Debunking *Identity Data Security Myths*

Introduction

Identity and access management (IAM) systems have become crucial elements of organizational processes, enabling users to access the necessary tools without needing administrative privileges. With organizations placing greater emphasis on data and the multitude of ways of using and accessing Data, organizations often are left with the question “We have got an Identity Access Management Product, do we also need a data security solution?”.

IAM is most effective when provisioning access to new systems, however, it cannot work in silos from a Data Security perspective. The increasing number of breaches forces us to look at the intersection of Data Security, User Identities and Authorization.

While Identity and Access Management (IAM) is vital, it's equally important to link defined roles in IAM systems to the data they have access to. Currently, IAM and security experts don't have the visibility into the data the specific IAM roles have access to, slowing down approvals for Data requests, impacting Data Worker productivity and delaying Data Projects. A solution like TrustLogix provides that visibility and makes Data and Security Owners more responsible.

Why Data Security is a Complex Puzzle

Multiple Teams and Agreements

Security measures often involve strict protocols that can impede agility and speed, which are crucial for business operations. Ensuring the least privilege access and enforcing policies at a granular level requires agreements across several teams that can hinder business operations. Balancing these competing demands can be challenging.

Steve Tout IAM Expert & Advisor, Identient emphasizes that “Data Security has traditionally been a drag on productivity but ensuring proper access is crucial and needs to be balanced with business needs to ensure data is managed, governed and protected”.

Disconnect Between Business Needs and Security

Business leaders may not fully understand security risks, while security professionals might not grasp the nuances of business operations, leading to misalignment.

Steve Tout points out that “Cybersecurity and data security professionals should learn the language of business and communicate technical concepts to business stakeholders to increase their value and bridge the communication gap between them”

Multiple Sources and Context

In the past access to data was through a simple web interface and mobile App. Today, there are different interfaces to access data such as Power BI Tools, Data Mart for ML Models Bots, Gen AI Platforms, Data Clean Rooms to marry with enterprise data platforms and enable users create their own Data product, Data API for Data Extracts & Applications etc. This diversity requires a review of access controls to ensure that access permissions are kept up to date.

It is essential to be aware of not just interacting with the system, but what happens to the data as it gets into recipient's hands?

Bhaskar Mulugu, quotes “We need to ensure expiration so that access control is not overwritten by one of the layers and data gets leaked. Access control needs to be applied at multiple layers. This is tough to explain to Business partners as they feel defining access at one specific level is good enough.

Traditional Data Security Approaches : Encryption & Classification Fall Short

Traditional data security methods such as Encrypting Data at Rest and in Motion may seem to be a solution however Bhaskar clarifies “Encrypting Data will raise the question in terms of Who will decrypt the data? If decryption falls into the wrong hands, it can create a significant issue. While decryption may be appropriate for certain classified data, it isn't suitable for every data interface”.

Additionally, Data Classification is effective when data remains in a single location. However, as data moves, organizations must adopt a more proactive approach that involves monitoring and governing access. This includes tracking who is accessing the data and ensuring that only those with the appropriate entitlements are doing so.

Disconnect between IAM Platform and Cloud Data Platform

Cloud Data Platforms leverage roles and grants to control access to tables , however these roles are not tied to IAM groups or attributes, so the user information in the two platforms exist in silos.

Data Platform teams must manually manage access through each individual platform and with multiple cloud data platforms, this means writing new code for each new user and data source. All this diminishes data owner productivity and delays data consumption.

Working in Silos: Lack of Visibility for IAM & Security Experts

In Predicts 2024: IAM and Data Security Combine to Solve Long-Standing Challenges Gartner® indicates that “while numerous security responsibilities are handed over to Cloud Service Providers, the protection of data and the management of access remain the end customers’ responsibility across all cloud service delivery models - IaaS,

Ganesh Kirti, CEO of TrustLogix re-emphasizes the fact that “ Both IAM and Data Security are shared responsibility of data consumers and cloud providers. However both work in silos - IAM has its own processes with visibility into applications and Data is flowing in from multiple sources. Entitlements and business SLA’s need to be applied on the data in the data lake to make sure sensitive data is used by the right people with right entitlements. This visibility exists in Data Layer but not for IAM experts. With lack of visibility, IAM and Data Security ends up being in Silos.

Defining Data Security and Protection

Steve Tout, IAM Expert & Advisor defines :

IDENTIENT

"Data Security is a report card of how well we deliver on the promise to protect and secure entrusted data in our organization".

Bhaskar Mulugu, Head of Enterprise Data Platform views:

VIALTO PARTNERS

"Data Security as coming together of governance, operation and security with the data products to get sign off ensuring the data is protected"

Ganesh Kirti, considers **“Data Security Posture Management(DSPM)** to be tools designed to scan data and determine whether the level of exposure puts it at risk”.

Ganesh further adds that **"Data Security Platform** is a broader category that encompasses DSPM; it not only identifies data risks but also implements protective measures such as anonymization, masking, and access controls like Role Based Access Control (RBAC) and Attribute Based Access Control(ABAC). As data becomes increasingly complex—being used, shared, and moved across various environments for purposes like data analytics and LLM training—Data Security Platforms have evolved to effectively identify and protect data at these points of movement”.

Role of IAM in Solving the Puzzle Blending Identity & Data

Gartner's Predicts 2024: IAM and Data Security Combine to Solve Long-Standing Challenges discusses a future where identity and data security vendors start to blend together. This was never possible in the past due to siloed vendors, and siloed internal processes. Data and Identity remains core components of the shared responsibility model that customers are on the hook for.

Considering Multiple Sources

Bhaskar Mulugu shares how IAM needs to consider multiple sources into account:

"IAM gives authentication and Authorization in terms of who the user is and what they can do which is converted into a role and the role is associated with access to specific data, tables etc. Data from multiple sources will have independent access controls; it is essential we honour the access controls with IAM privileges without delay.

VIALTO PARTNERS

Extending the Classification with Data Security Posture Management

While classification helps understand what sensitive data exists in the environment, understanding WHO has access to the data helps enterprises assess the necessity of access and share data only with those who truly need it. It would also help them better respond to data incidents given that the first question after an incident is always "what data was impacted?" followed by, "Who or what had access to this sensitive information?"

Ganesh Kirti suggests how TrustLogix helps addresses the issue :

"Implementing security and governance with monitoring on top of classification is key. As data moves across various systems from Snowflake to S3 bucket, ensuring consistent privileges to access data becomes complex. With the realities of multi-cloud data environments it's crucial to establish the right architecture at the storage level to solve these challenges. This is precisely what we focus on at TrustLogix"

Connecting IAM and Data Platform for Broader Visibility

Ganesh Kirti, stresses that "IAM experts not only need to have visibility w.r.t access of a user to a database or an application but also what type of data the user is accessing inside the data application. IAM Experts often are approvers of data requests and uphold the approval as they do not have visibility which impacts data consumer productivity". So having a solution like TrustLogix that brings that visibility to experts and allows them to implement the entitlements at the data layer is much needed".

Summary

As Data becomes increasingly central to business operations, Security leaders are under a meteoric level of pressure to deliver data quickly. Identity and Access Management(IAM) solutions cannot work in isolation. It must be integrated with Governance to enhance privacy regulations, ensure compliance and security to keep data secure with fine-grained access controls.

Gartner provides a similar perspective.
"Data security needs IAM as a part of the control surface, whereas IAM cannot effectively extend comprehensive access control without data security," the report says. "The result is that combining efforts can enable organizations to overcome long-standing and hard problems that arise when treating both disciplines in silos."

Access controls need to consider the IAM metadata (authentication and authorization that translates into roles associated with access to specific data, tables, etc.) to enable a fine grained data access.

TrustLogix a Multi-Cloud Data Security Platform enables organizations to take a proactive approach towards Data Security by :

- Leveraging IAM metadata to enable organizations implement role based as well as attribute based access to data.
- Compliment Data Classification by adding a layer of security and governance at Storage Layer (i.e Data Security Posture) as the data moves across multi-cloud data environments.
- Creating the visibility for IAM and Security Experts to what data a role has access to, enabling them to understand risks and approve data access requests - eventually enabling quick data consumption and faster data projects.