Plan Conditional Access Policies

At the end of this episode, I will be able to:

1. Plan Conditional Access Policies

Learner Objective: *Plan conditional access in Microsoft 365 environments*

Description: In this episode, you will learn about Conditional Access - a very powerful feature available in Azure AD. While this episode focuses on CA in general, specific information is given for how this feature can strengthen your Microsoft 365 security posture.

- The goal is to ensure only secure users and devices access the corporate resources.
- At their simplest - conditional access are if-then statements; if a user wants access to a resource, then that user must match certain conditions, or must perform a specific action.
- CA policies are enforced after the first-factor authentication takes place. Note that they are not intended to be a first line of defense.
- Signals for CA come from:
    - User or group membership
    - IP Location information
    - Devices
    - Applications
    - Real-time calculated risk detection (for example, Azure Identity Protection)
    - Microsoft Defender for Cloud Apps
- Actions that result from CA include:
    - Block Access
    - Grant Access
    - Grant Access - but then require something (for example, Terms of Use or Password Change)
- There is a Conditional Access Administrator role in Azure AD for admins in charge of CA
- Licensing requirements exist - you must have Azure AD Premium P1 or Azure AD Premium P2 licensing
- If a license expires - the CA policy is not removed - it just cannot be edited any longer
- Recommendations:
    - Apple CA policies to every app
    - Minimize the number of CA policies
    - Configure report-only mode
    - Plan for disruption
    - Set naming standards for policies
    - Block countries/regions from which you never expect sign in

---

Additional Resources:

What is Conditional Access
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview?WT.mc_id=Portal-Microsoft_AAD_ConditionalAccess