AKAMAI SOLUTION BRIEF

Visualize and Secure Kubernetes with Akamai Guardicore Segmentation

Kubernetes (K8s) remains one of the most widely adopted technologies for deploying and managing applications in cloud-native data centers, offering a kind of speed and flexibility that was never before possible. According to Gartner, 90% of global organizations will be running containerized applications in production by 2026 — up from 40% in 2021. In addition, by 2026, 20% of all enterprise applications will run in containers — up from fewer than 10% in 2020.[1] The growing popularity of this platform has attracted not only users, but attackers as well, forcing security teams to face challenges they were not initially prepared for.

New technology, new security challenges

A K8s cluster provides a complete ecosystem, including DNS services, load balancing, networking, autoscaling, and any other capability required for running applications. It's not surprising that K8s is seeing such a wide adoption, as it enables enterprises to achieve both rapid innovation and cost savings. However, the same attributes that make K8s so compelling also make it more challenging to secure.

It is an inherently flat network, meaning each pod can communicate with any other pod inside the cluster. Upon initial breach, the attackers can move laterally and gain access to all connected data centers. This is a typical ransomware attack process, but the same strategy can easily be leveraged by another attack vector.

According to the 2022 Red Hat State of Kubernetes Security Report, surveying more than 300 DevOps, engineering, and security professionals, 93% of respondents experienced at least one security incident in their K8s environments in the past 12 months, sometimes leading to revenue or customer loss.

The solution: microsegmentation

The K8s concept of application deployment itself is different and requires different security methods. Security teams cannot just "lift and shift" an existing security solution and expect it to work with this new technology. In order to secure K8s clusters, it must be done in a way that is native to K8s.

This is why Akamai offers a software-based segmentation solution that has dedicated support for securing K8s clusters. The solution behaves similarly for other workloads in your environment, including legacy systems, clouds, on-premises workloads, and containers. As a result, you can visualize, secure, and manage assets across your company through a single pane of glass.

Benefits

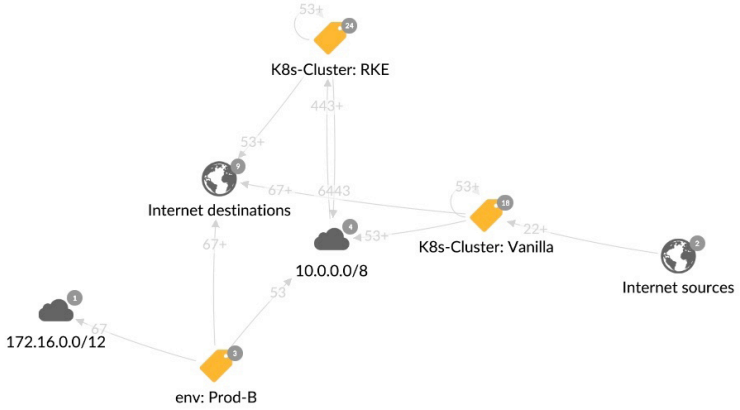
- Visualize, enforce, and monitor your K8s clusters through the same pane of glass and processes as any other assets
- Simply protect against advanced attacks that exploit K8s vulnerabilities
- Real-time and historical view of all connections between pods, services, and hosts or namespaces
- Out-of-the-box templates to easily ringfence K8s clusters
- Unified console and policy management across K8s, endpoints, on-premises, and cloud workloads
- Receive operational data on the deployed clusters, including the number of agents monitoring them and state of the Kubernetes orchestration

Akamai

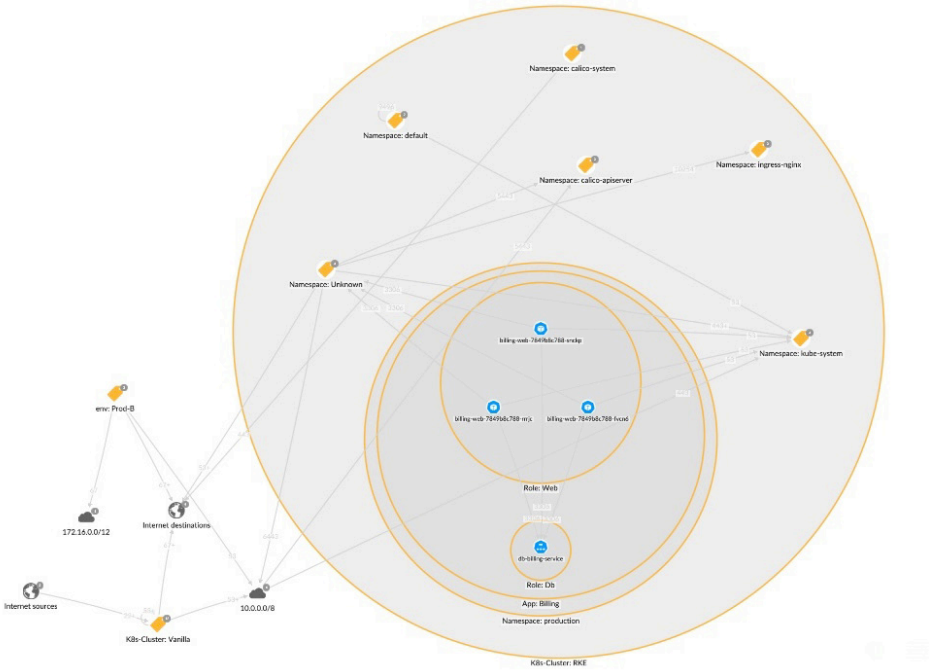
Key capabilities for segmenting Kubernetes clusters

Visibility. Akamai Guardicore Segmentation provides the ability to know what's running in your K8s environment and to confirm that your traffic is going only where you want it to go, which is critical to successful policy creation.

- **Interdependency maps** — Akamai provides a map for visualizing communications internally and across data centers for all types of technologies such as VMs, K8s, Docker containers, and more. These maps enable visibility and detection of any suspicious connection among pods, services, and hosts, or namespaces.
- **Labels** — The maps accurately reflect the way the applications are deployed in the cluster by using multiple layers of labels. This visualization describes the K8s hierarchy as it was planned by the app's managers. This level of detail helps Akamai's users understand exactly what is deployed in the cluster and the networking relations between the deployed apps and the rest of the infrastructure.



Clusters represented on the Reveal map. Double-clicking a cluster reveals the namespaces and their interconnections within the cluster.



Reveal map displays pod information

> 93% of respondents experienced at least one security incident in their K8s environments in the past 12 months, sometimes leading to revenue or customer loss.

Enforcement. To help minimize the attack surface in K8s clusters, a strict segmentation policy is required. A segmentation enforcement solution should address two main criteria: It should be nonintrusive, without any scale and performance limitations; and it should provide a flexible way to ringfence all levels of K8s objects, including namespaces, controllers, and K8s labels.

Akamai leverages the native Kubernetes Container Network Interface (CNI). The CNI consists of a network security policy plug-in that was originally designed for network segmentation enforcement in K8s. This is a nonintrusive method with no scale limitations. Dedicated templates enable users to ringfence Kubernetes business-critical applications — whether it's a namespace, application, or any other object.

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

Kubernetes application ringfencing template

Advanced monitoring. Using an advanced logging and monitoring system, a dedicated network log is adjusted to K8s networking, displaying destination services, node IPs, source and destination ports, and processes for every event. This provides an easy way to investigate anomalous activity in the network, and export data to a third-party application such as SIEM.

According to the 2022 Red Hat State of Kubernetes Security Report, security is one of the biggest concerns with K8s adoption, and security issues continue to cause delays in deploying applications into production.

Summary

Kubernetes has become an integral part of many business environments. It's a different approach than what's come before, offering resource usage efficiency, more streamlined development processes, and increased portability and scalability. But this different approach to application development necessitates a different approach to security as well.

Akamai Guardicore Segmentation provides one holistic solution that allows you to see communication flows across different types of deployments (bare metal, VMs, K8s, etc.) all from one map. It provides a nonintrusive and scalable K8s-native approach for visibility, monitoring, and enforcement that takes the burden off security and development teams, enabling your business to innovate quickly without sacrificing security.

To learn more, visit akamai.com or contact your Akamai sales team.

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