ANOMALIX

ANOMALIX CASE STUDY

IDAAS AND SSO

IDAAS and SSO

Background –Regional Health Insurance Company

Anomalix was selected by a Regional Health Insurance company to provide Cloud and On-Premise Identity-as-a-Service (IDaaS).

Anomalix IDaaS provides the following functionality:

1. Identity Governance and Administration for Customer and Employee Access – Access Review and Certification, Access Requests, Approval Workflows and Automated Access Fulfillment
2. Access – Authentication, Single-Sign-On (SSO), Run Time Authorization Enforcement
3. Intelligence – Access Visibility (Who Has Access To What), Real-time Identity Awareness (Who Should and Shouldn't Have Access To What), Audit and Event Logging and Reporting

The Regional Health Insurance provider has over 30K internal users and over 150K patients with up to 500 access related requests in a given day. These requests were directly to 20 mission critical applications that are heavily regulated with complicated request and approval workflow requirements. Additionally, the Regional Health Insurance provider had many disparate authoritative sources for identities and multiple points of entry for where an identity could be uniquely created.

This created a situation where administrators lacked the ability to enforce enterprise security policies at request time. Further, all access reviews and certifications were performed manually in spreadsheets. While the Regional Health Insurance provider centralized employee Identities, contractor Identities were managed disparately ranging from spreadsheets to cloud applications. Having centralized user visibility was a serious challenge.

How We Helped

Anomalix worked with the Regional Health Insurance provider to onboard 20 missioncritical applications to a centralized IDaaS platform providing Authentication and Active Directory-based Single-Sign-On, create custom approval workflows, and automate Active Directory fulfillment. This centralized platform facilitated the creation of segregation of duties rules, an automated quarterly supervisor and data steward access review, real-time dynamic HR rule enforcement (Joiner Mover and Leaver Process).

Conclusion

1. Created a single authoritative user repository
2. Created a way to onboard and manage contractor Identities
3. Automated controls to detect HR events and respond accordingly
4. Automated fulfillment for Active Directory access requests
5. Implemented enterprise business roles, automated birth right access
6. On boarded 200 applications onto a centralized identity governance platform
7. Improved the end-user access management experience
8. Strengthened Client’s overall security and audit posture

ANOMALIX

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144