GuardiCore Centra 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. However, these benefits come with new security concerns and gaps:

- New toolset - Operating in a cloud environment requires a whole new set of security controls that are different and separate from the existing on-premises tools.
- New Security Operation Model - As part of the AWS Shared Responsibility Model, using AWS workloads means taking responsibility for the security configuration in the cloud. This includes ways to protect and monitor network traffic both north-south and east-west and 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.

aws partner network

Advanced Technology Partner

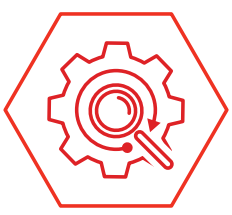
GuardiCore, an AWS Technology Partner, offers the Centra Security Platform to help bridge these gaps.

The GuardiCore Centra Solution for AWS

GuardiCore Centra provides visibility and protection for all workloads running in your AWS cloud. Centra provides micro-segmentation and application-level visibility, as well as breach detection and response, covering both AWS and on-premises 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 micro-segmentation policies around all servers 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 (FIM).



Automatic Discovery & Visibility

- Automatically discover applications and flows
- Integrate with AWS APIs to pull labels and asset information
- Quickly understand application behavior
- Granular visibility down to the process level (L7)

Powerful Segmentation & Enforcement

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

Threat Detection & 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 (FIM) prevents unauthorized changes