International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Identity and Access Management Tools

Mr. Vinay Jayprakash Pol

Bharti Vidyapeeth Institute of Management and Information Technology,
CBD Belapur, Navi Mumbai, Maharashtra, India

How to cite this paper: Mr. Vinay Jayprakash Pol "Identity and Access Management Tools" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.796-798, URL: https://www.ijtsrd.com/papers/ijtsrd23935.pdf

IJTSRD23935

ABSTRACT

Identity and access management is a vital information security control for organizations to minimize the insider threats and advanced persistent threats that are caused by mismanaged user's identities and access control on sensitive business applications.

Unauthorized access to business-critical IT applications results in information disclosure and financial loss for many organizations across the world.

Deployment of identity and access management as an essential information security control will enable organizations to detect or even prevent security breaches due to unauthorized access.

This paper elaborates necessary facts for making decisions towards protecting the organization's assets using IAM controls.

The purpose of this paper to compare various Identity and access management tools.

Keywords: *IAM, Identity and Access Management, SSO, Cyber Security, Authentication, Authorization*

INTRODUCTION

IAM

Identity and access management refers to the ability to manage user identities and their access to it resources such as systems, applications, files, and networks.

IAM solutions have been a critical aspect of IT infrastructure for many years now as they help to make work happen.

However, many IT admins have come to discover that traditional IAM solutions are struggling to manage the complexity of modern networks.

As a result IT organisations are now looking for new approaches to identify and access management.

Historically the most popular IAM platform has been Microsoft active directory.

Active directory is an on-prem IAM platform that was designed for on-prem windows-based environment.

When AD was introduced in 1999, most IT network were on-prem and windows-based.

Windows has remained the most popular enterprise operating system ever since.

However, IT networks started to change as Mac systems, Linux servers, web applications, alternative storage solutions, google apps, aws and the cloud came to market in the mid-2000s.

Solutions such as these weren't windows-based, nor they on-prem.

Consequently, active directory implementations began to struggle and have been ever since.

Of course, IT organizations could patch active directory with third party add-ons such as identity bridges, web applications single sign-on, privileged identity management and more to mitigate some of these traditional challenges.

The trouble with this approach, however, is that it adds significant cost and complexity, not to mention that modern IT organisations would rather shift their identity management infrastructure to the cloud.

The good news is that a next generation cloud IAM platform has come to market that is effectively active directory reimagined for modern networks.

IAM tools has the power to manage virtually any IT resource, without the help of costly third-party add-ons and without anything on-prem.

How IAM works?

It is more than just SSO or authentication, it's an ongoing process that continuously verifies a user's identity and enforces access policies each time a user logs into a cloud application.

So in the old ways there was only one remote access point the VPN.

Authenticate to the VPN and get access to all of the enterprise apps you need in one shot.

But nowadays an employee may need access to several different cloud apps throughout the workday.

This is a hassle for both users and IT.

Users have to remember many credentials which IT has to manage.

The solution to this program is SSO.

By having one credential for all cloud apps, user can easily log in once to several apps while IT saves time on password reset.

Well depends how you look at it.

While convenient, SSO can also be risky.

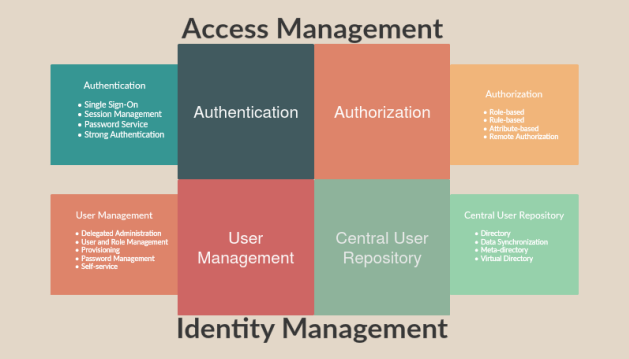
By allowing users to login to a bunch of apps with one credential, it leaves all cloud apps vulnerable if that credential were to be compromised.

This is exactly where Cloud Access Management comes in.

By combining Identity Verification, SSO and Access Policies Enforcement an Access Management Solution can continuously verify a user's identity and enforce access policies for each application.

So user gets an SSO experience while IT protects access to cloud apps.

IAM framework



1. Authentication

Authentication is a function using which a user enter their credentials to obtain access to application.

Once authentication of user is done, session is created for communication between user and application.

After maintaining the user's session, it provides Single-Sign-On service so that user does not require logging in into the system again.

2. Authorization

Authorization is a function that decides that a user is permitted to get access to a particular resource.

Authorization checks the resource access request from URL in web-based application and compares it with authorization policies that are stored in IAM.

3. User Management

User management consists of user management, password management, user /group provisioning and role /user management.

It provides various administrative functions such as identity creation, propagation and maintains user identity and provides.

One of its features is user life cycle management that allows enterprise to manage the lifespan of a user account, from the initial stage of provisioning to the final stage of de-provisioning.

Self-service is another feature in user management, so that user can update their data.

Another function of self service is self-password reset, so that they can reset password of their own.

4. Central User Repository

This is where all the information about user is stored.

Central user repository also provides identity data to other resources and verifies the credentials submitted by various users.

List of Tools

1. SailPoint
2. IBM
3. Oracle

1. SailPoint

Sailpoint is an eco-friendly model.

It's a powerful IAM tool against data breaches and data leakage.

Its capacity to work with large amounts of data provides a competitive advantage in a world where online data is getting bigger and bigger, as well as it improves security for global teams.

2. IBM

IBM Security Identity Governance and Administration is a suite that integrates their Security Identity Manager and their Security Identity Governance system (based on the recently acquired Cross Ideas platform).

This IAM solution includes user access management, identity management and governance, and regulatory compliance evaluation.

3. Oracle

The Oracle Identity Governance Suite is particularly convenient for large organizations.

It is a complete solution that uses analytics to address privileged account management, user administration and identity intelligence.

COMPARISION OF VARIOUS TOOLS

Features	IBM	SailPoint	Oracle
Access Management	Yes	Yes	Yes
Single Sign-On	Yes	Yes	Yes
Multi Factor Authentication	Yes	Yes	Yes
User Activity Compliance	Yes	Yes	
Identity Governance	Yes	Yes	Yes
Managed Security Services	Yes	Yes	Yes
User Provisioning	Yes	Yes	Yes
Automate Risk Mitigation	Yes		
Compliance Manager	Yes	Yes	Yes
Lifecycle Manager	Yes	Yes	
Identity Intelligence	Yes		
Governance Platform	Yes	Yes	Yes
Integration Modules	Yes	Yes	
Secure Token Service	Yes	Yes	Yes

Conclusion

Businesses that need to design and implement complicated IAM strategies and need strong support along the way would be the best suited for this tool.

Since IBM provides strategic, as well as deployment solutions, if an enterprise has an IAM problem and does not know where to start to solve it, IBMs IAM tool can help. IBM is an industry leader with both tradition and innovation capabilities,

Therefore, many enterprise businesses choose it as the best all-in-one identity access management (IAM) tool to reduce risks of insider threat and identity fraud, manage administrative compliance and automatically improve collaboration between users.

Reference

[1] https://www.sciencedirect.com/science/article/pii/S2215098617316750#s0225

[2] https://searchcloudcomputing.techtarget.com/feature/How-to-get-started-with-IAM-services-in-the-cloud

[3] https://www.getkisi.com/blog/identity-access-management-tools