Securing Office 365 with Conditional Access

Nathan O’Bryan

MVP: Office Apps and Services
MCSM: Messaging

@MCSMLab
https://www.mcsmlab.com

Security in the Cloud Era

- Shared responsibility model
- Microsoft is responsible for the infrastructure, you are responsible for your data
- Incredible pace of change
- Ports and IP Addresses model
- Microsoft has put a lot of work into security features, we have to understand and properly implement those features
- Security is a constantly evolving requirement – we are never done!

Microsoft security

- Physical security
  - Internal datacenter networks are segregated
  - Customer data is unintelligible to those with physical access
- Logical security
  - Lockbox
  - Servers run only whitelisted code
- Data security

Microsoft security

- User controls
  - Encryption
  - Data loss prevention
  - Azure Rights Management
- Admin controls
  - MFA
  - MDM/MAM
  - Exchange Online Protection
  - Cloud App Security

Microsoft security

- User controls
  - Encryption
  - Data loss prevention
  - Azure Rights Management
- Admin controls
  - MFA
  - MDM/MAM
  - Exchange Online Protection
  - Cloud App Security

Your security

- Patch!
- Understand your options
  - 1st party and 3rd party options
- Balance add-on services with cost
  - EM+S features are complex and expensive
- Auditing is your responsiblity

What is Conditional Access?

- An Azure Active Directory feature that allows administrators to implement automated controls for accessing cloud apps based on defined conditions
- Cloud apps
- Automated controls
- Defined conditions
- 5 Demos in this session

AD FS Claims rules

- Before conditional access, there was claims rules
- Claims are statements made about users that are used for authorizing users to claims based applications
- The claim can be about user name, identity or group. Each claim corresponds to a value stored in that claim
- Setting up and managing claims rules can be a lot of work
- AD FS 2019 Pluggable Risk Assessment Module (RAM)

Where does CA fit into EM+S deployment?

- Conditional Access works with other EM+S services
- Intune
  - Device compliance can change auth rules
- Azure AD Identity Protection
  - User risk can change auth rules
- Cloud app security
  - App being used can change auth rules

Intune app protection

- Formerly Microsoft Managed Application Management (MAM)
- Assigns specific conditions that must be met for access to applications
- No device enrollment is required
- Applies control over data in specific apps without managing the entire device

Cloud App Security

- Takes Conditional Access to the next level
- EM+S E5 license
- Great view into what is happening with your cloud applications

Which applications work with Conditional Access?

- First party Microsoft Office 365 apps
- Third party apps
- Azure AD Enterprise applications
- Anything that you authenticate to though Azure AD

Testing CA policies

- What if tool
  - You enter conditions for auth, it tells you what policies apply
  - Doesn't necessarily tell you “what user experience will be”
- Always use test accounts to verify authentication
  - First understand what policies you expect to be applied
  - Then understand what the user sees
- Troubleshooting unexpected behavior with CA policies can be difficult

Demo 1: Conditional Access Admin Portal

- Intro to the CA admin portal in Azure

Demo 2: Blocking Access from untrusted locations

- Users that should only be accessing Office 365 aps from work
- Often used for hourly workers

Demo 3: Requiring device enrollment for mobile application access

- Users must enroll devices before accessing Office 365 applications (email and documents)

Demo 4: Requiring multi-factor authentication for applications

- Users must use MFA to access Office 365 applications

Demo 5: Conditional Access for risky sign-ins

- Configure Conditional Access to work with Azure Identity Protection
- Force risky sign-ins to use MFA

Thank you

- Questions?
- @MCSMLab
- https://www.mcsmlab.com