Lösungsüberblick: Prisma Cloud Compute Edition

Neue Sicherheitsherausforderungen durch cloudnative Anwendungen

Konventionelle Sicherheitslösungen und -ansätze bieten keinen ausreichenden Schutz für Multicloud-fähige, hardwareunabhängige Anwendungen mit kurzen Entwicklungszyklen. Dies ist im Wesentlichen auf drei Gründe zurückzuführen:

- Die für die Erstellung und Bereitstellung der cloudnativen Anwendungen zuständigen Entwickler und DevOps-Teams agieren oft außerhalb der von klassischen Sicherheitsteams und -technologien überwachten Umgebungen. Hier sind Schutzmaßnahmen erforderlich, die auch die von den Entwicklern genutzten Infrastrukturen und Tools abdecken.
- Moderne Unternehmen setzen vielfältige Cloud-Umgebungen und -Services ein. Sie verfügen über komplexe Multicloud-Infrastrukturen und Hybridumgebungen und nutzen eine Kombination aus in der Cloud gehosteten virtuellen Maschinen, Containern, Kubernetes®, Container-as-a-Service-Lösungen (CaaS) und serverlosen Funktionen.
- Cloud-Umgebungen und die darin gehosteten Anwendungen durchlaufen dynamische Veränderungen. Daher benötigen Sicherheitsteams automatisierte Lösungen, mit denen sich die wachsende Zahl der in ständigem Wandel begriffenen Microservices ihres Unternehmens schützen lässt.

Konsistenter Schutz für Hosts, Container und serverlose Anwendungen

Als Kunde von Prisma™ Cloud Compute Edition erhalten Sie Zugang zur führenden cloudnativen Sicherheitsplattform, die Ihren Hosts, Containern und serverlosen Anwendungen in jeder beliebigen Cloud-Umgebung und in sämtlichen Phasen ihres Lebenszyklus umfassenden und konsistenten Schutz bietet. Da die Lösung selbst als cloudnative Anwendung konzipiert ist und sich über leistungsstarke APIs mit anderen Systemen integrieren lässt, können Sie mit Prisma Cloud Compute Edition alle Workloads Ihres Unternehmens schützen – unabhängig von der ihnen zugrunde liegenden Technologie und der jeweils verwendeten Cloud-Umgebung.

Schwachstellenanalysen: Schützen Sie sämtliche Phasen des Anwendungslebenszyklus – von der Entwicklung bis zur Produktion – mit beispiellosen Funktionen zur Identifizierung, Analyse und Behebung von Schwachstellen und Sicherheitslücken.

Compliance: Nutzen Sie anwenderfreundliche Compliance-Funktionen zur Umsetzung und dauerhaften Einhaltung der Anforderungen der CIS-Benchmark-Tests für Docker-, Kubernetes- und Linux-Umgebungen, zur Implementierung externer Vorgaben und unternehmensspezifischer Anforderungen sowie zur Durchführung der branchenweit ersten Compliance-Prüfungen für das Istio®-Service-Mesh.

CI/CD-Integration: Binden Sie leistungsstarke Sicherheitsmechanismen direkt in Ihre Continuous-Integration-Prozesse (CI) ein, damit jedes potenzielle Problem vor der Produktivsetzung identifiziert und behoben werden kann.

Überwachung des Laufzeitverhaltens: Sichern Sie Ihre skalierbare Cloud-Infrastruktur mit Tools, die mithilfe maschineller Lernverfahren für sämtliche Versionen aller Anwendungen automatisch Laufzeitmodelle erstellen, in denen nur die unbedingt erforderlichen Zugriffsrechte vergeben und die legitimen Anwendungen in einer Whitelist erfasst sind.

Cloudnative Firewalls: Schützen Sie cloudnative Anwendungen mit speziell für diesen Zweck entwickelten Layer-4- und Web-Application-Firewall-Funktionen.

Zugangskontrollen: Implementieren Sie Kontrollmechanismen, die eine genaue Überwachung und Steuerung des Zugriffs auf Cloud-Workloads und cloudnative Anwendungen ermöglichen und sich nahtlos mit IAM-Lösungen, Tools für die Verwaltung geheimer Informationen und anderen wichtigen Sicherheitstechnologien integrieren lassen.

So funktioniert Prisma Cloud Compute Edition

Die Lösung bietet Ihnen flexible Bereitstellungsoptionen, damit Sie Ihre Workloads und Anwendungen in jeder cloudbasierten Hosting- und Betriebsumgebung sichern können. Durch die Implementierung von umgebungsspezifischen Agenten – die als „Defender" bezeichnet werden – erreichen Sie starken, konsistenten Schutz für Ihre virtuellen Maschinen, Docker-Container, Kubernetes-Cluster, auf Pivotal Application Service laufenden PaaS-Apps und serverlosen Anwendungen. Möglich wird dies, indem die Defender das Anwendungsverhalten mit einer automatisch erstellten Whitelist abgleichen und sämtliche anomalen Aktivitäten unterbinden. Darüber hinaus kombiniert die auf dem „Defense-in-Depth"-Prinzip basierende Compute Edition cloudnative Firewall-Funktionen, die den Datenverkehr zwischen Cloud-Workloads sichern, mit Sicherheitsmechanismen für serverlose Ausführungsumgebungen, die das Laufzeitverhalten der einzelnen Anwendungen mithilfe von auf maschinellem Lernen basierenden Algorithmen analysieren und kontrollieren.

Ergänzend erhalten Sie eine nach Prioritäten geordnete Aufstellung der identifizierten Schwachstellen und Risiken sowie Zugriff auf Compliance- und Überwachungsfunktionen, die den gesamten Softwarelebenszyklus abdecken und sich in sämtliche CI-Prozesse, Docker-Registrys, Code-Repositorys und Produktionsumgebungen einbinden lassen. Außerdem profitieren Sie von Kontrollfunktionen der Enterprise-Klasse, mit denen Sie alle Ressourcen in Ihrer Cloud-Infrastruktur sowie geheime Informationen (Secrets), Kubernetes, Audit-Trails und IAM-Tools verwalten können.

Grundsätzlich handelt es sich bei Prisma Cloud Compute Edition um eine vom Kunden implementierte, gehostete und verwaltete Sicherheitslösung, die über ein Container-Image bereitgestellt wird und einen sicheren Anwendungsbetrieb in öffentlichen, privaten und hybriden Cloud-Umgebungen sowie in physisch isolierten Infrastrukturen ermöglicht. Alternativ können Sie sich auch für das SaaS-Bereitstellungsmodell entscheiden, das im Lösungsüberblick zu Prisma Cloud näher beschrieben wird.

Weitere Informationen

Wenn Sie mehr über Prisma Cloud erfahren möchten, können Sie die Website von Palo Alto Networks besuchen oder den Lösungsüberblick zu Prisma Cloud herunterladen.

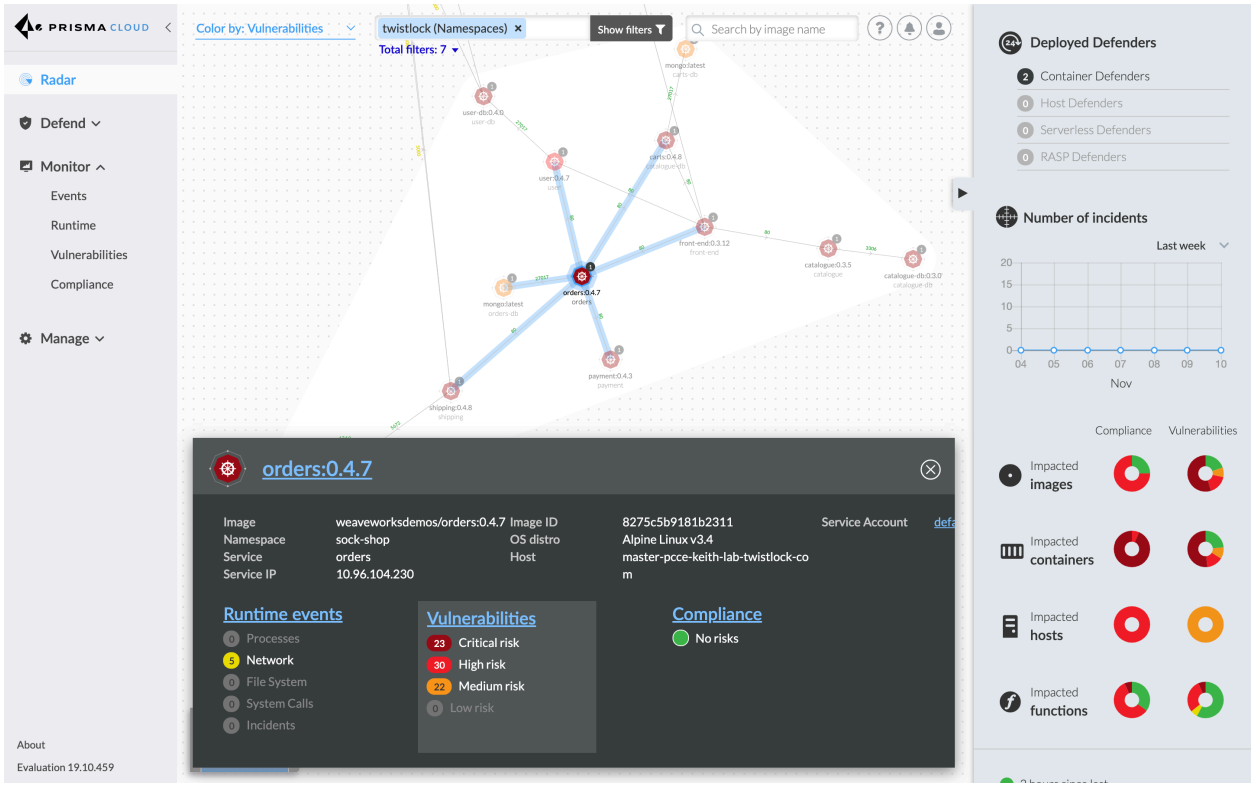

Abbildung 1: Vom Kunden betriebene Sicherheitsinfrastruktur in Prisma Cloud Compute Edition

Die wichtigsten Vorteile

- **Effektiver Schutz für sämtliche cloudnativen Technologien:** Mit Prisma Cloud Compute Edition stehen Ihnen alle Infrastrukturoptionen offen. Die Sicherheitsplattform schützt sämtliche cloudbasierten Anwendungskomponenten – unabhängig von der jeweils genutzten Betriebsumgebung.
- **Nach Prioritäten geordnete Risiko- und Kontextinformationen zu Ihren Cloud-Umgebungen:** Sie erhalten einen ständig aktualisierten und nach Prioritäten geordneten Überblick über die Schwachstellen und Risikobereiche in Ihrer für die Entwicklung und Produktion genutzten Cloud-Infrastruktur. Außerdem wird Ihnen ein Echtzeit-Konnektivitätsdiagramm angezeigt, das unter anderem über Bedrohungen in Ihren Ausführungsumgebungen Auskunft gibt.
- **Automatisierter, DevOps-tauglicher Cyberschutz:** Prisma Cloud Compute Edition versetzt Ihre Entwickler und DevOps-Teams in die Lage, neue cloudnative Anwendungen so schnell und sicher wie möglich für die Kunden bereitzustellen.