A Business Case - Leverage Entra Permissions Management to implement Least Privilege in the cloud.

With exponential increase in cloud identities and rise of related exploits, cloud environments are at increased risk of attack using a compromised identity. Here are a few key risks Entra Permissions Management helps mitigate and strengthens the overall cloud security posture.

Misconfiguration of cloud assets and excessive high-risk permissions increase risk of a security incident.

Attackers constantly look for cloud assets with default settings, insecure high privileges or lacking security controls. Research indicates that:

- An increasing percentage of enterprises unknowingly expose some applications, cloud assets, and APIs directly to unintended audience.[1]
- >80% of security incidents result due to misconfiguration.[2]
- Majority of security leaders (~60%) consider misconfiguration of the cloud platform as one of the biggest security threat.[3]

Statistically, >40% of the identities are inactive and the ones active use ~5% of their assigned permissions.[4] **Entra Permissions management** helps discover and mitigate over-provisioned / inactive users and service principals, and helps prevents compromise due to gaps in permissions management.

Mitigation of risk due to misconfiguration of permissions

Permissions right-sizing without visibility of usage is risky, and can cause business impact due to outage or delays due to insufficient access.

Permissions right-sizing without automation and visibility can be an expensive exercise. Identifying validity of permissions manually takes time and is virtually impossible to achieve at cloud scale without automation.

In addition, any unverified permissions changes can result in wasted hours and loss of business.

Entra Permissions management automates discovery of permissions continuously and at a cloud scale. For an average organisation with 1000 cloud identities, this automation can save weeks' worth of effort and eliminate any risk of business loss due to incorrectly implemented remediation.

Visibility of permissions usage for correct remediation

Traditional identity governance process only focusses on "membership validation" and leaves gaps in implementing Least Privilege.

Access reviews / certification process typically focusses on human identities only. Research indicates that cyberattacks that misuse machine identities have increased 1600% over the last five years[5]. In addition, the process limits itself to verification role or security group membership. As a result, the process does not discern overall active usage and hence the gap in permissions remains even after religiously certifying access.

Entra Permissions management provides coverage of both human and machine identities, and covers the full cycle of *cloud entitlements discovery*, *correlation of entitlements* across cloud services, and most importantly *Usage Visualisation*. It also helps detect inactive and over-permissioned machine identities, and helps minimise risk of compromise.

Identification of inactive / risky machine identities and Better access review coverage

[1] Gartner research on risk of cloud misconfiguration.
[2] Gartner POV paper on 'Is the cloud secure?'
[3] Statista Research - Biggest security threats in public clouds
[4] https://aka.ms/PermssionsManagementReport
[5] How Advanced Persistent Threats Misuse Machine Identities

Microsoft Security