Prisma Cloud
Lösungsüberblick

Anwendungssicherung vom Code bis zur Cloud

Prisma® Cloud ist eine cloudnative Plattform für den Anwendungsschutz (CNAPP), die zur Sicherung von Anwendungen in öffentlichen, privaten, Hybrid- und Multi-Cloud-Umgebungen geeignet ist. Im Gegensatz zu einer aus Punktlösungen bestehenden Infrastruktur bietet Prisma Cloud mit einer einzigen Plattform, in die ein breites Spektrum von Sicherheitsfunktionen integriert wurde, branchenführenden Schutz. Zu den Vorteilen dieses Ansatzes gehören ein reduziertes Risiko, eine geringere Anzahl von erfolgreichen Angriffen, bessere Zusammenarbeit zwischen Entwickler- und Sicherheitsteams, effizientere Arbeitsabläufe sowie eine verbesserte Compliance und ein höheres Sicherheitsniveau.

Risiko-prävention

Verhindern Sie, dass Risiken und Fehlkonfigurationen in die Produktion gelangen.

Transparenz und Kontrolle

Etablieren Sie kontinuierliche Transparenz und Kontrolle über Ihre Cloud-Umgebung.

Laufzeit-schutz

Profitieren Sie von Echtzeitschutz für Cloud-Workloads, Webanwendungen und APIs.

Abbildung 1: Code to Cloud™ – der einheitliche Ansatz von Prisma Cloud

Anwendungsbereiche für Prisma Cloud

Risikoprävention

Shift-Left-Ansatz und von Haus aus sichere Anwendungen: Prisma Cloud kann in Technologieökosysteme integriert werden, um zu verhindern, dass riskante oder falsch konfigurierte Anwendungen in die Produktion gelangen. Dazu bietet es:

- **Infrastructure-as-Code(IaC)-Sicherheit:** Identifizieren und beheben Sie Fehlkonfigurationen in Terraform, CloudFormation, ARM, Kubernetes und anderen IaC-Vorlagen.
- **Schutz von Secrets:** Finden und sichern Sie ungeschützte und gefährdete Secrets in allen Dateien Ihrer Repositorys und CI/CD-Pipelines.
- **CI/CD-Sicherheit:** Stärken Sie Ihre CI/CD-Pipelines, reduzieren Sie Ihre Angriffsfläche und schützen Sie Ihre Anwendungsentwicklungsumgebung.
- **Software Composition Analysis (SCA):** Beheben Sie Sicherheitslücken in Open-Source-Software und Verstöße gegen die Lizenzcompliance – mit kontextbasierter Priorisierung.

Transparenz und Kontrolle

Verschaffen Sie sich eine kontinuierliche Übersicht und die Kontrolle über Fehlkonfigurationen, das Identitäts- und Zugriffsmanagement, Daten, Schwachstellen und API-Endpunkte in all Ihren Cloud-Umgebungen. Prisma Cloud sichert Cloud-Infrastrukturen mit:

- **Management des Cloud-Sicherheitsniveaus (CSPM):** Überwachen Sie Ihr Sicherheitsniveau, erkennen und beheben Sie Bedrohungen und sorgen Sie für Compliance.
- **Management der Infrastrukturzugriffsrechte in der Cloud (CIEM):** Übernehmen Sie die Kontrolle über Berechtigungen in Multi-Cloud-Umgebungen.
- **Agentenlose Workload-Scans:** Durchkämmen Sie Hosts, Container, Kubernetes- und serverlose Anwendungen nach Schwachstellen und Bedrohungen.
- **Datensicherheit in der Cloud:** Identifizieren Sie sensible Daten und durchkämmen Sie öffentliche Cloud-Speicher nach Malware.
- **API-Transparenz:** Nutzen Sie diese Funktion zur Erkennung, Profilerstellung und Sicherung der APIs in all Ihren cloudnativen Anwendungen.
- **Cloud Discovery and Exposure Management (CDEM):** Verschaffen Sie sich eine bessere Übersicht und Kontrolle über Ihren IT-Teams unbekannte und andere nicht verwaltete Cloud-Assets, die über das Internet zugänglich sind.

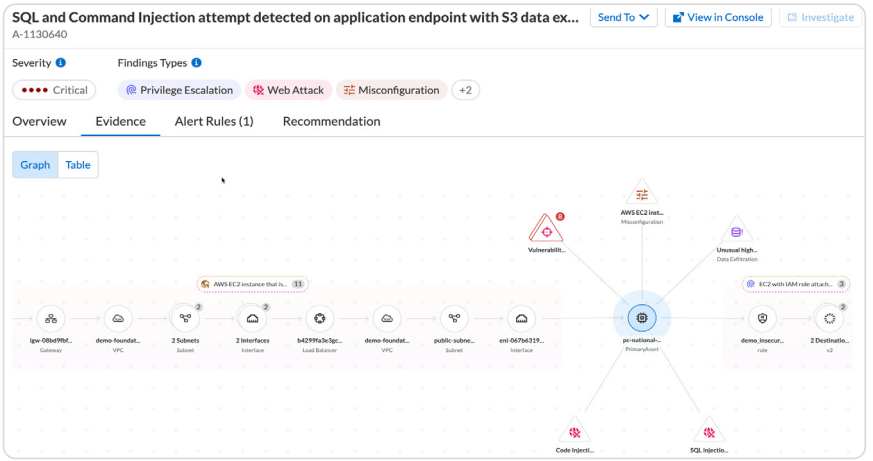

Abbildung 2: Angriffspfadanalyse

Prisma Cloud
Lösungsüberblick

Laufzeitschutz

Blockieren Sie Angriffe während der Laufzeit mit Prisma Cloud. Diese Plattform schützt Anwendungen in öffentlichen und privaten Clouds mit:

- **Erkennung von Cloud-Bedrohungen:** Erkennen Sie komplexe Bedrohungen, Zero-Day-Angriffe und Anomalien in Multi-Cloud-Umgebungen.
- **Hostsicherheit:** Schützen Sie VMs in öffentlichen und privaten Clouds.
- **Containersicherheit:** Schützen Sie Container und Kubernetes-Plattformen in allen öffentlichen und privaten Clouds.
- **Sicherheit in serverlosen Architekturen:** Schützen Sie serverlose Funktionen über den gesamten Anwendungslebenszyklus hinweg.
- **Schutz von Webanwendungen und APIs:** Schützen Sie Webanwendungen und APIs in öffentlichen und privaten Clouds.

Code-to-Cloud-Kontextinformationen

Unser einzigartiger Ansatz basiert auf Code-to-Cloud-Kontextinformationen. Dafür werden Daten aus allen Phasen des Anwendungslebenszyklus, von der Entwicklung bis zur Laufzeit, miteinander verknüpft, um Risiken zu minimieren und Angriffe zu verhindern. Prisma Cloud setzt Alarme in ihren Kontext, priorisiert kritische Risiken und bietet geeignete Gegenmaßnahmen an.

Transparenz vom Code bis zur Cloud

Sorgen Sie für umfassende Sicherheitstransparenz über alle Entwicklungs- und Cloud-Umgebungen hinweg.

Anwendungs-kontext

Priorisieren Sie Risiken mithilfe eines vollständigen Anwendungsinventars.

Angriffspfad-analyse

Decken Sie miteinander verbundene Schwächen auf und isolieren Sie ausnutzbare Angriffsvektoren.

Gegenmaßnahmen vom Code bis in die Cloud

Machen Sie Schwachstellen in der Cloud sofort unschädlich und verfolgen Sie sie bis zum Quellcode zurück, um sie endgültig zu beheben.

Abbildung 3: Code-to-Cloud-Kontextinformationen

„Palo Alto Networks macht uns die Arbeit leichter. Die Integration erfolgt nahtlos, wir erhalten vollständige Transparenz und die Automatisierungsfunktionen übernehmen den Großteil der Überwachungsaufgaben. Auch unsere Ressourcen werden dadurch nicht beeinträchtigt."

– Oussama Benzaouia, CISO, Teads

Lesen Sie die ganze Fallstudie.

„Das Portfolio von Palo Alto Networks ist in jeder Hinsicht gut durchdacht. Statt einer ganzen Sammlung von Punktlösungen haben wir eine Suite von Best Practices und erwiesenermaßen effektiven, miteinander verbundenen Sicherheitstechnologien. Unser Team kann sich auf wertschöpfende Aufgaben konzentrieren, weil wir wissen, dass die geschäftskritischen Sicherheitsprozesse im Hintergrund laufen und unsere neue digitale Infrastruktur schützen."

– Bob Bowden, Security Architect, Registers of Scotland

Lesen Sie die ganze Fallstudie.