AlgoSec for AWS

Security Management in the Hybrid Cloud

Challenges

Multiple security platforms, multiple clouds and multiple stakeholders

IT and Security staff find it difficult to create and maintain security in the cloud due to:

- **COMPLEXITY OF MULTIPLE LAYERS OF SECURITY CONTROLS –** Hybrid networks have multiple security controls, including AWS's built-in security controls, such as security groups and network ACLs. Cloud assets such as EC2 instances, DBaaS, and serverless functions need protection. Misconfigurations introduce security risks across various assets, including IaaS and PaaS.
- **MULTIPLE PUBLIC CLOUD ACCOUNTS** – Enterprises have multiple cloud instances spread across multiple accounts, regions and VPCs. Security professionals need to understand their different accounts, while managing them separately using different account consoles and multiple tools.
- **MULTIPLE STAKEHOLDERS MANAGING CLOUD DEPLOYMENT** – In on-premises networks, policies are typically managed by security teams. But in cloud environments such as AWS, multiple stakeholders manage changes to cloud configurations and security rules using different orchestration methods, challenging consistency and control, and increasing the risk of misconfigurations.
- **CHANGE PROCESSES SLOW DOWN BUSINESS -** Making changes in complex hybrid and heterogeneous enterprise environments is hard. Assessing the risk of changes is difficult, yet misconfigurations can cause outages and disrupt business.

The AlgoSec Solution

Hybrid cloud security policy and configuration management: Cloud security under one unified umbrella

AlgoSec seamlessly integrates with the AWS network security controls as well as firewalls, on-prem or virtually deployed in the cloud and other security devices to deliver unified security policy management across the hybrid network. AlgoSec also enables effective security management of the various security control layers across the multi-cloud estate. AlgoSec offers instant visibility, risk assessment, and central policy management, enabling a unified and secure security control posture, proactively detecting misconfigurations.

Benefits

Manage the entire hybrid security environment with AlgoSec

Continuous Visibility

Get a full network map of your entire hybrid network estate – both on-premises and in public and private clouds. Understand security policy with traffic simulation query.

Easy Migration

By automatically discovering, mapping and migrating connectivity configurations with firewalls and security groups, AlgoSec simplifies the complex process of migrating business applications to the cloud.

Central Management of Security Policies

Aggregated view of similar security groups across accounts, regions and VPCs

Hybrid Network Change Management

Leverage a uniform network model and change-management framework that covers the hybrid and multi-cloud environment.

AlgoSec on AWS

AlgoSec seamlessly integrates with all leading brands of firewalls, cloud security controls, routers, and load balancers to deliver unified security policy management. With the AlgoSec Security Management Solution, users benefit from holistic management and automation spanning on-premise, SDN and public cloud.

Features

Risk management

Proactively detect misconfigurations to protect cloud assets, including cloud instances, databases and Lambda functions. Easily identify risky security policy rules, the assets they expose and whether they are in use.

Policy cleanup

As cloud security groups are constantly adjusted, they can rapidly bloat. This makes it difficult to maintain, increasing potential risk. With AlgoSec's advanced rule cleanup capabilities, you can easily identify unused rules and remove them with confidence without impacting business continuity.

Case Study: Orange Cyberdefense

Challenges

- "Shadow IT" had taken over, causing security risks and friction with IT, who had to support it.
- Security policies were being managed in tedious and unmaintainable Excel spreadsheets
- Lack of verification that official firewall policies accurately reflect traffic flows.

Solution

- Automation of security policy change management and documentation of security policy changes
- Comprehensive firewall support for their multi-vendor, hybrid estate
- Ability to determine compliance and risk profiles
- Full visibility and control for IT, while enabling business agility

Results

- Ability to optimize rules and objects. They were able to go from 4,000 rules to 1,110 rules – a 72% reduction.
- Move to the hybrid cloud with the adoption of Amazon Web Services
- Able to reduce shadow IT and reclaim ownership of the cloud
- Full visibility of entire hybrid network – including both on-premise and, AWS security groups, and NACLs.

Get started with AlgoSec solutions on AWS

Visit AWS Marketplace or algosec.com to purchase or learn more.