cloud
CSA security
alliance®

What is IAM For the Cloud

Release Date: 07/13/2023

Identity and Access Management Working Group

What Is Identity & Access Management (IAM) For The Cloud?

cloud
CSA security
alliance®

What is Discussed?

1 The differences between cloud environments vs. on-premise that affect IAM

2 Retrospective analysis of IAM

3 Where is IAM Heading

4 The ever increasing significance of IAM in a cloud environment

5 Challenges organizations face when adopting IAM effectively for the cloud

6 Cloud IAM opportunities

7 Considerations and best practices for an effective IAM program for cloud environments

8 Tips for Security/IAM leaders and practitioners on communicating the value of IAM

The differences between cloud environments vs. on-premise that affect IAM

- Ownership: On-prem IAM provides complete ownership including software licenses, user administration, and ongoing capital expenses. In contrast, cloud IAM uses a shared responsibility model with a subscription approach, leveraging cloud service providers (CSP).

- Control: While on-prem IAM grants organizations full control, including aspects like vulnerability management and patching, these "security of cloud" tasks are handled by the CSP in a cloud-based IAM.

- Complexity: Cloud IAM can become complex and challenging with multiple IaaS, PaaS, and SaaS environments, particularly during access control reviews and deprovisioning of identities, leading to potential security risks.

Retrospective analysis of IAM

- IAM has evolved from the mainframe era to becoming a significant discipline in the client/server era with distributed applications and identity silos.
- Directory services, particularly Microsoft's Active Directory, were introduced to manage identity silos using LDAP and enabled same sign-on across platforms.
- Single Sign-On (SSO) was developed to alleviate the problem of multiple credentials, facilitating authentication and authorization across an organization's applications.
- Custom-built applications automated user lifecycle management and access policies, later evolving into Identity Governance and Administration (IGA) solutions.
- In the last decade, IAM moved to the cloud, leveraging its benefits and reducing the need for specialized maintenance resources.
- To streamline IAM use cases and reduce associated costs, solutions are converging to offer integrated IAM solutions like IGA, Privileged Access Management (PAM), Access Management, and Customer Identity and Access Management (CIAM).

Where is IAM Heading

- Cloud-first strategies are being adopted by organizations, leveraging IAM solutions unique to each platform and addressing new identity actors endemic to the cloud - machine identities, service accounts, workload identities, and human identities.
- Key Trends:
  - Decentralized Identity Models: Emergence of Blockchain and self-sovereign identity models where users control their own identity data.
  - Just-In-Time and Risk-Based Access Controls: Access provided only when and for as long as needed, with decisions based on user and resource risk levels.
- Cloud IAM Challenges: Managing users and entitlements spread across multiple cloud platforms, and handling ephemeral workloads instantiated by DevOps tools.
- IAM for the Cloud: Compared to on-prem, cloud IAM involves increased volatility and growth, the need for agility, and unique compliance risks. A shift in approach includes the increased use of APIs as opposed to group policy-based practices in on-prem environments.

The ever increasing significance of IAM in a multi-cloud/hybrid environment

- Cloud technology offers numerous benefits like pay-as-you-go, quick implementation, Opex vs. Capex, and scalability. This has led to significant growth in cloud implementation at both enterprise and consumer levels.
- Enterprises adopt hybrid and multi-cloud strategies, moving resources to the cloud where human/non-human entities require authentication/authorization. This shift increases vulnerability as resources are no longer within the network perimeter, necessitating the correct access to resources.
- Challenges in a multi-cloud environment include managing user access to various scattered resources, managing entitlements, and handling service accounts/Machine Identities running automated processes across different workloads.
- An effective IAM strategy is crucial in the cloud environment to address these challenges.
- IAM plays a critical role in protecting organizational assets and data, reducing risk, enabling compliance, and supporting the overall security strategy, highlighting its importance to senior leadership. Benefits of cloud migration such as improved multi-cloud visibility and maintaining visibility into role assignments can be emphasized to convey this value.

Challenges organizations face when adopting IAM effectively for the cloud

- Managing identities across multiple cloud environments
- Threat materialisation in cloud based Identity Providers
- Ensuring compliance with regulations and standards
- Managing identities for non-human entities
- Integration with emerging trends
- Keeping pace with the ever-evolving threat landscape
- Managing identities for external users and partners
- Addressing the unique challenges of BYOD and Identity
- Managing identities for IT/OT, that are located on-premise, but interface with cloud based solutions
- Maintaining visibility and control over role bindings and access controls

Cloud IAM opportunities

- IAM is the glue that binds Cloud services, providing the foundation for agile responsiveness to new business requirements.

- A sound Cloud IAM strategy can accelerate digital transformation initiatives, drive business model innovation, and expedite the transition to a data economy.

- The automation potential of Cloud IAM offers significant productivity for developers and builders.

- Cloud IAM can help reduce operational cost and streamline compliance and governance.

Considerations and best practices for an effective IAM program for cloud environments

Considerations

- Centralized management of identities, access and authorization across multi-cloud and hybrid environments
- Automation and integration with existing systems
- Robust and secure authentication methods
- Authorization and access control policies based on user roles and attributes
- Regular monitoring and auditing of access and activities
- Compliance with data protection regulations
- Integration with other security measures such as encryption and threat protection.
- Apply least privileges as much as possible and need to know basis rule
- Leverage advanced features such as JIT, PAM, and PIM
- Automating IAM Processes
- Comprehensive Monitoring and Auditing

Best Practices

- Implementing multi-factor authentication to secure access
- Creating and enforcing strong password policies
- Wherever possible shifting from strong passwords to passwordless
- Implementing role-based access control (RBAC) for users and applications
- Encrypting sensitive data (including credentials) in transit and at rest
- Regularly monitoring access and activity logs for anomalies and security incidents
- Continuously assessing and updating security policies to stay up-to-date with the latest threats.
- Understanding that IAM in a cloud environment directly impacts cloud data security.

Tips for Security/IAM leaders and practitioners on communicating the value of IAM

- Clearly articulate the business benefits of IAM, such as improved end-user experience, seamless single sign-on, improved security, compliance, and efficiency.
- Provide tangible examples of how IAM has helped other organizations achieve their security goals.
- Use data and metrics to demonstrate the ROI of your IAM program.
- Communicate the importance of IAM as a critical component of the organization's overall security strategy.
- Provide training and education to all employees to ensure that they understand the importance of IAM and their role in keeping the organization secure.
- Foster a security culture within the organization and encourage employees to report any security concerns.
- Regularly communicate updates and progress on the IAM program to all stakeholders.

Conclusion

- Managing IAM in the cloud presents unique challenges compared to on-premise environments, necessitating a clear strategy to secure assets and data.

- IAM teams should align with senior leadership to communicate IAM's value and its role in the overarching security strategy.

- Organizations must implement processes for monitoring and verifying identities, and understand the unique challenges associated with managing identities for both human and non-human entities.

Acknowledgements

- Lead Authors
  - Ravi Erukulla
  - Alon Nachmany
  - Ramesh Gupta
  - Shruti Kulkarni
- Contributors
  - Heinrich Smit
  - Jonathan Flack
  - David Strommer
  - Venkat Raghavan
  - Faye Dixon
  - Paul Mezzera
  - Ansuman Mishra
- Reviewers
  - Michael Roza
  - Radhika Bajpai
  - Claude Mandy
  - Shannon Chisenga
  - Shamik Kacker
  - Samuel Addington
  - Nishanth Singarapu
  - Adnan Rafique
  - Ivan Djordjevic
- CSA Analyst
  - Ryan Gifford