Devolutions

A Closer Look at Identity and Access Management in 2022

TODAY MARKS THE SECOND ANNUAL "IDENTITY MANAGEMENT DAY."

Today marks the second annual "Identity Management Day." Launched in 2021 by the Identity Defined Security Alliance (IDSA) and held on the second Tuesday in April, the occasion is an opportunity to educate organizational leaders and IT decision-makers on the importance of key aspects of identity and access management (IAM), including governance, practices, technologies, tools, and strategies.

IAM by the Numbers

Effective IAM has become more important in the last few years, as hackers and internal rogue users set their sights on privileged accounts that can contain "the keys to the kingdom" — i.e., confidential and proprietary data that is used to commit identity theft and sold on the dark web.

Despite the risks and costs, many organizations — especially small and mid-sized businesses (SMBs) — are not being proactive. For example, the Devolutions State of Cybersecurity in SMBs in 2021/2022 survey found that **52% of SMBs have experienced a cyberattack in the last year, and 10% have experienced 11 or more cyberattacks.** Yet despite this frequency, 61% of SMBs do not monitor the full roster of privileged accounts in their organization, and **20% of SMBs still use highly insecure methods to store passwords, such as spreadsheets, documents, and writing passwords down on paper.** As the Identity Management Institute highlights in its Identity and Access Management Report 2022:

Cybercriminals are constantly exploring new methods, which means the [IAM] market must remain dynamic to keep up. Just recently, a series of major breaches have again demonstrated that supposedly secure systems are often surprisingly vulnerable…Many enterprises are also exploring IAM strategies beyond basic authentication and access management. They're looking at how their processes can be reengineered to help them automate more of their operations and secure the most critical data portfolios. This is driving an increasing need for IAM technologies that provide solutions for sophisticated requirements that executive management and IT professionals alike must address.

Understanding Identity Management and Access Management

To fortify their IT security posture and reduce the risk of a potentially catastrophic breach — keep in mind that the average cost of a single data breach has climbed to a record $4.24 million USD per incident — organizations need to leverage IAM. But they must not make the mistake of assuming that identity management and access management are synonymous. Yes, there is overlap. However, they are distinct concepts:

- **Identity management combines digital elements and entries in a centralized database, in order to create a unique designation for each individual user.** These designations are monitored, changed, and removed as needed in order to enforce security, while at the same time granting end-users with the permissions they need to carry out various work-related tasks.

- **Access management governs whether or not end-users have permission to access networks, resources, apps, databases, etc.** This concept embraces all of the policies, processes, methods, systems, and tools required to maintain access that is privileged within a digital environment.

Essentially, identity management is concerned with WHO an end-user is, while access management is concerned with WHAT an end-user is authorized to do.

Problems Enforcing IAM

As we have discussed previously, one significant problem that many organizations face when they attempt to establish and enforce IAM is that **certain technologies — such as legacy systems, phones, and cameras — cannot use a federated system.** Although in theory, it is possible to manually create and maintain unique identity accounts for each user, in reality, this ranges from very impractical (for small companies) to virtually impossible (for larger companies).

And so, why don't organizations just eliminate privileged accounts that are shared across roles, teams, and/or groups, and avoid this problem altogether? The answer is that **some privileged accounts are necessary**, such as:

- Domain Administrator Accounts
- Local Administrator Accounts
- Emergency Access Accounts
- Application Accounts
- System Accounts
- Domain Service Accounts

The Way Forward: PAM

The solution to this dilemma is to implement a PAM solution that effectively closes the gap between identity management (authenticating end-users) and access management (granting appropriate permissions to end-users).

A PAM system extends the protection offered by an IAM system into the non-federated identity space through various built-in features and functions, including:

- **A vault that stores passwords** (and other sensitive data, such as building alarm codes, software license keys, etc.), and which is securely shared between multiple end-users.

- **Account checkout**, which allows SysAdmins to grant or reject an access request on a case-by-case basis, and if necessary, set time limits.
- **Notifications that alert SysAdmins** when certain events or actions take place involving end-users, roles, vaults, etc.
- **Automated mandatory password rotation upon check-in.**
- **Automated mandatory password rotation at a scheduled time/date.**
- **Account discovery** that automatically scans and identifies privileged accounts from an Active Directory provider so they can be updated, monitored, or deleted (more on this below).
- **Account brokering**, which automates workflows (e.g., open a VPN client, launch a remote access protocol, and access a privileged account) without providing end-users with passwords in the first place.
- **Session activity recording**, which is crucial for organizations that have contractors and third-party vendors.

Using a PAM Solution for Account Discovery

Research has found that 88% of organizations with more than one million folders lack appropriate access limitations, and **58% of organizations have more than 100,000 folders accessible to all employees**. Standalone identification providers such as IAM systems, databases, network equipment, and servers must be queried to discover accounts. However, as noted above, a PAM system can automatically discover privileged accounts so they can be updated, monitored, or deleted.

IAM Trends

To help leaders and IT decision-makers evolve their IAM roadmaps and architecture, Gartner has highlighted 6 IAM trends in 2022:

1. Connect anywhere computing will further drive need for smarter access control.

The pandemic unleashed the Remote Working Era, which in turn has placed unprecedented demands on access management deployments that must be able to distinguish between legitimate users and hackers or malicious bots. Gartner advises organizations to:

- Weave support for multiple options for user access, device access, and multiple generations of digital assets into a flexible modern identity infrastructure (identity fabric).

- Implement best practices, such as multifactor authentication (MFA), zero-standing privileges, and zero-trust architecture.
- Leverage adaptive access control – a context-aware access control that acts to balance trust against access risk, as a key element of zero-trust architecture.

2. Improving user experience for all users will be essential for securing digital business.

There is a clear link between ensuring positive end-user experience and increasing overall customer satisfaction. In other words, making employees happy is fundamental to making customers happy — and ultimately, driving competitive advantage, growth, and profitability. Gartner advises organizations to:

- Create a cohesive strategy for all external users (consumers, business customers, and partners). An example would be to align IAM priorities with business and IT priorities, deliver an omnichannel experience, and unify customer profile data.
- Apply a zero-trust approach to your organization's digital supply chain (e.g., provide end-to-end security and privacy protection of customer data and other digital ecosystem resources).
- Empower privileged users without sacrificing security by creating an identity for remote privileged users, which authenticates them every time they intend to perform administrative tasks or privileged operations. Then use a shared account that is controlled by a PAM solution.

3. Keys, secrets, certificates, and machines will require more attention.

Organizations must reimagine their IAM strategies in light of the dramatic increase in the volume of machines and their usage in both hybrid and multi-cloud environments. Gartner advises organizations to:

- Establish a fusion team that gathers requirements, provides leadership, defines ownership, lays out guidance, and sets reasonable expectations.
- Determine the machine identities the organization is using, and categorize them into devices and workloads.
- Find organizational and technical ways for your IAM teams to integrate different teams' tools of choice.

4. New applications and APIs will be needed to leverage the latest IAM development guidelines.

As pointed out by IT security executive and DATAVERSITY board member Nathanael Coffing: "Organizations are rapidly adopting new applications infrastructures required to create new business models and customer and partner connectivity. While these technological advancements are providing a multitude of opportunities for innovation among businesses, they have also increased cyberthreats and risks introduced by the distribution of modern cloud apps, growing API usage, and serverless computing." To address these risks, Gartner advises organizations to:

- Establish API access controls by defining new application strategies informed by relevant stakeholders (e.g., developers, DevOps, cloud, security, and IAM).
- Ensure that new applications from all sources are securely developed, sourced, and onboarded by implementing API access control, together with API discovery and API threat protection.
- Ensure alignment across the entire application life cycle by improving coordination between software acquisition teams (both central and divisional) and IAM teams.

5. Hybrid cloud and multi-cloud will drive ongoing IAM architecture maintenance/evolution.

Organizations need to add mature automated compensating controls, as they shift more digital assets to decentralized multi-cloud environments and function in a hybrid IT environment. Gartner advises organizations to:

- Integrate identity governance and administration (IGA), PAM, and cloud infrastructure entitlement management (CIEM) solutions to consistently manage and govern identities and permissions across all environments.
- Establish a single overarching framework for multi-cloud IAM that centralizes some functions, yet also leaves room for native tools.

6. IGA functions will evolve to enable decentralized architecture.

The accelerated pace of digitalization and cloud adoption means that organizations must evolve their IGA capabilities to align with a cybersecurity mesh architecture, and add support for identities in hybrid IT environments, identities in multiple cloud platforms, and machine identities. Gartner advises organizations to:

- Establish an identity fabric using a standards-based connector framework across multiple computing environments, in order to determine who has access to what — regardless of where the resources and users are located.
- Provide better management and orchestration of access policies.
- Use cloud identity analytics for continuous governance.

Concluding Thoughts from our VP of Business Solutions Maurice Côté

Governments everywhere are establishing new information security benchmarks and best practices. Five years ago, cyber risk insurance policies were asking about password managers. Now, we are seeing questions pertaining to PAM.

Although comprehensive enterprise-grade IAM solutions are beyond the reach of many smaller organizations, they must still take action and update their practices. Even using a ticketing system is a major improvement over ad hoc requests. A solution like Remote Desktop Manager can also significantly help in this area as well, as it removes accounts from the equation and allows companies to control who can access various devices. The PAM module in Devolutions Server goes even further by managing the lifecycle of privileged accounts and allows companies to create accounts with a much narrower scope (as compared to more broadly accessible admin accounts).