in time tec
CREATING ABUNDANCE

Case Study
Industry: Health Insurance

Securing Role-Based Access at Scale

Blue Cross of Idaho

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

Blue Cross of Idaho (BCI) needed to overhaul its approach to identity and access management to keep up with increasing regulatory pressure and internal inefficiencies. With overlapping permissions, excessive access rights, and growing security risks, the organization sought a scalable, secure, and compliant system to protect sensitive healthcare data.

At the same time, Blue Cross Blue Shield Association (BCBSA)'s broader modernization efforts emphasized the importance of seamless and structured identity control. In Time Tec engaged with BCI to implement a dual-layered solution: a robust CyberArk rollout for secure privilege and identity management, and a deeply 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

BCI was facing multiple access management issues that impacted both security and efficiency. Users were frequently assigned to overlapping roles, which gave them more permissions than necessary—introducing both compliance risk and management complexity. Meanwhile, security processes were fragmented and reactive, making it difficult to proactively manage identity risks or enforce consistent access policies. Regulatory compliance was also at risk, with sensitive patient and financial data spread across systems without a unified control strategy. BCI needed a solution that not only protected data but also simplified access, minimized user friction, and aligned with broader BCBSA modernization standards.

The Process

In Time Tec partnered closely with BCI to implement a comprehensive, two-pronged identity and access management solution that would meet the organization's current needs and scale with future demands. The first phase focused on strengthening security through the deployment of CyberArk's suite of tools. This included Privileged Access Manager (PAM) Cloud to secure sensitive accounts, Identity Security to enforce multifactor authentication and intelligent access controls, and Workforce Password Management (WPM) to centralize and monitor credential use. These implementations not only secured high-risk access points but also aligned with BCI's regulatory requirements across HIPAA, NIST, and PCI.

The second phase addressed 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, retiring obsolete configurations, and establishing clearly defined default roles and permission sets. Automation played a key role—SailPoint IdentityIQ was used to streamline user provisioning, while SSO functionality ensured secure, frictionless login experiences. Each step of the project was carefully planned and validated, with thorough documentation and stakeholder involvement throughout. This ensured uninterrupted operations, full team alignment, and a strong foundation 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.

in time tec

Get in Touch:

(208) 258-2424
info@intimetec.com