SECURITY POLICY MANAGEMENT FOR HYBRID AWS ENVIRONMENTS

Organizations are extending their on-premise data centers to Amazon Web Services (AWS) and other Infrastructure-as-a-Service (IaaS) platforms to maximize business agility and reduce costs. But with new, multiple-layered cloud security controls and network architectures that are fundamentally different from traditional on-premise data centers, security, network operations and application teams are struggling to migrate and maintain adequate security across their hybrid architectures.

Key challenges include:

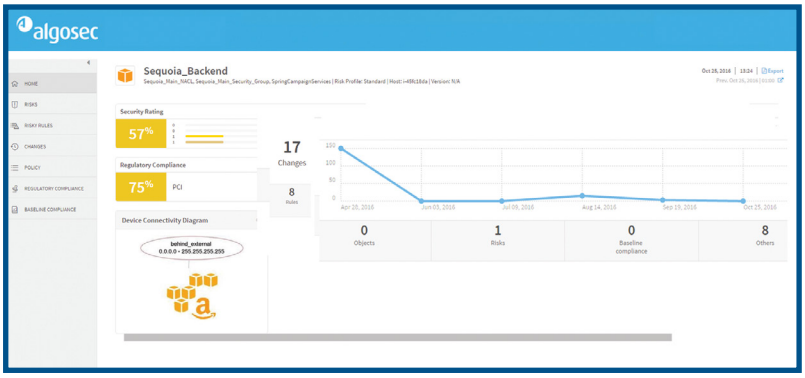
- Limited visibility of existing applications and their connectivity, as well as routing and security controls across the hybrid environment
- Ensuring that the Amazon security controls allow only the required connectivity and no more
- Manual, time-consuming and error-prone change management processes
- Continuous regulatory and corporate compliance in a business climate that demands agility
- Management of cloud security by multiple stakeholders, unlike the on-prem network where it is managed by security teams.

AlgoSec for Amazon Web Services

Unified visibility shows you all your assets and the multiple security constructs and configurations protecting them, ensuring that your entire hybrid environment is secure all the time.

AlgoSec reduces risk and boosts compliance by enforcing company and regulatory policies, verifying adherence to best practices and pro-actively detecting and alerting on misconfigurations.

AlgoSec automates management of security policies for multiple security controls across multiple clouds, regions and accounts, as well as for end-to-end connectivity in hybrid environments throughout the entire application lifecycle from deployment to decommissioning.



Key Benefits

- Full visibility and unified security policy management across the hybrid AWS environment
- Accelerated application migrations to AWS
- Management of the complexity of the multiple layers of cloud security while assessing risk and compliance, and providing recommendations
- Constant audit-readiness
- Automated security policy change management to eliminate misconfigurations
- Automatic notifications on security configuration discrepancies
- Network security change management at the speed of cloud deployment

aws partner network

Standard
Technology Partner

Easily Plan and Migrate Application Connectivity to AWS

AlgoSec automatically discovers and maps the existing network infrastructure, including security devices and application connectivity flows.

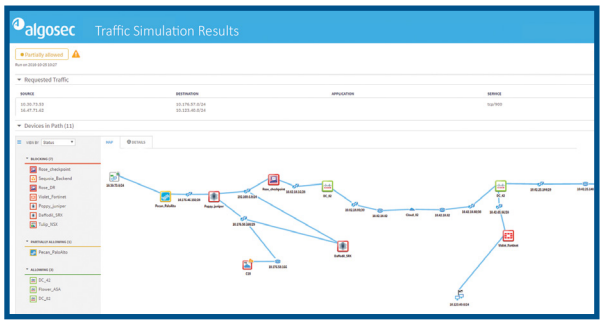
Through easy-to-use workflows, you can easily highlight the applications you want to migrate to the cloud and the servers and other resources to which they will be migrated. AlgoSec then automatically creates the change requests needed to implement the migration of application connectivity. If a change does not violate compliance requirements or create risk, it can be automatically deployed onto the relevant firewalls, AWS and 3rd-party security controls. The zero-touch approach simplifies extremely complex and risky processes, eliminates error, increases security and saves significant time and effort.

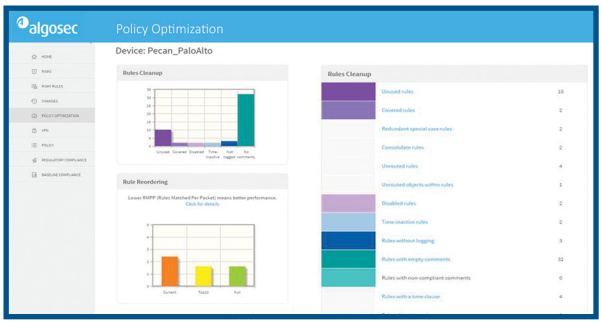
Manage Security Policies Across the Hybrid AWS Environment

Once your business applications are deployed on AWS, AlgoSec can automatically manage security controls alongside your traditional firewalls to provide unified security policy management across the entire hybrid enterprise.

With AlgoSec you can:

- Manage security across the entire hybrid environment from a single console
- Automatically manage all changes to the hybrid environment and proactively prevent non-compliant or risky changes
- Monitor unauthorized changes to AWS security controls and traditional firewalls
- Instantly generate reports for compliance with regulatory and corporate policies.





Comprehensive Support for Heterogeneous Environments

AlgoSec seamlessly integrates with all leading brands of traditional and next-generation firewalls and cloud security controls, as well as routers, load balancers, web proxies and SIEM solutions, to deliver unified security policy management across any hybrid cloud, SDN and on-premise enterprise network. Additional devices can be added via the AlgoSec Extension Framework.

amazon web services · AVAYA · BLUE COAT · BROCADE · Check Point SOFTWARE TECHNOLOGIES LTD. · CISCO · DELL SONICWALL · F5 · slack
FORTINET · Hillstone NETWORKS · HUAWEI · IBM · JUNIPER NETWORKS · Microsoft Azure · paloalto · splunk> · vmware · WatchGuard

algosec | BUSINESS-DRIVEN SECURITY MANAGEMENT

AlgoSec.com