AKAMAI-LÖSUNGSÜBERBLICK

Segmentierung für Hybrid-Cloudumgebungen

Wehren Sie Angriffe durch Segmentierung für Ihre Cloudinfrastruktur ab

Weil Anwendungen und Workloads zunehmend in die Cloud verlagert werden, stehen Sicherheitsteams und Cloud-Teams vor immer mehr Herausforderungen. Dazu gehört die Ausweitung der Segmentierung und der Zero-Trust-Prinzipien auf Anwendungen und Workloads in Cloudumgebungen. Mit Akamai Guardicore Segmentation können Unternehmen die Angriffsfläche reduzieren und Angriffe auf Anwendungen und Workloads in ihren Public-Cloudumgebungen verhindern, ohne dass dafür Agents installiert werden müssen. Dies wird durch die automatische Anwendungserkennung, die umfassende Visualisierung von Cloud-Flows, präzise Segmentierungsrichtlinien und Netzwerksicherheitswarnungen erreicht – und alles über eine einzige Konsole.

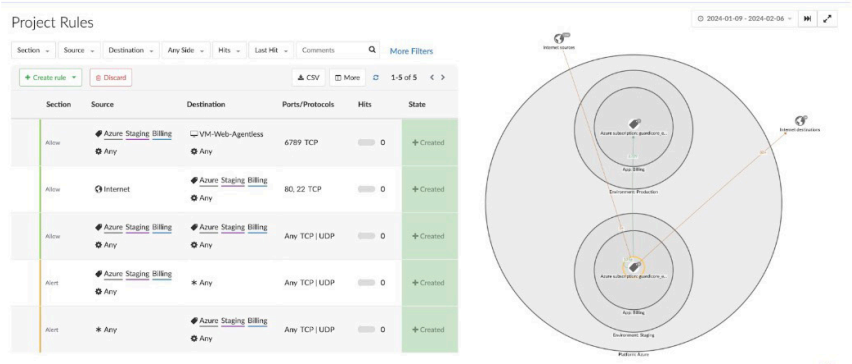
Einzigartige Cloudherausforderungen

Moderne Unternehmen verlassen sich zunehmend auf die Cloud, um ihre kritischen Systeme zu verwalten und ihre wertvollsten Daten zu speichern.

Laut dem IBM-Bericht „Cost of a Data Breach" (Kosten durch Datendiebstahl) 2023 betrafen 82 % der Sicherheitsverstöße Daten, die in einer Public oder Private Cloud oder in beiden Umgebungen gespeichert waren. Angreifern gelang es oft, Zugriff auf mehr als eine Cloudpattform zu erhalten, wobei 39 % der Sicherheitsverstöße mehrere Umgebungen betrafen und überdurchschnittliche Kosten von 4,75 Millionen US-Dollar verursacht wurden.

Die einzigartige und dynamische Natur der Cloud bedeutet, dass Cloudworkloads stärker externen Bedrohungen ausgesetzt sind als lokale Ressourcen. Sicherheitsteams stehen vor mehreren einzigartigen Herausforderungen:

- **Schlechte Transparenz**: Die Transparenz des Cloudanbieters basiert auf Rohprotokollen der Flows zwischen verschiedenen Workloads. Ohne ein klares Verständnis der Beziehungen zwischen verschiedenen Workloads und Anwendungen in Cloudumgebungen ist die Erstellung effektiver Sicherheitsrichtlinien fast unmöglich.
- **Keine Einzelrichtlinie**: Die Erstellung einer einheitlichen Richtlinie für Hybrid-Cloudumgebungen mit ausschließlich nativen Cloudsicherheitstools ist äußerst komplex. Dies liegt daran, dass jede Cloudinstanz ihre eigenen Objekte und Regeln und somit ihre eigenen Richtlinien hat, was zu einer fragmentierten Richtlinie führt.
- **Fehlende einheitliche Governance**: Sicherheit hat in der Cloud nicht immer Priorität. Dies führt zu Spannungen zwischen Sicherheitsteams und Anwendungseigentümern, die Workloads hochfahren, ohne dabei immer die Sicherheit zu berücksichtigen.



Schirmen Sie eine Azure-Anwendung mit automatisierten Richtlinienvorschlägen ab

Vorteile für Ihr Unternehmen

Visualisierung von Cloud-Flows über eine einzige Schnittstelle
Finden Sie heraus, wie Ihre Cloudworkloads und -anwendungen mithilfe einer dynamischen Netzwerkabhängigkeitsübersicht interagieren, und wenden Sie einfach Sicherheitskontrollen an.

Konsistente Segmentierungsrichtlinie
Implementieren Sie eine einzige Segmentierungslösung, die konsistent in Hybrid-Cloudumgebungen funktioniert, und vermeiden Sie anbieterspezifische Lösungen, die Sicherheitssilos schaffen.

Verhindern von Sicherheitsverstößen
Passen Sie Sicherheitsrichtlinien an Änderungen in Ihrer Cloudumgebung an und ersparen Sie Ihrem Team manuelle Updates.

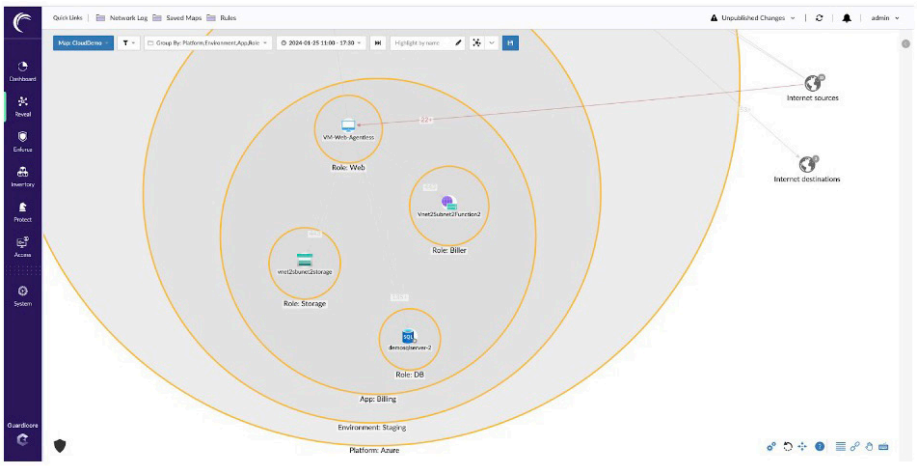
Akamai

Bekämpfen Sie Cloudsicherheitsbedrohungen

Akamai Guardicore Segmentation erweitert seine branchenführende Segmentierung auf Cloudanwendungen und -workloads. Durch die Ausweitung der Segmentierung auf Ihre Cloudressourcen wird jede nicht autorisierte Verbindung automatisch gestoppt. Dadurch werden laterale Bewegungen und Schäden durch Sicherheitsverstöße oder Ransomware eingeschränkt.

Wichtige Funktionen

- **Umfassende cloudnative Transparenz und Durchsetzung ohne Agents –** dadurch können Administratoren Cloudworkflows mithilfe einer interaktiven Karte der echten Netzwerkströme in nahezu Echtzeit visualisieren, die Anwendungsabhängigkeiten verstehen und die DevOps- und SecOps-Teams im Hinblick auf die Sicherheits-Governance für Cloudnetzwerke zusammenführen.
- **Hybride Durchsetzungs-Engine, die mehrere Durchsetzungspunkte nutzt –** damit können Unternehmen den Zweck der Netzwerkrichtlinie einfach definieren. Die Richtlinien-Engine von Akamai Guardicore Segmentation kümmert sich um den Rest und entscheidet dynamisch, welche agentbasierten und agentlosen Durchsetzungspunkte im gesamten Rechenzentrum verwendet werden.
- **Integrierte Reputationsanalyse und Threat Intelligence Firewall –** diese Funktionen wurden entwickelt, um im Falle eines Angriffs die Zeit bis zur Erkennung und Reaktion zu verkürzen.
- **Skalierbare und sichere Lösung –** so wird sichergestellt, dass die Daten nicht aus der Cloudumgebung entfernt werden und die Lösungsarchitektur innerhalb der Cloud automatisch skaliert wird.



Eine Übersicht für lokale und Hybrid-Cloudumgebungen

Weitere Informationen finden Sie unter akamai.com/guardicore.