ensurity
A Step Ahead!

Use Case - Contact Center - MNC

Implementation of **FIDO2 Authentication** for a contact center of a Global MNC

CUSTOMER : A Multi billion dollar health care MNC's having multiple offices and support centers across the globe

DATE OF IMPLEMENTATION : March 2020

ENVIRONMENT : Their development centers, spread across several geo-locations uses Microsoft cloud environment for its operations; and has deployed multiple Microsoft Windows systems that are connected to several local Domain Controllers that are joined to multiple Azure AD.

PROBLEM STATEMENT : Customer articulated the following as critical requirements

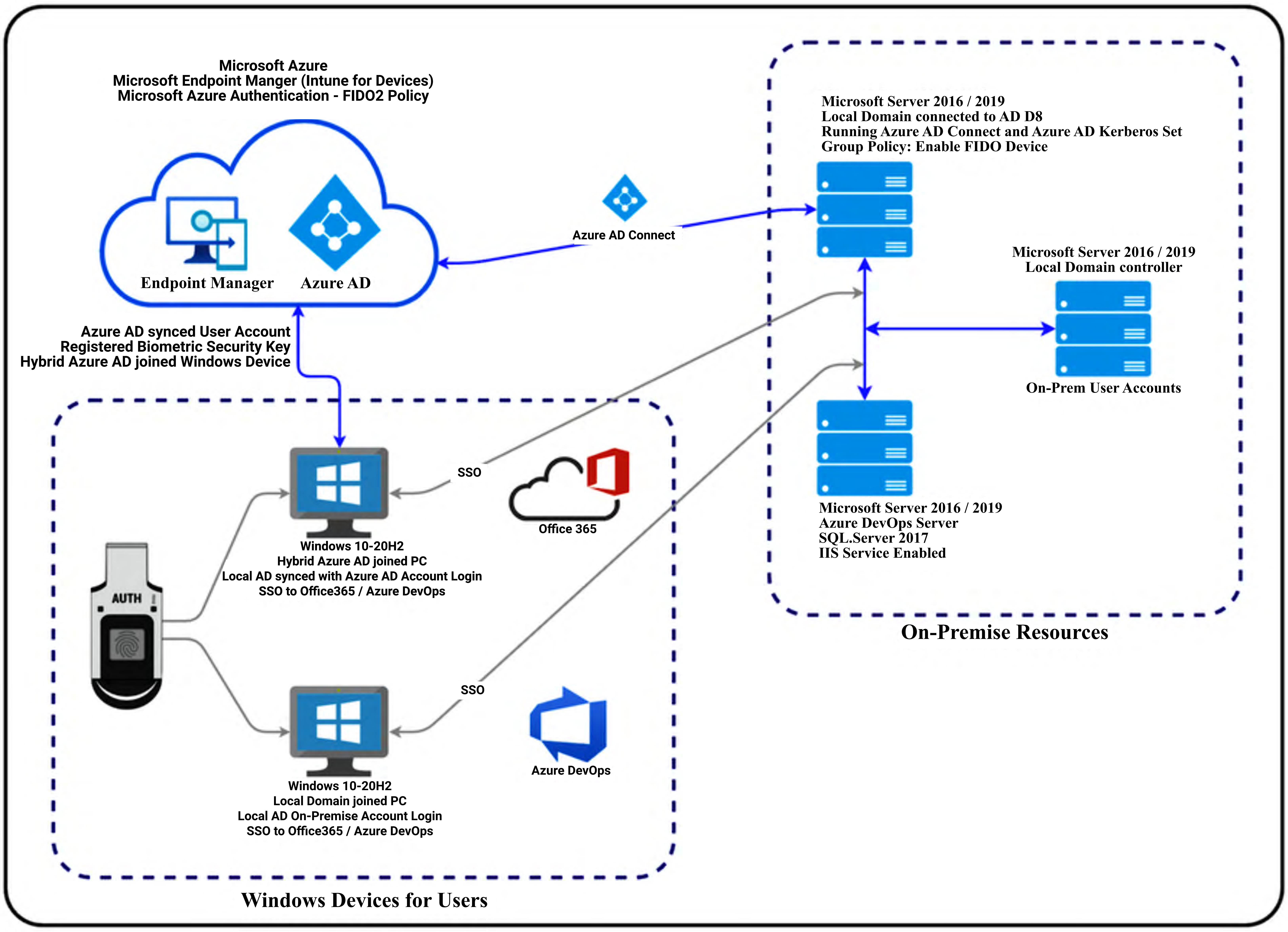
- Enable passwordless authentication to their Microsoft DevOps applications and ensure all their teams worldwide to integrate secure authentication through FIDO2 biometric security keys.
- Replace soft authenticators with biometric security keys and restrict employees from sharing their password and other authenticators.
- Enable employees to use any of the Hybrid joined PC's to login and access assigned enterprise applications

Solution Offered :

Ensurity helped customer to do a quick POC addressing their needs and subsequently rolled out its solution:

- Supplied Ensurity's FIDO2 certified “ThinC-AUTH” Biometric Security Keys and supported their Admins in configuring the security keys with user fingerprint registrations with PIN fall back option.
- Supported them in configuring their Windows 10 devices to support FIDO2 authentication
- Demonstrated and supported them in managing their Windows 10 devices through Microsoft Intune.
- Worked with them to configure the Hybrid Environment with the below architecture

Hybrid AD Connectivity



Microsoft Azure
Microsoft Endpoint Manger (Intune for Devices)
Microsoft Azure Authentication - FIDO2 Policy
Endpoint Manager
Azure AD
Azure AD Connect
Microsoft Server 2016 / 2019
Local Domain connected to AD D8
Running Azure AD Connect and Azure AD Kerberos Set
Group Policy: Enable FIDO Device
Microsoft Server 2016 / 2019
Local Domain controller
On-Prem User Accounts
Azure AD synced User Account
Registered Biometric Security Key
Hybrid Azure AD joined Windows Device
SSO
Office 365
AUTH
Windows 10-20H2
Hybrid Azure AD joined PC
Local AD synced with Azure AD Account Login
SSO to Office365 / Azure DevOps
Microsoft Server 2016 / 2019
Azure DevOps Server
SQL.Server 2017
IIS Service Enabled
On-Premise Resources
SSO
Azure DevOps
Windows 10-20H2
Local Domain joined PC
Local AD On-Premise Account Login
SSO to Office365 / Azure DevOps
Windows Devices for Users

The MNC company was able to secure their systems and eliminate risks of credential sharing and attribute users access to systems.