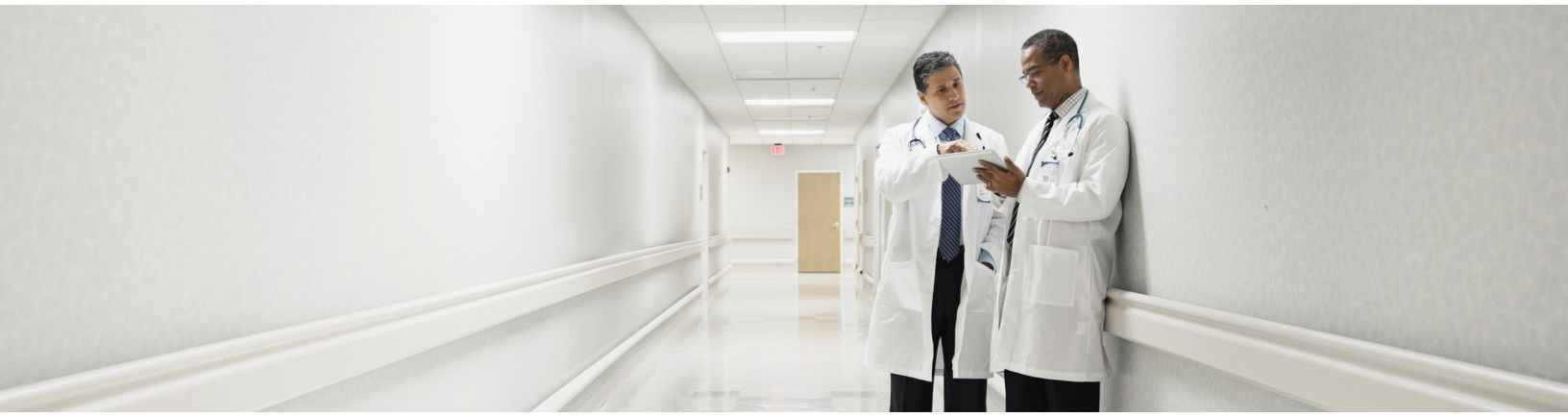
CLOUDKNOX

Success Story
FORTIFIRE



Fortifire Selects CloudKnox's Cloud Security Platform for AWS to Support Their Healthcare Clients

Company Background

Founded in 2002, Fortifire is a certified and trusted information security advisor for over 300 companies in Silicon Valley. Fortifire helps protect its clients from cybersecurity threats by providing solutions through Security Gap Analysis, Comprehensive Risk Assessments, Incident Response Forensics, and preventing insider threats through End Point Control.

Security Challenges in the Health Care Industry

The healthcare industry has been experiencing more data breaches than any other industry in the United States, accounting for more than 45% of all breaches. Last year, a new breach was reported almost every day – from phishing attacks to insider threats. According to the 2019 Verizon Insider Threat Report, insider threat attacks are one of the most damaging attack vectors to healthcare organizations. Healthcare was the only industry where insiders were responsible for a higher percentage of breaches than external actors. The most alarming part of this is that when breaches occur, it takes almost a year to discover, identify and contain a data breach.

The team at Fortifire understood early on how critical it is for healthcare organizations and healthcare service organizations, to protect their cloud infrastructure and applications from insider threats. Without a proactive approach, any health-related enterprise was leaving itself wide open to both accidental and malicious insider threats.

Fortifire Selects CloudKnox for Healthcare Client

One of Fortifire's key healthcare client was looking for a SaaS solution to help them protect their vast repository of Patient Health Information (PHI) data. They were looking for a solution that would not only protect sensitive data but also help them meet the very stringent HITRUST (The Health Information Trust Alliance) compliance requirements.

Because this client was an existing AWS customer, Fortifire selected CloudKnox's Cloud Security Platform in conjunction with Fortifire's IAM security consulting services. The platform had to be a SaaS model, truly multi-cloud, simple to deploy, and could scale with their projected growth of new AWS identities, services, and resources.

Key Requirements

1. Understanding the insider threat risk landscape

The Fortifire team needed to immediately assess their client's IAM risk posture including over-privileged human and machine identities. Secondly, they wanted to understand which high-risk permissions had been granted but not used. They also wanted to establish a baseline they could measure against benchmarks.

2. Continuous Enforcement of Least Privilege Policies

Finding it very cumbersome to manually track, trend and report on permission drift, Fortifire's client wanted a solution that provided granular visibility into 1) who had access to their AWS environment; 2) which privileges they had 3) which privileges they were using; 4) which privileges they were not using, and 5) which resources they were accessing. They also needed a simple way to right-size permissions that had drifted across all AWS accounts without having to purchase another solution.

3. Audit Preparation for HITRUST Compliance
During an audit, organizations are asked to prove compliance for any given period, which poses significant challenges in public cloud environments where the addition and deletion of new users, resources, services, roles, and permissions happens frequently. To keep up with these changes, Fortifire's client was looking for an automated cloud security platform to help them continuously audit and report on the status of users and privilege access.

The Results

According to Shaq Khan, CEO of Fortifire, "Our client initially considered building their own solution. However, they quickly realized that even doubling or tripling the investment in security, operations and development talent would never enable them to implement a robust cloud privilege management solution that could scale and meet the company's longer-term security and HITRUST compliance requirements."

The healthcare client purchased CloudKnox Cloud Security Platform for their AWS environment, and within a few weeks of deploying the platform the team was able to address all their original requirements and more:

1. Implemented least privilege policies across their AWS environment for all users, groups, roles, and resources:

- Removed all inactive users and groups from their AWS accounts
- Removed inactive users and excessive privileges from groups
- Right-sized (prune) excessive privileges from users, groups, roles, and resources
- Created custom roles based on a common set of permissions required to perform a function
- Significantly reduced the number of users and groups with unnecessary access to critical AWS resources (e.g., S3 buckets)
- Limited scope of users and roles to only resources they have and/or need access to ...

2. Continuously measure, evaluate, and compare the company's risk posture against benchmarks using CloudKnox's "Privilege Creep Index."

3. Demonstrate in minutes compliance with key HITRUST access management controls. According to a Fortifire client who is a Security and Compliance Officer, "Our security strategy and investment centers on reducing the risk of a breach of protected health information (PHI). Identity and access management is one of the three pillars of our strategy, which requires us to understand our risk posture and how it changes continuously." He went on to say, "CloudKnox is strategically important because it tells us when both internal and external users within our organization have more privileges than they need. Also, I can immediately remediate this risk right within the CloudKnox platform. This helps me justify more headcount and investment to mitigate that risk when communicating with the C-suite and the board."

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 identity risks. CloudKnox is based in Sunnyvale, CA.

May 12, 2021

www.cloudknox.io