CLOUDVISORY

CASE STUDY 03 | MULTI-CLOUD SECURITY

> **Cloudvisory was the only solution able to deliver manageable, granular micro -segmentation across our three main cloud environments. Our cloud deployments are more secure as a result.**

This well known retailer, with thousands of brick and mortar stores and a thriving e-commerce business, migrated applications to the public and private cloud over the last several years. In the competitive retail world, being agile and cost conscious have forced this move. Equally, with massive business volume increases during holiday periods, the company needed to leverage the elastic nature of cloud services in order to scale to these busy periods. As a motto, the company is driving cloud computing for optimal usability and security.

Taking a hybrid, multi cloud approach, the company is leveraging public cloud providers Microsoft Azure and Amazon Web Services (AWS) while using OpenStack for their private cloud. Supporting 10's of thousands of virtual instances across provders and environments (Dev/Test/UAT/Production), the Risk, and Security teams began to question whether security policies were meeting compliance requirements. With repeated known breaches across competitor environments, the Security team was focused on defeating the East/West threat posed by today's hackers. Operational teams, however, had difficulty verifying security policies using their traditional toolkit and doubted their policy controls were granular enough to fight back against the worrisome East/West threat. Thus, a cross-functional task-force was formed, defining a list of critical issues to be tackled:

1. Had limited to no visibility into the existing infrastructures across the 3 providers
2. Separate native security controls from each provider made consistency and accuracy in policy provisioning difficult, time consuming and costly
3. No central policy monitoring ,audit or enforcement of policy once it was manually provisioned
4. Limited granularity of policy controls – desire for micro-segmentation across all 3 providers
5. Time consuming to adjust policies as workloads migrate between providers
6. No way to easily control policy changes between environments (Dev/Test/UAT/Production)

Facing increasing complexity and risk from these highly elastic environments and a need to support millions of customers with the highest quality experience, the company set out to reduce risk, lower costs and speed business delivery through security automation.

As part of their detailed security and operations re-design they developed a must have list for a security automation solution:

- Discover the existing infrastructure objects and data flows across all providers and provide detailed visualization of the relationships of workloads across the 3 providers
- Centralized, automated real-time provisioning of workload level firewall policies using each provider's cloud native security controls
- Automate, granular, micro-segmentation of policies in order to halt the East/West threat
- Automate real-time, accurate adjustment of policies in response to environmental changes
- Provide real time monitoring and policy enforcement of the provider's native controls to alert on and block rogue activity

Examining and testing multiple security solutions available in the market, only one met their requirements: Cloudvisory's Contextual Security Platform (CSP). CSP proved its worth by deploying quickly and meeting all of the above requirements. Policy provisioning to cloud native security controls across all providers is now automated and highly accurate. Dynamic micro-segmentation is defeating the East/West threat. Policy changes in reaction to their elastic needs are automatic. Monitoring and enforcement allow the cross functional team is verify policy compliance through CSP's centralized management platform. The company has experienced an increase in agility and a reduction in risk and operational costs.

Reach out today for a demo and a test drive of Cloudvisory's Cloud Security Platform

WWW.CLOUDVISORY.COM