Azure Ad: What are the benefits and why should I use a purchased subscription?
By Marios Tsimaris – Junior System Consultant

What is Active Directory?

Active Directory (AD) helps businesses manage users, groups, and objects within their networks. So, you can assign users to groups, and assign each of those groups access to specific network resources, apps, and devices. This ability to control access at a variety of levels gives businesses the freedom to distribute resources to specific subgroups, which is critical for both resource management as well as compliance and regulation.

Understanding Azure Active Directory

Azure Active Directory (or Azure AD) enables you to manage identity (users, groups, etc.) and control access to apps, devices, and data via the cloud. That means that both identity and access are managed entirely from the cloud, and all your cloud apps and services will utilize Azure AD. It's important to note that Azure AD is immediately valuable for Microsoft apps, but it can be used to power the identity and access controls of your entire organization.

Different Azure Active Directory Plans

Let's look at some of Azure Active Directory licensing options. Before we begin, it's important to note that every Azure and Office 365 subscription, by default comes with Azure AD free edition. Based on the feature requirement, this can be upgraded to an edition which suits unique business needs.

1. Free Edition: The free edition of Azure AD offers the ability to manage users and groups, synchronize with the on-premise environment, use single sign-on to Microsoft products and includes all other popular SaaS applications.
2. Office 365 Edition: This edition provides cloud-centric application access and self-service identity management solutions designed for the cloud-first needs of task workers. With the office 365 edition of Azure Active Directory you can enhance productivity and reduce cost with features such as group-based access control, password self-reset for cloud applications, and Azure AD Application proxy to publish on-premises web applications using the Azure Active Directory.
3. Premium P1: Premium P1 edition of Azure Active Directory offers features to organizations that require access and identity management. Premium P1 has richer enterprise-level identity management capabilities and gives hybrid users access to all on-premises and cloud capabilities. The Premium P1 edition includes all the tools needed for information workers and identity administrators in hybrid environments for application access, identity protection, identity security, and access management. P1 supports advanced resources for administrations for delegation of dynamic groups and self-service group management.

4. <u>Premium P2:</u> This edition of Azure Active Directory offers advanced protection for both users and administrators. Premium P2 by default has all the features of P1 along with new and superior identity protection and privileged identity management.

Free vs. Office 365 Edition (E1, E3, E5, F3)

Typically, both of these Azure AD environments will be part of your existing license. So, if you only have an Azure license, you'll use the free version. Also, if you only have an Office 365 license, you'll use the Office 365 version. The Office 365 version has two advantages over the free version, multi-factor authentication and unlimited directory objects.

Of course, having more than one layer of authentication is critical in today's business environment, so these are not a small feature by any means. Unlimited Objects becomes a necessity for most businesses at a certain point, especially if you have over 20 employees OR you're using lots of cloud apps. Typically, you won't be selecting between these two. You'll either have an Office 365 license or you won't.

Premium Plan 1 vs Premium Plan 2

The Azure AD Plan 1 edition includes the following features:

- Multi-Factor Authentication into more than just Office 365, i.e. VPN or other cloud apps.
- Advanced Security and Usage Reports – be more aware in this threat riddled world
- Self-service password reset
- Advanced Group Access Management
- Conditional Access based on group, location, and device status – this helps users from becoming overwhelmed by prompts for MFA. It can use certain conditions as the second factor, like when a user utilizes a domain-joined PC to access that network or a mobile device enrolled in Intune.

Azure AD Plan 2 edition includes, on top of all the features of Plan 1:

- Identity Protection & Identity Governance
- This allows the detection of vulnerabilities and risky accounts, investigation of risk events
- Conditional Access policies that are risk-based, i.e. extra protections for someone coming in from a Tor browser, a questionable IP address, or a new login location.
- Privileged Identity Management – the ability to better control administrator access. Including the ability to set up temporary privileged accounts for contractors or help desk personnel working a weekend shift.

Everyone should be taking advantage of at least the free version of Multi-Factor Authentication! This is a great benefit to organizations and should be implemented today if it hasn't already been. We recommend taking advantage of one of the two different paid Azure Active Directory Plans to go with the free MFA that provide a better security experience.

Microsoft Service Level Agreement (SLA): Azure Active Directory Premium editions guarantee a 99.9% monthly availability. Free services, such as Azure Active Directory Free, don't have an SLA.

Marios Tsimaris is our Systems Consultant and he is working for IBSCY for the last 2 years. He is a member of our IT department which consists of 5 people and it is responsible for the day-to-day support and maintenance of our clients. His team is also fully responsible for the implementations of new and existing clients in Cyprus and internationally. He holds several certifications from Microsoft, Fortinet, VMWare and other vendors.