

Tight Access Controls, Strict Governance and Compliance for Leading Health Insurer

Client Overview

The client is an industry pioneer since the early 1900s, transforming healthcare through innovation and leadership. They are an association of several independently operated companies providing health insurance coverage across the United States.

The Business Situation

The client faced serious security vulnerabilities due to unauthorized access and increasing non-compliance in their environment. The current implementation of Privileged Access Management (PAM) solution, CyberArk had limited controls, addressed only preliminary use cases, involved manual processes, was not integrated with other enterprise applications, and had not been sufficiently documented. As part of their risk mitigation strategy, they wanted to improve their existing solution - on priority, to address current issues and gain full control over user access, governance, and compliance.

The Solution

Long 80 began the solutioning process with a thorough gap assessment to understand the threat landscape and areas of improvement in the existing access control system, CyberArk. This initial phase was followed by several improvements to and automation of processes and workflows in CyberArk. The PAM solution was fully integrated with other enterprise solutions to ensure that all critical applications and infrastructure elements were protected. The implementation details were completely documented, and robust process documents were created. Several optimizations were done to deliver a mature business strategy and robust governance, compliance. Continuous improvements are being done to help the client securely manage access controls of hundreds of employees, effectively manage issues raised across all enterprise applications, and drastically reduce unauthorized access and non-compliance.

Challenges

- PAM solution implemented with limited controls
- Siloed solution not fully integrated with enterprise applications
- Only initial and simple use cases addressed
- Existence of manual processes
- Lack of documentation, process documents
- Increasing unauthorized access, non-compliance

Solution Highlights

- Complete gap assessment to understand threat landscape, improvement areas
- Improvements in, and automation of processes and workflows in CyberArk
- Full integration of CyberArk solution with other enterprise applications
- Thorough documentation and creation of robust process documents
- Optimizations for mature business strategy, and governance
- Continuous improvements to reduce unauthorized access, non-compliance

Solution Outcomes

- Enhanced levels of security, governance, and compliance
- Strict access controls for hundreds of employees
- Increased protection against internal threats and lateral movement
- Drastically reduced access and compliance issues
- Effective management of issues raised across enterprise applications
- Enhanced user experience due to better access management