FSi Strategies

Microsoft Partner
Microsoft

Gold Cloud Productivity
Gold Cloud Platform
Gold Collaboration and Content
Gold Security
Gold Communications

Azure Multi-Factor Implementation

A proactive security posture and utilizing Microsoft 365 services is critical and requires the right partner that can proactively fortify your organization's security against internal and external threats while giving users a streamlined experience. If you only use a password to authenticate a user, it leaves an insecure vector for attack. When you require a second form of authentication, security is increased because this additional factor isn't something that's easy for an attacker to obtain or duplicate. Azure AD Multi-Factor Authentication works by requiring two or more of the following authentication methods:

- Something you know, typically a password.
- Something you have, such as a trusted device that's not easily duplicated, like a phone or hardware key.
- Something you are - biometrics like a fingerprint or face scan.

At the end of this engagement FSi Strategies will implement Azure Multi-Factor Authentication (Azure MFA) with conditional access.

Day 1

- Work with client to determine policies
    - Determine licensing requirements
    - Determine what to exclude (location, specific users, service accounts, specific applications)
    - Determine what to include (user groups)
    - Additional policies
    - Rollout timeframe and groups
    - Schedule user training

Day 2

- Purchase and assign licenses if necessary
- Build Policy based on customer requirement
    - Create security groups as needed
    - Create new policies in Conditional Access
    - Label policies as needed
    - Select Assignment - MFA groups Include MFA users Exclude predetermined accounts/groups/apps
    - Add additional conditions (if applicable)
    - Configure device platform: include any device
    - Configure locations (if applicable)
    - Configure client app settings
    - Configure device filtering (if applicable)
    - Grant access and require MFA (if applicable)
    - Set policy to "Report-Only"

Day 3

- Conduct user training
- Determine rollout policy and if changes are needed based on reporting
- Set enforcement date based on user training and reporting

Day 4

- Enforce MFA
    - Change policy from Report-Only to On.