IAM CHALLENGES

Challenge1: Managing identities across multiple cloud environments

With the increasing use of multiple cloud environments, organizations face the challenge of managing user identities across all their cloud systems. This requires an IAM solution that can support multiple cloud environments and provide a single source of truth for identity information. A unified IAM solution will allow organizations to easily manage identities, control access, and enforce security policies across all their cloud systems. One such example is the usage of more than one software-as-a-service (SaaS) application. Creating a local identity for each of the SaaS application makes it very difficult to keep track of the all the people who have access, which in turn may result in leavers retaining access to such applications.

Challenge2: Threat materialization in cloud-based identity providers

Organizations are increasingly moving towards cloud-based identity providers (for example Google and O365). This usage brings in a challenge that is different from an on premise identity provider. Whilst on-premise identity providers have their own set of challenges in terms of threats and vulnerabilities, from an impact perspective it is small. Threats and vulnerabilities applicable to cloud-based identity providers have a larger blast radius and the impact could be huge.

Addressing this situation is tricky. Whilst for many organizations it makes business sense to move to cloud-based identity providers, organizations may also need to monitor the threat landscape to keep themselves ahead of the curve.

Challenge3: Ensuring compliance with regulations and standards

Organizations are required to comply with various regulations and standards such as GDPR, PCI DSS, and HIPAA, which impact their IAM strategy. An IAM solution must be capable of enforcing these regulations and standards to ensure that sensitive information is protected and that organizations are not at risk of non-compliance.

Challenge4: Managing identities for non-human entities

IAM solutions must also be capable of managing identities for non-human entities such as applications, services, and APIs. This requires a comprehensive IAM solution that can manage identities, provide visibility, control access, and enforce security policies for non-human entities.

Challenge5: Integration with emerging trends

IAM evolves in response to the threats faced. Evolving IAM trends include passkeys and password-less authentication. Cloud service providers and organizations need to factor in the evolving trends and prepare for transition with technology change and user education.

Challenge6: Keeping pace with the ever-evolving threat landscape

The threat landscape is constantly evolving, and organizations must ensure that their IAM solution is capable of adapting to new threats and vulnerabilities. Credential harvesting is as applicable to cloud IAM as it is to on-premise IAM. An IAM solution must be capable of providing real-time security intelligence, monitoring, and alerts to ensure that organizations are aware of new threats and are able to respond to them in a timely manner.

Challenge7: Managing identities for external users and partners

Organizations must also manage identities for suppliers, external users, and partners who need access to sensitive information. An IAM solution must be capable of controlling access and enforcing security policies for external users and partners, while also ensuring that sensitive information is protected from unauthorized access. Granting time-boxed Just-In-Time access is one way to address this challenge.

Challenge 8: Addressing the unique challenges of BYOD and identity

BYOD policies bring their own set of challenges for IAM, including managing identities for personal devices and ensuring that sensitive information is protected from unauthorized access. An IAM solution must be capable of addressing these challenges and providing a seamless and secure authentication process for employees using personal devices.

Challenge 9: Managing identities for IT/OT, that are located on-premise but interface with cloud based solutions

IT/OT devices like any other devices need identities. Managing these identities pose a challenge as traditional security measures like password rotation and MFA do not apply to OT. Organizations must manage these identities along with the vendors to ensure that any compromise of the cloud-based solution does not impact the OT devices and any compromise of the identity of an OT device does not impact the enterprise network. An IAM solution must be capable of managing identities for all types of resources, controlling access, and enforcing security policies, regardless of where the resources are located.

Challenge 10: Maintaining visibility and control over role bindings and access controls

Organizations must maintain visibility and control over role bindings and access controls to ensure that sensitive information is protected from unauthorized access. An IAM solution must provide real-time monitoring and alerts to ensure that access controls are being enforced correctly, and must also provide the ability to revoke access in real-time if necessary.