Azure Active Directory & Microsoft Endpoint Manager

Ensure that your environment is safe and secure!

With the recent expansion of remote-work capabilities for many companies, securing access to your environment is more important than ever. Whether your environment is housed entirely in the cloud, on-premises, or a hybrid of both, protecting it is a must. All it takes is for one bad actor to get access to an unprotected endpoint device — such as a phone or laptop — to cause untold damage.

In order to combat these dangers, RSM recommends implementing some of the best Microsoft-based security plans for protecting any business: Azure Active Directory (Azure AD) and Microsoft Endpoint Manager (MEM). These plans serve to deliver the modern workplace and modern management to keep your data secure both in the cloud and on-premises.

What are Azure Active Directory & Microsoft Endpoint Manager?

Azure AD and Microsoft Endpoint Manager are like inter-locking layers of shielding for your environment. While either plan is usable on its own, they serve best when implemented together.

Specifically, Azure AD protects access to resources and data using strong authentication and adaptive access policies without over-complicating the user experience. Microsoft Endpoint Manager includes the services and tools used for managing and monitoring mobile devices, desktop computers, virtual machines, embedded devices, and servers. When used together, you can rest assured that your environment is being kept safe in a veritable fort of cybersecurity.

More about Azure AD:

- There are four distinct licenses for Azure AD: Free, Office 365 Apps, Premium P1, and Premium P2, with each one providing increasing levels of security. RSM highly recommends the Premium P1 license, as this provides the fundamental components of environment security.
- Azure AD acts as the centralized hub in charge of environment security. With this identity control plane, you will have full visibility and control of your environment.
- It includes single sign-on, conditional access, self-service password reset, and multi-factor authentication, which all work together to allow you to easily, safely, and securely access your apps & data from anywhere.
- Additionally, this governance ensures the right people have access to the right resources, and only when they need it.
- For more information, please visit: Azure Active Directory

More about Microsoft Endpoint Manager:

- It includes the following services: Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot. Together, these form a unified platform critical to helping protect and manage your organization's devices and apps.
- These services integrate well with Azure AD for maximized security for both your on– and off-premises devices.
- For more information, please visit: Microsoft Endpoint Manager

What does Azure AD include?

- One of the most prominent security features is multifactor authentication (MFA), which adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone.
- Related to MFA, Azure AD also features Conditional Access policies which strengthen your security. This means that you can set when an MFA prompt will appear for a user, such as when they want to access a resource (e.g., accessing payroll).
- It also includes application federation and provisioning. This means that even third-party applications used by the company can be integrated into Azure AD to be properly secured.
- An Azure AD Premium P1 license also allows you to block legacy authentication (older methods of access that subvert MFA) such as Exchange Web Services. Where MFA locks your environment's front door, blocking legacy authentication locks the backdoor.
- And more!

What does Microsoft Endpoint Manager (MEM) include?

- MEM includes Microsoft Intune, which is a 100% cloud-based mobile device management (MDM) and mobile application management (MAM) provider for your apps and devices. Essentially, this allows you to apply security measures to all devices that can connect to your environment. Intune also integrates with Azure AD for seamless implementation.
- It also includes Configuration Manager, which is an on-premises management tool for desktops, servers, and laptops that are on your network or internet-based. You can use Configuration Manager to deploy apps, software updates, and operating systems. You can also monitor compliance, query, and act on clients in real time.
- And more!

Overall, both Azure AD and Microsoft Endpoint Manager are great tools that will help you organize and secure your business' online environment. Device and application management, secure endpoint access, and more all work together in order to provide the best security possible for your environment. For any business operating in the modern age, Azure AD and Microsoft Endpoint Manager are a necessity for your cyber protection.

Contact us!

Jonathan Blaue
Manager
Modern Work | Microsoft 365 Solution Architect

RSM US LLP
30 South Wacker, Ste 3300, Chicago, IL 60606
C: 312.860.3787 I **E:** jonathan.blaue@rsmus.com I **W:** www.rsmus.com