CLOUDKNOX

Case Study

Top 5 Global Pharma selects CloudKnox to help them mitigate the new #1 risk to cloud infrastructure – accidental misuse and malicious exploitation of high-risk permissions

Key Benefits

- **Granular visibility into every action performed** by a human or machine identity on any resource
- **Automated remediation** for easy creation and management of least privilege roles
- **Single interface with multi-cloud view** of all identities, actions and resources
- **Detect and alert on anomalous behavior** such as unusual activity, geo-location, and client type
- **Simple, non-disruptive deployments** in less than 30 minutes, fully operational within 24 hours
- **Works across key cloud platforms:** AWS, Azure, GCP, and VMware (NSX and vSphere)

> According to the Ponemon Institute, most data breaches in pharma occur during the move to the cloud.

Industry Overview

Pharma and biotech companies experience more data breaches than any other industry in the United States, given the high value of intellectual property. Pharma attackers are looking to break in, move laterally, remain undiscovered for long periods of time, and eventually exfiltrate the crown jewels. In fact, on average it takes about 350 days to identify and contain a data breach in the pharma industry.

According to the Ponemon Institute, most data breaches in pharma occur during the move to the cloud. So, as a top 5 global pharmaceutical company with a commitment to a cloud-first strategy, it was paramount that they find a solution that could protect them from both accidental misuse and malicious exploitation of privileged credentials.

The Challenge

The company had a mandate to accelerate the move of more than 50% of its total workloads to the cloud and were struggling with the level of risk exposure this would create around privileged access, specifically from over-provisioned human and machine identities with powerful permissions. The security team was determined to get ahead of the risk but lacked the level of visibility required to truly understand who in their expanding cloud environment had access to critical resources and what types of operations were they performing on them.

"Legacy Privileged Access Management (PAM) and Identity Governance & Access (IGA) vendors were proving inadequate for what we needed. **These solutions are simply not designed to address the identity permissions challenge** that is so unique to public cloud environments."

Pharma VP of Cloud Security

Within 24 hours, CloudKnox's Cloud Permissions Risk Assessment had uncovered the following risks:

- **Unauthorized Access/ Privilege Escalation:** As many as **50%** of their human identities were circumventing established security processes by assigning high-risk permissions to themselves and others or creating custom roles
- **Over-provisioned Active Identities:** More than **74%** of human identities were using less than 5% of permissions granted to them to perform their daily tasks
- **Over-provisioned Machine Identities:** Over **90%** of the company's service accounts had been granted high-risk permissions
- **Over-provisioned Super Identities:** Only **14%** of administrators who belonged to a super-admin group were using their high-risk permissions

The Solution: CloudKnox Cloud Permissions Management Platform

The company launched a formal project to analyze existing and new solutions to determine their ability to meet the evolving needs of both its security and cloud infrastructure teams. The process surfaced a number of key requirements:

- **Multi-cloud solution** that could quickly quantify their risk exposure from both human and machine identities with excessive high-risk permissions and establish a baseline they could measure against over time
- **Granular visibility** into 1) all identities with access to cloud resources; 2) identity permissions granted; 3) identity permissions used; 4) resources accessed by identities
- **Simple and automated** way to right-size permissions and roles without manual, tedious time consuming work
- **Scalable enough to support tens of thousands** of cloud compute instances across multiple cloud platforms
- **Quick deployment without disruption,** operational efficiency and immediate time-to-value for all stakeholders
- **An integrated compliance solution** that would continuously monitor their most sensitive resources for configuration drift and violations with a built-in option to download fixes and remediate misconfigured policies themselves or request the vendor to do so on their behalf

> **"CloudKnox was deployed faster than any enterprise security product in the history of our company** and immediately delivered results to multiple stakeholders in our organization."
>
> Pharma Director of Technology Security and Risk Strategy

The Results

The detailed findings and practical recommendations from the risk assessment culminated in a decision by the company to purchase the CloudKnox Cloud Permissions Management Platform for hundreds of cloud subscriptions. The deployment was achieved in a matter of hours, and within a few weeks of deploying the platform, the team was able to achieve the following results:

By leveraging CloudKnox's patented Activity-based Authorization protocol, JEP (Just Enough Privileges) Controller, and Anomaly Detection, the company was able to:

- **Gain granular visibility and insights** into every identity and their activity by displaying all granted permissions, used permissions, unused permissions and resources accessed
- **Remediate issues that were uncovered by the assessment** quickly and without the heavy operational costs associated with manual remediation efforts:
  - **Right-sized permissions** for all active identities, service accounts and super-identities by removing all high-risk permissions that had not been used for 90 days
  - **Tighten controls** for super identity (admin) groups by right-sizing high-risk permissions and removing inactive super identities from the group
  - **Limit the scope** of all human and machine identities to only the resources they needed access to perform their daily tasks
  - **Implement least privilege policies** across the company's entire cloud environment for all human and machine identities, roles and groups
- **Minimize impact to productivity** by allowing temporary (just-in-time) access to high-risk permissions and critical resources

"We were all blown away by the level of visibility we got from the CloudKnox risk assessment. It not only exposed all the identities in our environment that were grossly over-provisioned, but it also uncovered an alarming number of unauthorized human identities that were able to circumvent established security procedures to modify and assign high-risk permissions to themselves and others."

Pharma Director of Technology Security and Risk Strategy

- **Eliminate the practice of unauthorized assignment of permissions** and creation of custom roles by identities for themselves and others by formalizing an end-to-end process supported by CloudKnox's activity monitoring and auto-remediation functionality
- **Detect and respond to anomalous behavior** by receiving alerts prompted by the following deviations: identities accessing sensitive resources for the first time, using permissions that have never been used, logging in from a different IP address, performing actions during abnormal hours
- **Continuously measure, evaluate and compare** the company's least privilege posture against industry benchmarks using CloudKnox's Privilege Creep Index

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 a single extensible 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 the insider threat risk. CloudKnox is based in Sunnyvale, CA.

CLOUDKNOX
333 W El Camino Real
Sunnyvale, CA 94087
www.cloudknox.io

September 1, 2020, v1