CLOUDKNOX

Success Story

HORSLEY | BRIDGE
PARTNERS®

Photo © Ed Prasek. All rights reserved. Used with exclusive permission.

Enforcing the Principle of Least Privilege in AWS

Company Background

San Francisco-based Horsley Bridge Partners LLC is a principal investment firm specializing in fund of funds investments. It seeks to invest in venture capital, growth and smaller buyouts. Founded in 1983, the firm focuses on investing in the United States, Europe, and Asia and other emerging markets. It works in close partnership with the leading seed and early stage investors employing a highly selective approach focused on technology sectors. In addition to its San Francisco, California base, Horsley Bridge Partners has additional offices in London, England and Beijing, China.

Market Overview

Today's number one unmanaged risk to hybrid and multi-cloud environments are machine (e.g. service accounts) and human identities with excessive high-risk privileges. As enterprises embrace the cloud and its technology, they're realizing they lack the level of visibility and insight required to really understand what actions their identities are taking on critical cloud resources across their environment.

Moreover, identity access teams are asked to continuously and properly account for, and attribute privileges to each unique identity while keeping up with the proliferation of privileges, roles, resources and services across multiple cloud platforms – without exposing their enterprises to enormous risk.

The Challenge

Determined to get ahead of this risk, Horsley Bridge's security team embarked on a search for a solution that wouldn't involve hiring expensive consulting resources, writing complex scripts or impacting the team's daily productivity. They also sought a solution that was quick and easy to install and could scale with the growth of their business.

Horsley Bridge identified three key requirements for their ideal solution:

1. Establish Risk Posture Baseline

A tool that quickly and simply quantified risk exposure to critical cloud resources from machine and human identities with excessive privileges. They specifically wanted to understand which high-risk privileges had been granted but not used over the last 90-days. They also wanted to establish a baseline they could measure against over time.

2. Continuous Enforcement of Least Privilege Policies

Finding it very cumbersome to manually track, trend and report on privilege drift, Horsley Bridge wanted a solution that provided granular visibility into how each unique identity inherited their privileges, if they were using them and how they were using them across their AWS accounts. The team was focused on two identity groups in particular: Third-party contractors and service accounts:

Third Party Contractors: Horsley Bridge uses third party contractors to help manage elements of their AWS infrastructure and needed to better understand what privileges each contractor had vs, what they were actually using. The goal was to immediately prune (or right-size) the privileges that were not used over the last 90 days to avoid any unnecessary risk to their organization.

Service Accounts: The team noticed a significant increase in the number of service accounts used by applications to automate tasks (e.g. backups). As a best security practice, Horsley Bridge had instituted rigorous oversight of their machine identities and wanted an automated way to regularly monitor them to ensure they were only performing a minimal number of repetitive tasks with a fixed number of low-risk privileges. In the event one of these service accounts displayed suspicious behavior, the security team wanted instant alerts in order to mitigate the risk by enforcing least privilege policies.

3. Simple CIS Compliance Reporting and Management

An integrated compliance tool that continuously monitors AWS cloud resources for configuration drift and violations against industry regulated mandates and security best practices such as CIS Benchmarks. They also wanted the option to download fixes and remediate misconfigured policies themselves or request the vendor to remediate on their behalf.

The Solution

"CloudKnox," says CIO Jon Roller, "offers us a unique identity privilege management solution that has immediately transformed the way we uncover over-provisioned identities as well as the way we right-size and enforce least-privilege policies across our AWS environment.

"CloudKnox gives us deep visibility into every action our human—and especially machine identities—are performing on AWS resources using their Activity-based Authorization protocol. Their model allows us to not only automate the process of managing roles and privileges, but also allows us to create customized roles in AWS based on real historical identity activity data.

"Because they normalize the activity performed in AWS, the data is highly consumable, which means we can take immediate action to right-size roles and policies with their one-click JEP (Just-Enough-Privileges) Controller."

The Results

Within a few weeks of deploying the CloudKnox Security Platform, Horsley Bridge was able to:

- Significantly reduce the number of machine and human identities with access to critical AWS resources
- Implement least privilege policies across its AWS environment for all identities including third-party contractors and service accounts
- Measure the impact new identities have on their risk posture using CloudKnox's "Privilege Creep Index"
- Demonstrate to auditors in minutes compliance with CIS benchmarks and other regulatory mandates

Jon Roller states, "The CloudKnox Security Platform allows my team to focus on strategic initiatives and innovation without worrying about insider threats wreaking havoc in our AWS environment."

About CloudKnox Security

CloudKnox Security is the only Cloud Security Platform built from the ground-up to support the monitoring and management of identities, actions and resources across hybrid and multi- cloud environments using an Activity-based Authorization model. Through an extensible single platform, CloudKnox transforms how organizations implement the principle of least privilege and empowers security teams to proactively address accidental and malicious credential misuse by continuously detecting and mitigating identity risks. CloudKnox is based in Sunnyvale, CA.

May 12, 2021

www.cloudknox.io