Case study: Global financial institution automates hybrid cloud security with AlgoSec

Introduction

A leading global financial institution, operating across multiple continents, faced significant challenges in managing security policies across its complex hybrid cloud environment. With a vast on-premises data center footprint and an increasingly critical presence in public cloud platforms (AWS and Azure), the institution sought a unified, automated solution to enhance security, reduce risk, and streamline operations. This case study details how AlgoSec enabled them to achieve comprehensive visibility, automated policy management, and continuous compliance across their hybrid infrastructure.

The challenge

Navigating hybrid cloud complexity

The financial institution's hybrid cloud strategy, while offering agility and scalability, introduced several critical security and operational hurdles:

1. **Lack of unified visibility:** Security teams struggled with disparate tools and manual processes, leading to a fragmented view of security policies across on-premises firewalls (Cisco, Check Point, Palo Alto Networks) and public cloud security groups/ACLs. This made it difficult to identify misconfigurations, enforce consistent policies, and understand the true attack surface.
2. **Manual policy management:** Changes to security policies, whether for application deployment or network segmentation, required extensive manual effort. This involved coordinating across multiple teams (network, security, application), leading to slow change cycles, human errors, and potential compliance violations.
3. **Compliance and audit burden:** As a highly regulated entity, the institution faced stringent compliance requirements (e.g., PCI DSS). Demonstrating continuous compliance and preparing for audits was a time-consuming and resource-intensive process due to the lack of automated reporting and real-time risk assessment.
4. **Risk of misconfiguration:** The dynamic nature of cloud environments, coupled with manual processes, increased the risk of security misconfigurations, potentially exposing sensitive financial data and critical applications.
5. **Operational inefficiency:** Security teams were overwhelmed with routine tasks, such as policy cleanup, rule optimization, and troubleshooting connectivity issues, diverting resources from strategic security initiatives.

The solution

AlgoSec Cloud Enterprise

After a thorough evaluation, the financial institution selected AlgoSec Cloud Enterprise to address their hybrid cloud security challenges. The implementation focused on leveraging AlgoSec's core capabilities:

1. **Discovery and mapping:** AlgoSec Cloud Enterprise was deployed to automatically discover and map the entire hybrid network topology, including on-premises firewalls, routers, and public cloud security constructs (AWS Security Groups, Azure Network Security Groups). This provided a single, accurate source of truth for network connectivity and security policies.
2. **Automated policy analysis and risk assessment:** The platform continuously analyzed existing security policies against predefined compliance standards and internal security best practices. It identified risky rules, redundant policies, and potential attack vectors, providing actionable insights for remediation.
3. **Intelligent change management:** AlgoSec Cloud Enterprise's capabilities were integrated into the institution's change management workflow. This enabled automated, risk-assessed security policy change requests, from initial submission to design, approval, and automated provisioning across both on-premises and cloud security devices.
4. **Application connectivity management:** The institution utilized AlgoSec's application-centric approach to define and manage connectivity requirements for critical business applications. This ensured that security policies were aligned with application needs, simplifying troubleshooting and reducing downtime.
5. **Continuous compliance and auditing:** AlgoSec Cloud Enterprise provided real-time compliance monitoring and generated comprehensive audit reports, demonstrating adherence to regulatory mandates and internal policies. This significantly reduced the time and effort required for audit preparation.

The results: tangible benefits and enhanced security posture

The implementation of AlgoSec yielded significant, measurable improvements for the financial institution:

Reduced security policy change time by 70%

Automated workflows and intelligent policy design reduced the average time for security policy changes from several days to just hours, accelerating application deployment and business agility.

Improved compliance and audit readiness

Automated reporting and continuous monitoring ensured constant compliance, **reducing audit preparation time by 50%** and improving audit outcomes.

Eliminated 90% of manual errors

Automation minimized human error in policy provisioning, leading to fewer misconfigurations and a stronger security posture.

Enhanced risk mitigation

AlgoSec identified and helped remediate **over 1,500 risky or redundant rules** within the first six months, significantly shrinking the attack surface.

Achieved 100% policy visibility

A unified dashboard provided complete, real-time visibility into all security policies across the hybrid environment, enabling proactive risk management.

Increased operational efficiency

Security teams were freed from mundane, repetitive tasks, allowing them to focus on higher-value activities such as threat hunting and security architecture design.

Conclusion

By leveraging AlgoSec, the global financial institution successfully transformed its cloud security operations. They moved from a reactive, manual approach to a proactive, automated one, achieving unprecedented visibility, control, and agility. This not only strengthened their security posture and ensured continuous compliance but also enabled them to fully embrace their hybrid cloud strategy with confidence, supporting their ongoing digital transformation initiatives. AlgoSec proved to be an indispensable tool in navigating the complexities of modern, distributed IT environments.