AKAMAI-LÖSUNGSÜBERBLICK

Visualisieren und Sichern von Kubernetes mit Akamai Guardicore Segmentation

Kubernetes (K8s) ist nach wie vor eine der am weitesten verbreiteten Technologien für die Bereitstellung und Verwaltung von Anwendungen in cloudnativen Rechenzentren, mit noch nie dagewesener Geschwindigkeit und Flexibilität. Laut Gartner werden 90 % der globalen Unternehmen bis 2026 containerisierte Anwendungen in der Produktion ausführen, gegenüber 40 % im Jahr 2021. Darüber hinaus ist damit zu rechen, dass 20 % aller Unternehmensanwendungen bis 2026 in Containern ausgeführt werden. Im Jahr 2020 waren es weniger als 10 %.[1] Aufgrund ihrer wachsenden Beliebtheit zieht diese Plattform nicht nur Nutzer an, sondern auch Angreifer, was Sicherheitsteams dazu zwingt, sich Herausforderungen zu stellen, auf die sie anfangs nicht vorbereitet waren.

Neue Technologie, neue Sicherheitsherausforderungen

Ein K8s-Cluster ist ein komplettes Ökosystem, das DNS-Services, Lastausgleich, Networking, automatische Skalierung und sonstige für die Ausführung von Anwendungen erforderliche Funktionen umfasst. Die breite Akzeptanz von K8s überrascht nicht, denn mit ihnen können Unternehmen schnell Innovationen entwickeln und Kosten sparen. Doch es sind gerade die überzeugenden Eigenschaften von K8s, die die Sicherung erschweren.

Da es sich um ein flaches Netzwerk handelt, kann jeder Pod mit jedem anderen Pod im Cluster kommunizieren. Nach dem Eindringen ins Netzwerk können sich Angreifer lateral bewegen und sich auf alle verbundenen Rechenzentren Zugriff verschaffen. Dieser Vorgang ist typisch für Ransomware-Angriffe, dieselbe Strategie kann jedoch leicht bei einem anderen Angriffsvektor genutzt werden.

Für den State of Kubernetes Security Report 2022 von Red Hat wurden mehr als 300 Fachkräfte aus den Bereichen DevOps, Engineering und Sicherheit befragt. Davon haben 93 % in den letzten 12 Monaten mindestens einen Sicherheitsvorfall in ihren K8s-Umgebungen erlebt, der in manchen Fällen zu Umsatzeinbußen oder Kundenverlusten führte.

Die Lösung: Mikrosegmentierung

Das K8s-Konzept der Anwendungsbereitstellung unterscheidet sich von anderen Konzepten und erfordert andere Sicherheitsmaßnahmen. Sicherheitsteams können eine vorhandene Sicherheitslösung nicht einfach in der Erwartung mit Lift and Shift verlagern, dass die Lösung mit dieser neuen Technologie funktioniert. Die Sicherung von K8s-Clustern muss auf eine für K8s native Art und Weise erfolgen.

Aus diesem Grund bietet Akamai eine softwarebasierte Segmentierungslösung mit speziellem Support für die Sicherung von K8s-Clustern an. Die Lösung verhält sich für andere Workloads in der Umgebung auf ähnliche Weise, darunter Legacy-Systeme, Clouds, lokale Workloads und Container. Infolgedessen können Sie Ressourcen im gesamten Unternehmen in einer einzigen Lösung visualisieren, sichern und verwalten.

Vorteile

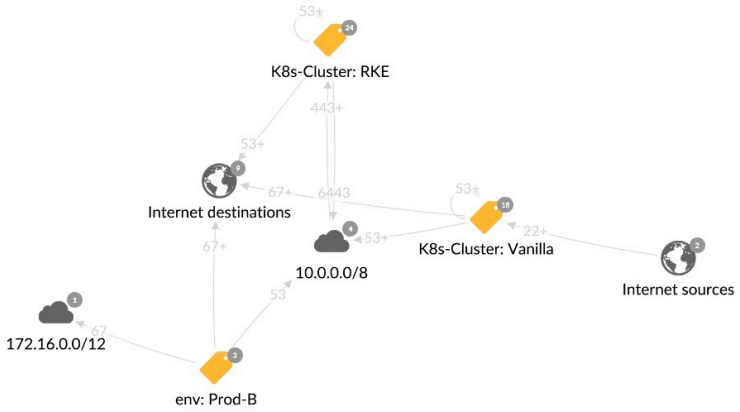
- Visualisierung, Durchsetzung und Überwachung in K8s-Clustern mit derselben Lösung und denselben Prozessen wie bei allen anderen Ressourcen
- Einfacher Schutz vor gezielten Angriffen, die K8s-Sicherheitslücken ausnutzen
- Echtzeit- und Verlaufsansicht aller Verbindungen zwischen Pods, Diensten und Hosts oder Namespaces
- Sofort einsatzbereite Vorlagen zur einfachen Abschirmung von K8s-Clustern
- Einheitliche Konsolen- und Richtlinienverwaltung für K8s, Endpunkte, lokale und Cloud-Workloads
- Empfang von Betriebsdaten in den bereitgestellten Clustern, einschließlich der Anzahl der sie überwachenden Agenten und des Zustands der Orchestrierung von Kubernetes

Akamai

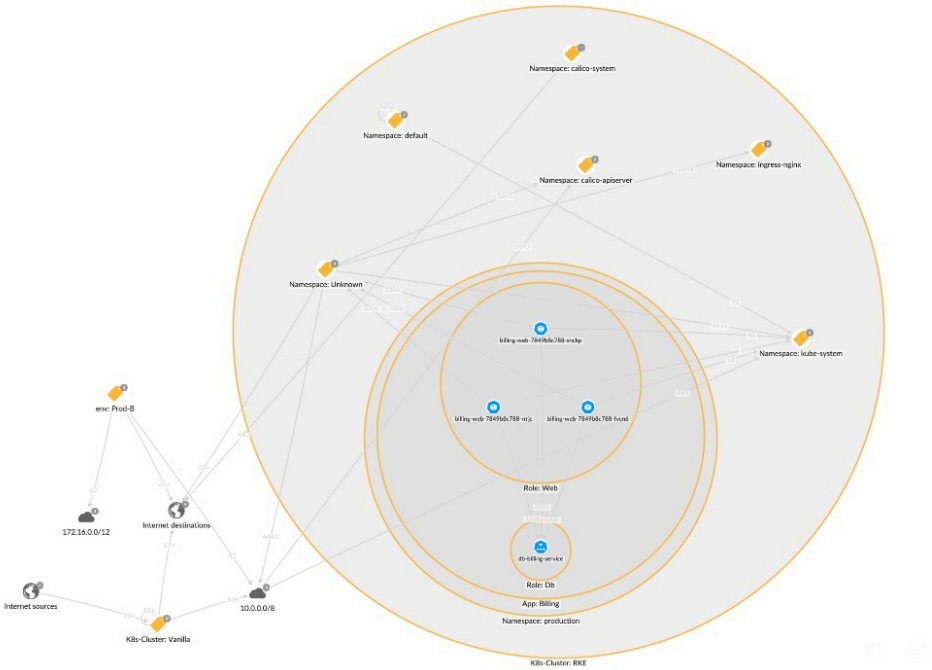
Wichtige Funktionen für die Segmentierung von Kubernetes-Clustern

Transparenz. Akamai Guardicore Segmentation gibt Ihnen Überblick darüber, was in Ihrer K8s-Umgebung ausgeführt wird. Sie können damit auch überprüfen, ob der Datenverkehr nur zum gewünschten Ort geleitet wird. Das ist für eine erfolgreiche Richtlinienerstellung von entscheidender Bedeutung.

- **Abhängigkeitsübersichten** – Akamai stellt eine Übersicht zur Visualisierung interner und rechenzentrenübergreifender Kommunikation bereit, und das für Technologien aller Art wie VMs, K8s, Docker-Container und mehr. Dank dieser Übersichten ist es möglich, verdächtige Verbindungen zwischen Pods, Diensten und Hosts oder Namespaces sichtbar zu machen und zu erkennen.
- **Labels** – In den Übersichten ist genau abgebildet, wie die Anwendungen im Cluster bereitgestellt werden. Erreicht wird das durch Verwendung mehrerer Ebenen von Labels. Die Visualisierung beschreibt die Hierarchie der K8s, wie sie von den Verwaltern der Anwendung geplant wurde. Dank dieser Detailgenauigkeit wissen Nutzer von Akamai genau, was im Cluster bereitgestellt wird und welche Netzwerkbeziehungen zwischen den bereitgestellten Anwendungen und der übrigen Infrastruktur bestehen.



In der Reveal-Übersicht dargestellte Cluster. Durch Doppelklicken auf einen Cluster werden die Namespaces und ihre Verbindungen innerhalb des Clusters angezeigt.



Anzeige von Pod-Informationen in der Reveal-Übersicht

> 93 % der Befragten erlebten in den letzten 12 Monaten mindestens einen Sicherheitsvorfall in ihren K8s-Umgebungen, der in manchen Fällen zu Umsatzeinbußen oder Kundenverlust führte.

Durchsetzung. Um die Angriffsfläche in K8s-Clustern zu minimieren, ist eine strenge Segmentierungsrichtlinie erforderlich. Eine Lösung zur Durchsetzung der Segmentierung muss zwei Hauptkriterien erfüllen: Sie darf nicht aufdringlich und muss frei von Einschränkungen in Bezug auf Skalierung und Performance sein, und sie sollte eine flexible Möglichkeit bieten, alle Ebenen von K8s-Objekten abzuschirmen, darunter Namespaces, Controller und K8s-Label.

Akamai nutzt das native CNI (Container Network Interface) von Kubernetes. Das CNI besteht aus einem Plug-in für Netzwerksicherheitsrichtlinien, das ursprünglich für die Durchsetzung der Netzwerksegmentierung in K8s konzipiert wurde. Das ist eine unaufdringliche Methode ohne Einschränkungen in Bezug auf die Skalierung. Spezielle Vorlagen ermöglichen es Nutzern, geschäftskritische Kubernetes-Anwendungen abzuschirmen. Dabei spielt es keine Rolle, ob es sich um einen Namespace, eine Anwendung oder ein anderes Objekt handelt.

Ring Fence a K8s Application by whitelisting inbound and outbound flows for an application on K8s cluster K8s-Cluster within Namespace

Vorlage für das Abschirmen kritischer Kubernetes-Anwendungen

Erweiterte Überwachung. Mithilfe eines erweiterten Systems zur Protokollierung und Überwachung wird ein dediziertes Netzwerkprotokoll an K8s-Netzwerke angepasst, das Zieldienste, Knoten-IPs, Quell- und Zielports sowie Prozesse für jedes Ereignis anzeigt. Damit bietet sich eine einfache Möglichkeit, anomale Aktivitäten im Netzwerk zu untersuchen und Daten in eine Drittanbieteranwendung wie SIEM zu exportieren.

Laut dem State of Kubernetes Security Report 2022 von Red Hat ist Sicherheit bei der Einführung von K8s eines der wichtigsten Anliegen. Sicherheitsprobleme führen bei der Bereitstellung von Anwendungen in der Produktion noch immer zu Verzögerungen.

Zusammenfassung

Kubernetes ist zu einem integralen Bestandteil vieler Geschäftsumgebungen geworden. Der Ansatz unterscheidet sich durch effiziente Ressourcennutzung, optimierte Entwicklungsprozesse sowie bessere Portabilität und Skalierbarkeit von vorangegangenen. Dieser andersartige Ansatz für die Anwendungsentwicklung erfordert jedoch auch einen anderen Sicherheitsansatz.

Akamai Guardicore Segmentation ist eine ganzheitliche Lösung, mit der Sie den Kommunikationsfluss bereitstellungsübergreifend (in Bare Metal, VMs, K8s usw.) sehen können – in einer einzigen Übersicht. Der unaufdringliche nicht intrusive und skalierbare K8s-native Ansatz für Transparenz, Überwachung und Durchsetzung entlastet Sicherheits- und Entwicklungsteams und versetzt Ihr Unternehmen in die Lage, ohne Abstriche bei der Sicherheit schnell Innovationen zu entwickeln.

Weitere Informationen erhalten Sie unter akamai.com oder vom Vertriebsteam von Akamai.

1. Gartner, The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem, Arun Chandrasekaran, Wataru Katsurashima, 18. August 2021.