AKAMAI SOLUTION BRIEF

Akamai Guardicore Segmentation Protection for AWS Workloads

The challenge: new world, old problems. Enterprises are increasingly migrating critical workloads to AWS to increase business agility, reduce costs, and improve scalability and performance. Security concerns include:

New toolset

Operating in a cloud environment requires a whole new set of security controls. These need to support AWS in the cloud and via AWS outposts on premises, as well as hybrid-cloud workloads. New challenges include organizations utilizing a shared cloud deployment model, and the dynamic application deployment models required to leverage the growth in edge computing.

New security operation model

As part of the AWS shared responsibility model, using AWS workloads in the cloud or on premises means taking responsibility of security configuration for applications and traffic. This includes ways to protect and monitor network traffic, both north-south and east-west, and ways to deploy controls to detect, prevent, and respond to breaches.

Reduced infrastructure visibility and control

The same advantages that make the AWS environment operationally attractive lead to reduced control and visibility of assets that are spread across multiple AWS accounts, VPCs, and network security groups, and the wider hybrid ecosystem of an organization.

Akamai Guardicore Segmentation solution for AWS

Akamai Guardicore Segmentation provides visibility and protection for all workloads running in your AWS cloud, outposts, and hybrid environments. It provides microsegmentation and application-level visibility, as well as breach detection and response, covering AWS, on premises, and other assets.

Key Benefits

- End-to-end solution to protect AWS instances, allowing DevOps and security teams to focus scarce resources on core tasks instead of data center security management
- Manage and enforce tight microsegmentation policies around all servers, containers, and Kubernetes clusters down to the process level
- Reliably detect policy violations and respond to them in real time
- Safeguard environments from potential breaches by using multiple intrusion detection and prevention methods, including reputation analysis, real-time dynamic deception, and file integrity monitoring

Highlights

Akamai is an advanced AWS Technology Partner with AWS Security Competency status, offering Akamai Guardicore Segmentation the highest level of visibility and segmentation on the hybrid cloud.

Akamai

Automatic discovery and visibility

- Automatically discover applications and flows
- Built-in AWS orchestration connector with easy APIs to pull labeling and asset information
- Quickly understand application behavior
- Application dependency mapping with granular visibility down to the process level (L7)

Powerful segmentation and enforcement

- Define segmentation policies in minutes
- Automatic policy recommendations
- Smart labeling and grouping that allow easy navigation across complex environments

Threat detection and incident response

- No configuration needed; value from day 1
- Multiple detection methods cover all types of threats
- Dynamic deception provides full network coverage
- Real-time file integrity monitoring prevents unauthorized changes

By selecting Akamai Guardicore Segmentation, we were able to bridge critical security gaps of microsegmentation and application-level visibility, as well as breach detection and response, covering both AWS and on-prem servers.

DevOps Team Leader
biotechnology firm

Take AWS security to the next level. Learn more at akamai.com

 | Support | | Published 07/22