DESCRIZIONE DELLA SOLUZIONE AKAMAI

# Visualizzazione e protezione di Kubernetes con Akamai Guardicore Segmentation

Il sistema Kubernetes (K8s) rimane una delle tecnologie più ampiamente adottate per la distribuzione e la gestione delle applicazioni nei data center nativi nel cloud, poiché offre un tipo di velocità e flessibilità mai raggiunto prima d'ora. Secondo Gartner, il 90% delle organizzazioni a livello globale riuscirà ad eseguire applicazioni containerizzate in produzione entro il 2026, partendo da un 40% nel 2021. Inoltre, entro il 2026, il 20% di tutte le applicazioni aziendali verranno eseguite in container, a fronte di meno del 10% nel 2020.[1] La crescente popolarità di questa piattaforma ha attratto non solo gli utenti, ma anche i criminali, costringendo i team addetti alla sicurezza ad affrontare sfide a cui non erano inizialmente preparati.

## Nuove tecnologie = nuove sfide per la sicurezza

Un cluster K8s fornisce un ecosistema completo, che include servizi DNS, bilanciamento del carico, connettività di rete, scalabilità automatica e le altre funzionalità richieste per le applicazioni che vengono eseguite. Ecco perché non sorprende che la tecnologia K8s venga adottata così ampiamente visto che consente alle aziende di innovarsi rapidamente e risparmiare in termini economici. Tuttavia, le stesse caratteristiche che rendono la tecnologia K8s così attraente la rendono anche più difficile da proteggere.

Si tratta di una rete intrinsecamente semplice, in cui tutti i pod possono comunicare tra loro all'interno del cluster. Dopo la violazione iniziale, i criminali possono muoversi in modo laterale e ottenere l'accesso a tutti i data center connessi. È questo il tipico processo di un attacco ransomware, tuttavia è possibile utilizzare la stessa strategia impiegando un altro vettore di attacco.

Secondo l'indagine descritta nel 2022 Red Hat State of Kubernetes Security Report e condotta su più di 300 DevOp, tecnici e professionisti della sicurezza, il 93% degli intervistati ha risposto di aver registrato almeno un problema di sicurezza nei propri ambienti K8s nel corso dei 12 mesi precedenti, il che, a volte, ha determinato una perdita di profitti o di clienti.

## La soluzione sta nella microsegmentazione

Il concetto stesso di distribuzione delle applicazioni alla base della tecnologia K8s è diverso e richiede metodi di sicurezza differenti. I team addetti alla sicurezza non possono semplicemente passare da una soluzione di protezione esistente ad un nuovo sistema di sicurezza e aspettarsi che tutto funzioni correttamente con la nuova tecnologia implementata. Per proteggere i cluster K8s, bisogna adottare metodi nativi per questa tecnologia.

Ecco perché Akamai offre una soluzione di segmentazione basata su software con un supporto dedicato per la protezione dei cluster K8s. Questa soluzione si comporta in modo simile ad altri carichi di lavoro già esistenti nel vostro ambiente, tra cui sistemi legacy, cloud, risorse on-premise e container. Di conseguenza, la soluzione vi consente di visualizzare, proteggere e gestire le risorse aziendali da un'unica posizione.

## Vantaggi

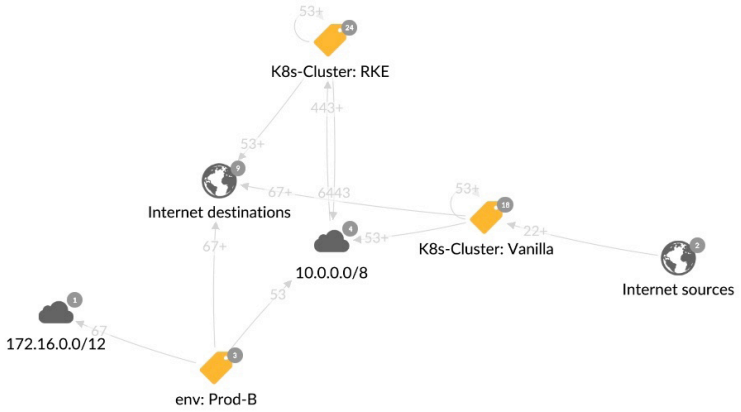
- Visualizzazione, applicazione e monitoraggio dei cluster K8s da un'unica posizione e tramite gli stessi processi di altre risorse
- Semplice protezione dagli attacchi avanzati in grado di sfruttare le vulnerabilità K8s
- Visualizzazione cronologica e in tempo reale di tutti i collegamenti tra pod, servizi e host o spazi dei nomi
- Modelli out-of-the-box per isolare in modo semplice i cluster K8s
- Gestione unificata di policy e console in sistemi K8s, endpoint e carichi di lavoro on-premise e su cloud
- Ricezione dei dati operativi sui cluster distribuiti, tra cui il numero di agenti che si occupano del loro monitoraggio e lo stato dell'orchestrazione di Kubernetes

Akamai

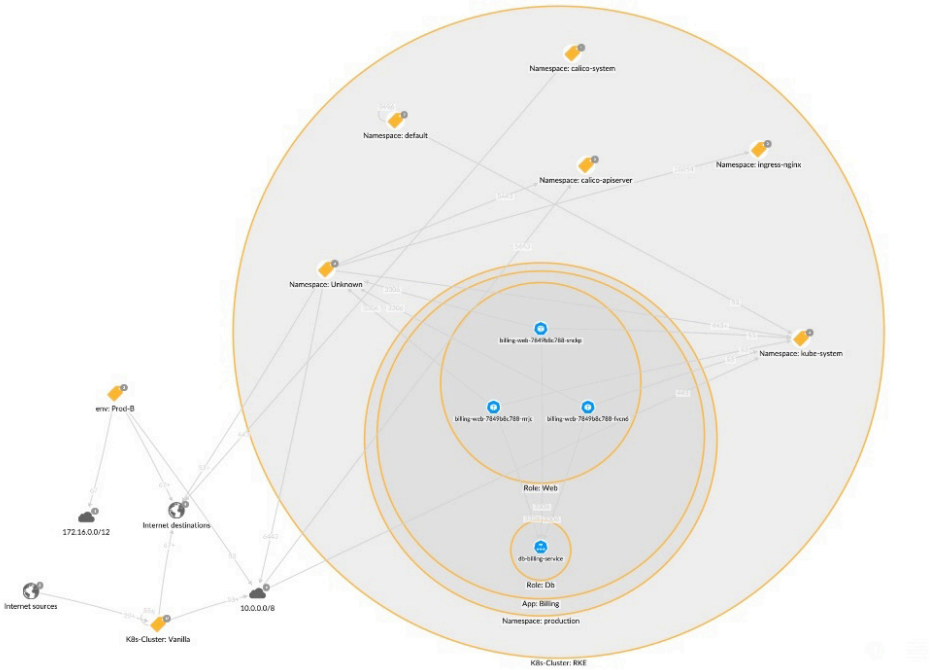
## Funzionalità principali per la segmentazione dei cluster Kubernetes

**Visibilità.** Akamai Guardicore Segmentation vi consente di sapere quali applicazioni vengono eseguite nei vostri ambienti K8s per verificare che il traffico dei dati sia indirizzato solo alle destinazioni corrette, il che è fondamentale per garantire il successo nella creazione delle policy.

- **Mappe di interdipendenza**: Akamai fornisce una mappa per la visualizzazione delle comunicazioni che avvengono internamente e nei data center per tutti i tipi di tecnologie, come VM, K8s, container Docker e molto altro. Queste mappe offrono funzioni di visibilità e rilevamento per eventuali connessioni sospette all'interno di pod, servizi e host o spazi dei nomi.
- **Etichette**: le mappe riflettono in modo accurato il modo con cui le applicazioni vengono distribuite nel cluster tramite l'utilizzo di più livelli di etichette. Questa visualizzazione descrive la gerarchia K8s come è stata pianificata dai responsabili delle app. Questo livello di dettagli aiuta gli utenti delle soluzioni Akamai a comprendere esattamente quali applicazioni sono state distribuite nel cluster, nonché le relazioni di rete esistenti tra le applicazioni distribuite e il resto dell'infrastruttura




*Rappresentazione dei cluster nella mappa completa. Facendo doppio clic su un cluster, vengono visualizzati gli spazi dei nomi e le relative interconnessioni all'interno del cluster.*




*La mappa completa visualizza le informazioni sul pod*

> Il 93% degli intervistati ha risposto di aver registrato almeno un problema di sicurezza nei propri ambienti K8s nel corso dei 12 mesi precedenti, il che, a volte, ha determinato una perdita di profitti o di clienti.

**Applicazione.** Per ridurre la superficie di attacco nei cluster K8s, è richiesta una rigorosa policy di segmentazione. Una soluzione di segmentazione deve soddisfare due requisiti principali: non deve essere intrusiva né prevedere limitazioni in termini di scalabilità e performance; e deve consentire di isolare in modo flessibile gli oggetti K8s di tutti i livelli, inclusi spazi dei nomi, controller ed etichette K8s.

Akamai si avvale della tecnologia CNI (Container Network Interface) di Kubernetes, che si basa su un plug-in della policy di sicurezza di rete originariamente progettato per applicare la segmentazione di rete nei cluster K8s. Si tratta di un metodo non intrusivo che non prevede limitazioni in termini di scalabilità. I modelli dedicati consentono agli utenti di isolare le applicazioni Kubernetes business-critical, inclusi spazi dei nomi, applicazioni o altri oggetti.

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

*Modello di isolamento delle applicazioni Kubernetes*

**Monitoraggio avanzato.** Tramite un sistema avanzato di registrazione e monitoraggio, un registro di rete dedicato viene adattato in base alla connettività di rete K8s per la visualizzazione di servizi di destinazione, IP dei nodi, porte di origine e destinazione, nonché processi per ogni evento. In tal modo, potete esaminare in modo semplice eventuali attività anomale registrate nella rete ed esportare i dati in applicazioni di terze parti come gli strumenti SIEM.

## Riepilogo

Il sistema Kubernetes è diventato parte integrante di molti ambienti aziendali. Si tratta di un approccio diverso rispetto alle tecnologie precedenti poiché offre un utilizzo efficiente delle risorse, processi di sviluppo più snelli e un maggior livello di portabilità e scalabilità. Tuttavia, questo diverso approccio allo sviluppo delle applicazioni ha bisogno anche di un altro approccio alla sicurezza.

Akamai Guardicore Segmentation offre una soluzione olistica che vi consente di visualizzare il flusso delle comunicazioni in vari tipi di implementazioni (bare metal, VM, K8s, ecc.) da un'unica mappa. Fornendo un approccio K8s nativo, non intrusivo e scalabile per la visibilità, il monitoraggio e l'applicazione, questa soluzione rimuove l'onere che grava sui team addetti alla sicurezza e allo sviluppo, consentendo alle aziende di innovarsi rapidamente senza compromessi per la sicurezza.

Come descritto nel 2022 Red Hat State of Kubernetes Security Report, la sicurezza è una delle principali preoccupazioni alla base dell'adozione della tecnologia K8s, i cui problemi continuano a causare ritardi nella distribuzione delle applicazioni in produzione.

**Per ulteriori informazioni, visitate il sito akamai.com o contattate il team di vendita di Akamai.**

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