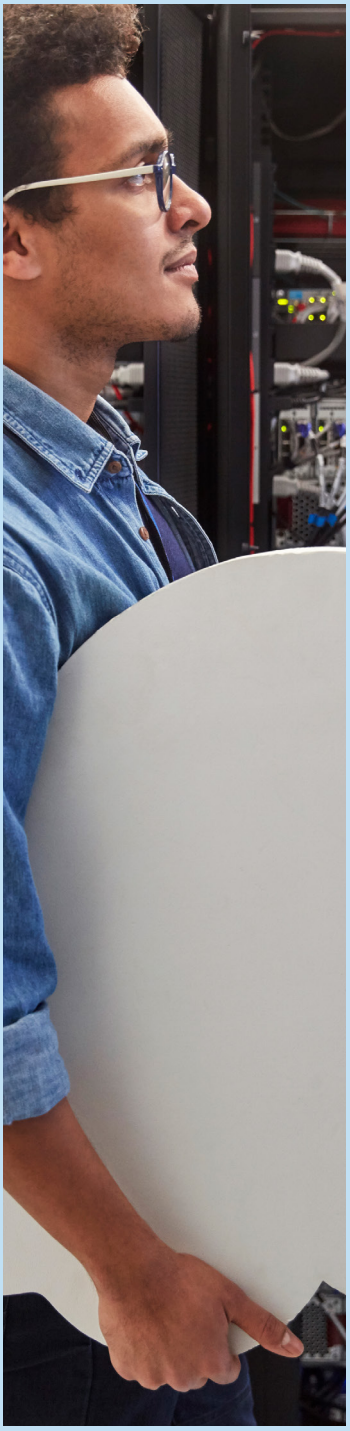
Infosys cobalt

VIEW POINT



ADOPTING PRINCIPLE OF LEAST PRIVILEGE IN THE CLOUD ERA

Infosys®
Navigate your next

The unprecedented times seen over the last 2 years has brought about an accelerated rise in adoption of cloud services amongst enterprises cutting across business verticals. This has resulted in greater proliferation of cloud identities (human and machine) and privileges, whose management has been of a larger concern. As per the Verizon's '2021 Data Breach Investigation Report' report, nearly 80% of privilege misuse related incidents are caused because enterprises could not establish visibility of excessive access to sensitive data. The challenge of securing cloud ecosystem is more complex as the traditional perimeter-based "castle and moat" defenses no longer apply to cloud platforms. It is essential that enterprises setup processes and systems establishing holistic visibility and governance into access provisioned in the cloud ecosystem. The agility, scalability and elasticity associated with cloud environments introduces a set of governance related challenges which need to be addressed within the overall construct of a cloud-aligned identity governance offering. This mesh of visibility and governance related concerns become more amplified in hybrid and multi cloud environments. Enterprises need to adopt solutions which can prevent misuse of privileges across complex multi-cloud environments.

The key proponent to strengthen privileged access in cloud is by enforcement of the principle of **least privileged access.** However, least privilege model does not imply that non-extinguishing privileges required to perform the role are granted across the lifecycle of cloud identities. Instead, privileges should be granted on-demand for the respective job or action and enterprises should adopt the Zero Standing Privileges (ZSP) framework. Aligned with the Zero Trust framework, a context-based dynamic privilege grant model will enable enterprises to securely adopt identity as the new perimeter. The management of secure cloud development practices need to keep pace with the dynamic nature of cloud resources and be integrated with the DevSecOps principles.

An integrated solution which caters to the 3 broader requirements of- visibility, zero standing privileges and governance- will suffice best for security and risk challenges presented by the multi-cloud and hybrid cloud environments. It should establish:

a. Visibility of cloud identities (human and machine) which have access across the cloud tiers

b. Dynamic, policy drive and context aware Just-In-Time access provisioning through balanced, risk aware posture of privileges mapped with Zero Standing Privilege framework

c. Governance for the access, ensuring long-standing accesses are remediated and no identity has more privileges than needed to perform their respective job role.

Enterprises should progress ahead in the Zero Trust journey with the adoption of zero standing privilege principles, JIT access, policy driven dynamic provisioning of privileges and comprehensive identity management and governance framework. To establish 360 degrees of visibility, enterprises should also integrate the logs from cloud environments with the User and Entity Behavioral Analytics (UEBA) and Security Information and Event Management (SIEM) engines. This allows identification of anomalous user behavior. The automation led and AI/ ML augmented capabilities allow for dynamic baselining of the access behavior patterns across cloud architecture, trigger alerts for detected anomalies and creation of dynamic access certification events within the integrated IGA platform.

In gist, to secure the enterprise journey in adoption of zero trust framework, the following must be considered in the adopted solution:

- Real-time and risk-aligned visibility through automated discovery of dynamic resources across hybrid and multi-cloud architectures
- Dynamic policy driven and context aligned JIT access for human and machine identities to cloud resources (applications, infrastructure, services etc.)
- Establish unified insights for detection and prevention of privilege abuse, misconfiguration through integration with UEBA and SIEM capabilities.
- Convergence of identity lifecycle management, governance and privilege management capabilities through adoption of next-generation IDaaS and PAMaaS technology construct that sufficiently address the need for cloud native and cloud aligned provisioning, identity lifecycle, privilege management and identity governance requirements
- Leverage AI and ML driven technology capabilities to baseline access patterns, identify anomalies and trigger risk-based dynamic certification requests
- Set up a continuous process of enforcing least-privilege policies, reduce the attack surface and create a balance between security and usability, with a focus on setup of frictionless user journey experiences

Infosys delivers managed Identity-as-a-service capabilities for enterprise leveraging the Saviynt IGA and Saviynt Cloud PAM solution offerings. With a rich experience in delivering enterprise scale projects aligned with Saviynt's cloud-first vision, Infosys enable enterprises to leverage the key business benefits of moving to cloud while managing the blind spots and vulnerabilities related to unmanaged or over privileged cloud identities. The Infosys' managed IDaaS and PAMaaS capabilities focus on outcome based, risk aligned provisioning and privilege management framework, aligned with digital transformation journey of the enterprise.

Infosys Cobalt is a set of services, solutions and platforms for enterprises to accelerate their cloud journey. It offers over 14,000 cloud assets, over 200 industry cloud solution blueprints and a thriving community of cloud business and technology practitioners to drive increased business value. With Infosys Cobalt, regulatory and security compliance, along with technical and financial governance comes baked into every solution delivered.

For more information, contact askus@infosys.com

Navigate your next