HORNETSECURITY

infinigate

MICROSOFT 365

THE ESSENTIAL COMPANION GUIDE

Foreword by Michele Guida from infinigate

Dear readers,

As a distributor of cybersecurity solutions, it is our pleasure to bring you this publication from Hornetsecurity: "Microsoft 365: The Ultimate Guide". In an era where digital transformation is inexorably driving our business world forward, end-user security is becoming an increasingly central factor in the success of organisations.

Our partnership with Hornetsecurity enables us to provide comprehensive guides and resources to help IT service providers optimise the protection of their end customers. By sharing best practices and collaborating with IT service providers, we strive to build trust and create long-term partnerships.

This book offers you not only technical solutions, but also valuable insights and advice on how to optimise the security of your end customers. It is a resource for administrators and IT staff managing a Microsoft 365 environment, as well as for business decision-makers preparing for cloud migration.

Our aim is to develop IT service providers into Managed Service Providers (MSP) in order to promote a co-operative relationship and ensure the highest level of security for end customers. We firmly believe that only through close co-operation and mutual trust can sustainable protection against the increasingly sophisticated threats of the digital world be achieved.

I invite you to study this book and benefit from the valuable insights that will help you to optimise the security of your end customers and make your journey with Microsoft 365 a successful one.

Yours sincerely,

Michele Guida
Business Development Manager, Infinigate (Schweiz) AG

INTRODUCTION

WELCOME TO THIS FREE EBOOK ON MICROSOFT 365 FROM HORNETSECURITY. WE'RE GOING TO SHOW YOU HOW YOU CAN USE THESE CLOUD SERVICES TO IMPROVE YOUR BUSINESS AND GET THE BEST OUT OF USING MICROSOFT 365. THIS IS THE THIRD VERSION OF THIS EBOOK AND IS CURRENT AS OF JULY 2023.

WHO SHOULD READ THIS EBOOK

The intended audience for this book is administrators and IT staff who run a Microsoft 365 environment. It covers the best practices and optimal configurations of the most important apps and features but also an overview of the suite, which is particularly useful for those either preparing to migrate to Microsoft 365 or who have already migrated and need to get the lay of the land. If you're a developer looking to create applications and services on top of the Microsoft 365 platform, this book is not for you.

If you're a business decision maker, rather than a technical implementer, this book will give you a good introduction to what you can expect when your organization has migrated to the cloud and ways you can adopt various services in Microsoft 365 to improve the efficiency of your business. If you're a Microsoft Partner managing other companies' deployments and using Microsoft 365 Lighthouse as a way to manage multiple tenants in one console, the contents of this eBook are completely valid for you.

STRUCTURE OF THIS EBOOK

The book is comprised of three parts. Part 1 (chapters 1-6) is an introduction to Microsoft 365. If you're already familiar with the basics, you may skip to Part 2 (chapter 7-13) to learn about day-to-day administration and management, best practices, and maintenance. The final part (chapter 14-16) focuses on three critical M365 topics all Microsoft 365 environments need to address, namely, security, backup, and compliance.

We'll cover the differences more deeply later in the book but here's a good place to clarify that **Office 365** (from now on referred to as O365), is email collaboration and a host of other services provided as a Software as a Service (SaaS) whereas **Microsoft 365** (M365) is Office 365 plus Azure Active Directory Premium, Endpoint Manager (Intune) – cloud-based management of devices and security plus Windows 11 Enterprise. Both are user-based subscription services that require no (or very little) infrastructure deployments on premises. For the small business plans (up to 300 users), only Microsoft 365 is available, and while both are available in the Enterprise plans, the huge benefits of the added services in Microsoft 365 does mean that just having Office 365 plans is unusual. As such we will mostly be referring to Microsoft 365 from here on.

This is the third version of this eBook and is current as of July 2023.

CONTENTS

PART 1 – OFFICE & MICROSOFT 365 BASICS 7

DROP YOUR BAGGAGE! 8
HOW TO KEEP UP 8
BE YOUR OWN GUINEA PIG 10
ADOPTION 11

CHAPTER 1 – WELCOME TO MICROSOFT (AND OFFICE) 365 12
OFFICE 365 12
MICROSOFT 365 13

CHAPTER 2 - MANAGING O365 AND M365 15
WEB PORTALS 15
POWERSHELL 17
MICROSOFT 365 LIGHTHOUSE 18

CHAPTER 3 - MIGRATING TO O365 19
MIGRATION 19

CHAPTER 4 - SUPPORTING M365 22
TEST CONNECTIVITY 22
CLIENT-SIDE TOOLS 24
SERVICE REQUESTS 26
SERVICE HEALTH 26
NETWORK CONNECTIVITY 26
MICROSOFT 365 DESIRED STATE CONFIGURATION 27

CHAPTER 5 – CLIENTS 29
DESKTOP CHOICES 29
MOBILE CHOICES 30
ONEDRIVE FOR BUSINESS 30
TEAMS 30
APPS ADMIN CENTER 30

CHAPTER 6 – WINDOWS 11 ENTERPRISE 32
WINDOWS 11 ENTERPRISE 32

PART 2 – MANAGING, MAINTAINING AND SUPPORT FOR MICROSOFT 365 34

CHAPTER 7 – AZURE ACTIVE DIRECTORY 35
ENTRA, PRIVA AND PURVIEW 35
MEET AAD & HYBRID IDENTITY 36
AAD CONNECT – YOUR UMBILICAL CORD 36
AZURE MFA 37
PUBLISHING APPLICATIONS 39
PREMIUM FEATURES 39
CONDITIONAL ACCESS POLICIES 40
MANAGING THE ACCOUNT LIFECYCLE 41

CHAPTER 8 – EXCHANGE ONLINE **42**
IT'S A HYBRID WORLD 42
BACKUP AND NATIVE DATA PROTECTION 43
AUTODISCOVER 43
MANAGING MAILBOXES 43
MAILBOX ARCHIVE 44
MAIL FORWARDING 44
SHARED MAILBOXES 44
MAIL CONTACTS AND USERS 45
DISTRIBUTION LISTS 45

CHAPTER 9 – ONEDRIVE FOR BUSINESS AND SHAREPOINT **46**
ONEDRIVE FOR BUSINESS 46
SHAREPOINT 47

CHAPTER 10 - MICROSOFT 365 GROUPS **49**
GROUP TYPES 49

CHAPTER 11 – TEAMS **52**
MEET TEAMS 52
TEAMS PHONE 53
MANAGING TEAMS 54
USING TEAMS 55
VIVA 56
EXTENDING TEAMS 57

CHAPTER 12 – OTHER OFFICE 365 APPLICATIONS **58**
PLANNER 58
STREAM 59
KAIZALA 59
POWERBI 59
POWER AUTOMATE 60
POWERAPPS 61
MICROSOFT LISTS 62
MICROSOFT LOOP 62

CHAPTER 13 – MICROSOFT INTUNE **63**
MOBILE DEVICE MANAGEMENT 64
MOBILE APPLICATION MANAGEMENT 64
MICROSOFT CONFIGURATION MANAGER 65
INTUNE SUITE 65

PART 3 – SECURITY, BACKUP & COMPLIANCE **66**

CHAPTER 14 - SECURITY IN O365 ..... **67**
365 TOTAL PROTECTION 68
365 PERMISSION MANAGER 68
MICROSOFT PURVIEW INFORMATION PROTECTION 69
MICROSOFT INFORMATION PROTECTION 69
OFFICE 365 MESSAGE ENCRYPTION 70
DATA LOSS PREVENTION 70
EXCHANGE ONLINE PROTECTION 70
DEFENDER FOR OFFICE 365 71

AUDITING 71
SAY GOODBYE TO PASSWORDS? 72
BLOCK USER ACCESS 73

CHAPTER 15 – SECURITY IN MICROSOFT 365 74
MICROSOFT 365 DEFENDER 74
MICROSOFT DEFENDER FOR ENDPOINT 75
MICROSOFT DEFENDER FOR IDENTITY 75
MICROSOFT DEFENDER FOR CLOUD APPS 76
SECURE SCORE 77
SECURITY IS EVERYONE'S RESPONSIBILITY 81
KEEPING MICROSOFT HONEST 81

CHAPTER 16 – BACKUP IN MICROSOFT 365 82
NATIVE DATA RESILIENCY 82
365 TOTAL BACKUP 84
NEVER STOP LEARNING! 85

PART 1

OFFICE & MICROSOFT 365 BASICS

MICROSOFT 365
THE ESSENTIAL
COMPANION GUIDE

This section introduces M365, how to do basic management, migrating to M365, support options, which client apps you're likely to support and manage and Windows 10/11. If you're already familiar with M365 and looking for more advanced insights into M365 administration, **skip straight to Part 2.**

DROP YOUR BAGGAGE!

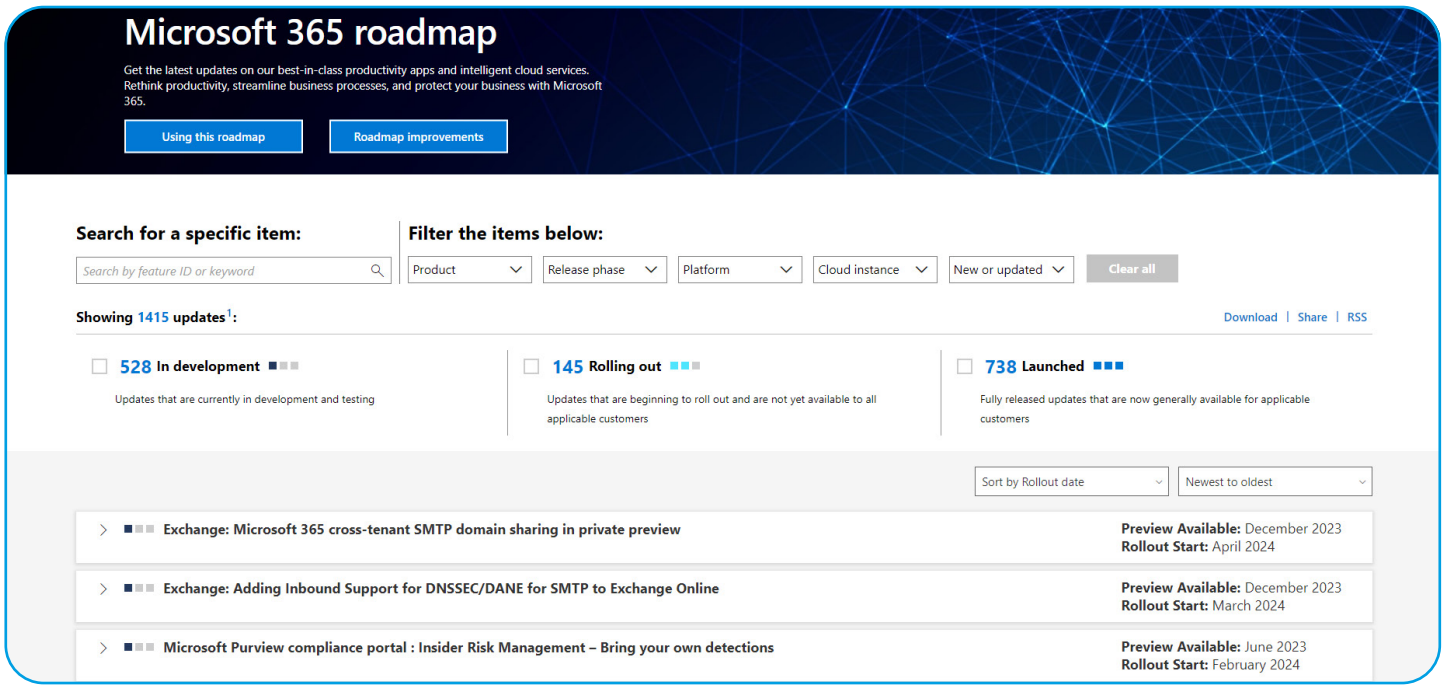
One of the most important things you need to do if you have a background with Exchange Server or SharePoint Server on-premises is to drop the idea that M365 is just a hosted Exchange or SharePoint. Some years ago, this was true and O365 was simply Microsoft hosting Exchange, SharePoint, and Lync servers in their datacenters, but this is no longer true. M365 is now a cohesive platform, with Exchange Online and SharePoint online providing some foundational building blocks for that platform but there are many other services built on top that you'll miss (or misunderstand) if you're still thinking in terms of hosted mail servers. A case in point is Microsoft Teams, a collaboration service that uses Exchange Online to store retained data and chats, SharePoint to store documents, Planner for lightweight project management and Azure AD for identity. All that complexity is managed by Microsoft, and you simply administer Teams as just another service. And that also means there'll never be a "Teams server" for on-premises, the required building blocks are just too complex for most businesses to deploy.

The other thing to let go of if you come from an on-premises background is planning for software upgrades every few years. Upgrading Exchange Server, as an example, can be a large project (depending on the size of your environment), taking months to plan and execute. M365 is a different world with smaller updates coming every day or week and your job thus transforms into assessing these changes, how they'll impact users, and managing change in the organization.

HOW TO KEEP UP

I have worked with Exchange Server since version 5.5 (1997), and I got used to the cadence of a new version every 2-3 years. I bought books and read up about all the new features and changes in preparation for the next iteration. That approach to software development is finished.

Nearly all software projects (and definitely those in M365) are now aiming at frequent, incremental changes. This brings several benefits, first each update is minor and no big project plan for the "upgrade" is required, secondly the developers can adjust course and continually add new features based on user feedback much faster.



The Microsoft 365 Roadmap

As an M365 administrator, however, this does bring a big challenge. Instead of being able to plan for and learn about a large set of new features coming in the next big release, new features are released daily, and you need to understand them and help your organization take advantage of them. There are several ways to manage this – depending on your learning style. Some people learn by reading, others by listening, others by watching videos and some people only learn by doing tasks themselves (and most of us learn best with a blend of these).

Here are some resources to add to your toolbelt for keeping up with changes in M365:

The Official Microsoft **365 roadmap** (microsoft.com) lets you filter on many different components of M365.

Staying on top of Office 365 Updates (techcommunity.microsoft.com) is a great blog post with links to various resources for managing the flood of updates, for different types of audiences.

What's **new in Microsoft Intune** details the weekly updates in Microsoft Intune.

What's **new in Azure Active Directory** covers monthly updates to Entra ID (previously Azure AD) (see chapter 7).
Azure AD Connect: Version release history covers updates to AAD Connect (see chapter 7).
Microsoft Mechanics is a YouTube channel with interviews and demos on upcoming features along with Office and Azure playlists.

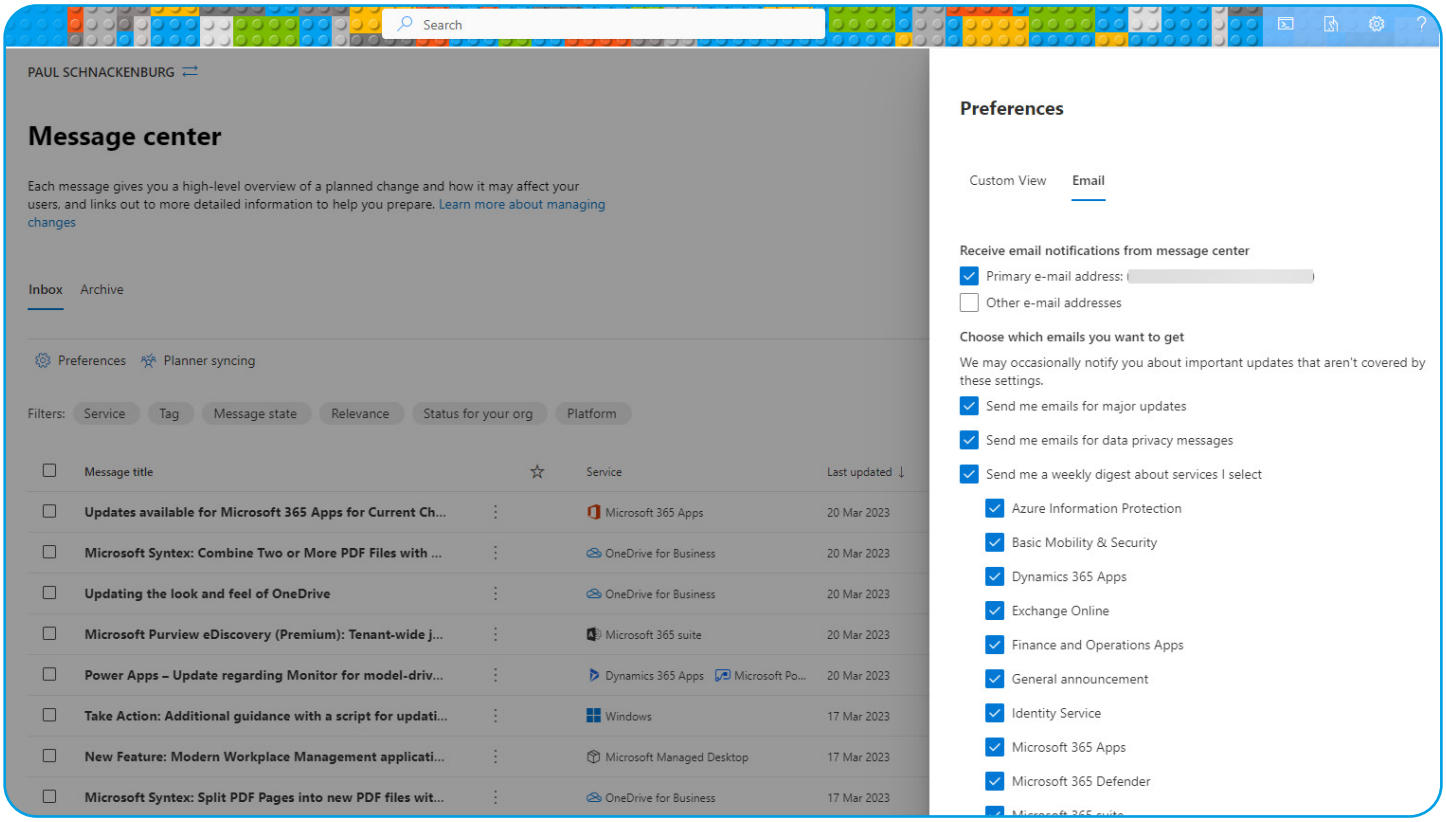
And finally, the **Message center** in the portal (chapter 2) shows a stream of what's changing

and new features – click the Preferences link to customize which services you get updates for and who should receive the weekly digest email – a best practice is to target an email distribution list so that staff who don't have access to Message center can receive weekly email updates.

BE YOUR OWN GUINEA PIG

It's important that as an administrator you are testing new features as they come out or ideally when they're in the preview phase. There are two tracks for updates released in O365, **Standard and Targeted**. The former is the normal rollout cadence while the latter ensures that you get new features as soon as they're ready.

In the past the recommendation was to have a small, separate test tenant for this where the whole tenant was in Targeted, if you have the budget this can be useful. Today it's more common to define members of the IT team and power users in your business with Targeted release for select users. There's also **an option** to ensure that your local Office Apps for enterprise installation receives updates ahead of the rest of your users.



Controlling notifications from the Message Center

ADOPTION

If your challenge is helping others in your business to get on board the M365 train, Microsoft has a **great community** and plenty of **resources** to help you, and if you need help to continue driving adoption across M365 workloads, join the free **Champions Program**.

Another great resource is **Fasttrack** which provides migration guidance for every M365 tenant (and Dynamics 365 and Azure), if you're on M365 and have 150+ seats you can converse with a migration expert online and if you have over 500 seats you can have **an engineer assist you in the migration** (remotely) and in subsequent adoption projects.

CHAPTER 1:

WELCOME TO MICROSOFT (AND OFFICE) 365

IN THIS CHAPTER WE'RE GOING TO LOOK AT THE DIFFERENT FLAVORS OF M365, HOW TO PICK BETWEEN THEM AND WHAT VALUE THEY PROVIDE TO YOUR BUSINESS. AS PREVIOUSLY STATED, IF YOU'VE ALREADY SET UP YOUR M365 ENVIRONMENT OR YOU'RE LOOKING FOR MORE ADVANCED INSIGHTS, PROCEED DIRECTLY TO PART 2.

A CORRECTLY IMPLEMENTED MICROSOFT 365 IS AN ENABLER FOR YOUR BUSINESS, MAKING IT EASY FOR YOUR STAFF TO WORK IN TEAMS AND COLLABORATE BOTH INTERNALLY AND WITH EXTERNAL PEOPLE IN A SECURE MANNER. IT ALSO ENABLES SECURE WORK FROM HOME/ANYWHERE FOR YOUR EMPLOYEES. APART FROM PICKING THE RIGHT FLAVOR OF M365 THE KEY TO A SUCCESSFUL ADOPTION IS PLANNING, END USER TRAINING AND ENSURING YOUR IT STAFF UNDERSTANDS THEIR NEW ROLE.

1.1: OFFICE 365

Microsoft has diminished their focus on Office 365 for quite a few years now and will continue to do so. For businesses smaller than 300 staff it's no longer an option and for larger businesses the recommendation is to look at Microsoft 365 plans (see below).

Some services mentioned in this chapter are explored more deeply in later chapters. We'll use the term SKU; it stands for Stock Keeping Unit and is a term that describes different licensing levels.

Your first decision here is between Business and Enterprise SKUs. The former tops out at 300 users so if you have a larger business (or expecting to grow), stick with the Enterprise flavors.

To clarify – **Microsoft 365 Apps for enterprise** (what **used to be called Office ProPlus**) is the new name for the desktop applications such as Word, Excel etc. that are available for Windows and Mac – some SKUs include it, and some don't. On the other hand, all plans include Office Online (renamed to just "Office" – not confusing at all), so Word, PowerPoint etc. running in a browser. Note that these online versions of Office are limited in functionality compared to their desktop brethren but are useful for quick edits.

On the Enterprise side (which is only a name, it doesn't have to be for a huge business, for example you could have five lawyers handling very sensitive data in an SMB using Enterprise E5) there's Apps for enterprise which only gives you Apps for enterprise and OneDrive file storage but no other cloud services. E1 gives you Office (Online) and Exchange, OneDrive, SharePoint, Teams, Yammer, and Stream, E3 gives you Microsoft 365 Apps for enterprise in addition to E1's cloud services and E5 adds PowerBI as a cloud service, along with several security features (see chapter 15).

Have a look at **the official comparison** which clearly illustrates the differences of these plans.

Microsoft 365 and Office 365 **Plan Options** covers all the plans, including tailored versions for Education, Government and country specific flavors for China and Germany.

The most important point is that the different SKUs within each family aren't mutually exclusive. In a small manufacturing business, you may have the factory workers on Business Essentials, the office staff on Business and the executives on Business Premium and in a larger business, users could be spread across E1, E3 and E5 licenses.

The **Microsoft 365 and Office 365 platform service description**, covers what the platform offers in minute detail.

1.2: MICROSOFT 365

Building on top of the O365 plans above, M365 adds Windows 10 Enterprise, Endpoint Manager (Intune) and Azure Active Directory Premium.

For Business (up to 300 users) there are three options, **M365 Business Basic** which gives you Office (online only), email, file sharing, Teams and security features. **M365 Business Standard** adds the desktop version of Office "Microsoft 365 Apps for Business", whereas **M365 Business Premium** adds iOS, Android and Windows 10/11 device management and policy enforcement from Intune plus many advanced security features. See more **here**.

On the **Enterprise** side there's F3 (for "Frontline" workers, used to be called F1) which gives you Office (Online), Windows 10 Enterprise, Active Directory Premium P1, Azure Information Protection P1 and Intune on top of O365 E1. E3 adds Active Directory Premium P1, Advanced Threat Analytics (ATA), Azure Information Protection P1, Windows 10 Enterprise and Intune on top of O365 E3. Finally, E5 adds Active Directory Premium P2, Microsoft 365 Defender, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity and Azure Information Protection P2, Windows 10 Enterprise, a host of security features and Intune on top of O365 E5.

It's tempting to think that "I'm a small business so I can save a few dollars with Business SKUs" but you need to be aware of some limitations. Your OneDrive for Business is limited to 1TB per user in Business, whereas in Enterprise you can increase this with a support call. Microsoft has made substantial changes to the Business Premium plan, and now includes all the features of **Azure AD Premium Plan 1**, so in addition to the security features already included (Conditional Access, self-service password reset and MFA), this adds cloud app discovery, Azure AD Application Proxy, dynamic groups and passwordless authentication. There are a lot of valuable security features in the Enterprise plans, particularly M365 E5, see chapter 15.

Be aware that you can move licenses between different SKUs (both upgrade and downgrade) and that you can upgrade Business SKUs to Enterprise SKUs. This discussion has been around the full SKUs and what features they contain but it's also possible to purchase individual features such as just Azure Active Directory Premium P1 as a stand-alone feature for instance. Depending on the needs of (some) of the users in your business you can tailor an exact package with just the features they need.

A great way to understand all the different parts of M365, how they fit together, and a quick description of each service is the **periodic table of Microsoft 365.**

The main take-away from this chapter is to not assume that if you're a small business you should automatically opt for a Business SKU, investigate exactly what features will serve your business needs and don't be afraid to mix different SKUs for different worker roles.

MAXIMIZE EMAIL SECURITY AND DATA PROTECTION FOR MICROSOFT 365
AVAILABLE IN
365 TOTAL PROTECTION
PLAN 4 - COMPLIANCE & AWARENESS
FREE TRIAL

CHAPTER 2:

MANAGING O365 AND M365

ONCE YOU HAVE YOUR TENANT SET UP IN M365 YOU'LL NEED TO MANAGE IT, IN THIS CHAPTER WE'LL GO OVER THE DIFFERENT INTERFACES YOU CAN USE.

IF YOU DON'T HAVE AN O365 / M365 TENANT SIGN UP FOR A TRIAL TENANT - SIMPLY CLICK TRY FOR FREE UNDER E3 OR E5. THESE TRIAL TENANTS LAST FOR 30 DAYS, ALTHOUGH YOU CAN EXTEND THE TRIAL FOR ANOTHER 30 DAYS BY CONTACTING SUPPORT.

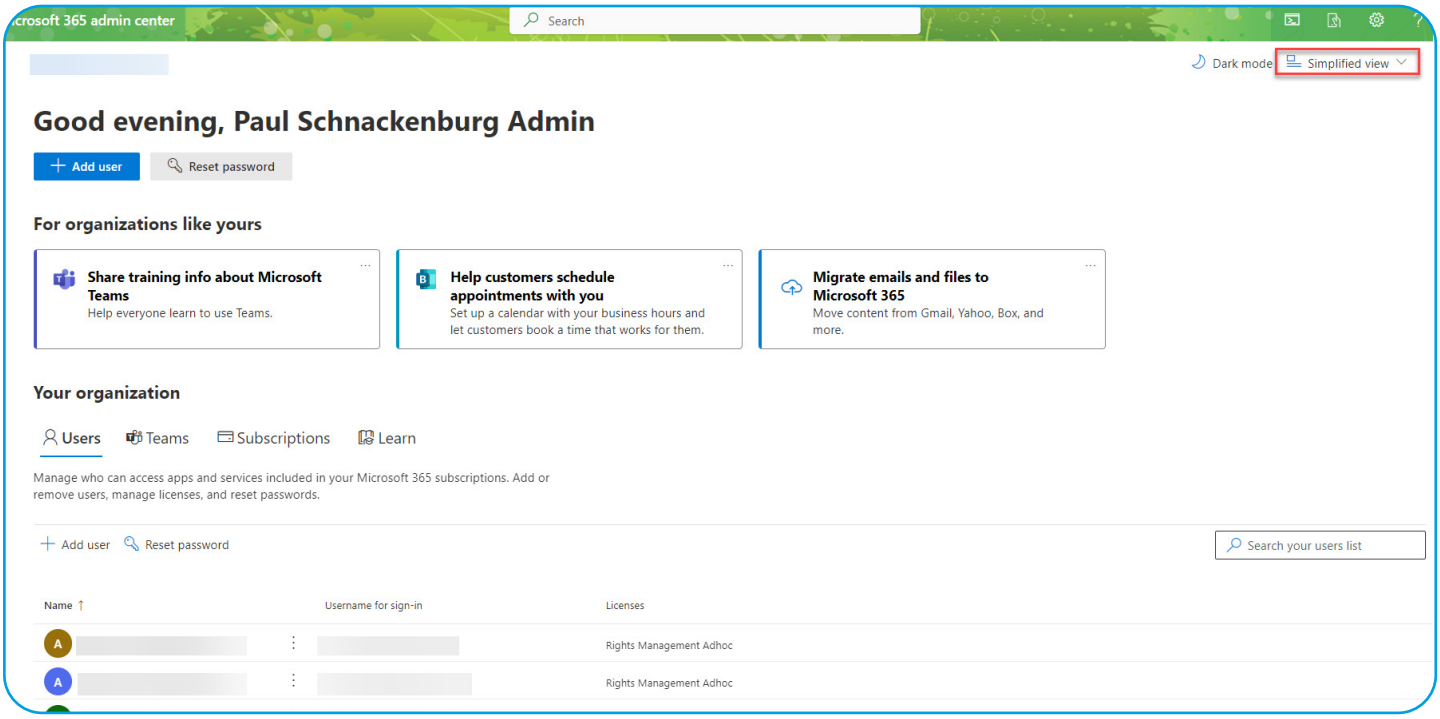
2.1: WEB PORTALS

The main portal is **admin.microsoft.com**, which you can also reach from **www.office.com**, by clicking on the Admin tile. On the left-hand side are links to manage Users, Groups, Billing and Settings etc. and further down under Admin centers are links to the individual portals for Exchange, Teams, SharePoint, OneDrive, and others. Depending on your SKU you will have slightly different links show up.

Highlights for day-to-day work include the ability to multi-select users (Users - Active users) and change their licensing for instance. You can manage invited external users, that have had documents shared to them from OneDrive or SharePoint for instance under Users – Guest users. You can also restore a recently (30 days or less) deleted user.

You can manage Groups and Shared mailboxes, like "sales@mycompany.com" that is accessed by several different people and Resources such as Rooms and Equipment (booking conference rooms or company cars). Billing is the area where you can purchase additional licenses, manage your Subscriptions and Payment methods and Support is where you lodge service requests. Under Settings is an area where you can configure different Services and add-ins whereas Setup lets you manage your email Domains. Reports has both Usage and Security reports while Health has two important areas; Service health shows you if there are any problems in the cloud with your resources and Message center has a list of updates and changes that are coming. Each individual Admin center lets you manage an individual service such as Azure Active Directory or Teams. **Msportals.io** has updated links for most of the different portals that you can access directly without going through the main portal.

Note that if you're a small business there's an option to have the admin center in Simplified view (instead of Dashboard view) which hides most of the complexity and provides easy access to the basic tasks of user, group, Teams, and device management. Just click Simplified view in the top right of the Home page in the admin center.



M365 Admin Center Simplified view

2.2: POWERSHELL

For small tenants you'll probably never have to venture beyond the web portal but if you have large amounts of users, you're going to want to automate common tasks in PowerShell using the newer **Azure AD module.**

To install the module, in an elevated PowerShell window simply run:

```
Install-Module -Name AzureAD
```

To connect (and optionally authenticate with MFA) use:

```
Connect-AzureAD
```

To check that everything is working use:

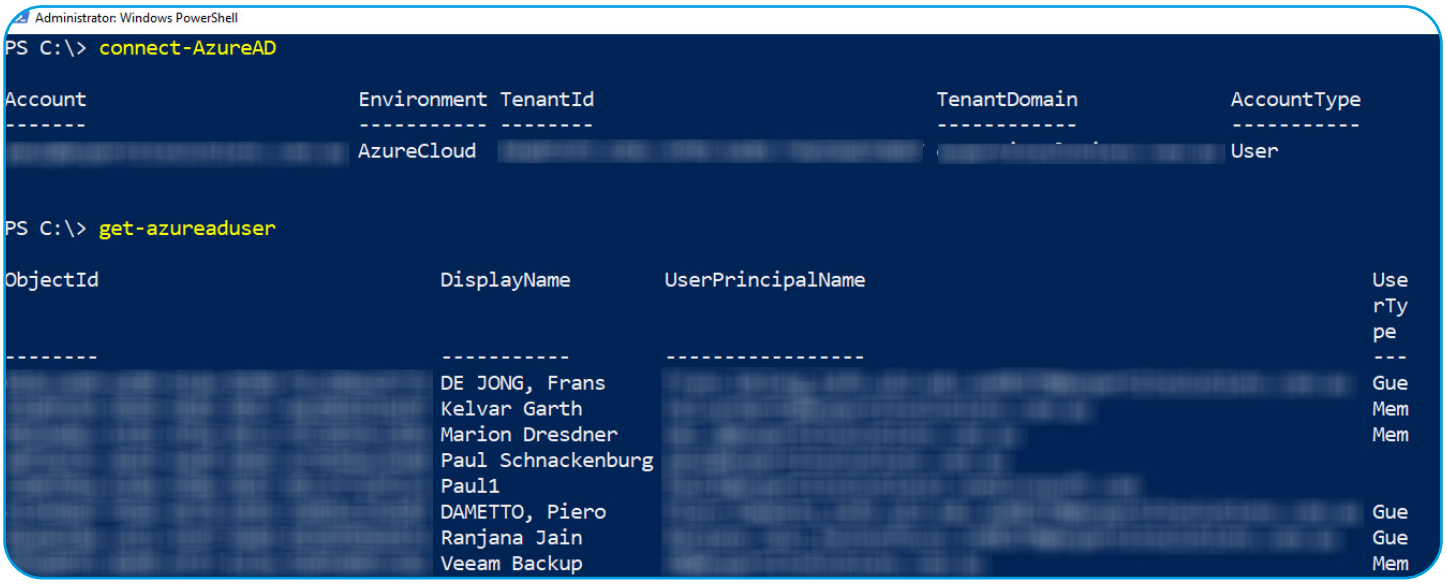
```
Get-AzureADUser
```

Which will give you a list of the users in your tenant.

Refer to the **full instructions**, including if you need to connect to government or Chinese / German tenants.

Once you're connected there are many tasks that you may want to do and perhaps automate such and **managing user accounts and licensing, creating SharePoint sites and managing users and groups, configuring Exchange settings, managing email migrations** (Chapter 3) and setting **Teams information**. Note that several of these require additional modules to be installed.
Microsoft has **finally documented** an official, scripted way to run a single PowerShell session connected to all the different services, whether you're using MFA (Chapter 7) or not.

For SharePoint (both Online and On-premises 2013/2016/2019) there's an open-source alternative / complement called **PnP PowerShell** to the official SharePoint module by the Patterns and Practices (PnP) team. The official SharePoint online cmdlets



```
Administrator: Windows PowerShell
PS C:\> connect-AzureAD

Account                    Environment TenantId                          TenantDomain            AccountType
-------                    ----------- --------                          ------------            -----------
[redacted]                 AzureCloud  [redacted]                        [redacted]              User


PS C:\> get-azureaduser

ObjectId                             DisplayName        UserPrincipalName                                  Use
                                                                                                           rTy
                                                                                                           pe
--------                             -----------        -----------------                                  ---
[redacted]                           DE JONG, Frans     [redacted]                                         Gue
[redacted]                           Kelvar Garth       [redacted]                                         Mem
[redacted]                           Marion Dresdner    [redacted]                                         Mem
[redacted]                           Paul Schnackenburg [redacted]
[redacted]                           Paul1              [redacted]
[redacted]                           DAMETTO, Piero     [redacted]                                         Gue
[redacted]                           Ranjana Jain       [redacted]                                         Gue
[redacted]                           Veeam Backup       [redacted]                                         Mem
```

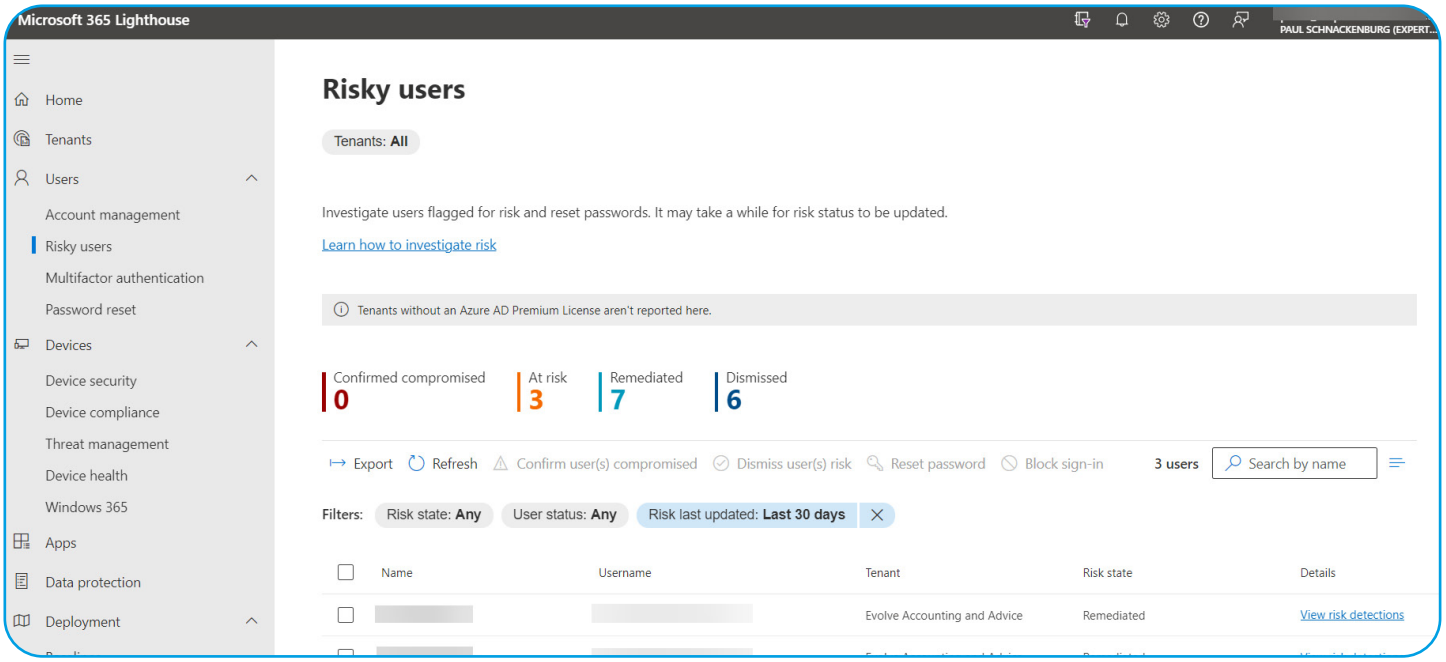
Connecting with PowerShell

are focused on creating / managing sites and users whereas the PnP cmdlets are useful for working with artifacts inside sites that have already been created.

If you need to manage M365 tenant settings or SharePoint Framework (SPFX) extensions, have a look at **CLI for Microsoft 365**, also by the PnP team, which **runs on Windows, macOS, Linux.** And if you can't be bothered installing CLI on your box you can **run it directly in Azure Cloud Shell.**

2.3: MICROSOFT 365 LIGHTHOUSE

If you're a Managed Service Provider (MSP), taking care of multiple M365 tenants you should be using Microsoft 365 Lighthouse, not to be confused with Azure Lighthouse. Both are technologies that allow service providers to manage multiple tenant clients, but where the Azure flavor is a way of allowing service provider users scoped access to Azure resources, M365 Lighthouse is a portal where you bring in multiple tenants and apply policies and management (including password resets for any user, in any tenant) into a single console.



Microsoft 365 Lighthouse

CHAPTER 3:

MIGRATING TO O365

IF YOU'RE A NEW BUSINESS THIS CHAPTER DOESN'T APPLY TO YOU – SIMPLY CREATE USER ACCOUNTS IN THE CLOUD, JOIN YOUR WINDOWS 10/11 DEVICES TO ENTRA ID AND MANAGE YOUR IOS AND ANDROID DEVICES WITH ENDPOINT MANAGER AND YOU'RE GOOD TO GO.

3.1: MIGRATION

Most businesses, however, have investments in existing technology on premises and need to migrate to M365. This chapter will cover your different options:

- Cutover migration
- Staged migration
- Express hybrid migration
- Minimal hybrid migration
- Hybrid migration
- PST-based migration
- IMAP migration
- Third party tools

If you don't have Exchange on-premises, i.e., you're using **Lotus Notes** / Domino, another email system, **Google Workspace** or another cloud email solution you're looking at either an IMAP migration or third-party migration services.

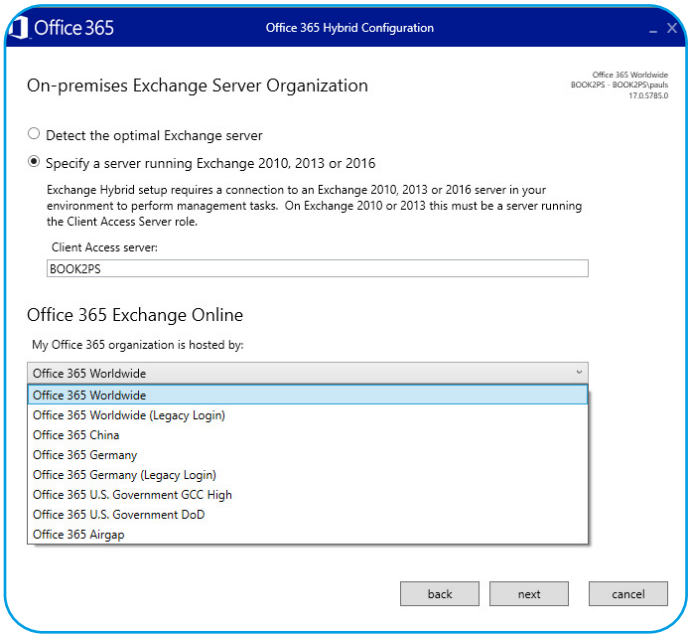
Most of the other migration methods rely on directory synchronization where your on-premises AD accounts are synched to Azure AD, which we'll cover in chapter 7.

If you're still on Exchange 2007, 2010 or 2013 (all no longer supported) a **Staged** setup allows you **to migrate mailboxes in batches**, once you've configured directory synchronization. Be aware that you'll need to manually reconfigure each user's Outlook profile to point to O365 when their mailbox has been migrated.

For smaller environments the **Cutover** approach is the easiest. Microsoft talks about **this method** for less than 2000 mailboxes (Exchange 2003+) but in the real world it's probably appropriate for 100-150 mailboxes or so, depending on internet bandwidth. The idea is that you move everyone's mailbox from on-premises to the cloud over a weekend or other appropriate downtime.

If you're on Exchange 2010+ and your plan is to move all mailboxes to the cloud over a few weeks, consider the **Express hybrid** option. If you're larger and are looking at a few months of migration time, look at the **Minimal hybrid** alternative. If you have a larger environment (Exchange 2010+) and you expect to be in a hybrid state for an extended time and you need the ability to move mailboxes from the cloud back to on-premises (offboarding) consider **Full Hybrid**. For a full breakdown of the different flavors of hybrid see **here**. The various types of hybrid **provide rich co-existence** with a unified Global Address list, sharing of Free/busy calendaring information and mailbox moves that are seamless for end-users, when their mailbox has been moved, they're just prompted to restart Outlook.

If you need to keep an Exchange server (or several) around on-premises be aware of the need to **keep it up to date so as to not be throttled**, and if possible, **look to retire it**, instead using PowerShell cmdlets to manage Exchange attributes in AD.



Hybrid Configuration Wizard

Microsoft's documentation will point you to the **mail migration advisor**, which may lead you on to the Hybrid Configuration Wizard (HCW), depending on your choices in the advisor. HCW will step you through the individual steps you must take, depending on the route you're taking, including the hybrid flavors as well as Staged and Cutover.

IMAP migrations lets you move from non-Exchange systems that support IMAP with a limit of 500,000 objects per mailbox and a maximum email size of 35 MB.

If you have PST files with email on premises you **can migrate them to Office 365**, there's even a PST Collection tool to track them down on your network

and collect them. If you have lots of them, you can even **ship them on disks to Microsoft.**

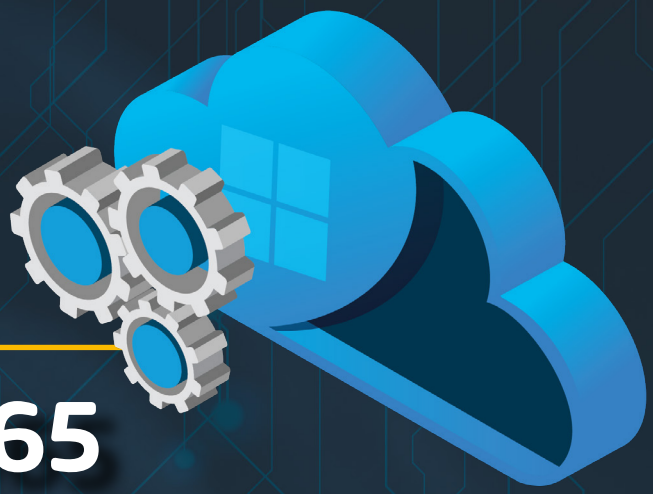
Once you have completed your migration, you'll need to consider your **Mail Exchanger (MX) DNS record** which will have been pointing to your on-premises mail server and now needs to be changed to point to Exchange Online instead. You also need to revisit your **Autodiscover DNS records** which is how Outlook and other email clients find the right Exchange server automatically.

If you're looking for a simple mailbox migration experience, Hornetsecurity offers the Mailbox Migration Tool (MMT) as part of **365 Total Protection Enterprise** / **Enterprise Backup.**

AVOID EMAIL SECURITY
BREACHES WITH
AI RECIPIENT VALIDATION
AVAILABLE IN
365 TOTAL PROTECTION
PLAN 4 - COMPLIANCE & AWARENESS
FREE TRIAL

CHAPTER 4:

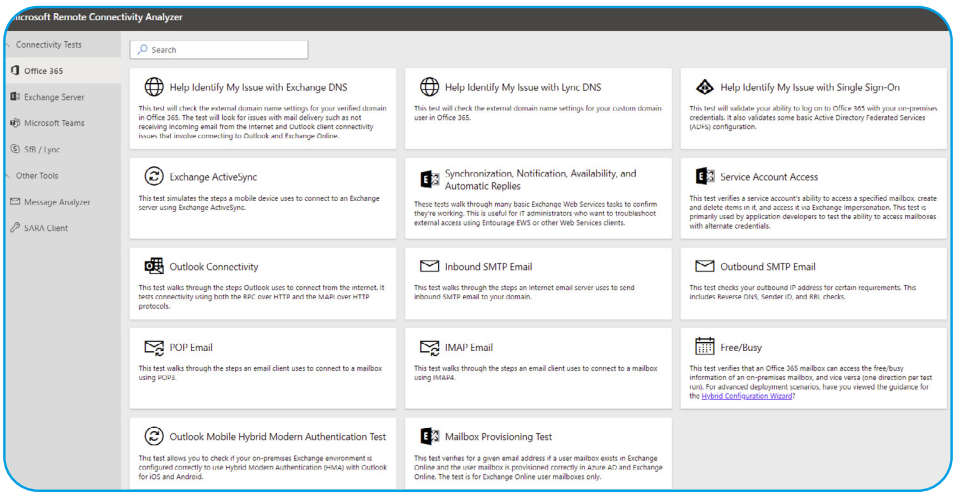
SUPPORTING M365



A BIG CHALLENGE FOR US IN IT, AT LEAST INITIALLY, IS THE LOSS OF CONTROL THAT THE CLOUD BRINGS. IF YOU HAVE A PROBLEM ON-PREMISES WITH EMAIL DELIVERY YOU CAN CHECK EVERY PART OF THE CHAIN TO SEE WHERE THE PROBLEM LIES. ONCE YOU HAVE MIGRATED TO M365 IT'S NOW A SHARED RESPONSIBILITY BETWEEN YOU AND MICROSOFT. IN THIS CHAPTER WE'LL LOOK AT TWO SELF-HELP TOOLS THAT I USE WHEN THERE'S TROUBLE AND THEN LOOK AT HOW YOU OPEN AND WORK A SUPPORT CASE WITH MICROSOFT.

4.1: TEST CONNECTIVITY

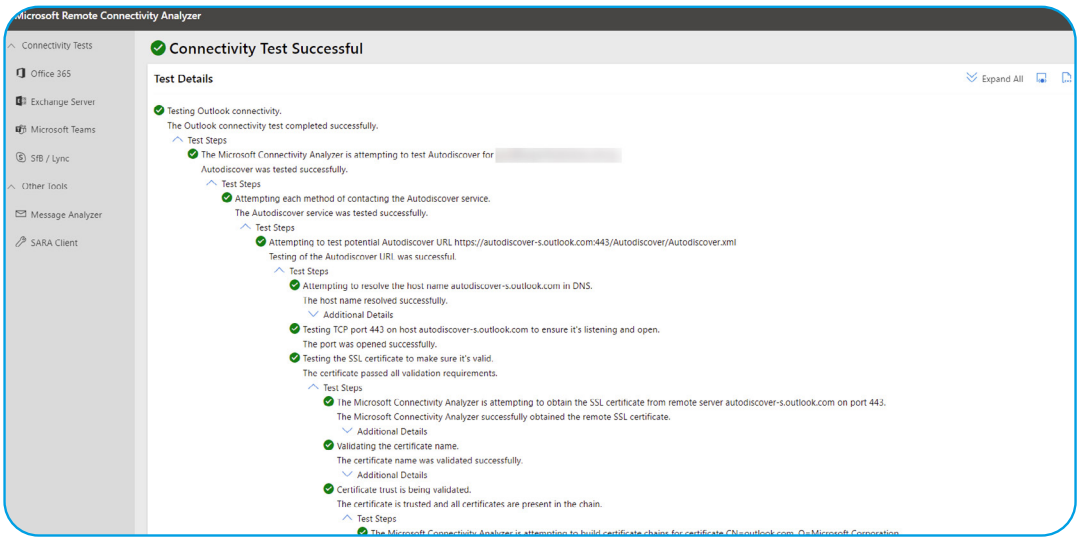
For email and Teams connectivity is a common cause of issues. Microsoft offers a useful tool; Microsoft Remote Connectivity Analyzer (MRCA or RCA) at **https://testconnectivity.microsoft.com/.**



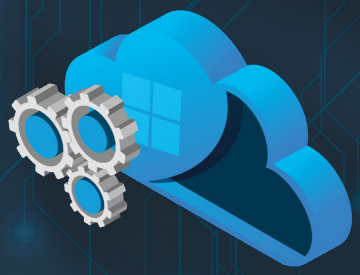
Remote Connectivity Analyzer

Here you can test several things: DNS entries, ActiveSync connectivity to Exchange, Outlook, and Outlook Autodiscover functionality and both inbound and outbound SMTP email etc. Pick the test you need to perform and enter the required information. Depending on the test you may need to enter a valid username and password – I suggest resetting the password of this account after you've completed the troubleshooting. The Captcha verification lasts for 30 minutes so if you're doing several runs as you change values you don't have to verify that you're a human every time.

The test output is comprehensive and should help you pinpoint the issue quite quickly.



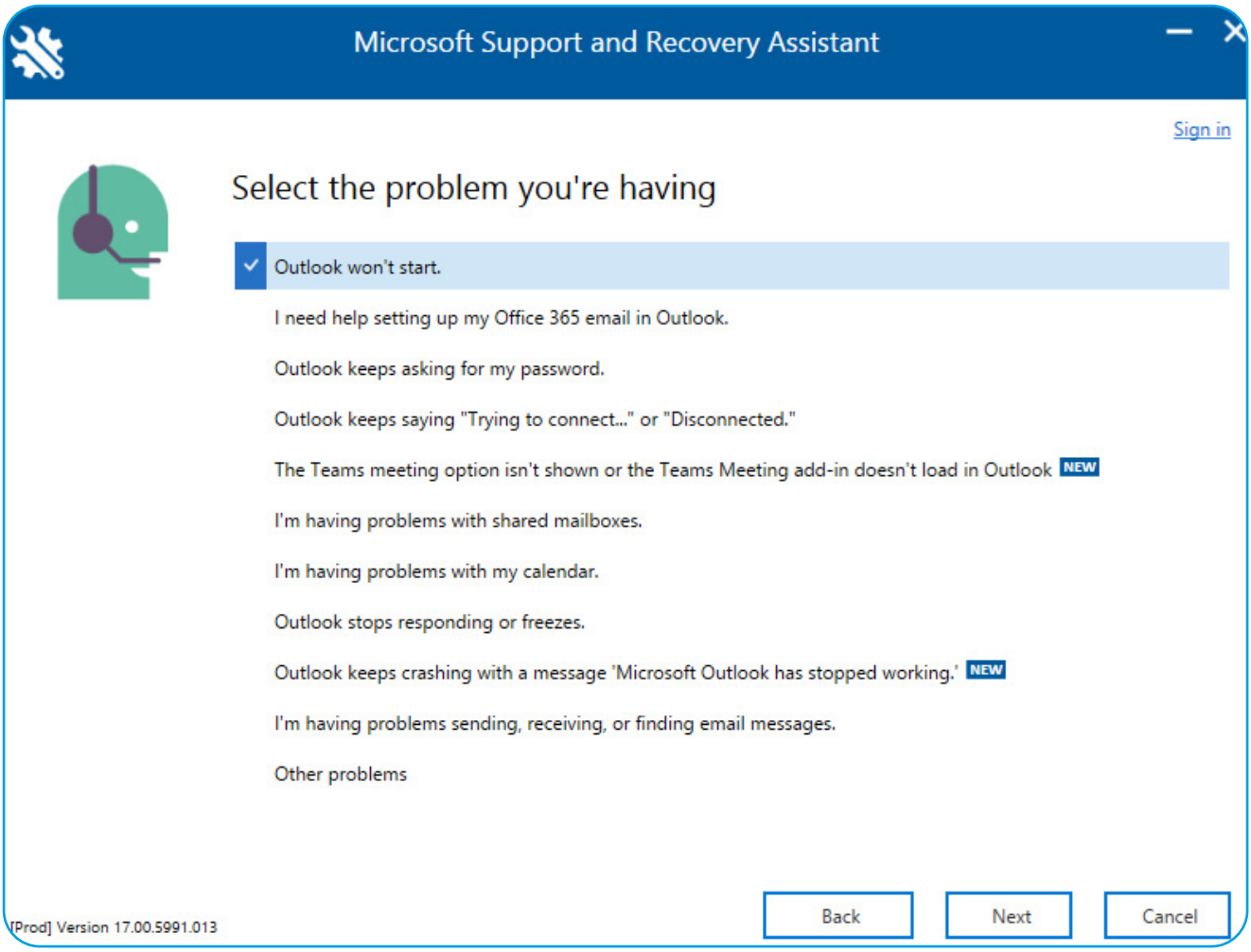
Connectivity test report



4.2: CLIENT-SIDE TOOLS

If the issue isn't connectivity related and instead you suspect an issue on a particular client device you should use the **Support and Recovery Assistant for Office 365 (SARA)** which will help identify Outlook, Dynamics 365 and OneDrive for Business issues as well as Apps for enterprise problems. It's a simple download which you run on the affected device; it steps you through a few questions to track down the problem.

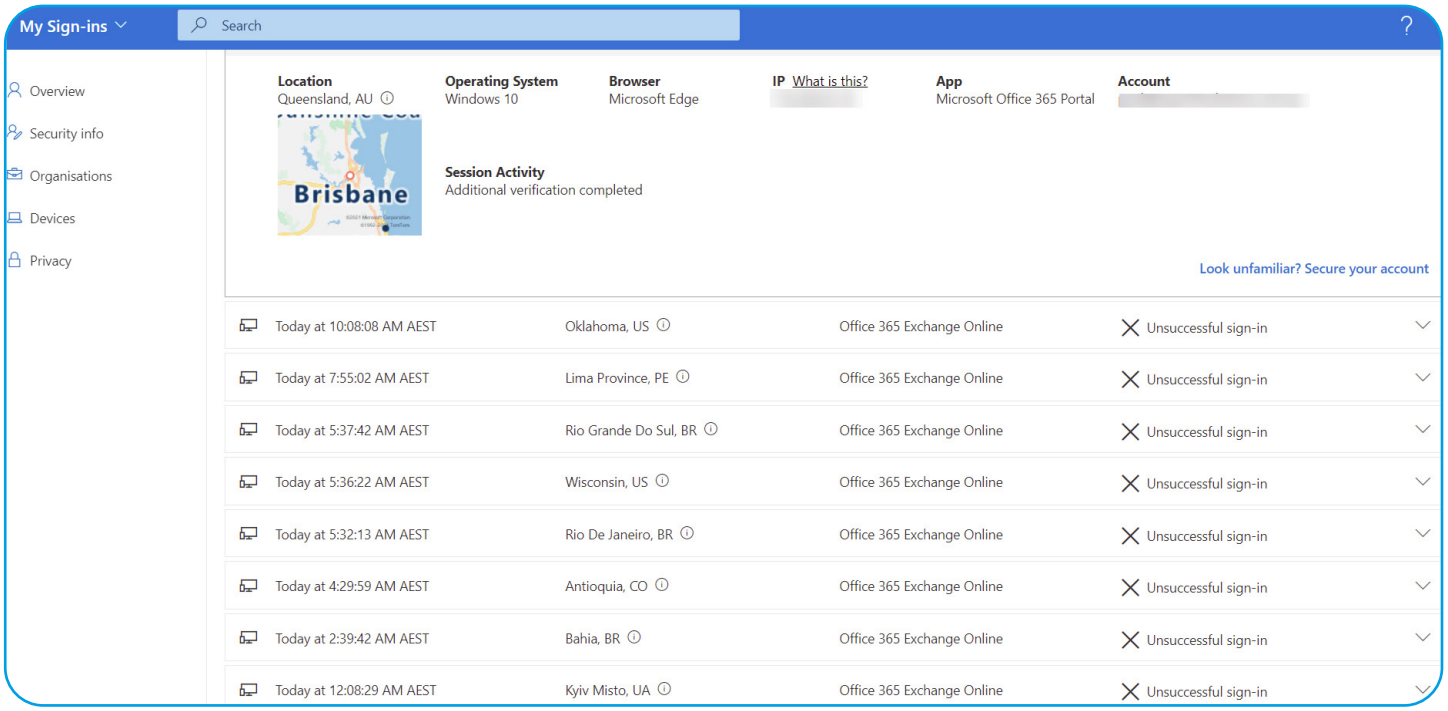
In my experience when you're struggling with profile or intermittent connection issues (that aren't due to a service side misconfiguration – see RCA) SARA is pretty good at tracking down the cause.



Support and Recovery Assistant

Another way to help end users help themselves are the **My Sign-ins**, **My groups** and **My Access** sites, which along with **My Applications** gives users a good way to manage their access of M365 services.

My Sign-ins is also an excellent education tool as it lists both successful logins and failed ones from attackers, here's a list of what my account looks like on a typical day (MFA is enabled on this account):



My Sign-Ins with attackers' login attempts

4.3: SERVICE REQUESTS

When you have exhausted the self-service options, click on the "Need help?" button in the lower right-hand corner of the portal. Start by entering a description of your issue which might give you some results for common issues and their solution. Once you hit enter the Contact support option at the bottom lights up. Enter your contact information and preference between phone and email. You can also attach screenshots or log files (up to five, each less than 25 MB), pick a time-zone and a language for the communication.

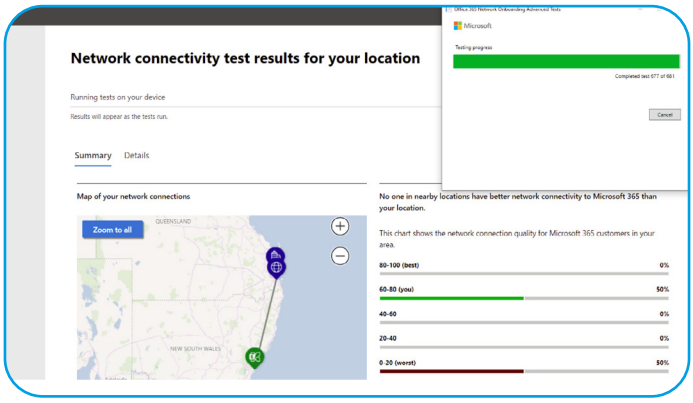
In my experience the support for M365 is good and generally tracks down the problem a lot faster than I would on my own searching forums and trying different solutions.

Behind the scenes – in the rare case that the support engineer needs access to a server that hosts your data, they use a "lockbox system" where they apply for access and a supervisor approves the request for a limited time. If you're on O365 / M365 E5 you may have turned on **Customer Lockbox**, which will involve you in that process and you have to approve the request as well.
If on the other hand the problem is located on your end the support engineers use Quick Assist in Windows to connect to your server or client PC in a view only mode and work through the issue with you.

4.4: SERVICE HEALTH

The Health section of the admin center provides overall health of the different services in M365 and if there are any outages / incidents affecting your tenant, provided you can access the portal. If the outage is affecting the portal or the health portion of it, try **https://status.office365.com/**. Also make sure to follow @Office365Health and @MSFT365Status on Twitter.

The Health section also offers an interesting new tool called **Network connectivity** which uses the OD4B client, together with the Windows Location Service and optional manual data gathering tests to identify each client's **connectivity quality to Office 365**. It's even got it its **own portal.**



Manual Network Connectivity test to Office 365

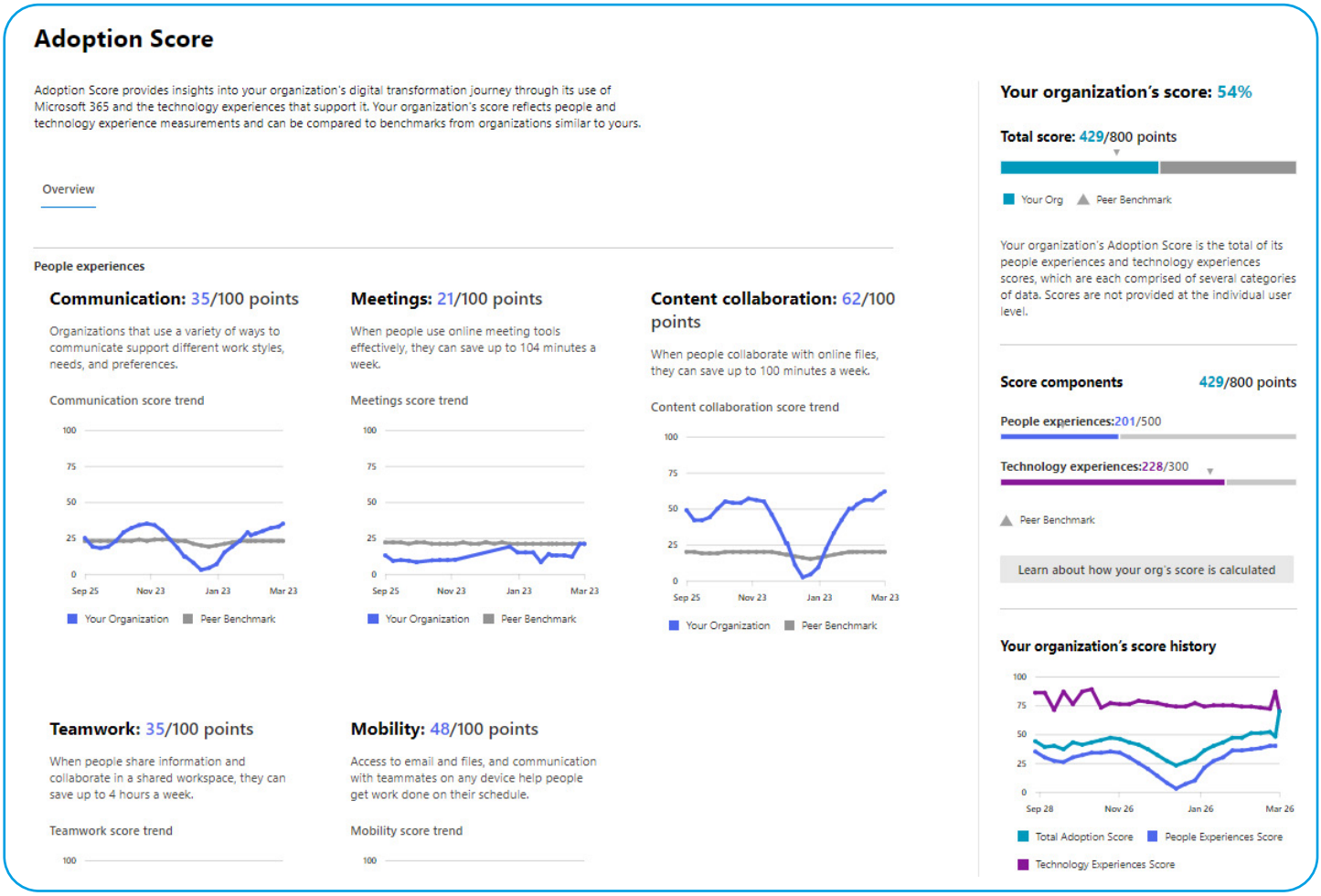
4.5: NETWORK CONNECTIVITY

Many businesses provide a substandard experience for their users by forcing them to use VPN connections back to the office and then onwards to Office 365 (overall a slower experience but a killer for Team's voice and video calls) or even proxying all outgoing traffic for "security". This last one is based in the erroneous assumption that all webservices / internet sites are "bad", and all traffic must be inspected, rather than differentiating between business services provided by Microsoft and others that can be trusted and dodgy websites and handling the traffic accordingly. Here's an **excellent article** outlining required and optional optimization

techniques for M365. Microsoft has also partnered with many ISPs, internet exchange partners (IXPs), and software-defined cloud interconnect (SDCI) providers for optimal connectivity to M365, Dynamics 365 and Azure using the **Azure Peering service.**

If your business is using a Software Defined WAN (SD-WAN) there's a feature called **informed network routing** that will further help optimize your connectivity by enabling data sharing between Microsoft and the SD-WAN provider to automatically reroute traffic where appropriate. Today only Cisco's IOS XE SD-WAN is supported but expect others to be added as the preview progresses.

The new **Productivity Score** is designed to help you understand where your business is at in its digital transformation journey and tracks metrics across two categories, People experiences and Technology experiences.



Microsoft 365 Adoption Score

4.6: MICROSOFT 365 DESIRED STATE CONFIGURATION

PowerShell has long had a feature called Desired State Configuration (DSC) – define how a system (VM, Application etc.) should look, apply the policy and the Local Configuration Manager ensures that the system has the right settings, checking periodically for drift. This is called Infrastructure as Code and is **now available for M365** so you could have a test tenant where you evaluate new configurations and settings which you can then export and apply to your production tenant. It can also be used to export all your configurations as a "backup", periodically reporting on changes in configuration and comparing your tenant's settings with best practices.

ENHANCE SPAM AND MALWARE PROTECTION
AVAILABLE IN
365 TOTAL PROTECTION
PLAN 4 - COMPLIANCE & AWARENESS
FREE TRIAL

CHAPTER 5:

CLIENTS

THERE ARE MANY PIECES OF SOFTWARE YOU CAN USE TO CONNECT TO M365 – IN THIS CHAPTER WE'LL LOOK AT THESE AND HOW YOU MANAGE THEM FROM A GOVERNANCE POINT OF VIEW.

5.1: DESKTOP CHOICES

Microsoft recommends the latest version of Chrome, Edge, Firefox or Safari or Internet Explorer 11 for accessing M365.

If you have the rich Office desktop client installed all supported versions should work with M365 but using the Apps for enterprise version for both Windows and Mac that's included with Business Premium and E3+ is preferred. You can **control which users get the recommended Current Channel** and who gets the Monthly Enterprise channel or the Semi-Annual Enterprise Channel flavor. If you want to live on the edge you can enroll in the **Office Insider program** to beta test new features.

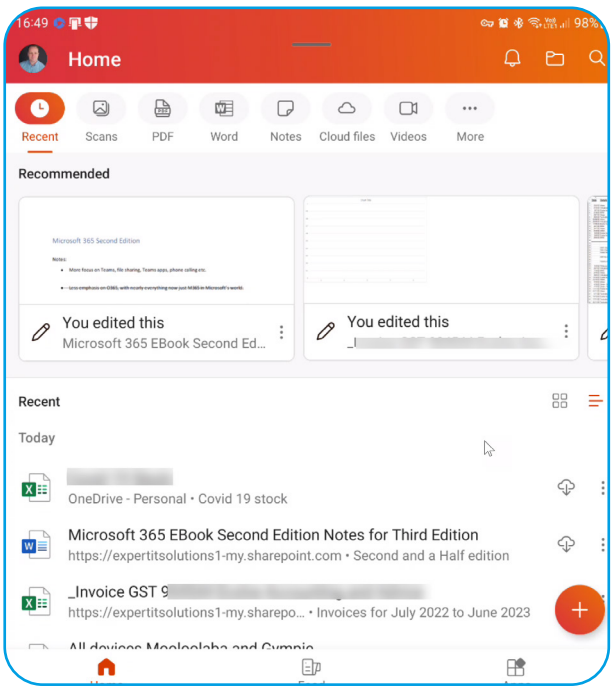
Outlook Web App (OWA) or Outlook for the web deserves special mention as it's extremely capable and not a "watered down" version of Outlook that runs in a browser. In fact, Microsoft often tests new features and approaches in the web client because they can deploy changes much quicker. You can use OWA policies to **control which features** are available to your end users.

You can control which protocols users can use to connect to Exchange with **Client Access Rules**.

5.2: MOBILE CHOICES

For many years the preferred way of connecting to Exchange online for email was to use ActiveSync, a protocol that both the mail client in iOS and Android supports (sort of – not all features were supported by each vendor). Microsoft now recommends using the free Outlook client app which lets Microsoft introduce new features much faster, without having to wait for Apple or Google to catch up. This app has been steadily growing in capability, including the ability to connect to Gmail and other email services and is now used by well over 100 million people.

There used to be separate Word, Excel etc. apps for mobile but they're all consolidated under the Microsoft 365 (Office) app that lets you open the different Office document types and edit them on mobile. It's free to install but functionality depends on what account you use to sign into it with.



M365 App (Office) on mobile

5.3: ONEDRIVE FOR BUSINESS

The sync client is automatically installed on Windows or Mac OS when Apps for enterprise is installed, and you can control its behavior using **this Group Policy template**. Please train your users to use OneDrive for Business – the power to have your files available on whatever device you happen to be using shouldn't be underestimated, particularly the ability to go to any device (if you don't have your own devices handy), sign in to **www.office.com** in any browser and edit those same files.

5.4: TEAMS

The Teams application (chapter 11) is Microsoft's all-in-one collaboration client with support for instant messaging chats, group chats, voice calls, video calls and if you have the licensing, PSTN calling to and from normal phones. Teams is replacing Skype for Business and starting in early 2019 the client is automatically installed when you install Apps for enterprise, if you need to deploy it using your favorite software deployment tool use this **MSI**.

At the time of writing a new Team's client app is in public preview which should fix the two main gripes people have with the current client: performance (the client is an electron app and uses a lot of CPU and memory) and swapping between different tenants.

5.5: APPS ADMIN CENTER

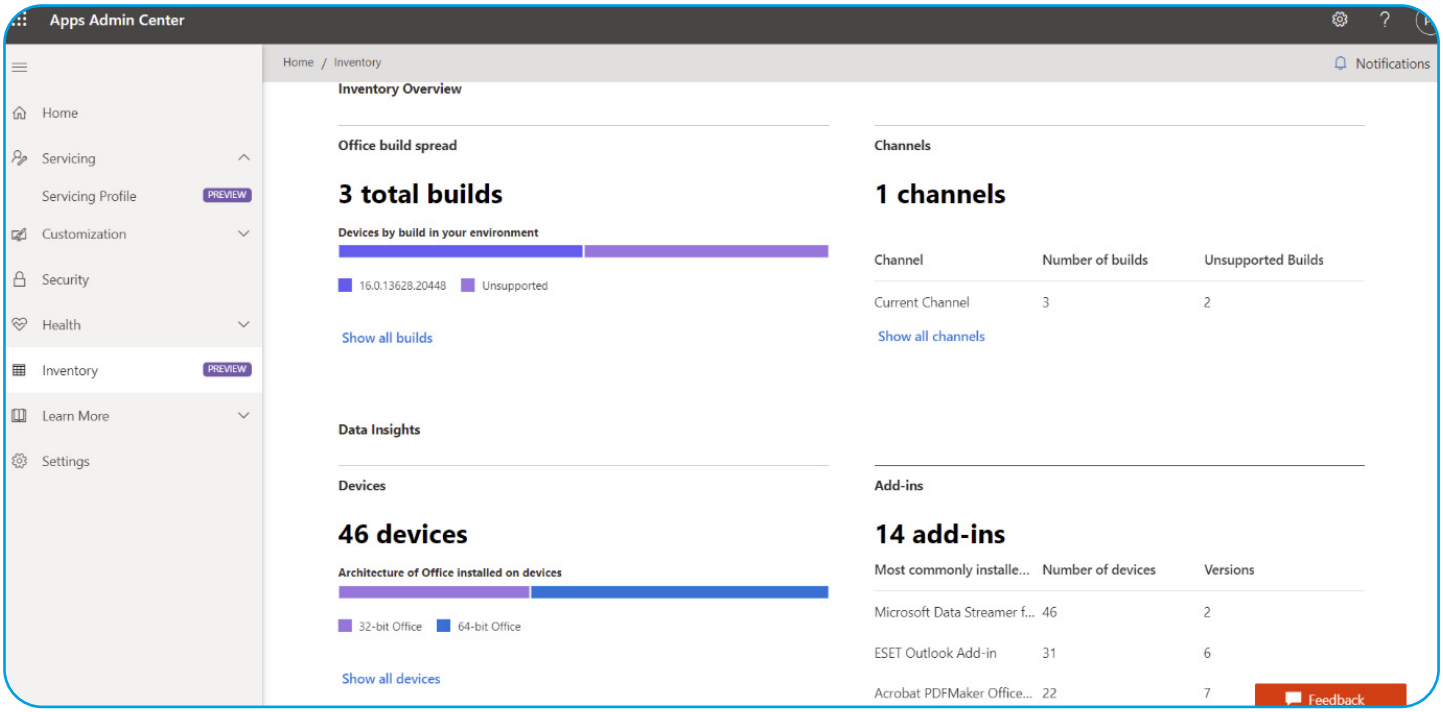
The Microsoft 365 Apps admin center is a very interesting take on cloud management for Apps for Enterprise (Office on the Windows desktop). Instead of managing the customization settings using the **Office Deployment Tool (ODT)** you use

the cloud portal to create the required XML files. The Apps admin center does so much more however. It inventories your Office installations across your tenant, tracks which versions and build numbers are installed, which ones are out of support and lets you build Servicing Profiles to deploy newer versions of Office. It also uses Security Policy Advisor to analyze current usage of the apps and lets you create and deploy policy configurations to all Apps for Enterprise installations (without relying on GPOs or MDM) plus tracks which add-ins are in use across all your devices.

If you have a large number of users, you may want to disable the option for users to download Apps for enterprise from **www.office.com** (M365 portal – Settings – Services & add-ins – Office software download settings) and instead deploy it using your favorite method. If your business is using System Center Configuration Manager, it can be used to **deploy and update Apps for enterprise.**
Since there's no additional licensing required for the Apps admin center, and you should investigate if it can make your life as an Office 365 administrator easier.

If you need to provide a modern printing environment for your users without having to bother with print servers or installing individual drivers for each printer on each device, consider **Universal Print.**

Another way you can tell how integrated the different components of M365 are, is with **Search**. This lets you search in various places in M365 and get relevant content for you, and only showing you content that you have access to, from within your tenant.



Apps Admin Center

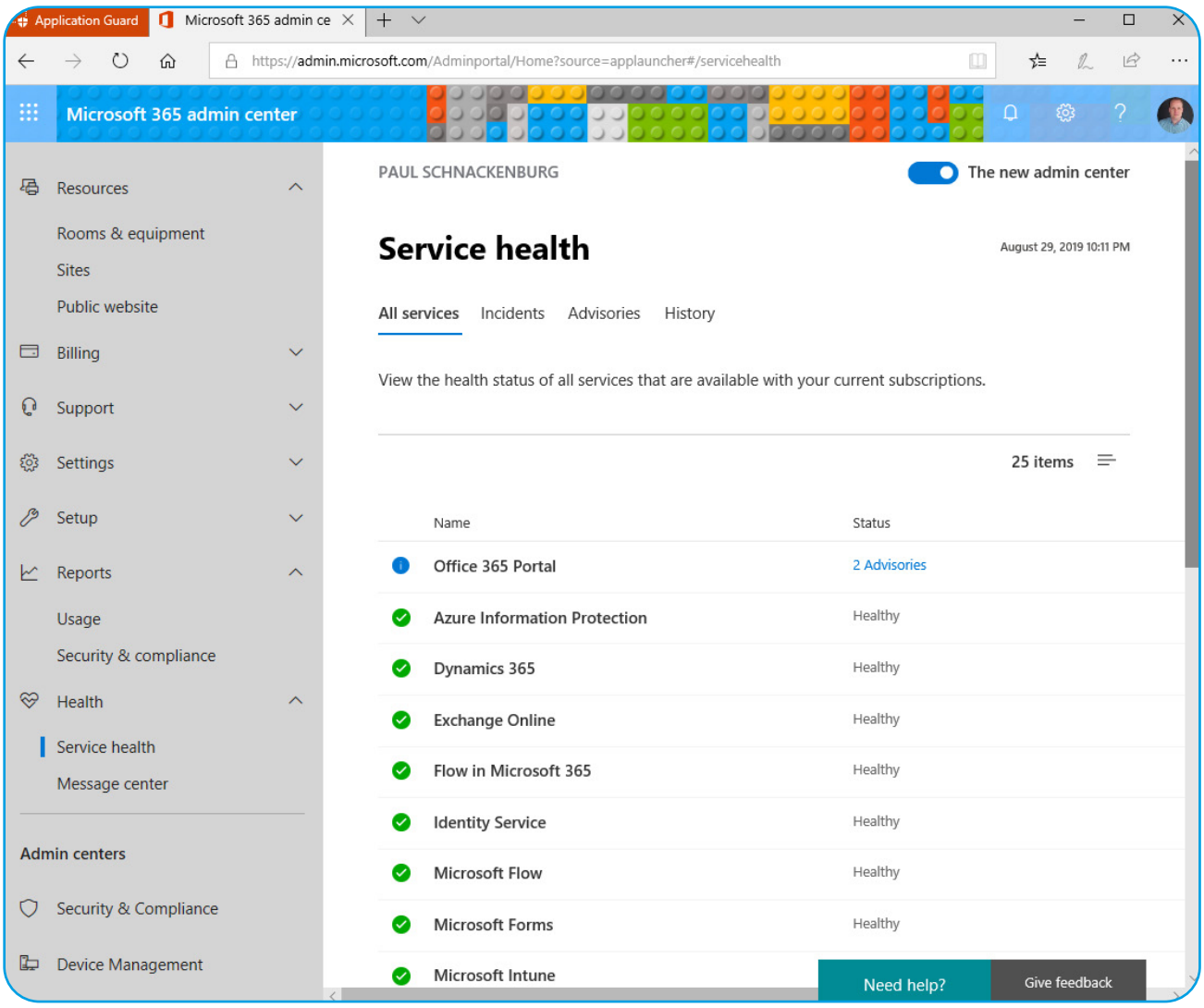
CHAPTER 6:

WINDOWS 11 ENTERPRISE

THE LAST PILLAR OF M365 IS WINDOWS 11 ENTERPRISE, FIVE DEVICES FOR EACH LICENSED USER WHICH WILL AUTOMATICALLY UPGRADE WINDOWS 11 PRO TO ENTERPRISE AS SOON AS A USER LOGS IN. IN THIS CHAPTER WE'LL COVER WHAT ADDITIONAL SECURITY FEATURES THIS BRINGS FOR YOUR ENTERPRISE.

6.1: WINDOWS 11 ENTERPRISE

Enterprise adds **Defender Application Guard**, and **Defender Application Control** on top of the security features you get in Windows 11 Pro. **Application Guard** protects your users when browsing potentially malicious sites using Edge in a hardware isolated manner. This technology has also **been extended to Word, Excel and PowerPoint.** **Application Control** on the other hand builds on earlier iterations of AppLocker and blocks untrusted applications from running, including plug-ins and add-ins.



Browsing in an Application Guard window

Always On VPN doesn't require Windows 11 Enterprise and is a successor to **Direct Access**, if you still need to use client VPN in your business.

Whilst it's not exclusive to Windows 11 Enterprise, look at **Windows Hello for Business** to improve your user's login experience as well as your security (a rare case of everyone wins in security) by moving away from passwords.

If you're deploying large numbers of Windows 11 devices and you want to reduce the burden of wiping each new device and installing your custom image, **consider using Windows Autopilot**, it's a powerful way to "deploy" Windows 11 by simply transforming the pre-installed image as it's delivered by your OEM.

PART 2

MANAGING, MAINTAINING AND SUPPORT FOR MICROSOFT 365

Herein we'll look at more advanced M365 features and configuration such as Entra for securing your user and workload identities, managing Exchange and SharePoint Online, Teams and how to centrally configure all your devices using Intune.

CHAPTER 7:

ENTRA ID

BEHIND M365 LIES A DIRECTORY WHICH HOLDS USER ACCOUNTS, GROUPS, AND OTHER SECURITY OBJECTS. FOR MANY YEARS THAT WAS KNOWN AS AZURE ACTIVE DIRECTORY, EVEN THOUGH IT HAD VERY LITTLE IN COMMON WITH ACTIVE DIRECTORY ON-PREMISES. AZURE AD WAS RENAMED TO ENTRA ID IN JULY 2023. IN THIS CHAPTER WE'LL LOOK AT ENTRA ID AND HOW YOU INTERACT WITH IT FOR M365.

7.1: ENTRA, PRIVA AND PURVIEW

Before we dive into Entra ID, let's look at the new portal where you'll be accessing it, **entra.microsoft.com**. All identity related services are housed here, whereas all Information Governance related features are in **compliance.microsoft.com**, called the Purview portal (Chapter 14), and it's got a section with all the privacy related features called Priva.

Apart from Entra ID, the Entra portal also houses **Entra Permissions Management** which inventories and right sizes administrative permissions across Azure, AWS and GCP (IaaS and PaaS) – not related to Microsoft 365 permissions. There's also Verified ID that will help in the future with new hires and managing external identities, and Global Secure access – however, these are outside the scope of this book.

7.2: MEET ENTRA ID & HYBRID IDENTITY

AD uses Kerberos and Group Policy, has a hierarchical structure, and is based on LDAP, none of which are cloud friendly. Entra ID operates over HTTPS, can be accessed from a REST API, and supports modern authentication protocols such as Security Assertion Markup Language (SAML), WS-Federation and OpenID Connect for authentication and OAuth for authorization. It also supports federation so you can connect it to other authentication systems.

There are three types of authentications supported in Entra ID: **Cloud based, Directory synchronization** and **Single Sign On (SSO) with AD FS.** The first one is appropriate when you don't have AD on premises (or you want to retire it) and you create accounts in the cloud only. It's definitely the simplest to configure. The other two require you to link your on-premises AD to your Entra ID tenant through the free **AAD Connect** tool.

7.3: AAD CONNECT – YOUR UMBILICAL CORD

AAD Connect (will presumably be renamed to Entra ID Connect) has had several predecessors over the years with different names – if you find an installation using DirSync or AAD Sync make sure to upgrade to AAD Connect as those tools are no longer supported. AAD Connect **supports connecting multiple on-premises directories to AAD**. There was also version 1 generation of AAD Connect which is deprecated, you should be using version 2, which updates itself automatically.

You can install the tool directly on a DC or on a member server. There's no true active / active HA option but you can set up a second installation of **AAD Connect** on a separate server in **Staging mode** and do a manual failover if the primary server is going to be offline for some time.

AAD Connect will synchronize user and group accounts in OUs you select (or the entire directory – not recommended) to Entra ID. You then assign licenses to those user accounts, and they can start using cloud services. Note that this also means that on-premises is always the place to create new accounts, and update, disable or delete existing ones.

There are a **few choices** in how you handle passwords in AD. The simplest one is to use **Password Hash Synchronization** which takes on-premises password hashes, hashes them again with a modern algorithm and stores the hash of the hash in the cloud. This gives your users SSO (even though technically it's "same sign in" as the two user accounts are in two different directories). Another benefit of this method is that Microsoft can alert you when they find credentials on the web / dark web with accounts from your tenant where the passwords match.

If you're adamant that your user's passwords can't be stored in the cloud (**not even a hash of a hash**), **Pass-through authentication (PTA)** is another option. You **set up agents** on several (minimum 3, maximum 40) Windows Server 2012 R2+ servers (no inbound ports required) and when a user signs in at **www.office.com** for instance, Entra ID will verify that the correct password is supplied by communicating with your AD on-premises through the PTA agents.

Both PTA and Password hash sync optionally lets you enable **Seamless Single Sign On** (Seamless SSO) where the user logs on to AD and when they access **www.office.com** they're automatically logged in.

A companion is **AAD Connect Cloud Sync**, which is configured from the cloud and only relies on lightweight agents on-premises, this also means

you have High Availability built-in, as long as you deploy multiple agents. Cloud Sync has slowly been gaining feature **parity** with AAD Connect and the main features missing today are support for device objects, the ability to sync from non-AD LDAP directories, PTA support, some filtering options and large groups with over 250,000 members. The blocker for many though will that there's no support for Exchange hybrid writeback. I expect Cloud Sync to eventually replace AAD Connect.

The traditional way of not storing password hashes in the cloud is to use **AD Federation Services (ADFS).** This is **much more complex and requires several servers** to be set up on-premises (or as VMs in Azure) but does offer more flexibility. If your organization has already deployed AD FS for other purposes, setting up federation with O365 is not a huge project but my (and Microsoft's) recommendation is to stick with PTA or Password Hash Sync. Given the Solarwinds supply chain breach and subsequent intrusion into various organizations using ADFS, along with Microsoft's recommendation over the last few years to migrate from ADFS to Azure AD, if you have ADFS deployed, it's **time to make the move** to Azure AD.

7.4: AZURE MFA

One of the best things that Entra ID unlocks is the easy set-up of Multi Factor Authentication (MFA) for users. Passwords are one of the weakest links in today's IT landscape and the majority of the breaches we see are due to someone's credentials being compromised. One solution to this problem is using MFA (sometimes known as 2FA or two step authentication) where authentication not only requires a username and password but also a device or a biometric gesture to be present. This drastically reduces (by **99% according to Microsoft**) the success of credential attacks.

MFA can call your phone, send a text message with a code, or send a notification / require a code from the free **Microsoft Authenticator app**. Unless absolutely required, do not use phone call or SMS, they're more insecure than the app options.

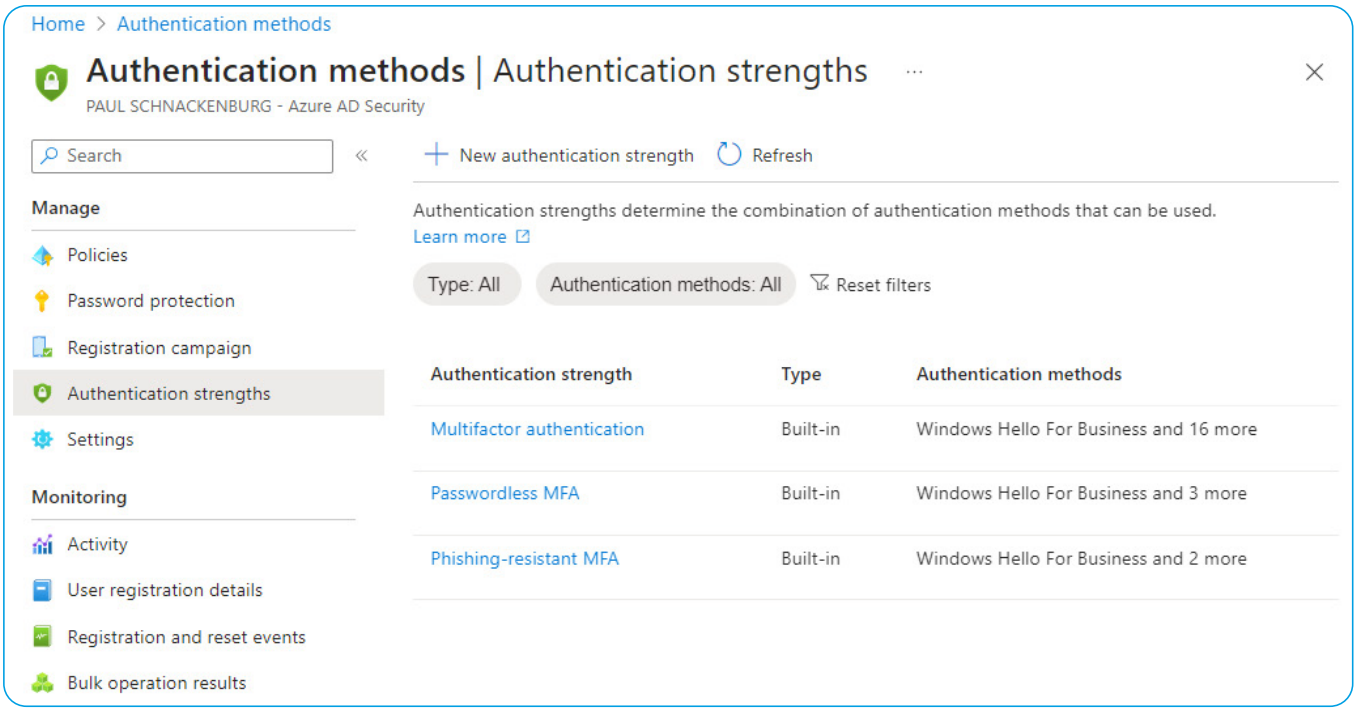
As a baseline all your privileged accounts (Global / Exchange / SharePoint / Compliance administrators etc.) MUST use MFA. **This is free at all tiers of O365** and is **simple to set up** and the user experience is relatively seamless if you install the app on your smartphone. If you're an IT decision maker, expect to receive pushback from your administrators on this point but to maintain an acceptable security posture, this step is non-negotiable – all administrators HAVE TO use MFA. As an aside I've been using Azure MFA for my own business tenant and all my client's tenants that I administer for many years now without issues.

You must however plan for times **when Azure MFA is unavailable** and this includes creating one (preferably two) Global Admin cloud accounts that are exempt from MFA and any CA policies. These accounts should have very long and complex passwords that are only available to high-ranking administrators and should have monitoring enabled so that if they're ever used alerts go off. These break glass / emergency access accounts should only be used to recover user access, for instance if Entra ID MFA is down you might disable MFA requirements for the duration of the outage to enable users to login and be productive.

Enabling MFA for your end users requires some planning and end user training. The level of tech familiarity your users have and whether they're normally working from corporate offices influences how to implement MFA. Administrators always get

MFA for free, if you're on the Business SKUs MFA its built in but both lack the advanced features that Entra ID Premium P1 (M365 E3) or Entra ID Premium P2 (M365 E5) offer. These include One-time bypass, Trusted IPs/**Named locations**; which lets you define corporate office IP address ranges where users will not be prompted for MFA. Note that all MFA levels let you (if you allow this feature) remember MFA on a trusted device for a set number of days (7-60). If a user has logged on to a device and successfully performed MFA, they won't be prompted on that device for the time period and if the device is lost or stolen either the user or you can "un-trust" these devices easily. Starting in May 2023, Microsoft enabled number matching for all Microsoft Authenticator approvals, so instead of just pressing Approve or Reject, you must enter a two-digit code shown on your computer screen. The app will also show you the geographical location that the MFA request comes from. Both features are designed to combat MFA fatigue attacks, where the attacker repeatedly tries to login, generating so many requests on your phone that in the end some users simply press Approve to make it stop.

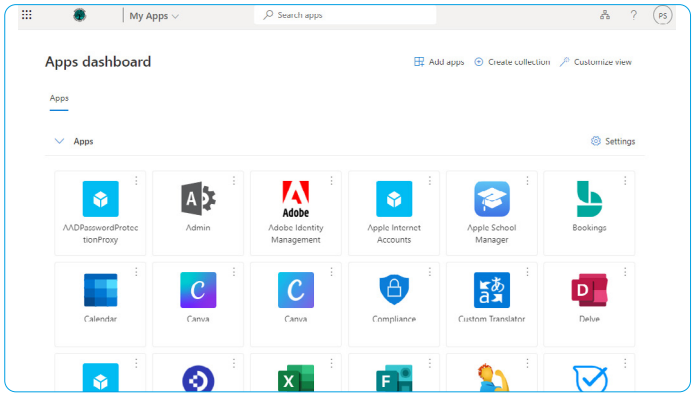
Microsoft now enables **Security Defaults** for all new tenants, and you **can enable it manually** for your existing tenants. This will enforce MFA for all users and administrators, using the Microsoft Authenticator app only, blocks legacy authentication (see chapter 15) and controls access to the Azure AD portal. While these security enforcements are a good starting point for a small business with limited requirements, I advise caution for more complex organizations, as there's no way to exclude break glass accounts or service accounts from MFA, or ways to handle users who don't have / can't access the authenticator app on a phone.



MFA Authentication Strengths

7.5: PUBLISHING APPLICATIONS

One of the most powerful features of Entra ID is the ability to **publish applications** (third party and **on-premises**) to your end users. These show up right next to the normal Office applications at **myapplications.microsoft.com** or **www.office.com** for users to launch with a single click.



MyApps portal

Take a corporate Twitter account for instance where several users have the username and password to send tweets on behalf of the company. Not only will you need to reset the password as soon as someone leaves the company (you don't want them tweeting as your organization after they've been fired) but you have little control over who else that password is shared with. If you publish Twitter through Entra ID and create an AD group to put users in that should have access, you simply add a user account to that group, they'll automatically have single-sign-on access to Twitter in the My Apps portal without ever knowing the password and once they leave the company and their account is disabled, they can't access it any longer. For some out of the 2400+ applications supported out of the box you can even configure **automatic provisioning** so that when you add a user to the AD Salesforce group an account is automatically created for them in Salesforce – again without them even knowing the password to it.

A popular option is using the AWS Single Sign-On app **to integrate AAD and AWS**.

7.6: PREMIUM FEATURES

Entra ID Premium P1 doesn't just unlock more MFA features, it also allows you to **ban commonly used passwords** in your on-premises AD (including **a custom word list**), enable users to **reset their own passwords** when they have forgotten them, integrate **MFA with Conditional Access** and let users register for both MFA and self-service password reset (SSPR) in **the same experience**.

AUTOMATE MICROSOFT 365
BACKUP AND RECOVERY
AVAILABLE IN
365 TOTAL PROTECTION
PLAN 4 - COMPLIANCE & AWARENESS
FREE TRIAL

The P2 level adds the full experience of Entra Identity Protection where you get **reports and can block authentications** based on the risk level of the user account and the sign in or even trigger an **"extra" MFA prompt** based on the risk profile of the authentication attempt. P2 also offers **Privileged Identity Management (PIM)** where you convert all administrative accounts to eligible accounts and users have to request elevation when they need to perform administrative tasks (known as "Just in Time administration").

Instead of assigning administrative roles in Entra ID to individual user accounts you can **now use groups to grant admin access**. The groups need to have a specific attribute set (isAssignableToRole) to true and static (rather than dynamic – automatically assigning user accounts to a group based on an attribute like "department" in the directory) user account membership.

Where AD has a hierarchical structure, relying on Organizational Units (OUs) to structure your user, machine and group accounts based on department, geography, or other approach, Entra ID is a flat structure. **Administrative Units (AUs) is a feature** that aims to change this, using AUs you can structure user and group accounts and then **delegate administrative permissions** to a single AU or AUs. The AU admins need Entra ID Premium licensing. Note that unlike OUs where an account can only be in a single OU, a group or user account can be a member of multiple AUs (up to 30).

If you have a large environment and Premium P2 licenses, consider using **entitlement management**, a way to group application, group membership (including Teams) and site access into a single access package. These are useful for internal users ("you are the new person in Marketing – here's your package that gives you all the access you need") and can also be used to grant access to external users. For partner organizations that you work with frequently you can even set it up so that their users can apply for packages, self-service style. Entitlement management can also get IT out of the role of assigning permissions by delegating package assignment to business users.

7.7: CONDITIONAL ACCESS POLICIES

Both P1 and P2 unlocks another powerful feature in Entra ID, **Conditional Access (CA)**. This lets you build policies around application access (both cloud an on-premises applications) based on the user account and what groups they're a member of, which application they're accessing, the state of their device, their location, the sign-in risk and which type of client application they're accessing it from. These "if this – then do that" rules greatly enhance the security of your data by managing risk factors affecting identity and access in M365.

Making it even easier to set up good CA policies are **templates** (in preview at the time of writing) covering Secure foundation, Zero Trust, Remote work, Protecting administrators and Emerging threats.

To make sure you don't create a policy by mistake that locks out the CEO five minutes before his board presentation, the option to deploy CA policies in **Report-only mode** lets you evaluate the impact the policies will have without actually enforcing them.

There's an **API for accessing CA policies**. This makes it possible to backup (using PowerShell for example) your CA policies, restore them, monitor changes, and treat them as code rather than manually manage them in the portal. You could also test policies in a test tenant before exporting them from there and importing them in your production tenant after they pass validation.

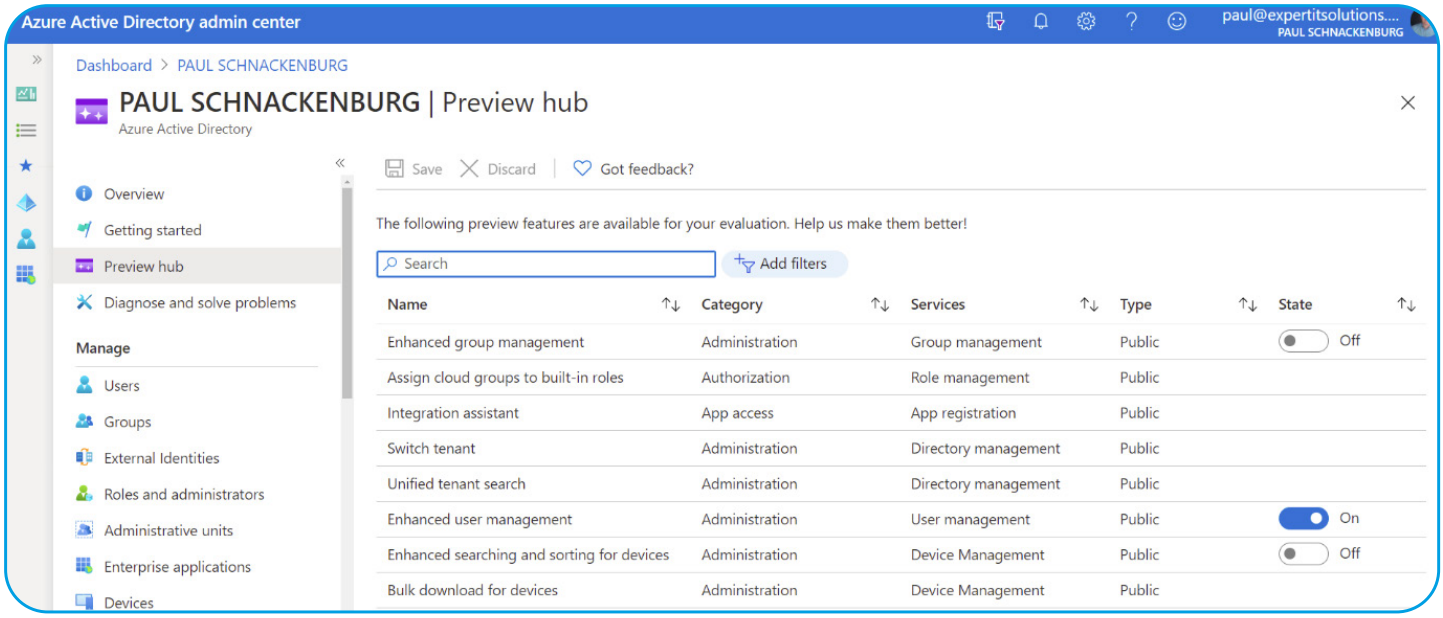
7.8: MANAGING THE ACCOUNT LIFECYCLE

Once you implement AAD Connect make sure you update your process documentation to consider the full lifecycle of user accounts, such as making sure they're given the right licenses, are added to the right groups, and when the time comes to disable the account the **right steps** are followed.

To make sure that users (and guests) don't accumulate access that they no longer need, **use Access Reviews** (Premium P2) which now lets you **review all guest accounts in one operation**, rather than on a per Team/M365 Group basis.

For a smaller O365 or M365 tenant chances are you'll never even need to go to the full Azure AD portal and instead you'll just do your user management in the M365 portal (Chapter 2). It's a good idea however to explore the "full" Entra portal over at **https://entra.microsoft.com.**

If you're keen to try out upcoming features in Entra ID, use the Preview hub to learn about and turn on public preview features.



Azure AD Preview hub

CHAPTER 8:

EXCHANGE ONLINE

EMAIL IS THE LIFEBLOOD OF BUSINESS COMMUNICATION, EVEN IN THIS AGE OF TEAMS AND SLACK AND NUMEROUS OTHER COMMUNICATION TOOLS. IT'S THE LOWEST COMMON DENOMINATOR – THE ONE TOOL THAT YOU CAN ALWAYS USE TO REACH SOMEONE IF YOU'VE GOT THEIR EMAIL ADDRESS. AND EMAIL IS A COMMODITY – EVERY BUSINESS NEEDS IT, BUT NO BUSINESS IS GOING TO BE MORE COMPETITIVE BY RUNNING IT "MORE EFFICIENTLY" THAN ANOTHER.

8.1: IT'S A HYBRID WORLD

One of the strengths of M365 over Google Workplace for instance is the clear migration path from what you have today to the cloud, because of Microsoft's large footprint in corporate datacenters around the world.

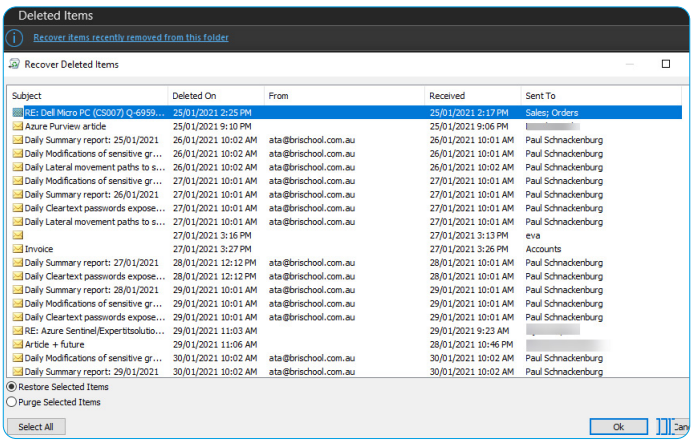
If you have Exchange 2013+ on-premises you can pick any of the migration methods we looked at in chapter 3, some of which provide a hybrid co-existence. The full hybrid option lets you continue running your on-premises infrastructure for as long as you'd like and move mailboxes in batches to the cloud on your own schedule. You can even move mailboxes back to on-premises should the need arise. As you'd expect there are many details to manage in a **hybrid setup**, including **prerequisites**, **ActiveSync connectivity** and **mailbox permissions** – especially when a user on-premises has permissions to a mailbox in the cloud or vice versa.

If all you're looking for is a simple way to move mailboxes from Exchange to Exchange Online – Hornetsecurity has a great **Mailbox Migration Tool.**

8.2: BACKUP AND NATIVE DATA PROTECTION

One thing to realize about O365 is that Microsoft is going to make sure that you don't lose your mailbox data which they do through the native data protection in Exchange – keeping three copies of your mailbox data on separate servers, along with a "lagged copy" (behind in time, for instances where the data is corrupted rather than lost) on a fourth server.

They DON'T, however, keep backup copies of your data going back into the past which may or may not be an issue for your business, depending on your regulatory needs. There are several third-party services on the market which will do backups of your Exchange and SharePoint online data. Hornetsecurity **365 Total Backup** is an excellent backup solution, for mailboxes, Teams, OneDrive for Business, SharePoint and files on endpoints **see chapter 16**.



Recover Deleted Items in Outlook

A deleted user account and mailbox can be recovered if no more than 30 days have passed.

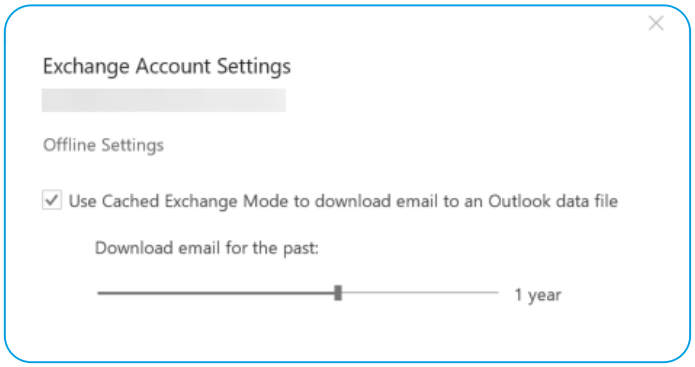
8.3: AUTODISCOVER

Whether your Exchange server is in the cloud or on-premises it's important that client applications can find it – this is the job of the Autodiscover records in DNS. There are a number of other DNS records required for M365 – find them in **this article.**

If you have a hybrid Exchange deployment the Autodiscover records need to point to your on-premises Exchange 2016/2019 Mailbox Server.

8.4: MANAGING MAILBOXES

There are many tasks associated with mailbox management, one of them is **quota management**. F3 licenses get 2 GB quotas, E1 are set at 50 GB (with a 50 GB archive) and E3+ have 100 GB quotas with archive mailboxes that can be max 1.5 TB. The difference between a mailbox and an archive mailbox is that the archive is only available when you're online. You can control how much mailbox data is stored offline on each device with a slider in Outlook.



Outlook offline cache setting

If you're migrating large mailboxes to Office 365, ensure they're smaller than 100 GB and no item is larger than 150 MB before starting the move.

In the Exchange console you can configure settings for a mailbox such as adding email aliases, see quota usage, control which clients (OWA, Unified Messaging) and the protocols (EAS, MAPI, IMAP and POP) the user can use, message retention and mailbox delegation. This last option lets you configure other users to **Send As** emails as the user, **Send on Behalf** where the recipient can see that the email is sent on behalf of the user, and **Full Access**.

8.5: MAILBOX ARCHIVE

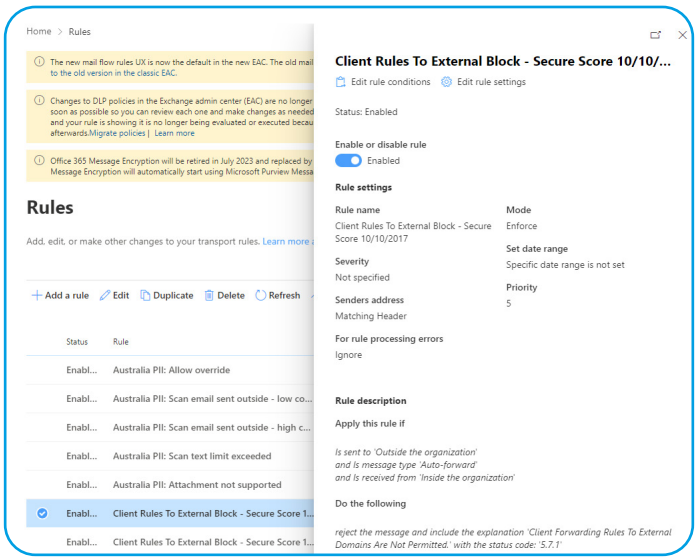
As mentioned earlier you can enable an Archive mailbox for mailbox content which essentially serves as a "bottomless" storage area for older content, hopefully stopping users from adopting PST files as an archiving solution. The Outlook mobile client (iOS and Android) cannot access Archive mailboxes. You can enable **auto expanding archives for E3 and E5 licensed users** using PowerShell:

```
Set-OrganizationConfig -AutoExpandingArchive
```

You can also enable Archive mailboxes on a per user basis. Note that the Archive folder that's created in a mailbox when you right click an item and select archive isn't related to the Archive mailbox.

8.6: MAIL FORWARDING

Be aware that users can set up their mailboxes to forward mail to an external email address (optionally delivering to both inboxes). This is something you should keep an eye on because while there may be legitimate business reasons to forward mail, it's also a favored attack vector for hackers where they silently read emails and then use that for various nefarious purposes. There's a report in the Mail Flow dashboard to show you what forwarding rules exist. You can also block **users from being able to forward mail** in several ways.



Mail Flow rule to block exterternal email forwarding

8.7: SHARED MAILBOXES

There are times when you'd like a mailbox that doesn't "belong" to a particular user such as sales@ or support@ where you have a team of users accessing the same alias. As long as the **Shared mailbox** doesn't have a larger quota than 50 GB or uses an Archive mailbox it won't consume a license. It's also one option for handling staff that have left your company while you still need to monitor their email for incoming emails, converting their mailbox to a shared mailbox and assigning access to the appropriate staff will free up the license to be assigned to a new user. From a security point of view, make sure direct login to shared mailboxes is blocked – users should only access shared mailboxes by adding them as an additional mailbox in Outlook.

8.8: MAIL CONTACTS AND USERS

Both Mail **Contacts** and **Users** show up in All contacts, the Global Address List (GAL) and the Offline Address Book (OAB). A **contact** is a pointer to an email address in an external system, whilst a **user** is also a pointer to an external address, but the user has O365 credentials to be able to access SharePoint Online or OneDrive for Business. The latter is a remnant of on-premises Exchange, modern external sharing such as Teams, Planner and others use **Azure Business to Business (B2B)** collaboration for guest access.

8.9: DISTRIBUTION LISTS

Grouping email addresses together to facilitate communication with teams of people is something that email systems have been doing for decades – in the Exchange Online Admin Center (EAC) you can create Distribution Lists (DL). Note that the default is to create an **M365 Group** instead and in fact **Microsoft is pushing to replace DLs with Groups**. **Dynamic Groups** make maintaining membership easier, basing the membership on an Entra ID attribute such as "department" – if that's set to Marketing for instance, the user is automatically included in the right group.

TAKE CONTROL OF
MICROSOFT 365 PERMISSIONS
EFFORTLESSLY
AVAILABLE IN
365 TOTAL PROTECTION
PLAN 4 - COMPLIANCE & AWARENESS
FREE TRIAL

CHAPTER 9:

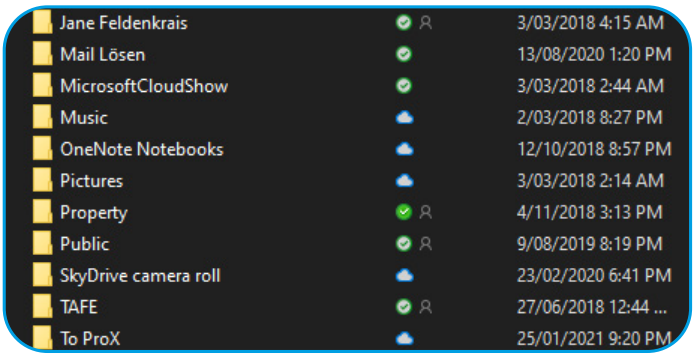
ONEDRIVE FOR BUSINESS AND SHAREPOINT

SHARING FILES AND PROVIDING AN INTRANET PLATFORM IS A CORE PART OF M365, IN THIS CHAPTER WE'RE LOOKING AT ONEDRIVE FOR BUSINESS (OD4B) FOR PERSONAL FILE STORAGE AND SHARING AS WELL AS WEB-BASED COLLABORATION IN SHAREPOINT.

9.1: ONEDRIVE FOR BUSINESS

OD4B builds on SharePoint Online to provide each licensed user with their own document storage; 1TB for most SKUs. This quota **can be increased** to 5 TB for certain licenses.

As mentioned, once you store files in OD4B you can access them from any device, through clients for Android, iOS, Windows, MacOS and a web interface. There are **some limitations** on file names, types and sizes to be aware of. The OD4B sync client lets you **see all files** on a device that you have synced, they can be in an **Online-only** state where you see them but they're not actually present on the device, when you open such a file it's downloaded and cached and thus **locally available**, a user can also pick one or more files to **always keep on this device.**



Cloud only local and pinned files in OD4B

You can restrict synchronization to only **domain joined devices**. To help users manage the contents of common folders you can use **Known Folder Move (KFM)** to synchronize the content of the Desktop, Documents and Pictures folders to OD4B and thus between devices.

9.2: SHAREPOINT

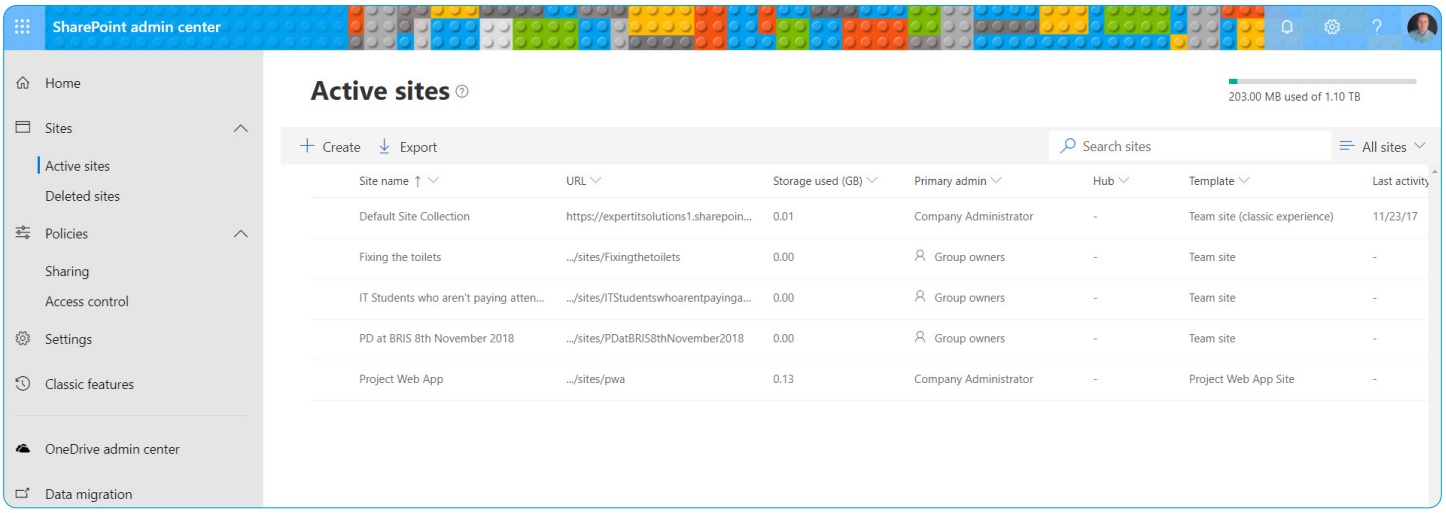
If you're an on-premises SharePoint administrator, you'll be familiar with managing the underlying infrastructure of your servers as well as the complex web of sites and document workflows that end users consume on top of it. If you're only now meeting SharePoint in the cloud for the first time, you'll likely have a very different experience where you see SharePoint simply as the underlying document storage for other applications (Teams, Groups, Planner) and perhaps as the platform for your company's intranet.

Building blocks in SharePoint are **sites** where content is stored, and you can control the layout, theme, navigation, and security with classic and modern flavors. If you're starting out or creating new sites, Modern sites are **the way to go** and there are a few different types available such as **Communication sites**, **Team sites** and **Hub sites**. Part of a larger vision for SharePoint, the modern sites and pages are very useful as they adapt to screen resolutions across smartphones and different size computer screens.

Search lets you find sites, files (including OneDrive for Business files), people and news content and if there are pictures in the content Artificial Intelligence (AI) will have extracted metadata and (if present) text content from those images. If you have configured a **hybrid deployment** your on-premises documents will show up in the search results as well. **Apps** are add-ins / Web parts that expand the functionality of sites and **Site collections** are a way to group sites with a similar purpose together.

To set up different sites, use **site templates** to get you started. If you're creating an intranet site, there's an excellent **Lookbook service** with beautiful sites, providing modern experiences.

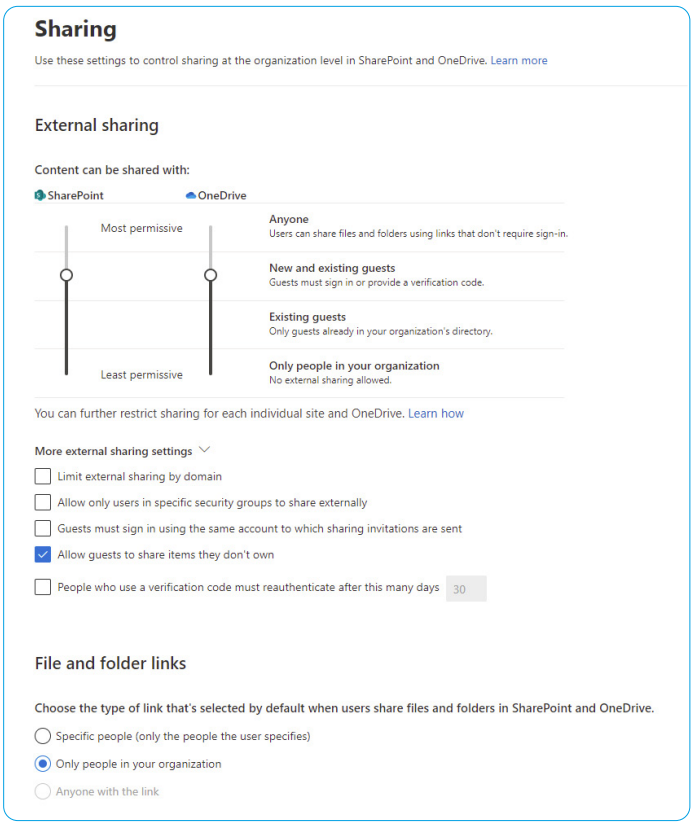
SharePoint Syntex is a technology that uses AI and ML to automate content processing and transforms content into knowledge. It understands your documents, processes forms and is applicable to large organizations with complex workflows and processes.



SharePoint Online Admin Center

Be aware of the **limits of SharePoint Online**, particularly the total storage available which is 1 TB + 10 GB per license purchased. Search is an area that you want to **spend some time customizing** so your end users have a good experience. Sharing is another area that you want to control as **how users can share content** internally and (critically) externally directly influences the balance between collaboration and security.

Migrating content from on-premises SharePoint Server and network file shares to M365 is the job of the **SharePoint Migration Tool,** as well as numerous third-party services. If users accidentally delete files or ransomware has encrypted stored files you can use the **Restore Files** interface to restore files and folders or entire libraries from up to 30 days in the past. There's also the **Recycle bin** (93 days retention) for individual file restores and **Restore Files** for OneDrive.



SharePoint and OD4B external sharing control

CHAPTER 10:

MICROSOFT 365 GROUPS

M365 GROUPS ARE A BASIC BUILDING BLOCK ACROSS DIFFERENT SERVICES, IN THIS CHAPTER WE'LL LOOK AT THE DIVERSE USES OF THEM.

10.1: GROUP TYPES

An area that often confuses new O365 administrators is the different types of groups, here's a short rundown to sort it out:

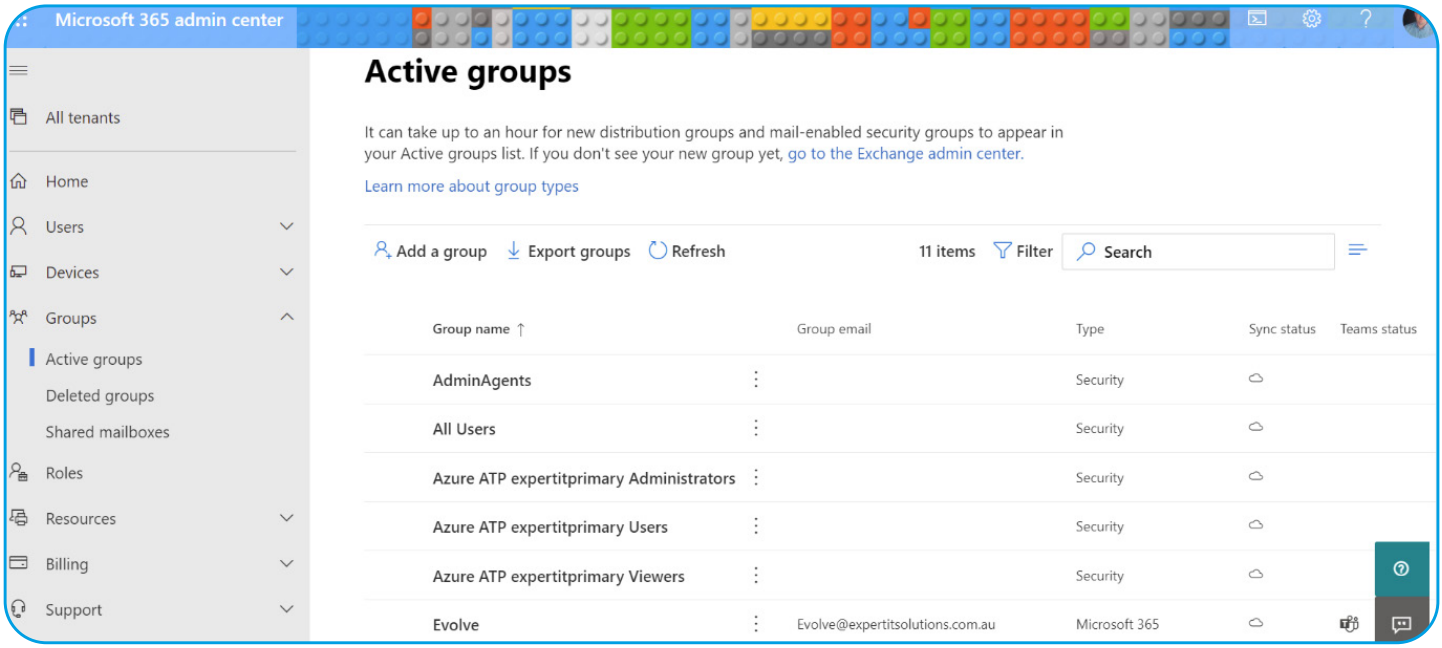
- **Microsoft 365 Groups** (the type covered in this chapter)
- **Distribution Groups** (Chapter 8)
- **Security Groups** are used to grant access to resources
- **Mail-enabled Security Groups** are also used to grant access and can also be emailed which will mean all members will receive a copy of the email
- **Shared Mailboxes** (Chapter 8)

While you can create Microsoft 365 Groups directly, you're more likely to interact with them as a building block, providing a single identity for all of M365, that services such as Teams, Yammer and others use. In addition, Outlook can use M365 groups, SharePoint Modern Team sites are built on them, and Stream and PowerBI use them to control access.

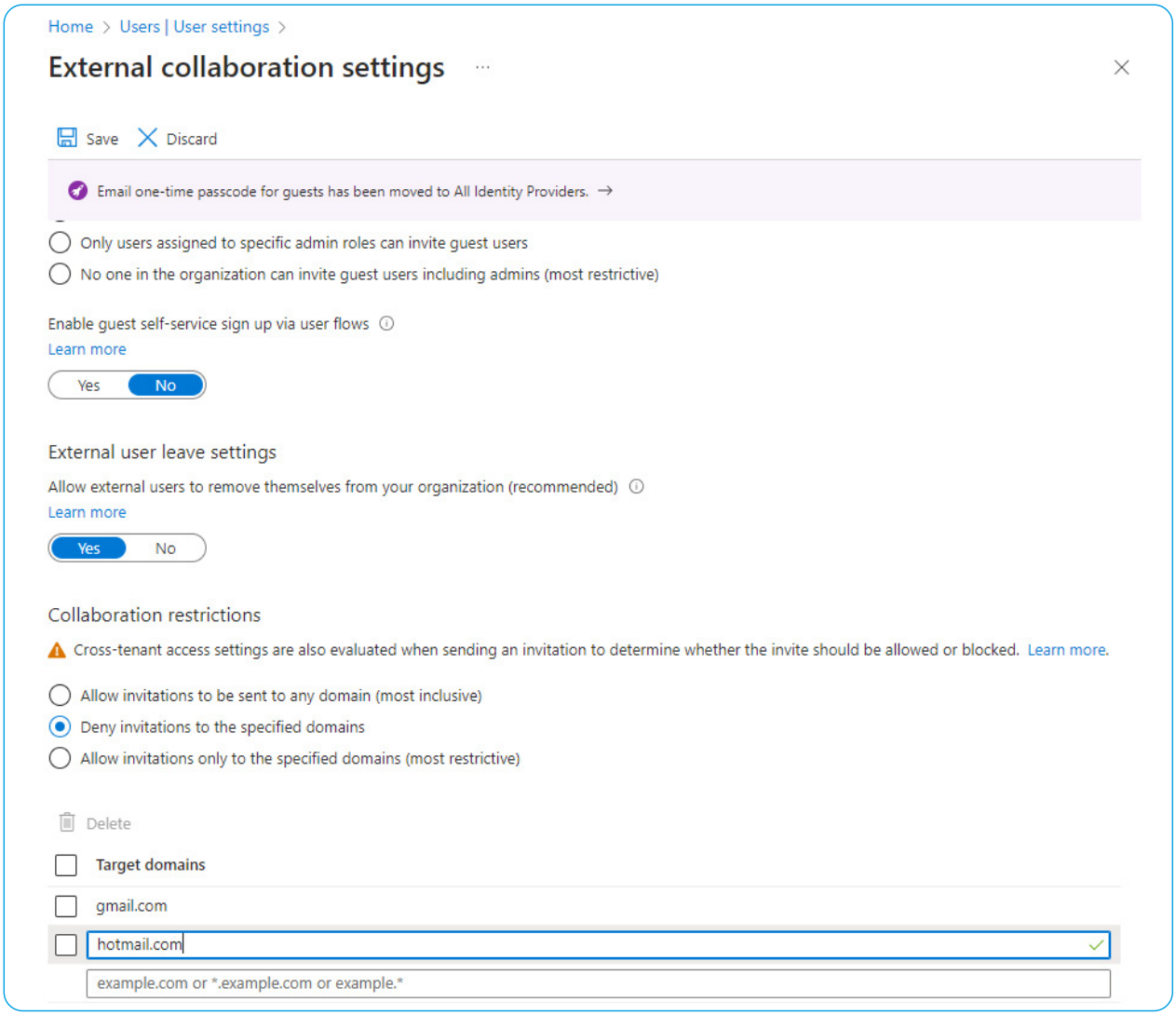
If configured thus you can write M365 Groups back to your on-premises AD where they manifest as distribution groups. You can't nest M365 Groups into other groups, and they can only contain actual M365 user accounts whilst Exchange Distribution groups can contain user accounts, mail users and contacts (see Chapter 8). Unless you've changed the defaults, any user in your tenant can create an M365 group which could **lead to governance issues.** You can instead **designate users** who can create groups. You can also use various **policy settings** to control O365 Group behavior in your tenant, such as **expiration policies** to manage the lifecycle of groups and you can control the **naming of groups** through policy.

It's easy to share content from within an M365 group with external users and M365 groups are also a shared repository of historical content as anyone who is a member can see all the content going back to when the group was first created. It used to be that each licensed user in your tenant gave you five B2B **guest licenses**, and you could use **one time passcodes** for external guests who don't have a Google, Microsoft Account (MSA) or an account in Azure AD.

That licensing model for external users has changed, Microsoft is bringing together Azure B2B and B2C (using Azure as a store for Consumer identities for your in-house developed application) and the new license model means each tenant can have up to 50,000 external users at no extra cost. Note that guests have full access to all group content by default. You can **control which domains** external users have to be (or can't be from) for external access.



Groups in the M365 Admin Center



External Collaboration settings in Entra - blocking specified domains

Today when you create a group it's **private** where the Owners of the group must approve a request to join, you can also make a group **public** where anyone can join. You can change the tenant default which will ensure new groups are public or you can change the setting on a group after you've created it. Each group can have up to 100 owners and over 1000 users; an individual user cannot create more than 250 groups. Like other constructs in M365 you have 30 days to **restore a group** once it's been deleted while individual documents in the group are housed in the SharePoint recycle bin for 93 days.

Dynamic groups are a neat way to reduce the administrative overhead of managing group membership manually, based on queries of Entra ID attributes, although be aware that it requires Entra ID Premium P1 licensing.

CHAPTER 11:

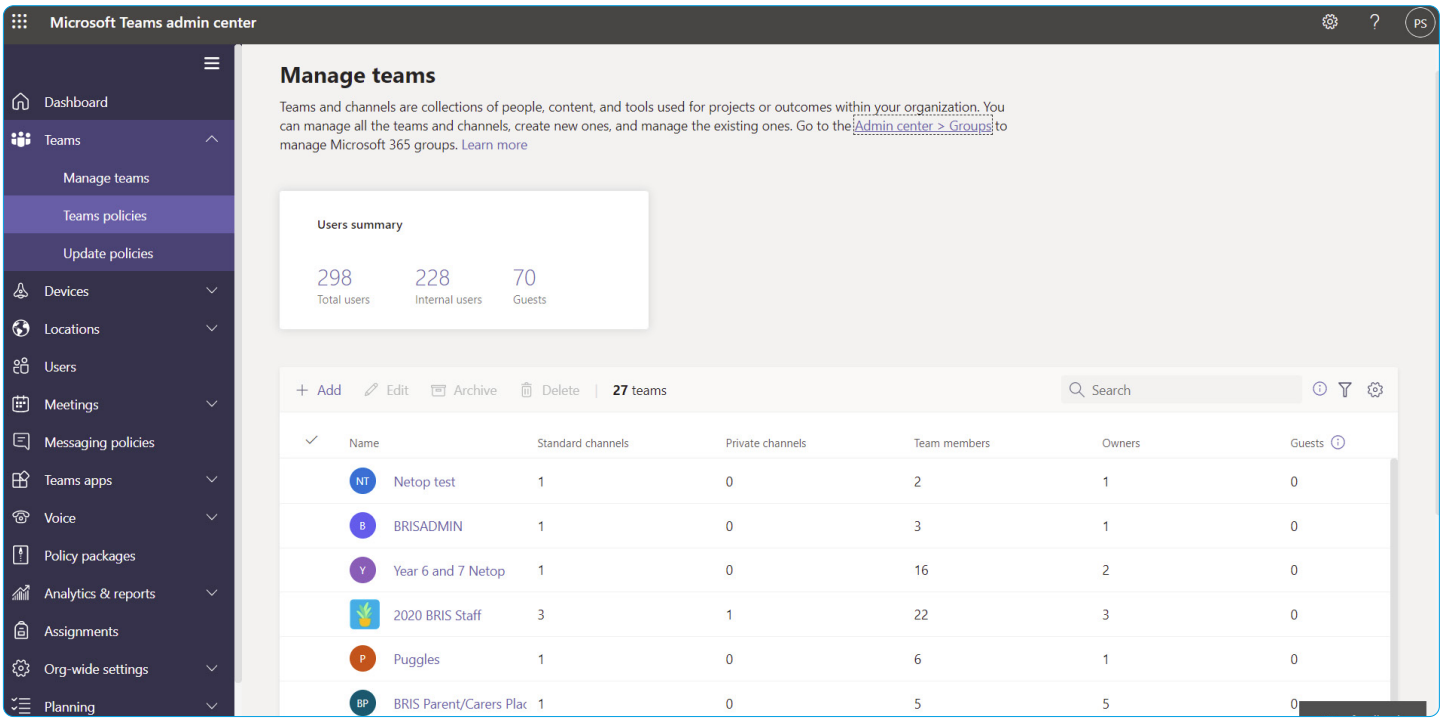
TEAMS

THERE HAVE BEEN MANY INSTANT MESSAGING / CHAT APPLICATIONS ATTEMPTING TO TAKE ON BUSINESS COMMUNICATION AND WITHOUT A DOUBT MICROSOFT'S TEAMS IS THE BEST YET. THIS IS IN NO SMALL PART FUELED BY THE COVID-19 PANDEMIC WHICH HAS SEEN TEAMS USAGE GROW FROM 13 MILLION DAILY ACTIVE USERS IN JULY 2019 TO OVER 300 MILLION (!) IN 2023. IN THIS CHAPTER WE'LL SEE WHAT TEAMS CAN DO FOR YOUR BUSINESS COMMUNICATIONS AND COLLABORATION.

11.1: MEET TEAMS

A lot of development is going into Teams to make sure it's the best place for groups of people to work together, the most recent evidence is the new **Teams client application** (public preview March 2023).

A Team **can have up to 25,000 users** but in my experience, it works best with smaller teams (up to a few hundred). If you're delivering a webinar style event with people just watching, there's a 20,000-attendee limit. There are client applications for Windows, MacOS (both updated bi-weekly), iOS and Android as well as a web-based interface (updated weekly). Like many things in M365 there are two components to successful adoption, the technical side, and the user training side.



Teams Admin Center

If you have conference rooms, make sure you consider the technology you outfit them with, Teams Rooms are a powerful way to use technology to connect staff in the office with staff working from home. Teams Rooms are split into Basic (free, up to 25 systems can have this type of license) and Pro, which comes with many **security, convenience and extra collaboration features**. The old **Teams Room** Premium licensing has been retired.

Until recently there were just Teams licensing (as part of M365 licensing) and a free Teams for smaller teams (which is being retired). In February 2023 a new, paid for, licensing tier called Teams Premium became available. As with any M365 feature set you need to carefully assess whether the additional features make business sense, for the users you license it for (not everyone needs to have Teams Premium). **Premium features** include protected meetings with watermarks on recordings (with the email address of the person recording), sensitivity labels for meetings and end-to-end encryption, as well as custom meeting templates and themes. For webinars there are a lot of extra features improving the overall experience, and finally virtual appointments manages these types of meetings, including SMS notifications.

11.2: TEAMS PHONE

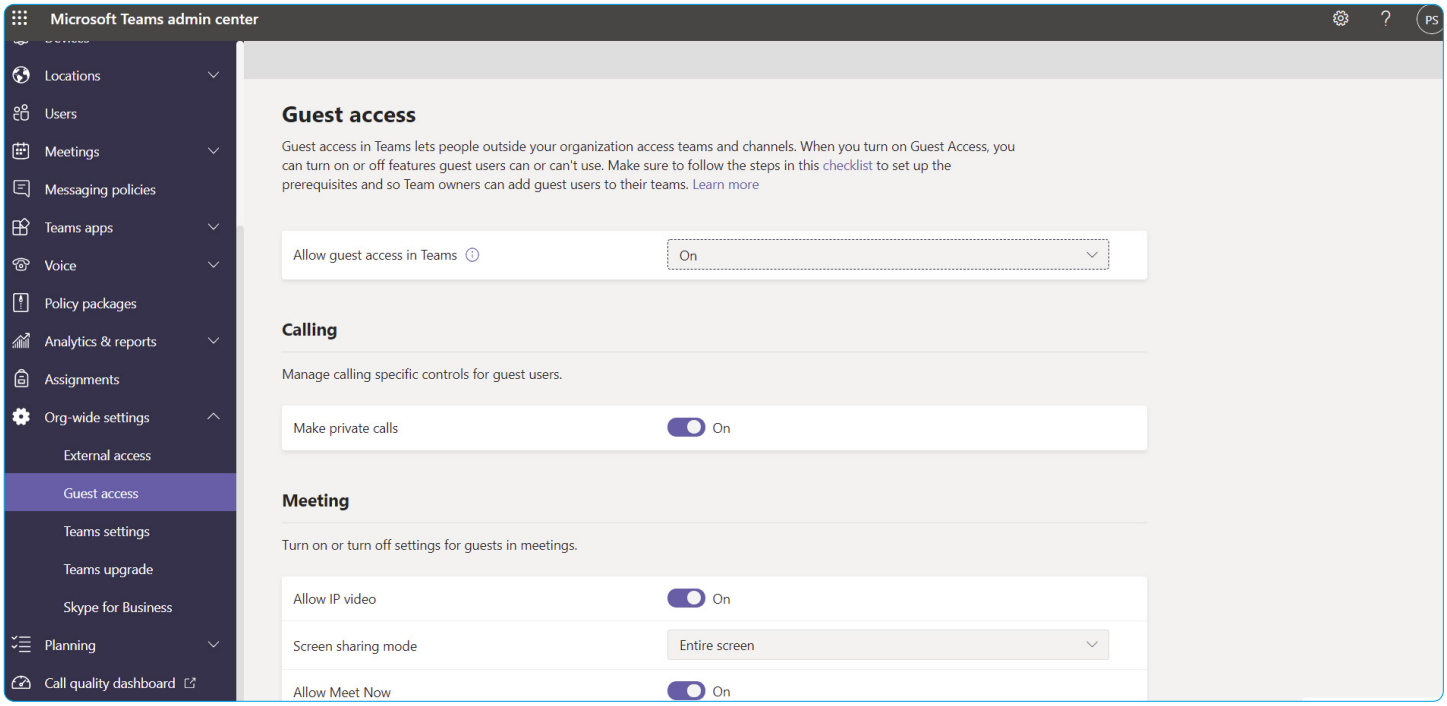
One great appeal of Teams is that you can **connect it** to the Public Switched Telephone Network (PSTN), allowing your users to call anyone in the world from their Teams client (on any platform) and have a phone number so anyone can call them. This combination of external phone calls, internal VOIP / video calls and video conference meetings or webinars,

easy **file sharing and co-authoring**, plus asynchronous Instant Messaging and chat is what has made Teams the de facto collaboration and communication hub in many businesses.

There are a few options on how to connect, and depending on your geographical location in the world not all will be available. You can use **Calling Plans**, where Microsoft is effectively your telco provider or **Operator Connect** if your existing telco participates in the program and can facilitate the connectivity. There's also **Phone Mobile** where an existing telco uses SIM-enabled mobile phone numbers with Teams, and finally **Direct Routing** where you connect on-premises infrastructure to Teams. And in larger environments you may be using several of these in combination.

11.3: MANAGING TEAMS

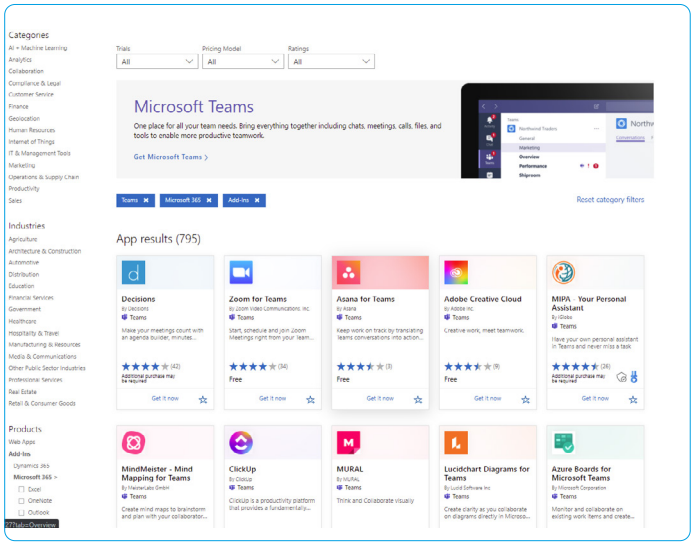
Your main interface is the **Teams Admin portal**, and there's a **PowerShell module** available. Underneath each Team is an M365 Group (Chapter 10) with the chat messages stored in Azure table storage, shared files in the Team's SharePoint library and personal files in each user's OD4B, voicemail and calendars are stored in user's Exchange mailboxes, and meeting recordings in Azure media services. If you're in a larger business, make sure to **plan for governance** of Teams early in your deployment. Visit your Tenant's Team's **Guest access settings** to make sure you have a good balance between security and collaboration for your business. Another handy feature is the ability to use **templates for Teams creation**, including creating your own custom templates.



Teams Guest Access settings

Each Team has a default General channel, and you can further create channels to organize communications, within each channel you can add tabs for Planner, OneNote, PowerBI, Stream, Wiki, websites and third-party apps. To limit the proliferation of Teams in your organization you can **limit who can create Teams** (by default all users can), as well as use **Private Channels in a Team**. You could have a Team for the Sales department with a private channel for only sales managers to discuss confidential information for instance.

There's also the ability to **share a Channel** with an external user, rather than sharing a whole Team. The main benefit for the invited user is that they can be logged in with their own tenant account and access the shared channel chat and documents without the need to sign out and sign back into Teams using their guest account. You can only create a new channel as a shared channel, you can't convert a normal channel to a shared channel.



Teams Third-Party Add-Ins

Delivering presentations using Teams is common, the **PowerPoint Live feature** makes it more interactive by allowing attendees to interact with the presentation at their own pace and **Presenter mode** gives you more control over how your presentation delivery shows up for the audience. To practice your delivery (in PowerPoint in general), use **Speaker Coach.**

A great feature is **breakout rooms**. This lets you send users to or ask users to pick "rooms" where they can collaborate with a subset of the users in a Team during a meeting, and then return to the main meeting later.

Recordings of Teams meetings (including **transcriptions**) used to be stored in Stream, now **they're saved in OD4B / SharePoint** where they can be shared easily (including with external attendees). A good tip is being aware of the default expiry of meeting recordings: 120 days. You can change that (for recordings in your tenant) in the Teams admin center - Meetings - Meeting policies - Recording & transcription. Speaking of transcriptions, if you have Teams Premium you can enable **translated captions**, so that a meeting delivered in English can be viewed by a German viewer with captions in their language, and another viewer can have captions in Chinese for example.

11.4: USING TEAMS

If you're used to communicating via email here are some guidelines to be effective with Teams. Use @ mentions to draw something to the attention of a specific Team member, a channel or a whole team. Be generous with your Praise when someone does something good for the Team, and if you want to acknowledge a message just Like it, instead of adding to the noise with a text-based reply. When

you're about to post about something – check if there's already a thread related to it and add to that instead and use the text styling (or a GIF / Sticker / Meme) when you want to get your point across and Sad, Angry or Happy reactions to contribute to the conversation when appropriate.

You can blur the background when you're in a video meeting, or **replace the background image** and if you have frontline workers that need to communicate with others, use the **Walkie Talkie** push-to-talk feature. You can also use **an avatar** to replace your video feed, handy for those Monday morning meetings when you've got a bad hair day, instead presenting a "cartoon" version of yourself.

Teams will **automatically translate messages** in other languages to the language set in your personal settings. And there's **offline functionality,** so if you're offline, Teams will save your unsent messages and send them when you're back online.

When you're in a meeting you can use **Together mode** which will show the video of each participant as if they were sitting in a lecture hall, removing the Brady bunch feel of the traditional grid of video feeds.

11.5: VIVA

If you needed any more proof how central Teams has become to Microsoft's vision and roadmap for modern collaboration and work, look no further than the **Viva** employee experience platform (EXP). Viva has eight pillars, all surfaced in Teams: **Viva Connections** takes your SharePoint Online Home site, Line of Business (LOB) applications, and other internal news sources and lets you target company news and connections to the right people. **Viva Insights** is the next iteration of My Analytics to help staff manage time and avoid burnout, integration with Headspace for guided meditations and a virtual commute function to wrap up the workday. For Managers there's a de-identified view to see how a team is fairing from a stress, mental health, and productivity point of view. There's also a Leaders view for executives to see the overall state of their staff. The third pillar is **Viva Learning**, surfacing **training courses and microlearning content** while integrating with **other Learning Management Systems** (Cornerstone OnDemand, Saba, SAP SuccessFactors and Workday) to make learning a natural part of everyone's daily work. Managers can schedule trainings and staff can share particularly good courses with each other and they're all available directly in Teams. **Viva Topics** builds on Cortex / Syntex and uses AI to organize company-wide content (in-house projects, products, acronyms) and staff expertise and surfacing this as topic cards / pages in Teams, Microsoft Search, SharePoint, and Office. Think of this as Wikipedia for your business.

Viva Goals applies the power of the objectives and key results (OKR) framework to help staff track their progress against goals. **Viva Engage** on the other hand connects people across an organization (this is really the new name for what used to be Yammer). The new **Viva Sales** integrates with any CRM (including of course Microsoft Dynamics 365) for deeper client insight and engagement. And finally, **Viva Pulse** (in public preview at the time of writing) helps leaders and managers to receive and act on internal feedback in an organization.

As you can probably tell from these brief descriptions, most of the Viva modules are likely to find their homes in larger enterprises as that's where the challenges of "managing people" at scale are most acutely felt.

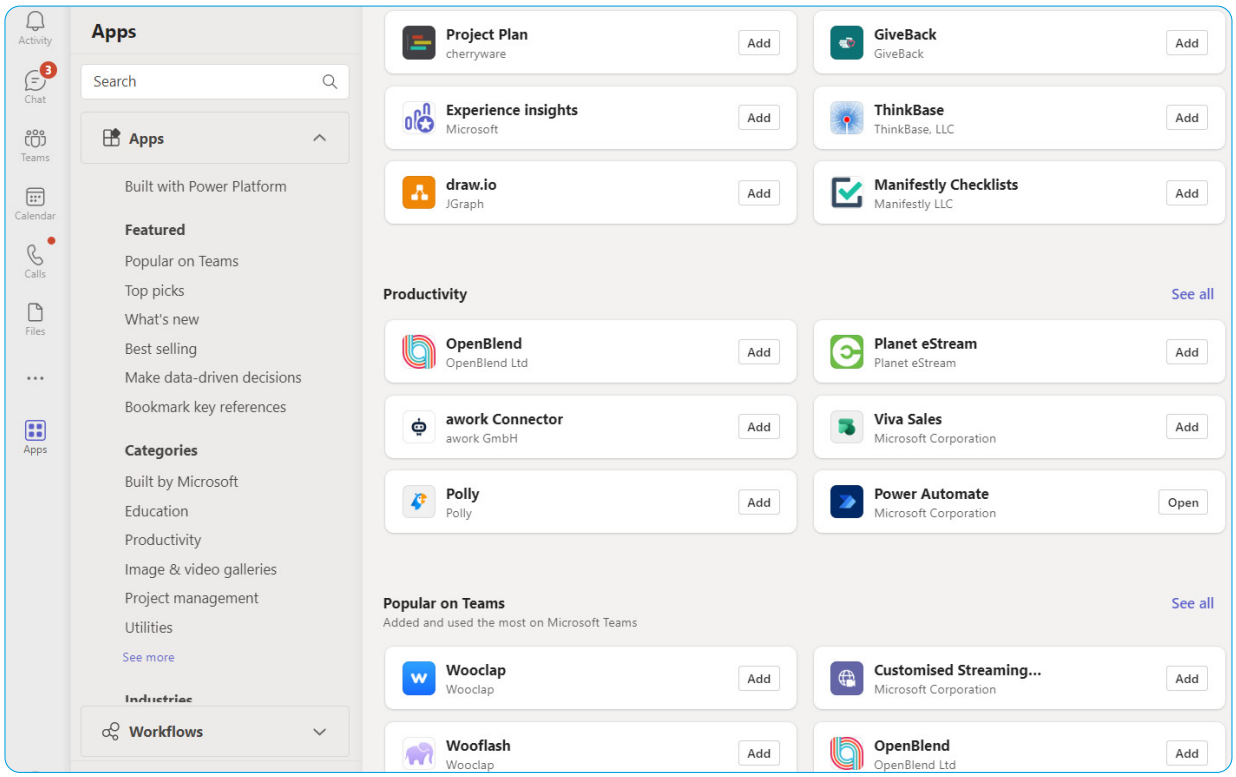
11.6: EXTENDING TEAMS

Another powerful capability is **adding apps** to Teams through the Teams Store. Microsoft tests and validates these apps. There are hundreds of different apps for integrating with other platforms, enhancing productivity, improve meetings, customer relationship management (CRM) and many more. A very popular app is **Microsoft Whiteboard**, free on all platforms, that you can use both inside Teams and standalone to brainstorm and plan together.

As an administrator you have granular control, you can **allow or block apps**, **control the permissions** they are given, manage how the **apps are made available** to users, plus **report on app usage**. You can also have **custom apps** developed in-house.

You can further **extend Teams with Bots** that can interact with your users naturally through chat or a notification bot that can push relevant information to your users.

With the advent of Slack (Team's main competitor) and Teams many people have (again) proclaimed the death of email. As usual we tend to see new technology as a direct replacement for the old while the reality is more nuanced. I find Teams more efficient for group-based work, the sharing of files and communication is superior to email but communication outside of client projects I'm involved in still relies on email. And you can use email to send messages to a channel in a Team.



Teams Guest Access settings

CHAPTER 12:

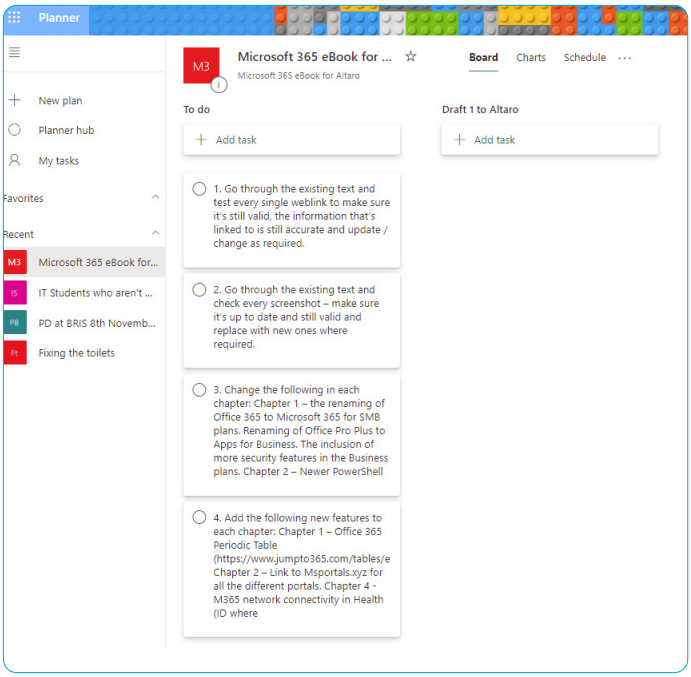
OTHER OFFICE 365 APPLICATIONS

THERE ARE MANY OTHER APPLICATIONS AND SERVICES IN THE O365 PORTFOLIO, IN THIS CHAPTER WE'LL LOOK AT SOME OF THEM WITH A BRIEF INTRODUCTION.

12.1: PLANNER

Microsoft has had Project for large scale project management for many years but for small to medium undertakings it's overkill (there's a steep learning curve) and this is where Planner shines. If you've ever used Trello, you should be comfortable with Planner's workflow.

There's a web-based interface, along with iOS and Android clients but no PC client. If you add a Planner tab to a Team, you can create a new plan or attach an existing one. You organize tasks into buckets, assign tasks to different people and track the progress of those tasks. Tasks can also be viewed in a Schedule (calendar) view, and you can export a plan to Excel.



A Plan in Planner

Other task management offerings from Microsoft includes To-Do (mobile, web and PC clients are available) which integrates with Outlook tasks.

12.2: STREAM

This is the best way to share **video** inside your company and it's similar to YouTube. There are clients for iOS and Android and a web interface but currently there's no licensing in place for sharing videos with people outside your tenant.

When you upload a video it'll be processed and if the people in it are speaking English, Chinese, French, German, Italian, Japanese, Portuguese, or Spanish it'll **automatically generate captions** which are searchable in Stream, making it easy to find the right video or point in the video. It'll also attempt to recognize people in the video and if successful will list those people with the video information. Teams used to use Stream to store meeting recordings, but they're now stored in OD4B / SharePoint.

12.3: KAIZALA

This is an application like Teams, designed for front-line / transient workers with poor connectivity. Think of this as a managed version of WhatsApp.

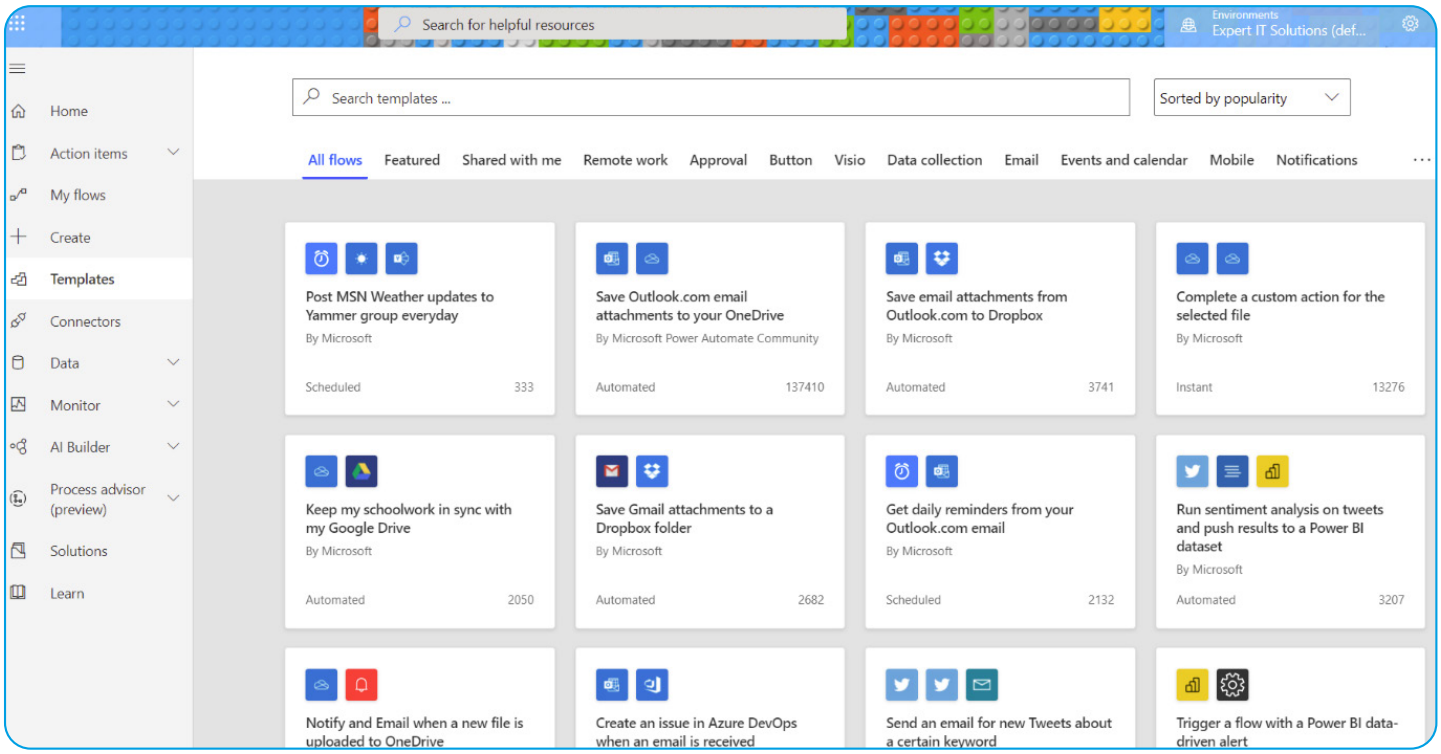
12.4: POWERBI

Visualizing data is important for any modern business who wants to be data-driven and PowerBI is Microsoft's answer. There's a desktop client where you build your dashboards, there's also a web interface. Licensing is **a bit of a challenge**, depending on what you've built and who you want to share it with.

It's a lot of fun to use and the results can be extremely useful for many aspects of your business.

12.5: POWER AUTOMATE

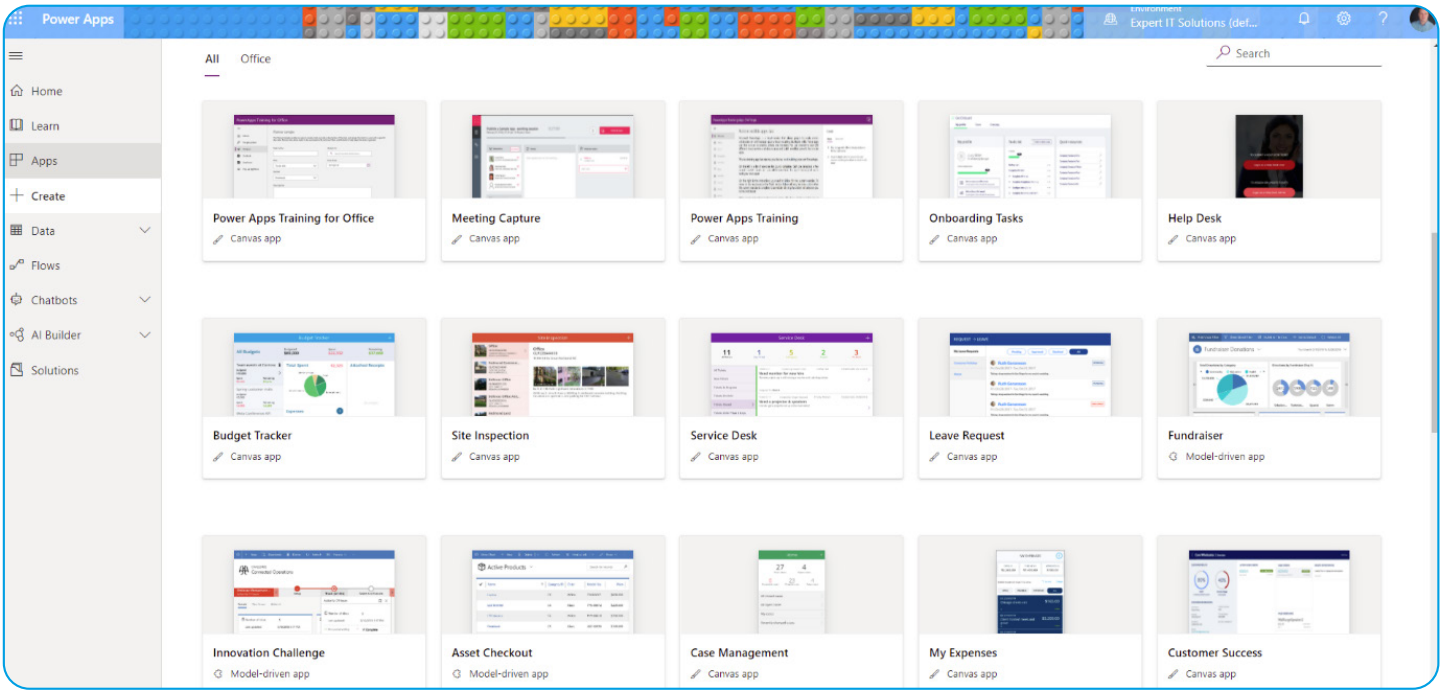
This deceptively simple, web-based tool is designed to automate tasks without having to write code (it used to be called Flow). Simply drag in actions, connect them to external systems and schedule them to run regularly or be triggered by an event. There are lots of templates to help you get started as well as connectors to hook into Microsoft and third-party systems. If you've used If This Then That or Zapier, **Power Automate** is easy to get started with.



Power Automate Templates

12.6: POWERAPPS

Ever wished you could equip your staff with a custom mobile app to gather or access data in the field but realized the development costs were too high? **PowerApps** is the solution, providing a low code / no code development environment to build applications that connect to SharePoint, Excel, O365, Dynamics 365 or SQL server on-premises or in the cloud; or the **Dataverse** platform. The resulting app runs on iOS, Android, in a web browser or in Teams and SharePoint Online. If you need to manage data in your apps there's **Dataverse** for Teams and the full Dataverse flavor.



PowerApps Templates

12.7: MICROSOFT LISTS

Yes, the old SharePoint list concept was given a new lease of life, including a **separate app** and is also available in Teams. Use it to track lists of "stuff" and manage information.

12.8: MICROSOFT LOOP

Potentially the most confusing technology Microsoft has released in recent years (currently in public preview) is **Loop**. The concept is fairly simple, you have Loop Components that you can embed in various locations, such as documents, Teams chats or an email, and these are kept in synch across these different places. Loop pages lets you bring together components, links, tasks, and other data. Finally, Loop workspaces are shared spaces bringing pages and components together. I find Loop most useful in the early stages of a project or an idea – brainstorm, work together with others on a concept and keep all ideas in synch with everyone you're working with.

The challenge today is that due to the underlying storage of Loop components being in user's personal OneDrive for Business, sharing outside an organization doesn't really work, and even inside a tenant it can be a challenge. If Microsoft can solve these challenges, Loop has an interesting future.

DETECT SOPHISTICATED ATTACKS WITH ADVANCED THREAT PROTECTION
AVAILABLE IN
365 TOTAL PROTECTION
PLAN 4 - COMPLIANCE & AWARENESS
FREE TRIAL

CHAPTER 13:

MICROSOFT INTUNE

M365 E3 AND E5 BRINGS YOU MICROSOFT INTUNE, MICROSOFT'S MOBILE DEVICE MANAGEMENT (MDM) CLOUD SERVICE. IN THIS CHAPTER WE'LL LOOK AT HOW IT CAN HELP YOU MANAGE DEVICES AND PCS, MOBILE APPS, PROTECT COMPANY DATA AND ENFORCE SECURITY POLICIES.

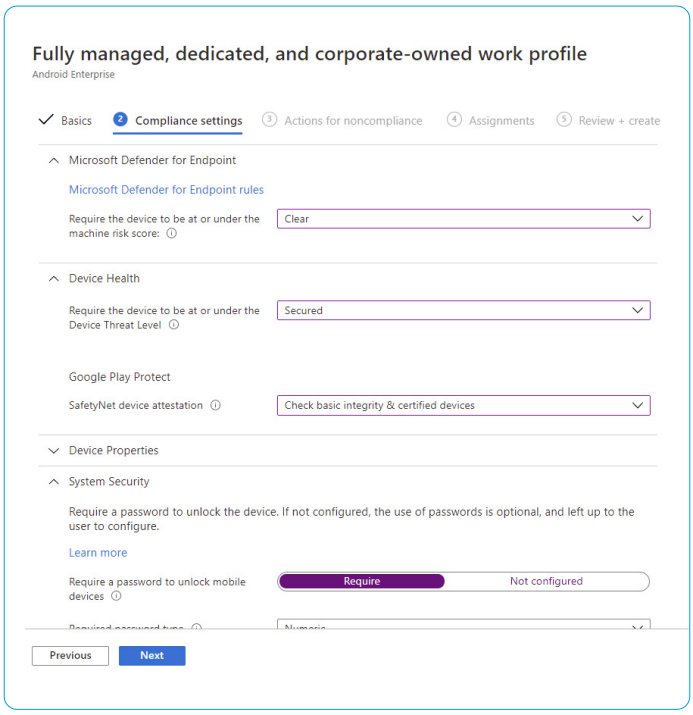
There used to be an on-premises product called System Center Configuration Manager (SCCM), now called **Microsoft Configuration Manager,** which you can integrate tightly with Intune.

There used to be a requirement that Intune administrators were licensed for Intune but **this is no longer the case**. **Endpoint analytics** is an interesting part of Intune, using signals from your devices to pinpoint problematic or slow PCs, it's part of the overall **Adoption score.**

If you have Windows 10/11 devices that serve specific functions (on a factory floor, at a nurses station in a hospital for example), you can use Cloud Configuration to **easily manage them entirely using Intune**, with scripted, baseline configuration settings.

13.1: MOBILE DEVICE MANAGEMENT

There are a couple of ways you can use Intune, if you have devices (smartphones, tablets, laptops) that are company owned you can **enroll them in Intune**. This gives you a great deal of control over the device, including the ability to manage settings, apps and the option to wipe the device should it be lost or stolen. You can also use Intune to manage OS updates for Windows devices, push out applications to devices, configure Wi-Fi profiles and deploy certificates as well as block iOS jailbroken and rooted Android devices.



Android Compliance Policy in Endpoint Manager

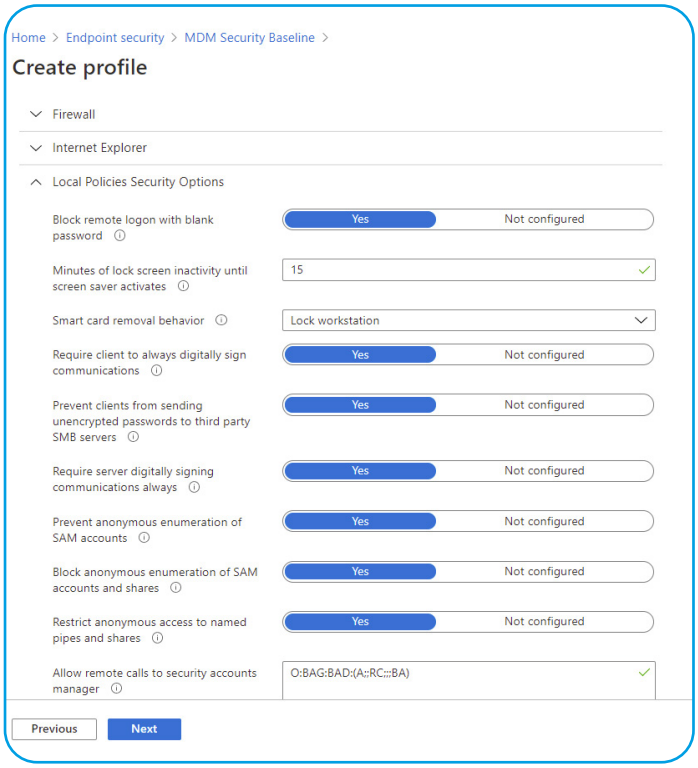
If the device is a personal device, owned by the employee, they may not be comfortable with enrolling the device so you can use Mobile Application Management (MAM) for those devices.

13.2: MOBILE APPLICATION MANAGEMENT

This less intrusive approach lets you create **app protection policies (APP)** across specific applications, with email being the classic example. Users want to access business email on their personal smartphone so you put policies around it where they can only use Outlook (free mobile app for Android and iOS), not the built-in mail apps and you can further protect corporate data so that a user can't copy business data to a non-business app (personal email app etc.). If the device is lost or stolen, you can wipe the corporate data off it while leaving personal photos etc. untouched.

Picking between MDM and MAM is going to depend on many factors such as your userbase, your employment contracts, business and security needs and more; make sure you spend some time in the **planning phase** to get it right.

Another part of managing mobile applications might be to connect them back to on-premises resources securely, Microsoft now offers their own VPN for iOS and Android called **Tunnel** – and it's integrated into the Microsoft Defender for Endpoint.



MDM Security Baseline

13.3: MICROSOFT CONFIGURATION MANAGER

If you have deployed MCM on-premises to manage your servers and traditional client PCs you can integrate Intune into your management flow **through Co-management** to leverage the best of both worlds and prepare your environment for a gradual migration to cloud management. Don't confuse this with **Hybrid MDM** which is the older, deprecated approach to marrying SCCM and Intune.

13.4: INTUNE SUITE

In true Microsoft fashion there are **add-ons for Intune** that you may want to consider for your business, if they solve a particular business problem for you. There are stand-alone add-ons, an Intune P2 plan and the full Intune Suite, which includes the following: **Advanced endpoint analytics** to track and optimize end user experiences, **Endpoint Privilege Management** which lets end users perform certain administrative tasks on their Windows device without being a local administrator and **Microsoft Tunnel for MAM** which extends the per-app VPN feature for Android and iOS apps to MAM. There's also **Remote Help**, which is a secure way to allow helpdesk to access the screen of staff to assist them and **Managing specialty devises** such as AR/VR headset and large smart screen devices.

PART 3

SECURITY, BACKUP & COMPLIANCE

MICROSOFT 365
THE ESSENTIAL
COMPANION GUIDE

CHAPTER 14:

SECURITY IN O365

IN THE EARLY DAYS OF CLOUD COMPUTING THERE WAS A LOT OF CONCERN AROUND THE SECURITY OF DATA MOVED TO "SOMEONE ELSE'S DATACENTER". I THINK IT'S CLEAR TO MOST CISOS TODAY THAT THE BIG PROVIDERS DO A MUCH BETTER JOB OF IT SECURITY THAN MOST BUSINESSES CAN DO (OR HAVE THE BUDGET TO DO). THEIR INCENTIVE IS ALSO STRONG, IF A LARGE BREACH HAPPENED IT COULD AFFECT MANY THOUSANDS OF BUSINESSES AND SO THEY SPEND A LOT OF MONEY ON MAKING SURE THEIR CLOUDS ARE AS SECURE AS THEY CAN BE.

That doesn't mean however that you can leave it all to Microsoft, there's something called the **Shared Responsibility Model** and all cloud providers have some version of this. There are some areas that are still your responsibility such as the endpoints that your users use to access cloud services, any on-premises infrastructure that's operating in a hybrid mode with O365 and user provisioning and de-provisioning. There are also many security controls in O365 that you need to customize to suit your business, where you and Microsoft share the security responsibility. In this chapter we'll look at these controls and where and how you configure them.

The foundation for "how you think about security" should be Zero Trust, instead of trusting a connection based on where it's coming from ("if it's on the internal LAN it's safe, from the outside it's dangerous"), every access is checked against your Conditional Access rules which gives you a much better security posture. And base your security on identity which is the new firewall and **keep up with new features in the security space.**

When thinking about how to defend your systems, don't forget to take into account attackers **moving from on-premises to the cloud**, as we saw in the Solarwinds breach. If you have M365 E5 licensing, you can use attack simulation training to test your users with fake phishing emails and provide bite sized training automatically to them based on their propensity to fall for them. If you'd like more control and optimization, try out Hornetsecurity's **Security Awareness Service** which delivers fully automated benchmarking, spear-phishing-simulation and e-training to sensitize and protect employees against cyber threats.

Remember Entra ID Premium P1 & P2 which you can purchase as add-ons to O365 (included in M365), we covered their security features in Chapter 7.

There's a strong argument to be made that relying on Microsoft both to provide the platform (Office 365) and also paying extra for advanced security features from the same company is a conflict of interest. After all, Microsoft could include more security features in the base platform (Office 365 E3 and Microsoft 365 E3 for example), rather than charging extra for them. As such, many enterprises choose to opt for a third-party service for advanced security services on top of the base platform, such as Hornetsecurity's 365 Total Protection.

14.1: 365 TOTAL PROTECTION

365 Total Protection is a cloud-based security solution that covers all aspects of an organization's Microsoft 365 security management and data protection: email security, backup and recovery, compliance, permission management and security awareness. The solution is specifically developed for Microsoft 365 and requires no hardware, software, or maintenance, while providing much-needed layers of additional security and data protection against spam, malware, and advanced threats.

365 Total Protection from Hornetsecurity comes in four different plans:

1. **365 Total Protection Business** gives you state of the art email security, spam and malware protection, signatures, and encrypted email.
2. **365 Total Protection Enterprise** adds email archiving, 10-year retention, eDiscovery, Advanced Threat Protection (ATP) sandboxing of suspect emails, URL scanning, QR code analyzer.
3. **365 Total Protection Enterprise Backup** adds automated backup of mailboxes, Teams, OneDrive and SharePoint and easy recovery, Windows endpoint backup and recovery.
4. **365 Total Protection Compliance & Awareness** adds Permission Manager, Security Awareness Service and AI Recipient Validation to the offering.

This wide range of Microsoft 365 security and compliance features is available in **one package** and in one license.

14.2: 365 PERMISSION MANAGER

One of the three pillars of Zero Trust, using least-privilege access, is remarkably hard to achieve at scale. This is particularly evident in SharePoint and OneDrive where you not only have a complex set of overlapping permission options, but also sharing of files and sites with external users, either through SharePoint, OneDrive, and now also commonly through Teams.

To inventory all these permissions that have been granted and reporting on them requires browsing multiple screens or running PowerShell scripts.

There's also no easy way to "right-size" permissions when they're too broad, nor a quick way to revoke permissions quickly across all sites when a user account is discovered to have been compromised for example.

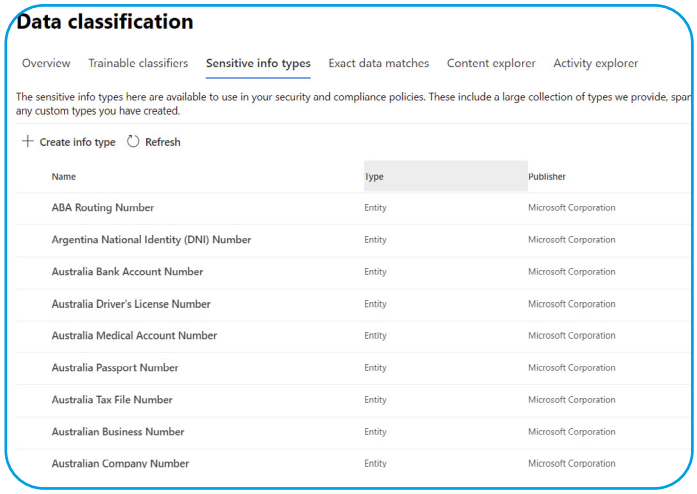
A unique product from Hornetsecurity, **365 Permission Manager** alleviates all these issues, and more. A centralized dashboard shows you all your sites, and how compliant they are with your sharing policies. To right-size permissions use the simple Fix button, or in the case of genuine business requirements for an exception to policy, Approve a special case. Built-in or custom policies that control external sharing, internal sharing and associated settings can be applied to individual SharePoint sites or OneDrive locations, improving governance and risk management considerably.

You can also see permissions across SharePoint, OneDrive, and Teams for a selected user, very useful when you suspect an account compromise, or perhaps in the case of an insider risk investigation. Another very useful feature is Quick Actions, which lets you perform bulk actions to manage permissions and maintain a compliant SharePoint, Teams and OneDrive infrastructure.

14.3: MICROSOFT PURVIEW INFORMATION PROTECTION

All the governance, Data Loss Prevention (DLP) and Information Protection features in M365 come under the Purview umbrella, with the portal located at **compliance.microsoft.com**.

Using **labels to classify data**, either manually or automatically through crawling documents or emails lets you start to govern your business information. Once a document has been labeled you can use MIP or OME to protect it (see below), or control access on Windows endpoints through policy as well as manage access in Office for Mac, Windows, iOS and Android.



MDM Security Baseline

14.4 : MICROSOFT INFORMATION PROTECTION

One of the most powerful and least deployed features is the ability to protect documents, no matter where they live. Traditional file / SharePoint document sharing tightly controlled access at the server level but as soon as a document is emailed to someone, or stored on a USB drive, that control is lost.

With Microsoft Information Protection (MIP) you can set up labels and rules that encrypt documents and that carry their user access with them so no matter how they're shared, only the right people have access. If you're getting started with MIP, you'll be using the built-in client in the Office apps on Windows, Mac, iOS and Android. It's important to configure **super user accounts** so that you can access documents when a user leaves the company. The list of sensitive information types (SITs) grows

ever longer and it's now possible to customize the confidence levels of rules, copy the built-in ones and customize them and create larger keyword dictionaries (catch every mention of a staff ID tag, or patient record number).

It's possible to **co-author protected documents in real time** (with AutoSave support!) and in larger deployments you can use variables in MIP rules to facilitate per-app content marking. You can apply labels (and optionally document encryption) to documents, SharePoint online sites, and on-premises SharePoint and file shares. You can also scan images using **Optical Character Recognition (OCR)** to catch sensitive information in screenshots and the like.

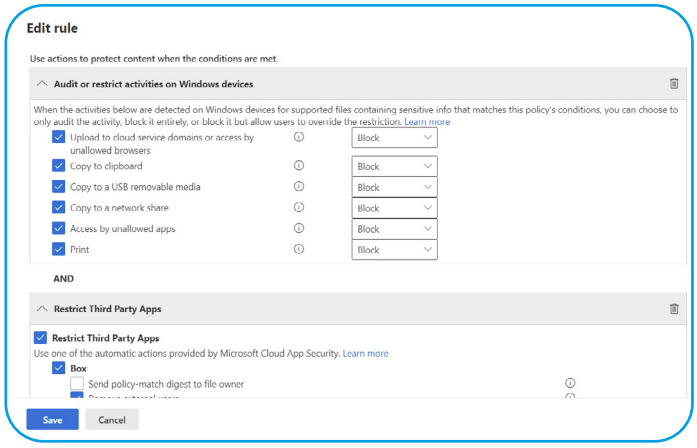
Sensitivity labels are now also available for **SharePoint sites, M365 groups and Teams**. This doesn't apply to content stored in those locations but rather manages privacy of the container, external user access and can also integrate with Conditional Access policies to block access from unmanaged devices for example. You can however configure a **default sensitivity label for a SharePoint site**.

14.5: OFFICE 365 MESSAGE ENCRYPTION

In a similar way to how MIP allows you to share protected documents with anyone, you can use **O365 Message Encryption** to send emails to anyone and know that only that person can access that email. Like MIP you can also set up rules so that emails with specific information in them (credit card numbers, social security numbers) are automatically encrypted.

14.6: DATA LOSS PREVENTION

The aim of **Data Loss Prevention (DLP)** is to help users do the right thing by alerting them when they're about to share sensitive data through email, SharePoint Online, OD4B or Teams. It can also be integrated with MIP as Microsoft continues the journey of unifying labeling and protection across M365. DLP protection has been extended to Windows 10 and 11 with **Endpoint DLP**, which can block upload of documents with sensitive content to cloud storage, copying sensitive information to the clip board, USB storage, network shares or printing. There's also an extension for Google Chrome that extends DLP protection to browser tasks. DLP has also **been extended to on-premises** using the MIP Scanner to find sensitive documents and alert management for DLP violations is also vastly improved.



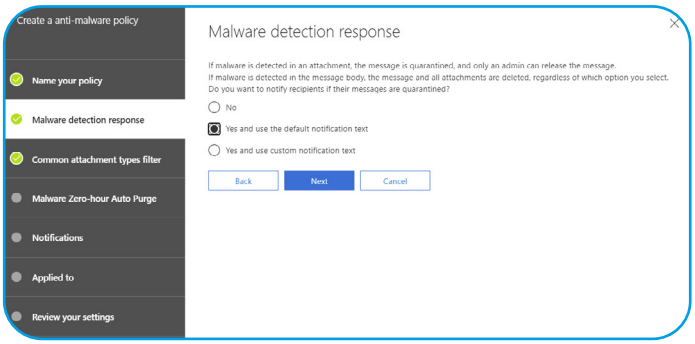
Endpoint DLP settings

14.7: EXCHANGE ONLINE PROTECTION

Exchange Online Protection (EOP) is the mail hygiene solution for Office 365 and can also protect your on-premises Exchange mailboxes if you're in a hybrid deployment (Chapter 8). There are a few settings you can control for EOP as well as some

additional configuration you should consider for complete spam protection such as **Sender Policy Framework** (SPF), **Domain-based Message Authentication, Reporting, and Conformance** (DMARC) and **Domain Keys Identified Mail** (DKIM).

If you find that EOP isn't catching enough malicious emails consider third party services, Hornetsecurity offers a free tool called **Threat Monitor** (requiring no changes to your MX records) that'll identify advertising emails (spam), threats and advanced threats emails and also lets you delete them from user's mailboxes. Threat Monitor provides valuable email statistical data for your tenant as to what EOP is missing, making the case for upgrading email hygiene services easier.



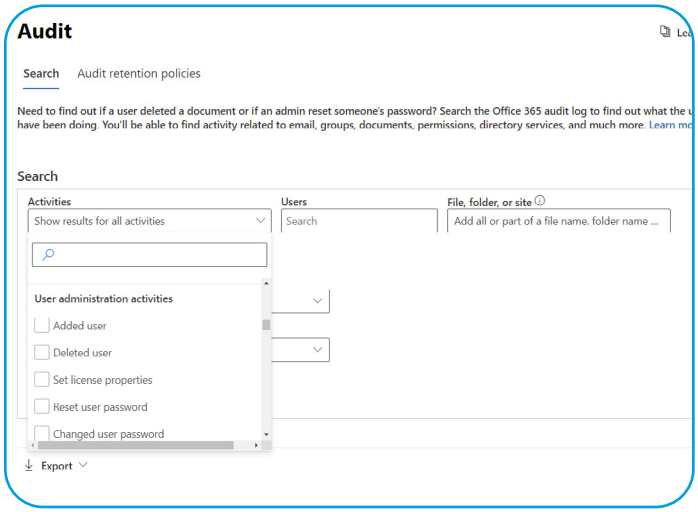
14.8: DEFENDER FOR OFFICE 365

Defender for O365 **protections** (available in O365 E5 or as standalone add-ons) builds on top of EOP and gives you **Safe Attachments** where attachments in incoming emails that may be malicious are opened inside a VM and checked before they're delivered to end users. **Safe Links** checks that links in emails and Office files aren't malicious at the time when users click on those links. **Anti-phishing** detects attempts to impersonate users, these protections also extend to SharePoint, OD4B and Teams.

If you find Defender for Office 365 too pricey (It's included in M365 E5, E5 Security or as a separate add-on) have a look at **Hornetsecurity's 365 Total Protection** which comes in a Business and an Enterprise flavor. Business gives you granular control over email categories and content so that you can block unwanted emails. You can set email signatures with company disclaimers and use either PGP or S/MIME for email encryption, with certificate handling built in. The Enterprise flavor adds email archiving / journaling with up to 10 years retention, eDiscovery and sandbox analysis of attachments, URL rewriting and scanning (both in emails and in attachments) and Contingency Covering through an email failover environment when Microsoft 365 is down.

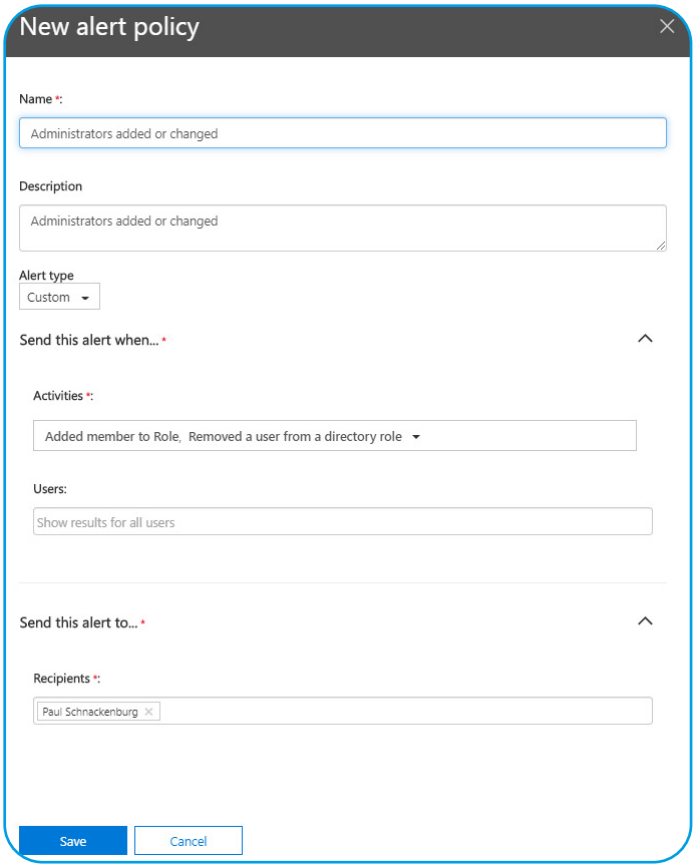
14.9: AUDITING

One of the great features of the unified platform of O365 is the ability to **audit user and administrator actions** across the entire platform.



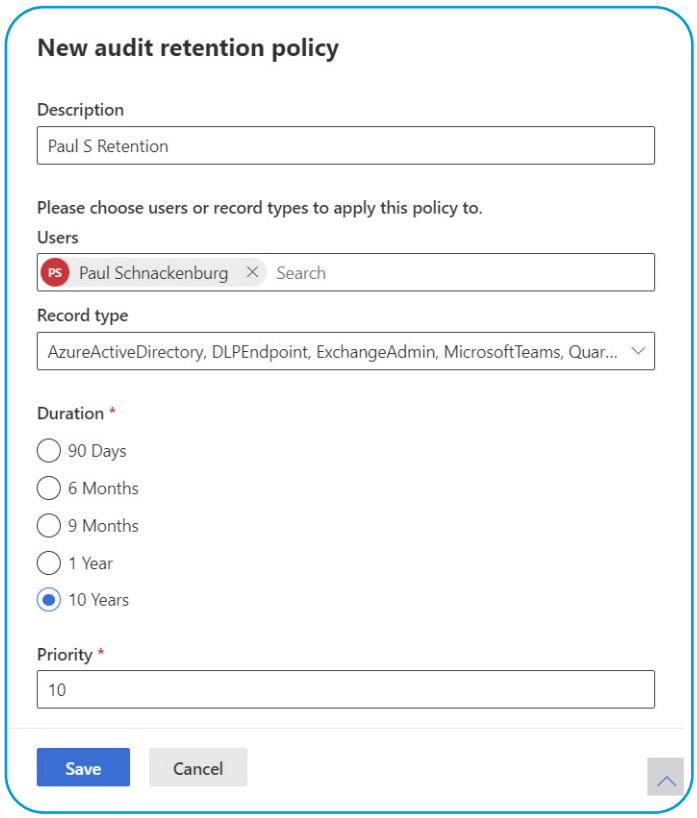
Audit log search

At a minimum you want to **configure alerting** on Entra ID actions, go to the Compliance portal – Search – Audit log search and see all the different activities you can audit and report on, as well as **create Alert policies** for.



Creating an Alert policy

By default, Office 365 audit logs are kept for 180 days (Entra ID logs for 30 days), which may not be sufficient for your business or regulations you must comply with. You have two options, use a third-party service to continuously export the logs and archive them for the time period you require, or assign M365 E5 (or M365 E5 Compliance / Discovery & Audit) licenses to the users who's logs you want to keep for longer. This unlocks the ability to keep the logs for 1 or 10 years.



Audit retention policy

14.10: SAY GOODBYE TO PASSWORDS?

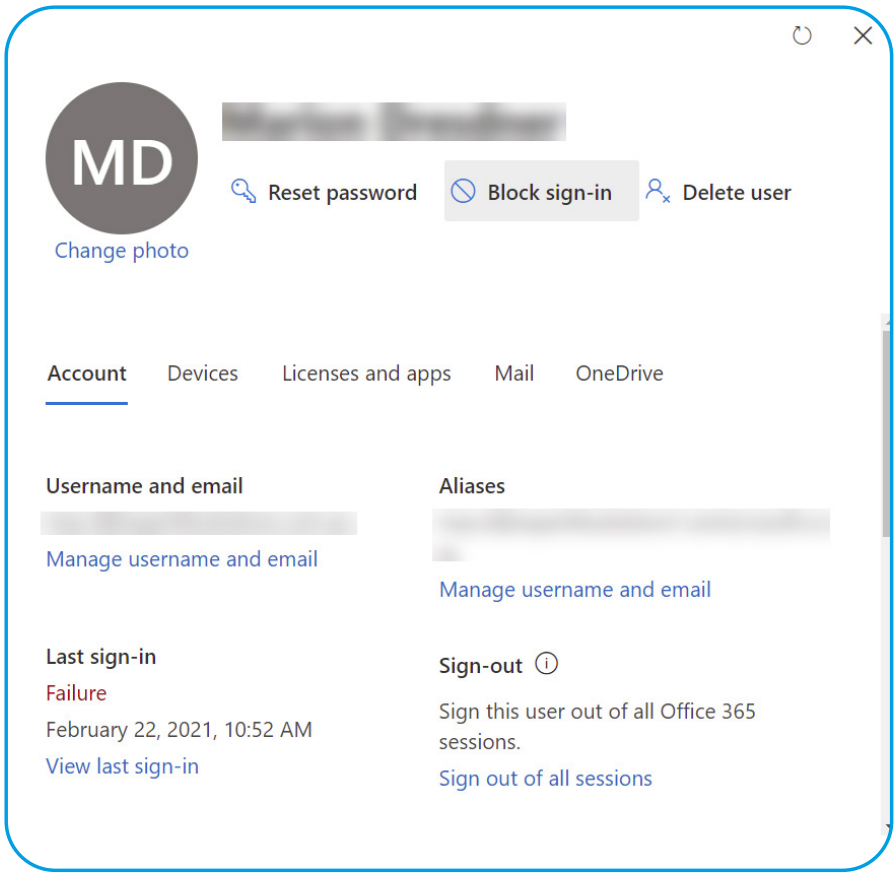
Ultimately the best way to manage passwords is to not have any stored in your directory and not have your users use any – this is called passwordless. There are **many steps on the journey towards this end goal**, today you can use the Authenticator app to sign in on an Azure AD account (not as a second factor but as the only factor), or Windows Hello for Business or a FIDO 2 hardware USB/NFC key.

In the meantime, enable **Password protection** to ban commonly used passwords (2000 in a list maintained by Microsoft plus up to 1000 custom words common in your organization/city/sports teams). This works seamlessly for cloud only accounts and can **easily be extended to on-premises AD**. When you require your users to register for MFA, they also register for Self-Service Password Reset **at the same time**.

14.11: BLOCK USER ACCESS

If you suspect or confirm that a user account has been compromised the first step should be to disable sign-in for the account in the Admin center.

You should be aware however that the user (or the attacker) isn't immediately logged out from services they're accessing, and it can take up to an hour until the block takes effect, due to the lifetime of refresh tokens. The solution to this issue is **Continuous access evaluation** which today only applies to Exchange, Teams and SharePoint online connectivity and will block access in near real time (occasionally up to 15 minutes latency due to event propagation).



Block sign-in for a user account

CHAPTER 15:

SECURITY IN MICROSOFT 365

THERE ARE MANY SECURITY TOOLS BUILT INTO THE O365 PLATFORM BUT WHEN YOU MOVE TO M365 E3 OR E5 YOU UNLOCK A WHOLE NEW SET OF ADVANCED FEATURES FOR SECURING YOUR BUSINESS. IN THIS CHAPTER WE'RE GOING TO LOOK AT THESE TOOLS, EXCEPT FOR ENDPOINT MANAGER WHICH WE'LL COVER IN THE NEXT CHAPTER AND WINDOWS 11 WHICH WE COVERED IN CHAPTER 6.

15.1: MICROSOFT 365 DEFENDER

Nearly all of Microsoft's M365 focused security products have the Defender brand, and the central console to work with them is **security.microsoft.com**. Here you'll find a comprehensive Extended Detection and Response (XDR) service that collects data from email, identity, endpoints, cloud services and alerts you to intruders across your M365 digital estate.

Here's a rundown of the different Defender services:

- **Microsoft Defender for Office 365** – This provides protection for emails, SharePoint sites, OD4B and Teams
- **Microsoft Defender for Identity** – This monitors your on-premises Active Directory (AD), integrates with your Security Information and Events Management (SIEM) tool and alerts you to account breaches, lateral movement and attacks involving AD
- **Microsoft Defender for Endpoint** – Centralized management of anti-malware on all endpoints in your environment (Windows, Linux, macOS, Android and iOS)
- **Microsoft Defender for Cloud Apps** – A Cloud App Security Broker (CASB), adding features to match the more modern buzz word, **SaaS apps security posture management.**

Microsoft also offers Microsoft Sentinel - a cloud based SIEM; Microsoft Defender for Cloud (for Azure, AWS and GCP IaaS and PaaS workloads) and Entra for identity management and protection.

15.2: MICROSOFT DEFENDER FOR ENDPOINT

Microsoft Defender for Endpoint (MDE) is a full-fledged Endpoint Detection and Response (EDR) security solution using Machine Learning (ML) behavior analytics for Windows, MacOS, Linux servers, iOS and Android devices. It inventories installed applications (Windows and MacOS) and through **Threat and Vulnerability Management (TVM)** prioritizes which applications bring the most severe risks to your organization based on how widely deployed each application is and the severity of the disclosed vulnerability. MDE also provides **Attack surface reduction rules** and **Next generation protection**, along with many other security features. MDE is available with, M365 E5 / E5 Security or as a standalone license.

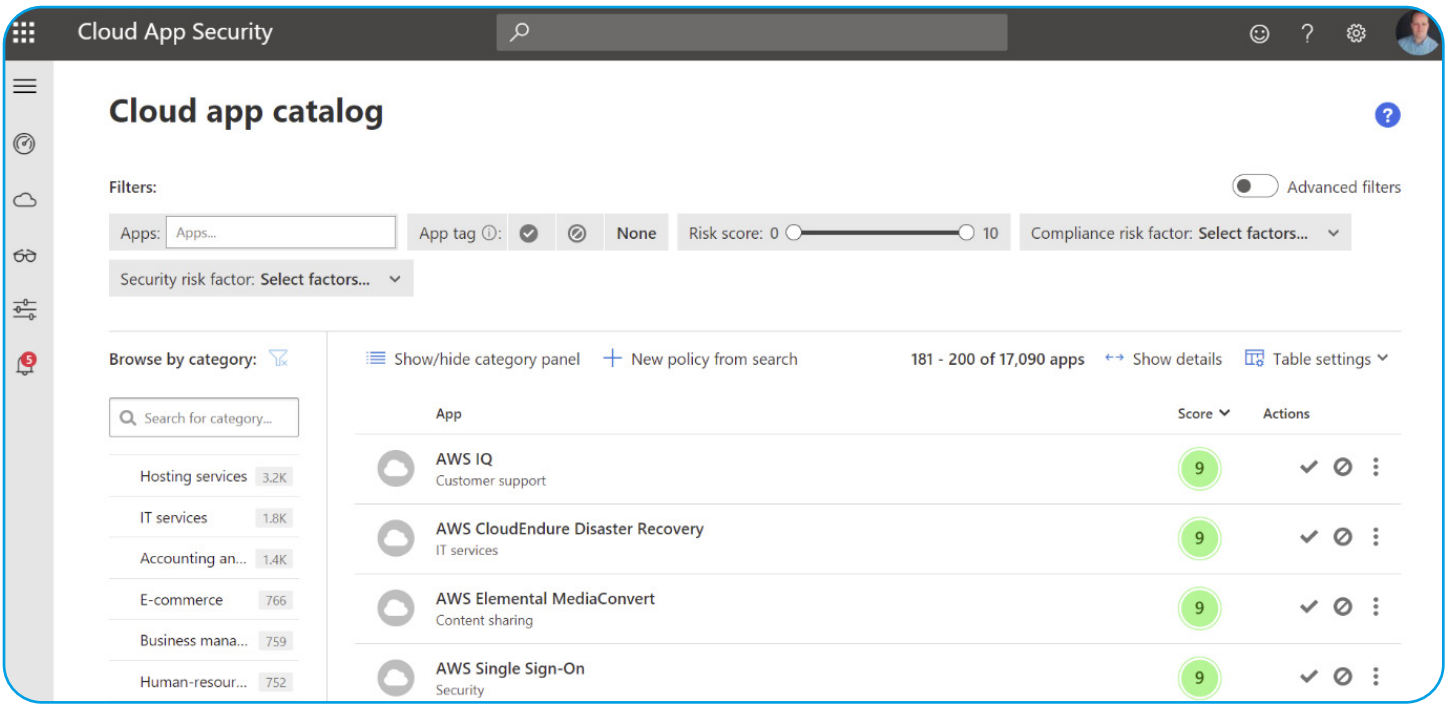
15.3: MICROSOFT DEFENDER FOR IDENTITY

With M365 E5 you can step up to **Defender for Identity** (MDI) which monitors your Active Directory Domain Controllers, and your Active Directory Federation Servers with only lightweight agents, the rest is taken care of by the cloud service. Any attacker that establishes a foothold on a device in your network must touch AD to move laterally and escalate privileges and MDI will catch them when they do.

STRENGTHEN THE
SECURITY AWARENESS
OF YOUR EMPLOYEES
AVAILABLE IN
365 TOTAL PROTECTION
PLAN 4 - COMPLIANCE & AWARENESS
FREE TRIAL

15.4: MICROSOFT DEFENDER FOR CLOUD APPS

Once upon a time when your users stayed in the corporate office all you needed to protect them was a good firewall but in today's world of "work anywhere, on any device" you need a new type of tool to protect them, a cloud access security broker. Microsoft Defender for Cloud Apps (MDA) is part of M365 E5 and protects your users in real time when they access cloud services. The catalogue of over 31,000 different cloud services gives IT a way to discover and manage Shadow IT (cloud services that users have provisioned without the IT department knowing) across your user base.



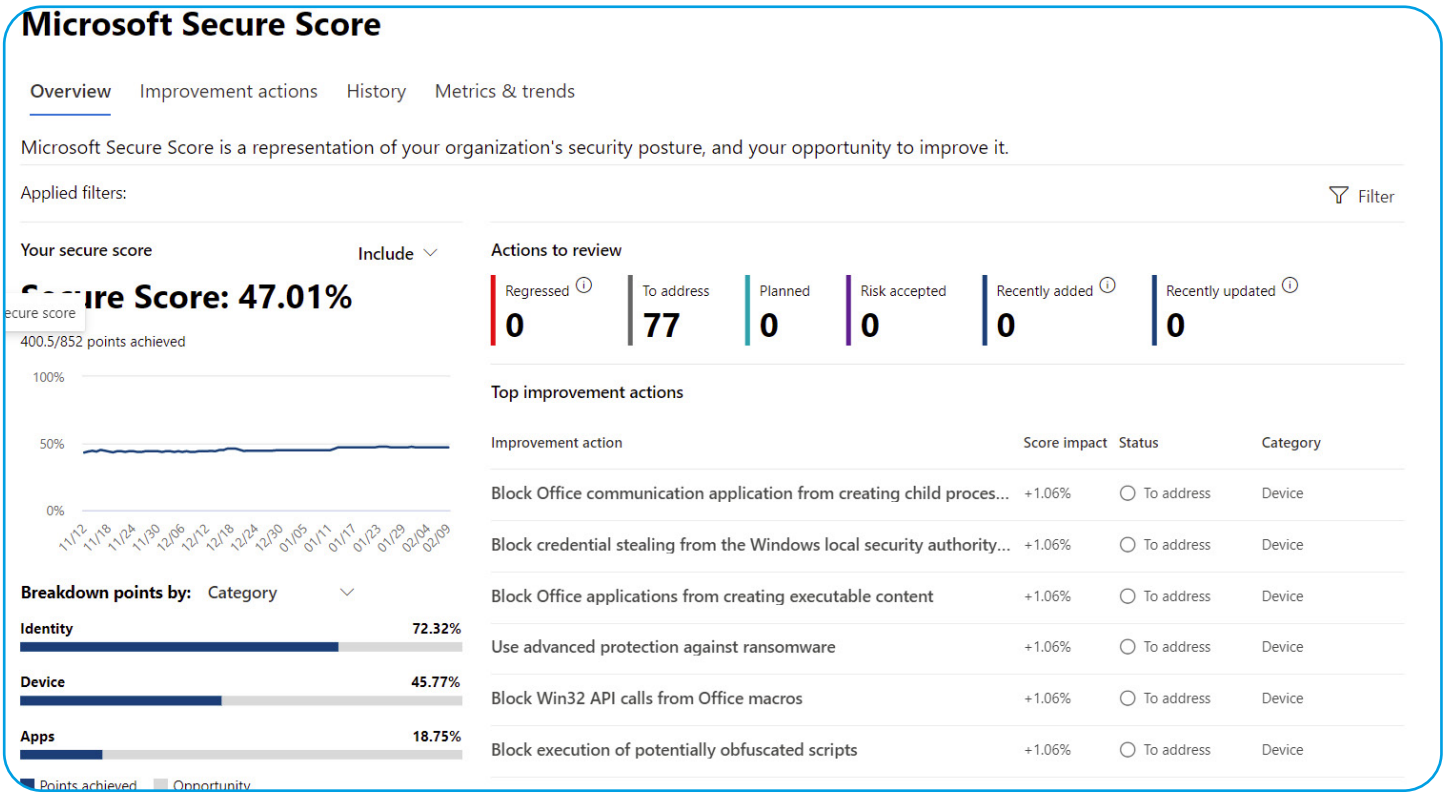
Cloud App Security SaaS catalog

15.5: SECURE SCORE

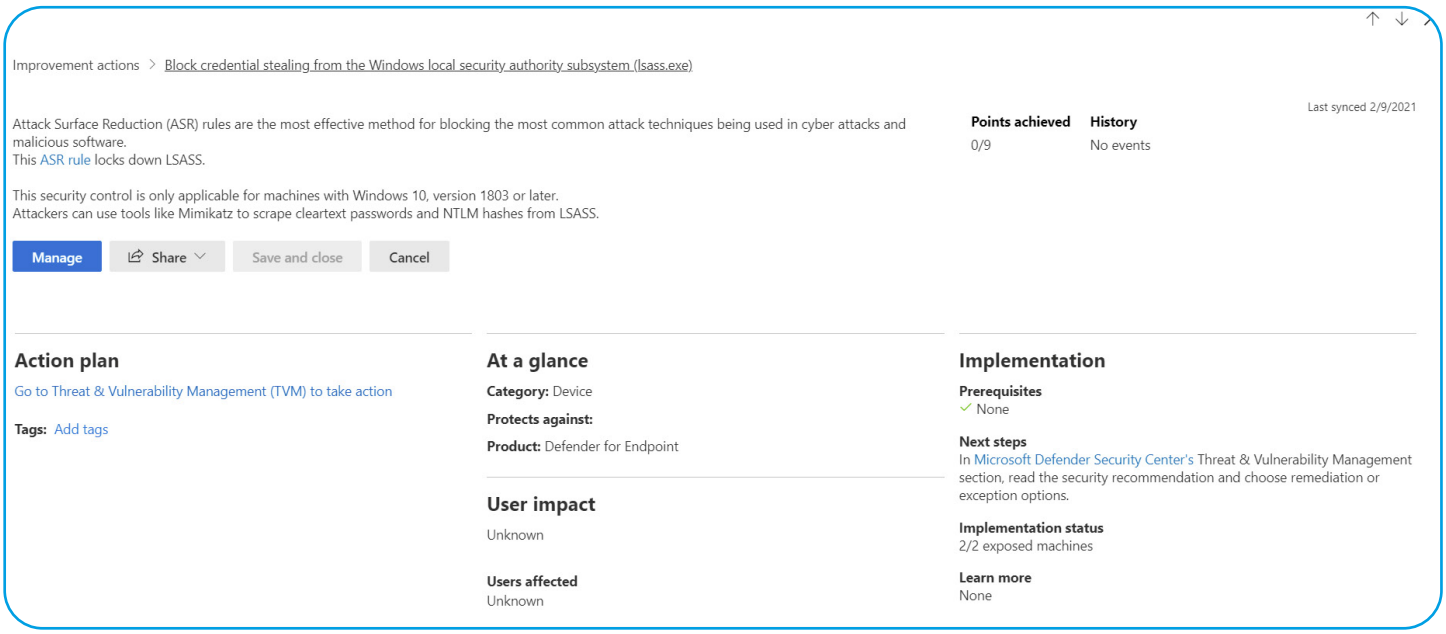
In the last chapter and this one we've looked at many of the security controls that you can use. But where do you start? How do you know what's most important to attend to? And where in all the different portals (or PowerShell) do you go to configure each setting?

The answers to these questions are in Secure Score, now part of the **Security portal**. Here you see an overall score for your tenant (for Identity / Data / Device / Apps and Infrastructure controls) and can compare it to the global average across M365, the average for your industry and for businesses of the same size. On the second tab you can see actions you should take to improve your score, how many points each action will give you and the user impact and administrative effort required.

The answers to these questions are in Secure Score, now part of the **Security portal**. Here you see an overall score for your tenant (for Identity / Data / Device / Apps and Infrastructure controls) and can compare it to the global average across M365, the average for your industry and for businesses of the same size. On the second tab you can see actions you should take to improve your score, how many points each action will give you and the user impact and administrative effort required.



Cloud App Security SaaS catalog



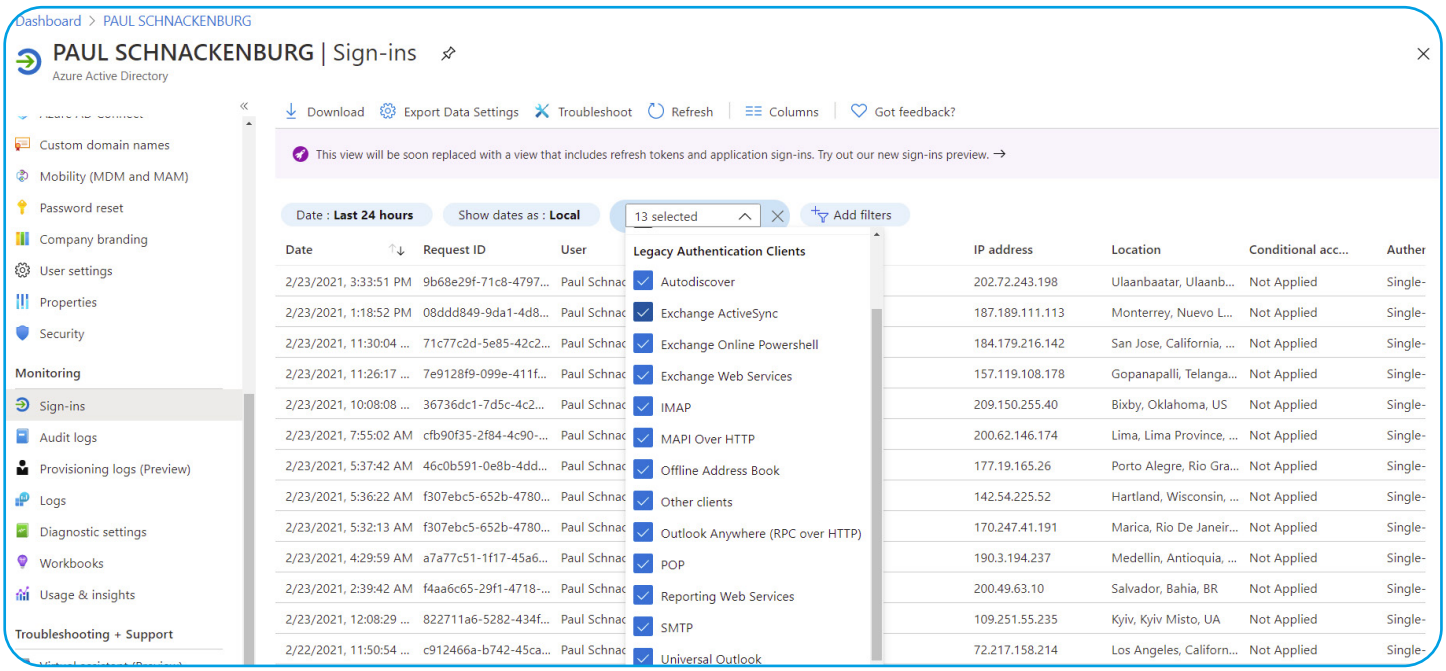
Example action to improve your security

Clicking on an action provides details as to what risks the control mitigates, which compliance regulation it matches, the ability to click a button to go directly to the right area to configure it and the option to tell the system that you have already mitigated this risk with a third-party service.

As you implement more controls you score increases (it can take 24-48 hours), and you track your progress on the History tab. Secure Score is the BEST place to start improving your tenant's security posture.

I'd like to highlight another control (apart from MFA) that'll gain you a quick win to improve overall security – **blocking legacy authentication**. This is because even if you have enabled MFA, attackers can still access your user's accounts with just a username and password through older protocols that don't support MFA. To investigate if there are any legitimate connections using these older protocols (which will need to be upgraded or exempt from your block legacy authentication policy) go to the Azure AD portal, click on Sign-ins under monitoring, click Add filters, pick Client app, then click "None selected" and add all 13 legacy connection options.

Here you can see a tenant with MFA enabled but legacy authentication still enabled with numerous failed access attempts.

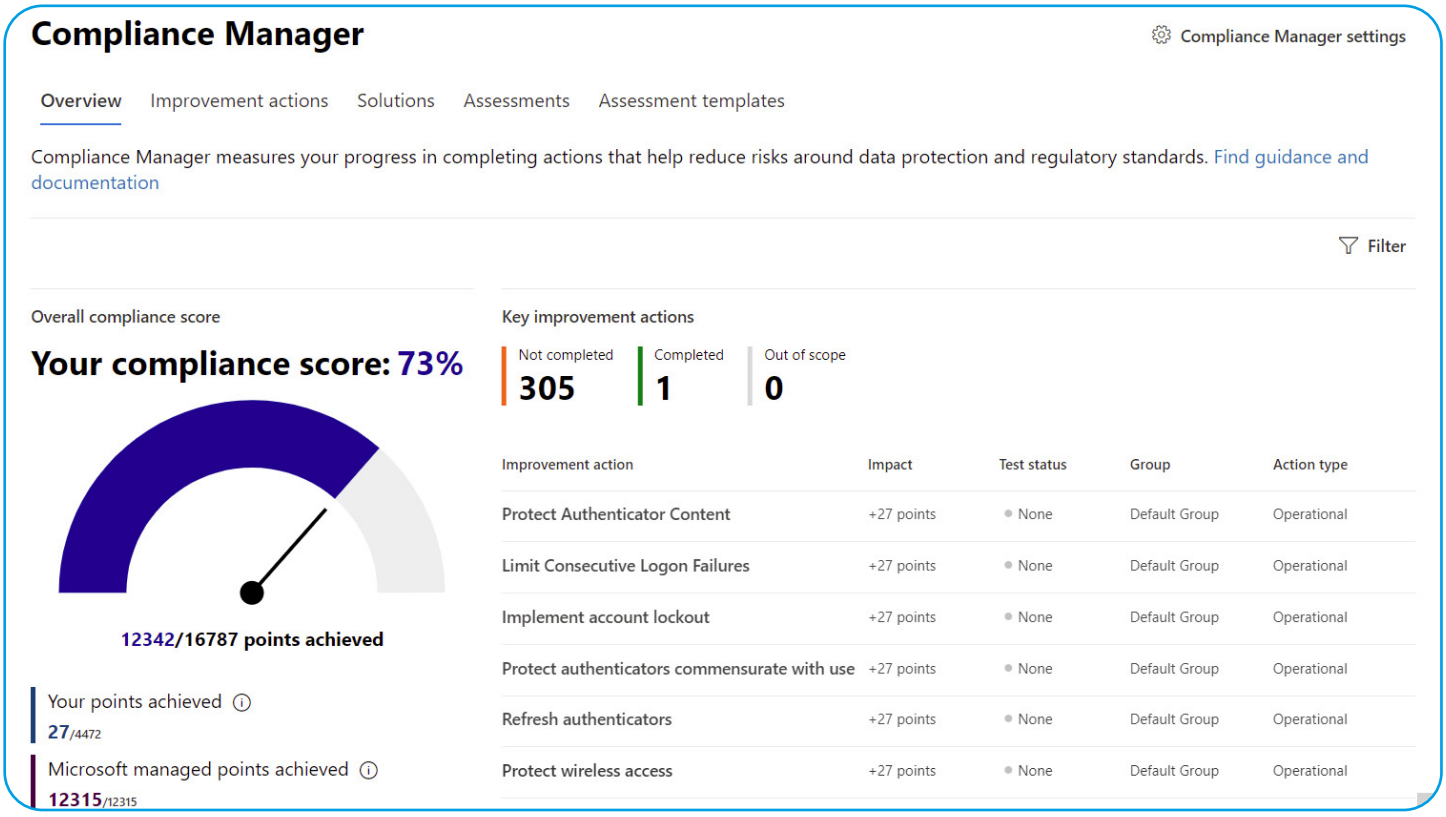


Entra ID Sign-in attempts using legacy authentication

Once you're certain there are no legitimate needs for legacy authentication, use **CA policies to block it.**

The concept of Secure score has spread to other parts of M365, in **Compliance Manager** there's Compliance Score to indicate how compliant your business is with regulatory frameworks you have to comply with. Microsoft has recently added hundreds of additional regulations from all over the world to help you track your compliance, assign tasks users to achieve and maintain compliance.

To manage compliance for your SharePoint and OneDrive sites and their security posture / sharing settings using the built in tools is an exercise in frustration as they're spread across several portals. In contrast, Hornetsecurity's **365 Permission Manager** provides a single pane to see the settings for every site in your tenant, apply policies, remediate compliance violations, see all access that a particular user has, produce reports and much more.



Compliance score in Compliance Manager

15.6: SECURITY IS EVERYONE'S RESPONSIBILITY

The last two chapters have given you a high-level overview of the many security features available across M365. The sad truth is that most small to medium businesses don't implement nearly enough of the features they have already paid for and even large enterprises struggle to get these protections in place for all their users.

This is partly due to the inherent complexity of many of Microsoft's native security features - remember the saying, "Complexity is the enemy of security". That's why many organizations are turning to third-party security solutions like Hornetsecurity to help them make key security features more accessible and reduce complexity.

On the other hand, security neglect is also due to a certain carelessness, which stems from the fact that in many businesses a mindset from the on-premise era still prevails, in which it was thought that (almost) everything was already done with a firewall - and IT shops will take care of it.

The world is a different place today: We must understand that the responsibility for security is in all of our hands and that our cyber defense chain can only be as strong as its weakest link.

Consider security awareness training for employees since it is essential to reduce the risk of cyberattacks, prevent data breaches, and ensure compliance with regulations. It empowers employees to recognize and respond to security threats, fostering a strong cybersecurity culture and protecting both company assets and reputation. Ultimately, investing in awareness training leads to cost savings and a safer digital environment.

15.7: KEEPING MICROSOFT HONEST

If the thought of paying for the underlying platform from Microsoft, and then paying again for the additional security features on top doesn't sit right with you, consider a third-party solution for your M365 security and compliance needs. Hornetsecurity offers **several different plans** with powerful Advanced Threat Protection for your email, data loss prevention (DLP), security awareness service (end user phishing simulation and training), email encryption, email archiving and more.

Hornetsecurity also offers an entire free eBook focused on securing a Microsoft 365 tenant, **The Microsoft 365 Security Checklist**. It covers all the security settings and configurations you need to know for each M365 license to properly secure your environment and goes into more detail of the actual settings than outlined here.

ELEVATE YOUR COMPLIANCE WITH EFFECTIVE PERMISSION MANAGEMENT
AVAILABLE IN
365 TOTAL PROTECTION
PLAN 4 - COMPLIANCE & AWARENESS
FREE TRIAL

CHAPTER 16:

BACKUP IN MICROSOFT 365

IN THIS CHAPTER WE LOOK AT THE NEED FOR DATA PROTECTION IN MICROSOFT 365 – WHAT MICROSOFT IS RESPONSIBLE FOR – AND WHAT YOUR ORGANIZATION IS RESPONSIBLE FOR.

16.1: NATIVE DATA RESILIENCY

As any capable cloud service, Microsoft takes the availability of customers data in M365 very seriously. As previously mentioned, **Exchange mailboxes have four copies**, three up to date ones and a fourth, lagged copy (up 24 hours behind). This last copy is used in case of a systemic corruption of the other three copies. These four copies are distributed across at least two datacentres. All of this is handled automatically by the system and not something end users will notice.

SharePoint and OneDrive for Business **storage similarly relies on data being stored in two separate Azure regions** – a write will only be considered completed if it's successfully written to both regions. And the underlying storage uses Append-Only, ensuring that earlier data can't be corrupted or encrypted by an attacker. This versioning also allows the restore of previous versions of files.

Sounds good right? Microsoft clearly takes steps to protect my data, so I don't have to worry about it? Not so fast – everything described above is about data resiliency, and high availability of your data. What it doesn't provide, outside of some limited options, is backup of your data.

Backup are copies of your production data, in a separate system, that's regularly (every hour, every day) copied from production data to the backup location. This provides the following features:

- The ability to "go back in time" and restore emails / documents / mailboxes / sites to a previous point in time – either to a production location, or a separate export location.
- The ability to access your production data in case of a catastrophic failure or outage of services in Microsoft 365.

In other words, data resiliency / high availability is not the same as backup. They're related but serve different purposes. Depending on your business needs or which compliance regulations you must comply with, you may need both.

Let's cover your native options for restoring earlier versions of data. With **Exchange items** (emails, contacts, calendar appointments), when they're deleted you can recover them from the Outlook Deleted Items folder. They're kept **there indefinitely** unless you change the policy in your tenant. If they're deleted from the Deleted Items folder, you can recover them for up to 14 days from the Recoverable Items hidden folder. You'll need to train your users how to do this themselves, or make sure your helpdesk team is prepared to assist on a regular basis as the user interface isn't exactly intuitive.

In SharePoint / OneDrive for Business **deleted documents** are kept by default for 93 days, first in a user accessible recycle bin, and if they're purged from there, in an administrator accessible recycle bin. Again, the restore process for a document deleted by mistake isn't straightforward so some training will be required.

To alter the defaults, you can use **Retention Policies** to keep items for longer (they're available for restore, even if users delete them out of their Deleted Items folder), these can be applied to both Exchange and SharePoint data. For Exchange you also use **In-Place and Litigation Holds** for select mailboxes to manage retention.

16.2: 365 TOTAL BACKUP

If you're looking to alleviate the challenges with using the built in data protection features as a recovery solution, Hornetsecurity provides a comprehensive M365 backup and recovery solution **365 Total Backup** or as part of **365 Total Protection Compliance & Awareness** . This protects mailboxes, Teams Chat, OneDrive for Business storage, SharePoint sites, plus Windows endpoints. It's simple to set up and provides comprehensive protection across your entire tenant.

NEVER STOP LEARNING!

We hope that this book and its links to more in-depth technical information has helped guide you on your journey to the cloud and once you have migrated, the continuing journey, as managing the ever-changing landscape of M365 is a never-ending ride.

As mentioned in Part 1, keeping abreast of the latest apps and features in M365 is a never-ending task so regularly check in with the official Microsoft resources but also be sure to visit the **Hornetsecurity blog** for articles on M365 administration and security.

If you prefer to consume your content in audio or video format, check out **The Security Swarm Podcast** – a weekly conversation of the most critical issues facing the world of cybersecurity today, hosted by Andy Syrewicze, Security Evangelist at Hornetsecurity. From the malicious use of AI tools to social engineering scams, each episode hones in on a pertinent topic dissected by an industry expert and backed up by real-world data direct from our Security Lab

Good luck!

ABOUT HORNETSECURITY GROUP

HORNETSECURITY

Hornetsecurity is a leading global provider of next-generation cloud-based security, compliance, backup, and security awareness solutions that help companies and organizations of all sizes around the world. Its flagship product, 365 Total Protection, is the most comprehensive cloud security solution for Microsoft 365 on the market. Driven by innovation and cybersecurity excellence, Hornetsecurity is building a safer digital future and sustainable security cultures with its award-winning portfolio.

Hornetsecurity operates in more than 30 countries through its international distribution network of 8,000+ channel partners and MSPs. Its premium services are used by more than 50,000 customers.

For more information, visit **www.hornetsecurity.com.**

ABOUT THE AUTHOR

PAUL SCHNACKENBURG
MICROSOFT CERTIFIED TRAINER

Paul started in IT when DOS and 286 processors were the cutting edge. He runs Expert IT Solutions, a small business IT consultancy on the Sunshine Coast, Australia. He also works as an IT teacher at a Microsoft IT Academy. Paul is a well-respected technology author and active in the community, writing in-depth technical articles, focused on Hyper-V, System Center, private and hybrid cloud and Office 365 and Azure public cloud technologies. He holds MCSE, MCSA, MCT certifications.

HORNETSECURITY | ars DISTRIBUTION Make IT easy

365 TOTAL PROTECTION

PLAN 4 - COMPLIANCE & AWARENESS

NEXT-GEN PROTECTION FOR MICROSOFT 365:
EMAIL SECURITY, BACKUP, COMPLIANCE & SECURITY AWARENESS

PLAN 1	PLAN 2	PLAN 3	PLAN 4
BUSINESS	ENTERPRISE	BACKUP	COMPLIANCE & AWARENESS
SPAM & MALWARE PROTECTION	ADVANCED THREAT PROTECTION	BACKUP & RECOVERY OF MAILBOXES & TEAMS	PERMISSION MANAGEMENT
EMAIL ENCRYPTION	EMAIL ARCHIVING	BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT	PERMISSION ALERTS
EMAIL SIGNATURES & DISCLAIMERS	EMAIL CONTINUITY	BACKUP & RECOVERY OF ENDPOINTS	PERMISSION AUDIT
			PHISHING & ATTACK SIMULATION
			SECURITY AWARENESS
			ESI® REPORTING
			COMMUNICATION PATTERN ANALYSIS
			AI RECIPIENT VALIDATION
			SENSITIVE DATA CHECK

365 Total Protection covers all aspects of an organization's Microsoft 365 security management and data protection: email security, backup and recovery, compliance, permission management and security awareness. The solution integrates seamlessly with Microsoft 365, providing much-needed layers of additional security and data protection against spam, malware, and advanced threats.

FREE TRIAL