AKAMAI-LÖSUNGSÜBERBLICK

Schutz von Workloads in AWS durch Akamai Guardicore Segmentation

Unternehmen nutzen weiterhin PaaS-Ressourcen in Amazon Web Services (AWS) und viele migrieren ihre kritischen Workloads in die Public Cloud. Diese Unternehmen sehen Vorteile wie geringere Kosten, verbesserte Skalierbarkeit und Performance sowie höhere Flexibilität im Unternehmen. Allerdings gibt es wichtige Sicherheitsbedenken, die mit dieser Umstellung auf die Cloud einhergehen, darunter:

Neues Toolset

Der Betrieb in einer Cloudumgebung erfordert völlig neue Sicherheitskontrollen. Diese Kontrollen müssen AWS in der Cloud und On-Prem über AWS-Outposts sowie hybride Cloud-Workloads unterstützen. Vorhandene Cloud-Sicherheitsgruppen sind möglicherweise für Assets und Ressourcen in der AWS-Cloud ausreichend, diese Kontrollen decken jedoch nicht den Schutz von zugehörigen Assets oder Ressourcen in anderen Umgebungen ab. Das bedeutet, dass Ihr Team mehrere Sicherheitstools verwalten muss, was zu potenziellen Sicherheitslücken führen kann.

Neues Sicherheitsmodell

Im Rahmen des Modells der geteilten Verantwortung von AWS bedeutet die Verwendung von AWS-Ressourcen in der Cloud oder On-Prem, dass Amazon nur für den Schutz der Infrastruktur verantwortlich ist, auf der alle in der AWS-Cloud angebotenen Dienste ausgeführt werden. Die alleinige Verantwortung für alle Anwendungssoftwares oder Dienstprogramme, die auf diesen Instanzen installiert sind, sowie für die Konfiguration der Sicherheitsgruppen liegt jedoch in der Verantwortung des Nutzers. Dazu gehört auch der Schutz und die Überwachung des Traffics (sowohl North-South als auch East-West) sowie die Implementierung von Kontrollmechanismen, um Sicherheitsverletzungen zu erkennen, zu verhindern und darauf zu reagieren.

Geringere Transparenz und Kontrolle der Infrastruktur

Dieselben Vorteile, die die AWS-Umgebung betrieblich attraktiv machen, können auch zu einer geringeren Kontrolle und Transparenz von Assets führen, die über mehrere AWS-Konten, Virtual Private Clouds (VPCs) und Netzwerksicherheitsgruppen verteilt sind, sowie zu einem breiteren hybriden Ökosystem eines Unternehmens.

Wichtigste Vorteile

- End-to-End-Lösung zum Schutz von Workloads in AWS, einschließlich PaaS-Ressourcen, sodass DevOps- und Sicherheitsteams knappe Ressourcen auf Kernaufgaben anstatt auf das Sicherheitsmanagement im Rechenzentrum verwenden können
- Strenge Richtlinien zur Mikrosegmentierung verwalten und durchsetzen, die über AWS hinausgehen und Assets umfassen, die On-Prem und sogar über Public Clouds hinweg verfügbar sind
- Richtlinienverstöße zuverlässig erkennen und in Echtzeit darauf reagieren
- Umgebungen durch mehrere Methoden zur Erkennung und Verhinderung von Eindringlingen vor potenziellen Sicherheitslücken schützen, einschließlich Reputationsanalyse und dynamischer Täuschung in Echtzeit

Akamai Guardicore Segmentation für AWS-Sicherheit

Akamai Guardicore Segmentation bietet eine einheitliche Lösung für Transparenz und Richtliniendurchsetzung für Workloads und PaaS-Ressourcen, die in Ihrer AWS-Cloud, Ihren Outposts und Ihren hybriden Umgebungen ausgeführt werden. Die Lösung bietet Mikrosegmentierung und Transparenz auf Anwendungsebene sowie Funktionen zur Erkennung von und Reaktion auf Sicherheitsverletzungen.

Automatische Erkennung und Transparenz

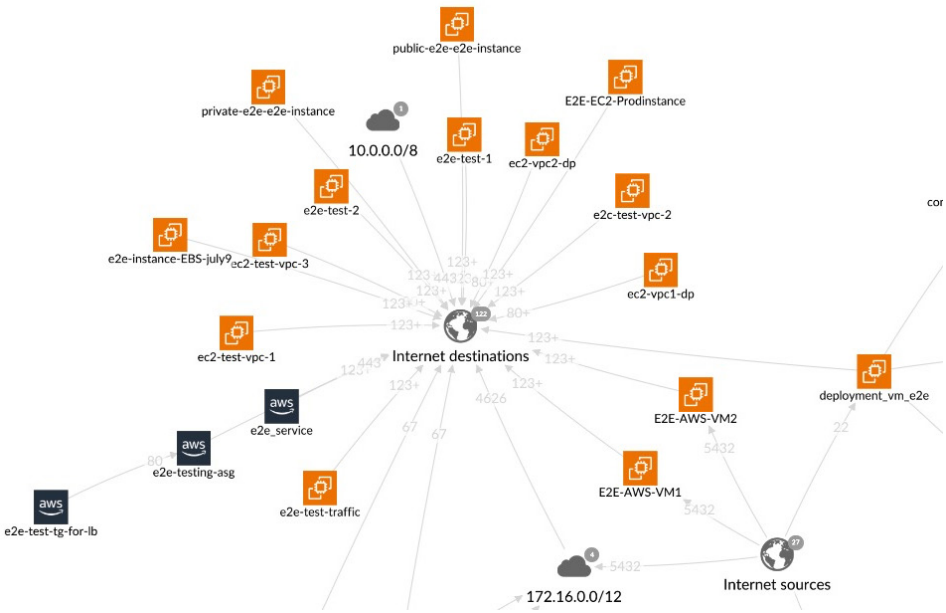
- Automatische Visualisierung von Anwendungen, Ressourcen und deren Kommunikationsabläufe
- Schnelles Verständnis und Baselining des Anwendungsverhaltens
- Zuordnung von Anwendungsabhängigkeiten mit granularer Transparenz bis hin zur Prozessebene (Layer 7)

Leistungsstarke Segmentierung und Durchsetzung

- Definieren von Segmentierungsrichtlinien in nur wenigen Minuten
- Automatische Richtlinienempfehlungen
- Intelligente Kennzeichnung und Gruppierung, die eine einfache Navigation über komplexe Umgebungen hinweg ermöglichen

Bedrohungserkennung und Reaktion auf Vorfälle

- Keine Konfiguration erforderlich; Mehrwert ab Tag 1
- Mehrere Erkennungsmethoden decken alle Arten von Bedrohungen ab
- Dynamische Täuschung bietet vollständige Netzwerkabdeckung



Visualisieren und schützen Sie Anwendungen und Ressourcen in AWS mit Akamai Guardicore Segmentation

> Durch die Entscheidung für Akamai Guardicore Segmentation konnten wir kritische Sicherheitslücken bei der Mikrosegmentierung und der Transparenz auf Anwendungsebene sowie bei der Erkennung und Abwehr von Angriffen sowohl auf AWS- als auch auf lokalen Servern schließen.
>
> **– DevOps-Teamleiter**
> **Biotechnologie-Unternehmen**

Nahtloser Schutz von Workloads und PaaS-Ressourcen in AWS. Weitere Informationen finden Sie unter: akamai.com/guardicore.