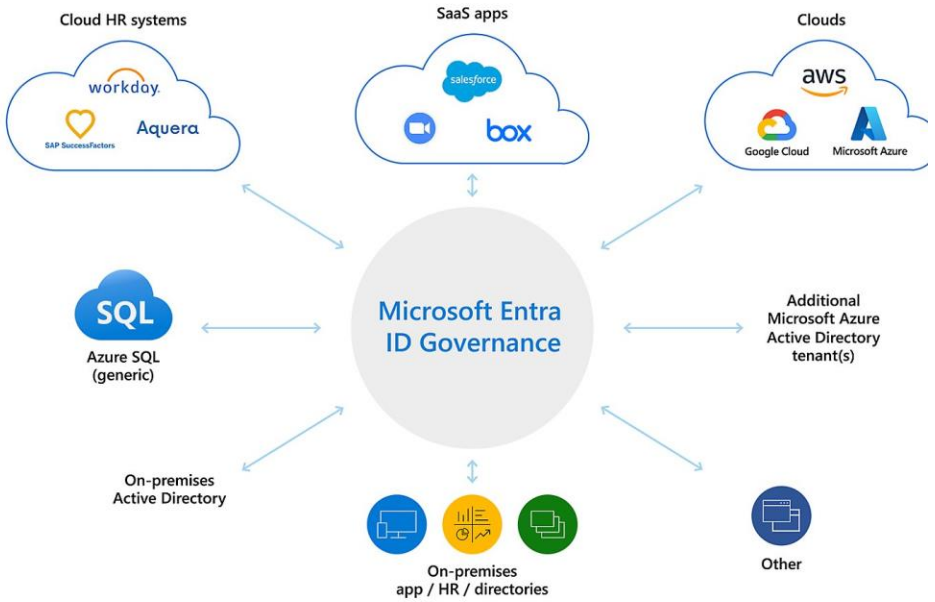
Microsoft Entra ID Governance Case Study



Problem

Organization needed a solution to securely manage identities of customers that was scalable, robust, and leveraged solutions that the organization was already familiar with to keep it simple to manage.

Solution

Spyglass worked with the organization to implement a net new Entra ID tenant that allowed for customer identities to be separate from the Organizational identities. To allow for easier management, the organization identities that needed access leveraged Cross Tenant Access so that they could use their own identities. Azure MFA and Authentication Methods were used in conjunction with Conditional Access policies to make sure users and administrators were properly sanctioned to connect to the service. Identity Protection, Privileged Identity Management, Access Packages, and dynamics groups were also used to help make sure permissions were handled appropriately and the identities were easy to manage.

Benefits

Once the implementation was completed and customers were leveraging the solution, the new solution allowed for more flexible permissioning options to allow distinct customers to vary the levels of MFA methods they could use, while being able to connect using their own identity providers. The Conditional Access policies helped protect the environment while dynamic groups and PIM allowed for the solution to abide by the Principle of Least Privileged.