Maximize enterprise user protection – Minimize Attack Surface – Increase user experience

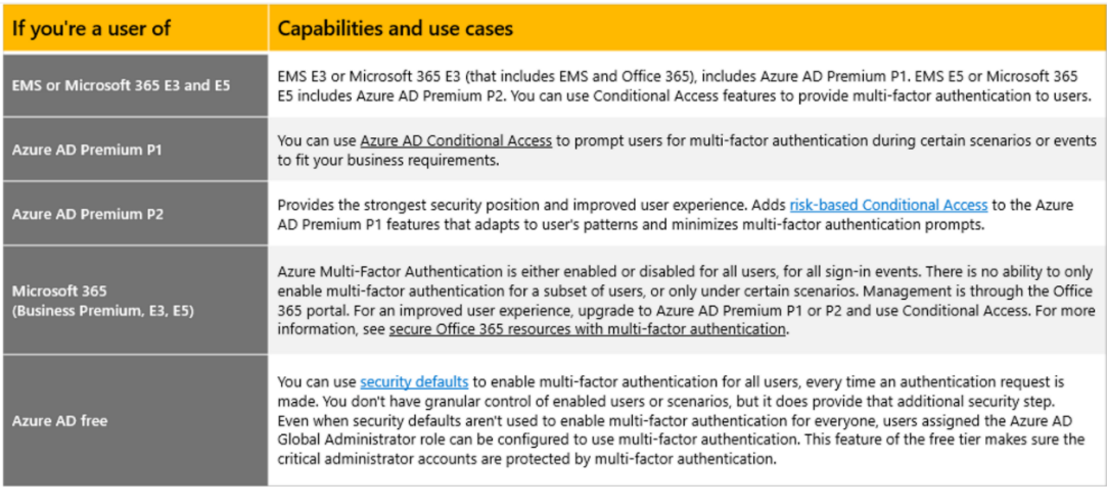
Your company's people, their mailbox and endpoint are at the main target of the raising number of modern cyber-attacks. Security breaches are common to begin from a single compromised account. How protected is your company's infrastructure against incidents to illegally obtain user credentials?

Azure Active Directory Premium (AADP) enables you to identify identity risks in real time, gain insight from the applications you use, and overall help you improve your organization's identity security level (Azure Identity Secure Score).
Byte Computer can help you gain full visibility and control of your environment. Ensure that the right users have access to the right resources whenever necessary and maintain sensitive information protected.

AADP is a secure, simple to utilize, unified service for identity and access management. Byte Computer offer managed services to implement, control and report over your business users, devices, applications, and data protection by enabling:

- Strong Multi-Factor Authentication (MFA) for User Identity verification
- Conditional Access and control policies to maintain the security of your company's resources, both in the Cloud and On-premises world.
- Automated admin notification with prompt and periodical reports (response) regarding potential risks from account breaches or unauthorized access attacks
- Rich insights for alerts and suspicious user behavior
- Additional security level managing user identities with Microsoft's integrated Zero Trust model.

Check the table below for Azure AD features availability.



If you're a user of	Capabilities and use cases
EMS or Microsoft 365 E3 and E5	EMS E3 or Microsoft 365 E3 (that includes EMS and Office 365), includes Azure AD Premium P1. EMS E5 or Microsoft 365 E5 includes Azure AD Premium P2. You can use Conditional Access features to provide multi-factor authentication to users.
Azure AD Premium P1	You can use Azure AD Conditional Access to prompt users for multi-factor authentication during certain scenarios or events to fit your business requirements.
Azure AD Premium P2	Provides the strongest security position and improved user experience. Adds risk-based Conditional Access to the Azure AD Premium P1 features that adapts to user's patterns and minimizes multi-factor authentication prompts.
Microsoft 365 (Business Premium, E3, E5)	Azure Multi-Factor Authentication is either enabled or disabled for all users, for all sign-in events. There is no ability to only enable multi-factor authentication for a subset of users, or only under certain scenarios. Management is through the Office 365 portal. For an improved user experience, upgrade to Azure AD Premium P1 or P2 and use Conditional Access. For more information, see secure Office 365 resources with multi-factor authentication.
Azure AD free	You can use security defaults to enable multi-factor authentication for all users, every time an authentication request is made. You don't have granular control of enabled users or scenarios, but it does provide that additional security step. Even when security defaults aren't used to enable multi-factor authentication for everyone, users assigned the Azure AD Global Administrator role can be configured to use multi-factor authentication. This feature of the free tier makes sure the critical administrator accounts are protected by multi-factor authentication.

To safeguard your user valuable information and to reduce possible risks of identity theft, it is recommended to deploy AADP for your user accounts.

Identity and Access Managed Services (AADP):

- Activation and configuration of Multi-factor Authentication for user entry with simple and strong data authentication (via app or call to mobile)
- Enforce conditional access policies for accessing Online and On-premise applications. Organizational role-based access control to cloud resources (RBAC)
- Configuration Active Directory, Azure Active Directory and hybrid solution for Office 365 users
- Leverage the Security Score analysis and implement proposals to increase protection

The AADP service can be combined with Microsoft Intune to develop the MFA access control tool and gain:

- Remote provisioning of corporate Windows mobile devices with Zero-touch provision e.g. Windows 10/11 via Intune
- Register, configure and centrally manage your resources on corporate, BYOD or shared devices.
- Preparation of a central console for device and application management policies to protect end user information (Microsoft Endpoint Manager).
- Audit and evaluate compliance stature Insights of compliance (compliance) for security policies.

Byte

solutions.unlimited