

Microsoft Entra Permissions Management

Infosys' Path with Permissions Management



Get to know Permissions Management

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) product that provides comprehensive visibility and control over permissions for any identity and any resource in Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP).

Discover how Permissions Management helps companies improve their security posture by ensuring the principle of least privilege access for any identities and resources in multicloud environments.

Today, over 89% of the organizations are already using multicloud.

Automation and DevOps revolution are making identities ever more powerful and causing exponential growth in them, leading to rapid expansion of the attack surface.

Using Permissions Management, organizations can implement least privilege access consistently and prevent data breaches caused by misuse and malicious exploitation of permissions.



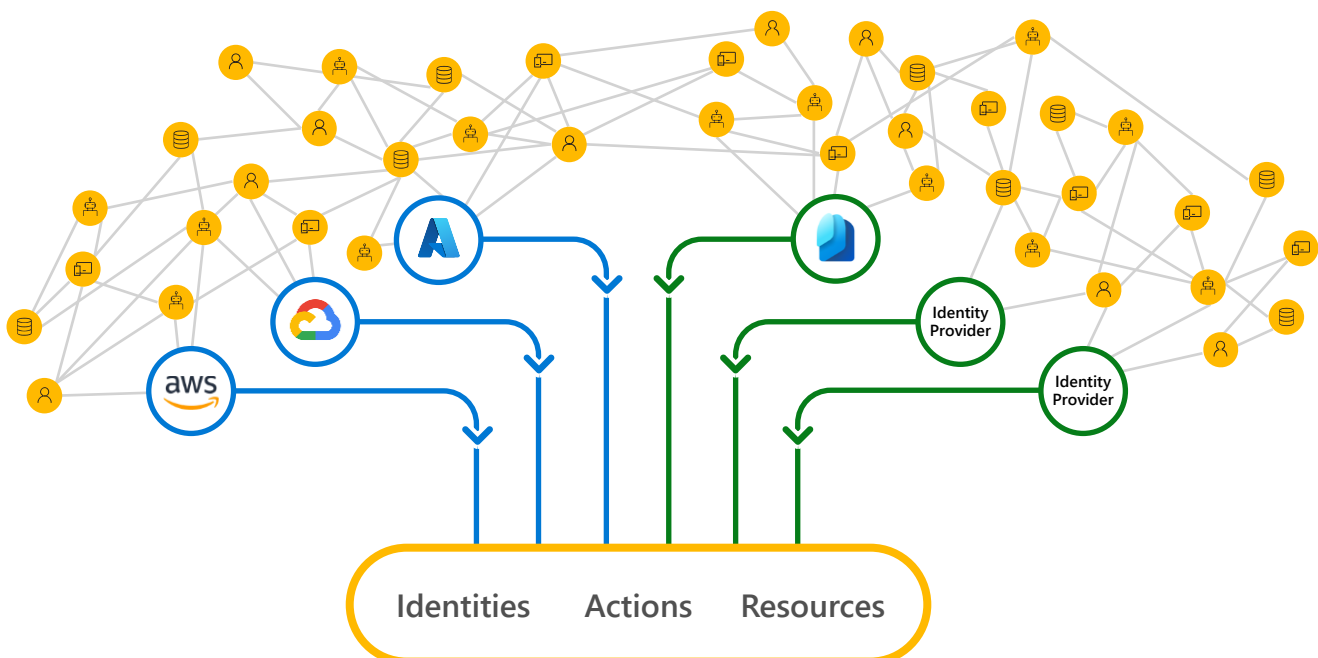
Optimizing Cloud Permissions: Path with Permissions Management

Permissions Management enables Infosys to **gain better visibility into the broader landscape of identity** within cloud environments. It assists them in implementing

role-based, fine-grained, and trackable access policies, thereby reducing the risks associated with overprovisioned identities and identity theft.



Microsoft Entra Permissions Management



Growing Permissions in Transition

Infosys' need to manage permissions arises from its growth over the past years. With expansion in teams and cloud adoption, Infosys encountered **challenges of overprovisioning at various levels**, including application and user permissions. Initially, there was **a tendency to grant more access** to accommodate the growing teams, leading to overlapping access privileges. This overlap potentially could have led to **Segregation Of Duties (SOD) violations**.

Furthermore, the transition to the cloud amid business growth has introduced new considerations, particularly regarding **identity and access over the open internet**.

As critical workloads increasingly migrate to the cloud, ensuring their auditability becomes essential.

Challenges arise when **third-party auditors inquire about permissions**, as manual verification processes prove time-consuming and prone to errors. Additionally, **the importance of protecting against security breaches** has escalated alongside the expanding adoption of cloud and the overprovisioning of growing identities.

These issues prompted Infosys to consider adopting a new solution to enhance visibility into cloud-native identities, ensuring that each group had appropriate access without unnecessary overlaps.



Optimizing Permissions for Cloud Native Identities

In addressing the challenges posed by the cloud era, Infosys identified Permissions Management as the most suitable option due to its **robust analytics capabilities and comprehensive coverage**.

It **seamlessly integrated into their existing cloud environment**, covering both user and workload identities and **offering a comprehensive view of the identity landscape**. Additionally, the deployment was swift and straightforward, with licenses activated and enhanced **analytics and visibility achieved within a single day**.

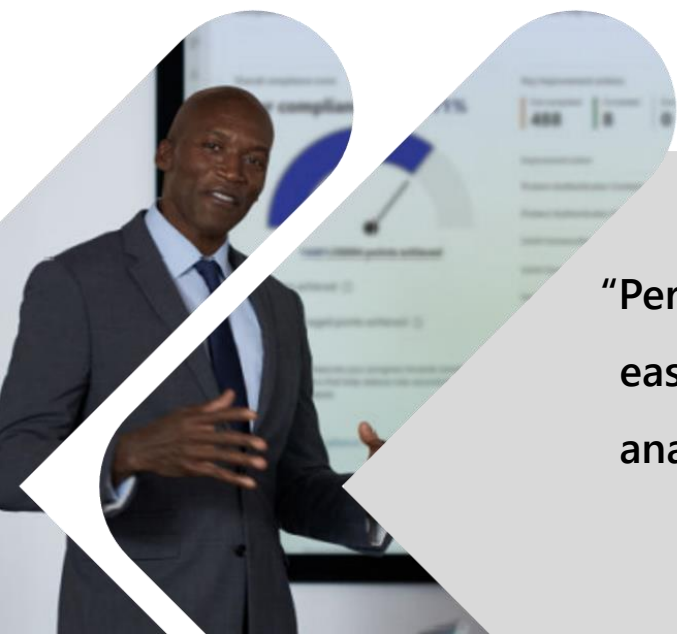
Initially, Infosys received a Permission Creep Index (PCI) score high-risk classification, which suggested that many identities had been granted high-risk permissions but were not using them, posing significant risk.



1 year PCI score change:
High risk > Low risk

However, **over the past year with Permissions Management, the PCI score decreased to a low risk level**.

This improvement demonstrated that each identity was utilizing all permissions and had minimal resource reach.



“Permissions Management was very quick and easy to implement and that it provided better analytics and visibility than other solutions.”

- Principal Solution Architect, Infosys

Enhancing Identity Security for Cloud

Permissions Management facilitated a regular review process involving key stakeholders such as cloud service owners, the cloud platform team, security engineers, and workload managers. By providing insightful analytics on the risk and impact of each cloud-native identity, Permissions Management empowered stakeholders to utilize analytics and activity logs for informed decisions on permission refinement, extension, or revocation,

thereby mitigating the blast radius.

Through this monthly permission review, **Infosys successfully reduced the total number of permissions by 57%, saving 40 hours of administrative effort per month.**

Moreover, the management of temporary external access for routine audits of cloud workloads has been fortified, ensuring both security and efficiency.

57% decrease in the number of permissions



40 hours per month saved in admin time

“Permissions Management enabled us to identify the blast radius and the effective risk of the identities and to decide which permissions need to be refined, extended, or revoked.”

- Principal Solution Architect, Infosys



About Infosys

Established in 1981, Infosys, an NYSE listed company, is a global leader in next-generation digital services and consulting. It enables clients in more than 50 countries to navigate their digital transformation with ease. With an AI-powered core that helps prioritize the execution of change, it empowers businesses with agile digital at scale to deliver unprecedented levels of performance and customer delight. In 2022, Infosys received the 'Top Employer' certification in 22 countries and is recognized as the fastest-growing IT services brand in the world by Brand Finance.

Learn more about Microsoft Entra Permissions Management

Try Permissions Management and run a free risk assessment to identify the top permission risks across your multicloud environment.

Request a 45-day trial



Learn more online



Additional resources

2023 State of Cloud Permissions Risks Report
aka.ms/CloudPermissionsReport

Solution Brief
aka.ms/PermissionsManagementSolutionBrief