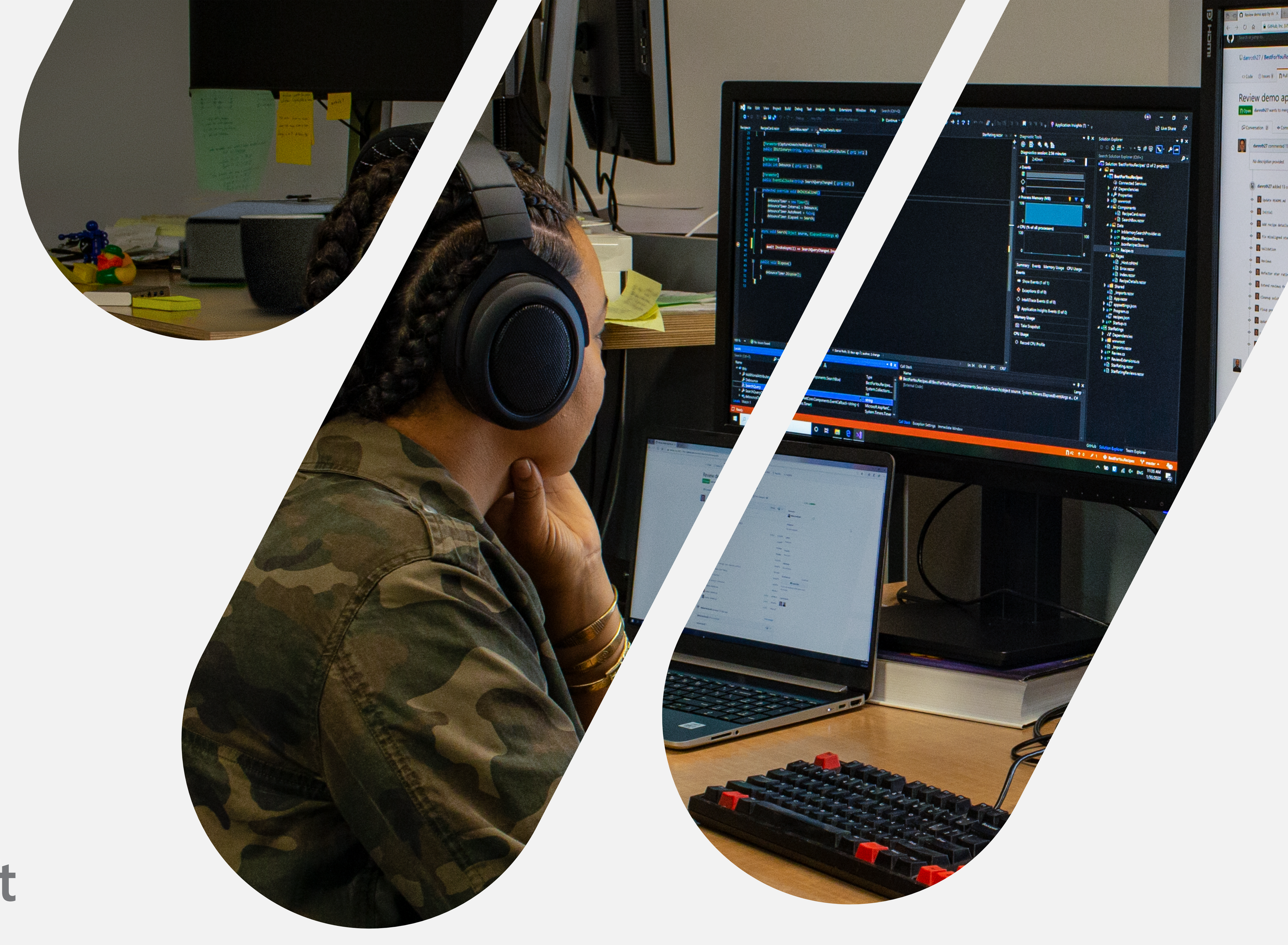


Microsoft

Introducing Microsoft Entra Workload Identities

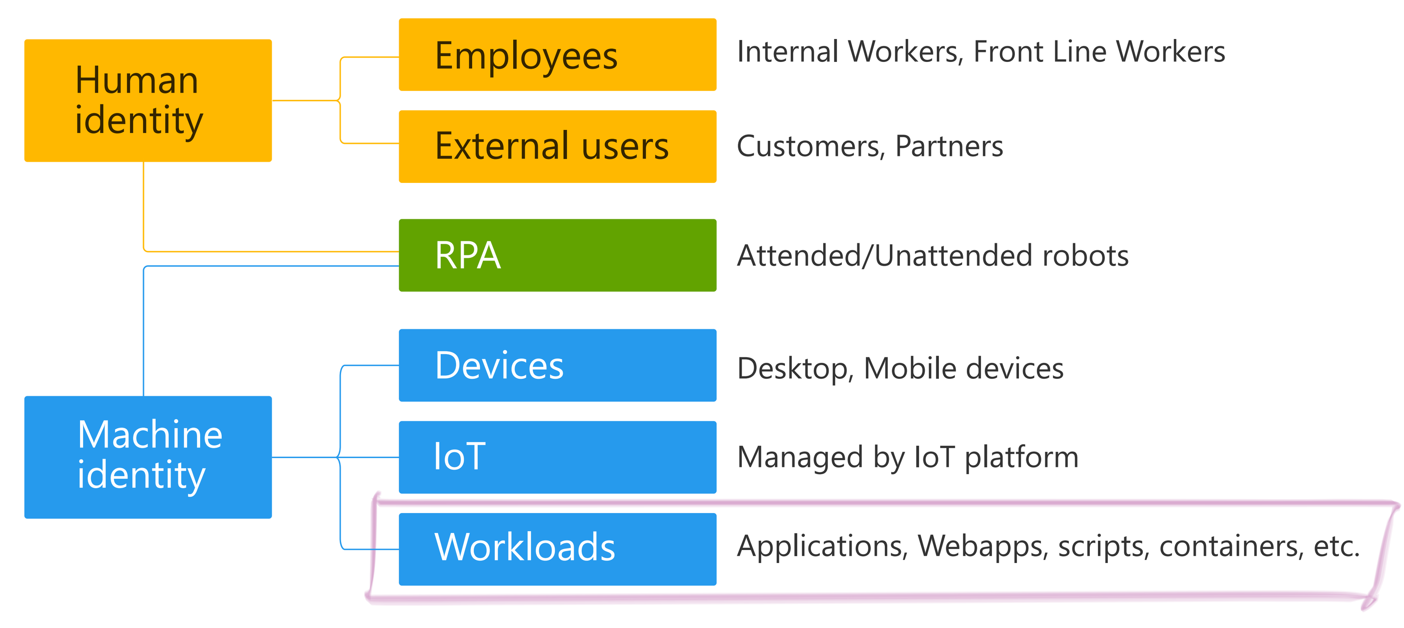
What are Workload Identities?

Just like users, a software workload needs an identity to access resources. Two common scenarios in Microsoft Entra 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.

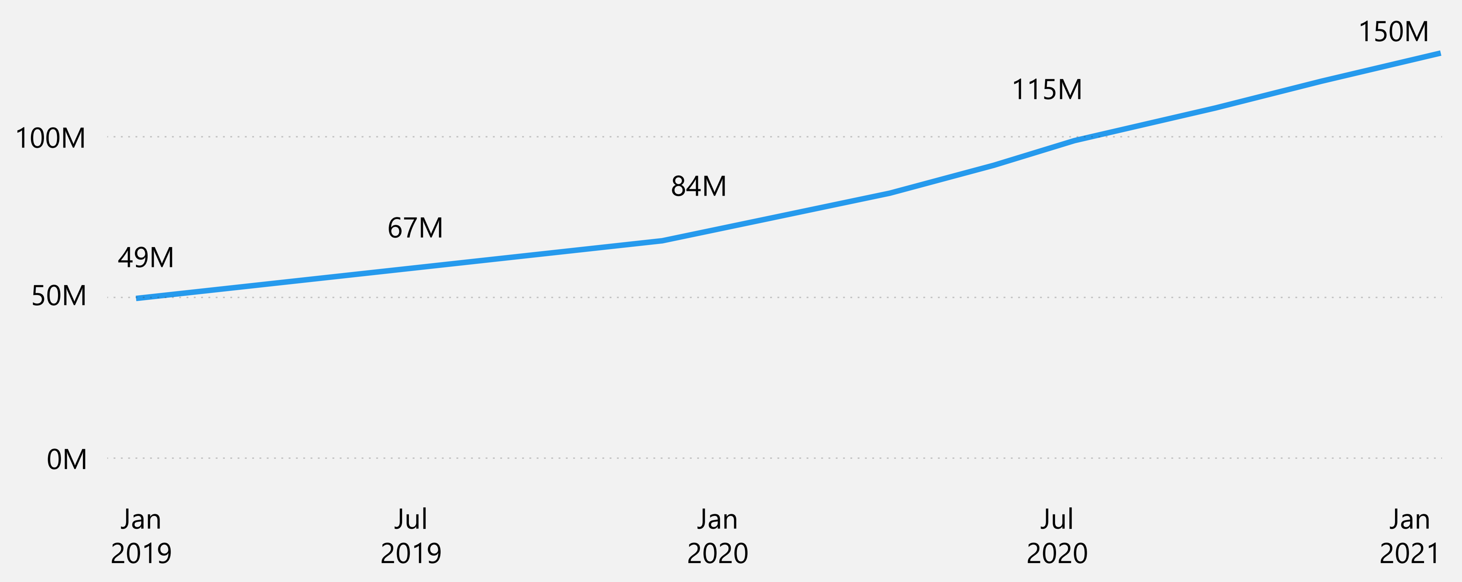
Identity types in Microsoft Entra



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.**

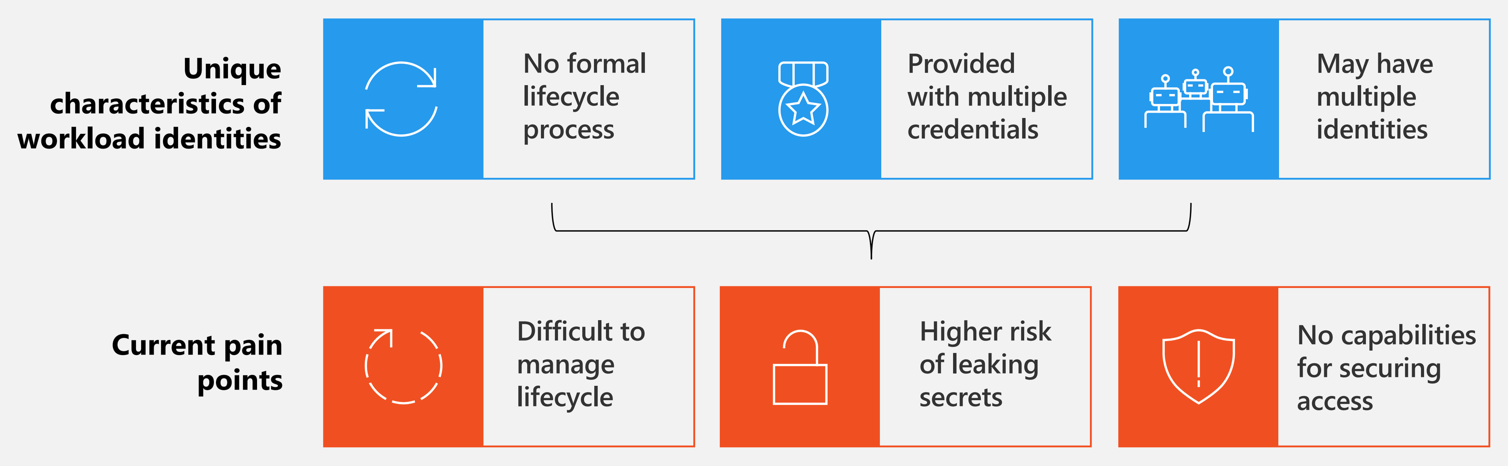
The number of workload identities* in Microsoft Entra



* The graph above shows the increase in workload identities on Microsoft Entra since January 2019. Note that Workload identities are referred to as Workload Principal Identities. The rate of Workload Principal Identities to be secured is only increasing.

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 needs 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.

Microsoft Entra Workload Identities helps resolve issues when securing workload identities

With Entra Workload Identities, you strengthen deployment of Zero Trust, empowering you to protect secrets, sensitive data, and other resources via the

- **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.