
# healthcare industry

Privileged Account Management helps healthcare company to mitigate insider threat and comply with HIPPA

**healthcare services**

**total assets**
$ 300 Million

**employees**
3,000+

**no. of privileged IDs**
1,000+

**devices integrated**
300+

**concurrent users**
50+

# client brief

According to the healthcare-focused results of the 2015 Vormetric Insider Threat Report (ITR), a full 62% of respondents identified privileged users—those who have access to all resources available from systems they manage—as the most dangerous type of insider. Partners with internal access and contractors ranked second and third, respectively.

The report pointed out that healthcare data has become highly desirable to bad actors, healthcare records selling for tens to hundreds of dollars. The enormous detail available in patient records is the reason for this, making it possible for criminals to not only apply for credit cards or loans, but to generate large sums from fraudulent medical charges, or even to compromise a patient's existing financial accounts.

In this position our client was constantly faced with rising requirements to meet their security risks and combat constant attacks on their It security structure.

# the challenge

The delivery of health care services—primary care to secondary and tertiary levels of care—is the most visible part of any health care system, both to users and the general public. There are many ways of providing health care in the modern world. The place of delivery may be in the home, the community, the workplace, or in health facilities.

Improving access, coverage and quality of health services depends on the ways services are organized and managed, and on the incentives influencing providers and users. Healthcare administrators are individuals or groups of people who act as the central point of control within hospitals. These individuals may be previous or current clinicians, or individuals with other backgrounds. There are two types of administrators, generalists and specialists. Generalists are individuals who are responsible for managing or helping to manage an entire facility. Specialists are individuals who are responsible for the efficient operations of a specific department such as policy analysis, finance, accounting, budgeting, human resources, or marketing.

These administrators often have direct access to confidential patient information which is stored in their data centers. Healthcare administrators have a dedicated technology support team to manage these data centers and IT for managing the healthcare core infrastructure. Leveraging technology for increasing growth has become a key agenda for healthcare industry over the years. With this new rules and regulations regarding patients confidential data have been enacted by various governments HIPPA is a key example of such rules.

In the recent years Healthcare industry has come under constant cyber-attacks specifically targeting patient's confidential data. Also with cases of privileged users stealing sensitive data have become widely known healthcare industry has become more vulnerable to breaches than ever before. Our team of consultants assessed such issues with a series of discussions with system administrators, patients, healthcare admins and IT steering committee members of healthcare industries. Based on the responses our client realized that the number of privileged users managing patients confidential data will double in the next 10 years has they continue to leverage technology to increase growth thus increasing insider threat from disgruntled employees.

# the solution

The initial phase of the project entailed rollout of Access Control Settings considering shared environment of the data center. This enabled approval for every access to sensitive data, improved productivity and access based on service tickets.
Maintaining the log for each access request was an added silver line to this solution. This feature allowed our clients in ensuring accountability and access on need-to-know basis for data center, application and technology support teams.

*ARCOS privileged account management solution, which is a multitier, lifecycle solution for securing and managing passwords, providing a granular access controls on critical commands and end to end monitoring of all activities associated with privileged accounts helped to meet HIPAA and other compliances for our client.*

Second phase of the project rollout focused on the creation of enterprise level. Password Vault which will enable healthcare industry to enforce an enterprise password policy across their most critical IT systems. ARCOS helps to establish a central management console for flexible operations of all actions associated with password management from requests to resets.

The Solution design provided better authentication and audit capabilities. ARCOS helps the healthcare industry to store and monitors critical audit trails of all privileged actions for audit, compliance and forensic purpose. ARCOS manages to provide highest satisfaction to Risk managers with mechanism for log review for critical sessions either as DVR like recording or as commands and further collaborative integration with SIEM solution provided a real-time alert mechanism.

The Key to successful implementation was a series of pre- implementation workshops that educated users on the technology's capabilities while allowing participants to play a role in defining the scope of the project.

Significant benefits of the consultative approach to ARCOS deployment are highlighted below.

| challenge | solution | benefit |
|---|---|---|
| Administrators need to remember multiple administrative passwords to login to different systems. | Single Sign On (SSO) | Significant reduction in managing account credentials & ability to administer systems using individual identity |
| All personnel had equal privileges for usage of credentials. | Custom Access Control Settings | ARCOS allowed risk team to define custom access control based on requirement and job profile. |
| No accountability for usage of Privileged IDs | SMART* Audit Trails | Comprehensive audit trails generation for compliance and review |
| Inadequate enforcement of password policy & IS control for system users | Secure Password Management (SPM)<br>. Change Control<br>. Electronic Vault<br>. Secured Printing | Seamless workflow & batch job oriented password management coupled with custom solution for storage ready secure envelopes. |
| Non accountability and trace for vendor activities | Vendor Access Controls | Comprehensive audit trails generation for compliance and review |
| Identity theft and sharing of critical system credentials. | Dual Factor Authentication (Soft Token based) | Minimize sharing of password. |
| Review of administrative user activities | Integration with Symantec Log Review Tool | Designing of interoperable workflow allowed for seamless integration with Log review tool to ensure end-to-end monitoring. |

*SMART refers to Specific, Meaningful, Aligned, Realistic, Time-based