Identity Protection and Governance Capabilities of Azure AD

Identity Governance In Azure AD

Azure AD identity governance allows organisations (for employees, business partners, vendors across services, applications on-prem and cloud) to:

- Govern the identity lifecycle
- Govern access lifecycle
- Secure privileged access for admin

Helps orgs answer these key questions:

- Which users should have access to which resources?
- What are those users doing with that access?
- Are there effective controls for managing access?
- Can auditors verify the controls are working?

Identity lifecycle

When planning identity lifecycle management for employees, many organisations go for the "join, move, leave" model. The identity is created when they initiallly join, they may be given more accesses as they move to a higher job role, then accesses are removed when they leave.

For many organisations, the identity lifecycle of employees is tied to the HR system - the HR system being the "source of truth". Azure AD Premium allows integration with clod based HR systems. When a new employee is added, Azure AD can create a corresponding user account.

Access lifecycle

Is the process of managing access throughout the users' organisational life. Throughout their time at the company, they'll require different levels of access as their role changes.

The access lifecycle process can be automated utilising dynamic groups. Dynamic groups enable admins to create attribute-based roles to determine membership of groups. When attributes of a user or device change, the system evaluates all group rules in a directory to see if the change triggers any useres to be added or removed.

Privileged access lifecycle

Monitoring privileged access is a key part of identity governance. When employees, vendors, and contractors are assigned administrative rights, there should be a governance process due to the potential for misuse.

Azure AD Priviliedged Identity Management (PIM) provides extra controls aimed at securing access rights - helping you minimise the number of people who have access to resources across Azure AD, Azure, and other Microsoft online services. PIM is a feature of Azure AD Premium P2.

Entitlement management and access reviews

Entitlement management is an identity governance feature that allows orgs to manage the identity and access lifecycle at scale. It automates access request workflows, access assignments, reviews, and expirations.

Pain points for managing employee access to resources can be:

- Users might not know what access they should have. Even if they do, they might not know which individuals to go to to approve it.
- When users find and get access to a resource, they might have access longer than required for business purposes
- Managing access for external users

Entitlement management includes the following to address the above:

Delegate the creation of access packages to non-admins. The packages containe resources that can be requested. Policies are then defined including rules such as which users can request access, who must approve access, and when access expires.

Managing external users. When a user who isn't in your directory requests access and is approved they are automatically invited and assigned access. When it expires, if there are no other access package assignments they are removed from your directory.

Entitlement management is a fature of Azure AD Premium P2.

Azure AD access reviews

Azure AD access reviews allow orgs to manage group memberships, access enterprise applications, and role assignment. Regular access revies ensure that only the right people have access to resources.

Access reviews can be created through Azure AD access reviews or Azure AD PIM. Reviews can be for both users and guests. When created it can be set up so that each user reviews their own access or to have one or more user review everyones access.

No access rights are changed until the review is finished - but a review can be stopped before its' scheduled end. When the review is complete it can be set to manually or automatically apply changes to remove access from a group membership (except for dynamic groups, or a group that was created on-prem).

Capabilities of Privileged Identity Management (PIM)

PIM is a service in Azure AD allowing you to manage, control, and monitor access to important resources in your org (in Azure AD, Azure, M365 and Intune as an example). A feature of Azure AD Premium P2

PIM is:

- JIT - provides privileged access only when needed - not before
- Time-bound. Start and end dates for access are assigned
- Approval-based
- Visible - notifications are sent when privileged roles are accessed
- Auditable - full access history is logged and can be downloaded

Why use PIM?

- Reduces change of malicious actor getting access by minimising total number who have access
- Time-limiting authorised users reduces risk of one of them affecting resources
- Oversight is provided to keep track of who is doing what with resources

Azure Identity Protection

Allows orgs to accomplish 3 key tasks:

- Automate detection and remediation of identity-based risks

- Investigate risks using data in the portal
- Export risk detection data to third-party utilities for further analysis