



# CYBERSECURITY THREATS AND HOW **MICROSOFT 365** CAN HELP PROTECT YOUR MOST SENSITIVE DATA

27<sup>th</sup> May 2021

Thank you for joining – we'll be starting soon



**the I.T. team**<sup>™</sup>  
Maintaining the health of your I.T. system



# WHAT DO WE HOPE YOU TAKE AWAY?

- Learn about possible attacks to your organisation
- Overview of the large variety of Security/Compliance features in M365
- Takeaway the key essentials for your organization, and ideally a direction
- Prescription – Pathway
- Ask questions, questions, questions!



# About the I.T. team

- Formed in 2011
- Office 365 since its inception
- Managed Services/IT support
- A wide range of IT services
- Major NFP base of customers
- Providing IT services to NZ & Australian organisations

---

**the I.T. team**<sup>TM</sup>  
Maintaining the health of your I.T. system



# IMPORTANCE OF SECURITY

- Attacks are increasing in frequency
  - Attacks are increasing in sophistication
  - Expectations are rising
  - NFP/NGO's have highly sensitive data
  - Ransomware and financial threats are becoming a factor and can be devastating
-



# HISTORICAL CONCERNS/PRIORITIES

1. Organisation from being prevented from working (and loss of data)
  2. Organisation (and individuals) having reputation damage
  3. Business Secrets and Finances being leaked out
  4. Customer/Personal private data being leaked
  5. Accidental leaking of sensitive data (from authorised personnel)
  6. Intentional extraction/leaking of sensitive data
-



# CLASSES OF PROTECTION

- Continuity
    - Security protection to prevent/minimise outages and lost productivity, includes Ransoms
  - Data Privacy/Security
    - Preventing data from being extracted by third parties
  - Data Traversal/Exfiltration Protection
    - Preventing unintentional and intentional data leaks from the inside.
-



# TYPES OF ATTACKS

- **Phishing** – Attacker targets employees by email or other unsafe links or websites
  - **Spear-Phishing** – attacker uses information specifically about a user to construct a more plausible Phishing attack
  - **Brute Force Attack** – attacker tries a large list of possible (or leaked) passwords for an account or set of accounts
  - **Device Compromise** – Malware on a device (virus, ransomware etc) without consent
  - **Lost or Stolen Device** – intentional or unintended access to a device
-

# Common Phishing

Action Required: Update your payment information now



○ Microsoft Online Services

○ [Redacted]

Thursday, October 4, 2018 at 8:15 PM

[Show Details](#)

Action Required: Update your payment information now

[email@microsoftonline.com](mailto:email@microsoftonline.com)>

⚠ To protect your privacy, some pictures in this message were not downloaded.

[Download pictures](#)

Attention: Your payment has been declined. Please update your payment information today to avoid service interruption. | [View this email in your browser.](#)

Office 365

## Your payment has been declined.

Please update your payment information now.

### UPDATE YOUR PAYMENT INFORMATION

**Organization:** Corporation

Our records indicate that the payment method you used to purchase Office 365 Business Premium was declined. Please contact your bank for the details on the failed charges.

**To avoid service interruption, please update your payment information now.**

Sign in to the [customer portal](#) with your User ID:

**Name:** John Doe

**User ID:** admin@corporation.com

We appreciate your prompt attention to this matter, and look forward to continuing to meet your business needs.

Sincerely,

The Microsoft Online Services Team





login



Not secure

agilones.com/Activate/#john@doe.com



← john@doe.com

Enter password

Password

[Forget Password](#)

Sign in

# MICROSOFT 365 vs OFFICE 365 PLANS

---

BUSINESS LICENSES				ENTERPRISE LICENSES	
<b>MICROSOFT 365 BUSINESS BASIC</b>  <i>formerly Office 365 Business Essentials</i>	<b>MICROSOFT 365 BUSINESS STANDARD</b>  <i>formerly Office 365 Business Premium</i>	<b>MICROSOFT 365 BUSINESS PREMIUM</b>  <i>formerly Microsoft 365 Business</i>	<b>MICROSOFT 365 BUSINESS APPS</b>  <i>formerly Office 365 Pro Plus</i>	<b>MICROSOFT 365 E3</b>	<b>MICROSOFT 365 E5</b>
Free	\$3.00 per user/month	First 10 licenses free; \$5.00 per user/month thereafter	\$3.00 per user/month	\$8.00 per user/month	\$22.80 per user/month



# CORE SERVICES IN M365

## Central Features of M365

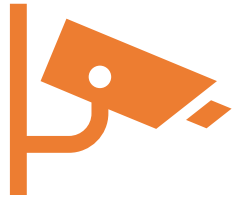
- Exchange Online (Email)
- Office Software (Word, Excel, Outlook)
- Sharepoint & OneDrive (Document Storage)
- Azure AD/Intune

## Assumptions?

---

## Priorities Preview

	01	02	03	04	05	06	07	08	09
Windows Updates	✓	✓	✓	✓	✓	✓	✓	✓	✓
Exchange Online Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windows Defender Antivirus	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multifactor Authentication		✓	✓	✓	✓	✓	✓	✓	✓
Defender for 365 (ATP)			✓	✓	✓	✓	✓	✓	✓
Azure AD Workplace Join				✓	✓	✓	✓	✓	✓
BitLocker				✓	✓	✓	✓	✓	✓
Conditional Access				✓	✓	✓	✓	✓	✓
Data Loss Protection Basic					✓	✓	✓	✓	✓
MDM (Mobile Device Mgmt)						✓	✓	✓	✓
Defender Firewall/Exploit							✓	✓	✓
Defender Identity/Endpoint								✓	✓
Risky Sign Ins								✓	✓
Data Loss Protection Adv.									✓
Microsoft 365 License: Basic	Basic		Premium					E5	



Security



Compliance



Identity



# SECURITY FEATURES

- Defender Firewall
  - Defender Exploit Guard
  - Defender Credential Guard
  - BitLocker
  - Windows Information Protection
  - Microsoft Defender 365 (AKA Advanced Threat Protection)
-



# COMPLIANCE FEATURES

- Azure Information Protection
  - 365 DLP for Emails & Files
  - Sensitivity Labels (Manual)
  - Retention Labels (Manual)
  - Litigation Hold
  - Office Message Encryption (Basic)
-



# IDENTITY FEATURES

- AD Premium (Plan1)
  - On Prem AD Sync for SSO
  - Cloud App Security Discovery
  - MFA
  - Conditional Access
  - Windows Hello for Business
-





# FOCUS FEATURES FOR TODAY

- Intune (Pre-requisite)
  - MFA (Identity)
  - Microsoft Defender for Office 365 (Security)
  - BitLocker (Security)
  - Defender Exploit Guard & Credential Guard (Security)
  - Litigation Hold (Compliance)
  - DLP (Compliance)
-

# Intune (Pre-Requisite)

- Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM).
- You control how your organisation's devices are used, including mobile phones, tablets, and laptops.
- Manage Applications
- Manage Configurations
- Manage Compliance

The screenshot displays the Microsoft Intune management console. The top navigation bar includes 'Home' and 'Windows | Windows devices'. The left sidebar lists various management areas: Windows devices, Windows enrollment, Windows policies, Compliance policies, Configuration profiles, and PowerShell scripts. The main content area is divided into two sections. The upper section, titled 'Windows devices', shows a list of devices with columns for Device name, Managed by, Ownership, Compliance, OS, and OS version. The lower section, titled 'Manage applications', shows a list of applications with columns for Name and Type. Both sections include search bars and filter options.

Device name	Managed by	Ownership	Compliance	OS	OS version
ITT-5CG8171GP	Intune	Corporate	Compliant	Windows	10.0.19042.985
ITT-5CG8327N0W	Intune	Corporate	Compliant	Windows	10.0.21318.1000

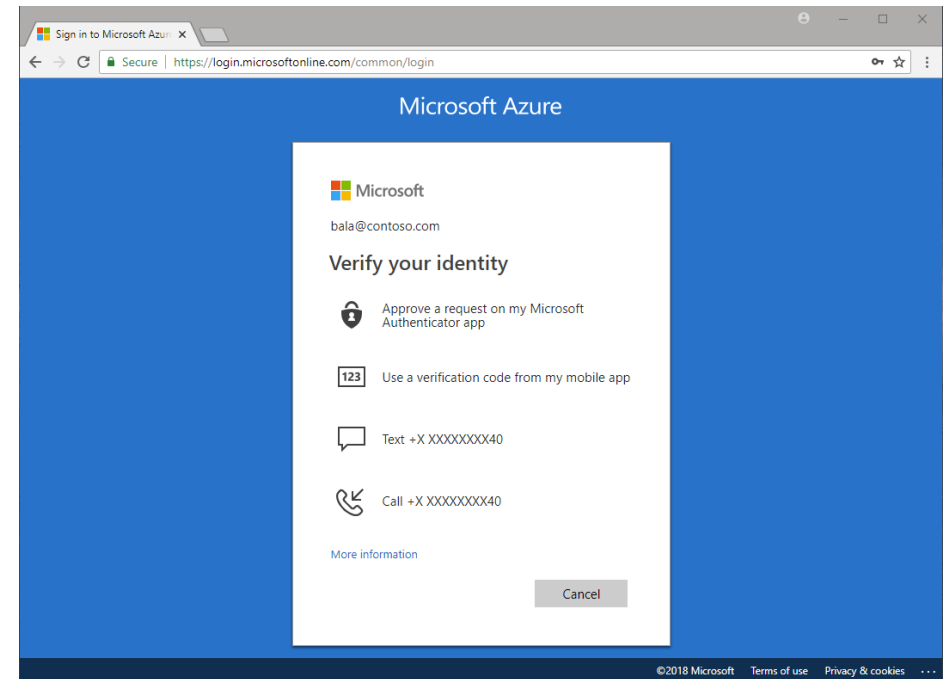
Profile name	Platform
Chrome - Custom Bookmarks	Windows 10 and later
Chrome - Enable Bookmarks Bar	Windows 10 and later
Chrome - Windows 10 Accounts	Windows 10 and later
Chrome ADMX Ingestion	Windows 10 and later

Name	Type
3CXPhone for Windows	Windows MSI line-of-business app
7-Zip	Windows MSI line-of-business app
Acrobat Reader DC	Windows app (Win32)
EPOS Connect	Windows MSI line-of-business app
Google Chrome	Windows MSI line-of-business app

# Identity – Multi Factor Authentication (MFA)

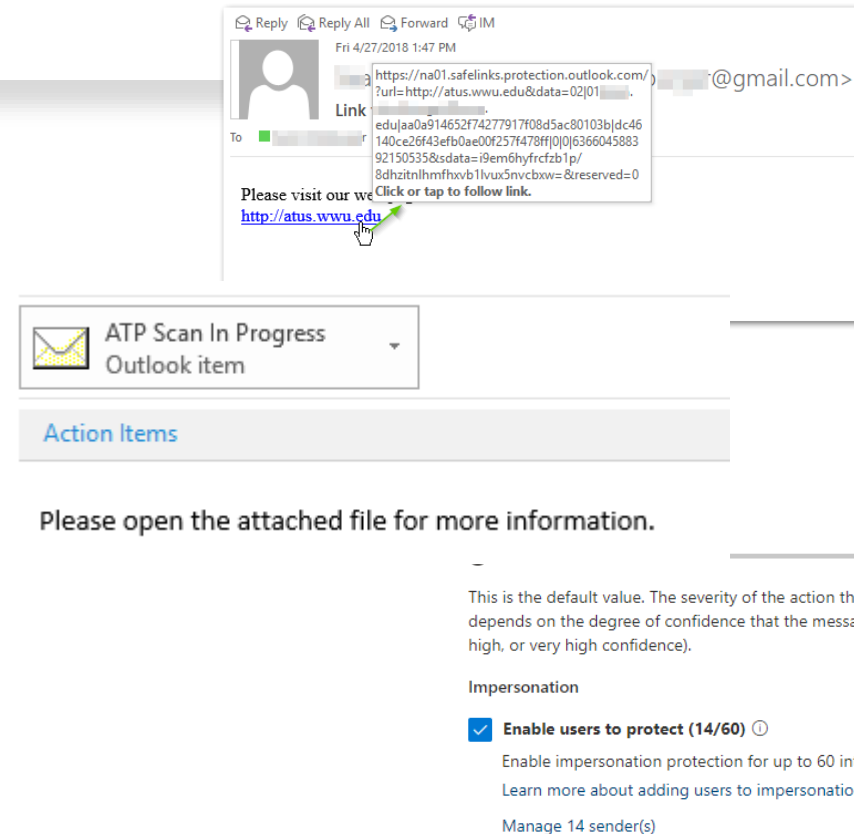
- Multifactor authentication (MFA) adds a layer of protection to the sign-in process. One factor authentication is just a password.
- Phone Call or SMS message
- App Code or Push Notification



# Security – Microsoft Defender for Office 365 (P1)

Contains the following technologies:

- Safe Links.
- Safe Attachments for SharePoint, OneDrive, and Microsoft Teams, Exchange.
- Anti-Phishing
- Real-time detections



# Security – BitLocker

Deployed with Intune

If computer is stolen, without the password the machine is useless.

If the device is stolen, the hard drive can not be taken out and its contents examined, as the data is encrypted.

Can set recovery key to be saved into Azure (Cloud) so if something happens to need the recovery key, it can be retrieved.





## BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

### Operating system drive

C: BitLocker on



-  Suspend protection
-  Change how drive is unlocked at startup
-  Back up your recovery key
-  Turn off BitLocker

### Fixed data drives

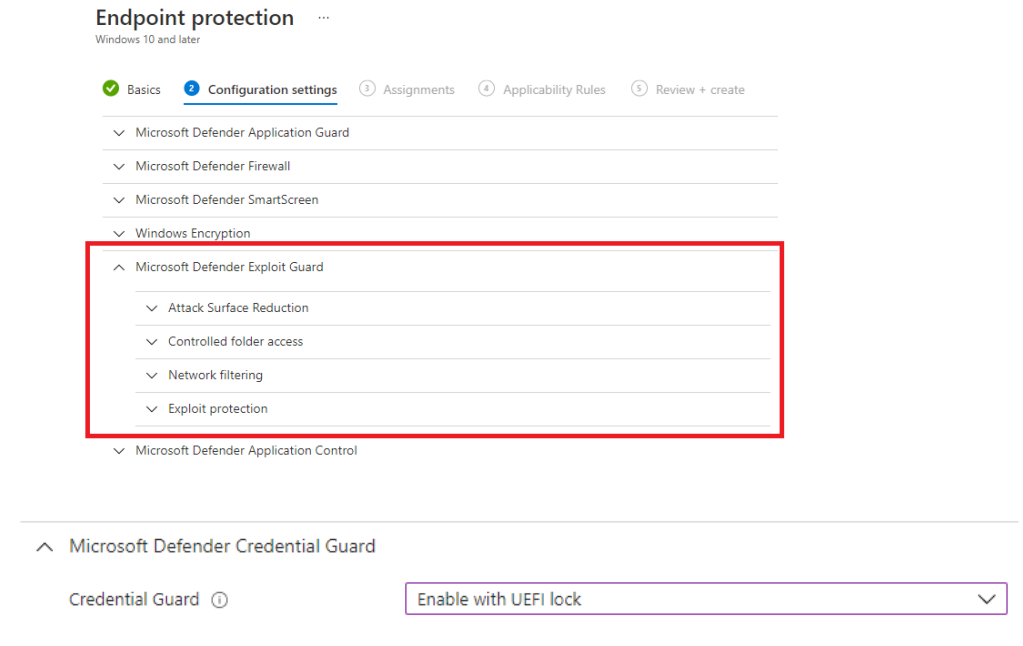
### Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

# Security – Microsoft Defender Exploit Guard

## Deployed with Intune

- **Attack Surface Reduction (ASR):** A set of controls that enterprises can enable to prevent malware from getting on the machine by blocking Office-, script-, and email-based threats.
- **Network Protection:** Protects the endpoint against web-based threats by blocking any outbound process on the device to untrusted hosts/IP through Windows Defender SmartScreen.
- **Controlled folder access:** Protects sensitive data from ransomware by blocking untrusted processes from accessing your protected folders.
- **Exploit Protection:** A set of exploit mitigations that can be easily configured to protect your system and applications.
- **Credential Guard:** virtualization-based security to isolate secrets so that only privileged system software can access them.

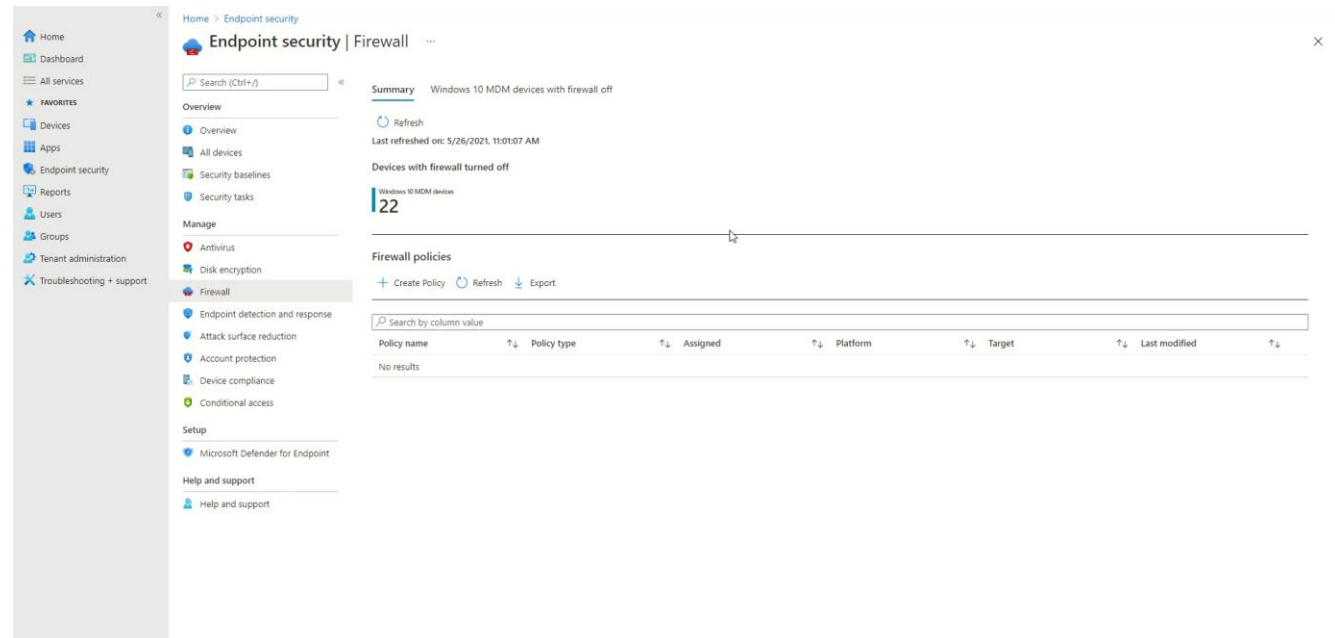


# Security – Microsoft Defender Firewall

A firewall is a network security system that monitors, and controls incoming and outgoing network traffic based on predetermined security rules.

Microsoft Defender Firewall can be managed from Intune:

- Forcing Microsoft Defender Firewall to be On in certain scenarios.
- Setting custom rules and pushing them out to all workstations.



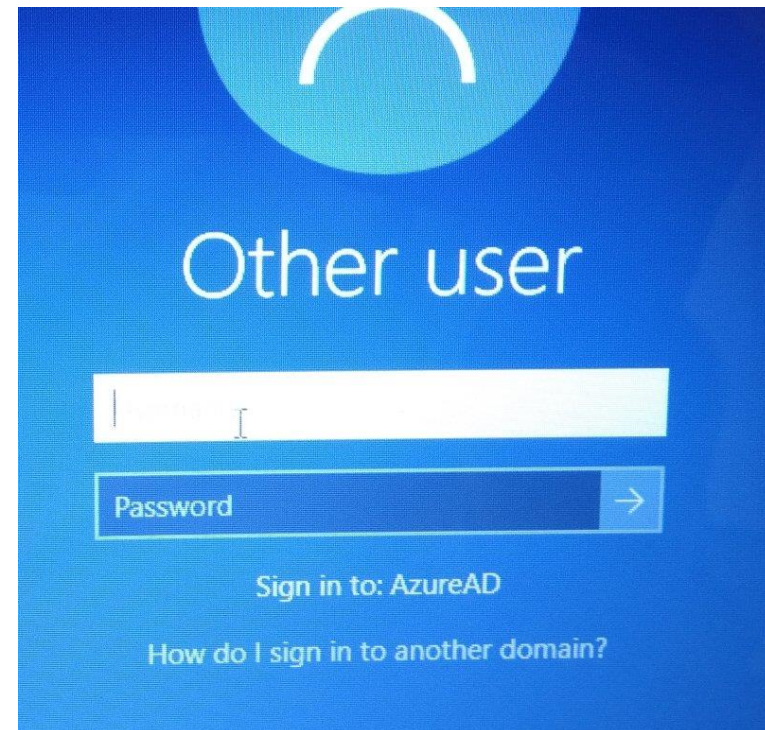
# Identity – AD Premium

Important for using **Azure AD Workplace Join** effectively:

- Allows Authentication of Workstation to AzureAD

Features over AD Basic:

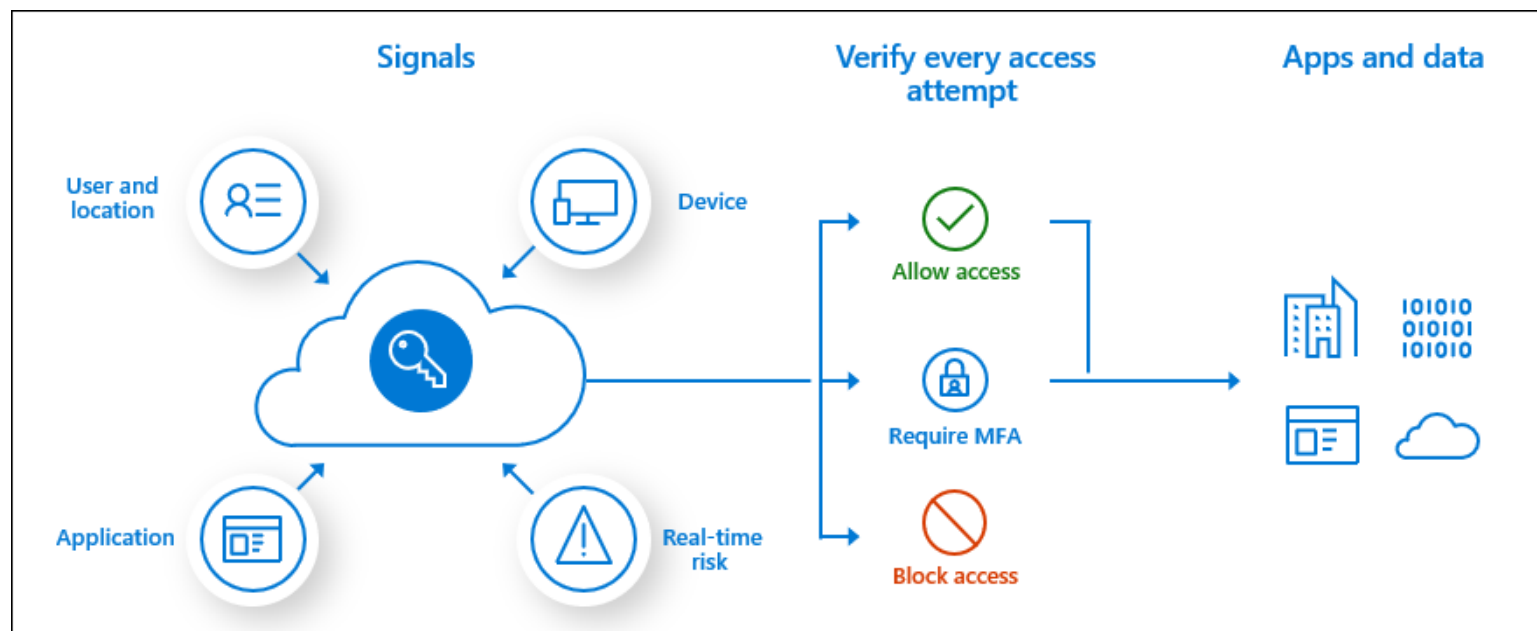
- Custom Banned Password
- Self-Service Password reset/change/unlock





# Identity - Conditional Access (& MFA)

Protects Cloud Applications from unauthorised access attempts.



# Identity - Conditional Access (& MFA)

Home >

Conditional Access | Policies ...

Azure Active Directory

«

+ New policy What if Refresh Got feedback?

Search policies Add filters

1 out of 1 policy found

Policy Name ↑↓	State ↑↓	Creation Date ↑↓	Modified Date ↑↓	
CA Policy	Report-only	5/18/2021, 11:46:10 AM	5/19/2021, 3:11:33 PM	...

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication context (Preview)
- Classic policies

Troubleshooting + Support

- Virtual assistant (Preview)
- New support request

# Compliance - Message Encryption (Basic)

## Office 365 Message Encryption

Allows you to send encrypted email to people inside or outside your organisation, regardless of the destination email address (Gmail, Yahoo! Mail, Outlook.com, etc.)

To view encrypted messages, recipients can either get a one-time passcode, sign in with a Microsoft account, or sign in with a work or school account associated with Office 365.



# Compliance – Litigation Hold

Prevents users from permanently deleting all or chosen content

Primary function of a Litigation Hold is to protect data in case there is a lawsuit in action, and some emails might be evidence

You can use it, as many other companies do, as a means to backup sensitive data, just in case

general

[Disable](#)

mailbox usage

contact information

MAPI: Enabled  
[Disable](#)

organization

email address

Litigation hold: Disabled  
[Enable](#)

► [mailbox features](#)

member of

MailTip

Archiving: Enabled  
Local archive created  
19.02 MB used, 0% of 50 GB.  
[Disable](#) | [View details](#)

mailbox delegation

Mail Flow

Delivery Options

Delivery options control forwarding and recipient limits.  
[View details](#)



# Compliance – Data Loss Prevention (DLP)

## What is Data Loss Prevention?

Detects sensitive content as it is used and shared throughout your organization, in the cloud and on devices, and helps prevent accidental data loss

- Block
  - Warn
  - Notify
-



# Compliance – DLP Sensitive Info Types

- Credit cards
- Bank Account number
- Drivers License number
- Inland Revenue / Tax Number number
- Ministry of Health / Medical Account Number
- Drivers Social Welfare number
- Business / Company Number
- Custom

*Next slide to showcase DLP warning on sending credit card info*

---

Info - Message (HTML)

Search

File

Message

Insert

Options

Format Text

Review

Help

Paste

Clipboard

Calibri (Bod)

11

A

A

Basic Text

Address Book

Check Names

Attach File

Link

Signature

Assign Policy

Follow Up

High Importance

Low Importance

Dictate

Sensitivity

Insights

View Templates

Send

To

[chris@yahoo.com](mailto:chris@yahoo.com)

Cc

Subject

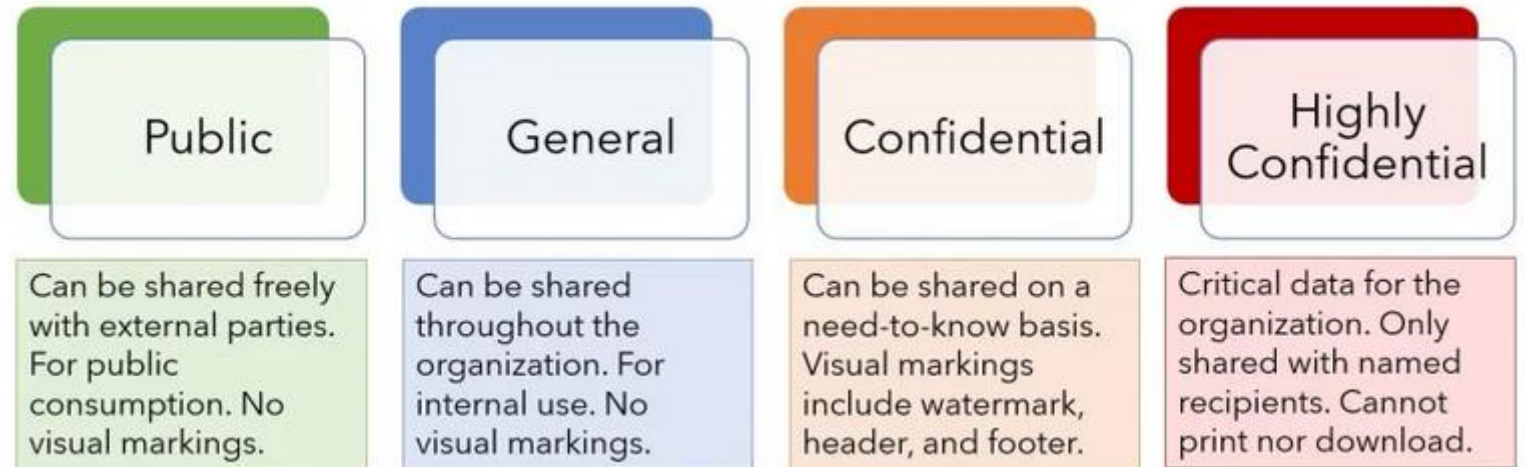
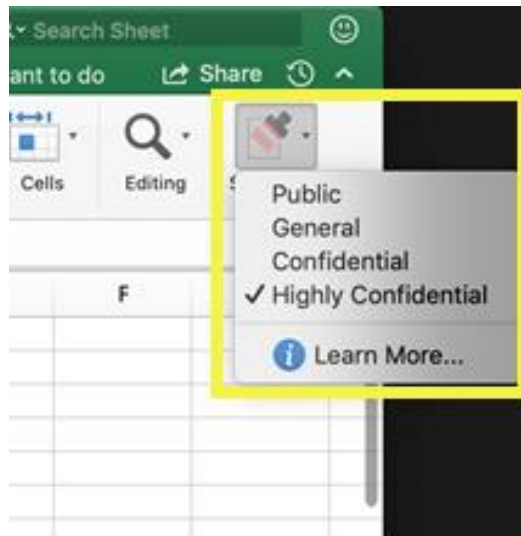
Info

Hi,

I

# Compliance –Sensitivity Labels

Enforce protection settings such as **encryption or watermarks** on labeled content. For example, your users can apply a **Confidential label** to a document or email, and that label can encrypt the content and apply a Confidential watermark

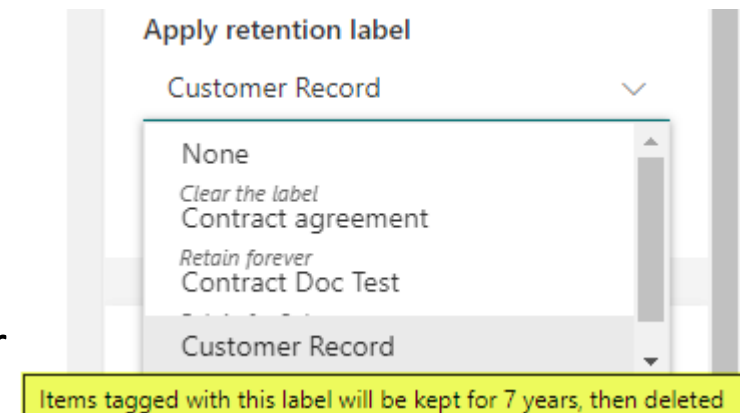




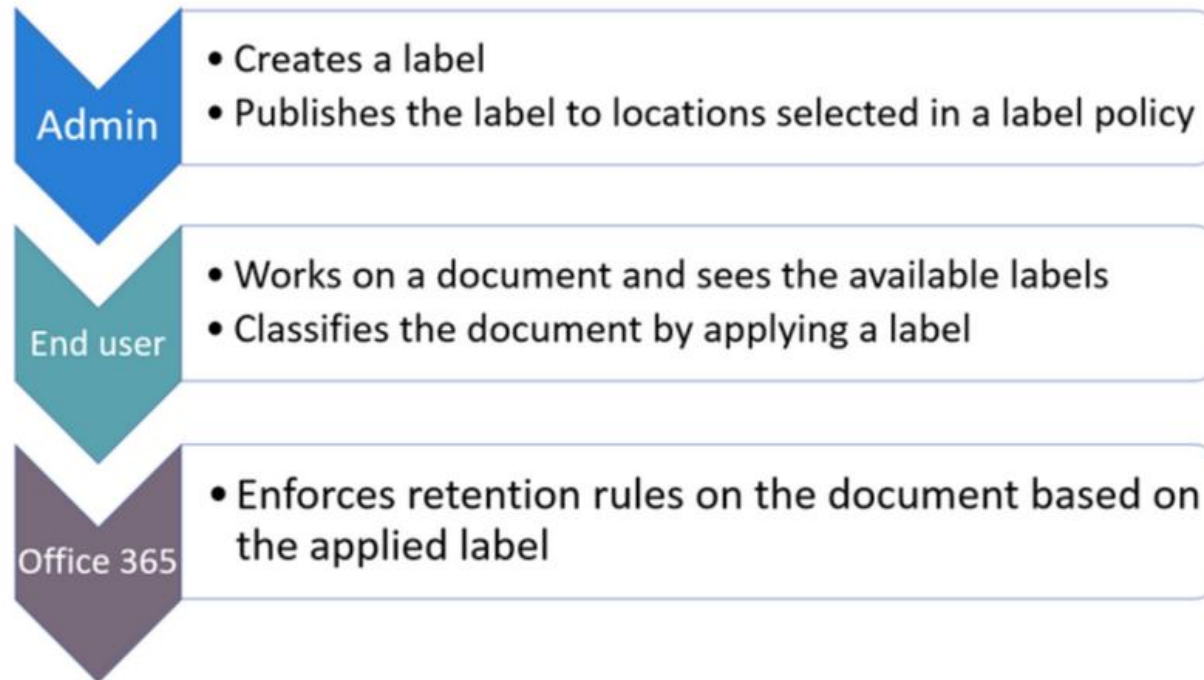
# Compliance – Retention Labels

Here are some things you can do with retention labels:

- Assign a label that **defines a date** upon which you can either delete the content or trigger a disposition review.
- Use a retention label to **classify content as a "record."** In this case, a label can't be changed or removed, and the content can't be edited or deleted.
- Start a retention period from when the **content is created** or from the time when the **label was applied**.
- Apply a default retention label to an entire document library

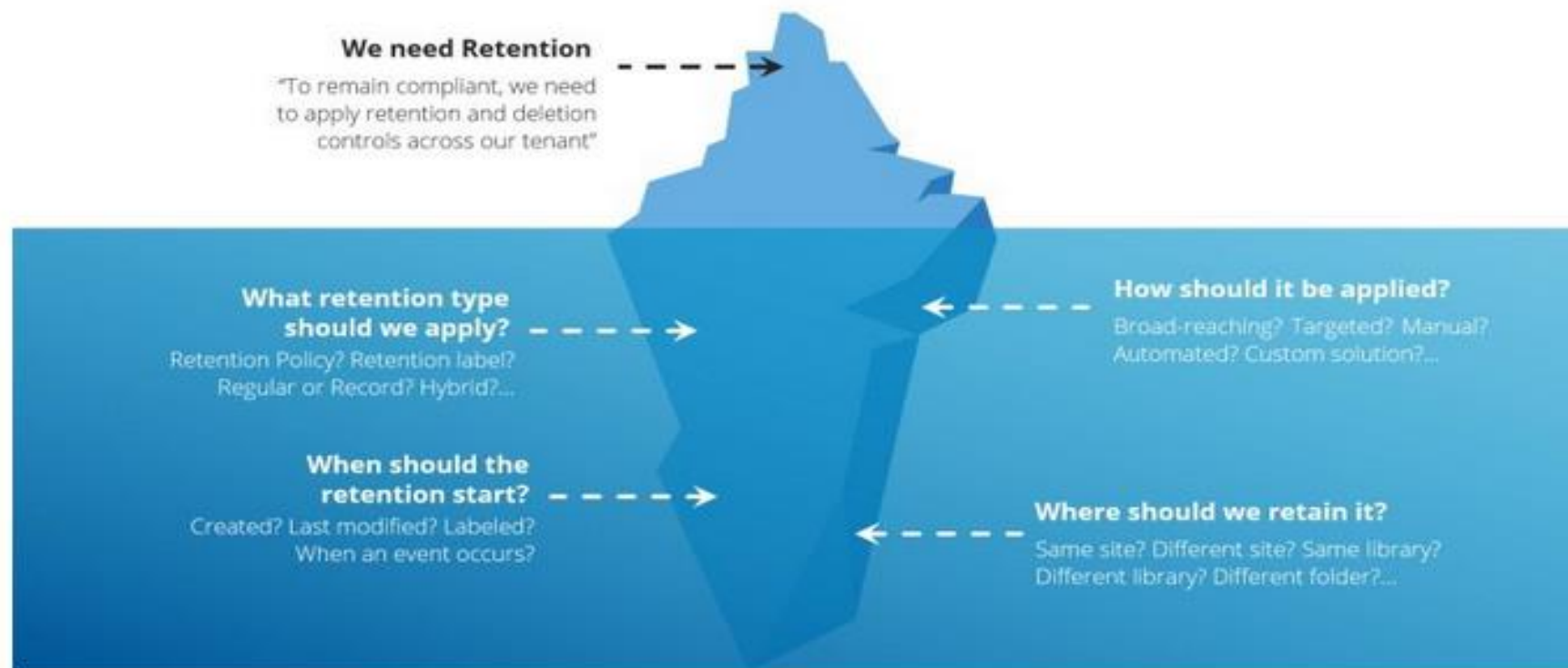


# Compliance – Labels Logical Workflow




# Compliance – Retention

## THE RETENTION ICEBERG



# Prescription

	01	02	03	04	05	06	07	08	09
Windows Updates	✓	✓	✓	✓	✓	✓	✓	✓	✓
Exchange Online Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windows Defender Antivirus	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multifactor Authentication		✓	✓	✓	✓	✓	✓	✓	✓
Defender for 365 (ATP)			✓	✓	✓	✓	✓	✓	✓
Azure AD Workplace Join				✓	✓	✓	✓	✓	✓
BitLocker				✓	✓	✓	✓	✓	✓
Conditional Access				✓	✓	✓	✓	✓	✓
Data Loss Protection Basic					✓	✓	✓	✓	✓
MDM (Mobile Device Mgmt)						✓	✓	✓	✓
Defender Firewall/Exploit							✓	✓	✓
Defender Identity/Endpoint								✓	✓
Risky Sign Ins								✓	✓
Data Loss Protection Adv.									✓
Microsoft 365 License: Basic	Basic		Premium						E5



# M365 E5 – Why?

- Trainable Classifiers to identify content to label
  - Automatic Sensitivity Labels
  - Auto-apply Retention labels based on machine learning classifiers
  - Advanced Audit & Advanced eDiscovery.
  - Azure AD Premium P2 – Risky Sign-ins, User Risk levels, Just-in-time privileged access
-

# Common attacks and Microsoft capabilities that protect your organization

Capabilities with blue text are included in this guidance.







# QUESTION TIME

[webinar@theitteam.co.nz](mailto:webinar@theitteam.co.nz)



# THANK YOU

the I.T. team has been in business since 2011.

Our focus has always been on offering a fresh range of I.T. related services and support designed to help client organisations maximise productivity and protect themselves from all kinds of data related risks.

**the I.T. team**<sup>™</sup>  
Maintaining the health of your I.T. system

---

[theitteam.co.nz](http://theitteam.co.nz)

**Maintaining the health of your I.T. system**

**the I.T. team**<sup>™</sup>  
Maintaining the health of your I.T. system