Identity and Access Management Trends for 2024

Security has become a prime concern with modern technologies and solutions, and password and network hacking is becoming increasingly accurate. Hacking an alphanumeric password

takes less than seconds.

Unprotected data or data not stored on a private server can be compromised. Large-scale breaches can cause reputation damage, financial losses, and, most importantly, exposure to sensitive clientele information.

Hence, IAM has become a priority for organizations to add that extra layer of security to the business network and a necessity if your organization has numerous departments with team members holding unique roles.

Through Identity and Access Management, organizations can record employee activity and moderate access to programs and applications, thus denying unauthorized access and detecting suspicious patterns, transactions, and errors.

Thanks to the introduction of IAM, organizations are now undergoing a secure and controllable digital transition in identity management and security. IAM aids in creating a user-centric and seamless digital workspace where most of the identity access management strategy is automated.

Organizations must develop optimal strategies to deploy IAM effectively. The friction involved in each IAM implementation determines an initiative's success or failure. In 2024, IAM researchers and vendors will concentrate more on new directions and security postures to make IAM implementation more successful.

> According to a recent study, nearly 78% of companies have disclosed an identity-related data breach that has negatively affected their operations. Furthermore, 96 percent of respondents believe that the hack and its consequences could have been avoid if they had used better identity-based zero-trust measures.

Hence it shouldn't be surprising that the global cloud identity and access management market is expected to expand at a **CAGR of 22.71%** to reach **USD 13.42 billion by 2027**. Although

identity and access management frameworks are nothing new, much can be done to keep intruders from breaking into your systems with conventional tactics and technologies.

Schedule A Call

Identity and Access Management Overview

Identity and Access Management (IAM) is controlled using procedures, guidelines, and technological identity access management tools to manage digital identities and restrict access to systems and data. IAM systems are made to prevent unauthorized access, data breaches, and other security threats while ensuring that only approved users have access to resources.

IAM is the process of controlling user authentication (verifying a user's identity), authorization (providing access to particular resources depending on a user's identity and rights), and user management (maintaining a user's sensitive data such as passwords, roles, and permissions). Effective IAM is crucial for maintaining security and regulatory compliance.

Let's quickly review some concerns businesses can resolve when implementing an all-encompassing IAM solution.

1) Cost Savings

One of the main issues businesses have been the rapidly rising expenses of resource management and control. IAM might decrease expenses related to managing user accounts and access credentials. In addition, organizations may effectively manage the resources needed to administer user accounts by automating identity and access management best practices operations. This also lowers the possibility of mistakes that could result in security problems.

2) Scalability

Identity and Access Management services can help manage the complexity of access control and user management as a business expands while upholding security and compliance.

3) Security

Identity and Access Management (IAM) provides a multi-layered defense system that incorporates access controls, privilege management, and multi-factor authentication to ensure that only authorized people can access critical information and resources.

4) Productivity

IAM (Identity and Access Management) can boost productivity by automating user access to resources and reducing the time and effort required to manage user accounts and passwords.

5) Compliance

Businesses must abide by several legal regulations, including SOX, GDPR, and HIPAA. Identity and access management solutions ensure that enterprises have the protection to secure user data and keep audit logs, which helps them comply with these regulations.

Useful link: IAM Best Practices for Optimal Cloud Security

Putting The Spotlight on IAM

The 2024 Identity and Access Management report strategy put a spotlight on primary challenges, gaps, and what works for organizations and security operations teams when it comes to confidential data, information, and workflows:

1) What are the biggest challenges in managing and regulating organizational access?

- Lack of automated processes – responsibility to manually create and define access roles and regulations
- A shortage of skilled employees
- High usage and dependency on mobile devices
- Minimal availability of budgets
- Unavailability of proper resources and technologies

2) How has unauthorized access been a significant cause for concern?

Perhaps one of the most significant challenges cybersecurity organizations face is concerning unauthorized access, which leads to

- Hindrance in business activities, workflows, and daily work
- A decline in employee productivity
- High system downtime
- Increased tickets and support for troubleshooting
- Considerable loss in revenues

3) Which Are The Leading Aspects of IAM Employed by Organizations?

- Role-based, limited access control
- Provisioning of automated users
- Single sign-on method
- Monitoring of workflows and application access
- Audit reporting

4) What Have Been The Leading Factors in Adapting an IAM Program?

- Cybersecurity
- Minimizing data breaches
- Enhancing operational efficiency

5) Which Area is Predicted to be a High Priority for IAM Investment by Organizations?

Organizations are carving out funds in annual budgets to leverage:

- Privileged access management
- Identity management and governance
- Multi-factor authentication program

6) Which authentication methods are popularly used and preferred?

- Username and password
- Software tokens
- Out-of-band authentication

Useful link: [5 Reasons Why Financial Sector Needs Identity and Access Management (IAM)]

How does IAM help your industry?

From finance to healthcare, IAM solutions have been offered to secure and manage identities while providing consumers with the convenient, seamless, real-time access they demand.

Finance	Government	Retail
Protect sensitive patient information	MFA for mission-critical legacy applications	Reduces IT costs with Single Sign-On
Meet mandatory compliance and regulatory measures	Controlling large user access and automating authentication	Manage vendor access via MFA and federated identity
Regulate staff access and defy “permission bloat.”	Protecting workflows and systems at entry points	Authenticate users across multiple locations
It gives organizations more control to speed up onboarding	To improve information security, identities must be monitored and handled regularly	Improves employee lifecycle management

Top 5 Identity And Access Management Trends in 2024:

Let's look at the development businesses and IAM trends that must be adopted in 2024.

1) Machine Identity Using Least Privilege and Zero Trust

IAMs should advocate for the Zero Trust security framework to combat cyber risks and defend hybrid cloud identity and access management environments, systems, and people against unidentified attacks.

Under the Zero Trust model, employees and individuals will be subject to authentication and verification checks during login and in-between sessions. This makes it necessary to provide identification before accessing any organization's resources. That is how businesses may use identity and access management solutions to enable machine identity.

Moreover, enterprises should support the minor privilege concept in conjunction with the Zero Trust model to ensure that employees with network access only have access to the systems they need. Such an IAM strategy enables firms to automate the machine identification idea.

2) Using Enhanced MFA for Further Security

We all know that Multi-factor Authentication (MFA) can protect our accounts and systems against unauthorized access.

According to a Verizon survey, over 90% of breaches involve phishing attempts. Therefore, threat actors can steal your passwords and essential authentication credentials.

Therefore, identity and access management solutions should focus more on requiring MFA via OTPs and provide a third layer of authentication by automatically checking usage patterns, IP addresses, locations, the devices they are using, etc.

Enabling risk-based authentication control (RBAC) functionality can give organizations long-term advantages. Therefore, identity and access management services companies also concentrate on enhancing the RBAC function through AI.

3) Ecosystem for Decentralized Identity

Organizations from many industries aim to employ decentralized identity ecosystems rather than centralized systems for identity management due to the rise in identity theft and privacy leakage over the past several years. As a result, IAM providers and product developers are concentrating on utilizing blockchain to advance identity management in a decentralized manner.

Due to the user-centric nature of such a system, implementing a decentralized identity ecosystem using blockchain technology will preserve user identity. The users will be in charge of maintaining their identifying information.

Additionally, it will encourage identity governance and administration (IGA) and other regulatory compliance to align with the organization's data privacy and security architecture.

4) Enhanced Identification and Security With AI and ML

Artificial intelligence (AI)–powered IAM systems can improve security and identity identification more precisely.

Using machine learning algorithms, the IAM system may learn from millions of user actions, behaviors, and authentication transactions. These algorithms can subsequently detect or anticipate anomalies or security breaches.

In the future, machine learning (ML) systems will monitor computer sessions, determine whether a natural person is using the system, forecast internal and external risks, and anticipate the pattern of a data breach.

5) More Attention Paid to User Consent and Data Privacy Through Compliance

Organizations and end users are paying more attention to data privacy and data consent as user data leakage and privacy violations are making headlines more frequently. IAMs must keep up with all the most recent compliances and policies relating to user or employee data.

According to new legislation, identity and access management companies must obtain user authorization before retaining or exploiting customers' personal information. As a result, IAM service providers strongly emphasize maintaining compliance with laws such as GDPR, COPAA, HIPPA, SOX, ISO/IEC 27017, and others.

Conclusion

We recognize the demand for a flexible, user-friendly IAM platform. Veritis, the Stevie Award winner, offers a one-stop shop for all your identity and access management solutions requirements. We provide an automated, centralized, compliant identity governance and administration system with access management and adaptive access management capabilities that address the present identity requirements and potential future difficulties.

Got Questions? Schedule A Call

Also Read:

- IAM Best Practices for Optimal Cloud Security
- Healthcare Identity and Access Management (IAM): Five Steps to Transformation
- 8 Best Practices for Robust Identity and Access Management (IAM) Strategy
- Top Tools and Security Protocols That Make IAM Successful!
- Best Practices for Effective 'Identity and Access Management (IAM)' Implementation
- IAM Implementation and Solutions To Emerging 'IT Security Challenges'