in time tec
CREATING ABUNDANCE

Case Study
Industry: Health Insurance

Securing Role-Based Access at Scale

Quick Stats

Verticals Served

- Cloud
- Cybersecurity
- IT Services

Technology Stack
CyberArk (Privileged Access Manager Cloud, Identity Security, Workforce Password Management), SailPoint IdentityIQ, AWS Identity Center, AWS CDK, SSO, ServiceNow

Team Size
5-7

Fixed or Ongoing Project
Ongoing Project

Project Build
Combined Framework

Background

A healthcare insurance company needed to overhaul its process. Its management was facing increasing regulatory pressure and internal inefficiencies. Its internal team had overlapping permissions, excessive access rights, and growing security risks. The organization wanted a system that was scalable, secure, and compliant to protect sensitive healthcare data.

They also needed to keep up with their parent company's broader modernization efforts. The organization emphasized the importance of seamless and structured identity control.
In Time Tec set up a dual-layer solution. This includes a strong CyberArk rollout for safe privilege and identity management. We built an integrated, AWS-based role restructuring to standardize access across all systems.

Key Results

Streamlined Access Control
Created standardized role-based permissions, reducing overaccess and improving manageability.

Improved Security Compliance
Implemented CyberArk solutions to strengthen data protection and meet NIST, HIPAA, and PCI standards.

Seamless User Experience
Automated user provisioning with SailPoint and established SSO functionality to enhance usability and reduce errors.

The Challenge

The healthcare insurance company was facing many access management issues that affected both security and efficiency. Users were overlapping roles, which gave them more permissions than necessary. Compliance became a risk, and management was complex. Meanwhile, security processes were breaking and reactive. Management had a hard time being proactive. They struggled to manage identity risks and enforce consistent access policies. Regulatory compliance was also at risk. Sensitive patient and financial data spread across systems without a unified control strategy. They needed a solution that protected data and simplified access. They had to reduce user friction. They were also required to follow the parent company's modernization and compliance standards.

The Process

In Time Tec teamed up with this healthcare insurance company. We installed a complete identity and access management solution with two key parts and developed a solution that meets the organization's current needs and scales their future demands. We worked in two phases:

1. Focus on strengthening security through the deployment of CyberArk's suite of tools. This includes:

- Privileged Access Manager (PAM) Cloud secures sensitive accounts.
- Identity Security enforces multifactor authentication and intelligent access controls.
- Workforce Password Management (WPM) centralizes and monitors credential usage.

These implementations secured high-risk access points. They also aligned with the parent company's regulatory requirements across HIPAA, NIST, and PCI.

2. Address widespread inefficiencies in user access across 45 AWS accounts. Many users had excessive or redundant permissions due to outdated role structures. In Time Tec resolved this by auditing existing access groups. We then retired obsolete configurations and established defined default roles and permission sets. Automation played a key role. We used SailPoint IdentityIQ to streamline user requirements. At the same time, SSO functionality ensured secure, frictionless login experiences.

We were careful when planning each step of the project. We validated with each step using thorough documentation and stakeholder involvement. This process ensured that operations ran without disruption. It aligned the team and built a strong base for ongoing access governance.

Results & Impact

Enhanced Security & Risk Reduction

- Deployed CyberArk PAM Cloud and Identity Security, securing privileged and non-privileged access.

- Implemented Workforce Password Management, reducing password-based vulnerabilities.

- Aligned with key frameworks including NIST, HIPAA, and PCI, improving compliance scores.

Operational Efficiency & Future Readiness

- Migrated legacy access structures without interrupting user access.

- Created centralized documentation for all access policies, changes, and ownership.

- Introduced monitoring and alerting systems for ongoing visibility and governance.

Streamlined User Management

- Created default roles and new Identity Center groups across 45 AWS accounts.

- Automated identity provisioning and login through SailPoint and SSO.

- Established a consistent least-privilege model, minimizing over access risks.

Upgrade Your IT Systems Now

Skyler Simmons (208) 867-4792
skyler.simmons@intimetec.com