



Identity

- Created through HR Automated application
- On-premise AD Account created and synced to Azure AD via Azure AD Connect


Licensing

- Microsoft 365 E3
- Azure AD P2

Applications used


- Microsoft 365
- SharePoint Online
- HR Application
- Dropbox

Azure AD Signals



- User Risk
- Sign in risk
- Applications
- Operating system (mobile and Windows)
- Device Compliance
- "Trusted" networks
- Multi-Factor authentication

Azure AD Controls



- Compliant device (personal and corporate)
- Hybrid Azure AD Joined
- App protection policies
- Approved app
- Multi-factor Authentication
- Terms of Use
- Limited web access (SharePoint and OneDrive)

Current Needs

- Ability to access organisation applications securely
- Use personal devices to access corporate data and applications securely
- Use Microsoft 365 on all corporate and personal devices
- Classify, protect, and label sensitive data

Corporate Devices Used

Windows 10 laptop

- Intune enrolled
- Managed by GPOs/SCCM
- Hybrid Azure AD Joined

Corporate Android mobile phone

- Managed and compliant by Intune
- Approved applications for Microsoft 365
- App Protection policies

Personal devices used

Windows device

- Azure AD Registered
- App protection policies
- Read only, web access to SharePoint and OneDrive

Personal iPhone/Android device

- Intune Enrolled
- Device compliant with Intune
- App Protection policies
- Approved applications

Limitations and Constraints

- No leaked credentials detection because PHS is not enabled
- User/sign-in risk policies are not enabled yet
- Limited number of AD P2 licenses