FIREEYE™

Lösungsübersicht

Verbesserte Governance-Richtlinien für mehr Cloud-Sicherheit

Das Problem
Governance-Richtlinien zu automatisieren, ist nicht schwierig, die Automatisierung von Governance-Richtlinien allein über rollenbasierte Richtlinien hingegen schon.

Festlegung strikter rollenbasierter Richtlinien in einem größeren Umfang ist eine besonders große Herausforderung.

Letzteres ist so kompliziert, weil dafür detaillierte Kenntnisse spezieller Sicherheitsfunktionen und der jeweiligen Umgebung erforderlich sind: das erwartete Verhalten und die Beziehungen zwischen den verschiedenen Instanzen (wie Anwendungsservices, Systemen und Anwendern), die bestimmten Sicherheitsmaßnahmen unterliegen.

Netzwerkrichtlinien werden nur selten von Mitarbeitern erstellt, die sich sowohl im Detail mit den rollenbasierten Sicherheitsfunktionen auskennen als auch einen umfassenden Überblick über die jeweilige Umgebung haben.

Wenn Daten von Cloud-Anbieter-APIs in Lösungen für künstliche Intelligenz eingespeist werden, erhalten die Systeme automatisch Kontextinformationen über das Umgebungsverhalten und können besser rollenbasierte Sicherheitsrichtlinien für Umgebungen aller Größen erstellen.

Verbesserung der Governance-Richtlinien durch maschinell erfasste Daten
Jeder Cloud-Anbieter hat eigene API-gestützte Sicherheitsmaßnahmen für rollenbasierte Governance-Richtlinien. Doch bei diesen detaillierten Sicherheitsfunktionen hapert es oft an der Konfiguration. Ob aus Bequemlichkeit, Unwissenheit oder sogar unlauteren Absichten – wichtige Sicherheitsfunktionen sind häufig falsch konfiguriert, selbst wenn die Bereitstellung automatisiert wurde.

Cloud-Anbieter stellen auch diverse Funktionen und Services für temporäre und Hyperscale-Umgebungen bereit. Ausgereifte Technologien zur Bereitstellungsautomatisierung sind weitverbreitet und werden sowohl für Sicherheitsfunktionen als auch die kontrollierten Ressourcen verwendet. Leider sind auch diese Sicherheitsfunktionen häufig falsch konfiguriert und werden selten (wenn überhaupt) überprüft, um eine detaillierte Konfiguration mit rollenbasierten Zugriffsrichtlinien sicherzustellen.

Unternehmen möchten ihre effizienten DevOps-Workflows beibehalten, die auf versionsbasierten, orchestrierten IaC-Bereitstellungen (Infrastructure as Code) und temporären Infrastrukturen basieren. Gleichzeitig müssen die SecOps-Teams die Transparenzlücke schließen und die Unternehmen benötigen dringend eine größere Transparenz und striktere Governance.

Sie brauchen intelligente Automatisierungsfunktionen, die die vorhandenen Workflows durch detailliertere Richtlinien verbessern, um die Kosten zu reduzieren und sowohl interne als auch externe Bedrohungen abzuwehren.

Die gängigsten Hürden
In den letzten zehn Jahren haben die Technologien zur Bereitstellungsautomatisierung die Technologien zur Automatisierung der Sicherheitsprozesse in Bezug auf die einfache Einführung, den Funktionsumfang und den Reifegrad deutlich überholt. Dieser Trend führt in mittelständischen und großen Unternehmen zu einem

Problem: Mehrere (verteilte) DevOps-Teams verwalten ihre eigenen Bereitstellungen mit den von ihnen bevorzugten Automatisierungslösungen, zum Beispiel Ansible, Chef, CloudFormation, Puppet, Salt, Terraform oder einem der vielen anderen Tools zur orchestrierten Bereitstellung von VMs, Containern und sonstigen Workloads über die Anbieter-APIs. Dadurch verliert das übergeordnete Sicherheitsteam den Überblick (und die Governance) über das Verhalten der verteilten DevOps-Ressourcen. Die Chancen, dass das Sicherheitsteam eigene (neue) Tools verwendet und die DevOps-Governance übernimmt, stehen eher schlecht.

Die SecOps-Teams haben Schwierigkeiten, ihre Tools in die Automatisierungstools der DevOps-Teams zu integrieren. Mit Technologien zur Bereitstellungsautomatisierung lassen sich Bereitstellungen effizient erstellen oder reproduzieren, aber sie bieten keinen Überblick über das Verhalten der Ressourcen. Governance ohne Transparenz ist wie Vertrauen ohne Kontrolle.

Die SecOps-Teams müssen einen Weg finden, diese Hürde zu überwinden, denn in vielen Unternehmen legen die Entwickler die meisten Sicherheitsrichtlinien für Cloud-Ressourcen fest. Das cloudbasierte mandantenfähige Self-Service-Modell hat die Effizienz und Konsistenz der Bereitstellungen deutlich verbessert, aber einige Unternehmen haben die Nachteile zu spüren bekommen, wenn Sicherheitsentscheidungen ohne entsprechende Fachkenntnisse getroffen werden. Viele Unternehmen wissen inzwischen, dass sie bessere Richtlinienprüfungen für mandantenfähige Self-Service-Lösungen benötigen, damit diese langfristig genutzt werden können.

Doch selbst wenn das SecOps-Team die Transparenzlücke mit einer technischen Lösung schließen und die notwendigen Kontextinformationen für die Erstellung rollenbasierter Sicherheitsrichtlinien abrufen kann, steht es vor weiteren Herausforderungen. Wenn sich die Kontextdaten nur durch aufwendige manuelle Verfahren erfassen lassen, ist der Prozess nicht skalierbar und kann daher nicht in großen Cloud-Umgebungen ausgerollt werden. Andererseits kann die Kontrolle der Produktionsressourcen nicht vollständig Maschinen überlassen werden. Es muss ein Gleichgewicht zwischen den Automatisierungsmodellen und den verschiedenen Technologieanwendern gefunden werden.

Anforderungen an eine Lösung

Governance-Lösungen müssen einen Überblick über die Konfiguration und das Verhalten der überwachten Ressourcen geben, damit die Governance-Prozesse analysiert und im Laufe der Zeit verbessert werden können. Die Herausforderung liegt dabei nicht in der Automatisierung an sich, sondern in der Ermittlung der am besten geeigneten rollenbasierten Sicherheitsrichtlinien, die per Automatisierung durchgesetzt werden sollen.

Da bereits in vielen Unternehmen ausgereifte Technologien zur Bereitstellungsautomatisierung genutzt werden, sollte der Schwerpunkt einer Governance-Lösung vor allem auf der automatisierten Erstellung besserer Governance-Richtlinien und der Ausgabe von Richtlinienempfehlungen liegen, ohne Änderungen außerhalb der Standard-Automatisierungsprozesse vorzunehmen.

Eine Governance-Lösung soll vorhandene Governance-Maßnahmen durch besser geeignete Richtlinien verbessern (nicht ersetzen). Dafür ist allerdings ein umfassender Überblick über den gesamten Ressourcenkontext erforderlich. Funktionen für maschinelles Lernen können Kontextdaten verarbeiten und das Verhalten der Ressourcen im Laufe der Zeit anpassen. Je mehr Kontext es gibt, desto umfassender ist das Modell und desto besser sind die erstellten Richtlinien. Daher muss eine Governance-Lösung die Erfassung, Verarbeitung und Korrelierung unterschiedlicher Kontextebenen für die Modellierung und Analyse des Ressourcenverhaltens automatisieren. Nur auf diesem Weg lassen sich Governance-Maßnahmen durch intelligente Richtlinien verbessern.

Die ideale Lösung nutzt KI-Technologien (künstliche Intelligenz, maschinelles Lernen), um das Abrufen detaillierter Kontextdaten über die Cloud-Anbieter-APIs zu automatisieren. Aus dem Gesamtkontext einer Ressource können dann die jeweils am besten geeigneten rollenbasierten Governance-Richtlinien abgeleitet werden. Mit diesen KI-gestützten Richtlinien werden die vorhandenen Governance-Prozesse und -Tools verbessert. Die Lösung sollte den Export von Richtlinienempfehlungen in ein natives Format unterstützen, das entweder für ein Update eines versionsbasierten IaC-Repositorys (Infrastructure as Code) oder für ein Update der mit der vorhandenen Bereitstellung verknüpften Sicherheitsrichtlinien über ein vorhandenes Automatisierungs-Tool verwendet wird.

Die Vorteile von Cloudvisory

Die Governance-Komponente von Cloudvisory bietet cloudnative Funktionen für Governance-Richtlinien durch direkte Kommunikation mit den Cloud-Anbieter-APIs. Sie automatisiert die Erfassung, Verarbeitung und erste Analyse der Sicherheitsereignisse von Workloads und Cloud-Services für mehrere Cloud-Konten und -Anbieter, ganz ohne Workload-basierte Agents. Cloudvisory erkennt Änderungen am Ressourceninventar und den Sicherheitskonfigurationen in Echtzeit, sodass Anwender individuelle Aktionen (wie Warnmeldungen, Rollback oder Abwehrmaßnahmen) für die erkannten Richtlinienverstöße ergreifen können.

Cloudvisory unterstützt die einzelnen Phasen auf dem Weg zu rollenbasierten Governance-Richtlinien. So können Unternehmen die Transparenzlücke schließen, kontinuierliche Compliance sicherstellen und ihre Governance-Maßnahmen verbessern. Die Governance-Komponente von Cloudvisory nutzt auch die detaillierten Kontextdaten der Transparenz- und Compliance-Komponenten, die auf Cloud-, Verlaufs-, Sicherheits- und Systemdaten basieren, um das Verhalten der Ressourcen automatisch anzupassen.

Mithilfe von maschinellem Lernen lassen sich schwierige und kostspielige Aufgaben bei der Erstellung rollenbasierter Richtlinien für die Ressourcen automatisieren. Cloudvisory bietet eine Engine für eine umfassende Richtlinienorchestrierung, um die Netzwerkmikrosegmentierung und andere rollenbasierte Sicherheitsrichtlinien durchzusetzen, aber sie ermöglicht Anwendern auch, ihre bevorzugten Tools für Governance und Orchestrierung auszuwählen. Die Governance-Komponente ist leistungsstark und kann auch große Multi-Cloud-Bereitstellungen ausschließlich mit rollenbasierten Governance-Richtlinien unterstützen. Außerdem ist sie flexibel, sodass Anwender bestehende Governance-Prozesse durch bessere Governance-Richtlinien ersetzen können.

Was spricht für Cloudvisory?
Mit Cloudvisory lassen sich komplexe, cloudspezifische Herausforderungen im gesamten Unternehmen effizient bewältigen.

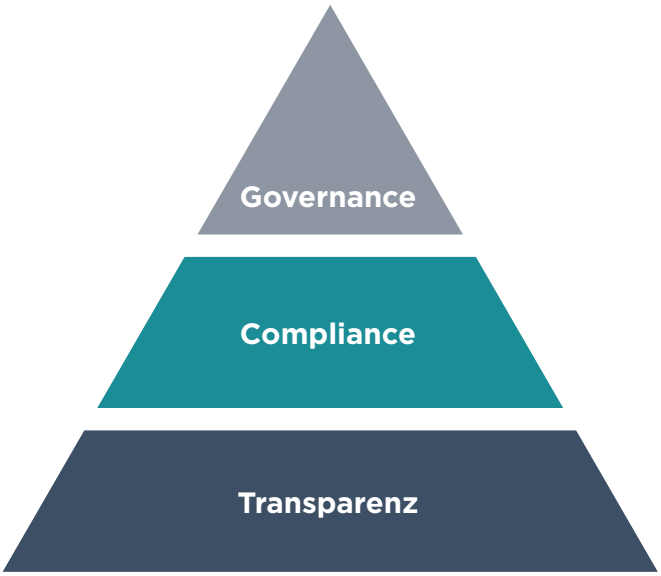
Mitbewerber machen oft große Versprechungen, bieten aber nur Punktlösungen für einen begrenzten Teil der Probleme. Viele Lösungen unterstützen nur Anbieter öffentlicher Clouds wie Kubernetes und OpenStack. Sogenannte „Multi-Cloud-Lösungen“ sind häufig agentenbasiert und endpunktspezifisch (Betriebssystem). Sie sind also nicht cloudnativ und lassen (zumindest) Cloud-Kontextdaten vermissen.

Die größten Probleme betreffen das gesamte System und erfordern daher umfassende Lösungen. Cloudvisory ist die einzige Komplettlösung für cloudnative Multi-Cloud-Governance. Nur Cloudvisory unterstützt agentenlose Governance in öffentlichen und privaten Cloud-Umgebungen wie AWS, Azure, Google Cloud, Kubernetes und OpenStack.

Selbst eine umfassende technische Lösung reicht unter Umständen nicht aus, da sie sowohl für die Anforderungen der Teams geeignet als auch mit den bestehenden Prozessen kompatibel sein muss. Mit Cloudvisory können Unternehmen und Geschäftsbereiche Governance-Richtlinien für ihre spezifischen Anforderungen und Ansprüche implementieren.

Sie können vorhandene Automatisierungstools weiterhin verwenden und intelligente, durch maschinell erfasste Daten verbesserte Governance-Richtlinien implementieren.

Zusammen noch effektiver
Die Governance-Komponente von Cloudvisory nutzt die Daten der Transparenz- und der Compliance-Komponenten, um intelligente cloudnative Governance-Richtlinien für komplexe und dynamische Multi-Cloud-Umgebungen bereitzustellen. Die Algorithmen für das maschinelle Lernen verarbeiten die detaillierten Kontextdaten der Transparenz- und der Compliance-Komponenten, die so viele Informationen wie möglich aus den Cloud-, Verlaufs-, Sicherheits- und Systemkontexten einer bestimmten Ressource umfassen. Mit mehr Kontextdaten lassen sich genauere Governance-Richtlinien erstellen. Und genau das ist dank der in Cloudvisory integrierten künstlichen Intelligenz mit weniger Zeit- und Arbeitsaufwand möglich.



Kontinuierliche Compliance für mehr Cloud-Sicherheit

So schließen Sie die Transparenzlücke in der Cloud-Sicherheit

Unterstützte Cloud-Serviceanbieter

- Azure
- AWS
- Google Cloud
- Kubernetes
- OpenStack

Unterstützte Betriebssysteme

- CentOS
- Red Hat
- Ubuntu Linux

Gartner Cool Vendor 2018

Cloudvisory wurde im Bericht „Cloud Security 2018“ als „Gartner Cool Vendor“ ausgezeichnet.

CIO APPLICATIONS TOP 25 AMAZON SOLUTION PROVIDERS 2017

CIO Applications führt Cloudvisory unter den „Top 25 Amazon Solution Providers“ auf.

AICPA SOC

Cloudvisory-SaaS wurde von einer unabhängigen Stelle gemäß SOC-2 zertifiziert.

Weitere Informationen zu FireEye Cloudvisory erhalten Sie unter:
https://www.fireeye.de/solutions/cloudvisory

FireEye, Inc.
601 McCarthy Blvd.
Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)
info-dach@FireEye.com

Über FireEye, Inc.

FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.

FIREEYE™