**Office 365 Security Features**

This document aims to give an overview of Office 365 security features that can be implemented to protect the organization.

**Multi-Factor Authentication**

Office 365 has 2 forms of multi-factor authentication that can implemented.

1. There is the basic built-in option which will work for many companies and it’s free. It’s easily configured with many options as to which form of authentiction you’d like (pin code, smart card, RSA token, etc)
2. There is Azure-multi-factor authentication is available for companies that require more control or need to meet some sort of compliance. This is an add on feature so there is an additional fee.

**Mobile Device Management**

Office 365 has 2 security features for BYOD management that would be suitable depending on your corporate BYOD policy.

1. There is a built-in Office 365 MDM that is suitable for companies where employees will only be accessing emails on a company issued phone.
2. There is Microsoft Intune for companies that allow employees that use their own phones, or are accessing more than just email, or if you just need more granular control over the devices. This is an add-on so there is an additional fee

**Advanced Threat Protection**

ATP is an add-on so there is an additional charge. Features include the following

1. SPF - User Sender Policy Framework . verifies which servers are authorized to send your email
2. DKIM - Domain Keys Identified Mail ensures trust between email servers best to use with SPF
3. DMARC - Domain-based Message Authentication, Reporting & Conformance dmarc.txt identifies your outbound email servers as authorized in DNS
4. ATP Policies - Anti-Phishing, Anti-Spam, safe links, safe attachments. These policies scan exchange online for these threats.
5. Threat intelligence - provides analytics from windows endpoints and tools like the threat simulator, etc.
6. ATP policies for Sharepolint, One Drive, and Teams

**Encrypted Email and Data Loss Prevention**

Data Loss Prevention ensures sensitive information doesn’t get sent outside your organization to begin with.

1. DLP policies monitors your environment for sensitive data and and prevents users from sending that information outside your organization. This applies email, sharepoint, one drive, and office apps). There are pre-set templates available for most regulatory and compliance needs.

**Azure Identity Protection**

Azure Identity Protection uses AI or Machine Learning to to understand how you work and flag unusual activity. If suspicious activity is detected (like logging into 2 different locations at the same time thousands of miles away from each other), there are steps you can take to keep the hacker out or force the user to perform a multifactor authentication

**Privileged Identity Management**

This feature is essentially PAM for Office 365 where you can use JIT (Just in Time) and JEA (Just Enough Administration) administration to give users just enough privilege for a set amount of time.