



Top Five IAM Trends to Watch for in 2020

Table of Contents

Introduction **03**

IAM & IoT **03**

Comparing Traditional IAM and IoT IAM **04**

IAM for Cloud Services **04**

Artificial Intelligence (AI) &
Machine Learning (ML) **05**

Consumer Identity &
Access Management **06**

Key Difference **07**

Bring Your Own Device (BYOD) **07**

Conclusion **08**



Introduction

A robust IAM (Identity and Access Management) solution has become an integral part of enterprise IT. A secure, flexible, and adaptive **Identity & Access Management** (IAM) solutions will enable organizations to improve employee's productivity and boost their overall security features.

Identity & Access Management is no longer limited to controlling access to a system or resource. Access control now also be applying to networks, internet connections, websites, printers, server rooms, software applications, Wi-Fi and many more.

In the recent past, we have seen a tremendous growth in technologies like IoT, Big Data, Cloud Computing, and BYOD. **IT Security** has obviously become a hot topic as each of these technologies depend on it, and with an increasing number of threats, **Data Security** has always been a prime concern. Limiting access to data and information according to their work requirement for the users helps to reduce the risk of data leakage.

With the advancement in technology and identity environment, it has become a challenge for the IT Security to manage with the traditional approach. IT leaders are required to develop their identity and access management (IAM) strategies, and the solution providers need to come up with new features & innovation.

In the near future, organizations will look for below five innovations in Identity & Access Management (IAM) solution:

IAM & IoT

IAM (Identity Access Management)

Along with new innovations in IAM, we can even witness a drastic growth in the field of IoT (Internet of Things). Every modern organization is looking forward to use IoT devices to help their business. That creates a huge need for secure Identity Access Management (IAM) solution. Every type of IoT device in an organization increases the security risk exponentially.

Defining and managing device identity in the constantly evolving IoT environment has become a top priority for IoT vendors. Traditional Identity and Access Management (IAM) approach could not deal with this challenge. Hence, IAM solutions and its design & architecture approaches need a massive change, keeping number of device connection in IoT environment and security concern in mind.

The purpose of IoT connected devices is to leverage the collection of data from the devices by linking it directly to the business systems. However, this linkage also creates a security **risk** if not managed properly.

In the IoT world, IAM solution should be able to identify each connected device, sensors, monitors, and manage and control their access to all type of sensitive and non-sensitive data. Creating identities for these items and managing appropriate access for these identities throughout the connected ecosystem will stretch the IAM approach to new limits. IAM solutions should not be solely concerned with managing people but also managing the hundreds of thousands of “things” that may be connected to an organization’s network.

Comparing Traditional IAM and IoT IAM

	Traditional IAM	IoT IAM
End Points to Manage	Typically < 100,000	Can be millions
System Administrator	IT & Security Departments	Operational Personnel, plant & Business Manager
Auditing	User-Centric	Device-Centric
Authenticating Process	Passwords, Biometrics	PKI Certificates, Device, Behaviors, Biometrics
Provisioning & Registration Process	Static	Dynamic, Application Driven
Self-service	Typically, Web Based	Support Bluetooth, DSRC, etc. Wireless Communication

IAM for Cloud Services

Cloud computing is massively on the rise, and it will continue to gain momentum. Organizations, regardless of their nature or size of the business are moving to cloud networks & infrastructure due to the benefits like cost-effectiveness, scalability, reliability, and flexibility. The tradition of “build vs buy” is being replaced by “rent vs buy”.

Cloud Network and **Infrastructure** has its own security concerns. After all, the data, information, and identities are hosted and managed by a third-party cloud provider in their Cloud Infrastructure.

Provisioning to Cloud Applications is less standard and has more complexity. IAM solutions need to build the right strategy for the future roadmap. New standards, such as SCIM (Simple Cloud Identity Management), are emerging, but have not been widely accepted yet.

IAM solution provider will require to build expertise to control the security concerns for Public **Cloud Services** like AWS, Azure and GCP. In an organization, if you are using hundreds of services from a Cloud provider, it may get difficult to understand who/what has access to which resources. This is challenging, but the IAM solutions, policies, approach, and capabilities are continuously growing.

However, in addition to standard IAM issues, organizations are facing few Cloud-Specific challenges as well like Orphan SaaS accounts, multiple admin accounts and users bypassing organization IAM controls which reflects a lack of control over the account lifecycle that many SaaS scenario presents. To handle these challenges, IAM solutions providers must come up with a better governance strategy for identities.

Artificial Intelligence & Machine Learning with IDAM

From Machine Learning to natural language processing, Artificial Intelligence and cognitive computing are elevating beyond speech recognition and rule-based systems to help organization consume and derive value from big data and drive decision-making through powerful analytics.

Artificial intelligence (AI) programming algorithms can be used to data-mine, and the technology like Big Data can reveal the suitable data patterns as part of the data analytics. Many Banking systems are already using this type of analysis globally to reduce fraud.

A Machine-Learning system based on Artificial Intelligence, can get to know a person incredibly well such that all the research and data collected about them, combined with multi-factor authentication, will securely identify most people.

The powerful method of IAM access patterns is the Behavioural analysis which can bring policy violations to the surface. The combine efforts of Artificial Intelligence (AI) and Machine Learning (ML) explicitly used to alert on behavioural changes in application and user. These changes could include the API client (e.g. web console vs Python Boto), the location of the API call (e.g. the US vs Europe), or the types of permissions.

Analytics combined with artificial intelligence will offer focus and discourse insights so each technical and non-technical worker will work longer and economical.

The innovation of new technologies has enhanced the present IAM compliance controls with the help of new insights and automated process. It can detect anomalies and potential threats and does not require an oversized team of security consultants.

It helps IAM solution to work in a preventative or even corrective approach of access management, rather working as reactive access management.

Consumer Identity & Access Management

Traditional businesses or the new-age ones, customer has always been every businesses priority. Every organization want to provide the best customer experience, and for this purpose, they request customers to provide valid data and information.

It is a common misconception that technology & approach for consumer identity and access management (CIAM) is the same as that for traditional identity access management (IAM).

Traditional IAM is designed to control employee access to internal data & application. It does not provide insights into who a user is. CIAM platforms, on the other hand, are designed to give companies maximum value from customer profile data and give a better insight into who this user is.

While traditional identity and access management (IAM) features are directed for employees, CIAM is focused on customers. Furthermore, traditional IAM solutions are designed to administering up to tens of thousands user records, but a high-volume brand will require a solution which should be capable of managing hundreds of millions of customer accounts.

However, the lines between traditional IAM and CIAM solutions are becoming increasingly blurred. There is a significant increase in features relevant to both types of identity management solution.

A well implemented CIAM solution will help the organization to achieve the proper balance of customer experience without any compromise on IT security or consumer data privacy.

Key Difference:

	IAM	CIAM
Business Drivers	Reduce Risk & Improve Efficiencies	Attract & Retain Users
Scale	Thousands of Users	Many Millions of Users
Identity Evolution	Employees Know When Hired	Consumers Identified Over Time
Privacy Protection	Employee-Centric	User-Centric
Service Levels	High	Extremely High
User Involvement	Employer Set Policies & Procedures	User Sets Preference & Profile

Bring Your Own Device (BYOD)

Many organizations are now adopting BYOD (Bring Your Own Device) approach and allowing their employee partner, customer, and visitors to connect to the corporate network using their own device. This increases the challenge for IT because they need to protect corporate data and yet provide the users with access to the corporate network using their own device. Mobile malware is also threatening security. Thus, it becomes extremely important for Zero-trust security architecture to protect the organisation's critical assets.

Employees, contractors, partners, and others are bringing in personal devices and connecting to the organization's network for professional and personal purpose, and IT team has no choice to manage or not to manage the devices. The challenge with BYOD approach is not only that outside devices are brought into the corporate network, but also IT need react quickly enough to protect the organization's data & assets, without disrupting employee productivity and still offering freedom of choice.

Key to this will be the quality of identity access management solution. It should be flexible enough to ensure restricted & controlled access to all critical applications and data, but at the same time, not imposing too much of security restriction for the everyday task that it starts hampering productivity. BYOD, wireless and mobile means that identity based on location or a corporate device is no longer a choice.

IAM solutions and approach should be quick, easy, and secure to grant and revoke access to corporate data & applications to employee and devices based on corporate guidelines or regulatory compliance.

A reliable enterprise Identity and Access Management (IAM) solution will incorporate a single access control policy, sign-on and separation of duties, among other features. Two other nuggets here include:

A better IAM strategy enables your line of business managers to have control over compliance, as they often know best who needs access to what

An IAM solution which includes both on-premises and mobility security features for access management ensures comprehensiveness

Conclusion

Identity access management will continue to evolve in scope and scale. It is very clear that an effective IAM solution should be secure, efficient, simple, productive, compliance, but the cost and complexity involved with deploying a robust IAM solution may delay the process for a most well-intentioned organization as well. The traditional security perimeter is shrinking. Corporates are searching for IAM solutions with mobile workforce in an organization and a highly distributed and complex network of applications.

Identity and access management approach are becoming more complex, and hence the ability to create process & policies based on granular, contextual information will become more and more important. IAM solutions should be able to make decisions based on various parameters like, user identity, location, device, and the requested resource. And deliver quick access permission to legitimate employees, partners, contractors, or guests—and easily revoke or deny privileges to unauthorized users.

Work with IAM solutions that may not yet be perfect, but flexible, governable, and scalable and keeps the future market trends in check.

Author Bio



Kunal Jaiswal is a Senior Technical Lead at Happiest Minds. He has over 10 year of experience in Identity & Access Management domain. Proficient to design, configure and implement IDAM solution. He has strong IT background with in-depth knowledge on NetIQ, MIM and RSA IDAM solution implementation along with developing different proof of concepts around this space for Happiest Minds. He is a Certified Novell professional and CCNA certified.

Business Contact business@happiestminds.com

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in the U.S., UK, The Netherlands, Australia and Middle East.