Microsoft Entra ID Governance

Central user and rights management in cloud landscapes

With Microsoft Entra ID Governance, users and access rights in different IT systems can be managed centrally and in a user-friendly way. The software supports efficient processes through extensive automation and self-service functions and ensures compliance and transparency requirements thanks to integrated reporting and monitoring.

Cloud-based access management

Microsoft Entra ID Governance is a cloud-based identity governance solution. It provides ways to control the identity lifecycle, access lifecycle, and secure privileged access for management. Features include creating workflows to automatically manage permissions, controlling app and resource access based on group memberships, and delegating access decisions to business groups, among others. Microsoft Entra ID Governance supports both on-premises and cloud-based applications and a variety of HR systems, such as SAP SuccessFactors, workday, and Microsoft Dynamics 365.

For the identity lifecycle

Access and authorization management in companies is a significant time and cost factor, as the implementation of identity and access management as well as its maintenance is usually associated with a lot of effort. In addition, in view of the advancing technical development, more and more different operating systems and applications are finding their way into companies. In addition, the number of mobile employees with the corresponding devices is growing steadily. More than ever, users are therefore dependent on being able to access their necessary data and applications in a targeted and remote manner. And always against the background of applicable safety regulations and legal requirements. However, by means of individual "isolated solutions" and manual processes, this can hardly be mastered on the part of the IT department.

For the lifecycle of accesses

With Microsoft Entra ID Governance, IT departments can determine what access rights users should have to different resources and what controls are required for enforcement, such as segregation of duties or revocation of access when changing jobs. The Microsoft Entra-ID has connectors to hundreds of cloud and on-premises applications. When a user tries to sign in to one of these applications, Microsoft enforces Entra ID Conditional Access policies. Access changes in apps and groups can be automated based on attribute changes. In addition, IT can delegate access management decisions to business decision-makers. Entitlement management allows you to control how users request access across packages of group and

team memberships, app roles, and SharePoint Online roles, and you can enforce segregation of duties checks on access requests. It also allows organizations to control which guest users have access to on-premises applications.

For the privilege lifecycle

Microsoft Entra Privileged Identity Management (PIM) provides additional controls for protecting access rights to resources in Microsoft Entra, Azure, other Microsoft Online Services, and other applications. In addition to multi-factor authentication and conditional access, Microsoft Entra PIM's just-in-time access and role change alerts capabilities provide you with comprehensive governance controls to protect your organization's resources (directory roles, Microsoft 365 roles, Azure resource roles, and group memberships). As with other forms of access, access reviews allow organizations to configure periodic recertification for all users with privileged administrator roles.

Product characteristics & features

- Coverage of all key areas of IAM in an integrated cloud solution
- Identity lifecycle management (e.g.: onboarding / reinstatement / termination / long-term sick leave / parental leave / pension and more)
- Integration with security and risk analytics of Microsoft Entra ID and the Microsoft 365 ecosystem
- Built-in support for decentralized identities
- Gateways for integration back into on-premises environments

Your benefits at a glance

- Manage access to on-premises, cloud, and hybrid resources as a public, multi-tenant cloud service
- Minimizing risk by restricting users' access to applications that are only needed
- Easy implementation of compliance requirements
- High flexibility due to the possibility of integrating non-SAP systems
- Numerous connectors for other systems
- High system compatibility, which enables expansion of existing infrastructures

"Managing access, identities, and privileges takes up too much human resources, especially in the IT department. Microsoft Entra ID Governance simplifies this challenge by centralizing administration and automating processes. This noticeably reduces the complexity of identity and access management. It also ensures that exactly the access rights that employees actually need are assigned in accordance with the rules – throughout the entire lifecycle of identities, access and privileges."

Markus Keller (Your IAM-Expert)