Akamai

WHITEPAPER

Schutz von Workloads in AWS durch umfassende Segmentierung – einfachere, schnellere Sicherheit

Lassen Sie sich nicht durch Sicherheitsbedenken von der Cloudeinführung abhalten. Mit nur einer Lösung erhalten Sie Transparenz, Schutz vor lateraler Netzwerkbewegung sowie Angriffserkennung und -reaktion in AWS.

Mehr als 60 % der Unternehmen weltweit nennen Sicherheit als Hauptgrund dafür, dass sie eine Cloudeinführung hinauszögern. Die Vorteile der Migration kritischer Workloads zu AWS liegen auf der Hand: weniger Infrastrukturkosten und Wartungsaufwand, verbesserte Skalierbarkeit und Flexibilität mit nahezu unbegrenzten Ressourcen und grenzenloser Leistung sowie der Einsatz neuester Innovationen wie maschinelles Lernen und KI, um Performance und Analysen zu optimieren. Doch leider halten Sicherheitsbedenken viele Unternehmen zurück.

Die Herausforderung der Sicherheit in AWS

Wenn Sie eine völlig neue Umgebung in Betracht ziehen, ist es kaum überraschend, dass Sie das Thema Sicherheit von Grund auf neu bewerten müssen. Vielleicht steigen Sie gerade erst auf die Cloud um oder Sie migrieren von einem anderen Anbieter, entscheiden sich für eine neue Hybridlösung oder fügen Ihrem bestehenden Ökosystem AWS hinzu. In jedem Fall erfordert die Cloud ein eigenes Toolset, um die einzigartigen Herausforderungen zu bewältigen, die diese Infrastruktur mit sich bringt. Einige Faktoren gelten für alle Cloudanbieter, während andere nur für Azure, Google Cloud Platform (GCP) oder AWS gelten. Hier einige der wichtigsten Überlegungen für Unternehmen, die Cloud- oder Hybrid-Cloud-Lösungen mit AWS-Technologie einsetzen:

Verständnis der gemeinsamen Verantwortung: Wenn Sie Ihre Workloads zu AWS migrieren, müssen Sie sich bewusst sein, dass Sie nach wie vor eine große Verantwortung tragen: Sie sind dafür zuständig, Kundendaten, Anwendungen und Plattformen zu schützen. Da viele Unternehmen dieses Modell der gemeinsamen Verantwortung nicht gänzlich verstehen, prognostiziert Gartner, dass bis 2025 99 % der Cloudsicherheitsfehler vom Kunden verursacht werden.

Mangelnde Transparenz: Was Sie nicht sehen können, können Sie auch nicht kontrollieren. In der Cloud gestaltet sich Transparenz viel komplizierter, insbesondere wenn es um den Schutz und die Visualisierung des East-West- und North-South-Netzwerktraffics geht. Es reicht nicht aus, den jeweiligen Trafficfluss im Vakuum zu betrachten. Ihre kritischen Assets können über mehrere AWS-Konten, Container oder Netzwerksicherheitsgruppen verteilt sein – und ohne den nötigen Kontext ist es schwierig bis unmöglich, sich einen genauen Überblick über Datenflüsse und Abhängigkeiten zu verschaffen.

Eingeschränkte Kontrolle für die Richtlinienerstellung: Wenn Ihr Unternehmen an Layer-7-On-Premises-Transparenz gewöhnt ist, sollten Sie jetzt nicht auf Layer-4-Transparenz zurückschalten und die detaillierten Einblicke und die umfassende Kontrolle verlieren, nur da sich Ihre Workloads jetzt in der Cloud befinden. Amazon-Sicherheitsgruppen unterstützen die Kontrolle des Traffics zu Layer 4. Doch mit Layer-7-Transparenz und -Kontrolle können Sie unabhängig von der zugrunde liegenden Infrastruktur mehr tun, als sich nur auf Ports und IPs zu verlassen – denn diese sind für Angriffserkennung oder Fehlerbehebung weitgehend unzureichend.

Containersicherheit: AWS verwendet Amazon-Sicherheitsgruppen, um Richtlinien für die Containersicherheit anzuwenden. Dies ist jedoch auf Cluster beschränkt und gilt nicht für einzelne Pods. Um einen umfassenden Einblick in die Kommunikation zu erhalten, benötigen Sie eine Lösung, die den Kontext eines Overlay-Netzwerks erkennt, das sich über Ihre Umgebung erstreckt, und die detaillierte Details auf Pod-Ebene bereitstellen kann. Und das Ganze wird noch komplexer, wenn Sie Netzwerkrichtlinien erstellen möchten, die sowohl VMs als auch Container umfassen. Denn das führt häufig dazu, dass Unternehmen zwei verschiedene Gruppen von Sicherheitskontrollen managen.

Bekämpfung dieser Probleme mit einer All-in-One-Sicherheitsplattform

Amazon stellt bestimmte integrierte Tools bereit, wie z. B. Amazon-Sicherheitsgruppen, mit denen einige der Herausforderungen bei der Migration Ihrer Infrastruktur in die Cloud bewältigt werden können. Wir empfehlen Unternehmen, das Potenzial von AWS IAM (Identity and Access Management) voll auszuschöpfen, indem sie Gruppen für die Zuweisung von Berechtigungen verwenden, regelmäßig die Anmeldedaten wechseln und IAM-Gruppen einsetzen, um die Einfachheit zu gewährleisten. Diese Tools allein sind jedoch nur ein Ausgangspunkt in der dynamischen Public Cloud von heute – insbesondere bei hybriden Umgebungen, die alles von veralteter Infrastruktur bis hin zu Multi-Cloud- und Containertechnologie enthalten können. Eine ausgereifte Sicherheitslösung ermöglicht es Ihnen, das Angebot von AWS durch eine Technologie zu ergänzen, die Schwachstellen beseitigt und nahtlos mit dem Rest Ihres Sicherheitspakets funktioniert, selbst in hybriden Umgebungen. Akamai Guardicore Segmentation bietet Folgendes:

Vollständige Transparenz von AWS-Instanzen

Je komplexer Ihre IT-Infrastruktur wird, desto wichtiger ist umfassende, automatisierte Transparenz. Manuelles Verschieben, Hinzufügen, Ändern und Löschen ist nicht nur unzuverlässig und anfällig für Lücken und Fehler, sondern verlangsamt auch Abläufe und ist somit ein Hindernis für die Einführung der Cloud. Im Gegensatz dazu werden durch verbesserte und automatisierte Transparenz sämtliche Anwendungen und Abläufe ermittelt, wodurch Sie umfassende Einblicke in Ihre Instanzen erhalten – bis hinunter zu einzelnen Prozessen.

Akamai Guardicore Segmentation umfasst eine leistungsstarke AWS-API, die Orchestrierungsdaten einbezieht und Ihnen wertvollen Kontext für die Kennzeichnung und Anwendungszuordnung liefert. Hierbei werden automatisch EC2-Tags zur Visualisierung von EC2-Instanzen abgerufen. Während Sie eine Baseline Ihrer Infrastruktur erstellen,

haben Sie alle Details, die Sie brauchen, um genau zu verstehen, wie Ihre Anwendungen miteinander kommunizieren, wo die Abhängigkeiten liegen und wie Richtlinien erstellt werden sollten, um flüssige Abläufe und Agilität zu ermöglichen. Anstatt eine separate Sicherheitslösung für jeden Cloudanbieter oder jede Cloudumgebung zu haben, können Nutzer native Cloudinformationen und AWS-spezifische Daten im selben Dashboard visualisieren. Unsere Lösung funktioniert über Plattformen, Infrastrukturen und Clouds hinweg, sodass garantiert keine blinden Flecken entstehen.

Segmentierung und Durchsetzung – eine Richtlinie, die der Workload folgt

Sobald Sie diese zentrale, einheitliche Übersicht für all Ihre Umgebungen erreicht haben, können Sie mit der Entwicklung und Implementierung von Sicherheitsrichtlinien beginnen. Anwendungsorientierte Richtlinien gehen über das hinaus, was Amazon-Sicherheitsgruppen allein erreichen können, und bieten Layer-7- statt Layer-4-Präzision. Einige Unternehmen setzen lokale Next-Generation-Firewalls ein, um laterale Netzwerkbewegung zu begrenzen, doch dieser Ansatz unterstützt nur eine grobe Segmentierung des East-West-Traffics. Als Lösung für detaillierte Segmentierungskontrollen ist das unerschwinglich, da umfangreiche Infrastruktur- und Netzwerkänderungen erforderlich sind, um den Traffic durch die Firewall umzuleiten. Und selbst bei einer On-Premises-Option stellt sich weiterhin die Frage, wie Unternehmen diese Kontrollebene in der Cloud beibehalten können. Die Antwort ist Layer-7-Mikrosegmentierung mit Richtlinien, die für dynamische Workloads entwickelt wurden, ohne dass die zugrunde liegende Netzwerkinfrastruktur geändert werden muss. Da sich die Richtlinie an der Workload selbst orientiert, sind manuelle Änderungen überflüssig, und Ihr Unternehmen ist in der Lage, die Agilität zu steigern und dynamische DevOps-Ansätze zu implementieren. Durch die Vereinfachung hybrider Umgebungen kann eine einzige Mikrosegmentierungsrichtlinie Regeln über Regionen, VPCs, Container, VMs und On-Premises durchsetzen – alles mit einem einheitlichen Richtlinienausdruck. Anhand der Transparenz, die wir Ihnen bieten, können Sie Segmentierungsrichtlinien in wenigen Minuten definieren und anwenden. Der Prozess der Richtlinienerstellung wird außerdem durch automatische Richtlinienempfehlungen verbessert, die erstklassige Sicherheitsprotokolle für die Public Cloud bereitstellen.

Angriffserkennung und Vorfallsreaktion in AWS Cloud

Mit einer umfassenden Lösung wie Akamai Guardicore Segmentation können Sie Ihre AWS-Sicherheit über Segmentierung oder Transparenz hinaus verbessern. Die Erkennung von Richtlinienverstößen ist ein wichtiger Teil der Angriffserkennung, da Sie so in Echtzeit auf potenzielle Cyberbedrohungen reagieren können – mit Präzision auf Anwendungsebene. Wir bieten verschiedene Methoden zur Erkennung von Sicherheitsverletzungen, die in Hybrid-Cloud-Umgebungen sofort auf böswillige Absichten aufmerksam machen:

- **Reputationsanalyse:** Erkennen Sie automatisch verdächtige Informationen innerhalb von Datenflüssen: von Domainnamen und IP-Adressen bis hin zu Datei-Hashes und Befehlszeilen.
- **Dynamische Täuschung:** Leiten Sie Angreifer ohne ihr Wissen in eine interaktive Honeypot-Umgebung um, in der Sie sicher aus ihrem Verhalten lernen können.
- **Tools zur Beschleunigung der Vorfallsreaktion:** Durch die Integration von AWS können Richtlinienverstöße oder Sicherheitsvorfälle in Echtzeit an AWS Security Hub gesendet werden.
- **Individuelles Threat Hunting:** Nutzen Sie die Infrastruktur von Akamai Guardicore Segmentation sowie globale Bedrohungsinformationen von Akamai, um auch die am besten getarnten Bedrohungen in Ihrer Hybrid-Cloud-Umgebung zu stoppen – mit unserem Service Akamai Hunt.

Die richtige Kombination für mehr Sicherheit in AWS und darüber hinaus

Die Umstellung auf die Cloud muss nicht bedeuten, dass Sie sich mit weniger Sicherheit, Transparenz oder Kontrolle zufriedengeben müssen, als Ihr Unternehmen in der On-Premises-Umgebung genießt. Mit Akamai Guardicore Segmentation erhalten Sie eine umfassende Übersicht über Ihre AWS-Instanzen und Ihre gesamte Infrastruktur. Mit dieser grundlegenden Übersicht können Richtlinien nahtlos erstellt werden und die AWS-Sicherheitsgruppen werden so erweitert, dass eine detaillierte Kontrolle ohne manuellen Support möglich ist. Ergänzt durch Angriffserkennung und Vorfallsreaktion erhalten Sie so eine End-to-End-Plattform, die Sie in der AWS Cloud umfassend schützt.

Weitere Informationen finden Sie unter akamai.com/guardicore.