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. The need for an effective security solution has become even more critical, though, as 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. One of the best ways to secure Kubernetes clusters is with microsegmentation, and Akamai's leading solution provides the capabilities you need to easily visualize and secure your deployments.

New technology, same old security challenges

A K8s cluster provides a complete ecosystem for running applications, including DNS services, load balancing, and more. Kubernetes then orchestrates containerized applications across multiple clusters, facilitating seamless interactions between services. This interconnectedness, though convenient for development, can introduce familiar security vulnerabilities.

It creates an inherently flat network, meaning each pod can communicate with any other pod inside the cluster. Upon initial breach, an attacker can move laterally and gain access to all connected clusters, and then onto the rest of the data center. According to the 2024 Red Hat State of Kubernetes Security Report, 46% of respondents lost revenue or customers due to a container or Kubernetes security incident.

Why microsegmentation matters for securing Kubernetes

Microsegmentation addresses K8s security challenges by mitigating the risks associated with lateral movement. By implementing granular security policies that control traffic between individual components, you can deny lateral movements even when one part of your cluster is attacked.

It's important to note that security teams cannot just "lift and shift" an existing security solution and expect it to automatically work with this new technology. In order to secure K8s clusters without affecting performance, it must be done in a way that is native to K8s.

Benefits for your business

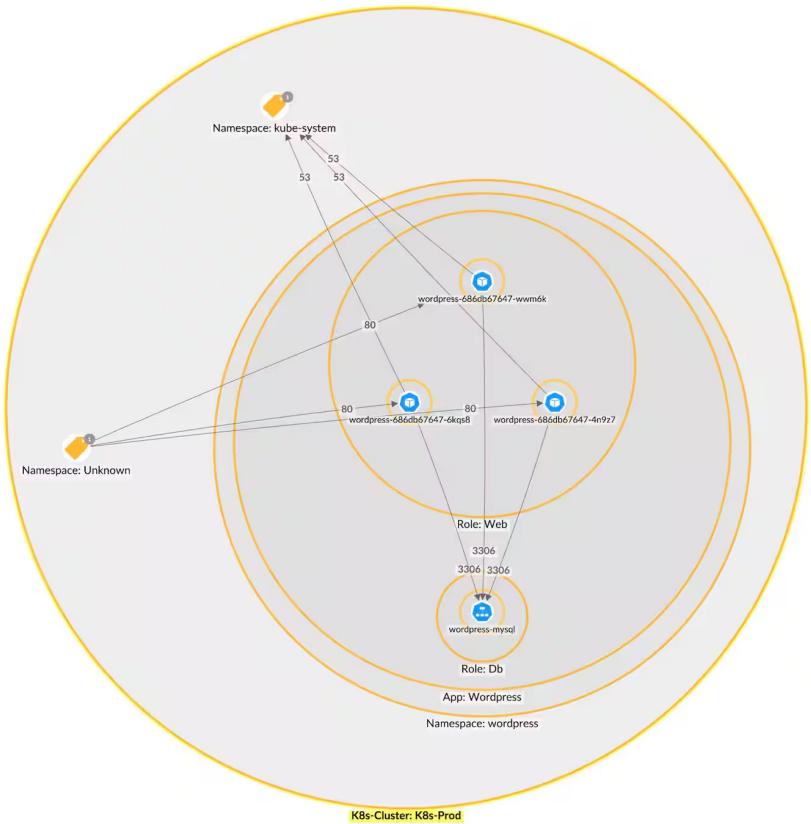
- Visualize, monitor, and control K8s cluster communications within a unified management console
- Implement precise microsegmentation policies to enhance your K8s security posture
- Out-of-the-box templates to quickly ringfence K8s clusters and reduce operational overhead
- Scales seamlessly with your infrastructure so you can build fast without sacrificing security
- Unified console and policy management across all assets, including 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

This is why Akamai offers a software-based microsegmentation solution that has dedicated features for securing K8s clusters. The solution behaves similarly for other assets in your environment, including legacy operating systems, public cloud resources, on-premises workloads, and more. As a result, you can visualize, secure, and manage assets across your company through a single unified console.

Key capabilities for segmenting Kubernetes clusters

Visibility. Know what's communicating with and within your K8s environments with comprehensive traffic visualization. The visibility provided by Akamai Guardicore Segmentation forms the basis for K8s security, confirming that your traffic is going only where you want it to go, which is critical for creating successful security policies.

- **Interdependency maps** — Akamai provides a map for visualizing communications within and across data centers for all types of technologies, including VMs, K8s clusters, Docker containers, and more. These maps enable you to understand application deployments and network relationships thoroughly, while also detecting suspicious connections among pods, clusters, 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.



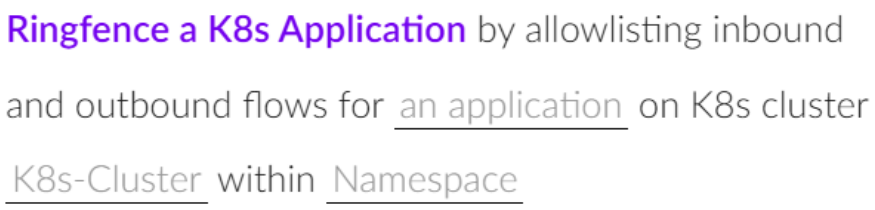
Clusters represented on the Reveal map. Double-clicking a cluster reveals the namespaces and their interconnections within the cluster.

> Observe the current behavior of these workloads first, then work with the same cross-functional team to identify approved dependencies before enforcing microsegmentation rules.
>
> **– Gartner® Strategic Roadmap for Zero-Trust Security Program Implementation**

Enforcement. To minimize the attack surface in K8s clusters, microsegmentation must be implemented. This should occur in a way that is 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 accomplishes this by leveraging the native Kubernetes Container Network Interface (CNI) controller on each node for enforcing microsegmentation policies. 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 of enforcement with no scale or performance limitations.

Dedicated policy templates within our solution enable users to quickly ringfence Kubernetes business-critical applications — whether it's a namespace, application, or any other object.



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.

Summary

Kubernetes has become an integral part of many business environments. It's a different approach to application development, offering resource usage efficiency, more streamlined build processes, and increased portability and scalability. But this approach brings along with it some familiar security challenges.

Akamai Guardicore Segmentation provides one holistic solution that allows you to see communication flows across different types of deployments, including K8s clusters and cloud environments, 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.

According to the 2024 Red Hat State of Kubernetes Security Report, security continues to be one of the biggest concerns with K8s adoption, with 67% of respondents delaying or slowing down K8s deployment due to security concerns.

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

Gartner, Strategic Roadmap for Zero-Trust Security Program Implementation, Dale Koeppen, John Watts, 27 March 2025. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

| Published 05/25