What is **Identity and Access Management?**

CONTENTS

© 2019 Sennovate. All Rights Reserved

IAM is about defining and managing the roles and access privileges of individual network users, and the circumstances in which users are granted or denied those privileges. Typically, users can be customers (customer identity access management CIAM) or employees (employee identity management).

Overview

With ever changing complex compute environments and constant increasing security threats, the importance of identity access management (IAM) has gained significant importance. In the current day context, IAM incorporates elements of biometrics, machine learning, artificial intelligence (AI), risk-based authentication, and identity-as-a-service (IDaaS). A data breach report from Verizon indicates 97% of breaches are preventable, making a good enough case for IAM.

A typical IAM access life cycle comprises with directory of personal data the system uses to define individual users, and set of tools for adding, modifying and deleting that data; a system that regulates user access, and an auditing and reporting system to oversee these related activities. The goal or purpose of IAM systems is single digital identity per individual.

Benefits of IAM

- Decrease in help desk calls for IT support on password resets
- Allows administrators to automate IAM and save time costs enhance service delivery
- IAM helps IT teams to define access policies for whom and which data to be given access
- Better control of user access reduces internal and external breaches

© 2019 Sennovate. All Rights Reserved

Identity and Access Management

Providing the right people with the right access at the right

Authentication

- Single Sign-On
- Session Management
- Password Service
- Strong Authentication

Authorization

- Role-based
- Rule-based
- Attribute-based
- Remote Authorization

User Management

- Delegated Administration
- User and Role Management
- Provisioning
- Password Management
- Self-service

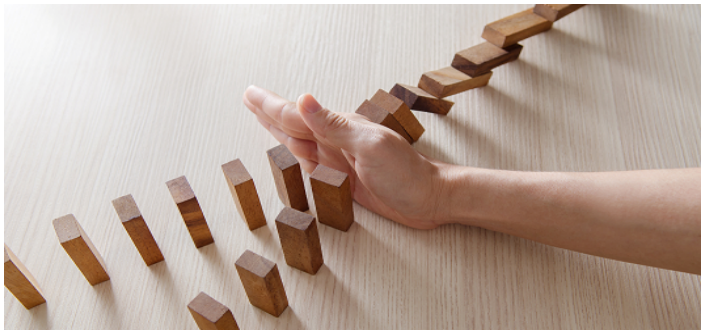
Central User Repository

- Directory
- Data Synchronization
- Meta Directory
- Virtual Directory

© 2019 Sennovate. All Rights Reserved

Open standards & IAM

IAM is supported with open specifications like SAML for exchange of security policies, its inter-operability across vendor platforms providing authentication and authorization services. OpenID, WS Trust, WS Federation, OAuth are similar standards supporting IAM.



Challenges with IAM

Dimensional Research released a report, Assessment of Identity and Access Management in 2018.' Based on a survey of more than 1,000 IT security professionals, the report stated, 59 percent said that data protection was their biggest concern about their organization using IAM. Only 15 percent said they were completely confident their organization would not be hacked due to their access control system. Security professionals concerned about integrating IAM with legacy systems (50 percent), moving to the cloud (44 percent), and employees using un-approved technology (43 percent).

IAM systems hold the key to valuable assets and critical systems in an organization, in case of failure of IAM will be critical. Much planning and collaboration is required before implementation. Hence managing different users in different situations and computing environments automatically and in real-time.

© 2019 Sennovate. All Rights Reserved

Regulations

Regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA hold organizations accountable for controlling access to customer and employee information.

CIAM – An added approach to IAM

Consumer Identity and Access Management (CIAM), is also known as B2C IAM. CIAM technology centres around customer identities, provides more security, control and visibility of data and information. CIAM primarily be seen as a business enabler. Most of CIAM platforms are cloud-based due to the scalability and performance it offers to manage many customer interactions. Besides, on-premises platform does co-exist at the enterprise level

IAM Integrator

The role of an integrator is multi-functional and complex. The integrator role is to act, understand customer business requirements, and interface with the customer and vendor if required. The integrator ensures that achieving interoperability, collating information, data flow, protocol conversion and routing is well taken care.

© 2019 Sennovate. All Rights Reserved

IAM Vendors

IAM vendor scape is fairly big one, consisting of both pure-play providers such as Okta and OneLogin and large vendors such as IBM, Microsoft and Oracle. Below is a list of leading players based on Gartner's Magic Quadrant for Access Management, Worldwide, which was published in June 2017.

Market Trends

In 2018, the global IAM market size was estimated at over US$ 8 billion, and is expected to experience a CAGR of over 12% from 2018 to 2025. The biggest spenders on security are seen from government organizations and large-scale industries, owing to strict regulatory compliances. The BSFI end-user segment is also seen as a big user owing to higher level of security for customer data. North American market is estimated to get highest revenue share due to products and technological developments, and government initiatives. The APAC market is expected to grow in terms of revenue, owing to investments for security software by large scale enterprises.

Based on IAM deployments, the target market is segmented into cloud, hybrid, and on-premise. The cloud IAM deployment segment is expected to register a significant growth in terms of revenue owing to increasing adoption of cloud-based IAM services. Enterprise is expected to move in the hybrid direction.

© 2019 Sennovate. All Rights Reserved

Sennovate's IAM Solutions

- Single Sign On (SSO)
- Multi Factor Authentication (MFA)
- Privileged Access Management
- Identity Governance and Administration
- User Provisioning & Lifecycle Management
- Audit And Compliance
- Enterprise Password Management
- Directory Integration

Sennovate's IAM Services

Identity & Access Management Consulting

Sennovate is on the cutting edge of using Artificial Intelligence (A.I.) to make your job easier and give you greater peace of mind — through our product-specific A.I. Security Assistants (Okta, SailPoint, CyberArk, Thycotic, etc.)

Identity & Access Management Design & Implementation

Our security experts can design the perfect Identity and Access Management solution for you — choosing the best products and infrastructure for your needs — and also serve as ongoing security advisors to your in-house IT staff.

Infrastructure Management Services

We ASSESS your information security needs, DESIGN and implement the right solution, and then MANAGE that solution for you seamlessly. Also, our A.I. Security Assistants help you get optimal results with greater peace of mind using Artificial Intelligence.

Managed Security Services

We can completely manage your Identity and Access Management infrastructure on-premises or in the cloud — acting as a seamless extension of your IT team and taking on the responsibility of ensuring up time and security.

© 2019 Sennovate. All Rights Reserved

Powered by AI

Schedule Free Assessment

Call: +1 925 918 6618

SENNOVATE

Sennovate is a global Managed Security Services Provider (MSSP) that specializes in Identity and Access Management (IAM). Our solutions helps companies meet complex compliance requirements, and leverage their IT more effectively for better business results.

 Sennovate

 Sennovate

 Sennovate

+1 925 918 6618 | sales@sennovate.com | www.sennovate.com