Schutz von Cloud-Workloads

Sichern Sie Hosts, Container und serverlose Umgebungen über den ganzen Anwendungslebenszyklus hinweg

Sichern Sie Hosts, Container, Kubernetes®- und serverlose Umgebungen über den ganzen Anwendungslebenszyklus hinweg. Kombinieren Sie den Laufzeitschutz mit Schwachstellenmanagement und Compliance. Mit Prisma™ Cloud können beliebige cloudnative Workloads von der Entwicklung über die Implementierung bis hin zur Nutzung geschützt werden.

Bei IT Central Station auf Platz 1 in der Cloud-Workload-Sicherheit	Bei IT Central Station auf Platz 1 in der Container-sicherheit	Bei über 40 der Fortune 100 im Einsatz
Schützt Workloads in Hybrid- und Multi-Cloud-Umgebungen	Schützt Linux- und Windows-Container in Kubernetes- und anderen Container-Plattformen	Schützt führende Unternehmen, über 1.800 Kunden weltweit

Konsistenter Schutz für jede cloudnative Architektur

In modernen Unternehmen laufen Cloud-Workloads und cloudnative Anwendungen auf einer Mischung aus virtuellen Maschinen (VMs), Containern und Kubernetes, Platform as a Service-Angeboten (PaaS) und serverlosen Funktionen. Deshalb stellt Prisma Cloud ein einheitliches Agenten-Framework bereit, mit dem Sie all diese Workloads und Architekturen schützen können.

Integrierte Sicherheit für den gesamten Anwendungslebenszyklus

Prisma Cloud integriert die Funktionen einer Cloud-Workload-Sicherheitsplattform (CWPP) in den gesamten Anwendungslebenszyklus. Damit versetzt es Unternehmen in die Lage, das Schwachstellenmanagement und die Compliance in die CI-Prozesse (Continuous Integration) und die CD-Abläufe (Continuous Delivery) zu integrieren, die Containerregistrys und die serverlosen Repositorys pausenlos zu überwachen und das Laufzeitrisiko für alle Hosts, Container, Images und serverlosen Funktionen zu priorisieren.

Module

Host-Sicherheit

Prisma Cloud Host Security schützt Linux- und Windows®-Hosts in Public und Private Clouds mit leistungsstarken Funktionen wie:

- **Schwachstellenanalysen**: Es durchsucht die Hosts kontinuierlich nach Schwachstellen und erfasst die größten gefundenen Risiken in einer Top-10-Liste.
- **Compliance:**: Benutzer können die mitgelieferten Konfigurationsprüfungen nutzen, um die Compliance mit dem Linux CIS Benchmark und vorgegebenen Windows-Konfigurationen zu überwachen und durchzusetzen oder ihre eigenen Compliancеprüfungen implementieren.
- **Laufzeitschutz**: Die Lösung beobachtet das Workload-Verhalten, erstellt automatisch Profile und meldet ungewöhnliche und böswillige Aktivitäten. Die Verfolgung von Lese- und Schreibzugriffen auf Dateien und Ordner, die Inspektion der Hostprotokolle und eine Sprache zur Erstellung eigener Laufzeitregeln stehen als integrierte Funktionen zur Verfügung.
- **Netzwerktransparenz**: Alle Netzwerkkommunikationen der Hosts sind in Echtzeit sichtbar.
- **Zugangskontrollen**: Benutzer können Zugangskontrollen für Cloud-Workloads etablieren und überwachen.
- **Scannen von Amazon Machine Images (AMI)**: AMIs können nach Schwachstellen durchsucht werden, bevor die VMs in Amazon Web Services (AWS®) implementiert werden.

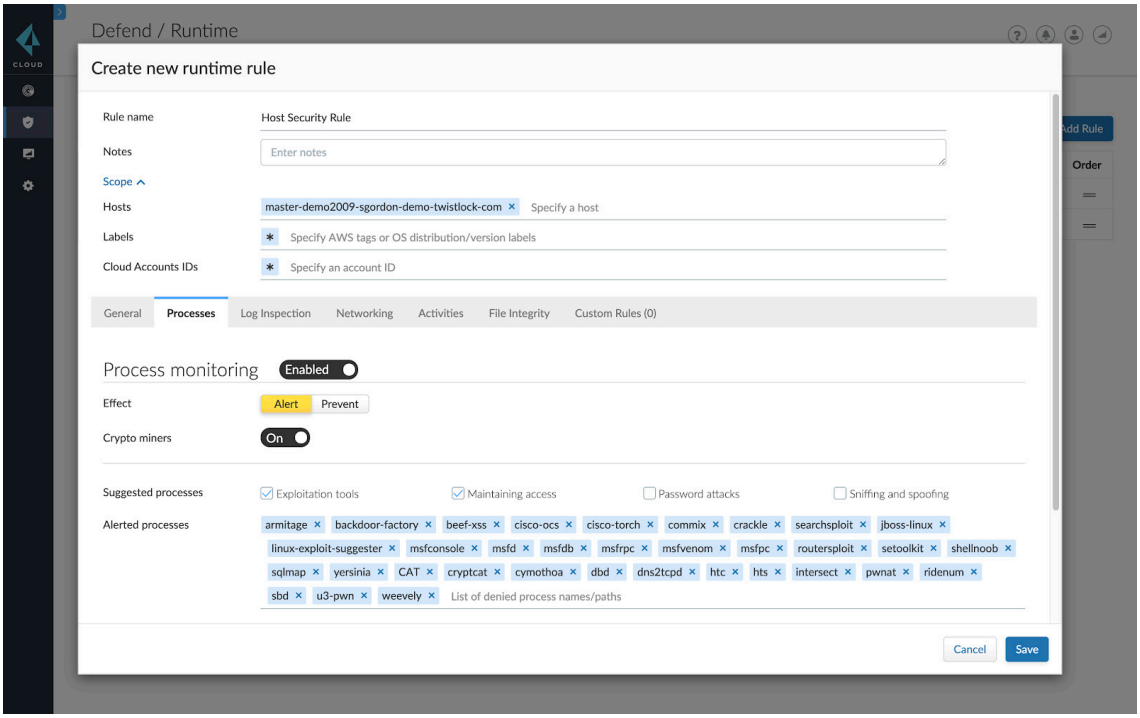

Abbildung 1: Host-Sicherheitsmodul

Containersicherheit

Prisma Cloud Container Security schützt Container und Kubernetes in Public und Private Clouds und bietet:

- **Schwachstellenanalysen**: Ermöglichen einen korrekten Überblick über Schwachstellen in Images und Containern. Eine Top-10-Liste der gefährlichsten Schwachstellen hebt die größten Risiken hervor, darunter alle bekannten CVEs. Sie wird durch Empfehlungen für die Behebung und eine nach Ebene aufgeschlüsselte Image-Analyse ergänzt.
- **Compliancеprüfungen**: Die Lösung enthält über 400 vorkonfigurierte Compliancеprüfungen, unter anderem CIS Benchmarks für Docker®, Kubernetes, Linux, Windows-Konfigurationen und Istio®. Diese anpassbaren Vorlagen erleichtern die Compliance mit PCI DSS, DSGVO, HIPAA und NIST SP 800-190.
- **Laufzeitschutz**: Die Erstellung von Laufzeitrichtlinien für Prozess-, Netzwerk- und Dateisystemsensoren kann automatisiert werden, um laufende Anwendungen zu schützen und dafür zu sorgen, dass die Sicherheitsinfrastruktur mit den Anwendungen mitwächst. Funktionsreiche anpassbare Laufzeitregeln tragen zum Schutz containerisierter Anwendungen bei.
- **Netzwerktransparenz**: Der gesamte Netzwerkverkehr der Container und Kubernetes-Umgebungen ist in Echtzeit sichtbar.
- **Zugangskontrollen**: Implementieren Sie Kontrollmechanismen, die eine genaue Überwachung und Steuerung des Zugriffs auf cloudnative Anwendungen ermöglichen und sich nahtlos mit IAM-Lösungen, Tools für die Verwaltung geheimer Informationen und anderen wichtigen Sicherheitstechnologien integrieren lassen.
- **CI/CD-Sicherheit**: Integrieren Sie die Sicherheit in Ihre CI/CD-Prozesse. Sie können feinkörnig Schwellenwerte definieren, um Manipulationsversuche an anfälligen Images oder die Verletzung von Compliance-Richtlinien zu melden und zu unterbinden.

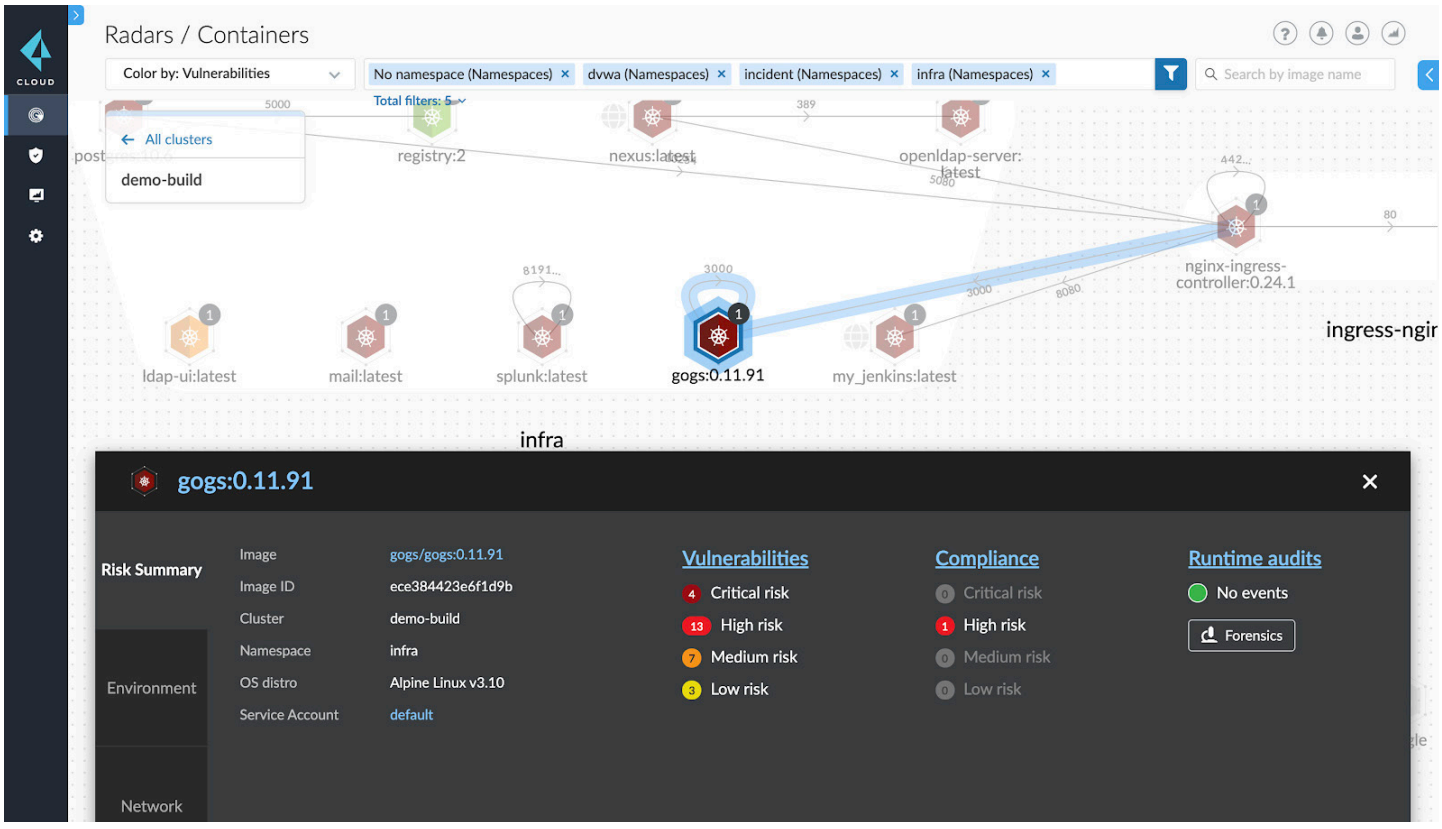

Abbildung 2: Containersicherheitsmodul

Sicherheit in serverlosen Architekturen

Prisma Cloud Serverless Security schützt serverlose Funktionen über den ganzen Anwendungslebenszyklus hinweg und bietet:

- **Schwachstellenanalysen**: Durchsucht Funktionen (von den integrierten CI-Tools und serverlosen Repositorys bis zu Laufzeitumgebungen) kontinuierlich nach Schwachstellen, um einen vollständigen Überblick über das serverlose Risiko während des gesamten Lebenszylus zu bieten.
- **Complianceprüfungen**: Identifiziert Fehlkonfigurationen und Probleme wie Funktionsarchive, die private Schlüssel enthalten, und zu umfangreiche Zugangsrechte für DevOps- und Sicherheitsteams.
- **Laufzeitschutz**: Zeigt die auf AWS Lambda laufenden Funktionen in Echtzeit in einem Radarbild an, einschließlich der Funktionstrigger, des Risiko- und Compliance-Status und aller verbundenen Amazon- und AWS-Dienste wie CloudWatch, Elastic Cloud Compute (Amazon EC2®) und DynamoDB®, und schützt laufende AWS-Lambda-Funktionen vor unerwünschten Prozess-, Netzwerk- und Dateisystemaktivitäten.
- **CI/CD-Sicherheit**: Integrieren Sie die Sicherheit in Ihre CI/CD-Prozesse. Sie können feinkörnig Schwellenwerte definieren, um Manipulationsversuche an anfälligen Funktionen oder die Verletzung von Compliance-Richtlinien zu melden und zu unterbinden.

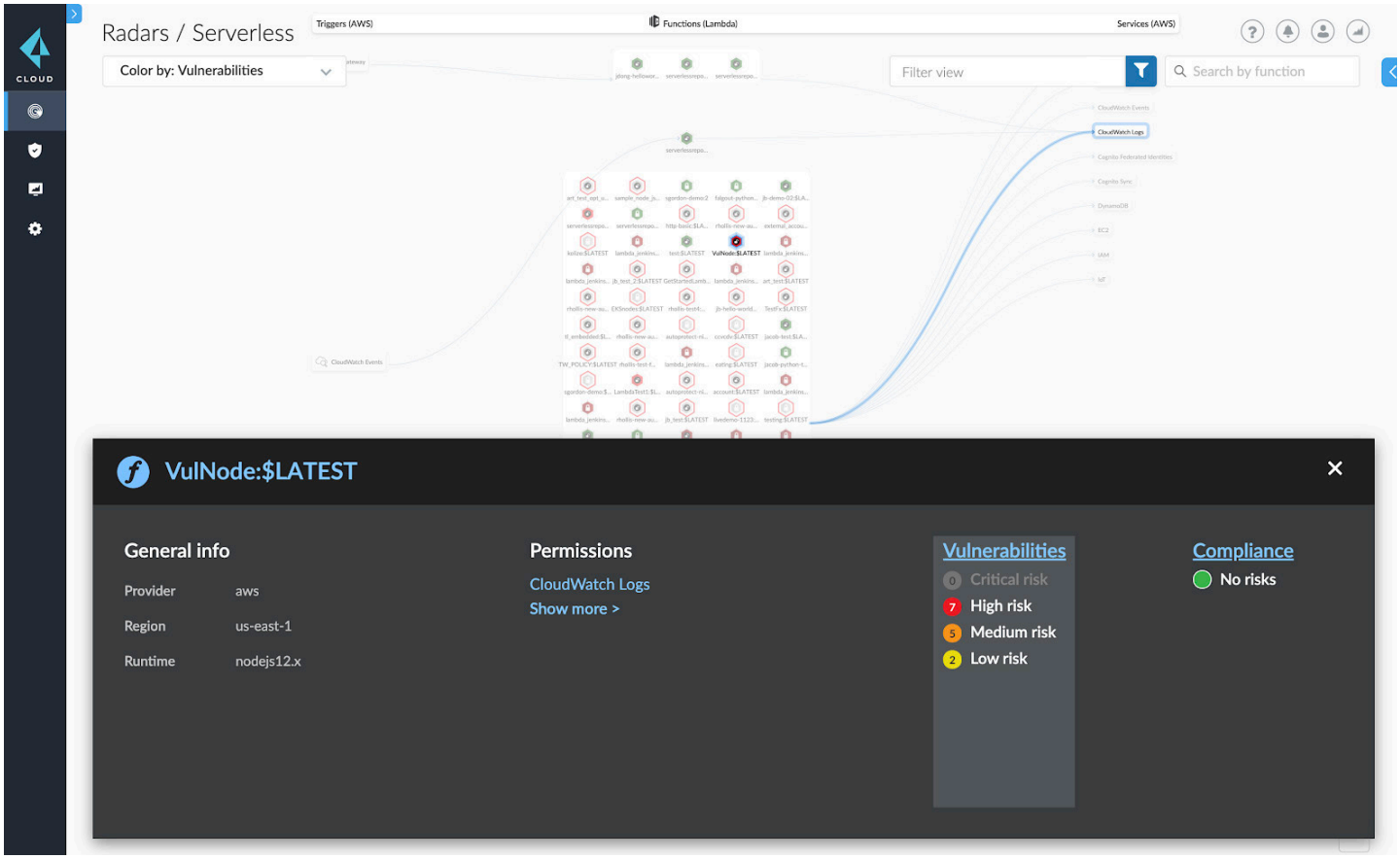

Abbildung 3: Sicherheitsmodul für serverlose Anwendungen

Sicherung von Webanwendungen und APIs

Prisma Cloud Web Application and API Security schützt alle Private- und Public-Cloud-Umgebungen vor den 10 gefährlichsten Layer-7- und OWASP-Bedrohungen und bietet:

- **Schutz vor den OWASP Top-10**: Meldet oder blockiert die in den OWASP Top-10 aufgeführten Angriffstaktiken wie SQL-Injektion, Cross-Site-Scripting (XSS), Shellshock und Brute-Force-Methoden zum Knacken von Anmeldedaten.
- **API-Schutz**: Identifiziert geschützte und ungeschützte APIs und unterstützt die Konfiguration von Sicherheitsregeln und -maßnahmen.
- **Hochladeschutz**: Sie können sich benachrichtigen lassen, wenn Dateien hochgeladen werden, oder das Hochladen von Dateien mit bestimmten Endungen oder Inhalten einschränken. Mit nuancierten Regeln können Sie festlegen, ob das Hochladen bestimmter Dateiformate wie Audio, komprimierte Archive, Dokumente, Bilder oder Videos gestattet oder blockiert werden und/oder Warnmeldungen generieren soll.
- **Standortbasierte Zugangskontrollen**: Sie können den Webzugang von Clients mit bestimmten IP-Adressen bzw. in einzelnen Netzwerken oder Ländern blockieren.
- **HTTP-Header-basierter Schutz von Webanwendungen**: Sie können anhand der HTTP-Headernamen oder -werte Kriterien definieren, um den Zugang zu Webanwendungen zu gestatten oder zu blockieren.

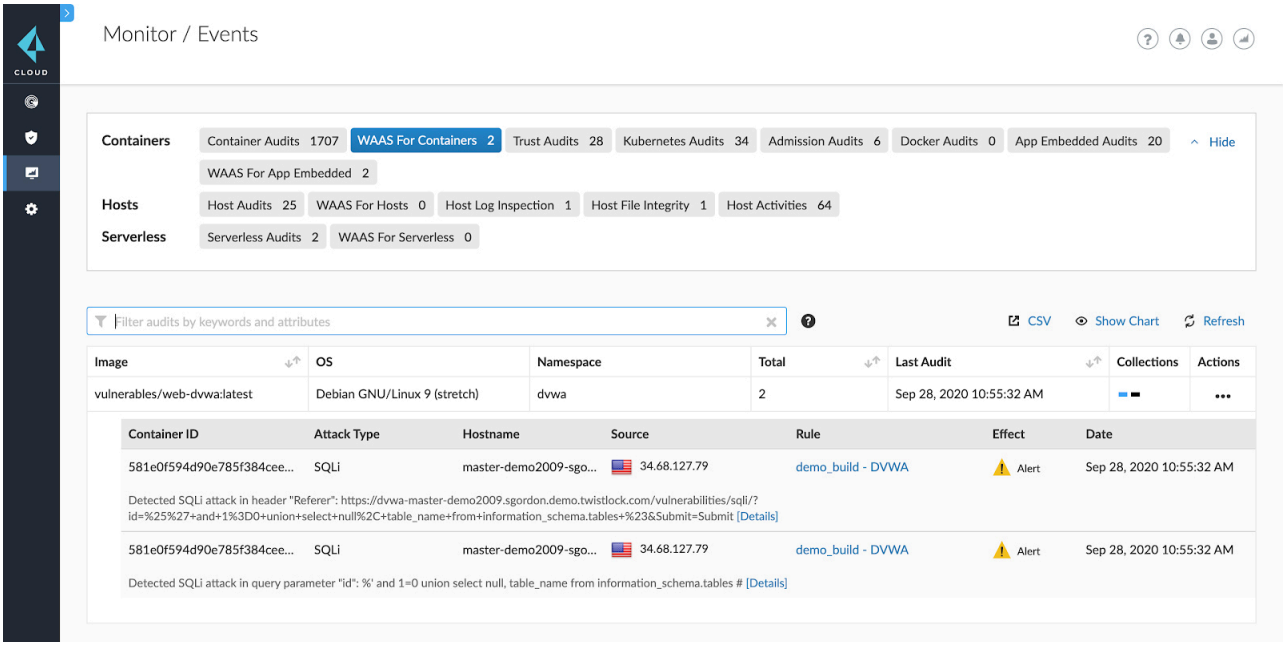

Abbildung 4: Modul zur Sicherung von Webanwendungen und APIs

Prisma Cloud ist eine umfassende cloudnative Sicherheitsplattform, die mit branchenführenden Sicherheits- und Compliancefunktionen Anwendungen, Daten und cloudnative Technologien während des gesamten Entwicklungslebenszyklus schützt, auch in Hybrid- und Multi-Cloud-Umgebungen. Mit seinem integrierten Ansatz entfernt Prisma Cloud die Sicherheitseinschränkungen rund um cloudnative Architekturen, anstatt sie nur zu maskieren. Im gesamten Anwendungslebenszyklus werden voneinander isolierte Sicherheitsprozesse beseitigt, was die Einführung eines DevSecOps-Ansatzes und schnellere Reaktionen auf sich ändernde Sicherheitsanforderungen in cloudnativen Architekturen ermöglicht.

Weitere Informationen finden Sie auf unserer Website und in dieser Demo.

„Prisma Cloud hilft unserem Unternehmen, das DevSecOps-Konzept umzusetzen, bei dem die Sicherheit in jeder Entwicklungsphase überprüft wird. Wenn wir Schwachstellen oder Probleme finden, beheben wir sie, bevor wir in die Produktion gehen."

– Nicola Mutti, Head of Security, Cuebiq
Lesen Sie die ganze Fallstudie

paloalto NETWORKS
Oval Tower, De Entrée 99–197
1101 HE Amsterdam
Niederlande
Telefon: +31 20 888 1883
www.paloaltonetworks.de