Vorteile von Prisma Cloud für GCP

Schützen Sie alle Ressourcen in Ihrer Google Cloud Platform-Umgebung mit Prisma Cloud

Benefits of Prisma Cloud for GCP

- Visualisierung aller verbundenen Ressourcen in Ihrer GCP-Umgebung
- Sicherstellung andauernder Compliance und einfache Erstellung von Berichten in Ihrer GCP-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 nativen GCP-Diensten, einschließlich Cloud Security Command Center

Prisma Cloud vereinfacht die Gefahrenabwehr in der Cloud für GCP

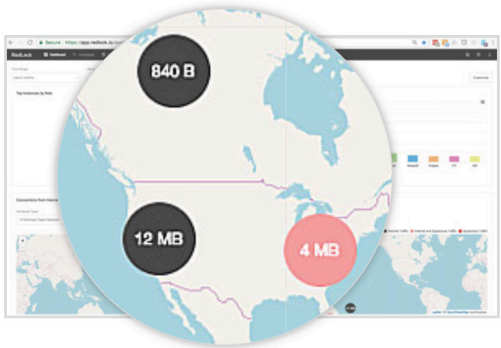
Die Anzahl der Einsätze beim Public Cloud Computing übersteigt mittlerweile die Cybersicherheitsabwehr. Das Fehlen einer physischen Netzwerkgrenze zum Internet, das Risiko versehentlicher Veröffentlichungen durch unerfahrene Benutzer, die dezentrale Sichtbarkeit und die dynamische Beschaffenheit der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

Prisma™ Cloud (ehemals RedLock) ist ein Cloudsicherheits- und Compliance-Service, der 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 GCP

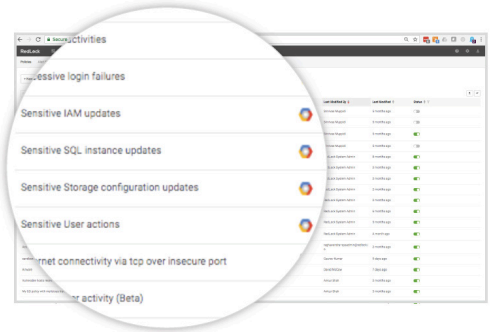
Unübertroffene Übersicht

Visualisieren Sie Ihre gesamte Google Cloud Platform (GCP™)-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 GCP-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 GCP-Umgebung.

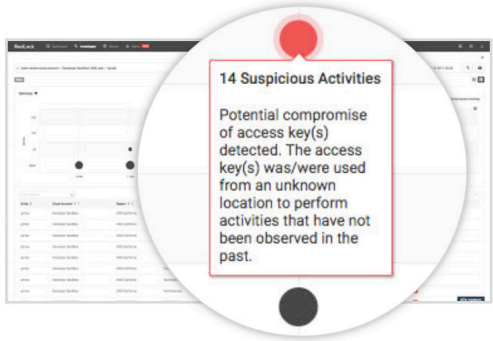


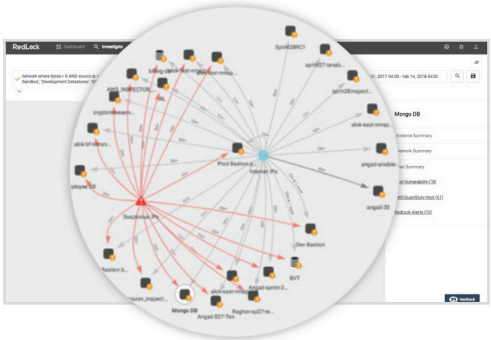
Sicherung von Richtlinien

Mit Prisma Cloud können Sie Sicherheitsmaßnahmen für DevOps erstellen. So können Sie Ihre agile Entwicklung beibehalten, ohne bei der Sicherheit Kompromisse einzugehen. Sie können 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

PPrisma Cloud entdeckt automatisch Anomalien im Benutzerverhalten und anderem Verhalten in Ihrer GCP-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.



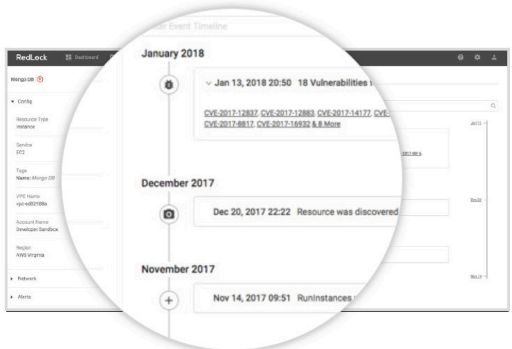


Untersuchung von Vorfällen

Durch das umfassende Verständnis der GCP-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.

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 Cloud Security Command Center

Prisma Cloud kann in Googles Cloud Security Command Center integriert werden und Ihnen somit eine Übersicht über Sicherheits- und Compliance-Risiken in Ihrer gesamten GCP-Umgebung zur Verfügung stellen. So können die Mitarbeiter, die für die Sicherheit zuständig sind, schnell Daten erfassen, Bedrohungen identifizieren und handeln, bevor geschäftliche Schäden oder Verluste auftreten.

Entwickeln eines Plans zur Cloud-Gefahrenabwehr für GCP

Mit Prisma können Sie ein Gefahrenabwehrprogramm für Ihre Cloud in der gesamten GCP-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 DSS 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 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-Agility gegeben, ohne dass dabei die Sicherheit beeinträchtigt wird.
- **SOC-Tauglichkeit:** Mitarbeiter für Sicherheitsmaßnahmen werden geradezu mit Warnungen überflutet, die nur wenig Kontext zu Problemen enthalten, sodass die zeitige Sichtung all dieser Warnungen zum Problem wird. Prisma vereinfacht die Identifizierung von Schwachstellen, erfasst Bedrohungen, untersucht aktuelle oder frühere Vorfälle und behebt diese Probleme innerhalb von Minuten in Ihrer gesamten GCP-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
Ziele: • Sicherstellung der Compliance • Sicherheitsmanagement	**Ziele:** • Zentrale Übersicht • Erkennung von Bedrohungen • Verwaltung von Schwachstellen **+ Ziele aus Schritt 1**	**Ziele:** • Automatische Behebung • Untersuchung von Vorfällen **+ Ziele aus Schritt 1**

Prisma Cloud Security Suite

Abbildung 1: Reifegradmodell der Gefahrenabwehr für die Cloud

Prisma Cloud bietet eine ausführliche Übersicht, Erkennung von Bedrohungen und schnelle Reaktionen in Ihren Public-Cloud-Umgebungen, einschließlich Google Cloud Platform, Amazon Web Services (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 ist Teil der Palo Alto Networks Security Operating Platform® und unterstützt Organisationen mit einem multidimensionalen Ansatz zur Public-Cloud-Sicherheit durch Inline-, API- und Host-basierte Schutztechnologien, die zur Minimierung der Angriffsmöglichkeiten ineinandergreifen.

Mit der Security Operating Platform wird der Schutz auf Ihr gesamtes Netzwerk erweitert. Der umfassende Schutz gilt unabhängig von Ihrem Standort. Ganz gleich, ob sich Ihre Anwendungen vor Ort befinden oder virtualisiert werden und damit Schutz in einer privaten Cloud wie VMware NSX®, Cisco ACI®, KVM oder OpenStack® erfordern, ob sie in eine Public-Cloud ausgelagert sind oder in einer SaaS-Anwendung liegen: Wir können Ihre Daten schützen.

Erfahren Sie mehr auf unserer Website: www.paloaltonetworks.com.

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