheits- und Compliance-Service, der auf dynamische Art und Weise Änderungen der Ressourcen entdeckt und fortlaufend Rohdatenquellen korreliert, einschließlich Benutzeraktivitäten, Ressourcenkonfigurationen, Netzdatenverkehr, Bedrohungsdaten und Sicherheitslücken. So entsteht ein vollständiger Überblick über Risiken in der Public Cloud. Durch einen innovativen, maschinell lernenden Ansatz können Organisationen durch Prisma Risiken schnell priorisieren, ihre agile Entwicklung beibehalten und ihren Verpflichtungen gemäß dem Modell der gemeinsamen Verantwortung nachkommen.

Hauptmerkmale und Vorteile bei der Absicherung von AWS

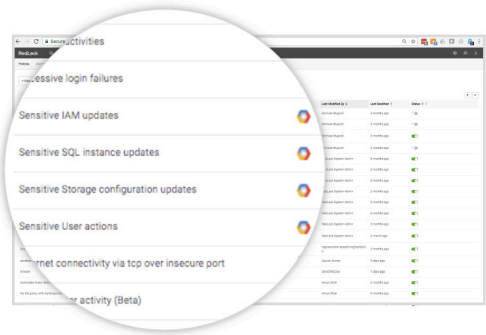
Unübertroffene Übersicht

Visualisieren Sie Ihre gesamte AWS®-Umgebung, bis hin zu jeder einzelnen Komponente. Prisma Cloud findet Cloud-Ressourcen und -Anwendungen durch das fortlaufende Korrelieren von Konfigurationen, Benutzeraktivitäten und Netzdatenverkehr. Durch die Verbindung dieses umfassenden Verständnis der AWS-Umgebung mit Daten aus externen Quellen, wie zum Beispiel Feeds über Bedrohungsdaten und Scanner für Sicherheitslücken, kann Prisma einen vollständigen Kontext für jedes Risiko bereitstellen.



Vereinfachte Cloud-Compliance

Prisma Cloud enthält vorgefertigte Richtlinien, die den Best Practices von Industriestandards entsprechen, beispielsweise CIS, DSGVO, NIST, SOC 2 und PCI. Zusätzlich können Sie individuelle Richtlinien erstellen, die den Anforderungen Ihrer Organisation entsprechen. Prisma prüft ständig auf allen verbundenen Ressourcen, ob Verstöße gegen Richtlinien vorliegen und unterstützt One-Click-Reports zum vereinfachten Prüfen Ihrer AWS-Umgebung.

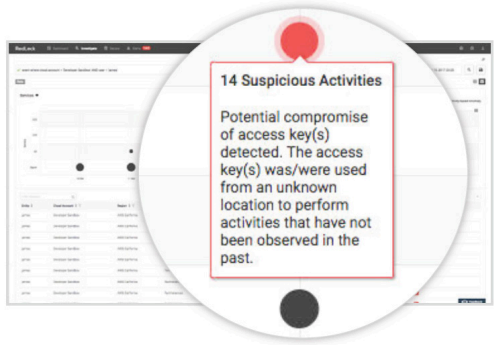


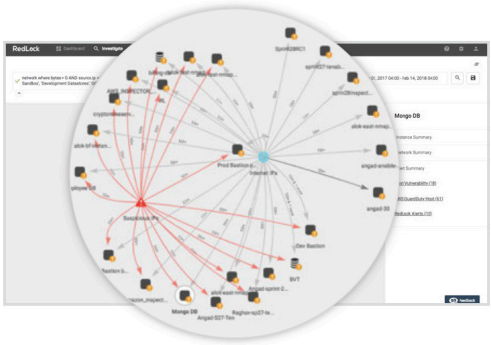
Sicherung von Richtlinien

Mit Prisma Cloud können Sie Sicherheitsmaßnahmen für DevOps erstellen. So können Sie Ihre agile Entwicklung beibehalten, ohne bei der Sicherheit Kompromisse einzugehen. Sie können so Bedrohungen, einschließlich riskanter Konfigurationen, vertraulicher Benutzeraktivitäten, unbefugtem Netzzugang und Host-Schwachstellen, schnell entdecken. Prisma erstellt automatisch Risikoeinstufungen für jede Ressource. Diese basieren auf den Auswirkungen auf das Unternehmensrisiko, Verstößen und Anomalien. SecOps können so schnell die riskantesten Ressourcen identifizieren und die Mängelbeseitigung dementsprechend priorisieren.

Erkennung von Bedrohungen

Prisma Cloud entdeckt automatisch Anomalien im Benutzerverhalten und anderem Verhalten in Ihrer AWS-Umgebung, erstellt Referenzwerte für das Verhalten und markiert jede Abweichung davon. Beispielsweise wird ein potentieller Accesskey-Verstoß markiert, wenn ein Benutzer versucht, in kurzem zeitlichen Abstand von zwei verschiedenen Standorten aus Accesskeys zu verwenden und dies geographisch nicht möglich ist.



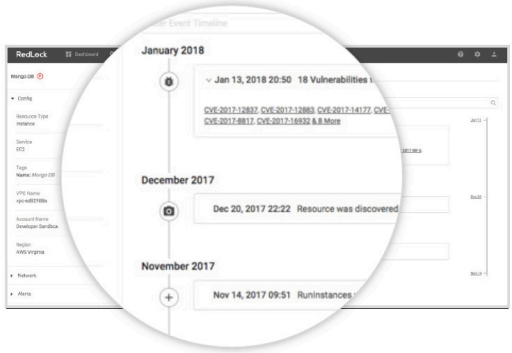


Untersuchung von Vorfällen

Durch das umfassende Verständnis der AWS-Umgebung beträgt die Untersuchungszeit bei Prisma Cloud nur Sekunden. So können Sie Probleme schnell bestimmen, Upstream- und Downstream-Wirkungsanalysen durchführen und den Änderungsverlauf einer Ressource überprüfen, um ein besseres Verständnis für die Ursache eines Vorfalls zu erlangen. Beispielsweise können Sie eine Abfrage starten, die alle Datenbanken findet, die im letzten Monat direkt mit dem Internet kommuniziert haben. Die daraus entstehende Karte findet alle diese Fälle und hebt die Ressourcen hervor, die möglicherweise beeinträchtigt wurden. In diesem Fall kommunizieren sie mit einer bekannten verdächtigen IP-Adresse.

Kontextbezogene Warnungen und adaptive Reaktionen

Mit Prisma Cloud kann Ihr Team dank kontextbezogener Warnungen schnell auf Probleme reagieren. Diese Warnungen, die basierend auf einer zum Patent angemeldeten Risikobewertungsmethode ausgelöst werden, liefern den Kontext zu allen Risikofaktoren einer Ressource. So wird es einfacher, die wichtigsten Probleme zuerst zu beheben. Sie können Warnungen senden, Strategien abstimmen oder eine automatische Behebung durchführen. Sie können die Warnungen außerdem an Tools wie Slack®, Splunk® und unser eigenes Tool Demisto® senden, damit Probleme behoben werden. Im Falle gefährdeter Datenbanken erstellt Prisma eine kontextbasierte Warnung, die Informationen über die Risikofaktoren enthält und löst damit eine automatische Reaktion aus.



Integration mit Amazon GuardDuty

Die kontextbezogene und durch maschinelles Lernen unterstützte Sicherheits- und Compliance-Überwachung von Prisma Cloud lässt sich nativ mit Amazon GuardDuty® integrieren und liefert so eine dauerhafte Überwachung von schädlichem oder unautorisiertem Verhalten in Ihrer gesamten AWS-Umgebung. So finden Sie Aktivitäten wie ungewöhnliche API-Aufrufe oder potentiell unautorisierte Bereitstellungen, die auf eine mögliche Beeinträchtigung Ihres Accounts hinweisen, einschließlich potentiell beeinträchtigter Vorgänge oder Auskundschaftung durch Angreifer.

Entwickeln eines Plans zur Cloud-Gefahrenabwehr für AWS

Mit Prisma Cloud können Sie ein Gefahrenabwehrprogramm für Ihre Cloud in der gesamten AWS-Umgebung entwickeln – von Anfang bis Ende und mit den folgenden Funktionen:

- **Sicherstellung der Compliance:** Das Anpassen der Cloudressourcen-Konfiguration an Compliance-Richtlinien wie CIS, DSGVO, PCI und HIPAA kann sehr viel Zeit in Anspruch nehmen. Mit vorgefertigten Richtlinien ermöglicht Prisma eine dauerhafte Überwachung, automatische Behebung und One-Click-Reports und vereinfacht somit das Einhalten der Compliance.
- **Sicherheitsmanagement:** Unvollständige Sichtbarkeit und ungenaue Kontrollen über Änderungen in dynamischen Public-Cloud-Computerumgebungen erschweren das Sicherheitsmanagement. Prisma Cloud ermöglicht die Validierung von Architekturen durch die Sicherung von Richtlinien, sodass Risiken bei den Ressourcenkonfigurationen, der Netzwerkarchitektur und den Benutzeraktivitäten erfasst und automatisch behoben werden können. Mit Prisma ist die Unterstützung der DevOps-Agilität gegeben, ohne dass dabei die Sicherheit beeinträchtigt wird.
- **SOC-Tauglichkeit:** Mitarbeiter für Sicherheitsmaßnahmen werden geradezu mit Warnungen überflutet, die nur wenig Kontext über die Probleme enthalten, sodass die zeitige Sichtung aller Warnungen zum Problem wird. Prisma vereinfacht die Identifizierung von Schwachstellen, erfasst Bedrohungen, untersucht aktuelle oder frühere Vorfälle und behebt innerhalb von Minuten Probleme in Ihrer gesamten AWS-Umgebung.

Schritt 1: Einführung	Schritt 2: Erweiterung	Schritt 3: Skalierung
Cloud Footprint: • Dutzende Aufgaben • Wenige Cloud-Accounts	**Cloud Footprint:** • Hunderte Aufgaben • Viele Cloud-Accounts	**Cloud Footprint:** • Mehrere Cloud-Provider • Tausende Aufgaben • Dutzende Cloud-Accounts
Objectives: • Sicherstellung der Compliance • Sicherheitsmanagement	**Objectives:** • Zentrale Übersicht • Erkennung von Bedrohungen • Verwaltung von Schwachstellen **+ Ziele aus Schritt 1**	**Objectives:** • Automatische Behebung • Untersuchung von Vorfällen **+ Ziele aus Schritt 2**

Abbildung 1: Reifegradmodell der Gefahrenabwehr für die Cloud

Prisma Cloud Security Suite

Prisma Cloud bietet ausführliche Übersichten, die Erkennung von Bedrohungen und schnelle Reaktionen in Ihrer gesamten öffentlichen Cloud-Umgebung, einschließlich Google Cloud Platform (GCP™), AWS und Microsoft Azure®. Durch die einzigartige Kombination aus ständiger Überwachung, Sicherstellung der Compliance und Sicherheitsanalysen können Mitarbeiter, die für die Sicherheit zuständig sind, schneller auf die schwerwiegendsten Bedrohungen reagieren, indem manuelle Untersuchungen durch automatisierte Berichte, Priorisierung von Bedrohungen und Behebung ersetzt werden. Mit dem auf API basierenden Ansatz sorgt Prisma für cloud-native Sicherheit.

PRISMA CLOUD
BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Zentrale: +1.408.753.4000
Vertrieb: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com