ANOMALIX

ANOMALIX
WHITE PAPER

Evolve Your IAM Strategy

Evolve Your IAM Strategy

Identity Access Management (IAM) has traditionally been limited to managing access. IAM practices were based on managing access lifecycles for employees, contractors, and outside vendors. The goal of IAM is to identify, authenticate and authorize individuals that utilize IT resources including hardware and applications. The reach of IAM now extends further than traditional employee and contractor paradigms. IAM programs must evolve to govern the adoption of new broad-reaching technologies and the users that are eager to access them anywhere, anytime through a variety of devices.

The expansion of IAM into digital transformation categories such as Cloud, Internet of Things (IoT), Industry 4.0, and Consumer IAM (CIAM) requires programs to evolve with changing business environments.

Cloud refers to software and services that run on the Internet versus on-premise. While the cloud has many benefits, including access to information from any device connected to the Internet, security teams can easily lose insight to who and what has access into their infrastructure.

The Internet of Things, IoT, refers to the physical devices that are connected to the internet. Physical devices range from consumer items like wearables to serious items like robots or driverless vehicles. IoT devices continuously collect and transmit data and are a new challenge for security teams to protect organizations from connected devices.

Industry 4.0 refers to the next phase in the Industrial Revolution that focuses on automation, machine learning, and real-time data in manufacturing technologies. Similar to IoT, Industry 4.0 connects smart machines and factories to the Internet. When machines, supply chains, and robots are connected, security leaders are charged to understand who and what has access.

Customer IAM, CIAM, refers to organizations securely capturing and managing customer identities and data while accessing applications. CIAM plays an important role in digital transformation and organizations must establish a secure and seamless omnichannel customer experience.

As organizations embark on digital transformations, IAM programs have emerged as business facilitators. Now coupled with business initiatives, IAM leaders must be prepared to deliver security and provide value such as identity analytics, fraud prevention, privacy management, etc. Unreliable IAM programs during this transformative time put organizations at risk for breaches. In order to maximize the benefits and compliance in today's environment, security leaders must establish a program that ties to every business activity.

IAM program expansions give leaders the opportunity to learn, add value, and increase budgets. According to Gartner, 53% of IT leaders expect their IAM budget to increase over the next 12 months. IAM leaders must recognize the need for programs to expand, mature and adjust to new conditions.

With organizations focused on digital transformation, cloud integration, IoT, and so on, IAM leaders must partner with other areas of the business to evaluate opportunities for programs to utilize existing or create new capabilities..

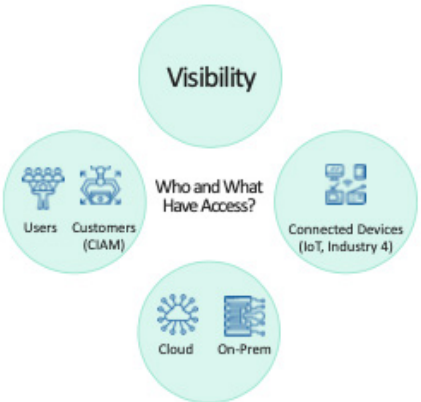
Vision
To build a successful, future-facing IAM program that supports current and future business activities, security leaders should:

- Expand knowledge of new conditions and tie benefits of the IAM Program directly to business outcomes
- Communicate to stakeholders and Executive Management
- Enlist stakeholder support and determine a champion
- Challenge IAM staff to assess new initiatives and interact with other areas of the business

IAM leaders and staff must expand their knowledge of the new conditions. Leaders should understand the evolving conditions and tie benefits of IAM programs directly to the business while ensuring the proper advocates within the organization. Security leaders need to prioritize IAM programs to meet new business needs.

Where to begin?
Identity and Access Management begins with visibility. IAM leaders should gain insight into all of access, resources, usage, and identities across the organization. The reach of IAM has evolved beyond employee and contractor access, gathering data is necessary to gain full visibility. Conduct research on who and what has access to identify areas where IAM needs can be improved. Once opportunities are uncovered, reach out to business leaders to communicate your observations.

The create a modernized agile IAM program that aligns with business initiatives, full visibility is required. To gain visibility, establish communication channels to help recognize IAM opportunities.



Conclusion

Anomalix possesses the experience and expertise to solve the most complex IAM problems within an organization. Our diverse team has deep technical background centered around IT security and IAM. As trusted advisors, our Subject Matter Experts (SME) begin by defining business initiatives and providing advisory and implementation services to ensure IAM programs achieve business initiatives. Anomalix has the knowledge to build, adapt, and evolve your IAM program beyond traditional security functions to include identity analytics, fraud prevention, privacy management, and more.

Anomalix Identity as a Service (IDaaS) modernizes your IT. This cloud-based managed service provides an alternative to in-house IAM programs that lower cost of ownership, increases time to market, and provides leaders the flexibility to focus on larger business initiatives. Anomalix managed services offers intelligent, next-generation solutions.

What are the results?
As a result of an effective IAM program, security and risk management leaders can effectively govern access beyond username and passwords. The role of IAM leaders has evolved into becoming consultative business partners.

Established Communication Channels
Whether inserting themselves into digital transformation projects or attending/reviewing department meetings, IAM leaders can stay informed on new projects and opportunities to assist. Communication with the teams enables IAM leaders to tie the benefits and results to business initiatives successes. If the IAM program is in its infancy, developing communication channels will be a great foundation.

A Strong IAM Advocate to Communicate goals and results
Enlisting an advocate or champion is a critical resource for IAM program success. This resource should be a well-respected individual with the relationships and voice to communicate the goals and results of the program. A strong advocate will vocalize alignment between business initiatives, program capabilities, and their need to safeguard the business.

Development of IAM Interactions
A successful IAM program requires an opportunistic staff that is eager to work inside and outside the organization. The expectations for IAM staffs are evolving to include business awareness along with technical expertise, which requires the IAM staff to network and interact with business partners while seeking outside expertise when necessary. Encouraging IAM interactions keeps your staff aware and educated.

With the digital transformations on the forefront, organizations must include IAM in their ongoing business initiatives. Evolved IAM programs need to verify people, connected things, customers and applications seeking access to ensure they are who they claim to be (identity management) and authorized to use specific resources (access management).

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

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