AKAMAI SOLUTION BRIEF

Protecting Workloads in AWS with Akamai Guardicore Segmentation

Enterprises continue to leverage PaaS resources in Amazon Web Services (AWS), and many are migrating their critical workloads into the public cloud. These enterprises are seeing benefits that include reduced costs, improved scalability and performance, and increased business agility. However, there are pressing security concerns that come with this shift to the cloud, including:

New toolset

Operating in a cloud environment requires a whole new set of security controls. These controls need to support AWS in the cloud and via AWS outposts on-premises, as well as hybrid cloud workloads. Existing cloud security groups might be sufficient for assets and resources in the AWS Cloud, but those controls do not extend to protect related assets or resources in other environments. This means your team has to manage multiple security tools, which can result in potential security gaps.

New security operation model

As part of the AWS Shared Responsibility Model, using AWS resources in the cloud or on-premises means that Amazon is only responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. But any application software or utilities installed on those instances, as well as security group configuration, are the sole responsibility of the user. This also includes protecting and monitoring traffic, both north-south and east-west, and deploying controls to detect, prevent, and respond to breaches.

Reduced infrastructure visibility and control

The same advantages that make the AWS environment operationally attractive can also lead to reduced control and visibility of assets that are spread across multiple AWS accounts, virtual private clouds (VPCs), and network security groups, as well as the wider hybrid ecosystem of an organization.

Key benefits

- End-to-end solution to protect workloads in AWS, including PaaS resources, allowing DevOps and security teams to focus scarce resources on core tasks instead of data center security management
- Manage and enforce tight microsegmentation policies that extend beyond AWS to include assets that live on-premises and even across public clouds
- 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 and real-time dynamic deception

Akamai Guardicore Segmentation for AWS security

Akamai Guardicore Segmentation provides a unified solution for visibility and policy enforcement for workloads and PaaS resources running in your AWS cloud, outposts, and hybrid environments. It provides microsegmentation and application-level visibility, as well as breach detection and response capabilities.

Automatic discovery and visibility

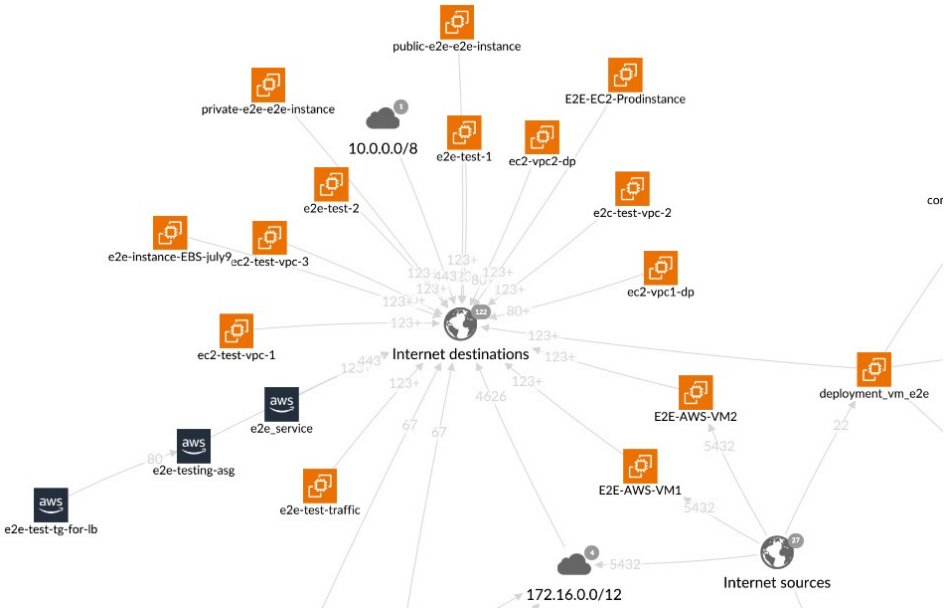
- Automatically visualize applications, resources, and their communication flows
- Quickly understand and baseline application behavior
- Application dependency mapping with granular visibility down to the process level (Layer 7)

Powerful segmentation and enforcement

- Define segmentation policies in just 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



Visualize and protect applications and resources in AWS with Akamai Guardicore Segmentation

> 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**

Seamlessly protect workloads and PaaS resources in AWS. Learn more at akamai.com/guardicore.