Leitfaden: Managementtools für das Cloud-Sicherheitsniveau

paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

Inhalt

PRISMA BY PALO ALTO NETWORKS

Eine gute Cloud-Sicherheitshygiene beginnt mit einer vollständigen Übersicht über das Sicherheits- und Complianceniveau jeder Ressource, die Sie in Ihrer Cloud bereitstellen. Diese Transparenz in einer einzelnen Cloud-Umgebung zu erreichen ist relativ unkompliziert, denn dort können Sie sich stark auf die nativen Überwachungs- und Auditingtools Ihres Cloud-Anbieters stützen und Lösungen von Drittanbietern verwenden, um Lücken zu schließen (z. B. in der Bedrohungserkennung). In einer Multi-Cloud-Architektur wird aber die Aufrechterhaltung eines starken Sicherheitsstatus sehr schnell sehr viel aufwendiger.

In einer solchen Umgebung ist es viel schwieriger, eine zentrale Transparenz zu erreichen sowie Richtlinien und Complianceregeln konsequent durchzusetzen. Außerdem ist es hier komplizierter, Bedrohungen zu erkennen und Sicherheitslücken schnell zu beheben, da die Komplexität der Bedrohungen in verteilten, mehrschichtigen Architekturen sehr hoch ist.

Sie können sich diesen Herausforderungen jedoch stellen – und das sollten Sie auch, wenn Sie die Vorteile einer Multi-Cloud-Architektur nutzen möchten, ohne Kompromisse bei der Sicherheit einzugehen. Dieser Leitfaden führt Sie durch die spezifischen Herausforderungen, vor die das Management des Cloud-Sicherheitsniveaus (Cloud Security Posture Management, CSPM) Sie in einer Multi-Cloud-Architektur stellt. Anschließend wird erörtert, wie Sie ein Toolset und eine Strategie für das CSPM aufbauen, die diese Herausforderungen effektiv angehen, indem sie zentrale Transparenz, Compliancemanagement, Bedrohungserkennung, Datensicherheit und Automatisierung speziell für Multi-Cloud-Umgebungen bieten.

Die besonderen Herausforderungen des Multi-Cloud-CSPM

Ein CSPM, das in einer einzelnen Cloud-Umgebung funktioniert, kann nicht einfach für die Anforderungen einer Multi-Cloud-Architektur skaliert werden. Im Hinblick auf die Sicherheit unterscheiden sich Multi-Cloud-Umgebungen in vielerlei Hinsicht grundlegend von einzelnen Clouds.

Voneinander isolierte, verteilte Daten

Daten in einer Multi-Cloud-Umgebung sind auf mehrere Clouds verteilt. Beispielsweise können Sie umfangreiche Daten in einer kostengünstigeren Cloud speichern und andere Daten in einer Cloud, die mehr kostet, aber schnelleren Zugriff bietet. In einem anderen Anwendungsfall können Sie Daten auf verschiedene Cloud-Regionen verteilen, um sie so nah wie möglich am jeweiligen Endbenutzer bereitzustellen.

Verteilte Daten sicher und frei von Malware zu halten, ist schwieriger. Sie sollten sich vergewissern, dass für jeden Datenspeicher in jeder Cloud geeignete Regeln für das Identitäts- und Zugriffsmanagement (IAM) vorhanden sind. Darüber hinaus müssen Sie sicherstellen, dass jeder Bucket geeignet konfiguriert ist, und was das bedeutet, hängt vom Cloud-Anbieter (CSP) ab.

Verteilte Anwendungen

Oft sind in Multi-Cloud-Umgebungen auch Anwendungen und die zugehörigen Tools verteilt. So können Sie beispielsweise Instanzen derselben Anwendung als Duplikate in verschiedenen Clouds ausführen, damit sie auch dann verfügbar ist, wenn eine Cloud ausfällt; oder Sie können eine Toolchain für die Entwicklung in einer Cloud hosten, aber ihre Ergebnisse von dort aus in einer anderen bereitstellen.

In diesem Kontext erfordert ein effektives CSPM ein Verständnis des Sicherheitsniveaus aller einzelnen Services und Ressourcen, aus denen jede Anwendung besteht. Es reicht nicht, sämtliche Instanzen einer Multi-Cloud-Anwendung einzeln zu überwachen. Sie müssen wissen, wie sich das Sicherheitsniveau einer Instanz auf andere auswirken kann. Können Instanzen beispielsweise so interagieren, dass eine Sicherheitsverletzung in einer Cloud-Umgebung auf eine andere übergreifen kann? Eine kontinuierliche Überprüfung der Anwendungskonfigurationen auf die Einhaltung bestehender Richtlinien hilft, sich vor solchen Risiken zu schützen.

Da das Bereitstellen von Anwendungen über mehrere Clouds hinweg komplexer ist, wird es zudem noch wichtiger, die Sicherheit in die Entwicklungspipeline für Anwendungen zu integrieren, statt sie nachträglich hinzuzufügen. Es dauert viel länger, eine Sicherheitslücke zu beheben, sobald die Anwendung in die Produktion gelangt ist – zumal, wenn der Code, der sie verursacht, in mehreren Umgebungen bereitgestellt wird. Durch die Integration von Sicherheitskontrollen in die Entwicklungspipeline für Anwendungen minimieren Sie das Risiko, solche reaktiven, korrigierenden Maßnahmen durchführen zu müssen, wenn eine Anwendung bereits in Produktion ist.

Mehrere Bedrohungsarten und Sicherheitslücken

Moderne Bedrohungen sind vielfältig, von böswilligen Insidern, die APIs missbrauchen, bis hin zu Cryptojacking, Datenausschleusung, Malware in Containerimages, SQL-Injektions-Sicherheitslücken in Anwendungen und mehr. Keine einzelne Art der Bedrohungserkennung kann vor allen schützen. Malwarescans oder Konfigurationsaudits allein schützen Ihre Umgebungen nicht. Stattdessen sollten Sie Threat Intelligence aus zahlreichen Quellen sammeln, sie analysieren und die Ergebnisse bekannten Bedrohungen zuordnen. Sie müssen auch in der Lage sein, regelbasierte Richtlinien mit auf maschinellem Lernen basierenden Richtlinien zu ergänzen, um selbst unbekannte Bedrohungen zu erkennen.

Mehrere Benutzer und Berechtigungen

Schon bei einzelnen Cloud-Umgebungen kann die Durchsetzung einer guten IAM-Hygiene eine Herausforderung sein. Wenn zahlreiche verschiedene Richtlinien mit Benutzern verknüpft sind (z. B. vom CSP oder vom Benutzer verwaltete Richtlinien; Richtlinien, die anderen Gruppen, Rollen, Ressourcen oder Zugriffssteuerungslisten zugeordnet sind), ist die Durchsetzung unterschiedlicher Zugriffsrechte für eine einzelne Cloud-Umgebung schwierig genug.

In Multi-Cloud-Umgebungen wird dies noch komplizierter, da Benutzerrechte und Berechtigungen bei verschiedenen CSPs unterschiedlich definiert sind. Sie müssen nicht nur für jede Cloud andere IAM-Konfigurationen überwachen, sondern auch in der Lage sein, die für jede Cloud definierten Benutzerrollen und Berechtigungen an die Anforderungen der einzelnen Benutzer anzupassen. Sie können nicht einfach in jeder Cloud dieselben Anmeldedaten für die gleichen Benutzer überprüfen.

Größere Angriffsfläche

Mehr Clouds bedeuten unter anderem mehr Konten, Zugriffssteuerungsrichtlinien und Services. All dies summiert sich zu einer größeren Angriffsfläche und bietet Angreifern mehr Möglichkeiten, eine falsch konfigurierte Ressource, zu breit gefasste Berechtigungen oder eine Sicherheitslücke im Code auszunutzen, um in Ihre Umgebung einzudringen.

Zugleich erschwert die fehlende zentrale Übersicht und Kontrolle in einer Multi-Cloud-Umgebung die Erkennung von Sicherheitslücken und Bedrohungen. Wenn Sie nicht mit den Tools eines einzelnen CSPs alle Konfigurationen für all Ihre Services überwachen und prüfen können, ist es schwieriger, Fehlkonfigurationen zu verhindern, die zu einer Sicherheitsverletzung führen können.

Das Multi-Cloud-CSPM meistern: Vier wichtige Merkmale und Funktionen

Die Bewältigung der beschriebenen Sicherheitsherausforderungen in Multi-Cloud-Umgebungen erfordert eine CSPM-Strategie und ein Toolset mit vier wichtigen Merkmalen.

Vollständige Transparenz, Compliance und Governance

Die Grundlage für ein erfolgreiches CSPM für mehrere Clouds ist die Fähigkeit, sämtliche Ressourcen bei allen CSPs kontinuierlich zu überwachen und zu prüfen. Wenn ein neuer Service oder eine neue Workload bereitgestellt oder eine Konfiguration geändert wird, sollten Ihre Tools in der Lage sein, die Aktualisierung zu erkennen und zu scannen, um sicherzustellen, dass sie mit den Sicherheitsanforderungen und Best Practices übereinstimmt.

Bei Abweichungen sollten die Tools eine entsprechende Warnmeldung an Ihr Team schicken und Behebungsoptionen empfehlen. Die Tools sollten in der Lage sein, einfache Korrekturen (z. B. das Aktualisieren einer falsch eingegebenen IP-Adresse oder das Hinzufügen einer fehlenden Anweisung zu einer IAM-Richtlinie) automatisch anzuwenden und solche Probleme zu beheben, ohne darauf zu warten, dass ein Sicherheitsteam die Änderung vornimmt.

Es ist auch wichtig, von vornherein zu verhindern, dass unsichere Konfigurationen in die Produktion gelangen, um die Anzahl der zur Laufzeit generierten Warnungen zu reduzieren. CSPM-Tools sollten in der Lage sein, IaC-Vorlagen (Infrastructure-as-Code) auf Fehlkonfigurationen zu scannen und Richtlinien nicht nur zur Laufzeit, sondern auch im gesamten Softwareentwicklungszyklus durchzusetzen.

Umfassende Bedrohungserkennung

Da Bedrohungen in Multi-Cloud-Umgebungen meist komplex sind, müssen CSPM-Tools Threat Intelligence aus zahlreichen Quellen sammeln, um Risiken genau zu analysieren. Zu diesen Quellen gehören IaC-Konfigurationen, Containerimages und Images von virtuellen Maschinen (VMs) in der Cloud, die viele Teams bereits auf Sicherheitslücken scannen.

Das bloße Scannen dieser Komponenten reicht jedoch nicht für eine vollständige Bedrohungsanalyse und -erkennung aus. Hierfür benötigt Ihr Unternehmen auch stets zuverlässige Threat Intelligence, damit Sie die neuesten Bedrohungen erkennen und ihren Schweregrad einschätzen können. Wichtig ist auch die Fähigkeit, Anomalien im Netzwerk zu erkennen und sie mit anderen Arten von Threat Intelligence in Beziehung zu setzen, um sich ein volles Bild der potenziellen Risikoauswirkungen jeder Bedrohung zu machen. Dazu gehören auch Daten aus der Analyse des Anwender- und Objektverhaltens (UEBA).

Mit anderen Worten: Eine moderne Bedrohungserkennung erfordert die Analyse mehrerer Datenquellen und die Fähigkeit, diese Daten miteinander zu verbinden und in einen bestimmten Kontext zu setzen. Dies ist nicht nur wichtig, um Bedrohungen in komplexen, vielschichtigen Umgebungen zu identifizieren, sondern auch, damit Teams Risiken schnell priorisieren und Bedrohungen beseitigen können. Nur durch eine umfassende Bedrohungserkennung können Sie Anomalien im Netzwerk etwa mit einem unsicheren Containerimage in Verbindung bringen oder feststellen, von welchem Konto eine Sicherheitsverletzung ausgeht. Wenn Ihr Team Bedrohungen schneller verstehen kann, kann es sie auch schneller beheben und so die durchschnittliche Problembehebungszeit minimieren.

Integrierte Datensicherheit

Unabhängig davon, was für Daten Sie in der Cloud speichern und ob sie personenbezogene Informationen enthalten, ist für ihre Sicherheit eine mehrgleisige Verteidigung erforderlich, die den Zustand und Status Ihrer Daten detailliert sichtbar macht. Dafür müssen Sie die Konfiguration jedes Speicher-Buckets in Ihren verschiedenen Speicherservices überwachen können, um sicherzustellen, dass Daten nicht versehentlich für nicht autorisierte Benutzer oder Anwendungen zugänglich sind. Zugleich sollten Sie den Inhalt von Buckets prüfen, um festzustellen, ob sie personenbezogene Informationen enthalten, die besonderen Complianceregeln oder anderen Anforderungen unterliegen.

Die Erkennung von Malware in gespeicherten Daten ist ein weiterer wichtiger, aber oft übersehener Teil der Datensicherheit in der Cloud. Dabei müssen nicht nur Speicher-Buckets, sondern auch Datenbanken, VM-Dateisysteme, Container-Speichervolumes und sogar kurzlebige Container-Dateisysteme auf Anzeichen von Malware untersucht werden.

Da es bei der Datensicherheit in der Cloud häufig darauf ankommt, das richtige Gleichgewicht zwischen Schutz und Verfügbarkeit zu finden, sollten Ihre CSPM-Tools es Ihnen außerdem ermöglichen, das Gefährdungsrisiko von Daten zu berechnen, und Empfehlungen geben, die helfen, die potenziellen Auswirkungen einer Sicherheitsverletzung zu begrenzen. Wie vertraulich sind Ihre Cloud-Daten und welche Zugriffskontrollen sind folglich angemessen? Sollten Sie weniger granulare Zugriffsrichtlinien verwenden, um die Verwaltung zu vereinfachen? Tools, die das Gefährdungsrisiko berechnen können, helfen Ihnen, Fragen wie diese leichter zu beantworten.

Automatisierung für die Warnungsbehebung

Multi-Cloud-Umgebungen sind von Natur aus komplexe, groß angelegte Umgebungen. Die Durchsetzung der genannten Sicherheitsprozesse und die Überwachung innerhalb dieser Prozesse sind nur möglich mit Tools, die die Umgebung automatisch auf Sicherheitsrisiken überwachen und bei ihrer Behebung helfen können.

Das bedeutet nicht, dass das Multi-Cloud-CSPM vollständig automatisiert werden sollte. Manuelle Eingriffe werden immer notwendig sein, um auf komplexe Sicherheitsvorfälle zu reagieren oder Risiken zu beurteilen, die für Ihre CSPM-Tools allein zu kompliziert sind. Routinemäßige Sicherheitsüberprüfungen, Audits und Problembehebungen sollten jedoch automatisiert werden, damit sich Ihr Team auf die wichtigen Aufgaben konzentrieren kann.

Die Grenzen der Tools von Cloud-Anbietern

CSPs bieten zahlreiche Tools, die einige der in diesem Leitfaden beschriebenen Risiken bekämpfen können. Datensicherheitsservices wie Amazon Macie® und Google Cloud DLP können etwa Datensicherheitslücken in Speicher-Buckets und Datenbanken beurteilen. Überwachungstools wie Amazon CloudWatch und Microsoft Azure® Monitor können Warnungen für bestimmte Arten von Ereignissen generieren, die möglicherweise auf Sicherheitsrisiken hinweisen. Diese Tools sind nützlich, und Sie können sie als Teil Ihres CSPM-Toolsets nutzen. Tools von CSPs sind jedoch zwei wesentliche Grenzen gesetzt:

1. **Sie sind nicht als umfassende, durchgängige CSPM-Lösungen konzipiert**. Sie können vielleicht einige Konfigurationsdateien überprüfen oder einige personenbezogene Daten in bestimmten Datenspeichern finden, aber sie werden nicht kontinuierlich Containerimages scannen, Netzwerkanomalien erkennen oder Bedrohungen automatisch beseitigen.
2. **Die Tools jedes CSPs funktionieren nur für seine eigenen Clouds**. Mit anderen Worten: Die Tools von Google funktionieren nur für Google Cloud, die von Amazon nur für Amazon Web Services, die von Microsoft nur für Azure und so weiter.

Sich in einer Multi-Cloud-Umgebung allein auf die Tools der CSPs zu verlassen, bedeutet, mit sehr vielen unterschiedlichen Tools zu jonglieren – eine schwierige und ineffiziente Aufgabe. Es ist unmöglich, Daten von all diesen Tools effizient miteinander in Beziehung zu setzen. Das verhindert eine umfassende Bedrohungserkennung für sämtliche Datenquellen in Ihrer Multi-Cloud-Umgebung.

Fazit

Kurz gesagt erfordert das Multi-Cloud-CSPM eine umfassende Sicherheitsplattform, die kontinuierlich und präzise auf Fehlkonfigurationen, Sicherheitslücken und Bedrohungen hinweisen kann.

Prisma® Cloud von Palo Alto Networks bietet die nötige Automatisierung und zentrale Übersicht, um die Herausforderungen der Multi-Cloud-Sicherheit effektiv anzugehen. Prisma Cloud erfasst Daten aus Ablaufprotokollen, Konfigurationsprotokollen und Auditprotokollen in all Ihren Cloud-Umgebungen und bietet Ihren Sicherheitsteams so eine zentrale Ansicht zur Überwachung des Sicherheits- und Complianceniveaus Ihrer gesamten Umgebung.

Da Prisma Cloud außerdem eine Bedrohungserkennung anhand ungewöhnlicher Aktivitäten und Auswirkungen bietet, kann Ihr Team den Schweregrad jeder Bedrohung besser verstehen und entsprechende Maßnahmen ergreifen. Mit Prisma Cloud verschwenden Sie keine Zeit mehr damit, zu raten, auf welche Bedrohungen Sie zuerst reagieren sollten, und müssen nicht mehr versuchen, die Ursache komplexer Sicherheitsvorfälle zu identifizieren.

Mit den automatisierten Behebungsfunktionen von Prisma Cloud kann Ihr Team viele Arten sicherheitsrelevanter Fehlkonfigurationen schnell und automatisch beheben und dabei den Status der Behebung über ein zentrales Dashboard überwachen.

Um mehr darüber zu erfahren, wie Prisma Cloud Ihr Team bei der Verwaltung des Sicherheitsniveaus komplexer Multi-Cloud-Umgebungen unterstützen kann, können Sie sich eine Demo der Plattform in Aktion ansehen oder ein Gespräch mit einem Experten von Palo Alto Networks vereinbaren.

paloalto NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de