

MICROSOFT ENTRA PERMISSIONS MANAGER

Discover, remediate, and monitor permission risks for any identity and any resource across your cloud infrastructure.



As organizations massively adopt a multicloud strategy, several trends are stressing the need for better visibility and tighter control for cross-cloud access management.

Number of identities on the rise

User and workload identities (identities attributed to virtual machines, web apps, containers, scripts, etc.) are increasing significantly.

Explosion of cloud workloads

Organizations are moving more and more applications and services to the cloud.

65% of IT Decision Makers worry about data breaches when thinking about excessive permissions in their environment.

Implications

- Lack of visibility across clouds
- Increased complexity to implement consistent access policies
- Increased risk of security breach

Inconsistent access management models

Each cloud follows its own access management operating model, making it challenging to implement consistent security policies.

Increasing permissions gap

The gap between permissions granted and permissions used is expanding, leaving the door open for misuse and attacks.

75% of IT Decision Makers say that real-time cross-cloud permission discovery & analytics is the most critical capability to efficiently manage permissions in laaS and PaaS.

What is Microsoft Entra Permissions Management?

Permissions Management is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility and control over all permissions for any identity and any resource across all major clouds – Microsoft Azure, AWS, Google Cloud Platform – and identity providers. It provides a unified platform where you can assess, manage, govern, and protect permissions and identities consistently.







Benefits of Permissions Management

As organizations massively adopt a multi-cloud strategy, several trends are stressing the need for better visibility and tighter control for cross-cloud access management.



Get granular cross-cloud visibility

Get a comprehensive view of every action performed by any identity on any resource.



Enforce Least Privilege

Right-size permissions based on usage and activity and enforce permissions on-demand at cloud scale.



Uncover Permission Risk

Assess permission risk by evaluating the gap between permissions granted and permissions used.

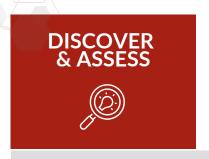


Monitor & Detect Anomalies

Detect anomalous permission usage and generate detailed forensic reports.



Permissions Management helps you strengthen your security posture by enforcing the principle of least privilege across your entire digital estate







User and workload identities.







Microsoft Entra Permissions Management allows you to:

- Get a multi-dimensional view of your risk by assess identities, permissions and resources.
- Automate least privilege policy enforcement consistently in your entire multicloud infrastructure.
- Prevent data breaches caused by misuse and malicious exploitation of permissions with anomaly and outlier detection.

Resources supported include compute resources, container clusters, serverless functions, and databases across Amazon Web Services, Microsoft Azure, and Google Cloud Platform.





