synergi

Securing your Office 365 / Microsoft 365 Environment

Whitepaper

Unit 2, Staithes, The Watermark, Gateshead. NE11 9SN

www.teamsynergi.co.uk

TABLE OF CONTENTS

DOCUMENT CONTROL

Authors:	Paul Burns, Chief Technology Officer Martin Nichols, Senior Support Consultant
Version:	1.0
Date:	06/04/2020

INTRODUCTION

Free Synergi whitepaper & support to help customers

The recent outbreak of Coronavirus (Covid-19) has seen the most dramatic changes most of us have ever experienced in our working lives. These changes have put a great deal of pressure on IT teams and businesses to quickly adapt and setup users for home working. Due to the pressure of driving rapid enablement and availability, in some instances security will have been an afterthought.

We have developed this Synergi whitepaper as we want all businesses to be protected through these challenging times and not be adversely impacted by cyber security issues. The importance of secure access to all of your systems and data should now be extremely high on your agenda, particularly as the period of remote working is likely to be extended for some months to come. We have also unfortunately already seen evidence of cyber criminals using this disruption to target and exploit businesses and individuals as the news link below explains;

https://www.itv.com/news/2020-03-16/cyber-criminals-looking-to-exploit-peoples-fears-over-coronavirus/

The good news is that as a subscriber of Office 365, Microsoft 365 and for some Enterprise Mobility & Security (EMS) there are many out of the box security features you already have access to, are simple to deploy and can improve your overall security posture.

This brief whitepaper provides some basic information and links to help you deploy additional features and better protect your environment and users. To keep this document brief we have not covered many areas including the continued importance of cyber security training as part of the recommendations below, but if you want further advice and guidance on any security related matters or you would like our assistance with deployment or training please contact us.

FEATURES & PLANS

To decide on the most appropriate features for your business please review the sections below which provide a brief description of what each will provide. Listed next to each feature is the relevant plans that the specific option applies to. Further details are then provided on some of the key features including links to deployment, training guides and some important considerations.

Once you have read the whitepaper and reviewed your current security posture you may decide to implement some changes. There are links throughout this whitepaper with guides from Microsoft and some videos on how to deploy the features. Having read the whitepaper if you would prefer us to review your current position and offer a comprehensive security review of your environment and deploy any features for you just let us know.

It is important to note that access to some of the security features listed will vary depending on the plans you subscribe to currently.

For any existing Synergi customers that have a support contract we will provide you with 1 hour of free support assistance from the team to get you started with the implementation of new security measures you decide to adopt.

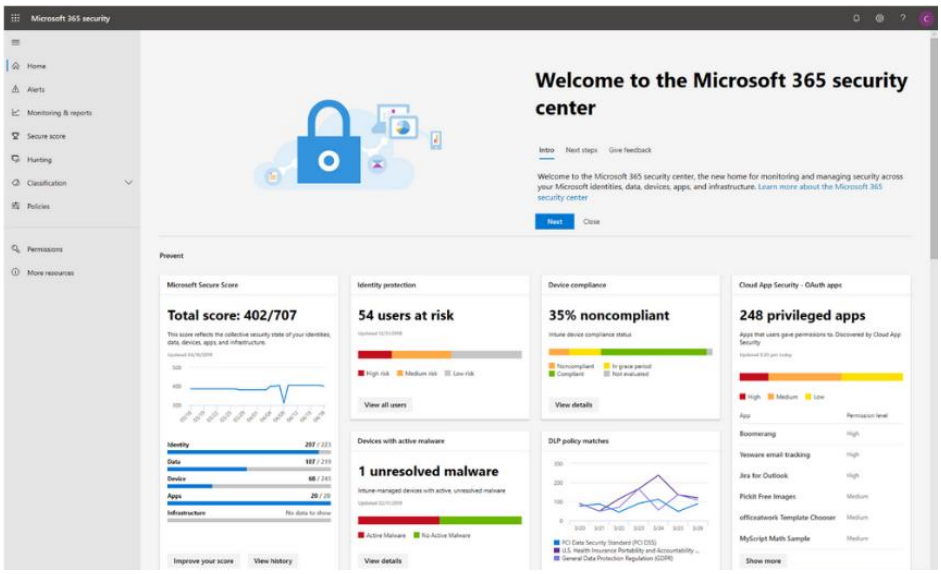
SECURITY FEATURES

1.1 Secure Score

Availability – All plans

First of all let's take a look at Secure Score. Secure Score is a good starting point and is a free tool built into all Office 365 and Microsoft 365 plans. It is designed to help you understand your current Office 365 security position, help you to identify issues and make improvements. If you are a 365 admin level user you should be able to access Secure Score.

Please note Microsoft are currently working on new versions of the Secure Score dashboards and these are accessible in preview mode by clicking the blue link near the top of the screen "Try the preview version". Depending on your 365 subscription you will have different options available to you to review. On the preview version under the metrics and trends tab you can compare your own Secure Score % with similar organisations using 365.



Link to your Microsoft Secure Score dashboard
https://security.microsoft.com/securescore

Learn more & understand how to implement Secure Score recommendations
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-secure-score?view=o365-worldwide

1.2 Multi Factor Authentication (MFA)

Availability - M365/O365

Using multi-factor authentication is a very effective way to improve the security for your Office 365 environment and basic configuration is simple. Once enabled your users will login as normal and a prompt will then ask them to enter a code from a text message or via an authenticator App on a mobile device (various free options are available). This security feature can prevent unauthorised access to your 365 environment. Recently user credential theft has seen an increase in targeted attacks from cyber criminals looking to exploit stolen credentials, most typically for financial fraud. Multi-factor authentication is also called 2-step verification.

MFA can also be applied to external guest access. There is a conditional access rule you can apply "Require MFA always for guest and external users" When activated this will prompt guests to register for MFA in your tenant. This does not conflict with any existing MFA policies they may already be using. When they access any resources in your tenant any guests or external users are then prompted for MFA authentication for every request.

MFA deployment guide
https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

Conditional access rules
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

Tutorial on MFA for guest users
https://docs.microsoft.com/en-us/azure/active-directory/b2b/b2b-tutorial-require-mfa

Video guide - MFA deployment
https://support.office.com/en-us/article/set-up-multi-factor-authentication-in-microsoft-365-business-a32541df-079c-420d-9395-9d59354f7225

Points for consideration

- 2 step verification requires the use of a secondary authentication tool, if you don't use company mobiles you may need to ask permission from users to use their personal mobiles for the Authentication app or inbound text messages.
- You will need to consider how often users are prompted for MFA challenges as this can impact productivity. Settings to alter this extensively are available with some of the Office 365 plans.
- For external guest access make sure they are aware you are using MFA rules which will enforce better security on any shared documentation.

1.3 Device & Application Management

Availability – M365 / EM&S

Microsoft Intune is a product within Microsoft 365 that provides both device and application management capabilities. Device management allows you to manage your company owned devices centrally, by deploying policies such as encryption via BitLocker for Windows 10 to secure your devices.

Application management can be used to protect data within Office 365 apps even on a users' personal device, allowing users to use their own iPhone or Android device to access apps such as Outlook & Teams whilst still securing the data. You can create your own app protection policies within Microsoft Intune to achieve this.

Intune Quick Start guide
https://docs.microsoft.com/en-us/mem/intune/fundamentals/setup-steps

Configure app protection policies
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies

Video guide - creating app protection policies
https://youtu.be/34jGh463ojM

Points for consideration

- Intune has a vast range of features that can be configured, app protection can provide an effective and quick method to add a layer of protection to users signing into Office 365 apps.
- Use the Company Portal app by Microsoft to create your own corporate app store containing approved business applications.

1.4 Advanced Threat Protection (ATP)

Availability – Included in M365 Business / Enterprise E5. Available as add-on license.

Microsoft Office 365 Advanced Threat Protection (ATP) is a set of tools that provides further protection against malicious threats within email and other collaboration tools such as Microsoft Teams.

Cyber criminals often use phishing campaigns to target users with email messages that may contain malicious URL's or attachments, the features within ATP are designed to protect users against this.

The following are core features within ATP:

ATP Safe Links

Safe links can protect users against visiting malicious websites by providing time-of-click verification for URL's to check if the site is malicious.

Safe links work in emails and within Microsoft Office applications for Windows 10, iOS & Android.

Office 365 administrators can configure safe link policies within the security admin portal:

https://support.office.com/en-gb/article/manage-atp-safe-links-61492713-53c2-47da-a6e7-fa97479e97fa

ATP Safe Attachments

The safe attachments feature scans attachments within emails and takes action on attachments which are detected as malicious.

Safe attachments can also be configured for use within OneDrive, SharePoint & Teams.

Office 365 administrators can configure safe attachments policies and actions within the security admin portal:

https://support.office.com/en-gb/article/manage-atp-safe-attachments-e7e68934-23dc-4b9c-b714-e82e27a8f8a5

ATP anti-phishing protection

ATP anti-phishing provides protection against phishing attempts within Office 365 email by detecting against impersonation attacks. Checks can be performed against users and domains to verify if a sender is attempting to impersonate a genuine contact.

Office 365 administrators can configure anti-phishing policies within the security admin portal:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#set-up-an-anti-phishing-or-atp-anti-phishing-policy

Points for consideration

- The tools outlined above are an additional layer of protection against threats in Office 365, it is not guaranteed that 100% of malicious files or links can be detected and blocked.
- The 'Dynamic Delivery' feature within Safe Attachments can be configured to deliver emails without the attached file, the file is then added back once the email scanning is complete. This is useful for scenarios where you don't want to delay emails from being received whilst scanning is underway.

1.5 Use dedicated admin accounts & MFA

Availability – All plans

Any administrative accounts that are used to manage your Office 365 or Microsoft 365 environment will include elevated permissions. Clearly this makes them a very valuable target for any cyber criminals. You should only use admin accounts for administration level tasks to reduce the risk of any compromise. All system admins should have their regular user account and a completely separate admin account for when they need to perform any admin level tasks.

Admin Roles in Office 365
https://docs.microsoft.com/en-gb/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

Video guide - adding admin users to Office 365

https://youtu.be/KEKv6ZwO1nM

Points for consideration

- Ensure all of your admin accounts use MFA please see 1.2 above for more information on enabling this feature.
- Only use admin accounts for tasks that need elevated permissions. Once complete ensure you log out of the admin account before continuing.
- You should never use admin accounts to register for any 3rd party services.
- Always close down all other windows and applications prior to logging in as an admin user. Ideally perform a clean reboot before completing admin tasks.

1.6 Protection against Malware and Ransomware in Email

Availability – All plans that include Exchange

If you are using Office 365 and are using the Exchange element your email messages are automatically protected against malware via the Exchange Online Protection feature (EOP). The areas covered by EOP are;

- Ransomware – If delivered and opened this can have a serious impact, encrypting important files and folders and preventing access to critical information. Without a reliable backup these files can often be lost permanently even if the ransom is paid.
- Viruses – If delivered these can be transmitted across the network and can carry a variety of payloads from enabling remote access to your machine through to data destruction.
- Spyware – This will typically sit in the background harvesting information and data, often user account details and passwords, once collected these can then be used by cyber criminals to access your systems and information.

How to turn on Malware protection for M365
https://support.office.com/article/02b5783a-eea0-42e8-8856-62440718c3f0

Information about the Malware protection available in Office 365
https://docs.microsoft.com/en-gb/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide

Points for consideration

- End user training is critical in the fight against cyber criminals. No security system will provide a 100% guaranteed protection against Malware, Viruses and Ransomware so end user vigilance is critical. Cyber security training should be considered for all end users on an ongoing basis.
- There are sophisticated endpoint protection solutions available which can prevent the impact of Ransomware attacks and allow files to be recovered in some cases without resorting to backups. You should consider if these are necessary.
- With good backups in place the impact of a Ransomware attack in particular can be mitigated. A secure backup solution may be worth considering.

1.7 Disable auto forwarding for email

Availability – M365/0365

Auto forwarding for email allows users to automatically forward a copy of emails to another email address, this can be useful in specific scenarios. However, this can also be exploited within breached Office 365 accounts. Cyber criminals may gain unauthorised access to an Office 365 account and place an email forward to an external email address, allowing them to discreetly receive a copy of a users' email – until the forward is discovered and disabled.

By disabling this feature within Exchange Online, you can prevent emails from being auto-forwarded outside of the organisation.

Stop auto-forwarding emails
https://docs.microsoft.com/en-gb/archive/blogs/exovoice/disable-automatic-forwarding-in-office-365-and-exchange-server-to-prevent-information-leakage

Video Guide - disabling auto forward
https://support.office.com/en-us/article/stop-auto-forwarding-emails-in-microsoft-365-f9d693ba-5c78-47c0-b156-8e461e062aa7

Points for consideration

- You should identify if any service accounts within Office 365 need to auto-forward email to an external address , as an example this could be a mailbox within O365 that forwards its mail to a 3rd party HR system that you use within the business.
- This setting should be used in conjunction with other tools such as Multi-Factor Authentication, to reduce the overall possibility of accounts being breached.

1.8 Message Encryption

Availability - M365, Enterprise E3, E5 and most Education and Government plans

Office Message Encryption (OME) is included with many plans and can be added via Azure Information Protection Plan 1 if it's not already available in your plan. Office message encryption allows you to send and receive encrypted messages both within your organisation and to external recipients.

The encryption features work with 3rd party email providers including Outlook.com, Yahoo!, Gmail, and many others. Email encryption provides a safeguard to ensure that only intended recipients can access information sent via an email. This can prevent accidental disclosure of confidential information and helps reduce the likelihood of a reportable GDPR data breach.

By default two options are available in Outlook message encryption – Do not forward and Encrypt. It is also possible to configure additional options that will apply a label to email, for example; Confidential.

Office 365 Message Encryption
https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide

Sending encrypted emails from Outlook
https://support.microsoft.com/en-gb/office/send-view-and-reply-to-encrypted-messages-in-outlook-for-pc-eaa43495-9bbb-4fca-922a-df90dee51980?ui=en-us&rs=en-gb&ad=gb

Video Guide - sending encrypted messages in Office 365
https://youtu.be/nTm3yStF8S0

Points for consideration

- Message encryption will often rely on the end user selecting the option at time of sending. Whilst this is a simple task the importance of doing so needs to be understood by all users to be effective, Cyber security training can help with this.
- It's worth considering what communication needs to be encrypted and getting the balance right. For some recipients they will need to use a one-time passcode provided which will clearly create additional steps for them.

THE ESSENTIALS

We advise you to run Secure Score and review the full list of options available to you. We do however fully understand that at this challenging time you may not currently be able to commit the time to do this. If this is the case then take a look at our top security suggestions below to help get you started and put your business in a more secure position. These suggestions are covered in more detail in the sections above;

1. MFA – This one feature can help prevent unauthorised access to your end user account. Simple to enable for most and a key preventive feature against hacking and financial theft. As a minimum all Admin accounts should be protected, but you should also consider normal users and external guest access, ideally this should be enforced across all.
2. App Protection – Ensures your corporate data stays within a company managed application and prevents intentional or unintentional data loss, helping keep your users productive. App policies are simple to deploy and can be enabled for corporate or personal mobile devices and they don't have to be managed via Intune.
3. Disable auto forward – Simple to implement and by disabling auto forward to external recipients this can prevent cyber criminals exporting corporate data or intercepting private business communications. Auto forwards have often been used for financial cyber fraud.
4. ATP – Enabling the core features is a simple process and provides an enhanced email filtering service for 365 that helps detect unknown malware and viruses and provides a safeguard against harmful links, attachments and phishing in real time.

FURTHER LINKS AND GUIDANCE

Please see the links below for further guidance on deployment options and to learn more about Office 365 security and the features available.

Type	Description	Link
Video	Fun introduction to Office 365 Security features	https://youtu.be/bEpZwb7XFEg
Online Learning	Understand more about Cloud security	https://docs.microsoft.com/en-gb/learn/modules/cmu-cloud-security/
Online Learning	Introduction to security in M365	https://docs.microsoft.com/en-gb/learn/modules/security-in-m365/
Online Learning	Use Reporting in M365 Security centre	https://docs.microsoft.com/en-gb/learn/modules/m365-security-management-secure-score/
Online Learning	M365 Learning Pathways – create a custom learning plan to help with M365 features and adoption	https://docs.microsoft.com/en-gb/office365/customlearning/
Web Document	Auditing and reporting on B2B users (Guest Access)	https://docs.microsoft.com/en-us/azure/active-directory/b2b/auditing-and-reporting
E-book	10 Tips for introducing the Zero Trust Security model	https://clouddamcdnprodep.azureedge.net/gdc/gdcHNvbgf/original
Online Tool	Find out how mature your security is against the Zero Trust Framework	https://info.microsoft.com/ww-landing-Zero-Trust-Assessment.html
Video	Learn more about Microsoft Defender ATP Security configuration	https://youtu.be/8E3smJ_g7lw

Please note this whitepaper does not represent comprehensive IT security advice for your business but focuses on some of the security features of Office 365, Microsoft 365 & Microsoft EM&S. The whitepaper seeks to provide advice and guidance on the features available to improve your security posture which should enable you to take positive steps to protect critical business data and create a safer working environment for your users. If you want professional security advice on your entire IT environment or help with any elements of 365 security deployment please contact the team at Synergi.