Microsoft

Extend the reach of Azure AD into apps and services: **An introduction to workload identities**

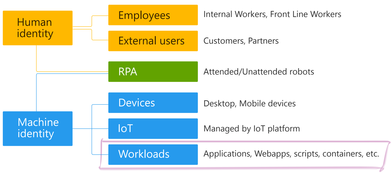
What are Workload Identities?

Just like users, a software workload needs an identity to access resources. Two common scenarios in Azure AD today for workload identities are:

- **Managed identities:** Used by developers to provision their service with access to an Azure resource such as Azure Key Vault or Azure Storage.
- **Application identities:** Enable access to resources when IT admins or developers deploy apps in their environment.

Workload identities are part of machine identities for software workloads, such as applications, services, scripts, or containers that require authentication and authorization as they access resources in cloud environments.

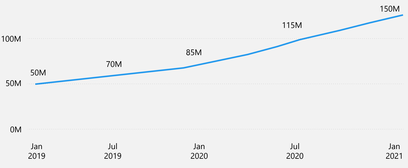
Taxonomy of identities in Azure AD



Need for securing workload identities

Identity and Access management solutions such as AM (Access Management), IGA (Identity Governance and Administration), and PAM (Privileged Access Management) tools have historically been geared toward the more imminent need for managing human identities. **Equal focus must now be paid to the management and governance of workload identities to deploy Zero Trust into your environments.**

The number of workload identities* managed by Azure AD

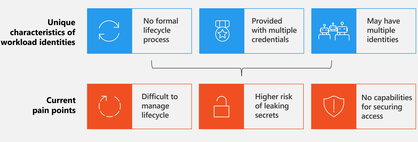


* This graph presents the number of workload identities that requested access tokens more than once. Workload identities in this graph are referred to as service principles in Azure AD.

Note: This number is not included into the Azure AD MAU that we report in earrings.

Challenges in securing workload identities

Human users typically have a single identity used to access a broad range of resources. Unlike a human user, a software workload may deal with multiple credentials to access different resources and those credentials need to be stored securely. It's also hard to track when a workload identity is created or when it should be revoked.



To date, no single solution addresses today's challenges in managing workload identities. Enterprises risk their applications or services being exploited or breached because of difficulties in securing workloads identities.

Workload identities in Azure AD resolves securing workload identity issues.

With workload identities, you strengthen deployment of Zero Trust, empowering you to protect secrets, sensitive data, and other resources via the following features:

- **Secure access with adaptive policies**
  - Conditional access for workload identities
  - Customer security attributes
- **Intelligently detect compromised identities**
  - Identity protection for workload identities
- **Simplify lifecycle management**
  - Access review for workload identities assigned to privileged roles
  - Workload identity federation
  - Managed identities for Azure resources

Workload Identities evolves continuously. More features come available often to help provide a clear view into the security of your secrets, assets, and other resources.