ANOMALIX

ANOMALIX WHITE PAPER

Why You Should Invest In Iam Solutions

Why You Should Invest In Iam Solutions

Despite industry advances in Identity Access Management (IAM), some of the most recent and largest data breaches are due to insufficient or compromised access protocols. IAM is a gateway for significant critical business processes that include supply chain, digital transformation, Customer Identity Access Management (CIAM) payment, IoT functions and more.

IAM is a facilitator of business processes that enhance a company's value but can be compromised if insufficient controls are in place. Data breaches are expensive to rectify, destroy customer trust and can seriously damage a company's financial standing and reputation. Yet despite advancements, few companies have an effective IAM program in place. What investments do you need to put a successful IAM program in place that is effective, reduces risk, and improves trust?

Vision
IAM advances focus on where vulnerabilities exist in today's systems. A recent study by Centrify indicated that 74% of respondents who have experienced a breach report it is due to access to a privileged account. One example includes a breach in 2017, where Deloitte, one of the largest US consulting firms, had their email server accessed from a compromised administrator password. The incident included accessing proprietary emails from six US government agencies, including numerous sensitive and confidential documents.

Historically, data repositories were located within a company's networks and databases. With advances in cloud technology and remote access by business partners, API's, and IoT technologies, data is located outside the organization, yet access must still be tracked and controlled.

Limiting access while still providing access to an expanding number of stakeholders is a challenging issue. Solving this pervasive problem requires a holistic approach that includes not only data solutions, but collaboration between IT and all departments where IAM must be implemented and monitored. IAM is a link to valuable business processes and IT specialists must have the business knowledge to understand the implications and risks associated with that link.

Understanding where to invest financial, system, and human resources is critical to protecting sensitive data and the organization's reputation.

Solutions

Focus on Privileged Access Management (PAM) to control sensitive data
Executives, network administrators, and positions with significant responsibility typically have the greatest access to sensitive data and often use less-than-secure passwords that can easily be compromised. Hackers target these "privileged" passwords since they represent a gateway to a vast treasure trove of data

that can be hacked, ransomed, or destroyed.

PAM addresses users with high levels of access to secure information and segregates them from other levels of users in the organization. This approach gives the least amount of access to users, including those who need limited access, including vendors, distributors, or service partners. This is similar to the Pareto principle where 80 percent of the assets are controlled by 20% of the people. Targeting the "20%" or privileged users can help reduce risk of a significant breach.

Integrate your PAM with Identity Governance and Administration (IGA) to create a laser-focused IAM management strategy
Traditionally, IGA has focused on the end users of data and included access requests, workflow management, password management, and authentication processes. PAM and IGA traditionally address internal systems like infrastructure, databases and networks to keep data access secure. By incorporating IGA and PAM together, companies can develop a governance program that develops processes for specific levels of users to better protect all internal digital assets. This two-tiered, comprehensive approach reduces risk, ensures access to appropriate users and meets compliance requirements.

Understanding current users and consumers of data is critical for today's systems. But it is also vital that PAM and IGA be built into future systems. To do this means starting early, when the future initiatives are at their initial stages. Including IT leaders in these business discussions will ensure that data is kept safe, is accessed by the right people, and IAM processes provide a secure and seamless customer experience.

Implement a Zero-Trust approach
Some companies are considering a Zero Trust and MFA change from the traditional "trust, then verify" to "never trust, always verify" approach to IAM. This methodology is more conservative but can reduce access to the most complex platforms that include valuable data.

PAM and IGA approaches typically control access to internal systems like networks and databases. But today's systems go far outside of the four walls of the office and include Cloud, Big Data repositories, DevOps operations and containers. Access is not limited to humans, but also includes API's and devices within or outside of the organization, so controlling access to valuable company data is critical. A six step approach is used in a Zero Trust process.

- **Verify Who** – Authenticate who is accessing the systems, which may include people, machines, services, and workloads who access data. Multi Factor Authentication (MFA) is integrated into all processes.
- **Understand Why** – Recognize why the person or system needs access (aka Contextualized Access).
- **Secure Admin Environment** – Prevent potential malware by requiring the workstation requesting data to be disconnected from internet or email applications.
- **Grant Least Privilege** – Provide the lowest level of required access to the user.
- **Audit Everything** – Audit all transactions, not just the risky ones.
- Adaptive Control – Recognize instances when access may include the right credentials, but may be being accessed from a wrong place, and put proto-

cols in place to adapt or restrict access.

Make IAM a highly visible, critical priority in the organization
User identity access management protects access to critical data yet may have low visibility within a company. It is important to make IAM projects highly visible, incorporate them into current and future business ventures, and gain executive support to ensure that IAM projects are successful.

Training and education of IT staff is also vital. Companies may use different software solutions for their IAM needs, so it is important to create IAM generalists who understand security and how it can be protected. The focus should be not only on improving IT skill sets, but also ensuring that IT workers at all levels have a well-rounded understanding of business and company goals to understand how the software will solve business, customer, and industry problems.

Conclusion

Anomalix has the systems and security expertise to create IAM applications that control access to the right users and reduce potential attacks that can threaten your company's data integrity and reputation. Anomalix offers a purpose-built platform for the modern organization that enhances data visibility by:

- Detecting and responding to fraudulent attempts that jeopardize sensitive data.
- Discovering what devices are attempting to gain access.
- Identifying what data is being transferred and from what location.
- Creating a compliant view that is rich in data and respects privacy settings for all internal users, customers, and business partners.

Anomalix is a Gartner recognized solutions and services company for Identity and Access Management, protecting and enabling some of the largest brands in the world everyday. Learn more about the products and services we offer.

Where to Begin
Understanding where to invest your time, energy and budget is critical to your Identity Access Management success. The first step is to understand the current state of access management within your organization by asking these questions.

Identify your IAM infrastructure level.

1. Level one: IAM – do you have basic access management protocols in place to control access to internal databases, networks, and infrastructure?
2. Level two: IGA – do you have access governance tools, policies and procedures that oversee who has access to internal systems, passwords, roles and authentication?
3. Level three: PAM – do you have protocols in place that address privileged users who control your most vulnerable data?
4. Level four: Zero Trust – do you have IAM in place for not only internal but external data repositories for Big Data, Cloud, and DevOps?

Focus on visibility and education.

Train and Develop IAM Specialists. Identity and access is an important link between users (both human and machine) and business processes. It is important for IT personnel to understand not only the technical aspects of that connection, but the business aspects as well. In addition, a company may use many IAM software solutions and developers and administrators must be well versed in multiple applications. Therefore, companies may need to develop IAM Specialists who understand multiple applications, business processes, and end user data needs. Internal training and development programs may need to enhance the technical skills of IT staff members.

Increase the visibility of IAM in the organization. IAM projects aren't just IT projects. Their impact crosses departmental lines and silos and impacts the customer experience. It is for that reason that IAM management projects need executive commitment and sponsorship to be successful. IAM need to be included in not just today's systems, but in tomorrow's plans to ensure that data remains secure, but the company's reputation and trust remain intact.

What are the results

The purpose of an identity access management solution is to keep one of your greatest assets – your data – safe. IAM is the bridge that connects people, machines, and data both internal and external to your organization. Creating an IAM foundation that limits access to the right people through PAM, governs that access through IGA, and provides advanced security through Zero Trust solutions keeps your valuable data safe and business reputation intact.

No systems exist in a vacuum. Connecting IT leaders, department heads, executive sponsors and stakeholders helps to design and implement systems that serve your current and future customers and heighten the visibility in your organization.

As the value of information increases, so will the malicious attempts to access your data. Investing in an IAM system, and the people to support it, will offset the exponential costs required to correct the situation after an attack.

ANOMALIX

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

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