Das beste Sicherheitslevel in der Cloud

Umfassende Sicherheit für die zunehmend komplexer werdenden Multi-Cloud-Umgebungen lässt sich mit herkömmlichen Security-Mitteln nicht erreichen. Mit Prisma Cloud von Palo Alto Networks steht nun eine wegweisende cloudnative Sicherheitsplattform mit zentraler Verwaltung für jedes denkbare Cloud-Netzwerk zur Verfügung.

Cloud-Workloads erfahren eine stetige Zunahme. Gleichzeitig steigt die Komplexität von Cloud-Umgebungen kontinuierlich an, und Entwicklungs- und Anwendungszyklen werden kürzer. Folglich wächst auch die Verantwortung der einzelnen Organisationen, ihre digitalen Assets zu schützen. Der wirkungsvollste Ansatz zur Steigerung der Sicherheit von Cloud-Netzwerken vereint Faktoren wie Prävention und Transparenz.

Prisma Cloud von Palo Alto Networks ist eine umfassende cloudnative Sicherheitsplattform (CNSP), die Anwendungen, Daten und Technologien wie Container mit branchenführenden Sicherheits- und Compliance-Funktionen während des gesamten Lebenszyklus in Multi-Cloud-Umgebungen schützt. Dazu baut Prisma Cloud auf fünf Pfeiler: Management des Cloud-Sicherheitsniveaus (CSPM), Schutz für Cloud-Workloads (CWPP), Management der Infrastruktur-Zugriffsrechte (CIEM), Netzwerksicherheit (CNS) sowie DevSecOps- und Shift-Left-Sicherheit.

CSPM: Cloud-Sicherheitsniveau managen

Eine effektive Cloud-Sicherheit erfordert einen kompletten Überblick über alle verwendeten Ressourcen aller genutzten Cloud-Anbieter. Ein vollständiges Inventar bildet dabei die Basis für die Verwaltung des Cloud-Sicherheitsniveaus. Das CSPM-Modul von Prisma Cloud überwacht und protokolliert die Ressourcen in puncto Konfiguration und Compliance. Dazu analysiert und normalisiert die Lösung Log- und Audit-Daten aus den unterschiedlichsten Cloud-Datenquellen.

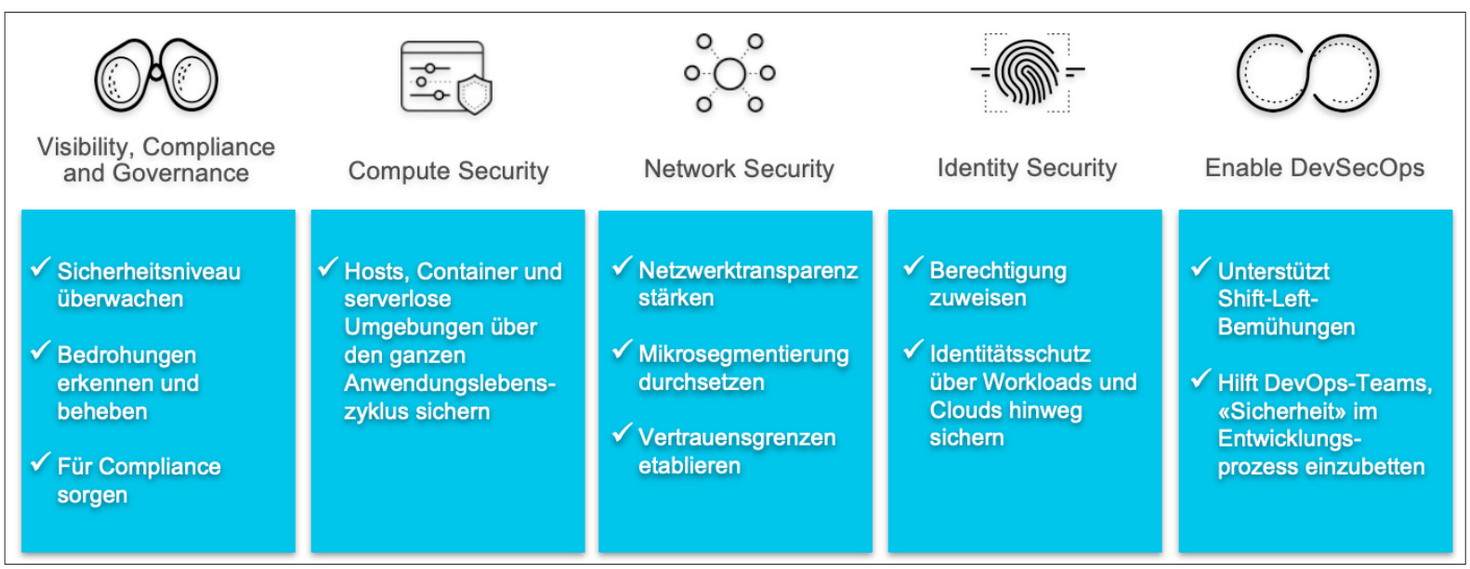
Durch die Analyse von Anwender- und Objektverhalten, kombiniert mit der Überwachung von Workloads und Netzwerken, werden verdächtige Aktivitäten erkannt. Die so gewonnenen Insights werden – unterstützt durch maschinelles Lernen – miteinander verknüpft und bewertet. So werden Risiken und Sicherheitsprobleme der genutzten Ressourcen zentral ersichtlich. Prisma Cloud unterstützt Security-Verantwortliche beim Beheben dieser Probleme, indem es Vorschläge macht und die nötigen Massnahmen anhand von Vorgaben teilweise vollautomatisch umsetzt.

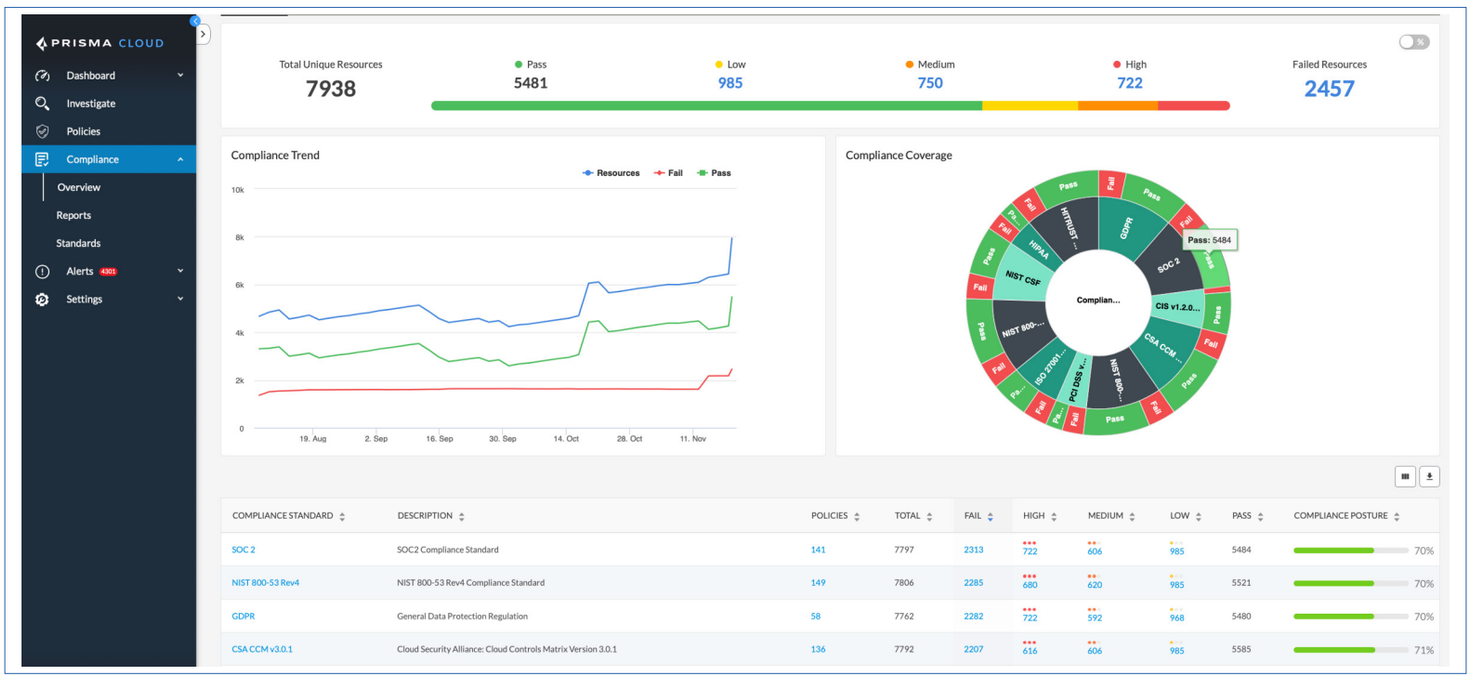
CWPP: Cloud-Workloads schützen

Unternehmen haben heute eine breite Palette an Tools und Technologien zur Verfügung, um ihre Workloads in der Cloud zu betreiben und moderne Anwendungen bereitzustellen. Oft wird dazu eine Kombination von virtuellen Maschinen, Platform-as-a-Service-Angeboten, Containern und serverlosen Funktionen für spezifische Aufgaben genutzt. All diese Workloads gilt es zu schützen.

Prisma Cloud integriert alle Funktionen einer umfassenden Cloud-Workload-Sicherheitsplattform unter einem Dach. Dabei überwacht ein einheitliches Agenten-Framework den gesamten Anwendungslebenszyklus. Unternehmen können so das Schwachstellenmanagement und die Compliance in ihre Continuous-Integration-/Continuous-Delivery-Prozesse einbetten. Dabei werden Code-Repositories und Container-Registries laufend überwacht.

Die Lösung beobachtet das Workload-Verhalten anhand von Profilen, etwa für Prozess-, Netzwerk- und Dateisysteme. So lassen sich mittels Laufzeitrichtlinien die Anwendungen schützen und ungewöhnliche Aktivitäten protokollieren und unterbinden. Die gesamte Netzwerkkommunikation kann in Echtzeit eingesehen werden, was die Transparenz erhöht und die Fehlersuche, beispielsweise in Container-Umgebungen, vereinfacht. Weitere Funktionen von CWPP sind der Schutz von Webanwendungen vor OWASP-Top-10-Angriffs-





taktiken, API-Schutz und standortbasierte Zugangskontrollen.

CIEM: Infrastruktur-Zugriffsrechte verwalten

Angesichts der extrem dynamischen Entwicklung der Cloud-Angebote verlieren viele Unternehmen die Übersicht über die vergebenen Benutzer- und Maschinenidentitäten und deren Rechte. Es ist schwierig, nach dem Least-Privilege-Prinzip nur die wirklich erforderlichen Zugriffsrechte zu vergeben. Dies stellt ein enormes Sicherheitsrisiko dar. Prisma Cloud durchsucht IaaS- und PaaS-Umgebungen kontinuierlich, analysiert sämtliche Benutzer- und Maschinenidentitäten in allen Cloud-Umgebungen hinsichtlich Rechten, Rollen und Vorgaben und behebt Risiken beim Identitäts- und Zugriffsmanagement automatisch.

CNS: Netzwerk im Cloud-Zeitalter sichern

Eine traditionelle IP-basierte Mikrosegmentierung funktioniert in heutigen cloudnativen Infrastrukturen nicht, da die Ressourcen in der Regel nicht mehr statisch adressiert sind. Prisma Cloud setzt deshalb auf eine identitätsbasierte Mikrosegmentierung: Die Sicherheit wird durch Identitäten und Richtlinien auf App- beziehungsweise Workload-Ebene vom Netzwerk entkoppelt. Dies erlaubt gleichzeitig eine einfachere Skalierung.

Ausserdem erstellt die Lösung ein ganzheitliches, kontextbezogenes Bild des Netzwerkrisikos, indem sie die implementierten Firewall-Regeln in cloudnativen Umgebungen einbindet und diese mit den Netzwerk-Kommunikationsprotokollen der Cloud-Anbieter abgleicht. Die daraus gewonnenen Erkenntnisse werden mithilfe von Threat Intelligence weiter angereichert und bewertet. So können auch fortgeschrittene Bedrohungen wie Cryptojacking, mit Malware infizierte Instanzen oder das Einnisten und Ausbreiten von Schädlingen in Cloud-Umgebungen erkannt und abgewehrt werden.

Der Schutz der Unternehmen erfordert nicht bloss mehr Sicherheitsmassnahmen, sondern auch neue Ansätze für die Sicherheit der gesamten Cloud-Umgebung.

Speziell für Container-Umgebungen hat Palo Alto Networks zudem die Next-Generation Firewalls der CN-Serie entwickelt. Diese bieten einen umfassenden NGFW-Schutz – unabhängig davon, wo die Apps gehostet werden (mit Kubernetes oder OpenShift im eigenen Rechenzentrum oder mit Google Kubernetes Engine [GKE], Azure Kubernetes Service [AKS] oder Amazons Elastic Kubernetes Service [EKS] aus der Public Cloud).

Sicherheit in der DevSecOps- und Shift-Left-Welt

Viele Organisationen haben Schwierigkeiten bei der Abgrenzung zwischen ihrer eigenen Sicherheitsverantwortung und der ihres externen Cloud-Service-Providers. Gleiches gilt auch intern: Es wird mehr Verantwortung in die Hände der Entwickler verlagert (Shift Left). Prisma Cloud bietet eine intuitive, automatisierte Möglichkeit für Entwickler, über ihre bestehenden DevOps-Workflows und -Tools Schwachstellen sowie Fehlkonfigurationen etwa in Infrastructure-as-Code-Vorlagen (IaC) zu finden und zu beheben. Wenn Probleme so schon während des Entwicklungszyklus erkannt werden, sinken Zeitbedarf, Kosten und Risiken.

Beste Sicherheit für Cloud-Umgebungen

Die schnelle Einführung unterschiedlicher Cloud-Technologien hat Cyberkriminellen exponentiell mehr Möglichkeiten für Angriffe und für Datendiebstahl eröffnet. Doch der Schutz der Unternehmen erfordert nicht bloss mehr Sicherheitsmassnahmen, sondern auch neue Ansätze für die Sicherheit der gesamten Cloud-Umgebung. Mit Prisma Cloud bietet Palo Alto Networks eine der umfassendsten cloudnativen Sicherheitsplattformen (CNSP) mit zentralem Management, die Daten und Anwendungen über den gesamten Lebenszyklus schützt – in jeder Cloud.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch