WHITE PAPER

IMPROVING CLOUD SECURITY WITH EFFICIENT CLOUD IDENTITY & ACCESS GOVERNANCE

Abstract

Enterprises today are at different stages of cloud adoption. Each stage and structure (multi-cloud, hybrid cloud or single cloud) demands different control adoption. This whitepaper discusses the controls and governance required to successfully manage explosion of identities and entitlements as enterprises embark on digital transformation journey. It highlights on the reach, significance and requirement for multiple identity and entitlement management for principals spread across on-premise and cloud. The authors have talked inn depth on CIEM (Cloud Infrastructure Entitlement Management), IGA (Identity Governance and Administration) and Privilege Access Management.

Infosys®
Navigate your next

Introduction

Understanding Cloud Identities & Access

Let's first understand the scope and form of identities on cloud and in the hybrid landscape. Digital identity on cloud is not limited to be associated with a human being, rather it could be assigned to a compute service e.g., VMs or Container, or to a server less service e.g., app service or lambda function, or to any entity that can talk to other entity or service on cloud.

Similarly, the accesses (entitlements or roles) are not only limited to enterprise business apps/systems. The entitlements/permissions can belong to any service or data holding entity on cloud or hybrid environment. E.g., An S3 bucket in AWS account or a storage account in Azure may have several types of permissions attached with that. In general roles can hold list of permissions on any cloud service. Some of these permissions are privileged or highly privileged permissions.

Understanding key elements of governance for identities and accesses on cloud

Managing who has access to what, why, how, when and till what time is a real challenge in the cloud due to fast moving changes in the cloud landscape. To bring a continuous 360-degree view on identity and access governance on cloud, it's important to address the following requirements:

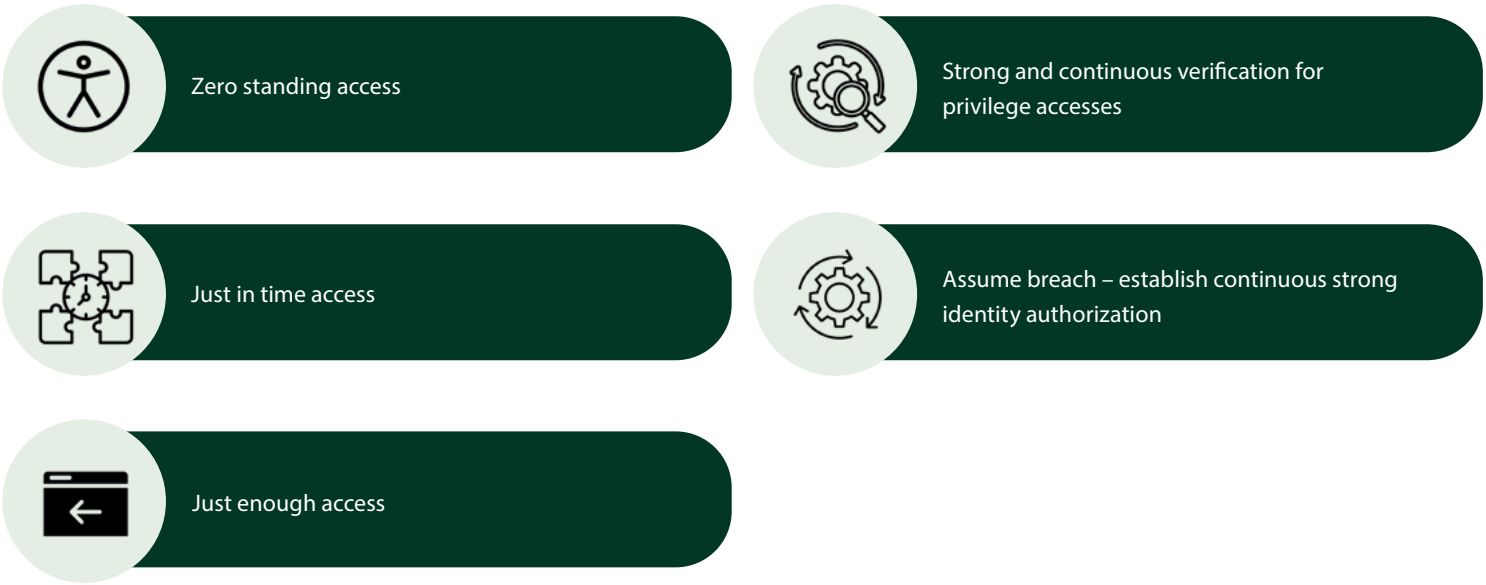
- Policy driven access criteria both for human users and to any non-human e.g., workload, bot services etc
- Cataloguing of cloud permissions with categorization of privilege/risky and non-risky permissions
- Potential risks associated with any permission grants on cloud entities, services holding or processing sensitive and confidential data
- Monitoring and reporting with any time view on who has what access
- Monitoring and reporting with risk visibility associated with assigned accesses due to various reasons such as misconfiguration, poor access control, or policy violations
- Visibility on potential possibilities of data breaches due to above mentioned risk scenarios
- Risk based access recertification – especially for identified privilege entitlements and identities on cloud
- Auditability for granted permissions – especially to human users and for assigned privilege roles and accesses on cloud services
- Clearly defined ownerships and RACI for RBAC on cloud services
- Defined operating model and standard procedures to mitigate risks associated with permissions and policy/compliance violations

The problem in hand

With emergence of modern applications and dynamic threat vector, organizations are pushed to embark on a digital transformation journey. Demands of varying identity fabric across on-premises and cloud landscapes, makes handling of identity and entitlement explosion even more complex and requiring high level of competence.

Enforcing Identity Governance principles on cloud and hybrid environment

One of the most prominent defense strategies lay around enforcing strong identity and access governance on cloud and hybrid environment. In fact, the governance elements are embedded in with zero trust identity principles such as:



This will lead to ensuring a strong cloud security posture and reducing risk posture. Thus, Cloud Identity Access Governance is even more important to be enforced than ever.

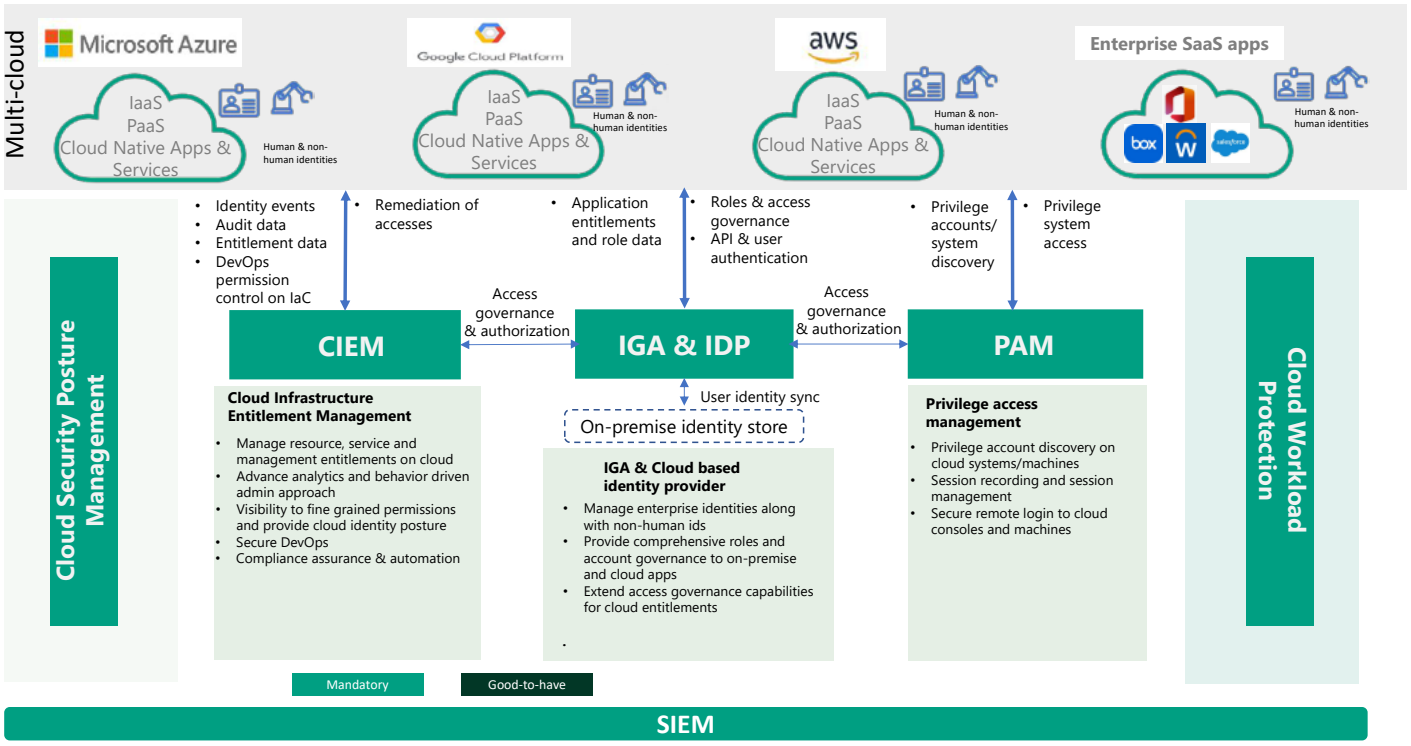
Enterprise may have existing investment on few solutions and capabilities such as Enterprise IGA, Centralized IDP and Privilege Access Management. But these solutions are working in silos, without complimenting each other without sharing access and risk information. Cloud Identity & Access Governance can be achieved with an enterprise specific common approach. Here the existing investments are optimized along with new investments on gap areas such as automated discovery of assets and access profile for them.

For this Infosys proposes Cloud Identity Governance enforcement with its Cloud IAM factory approach. The key solution tenets for this approach are:

- Rich cataloguing of cloud permissions along with their risk level categorization
- Policy based (role-based and risk-based) access provisioning with ITSM or with IAMOps pipelines
- Multi-Level approval workflows for privileged and highly privileged permissions
- User access reporting
- Access risk identification and mitigation
- Approver authority delegation
- Periodic and risk-based privilege access certification
- Forensic investigation and auditability
- Access privilege services and data on cloud and hybrid environment through secure channels e.g., Enterprise Privilege Access Management solution (CyberArk, Entra PIM, AWS etc.)

Though human enterprise users float into cloud with combination of enterprise AD, IGA cloud connectors and group/role structure replication on Cloud IAM (Identity & Access Management) service, Non-human users are more cloud specific and require complete governance pivot to understand and manage. Identity being the spear of all cloud exploits below is representation of the technologies involved and specific information exchange.

Infosys recommends utilizing potential of enterprise IGA, IDP and PAM solutions along with cloud infrastructure entitlement management capabilities.



IGA:

While IGA will help on managing the enterprise user's identity life cycle, govern their accesses on enterprise apps and system, it can also help managing, non-human identity life cycle, governance of their accesses on multi-cloud environments, with the help of their cloud specific provisioning and entitlements/role aggregation connectors.

PAM:

On the other hand, Privilege Access Governance for many of privilege permissions on cloud, also to be achieved with PAM and IGA solutions integration.

IDP:

Organization with existing IDP will always help ensuring contextual and risk-based authentication policies enforcement, especially with human driven accesses.

CIEM:

Organizations still require capabilities to discover assets and services specific access profiles and evaluate the access risk posture on a continuous basis. Along with those capabilities, additional capabilities such as blast radius view based on misconfigured or over permissive access risk, data breach likelihood prediction and actionable risk mitigation recommendation are also required.

Understanding vital role of Cloud Infrastructure Entitlement Management solution to enforce Cloud Identity and Access Governance.

Continuous governance and validation for all cloud identities is need of the hour. Enterprises need an automated solution that continuously validates both human and non-human cloud identities. Evaluation needs to be backed with risk association for each identity and view into the potential damage the identity can cause. Continuous evaluation also provides insight into privilege creeps and potential deviation from baseline activity for an identity.

Below are some of the challenges addressed by CIEM:

Correctly estimating the cloud asset inventory to cover all workload security

Creating visibility into net-effective permissions identity entitlements

Implementing controls to ensure principle of least privilege and least access

Reducing identity blind spots in enterprise cloud environments

Ensuring common identity policy controls across hybrid and multi cloud platforms

Creating alerts by triaging Identity, Data and Risk actors

Managing complexities around small duration access (JIT Access)

Fundamentals delivered by CIEM:

Continuous identity hygiene and inventory

The tool continuously evaluates cloud identities and associated entitlements. Post identity inventory, hygiene-based policing is applied and alerts if any are documented or orchestrated with tools downstream.

IAM Security baselining and entitlement normalization

CIEM will help to create a baseline policy structure for acceptable identity posture. The tool will also help to define the reach of the identity by orchestrating the potential reach of the identity. This combined with the continuous identity inventory evaluation helps to reduce the unknown in terms of identity and its potential impact on resources in cloud.

Principle and permission-based risk correlation

The tool helps to chart out the risk correlation between the entitlements of identity principal and impact that principal can cause if its identity goes rogue. Assuming admin role, assuming roles to move from UAT to prod environments are some of the examples of value delivered.

Data and identity combined risk view

The tool helps to classify data (for some OEMs), integrate classification data from 3rd Part tools (for some OEMs) or learn from tags associated with data sources to create data specific identity policies. These policies then help to magnify identity related risk score by defining potential risk of escalated identities having access to confidential data.

Functional pillars in adoption of CIEM:

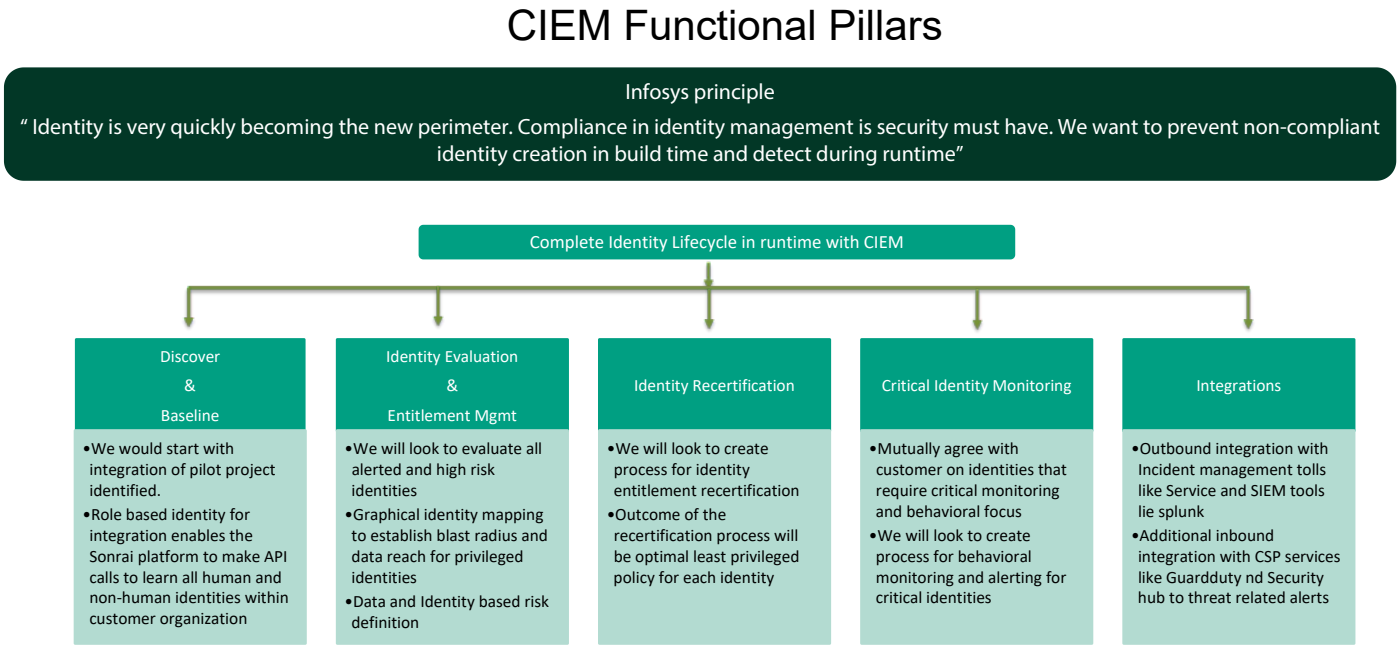
> Cloud Infrastructure Entitlement Management (CIEM) offerings are specialized identity-centric SaaS solutions focused on managing cloud access risk via administration-time controls for the governance of entitlements in hybrid and multi-cloud IaaS. They typically use analytics, machine learning (ML) and other methods to detect anomalies in account entitlements, like accumulation of privileges, dormant and unnecessary entitlements. CIEM ideally provides remediation and enforcement of least privilege approaches. - Gartner

Based on the above Gartner definition for CIEM, below is a simplified functional principle

> *"Identity is very quickly becoming the new perimeter. Compliance in identity management is security must have. We want to prevent non-compliant identity creation in build time and detect during runtime."*

In adoption of CIEM, this paper looks at mitigating all the challenges with regards to cloud identity governance. It further looks at creating standardized industry aligned baseline identity policies, understanding through workshops with enterprise security and application teams to understand critical identities, define process for periodic privileged identity recertification and integration options to correctly get data or orchestrate outcomes with downstream tools like ITSM or SIEM

Below is a diagram representing functional pillars for CIEM adoption:



Integrate the pilot cloud project/account/subscription into the CIEM. As part of the integration process role based identity is created. This identity enables the CIEM platform to make API calls to learn all the human and non-human identities within customer organization. The discovery process mentioned below starts post integration.

Identity Discovery and Baseline Policing

Post integration, identity discovery is done by the CIEM platform for both human and non-human cloud identities. The immediate outcome is that all the known and unknown cloud identities are documented to create an accurate cloud identity inventory. After the inventory is secured, you can verify against your known identity database. You will be surprised with the number of unknown identities.

After confirming the identity inventory, we will proceed to create baseline for the identity management and policing. Below are the fundamental policy frameworks that will be applied:

Identity evaluation and entitlement mapping

We will look to put in initial efforts to evaluate all alerted and high risk identities.

Charter items:

1. CIEM allows complete identity evaluation from perspective of access, activity and potential risks based on policy framework.
2. Each identity risk results in an alert with potential remediation or false positive dismissal option. The alerts are further marked with severity. The severity tag is helpful to identify roadmap for potential remediations of identity deficiencies.
3. Each identity risk is also supported with relation graph indicating the potential reach for the identity. This helps to understand reach of identity and potential damage it can cause in the enterprise cloud landscape.
4. Document the potential mitigation data provided by CIEM platform. This action steps that will be included in the correction roadmap. Some platforms offer identity remediation. However according to this paper, there should be a single location for all cloud changes. So downstream workflows need to be created to enable IAC tools to take corrective actions.

Define Process for Process for periodic identity recertification

We will look to create process for identity entitlement recertification and optimal least privileged policy creation.

Charter items:

1. CIEM tool will identify and create an alert for all high privileged identities. You can further boost this logic by defining some of your critical cloud services.
2. Grade the alerts and define escalation path with workflow steps for recertification for each privileged cloud identity.
3. Stakeholder needs to provide approval and acceptance of participation in the recertification workflow.
4. Evaluation with entitlement utilized from CIEM tool to create right sized identity policy.

Identifying critical identities for hyper care

After the initial tool fitment and POC establishment, more granular identity perspective will be established. In partnership with the enterprise security and application teams, identify critical identities and place them under hyper care.

Charter items:

- With a key stakeholder workshop identify cloud identities both human and non-human that are critical to the enterprise
- Enable greater detection and visibility for the identity so that it can monitored to create a baseline
- Baseline will typically cover aspects such as:
    - o Geography from where identity is used
    - o Who is using the identity?
    - o What is being accessed?
- Alert workflow for any deviation from baseline

Inbound and Outbound Integrations

After all the CIEM tool level configurations, orchestrate the outcomes with multiple inbound and outbound integrations.

Charter Items:

- o Typical out of box integrations supported by most OEMS:
    - o Slack
    - o ServiceNow
    - o Jira
    - o Sentinel
    - o Email
    - o Splunk App
    - o Aws Security Hub
- o Additional customized use case that might be helpful are below:
    - o Integration with external vulnerability management tools such as AWS Inspector or Tenable
    - o Pull the workload related information. Use it for network and identity risk amplifiers for resources
    - o Integration with IGA tool like SailPoint for additional Identity governance controls

Now that the CIEM tool is established with compete adoption. Let us look at some of critical use cases that can be delivered:

Use Cases:

Use Case	Sub-Function	Benefits
Gain immediate visibility over permissions and entitlements across multi-cloud infrastructure	Discover and Baseline	Multi-Cloud landscape can be adequately monitored if identity view and policies can scale across CSPs
Maintain a continuous comprehensive identity inventory	Discover and Baseline	Consistent identity inventory lends itself to accurate policing and alerts
Mitigate privilege creep by continually illuminating and right-sizing excessive permissions	Access Recertification	Privilege escalation is a prominent risk vector in cloud
Graph all trust relationships between identities and data	Identity Evaluation	Trust relationship graph gives insights into potential risks and lateral movement of risks
Understand the risk associated with over-provisioned identities and entitlements, with a single risk score	Critical Identity Monitoring	Compete identity inventory view from risk perspective
Accurate view into each cloud entity entitlement at all times	Identity Evaluation	Continuous identity evaluation and entitlement normalization
Automatic detection and audit of dormant accounts	Identity Baselining	Removal of Dormant account. Reducing the attack surface for the enterprise.
Data classification-based identity risk definition	Critical Identity Monitoring	Identifying identities with access to critical data sources will help to mitigate any data-based identity risk
Ensuring Least Access Privilege implementation	Identity Discovery and Baselining	Least privilege is important but equally important is to ensure that the identity created only has access to required resources

Outcome:

- Consistent identity visibility and hygiene across multiple cloud platforms
- Complete identity lifecycle management for all cloud identities
- Automated check to ensure delivery of all identity entitlements with security and governance plugged in
- Incident and change management gating controls for all phases of identity lifecycle
- Principle of Least Privilege and Least Access adherence as guiding principle
- Identity based risk definitions and alert/recertification for escalated privilege

Conclusion

Enterprise today faces the mammoth task of managing the explosion of identities brought forward by the digital transformation era. With identity being the primary threat vector, the task further multiples itself. The traditional way of handling identities also doesn't cover all bases. Hence it is necessary to pivot, adopt new tools and technologies but at the same time continue using the parts of old technology that provide desired outcome. this paper talks about an amalgamation of technologies from CIEM to the traditional IGA and PAM. Though the task is monumental the document charts out aspects and use cases which if adopted that simplify some if not all the identity related pain areas.

References

https://sonraisecurity.com/blog/the-basics-of-cloud-infrastructure-entitlement-management-ciem/

https://sonraisecurity.com/blog/when-would-you-use-ciem-solutions/

https://www.rapid7.com/fundamentals/ciem/

https://www.gartner.com/en/articles/iam-leaders-plan-to-adopt-these-6-identity-and-access-management-trends

https://ermetic.com/blog/cloud/how-to-implement-ciem-a-checklist/

About the Authors

Nitin Bajpai

Principal Consultant, Infosys CyberSecurity

Nitin is an experienced and accomplished Information Security Professional with 18+ years of experience, spanning all facets of Information Technology and Security. His proficiency include design & implementation of Identity Security solutions, Cloud and Digital Work Place Security, Zero Trust Enterprise Architecture, Emerging Technologies and Security Advisory. Nitin has been working with Infosys for more than past 5 years. Nitin is a member of Infosys Cyber Innovation team. In his current role he is contributing in exploring and developing possible cyber defense approaches to counter emerging security challenges in ever changing technological landscape.

Vinit Ajgaonkar

Principal Consultant, Infosys CyberSecurity

Vinit possesses rich experience in Cyber Security domain of more than 14 years. He is currently a part of the Infosys Cyber Innovation, Strategy & Excellence Team which dwells into next generation cyber security solutions and strategies. Vinit is a cloud security architect with a panache for helping customer in their digital transformation journey. He has the right mix of technology thought

leadership backed by hands-on tool/technology focused curiosity. He has very god problem solving skills and learning new technologies.

For more information, contact askus@infosys.com

Infosys®
Navigate your next