AKAMAI SOLUTION BRIEF

Segmentation for Hybrid Cloud Environments

Contain attacks with segmentation for your cloud infrastructure

With the growing shift of applications and workloads to the cloud, security and cloud teams are facing a growing number of challenges. One of those is extending segmentation and Zero Trust principles to applications and workloads in cloud environments. With Akamai Guardicore Segmentation, organizations can reduce the attack surface and contain attacks on applications and workloads in their public cloud environments — without installing agents. This is achieved through automatic application discovery, comprehensive visualization of cloud flows, precise segmentation policies, and network security alerts — all from a single pane of glass.

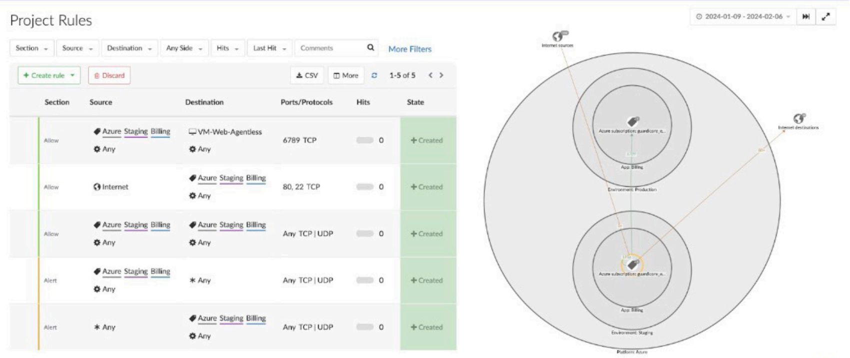
Unique cloud challenges

Modern organizations increasingly rely on the cloud to manage their critical systems and store their most valuable data.

According to the IBM Cost of a Data Breach Report 2023, 82% of breaches involved data stored in the cloud — public, private, or both environments. Attackers often managed to gain access to more than one cloud platform, with 39% of breaches spanning multiple environments and incurring a higher-than-average cost of US$4.75 million.

The unique and dynamic nature of the cloud means that cloud workloads are more exposed to external threats than on-premises resources are. Security teams are dealing with several unique challenges:

- **Poor visibility** — The cloud provider's visibility is based on raw logs of the flows between different workloads. Without a clear understanding of the relationships between different workloads and applications inside cloud environments, creating effective security policies becomes almost impossible.
- **No single policy** — Creating a consistent policy across hybrid cloud environments using only native cloud security tools is extremely complex. This is because each cloud instance has its own objects and rules, and therefore its own policies, resulting in a fragmented policy.
- **Lack of unified governance** — Security isn't always a priority in the cloud. This creates friction between security teams and app owners who spin up workloads without always taking security into consideration.



Project Rules

Section	Source	Destination	Ports/Protocols	Hits	State
Allow	Azure Staging Billing Any	VM-Web-Agentless Any	6789 TCP	0	+ Created
Allow	Internet	Azure Staging Billing Any	80, 22 TCP	0	+ Created
Allow	Azure Staging Billing Any	Azure Staging Billing Any	Any TCP | UDP	0	+ Created
Alert	Azure Staging Billing Any	* Any	Any TCP | UDP	0	+ Created
Alert	* Any	Azure Staging Billing Any	Any TCP | UDP	0	+ Created

Ringfence an Azure application using automated policy suggestions

Benefits for Your Business

Visualize cloud flows using a single interface
Gain a deep understanding of how your cloud workloads and applications interact using a dynamic network dependency map, and easily apply security controls.

Apply consistent segmentation policy
Deploy a single segmentation solution that works consistently across hybrid cloud environments, avoiding vendor-specific solutions that create security silos.

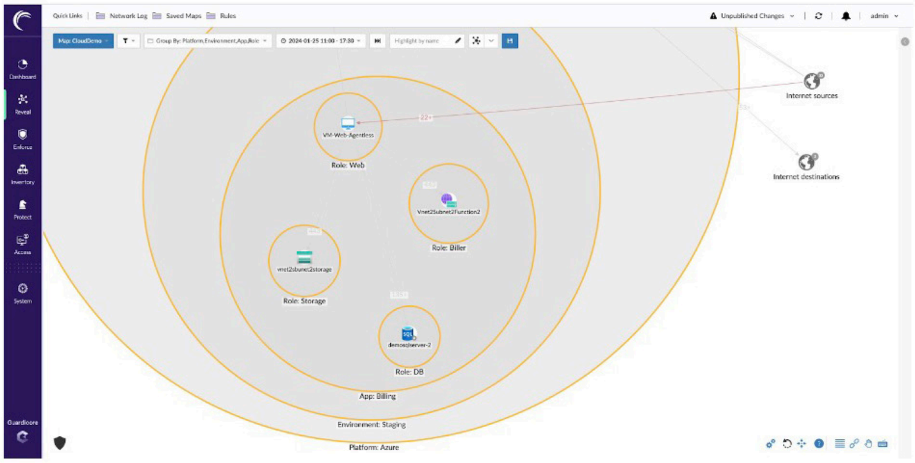
Stop breaches
Adapt security policies to any change within your cloud environment and save your team the burden of manual updates.

Prevent cloud security threats

Akamai Guardicore Segmentation extends its industry-leading segmentation to cloud applications and workloads. By extending segmentation to your cloud assets, any unauthorized connection is automatically stopped, thereby restricting lateral movement and damage from breaches or ransomware incidents.

Key capabilities

- **Comprehensive agentless cloud-native visibility and enforcement** enables administrators to visualize cloud workloads using a near-real-time interactive map of true network flows, understanding the application dependencies and bringing together DevOps and SecOps teams in cloud network security governance.
- **A hybrid enforcement engine leveraging multiple enforcement points** allows an organization to simply define the intent of network policy and have the Akamai Guardicore Segmentation policy engine take care of the rest, dynamically deciding which agent-based and agentless enforcement points are used across the data center.
- **Integrated reputation analysis and threat intelligence firewall capabilities** are designed to reduce time to detection and incident response time in the event of a breach.
- **A scalable and secure solution** ensures data does not leave your cloud environment, and solution architecture scales automatically within it.



A single map for on-prem and hybrid cloud environments

Please visit akamai.com/guardicore for more information.

| Support | Published 02/24