

“Security is our top priority and we are committed to working with others across the industry to protect our customers.”

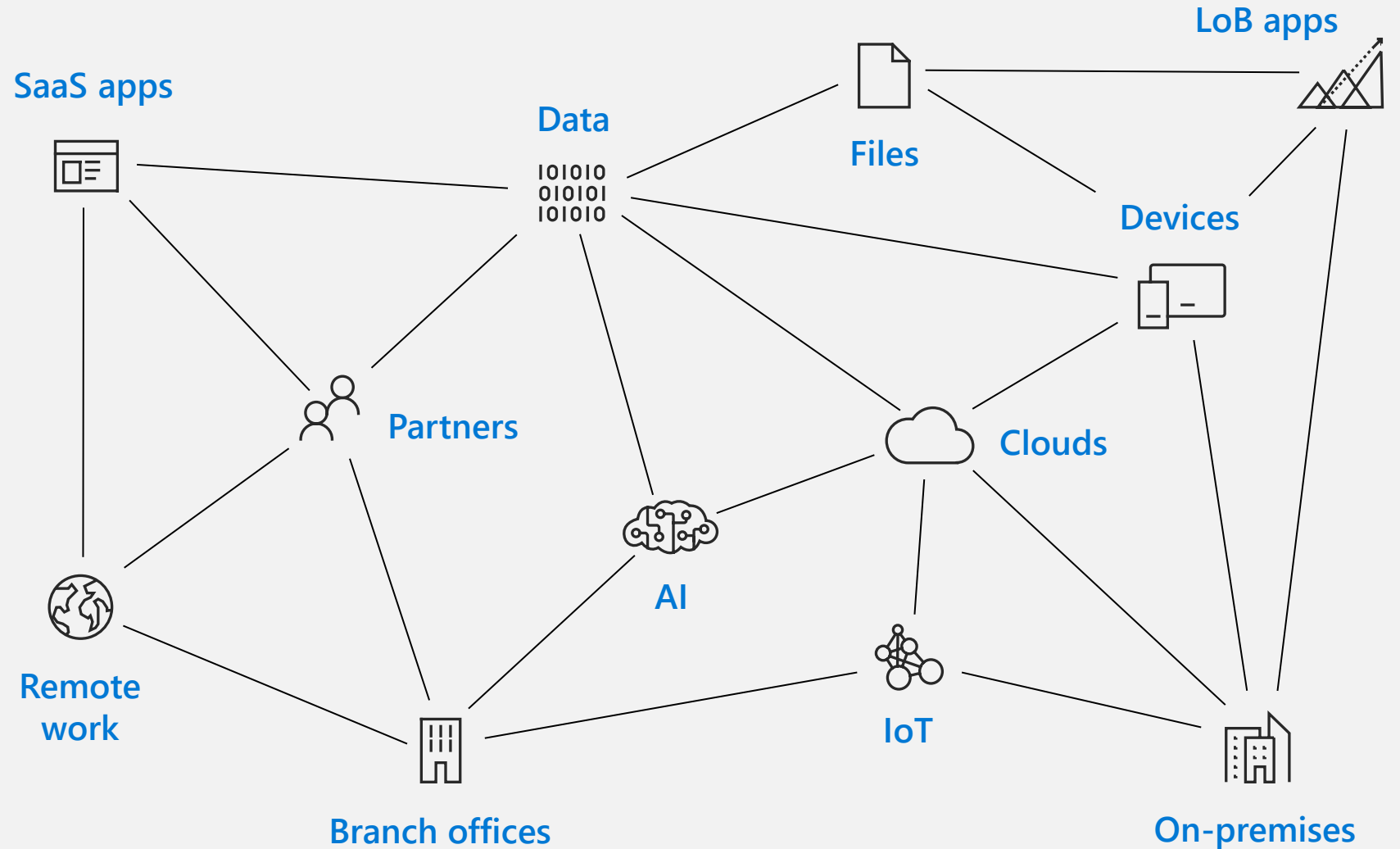
Satya Nadella
Chief Executive Officer, Microsoft Corporation

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships





Digital transformation has stressed your existing security practices



SaaS adoption challenge

73%

of enterprises indicated security as a top challenge holding back SaaS adoption*

80%

>80% of employees admit to using non-approved SaaS apps in their jobs**

• Cloud Security Alliance (CSA) survey, Cloud Adoption, Practices and Priorities Survey Report 2015

** <http://www.computing.co.uk/ctg/news/2321750/more-than-80-per-cent-of-employees-use-non-approved-saas-apps-report>

Identity may be your biggest weakness

~ 2B

The global
mobile workforce
by 2020¹

73%

of passwords
are duplicates²

40%

of passwords
are eventually
compromised³

1. Strategy Analytics. "Global Mobile Workforce Forecast Update 2016-2022." Oct 2016.
2. Entrepreneur.com. "Password Statistics: The Bad, The Worse, and The Ugly." June 3, 2015.
3. DARKReading. "Data Breach Record Exposure Up 205% from 2016." Nov 8, 2017.

Cybercriminals target businesses of all sizes

One in four SMBs targeted ⁽¹⁾



24% customer's privacy violated
20% trade secrets leaked

Average loss ⁽²⁾

\$79,841



33% spent more solving the problem
than it would have cost to prevent it ⁽¹⁾

(1) Source: Small Business Cyber Security Study, Microsoft & YouGov, April 2018

(2) Source: Better Business Bureau "2017 State of Cybersecurity Among Small Businesses in North America." https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

Microsoft Security



Identity and access management

Your universal platform to manage and secure identities.



Threat protection

Stop attacks with integrated and automated security.



Information protection

Protect your sensitive data—wherever it lives or travels.



Cloud security

Safeguard your cross-cloud resources.

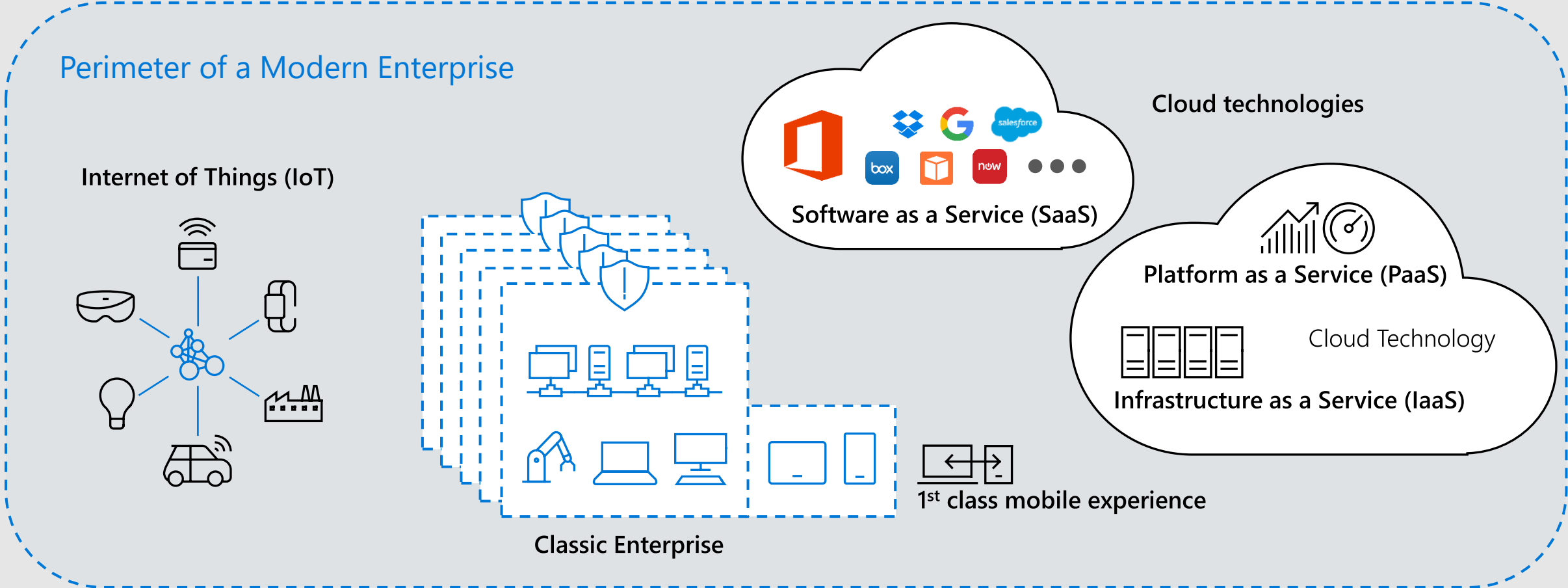


**So why is Identity
so important?**



Your Enterprise in Transformation

Requires a modern identity & access security perimeter



Engage
your customers



Empower
your employees



Optimize
your operations

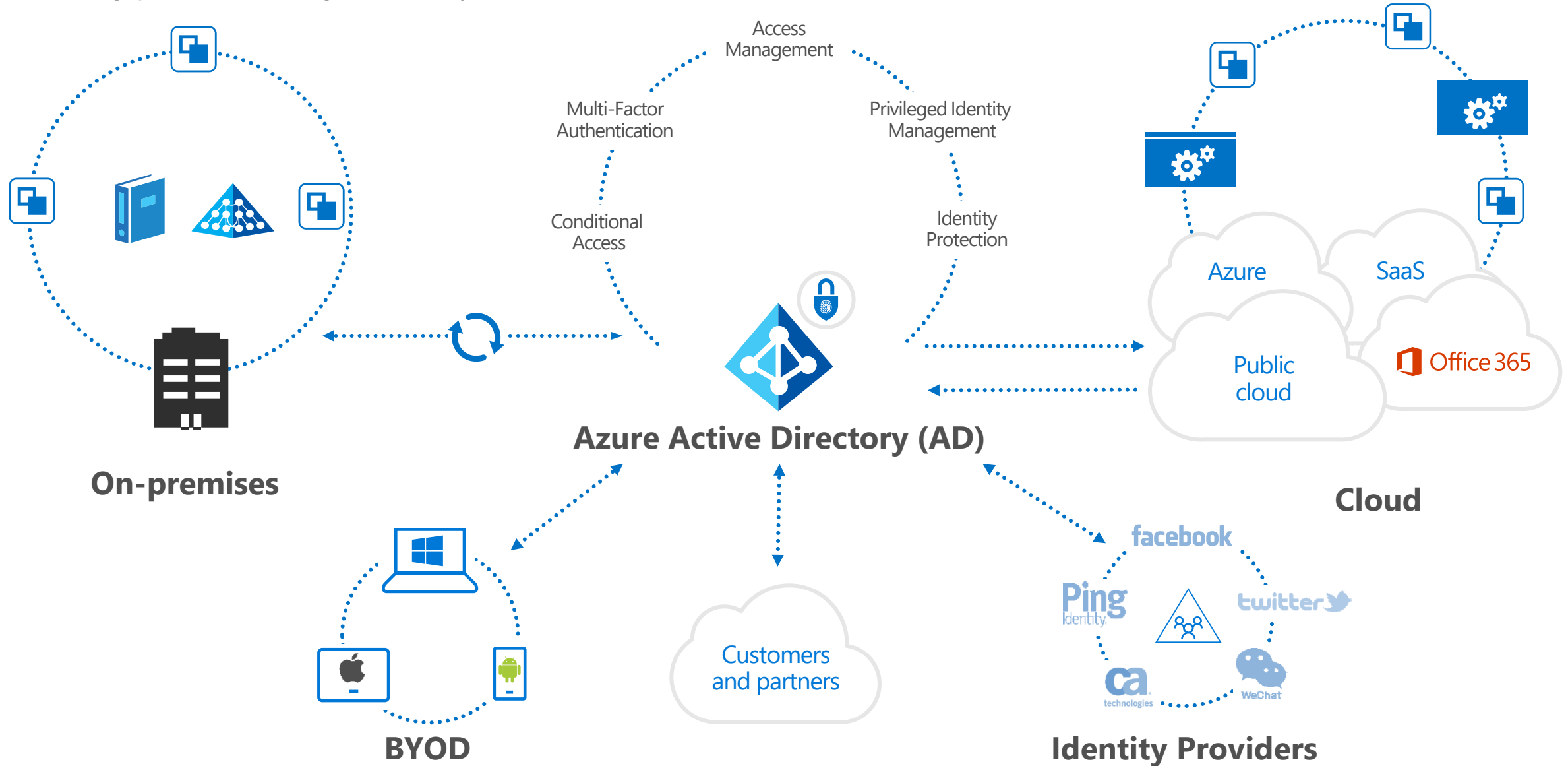


Transform
your products



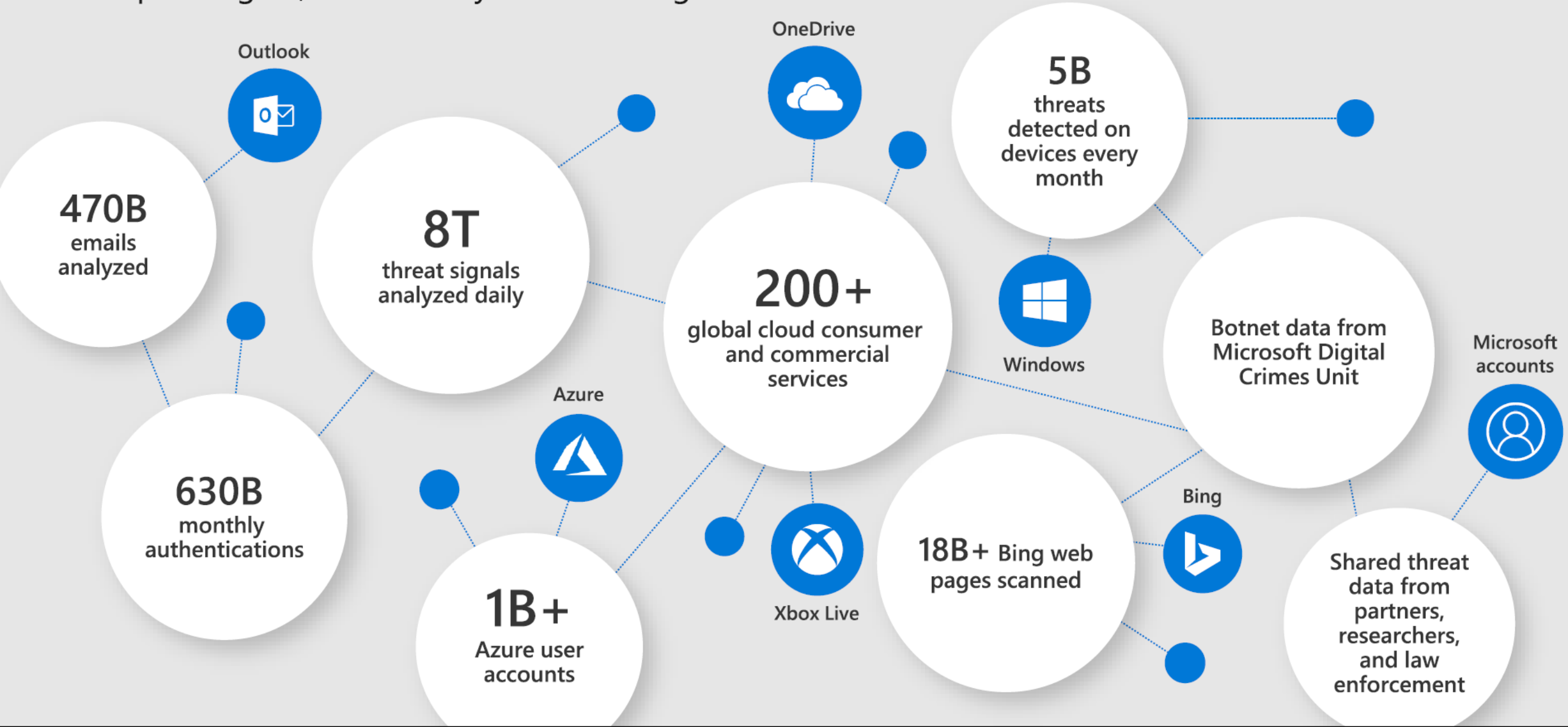
Identity as the Control Plane

A strong protected single identity at the center of the business

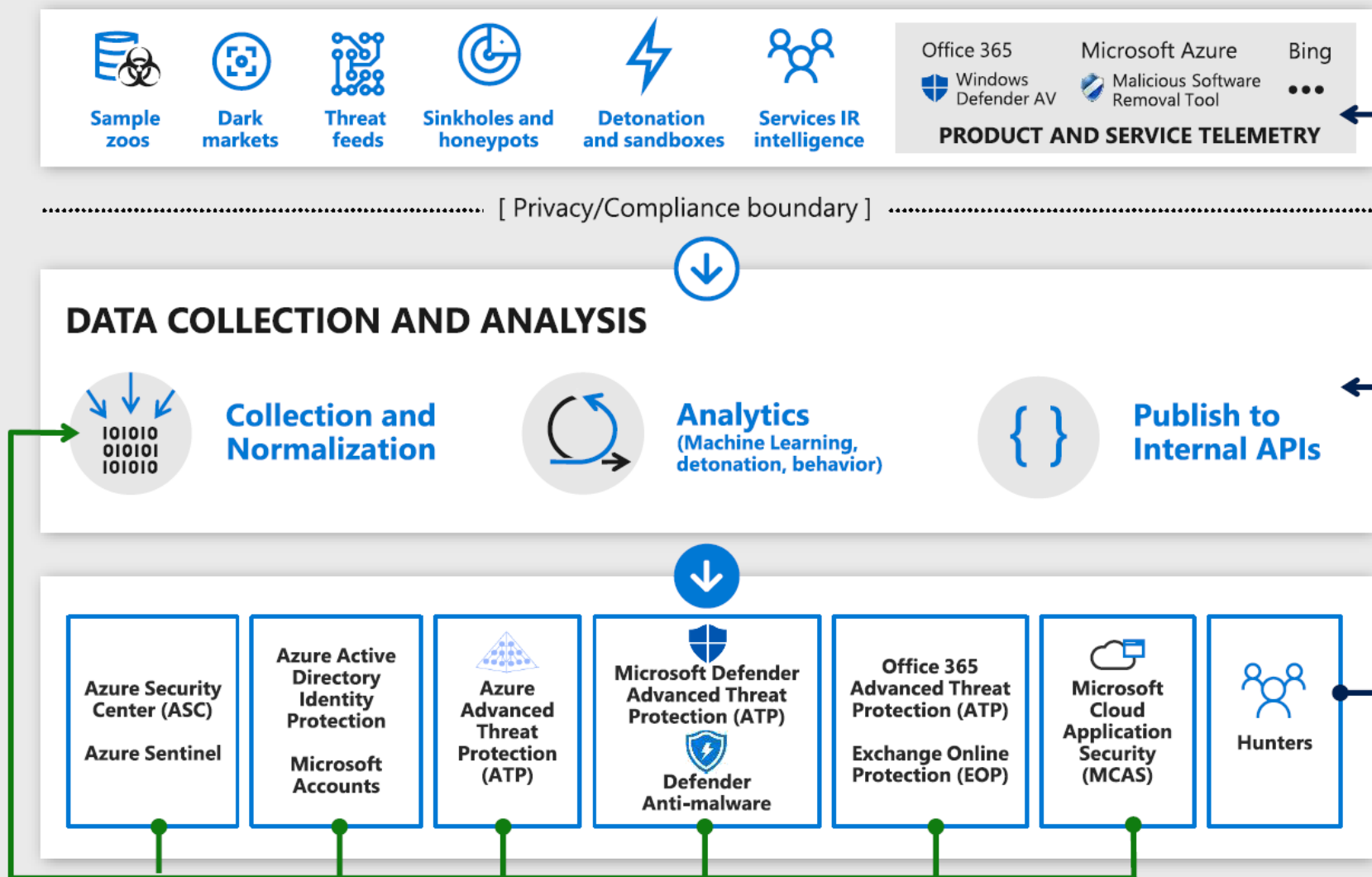


Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Inside The Intelligent Security Graph



➔ Products instrumented to strict privacy/compliance standards
See [Microsoft Trust Center](#)

➔ Analytics help fuel new discoveries

➔ Products send data to graph

➔ Products use Interflow APIs to access results

➔ Products generate data which feeds back into the graph

➔ Hunters identify attacks, improve analytics, feed back into product design



Microsoft Security—a leader in 5 Gartner magic quadrants



Access Management



Cloud Access Security Brokers



Enterprise Information Archiving



Endpoint Protection Platforms



Unified Endpoint Management Tools

*Gartner "Magic Quadrant for Access Management," by Michael Kelley, Abhyuday Data, Henrique, Teixeira, August 2019

*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Steve Riley, Craig Lawson, October 2019

*Gartner "Magic Quadrant for Enterprise Information Archiving," by Julian Tirsu, Michael Hoech, November 2019

*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Peter Firstbrook, Dionisio Zumerle, Prateek Bhajanka, Lawrence Pingree, Paul Webber, August 2019

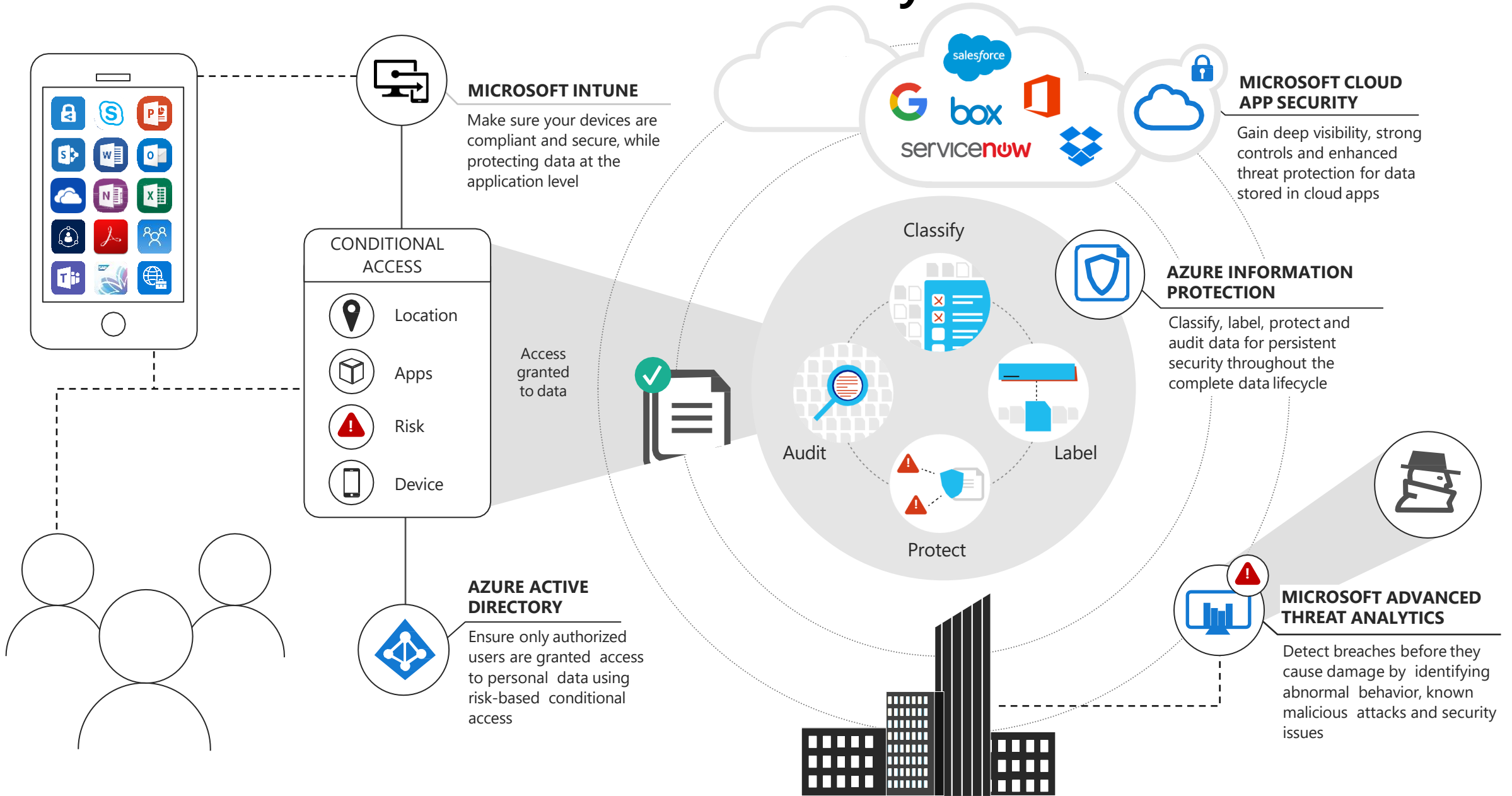
*Gartner "Magic Quadrant for Unified Endpoint Management Tools," by Chris Silva, Manjunath Bhat, Rich Doheny, Rob Smith, August 2019

These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

Microsoft Intelligent Security Association



Microsoft 365 Business Premium Security





Multi-Factor Authentication (MFA) overview



Almost everyone hates passwords

Users



IT Admins



Hackers



Passwords are expensive and insecure

Password reuse
across multiple
accounts

73%
of passwords are
duplicates

Passwords are
the weak link

81%
of breaches
leveraged
passwords

Data breaches
are expensive

\$3.86
million, the
average total
cost of a data
breach

Passwords
generate tons
of support calls

20%
of help desk calls
are related to
password resets

Your password doesn't matter, but MFA does

81%

of breaches leverage stolen or weak passwords



MFA Credentials



Windows Hello



FIDO2 Security key



Microsoft Authenticator



OATH Hard Tokens



SMS, Voice

Multi-factor authentication prevents 99.9% of identity attacks

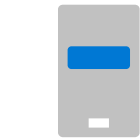
Free MFA options in all Azure AD subscriptions

Multi-Factor Authentication

Verify user identities with strong authentication to establish trust



We support a broad range of multi-factor authentication options



Push Notification



SMS, Voice



Soft Tokens OTP



Hard Tokens OTP

Including passwordless technology



Microsoft Authenticator



Windows Hello



FIDO2 Security key



Biometrics



Multi-factor authentication prevents 99.9% of identity attacks

1

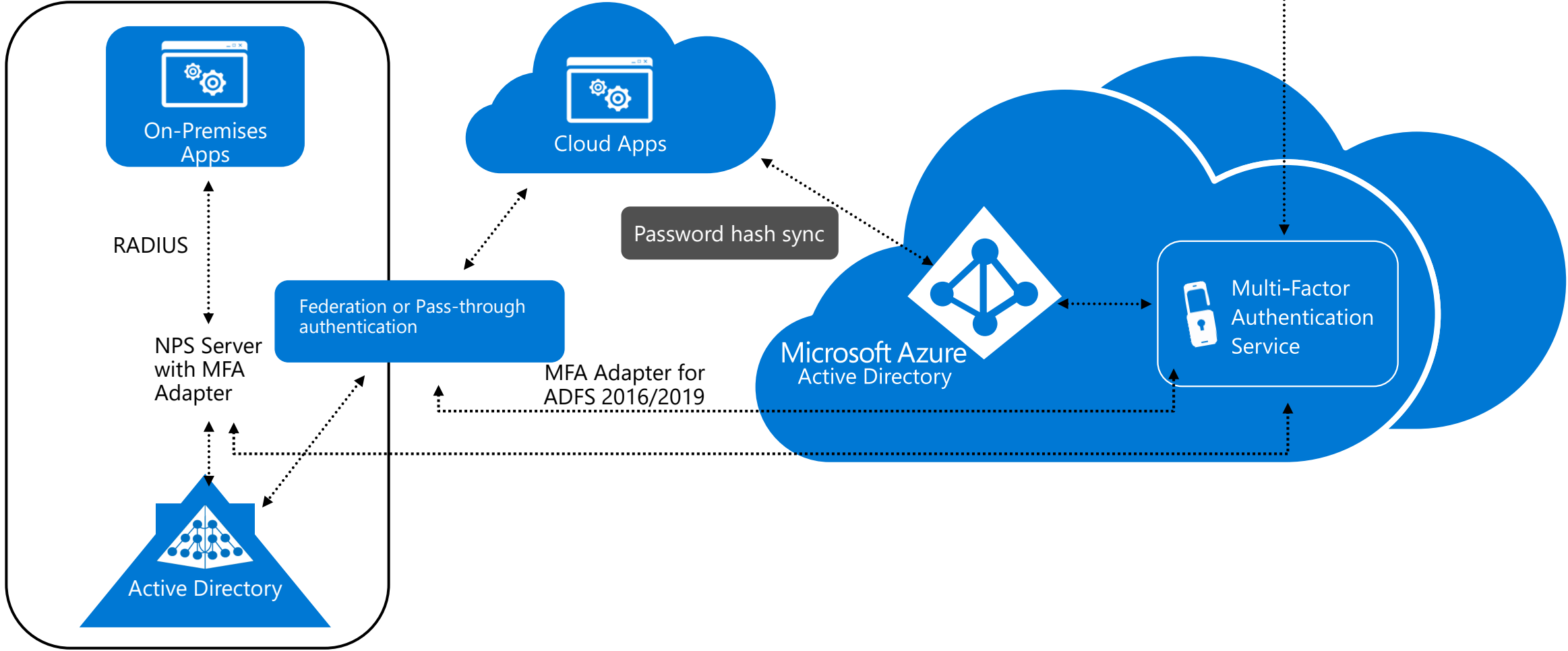
Users sign in from any device using their existing username/password

2

Users must also authenticate using their phone or mobile device before access is granted



On-Premises



Azure MFA – features vs. licensing

Feature	Azure AD Free - Security defaults	Azure AD Free - Azure AD Global Administrators	Office 365 Business Premium, E3, or E5	Azure AD Premium P1 or P2
Protect Azure AD tenant admin accounts with MFA	•	• (Azure AD Global Administrator accounts only)	•	•
Mobile app as a second factor	•	•	•	•
Phone call as a second factor		•	•	•
SMS as a second factor		•	•	•
Admin control over verification methods		•	•	•
Fraud alert				•
MFA Reports				•
Custom greetings for phone calls				•
Custom caller ID for phone calls				•
Trusted IPs				•
Remember MFA for trusted devices		•	•	•
MFA for on-premises applications				•

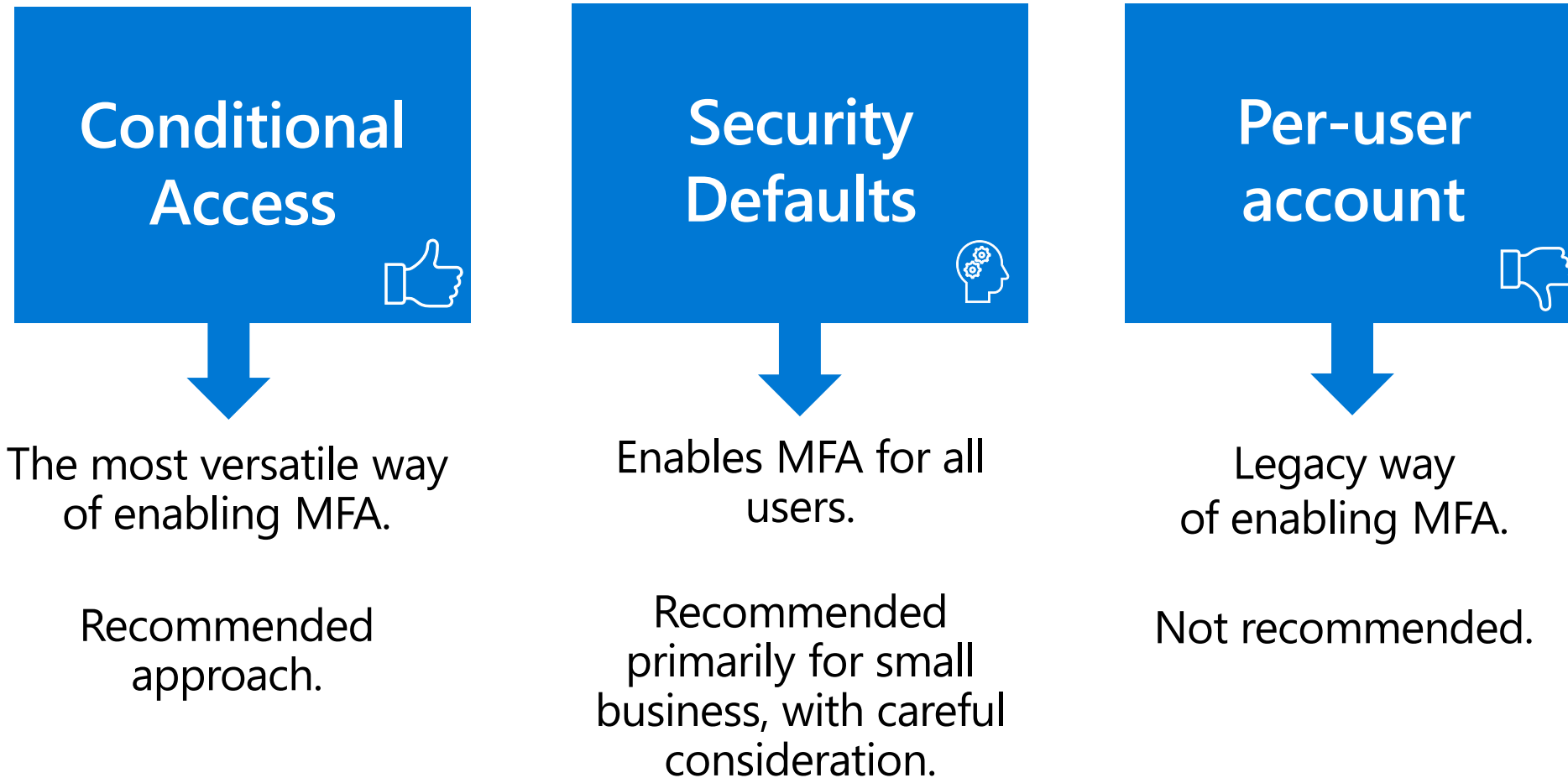


Ways to enable MFA



Ways to enable MFA

Multi-factor authentication can be enabled in these three ways:





Azure AD Security defaults (Enabling MFA for all users)



What are Security defaults?

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'Contoso - Properties' page for an Azure Active Directory instance. The 'Directory properties' section is visible, showing fields for Name (Contoso), Country or region (United States), Location (United States datacenters), Notification language (English), and Directory ID (69997834-fa40-45da-bad8-382c3bdc66c3). A dialog box titled 'Enable Security defaults' is overlaid on the right side of the screen. The dialog box contains the following text: 'Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks. [Learn more](#)'. Below the text, there is a toggle switch labeled 'Enable Security defaults' with 'Yes' selected and 'No' unselected. The 'Yes' button is circled in red.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Contoso - Properties

Contoso - Properties
Azure Active Directory

Search (Ctrl+)

Save Discard

Directory properties

Name *
Contoso

Country or region
United States

Location
United States datacenters

Notification language
English

Directory ID
69997834-fa40-45da-bad8-382c3bdc66c3

Enable Security defaults

Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks. [Learn more](#)

Enable Security defaults

Yes No

Azure AD Security Defaults

What does that button do?

- **Unified Multi-factor registration**
 - Users have 14 days to register
- **Multi-factor enforcement**
 - Users with privileged accounts will be required to perform MFA
 - Protect privileged Actions (Azure portal, Azure PowerShell, Azure CLI)
 - Protect All users – MFA challenge when needed
- **Block Legacy Authentication**
 - Clients that don't use modern authentication(e.g Office 2010 client)
 - Any client that users older mail protocols such as IMAP, SMTP or POP3

Azure AD Security Defaults

Things to consider!

- **Authentication methods**
 - MFA only available using the authenticator app
- **Break-glass Accounts**
 - Security defaults apply to all accounts. You won't be able to deploy break glass accounts that won't be expected to perform MFA
- **Conditional Access**
 - Can't be combined with Security Defaults
 - Enabling Conditional Access policies prevents you from enabling Security Defaults
 - All these defaults can be achieved using Conditional Access
- **Blocking Legacy Authentication**
 - First need to understand if there are users that have apps using legacy auth
 - Need to make sure you are using at least Office 2013 (with registry change*) and above
 - Modern authentication needs to be enabled in the Office 365 tenant and Skype for Business Online (tenants created before August 2017 only)
 - Exchange Hybrid configurations may need to be updated to support Modern Auth



Conditional Access overview



What is Azure AD Conditional Access?

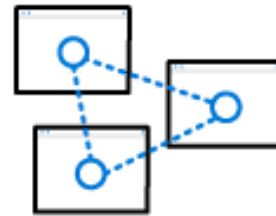
Conditional access is a capability of Azure Active Directory that enables you to enforce controls on the access to applications in your environment based on specific conditions from a central location.



**Location and
User-based
conditional
access**



**Device-based
conditional
access**



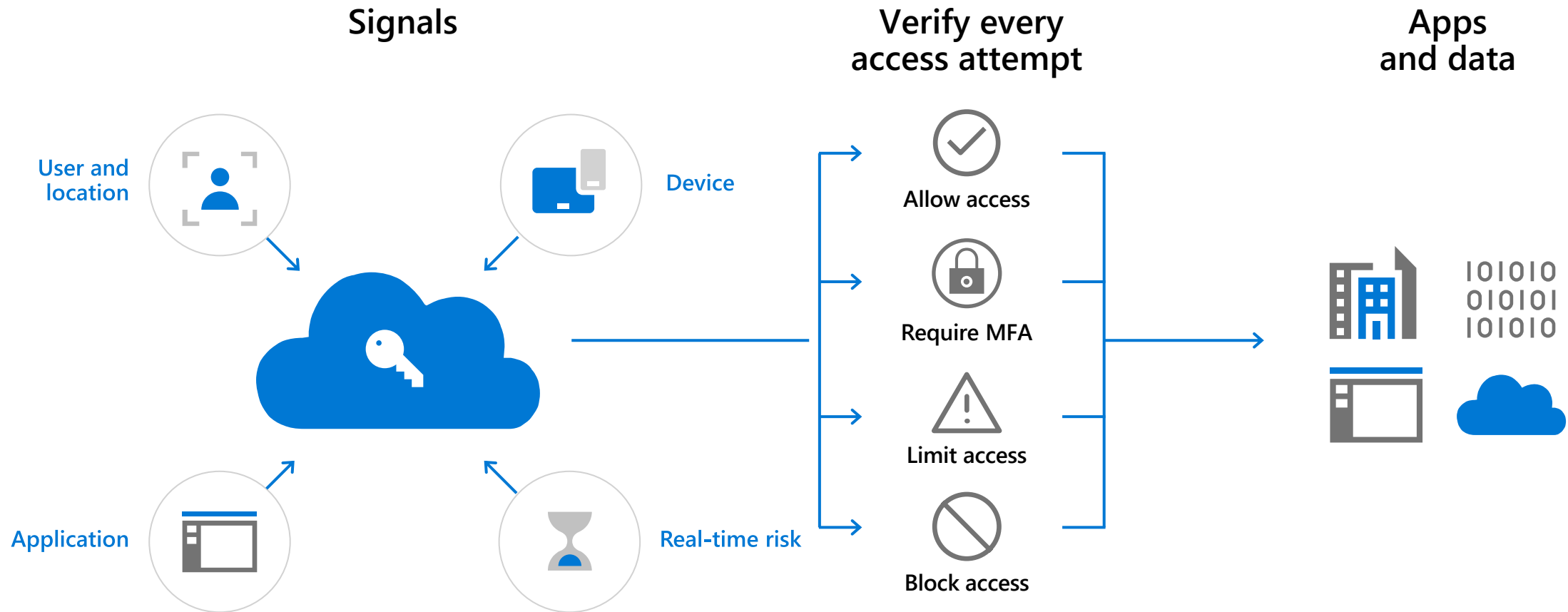
**Application-
based
conditional
access**



**Risk-based
conditional
access**

Conditional Access – general overview

Enforce strong protection policies and risk assessment to grant access to employees and partners



Conditional Access Policy

Assignments



Policy Application

Conditions



Policy Evaluation

Controls



Apply Restrictions

Conditional Access Policy Lifecycle

- Report-only mode
- Conditional Access Insights
- Enhanced troubleshooting

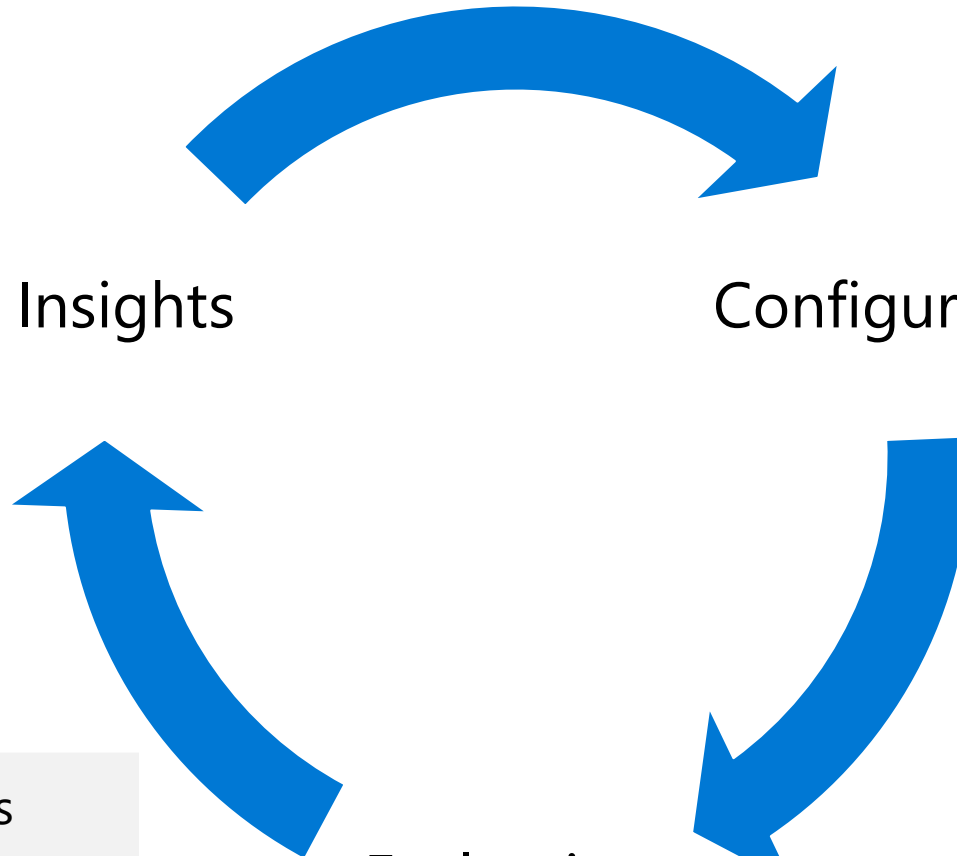
Insights

Configuration

- Templates
- Summary view
- Conditional Access API

- Targeting device groups
- Target actions
- Integrations with MCAS

Evaluation



Conditional Access Policy Prerequisites

- Azure AD Tenant
- Global Admin Credentials
- AAD P1 / EMS E3 or higher licenses
- Recommended:
 - Good: Enable modern authentication for apps/services including Office 365
 - Better: Upgrade to clients / mobile devices that support modern authentication
 - Best: Block the use of legacy authentication protocols in your tenant
- Optional: MS Intune/MDM for device management and health attestation



Assignments



Assignments – to which users and groups and which cloud applications does the policy apply?

Users and groups

Include or exclude specific users and/or groups or directory roles.

Cloud Applications

Include or exclude specific AAD apps or apply to all cloud apps.

How to use

These filters support both including and excluding. This allows a policy to focus on a group or on apps, or it allows other apps or users to be exempted from this policy.

The screenshot displays the 'New' policy configuration interface in Microsoft Entra ID. The main panel on the left is titled 'New' and contains the following sections:

- Info:** Name field with the example 'Device compliance app policy'.
- Assignments:** Three expandable sections: 'Users and groups' (0 users and groups selected), 'Cloud apps' (0 cloud apps selected), and 'Conditions' (0 conditions selected).
- Access controls:** Two expandable sections: 'Grant' (0 controls selected) and 'Session' (0 controls selected).
- Enable policy:** A toggle switch currently set to 'Off'.

Two secondary windows are open to the right, both in 'PREVIEW' mode:

- Users and groups:** Features 'Include' and 'Exclude' buttons (highlighted with red boxes), radio buttons for 'None', 'All users', and 'Select users and groups' (selected), and a 'Select' button. A search bar is present with the text 'Search by name or email address'. Below the search bar, two user entries are visible: 'AADSS_9b80b041e375' and 'AADSyncSched_33d13'.
- Cloud apps:** Features 'Include' and 'Exclude' buttons, radio buttons for 'None', 'All cloud apps', and 'Select apps' (selected), and a 'Select None' button. A search bar is present with the text 'Search Applications...'. Below the search bar, three application entries are visible: 'APIExplorerBeta', 'Graph Explorer 2 PPE', and 'GraphExplorer'.

Red arrows point from the 'Users and groups' and 'Cloud apps' sections of the main 'New' panel to their respective preview windows.

How Are Conditional Access Policies Applied?



All policies are evaluated* for application and their respective conditions are AND'ed



If policy applies, controls are enforced (controls within each policy may be AND'ed or OR'ed)



Block always wins and cannot be "unblocked"



To "unblock" a user, exclude them from the blocking policy



This will likely require the creation of an "exception" policy for to cover the new scenario

*Conditional access policies are assessed for all sign-in and authorization requests, not for each application request



Conditions



Conditions

Conditional Access policies triggers based on Conditions.
Conditions are logically 'ANDed'.

"When this happens" is called **conditions**.

Conditions available:

- Device platforms
- Device state
- Locations
- Client apps
- Sign-in risk

The image displays a series of screenshots from the Microsoft Conditional Access configuration interface. On the left is the main 'New' policy configuration page. A red arrow points from the 'Conditions' section to a 'Device platforms' configuration dialog. Below that is a 'Device state (preview)' dialog. To the right are 'Locations' and 'Client apps (preview)' configuration dialogs, and finally a 'Sign-in risk' configuration dialog.

Device platforms configuration:

- Configure: Yes
- Include/Exclude buttons
- Radio buttons: All platforms (including unsupported), Select device platforms
- Checkboxes: Android, iOS, Windows Phone, Windows, macOS

Device state (preview) configuration:

- Configure: Yes
- Include/Exclude buttons
- Text: Select the device state condition used to exclude devices from policy.
- Checkboxes: Device Hybrid Azure AD joined, Device marked as compliant

Locations configuration:

- Configure: Yes
- Include/Exclude buttons
- Radio buttons: Any location, All trusted locations, Selected locations
- Select: None

Client apps (preview) configuration:

- Configure: Yes
- Text: Select the client apps this policy will apply to
- Checkboxes: Browser, Mobile apps and desktop clients, Modern authentication clients, Exchange ActiveSync clients, Apply policy only to supported platforms, Other clients
- Warning: Exchange ActiveSync currently does not support all other conditions

Sign-in risk configuration:

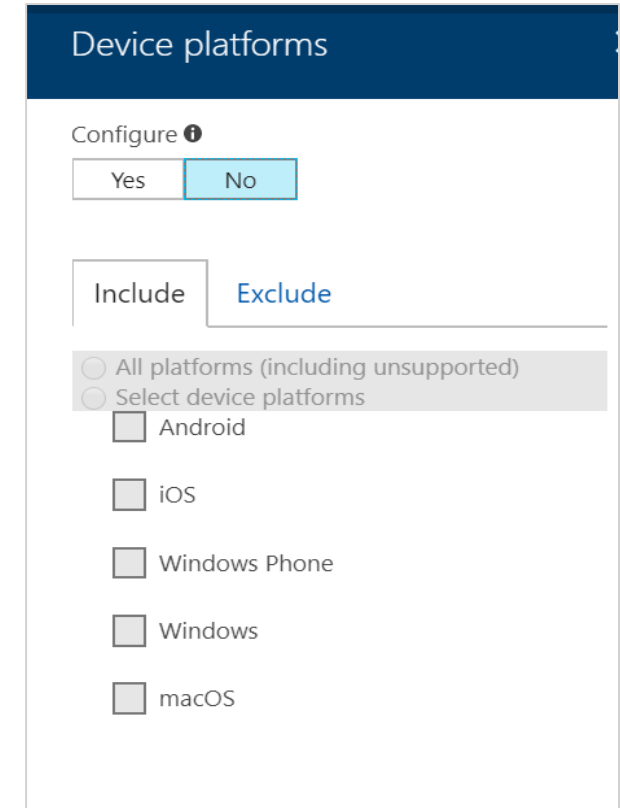
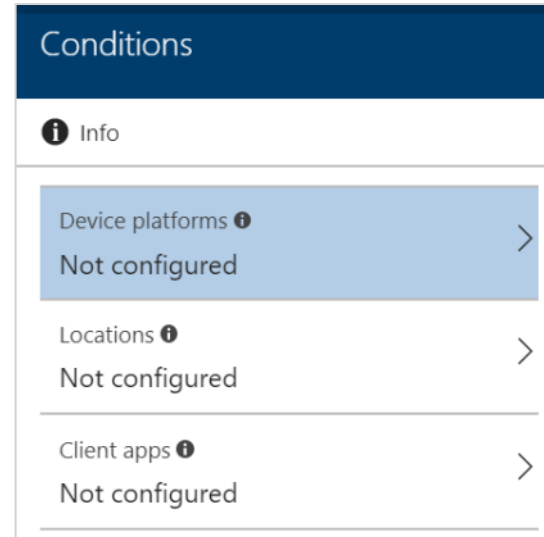
- Configure: Yes
- Text: Select the sign-in risk level this policy will apply to
- Radio buttons: High, Medium, Low, No risk

Conditions: Device platforms

Device platforms

- All platforms (including unsupported)
- Android
- iOS
- Windows Phone
- Windows Desktop
- macOS

If you choose **All platforms**, you can exclude specific platforms on the Exclude tab



Conditions: Locations

Locations

- Typically, trusted locations are network areas that your IT department controls.
- Trusted named locations are also used by Azure Identity Protection and Azure AD security reports to reduce false positives.

Country / Region

- Using this option you can select one or more country or region to define a named location. Consider defining countries into **Doing Business In** vs **Not Doing Business In** for defining policies.

Include unknown areas

- Some IP addresses are not mapped to a specific country. This option allows you to choose if these IP addresses should be included in the named location. They could be checked when the named location policy applies to unknown locations.

Locations

Control user access based on their physical location. [Learn more](#)

Configure ⓘ

Yes No

Include Exclude

Any location
 All trusted locations
 Selected locations

Select None >

New

* Name
Countries we do business with ✓

Define the location using:

IP ranges
 Countries/Regions

New Zealand ▾

Include unknown areas ⓘ

Conditions: Device state

Conditional Access can check if a device used for authentication are under some sort of organizational control. We call these "Managed Devices"

To become a managed device, a registered device must be either a Hybrid Azure AD joined device or a device that has been marked as compliant.

Policies can be created to exclude managed devices from certain policies like that may be only required to apply for *unmanaged* devices that will be more likely personal devices.

The screenshot shows two side-by-side windows from the Azure AD Conditional Access console. The left window, titled 'Conditions', lists several configuration options, all currently set to 'Not configured'. The 'Device state (preview)' option is highlighted in light blue. The right window, titled 'Device state (preview)', shows the configuration for this condition. It includes an 'Info' icon, a 'Configure' section with 'Yes' and 'No' radio buttons (where 'Yes' is selected), and 'Include' and 'Exclude' radio buttons (where 'Include' is selected). Below this, there is a text prompt: 'Select the device state condition used to exclude devices from policy.' followed by two unchecked checkboxes: 'Device Hybrid Azure AD joined' and 'Device marked as compliant'.

Conditions	Device state (preview)
Info	Info
Sign-in risk i Not configured >	Configure i <input checked="" type="radio"/> Yes <input type="radio"/> No
Device platforms i Not configured >	<input checked="" type="radio"/> Include <input type="radio"/> Exclude
Locations i Not configured >	Select the device state condition used to exclude devices from policy.
Client apps (preview) i Not configured >	<input type="checkbox"/> Device Hybrid Azure AD joined i
Device state (preview) i Not configured >	<input type="checkbox"/> Device marked as compliant i

Conditions: Client apps

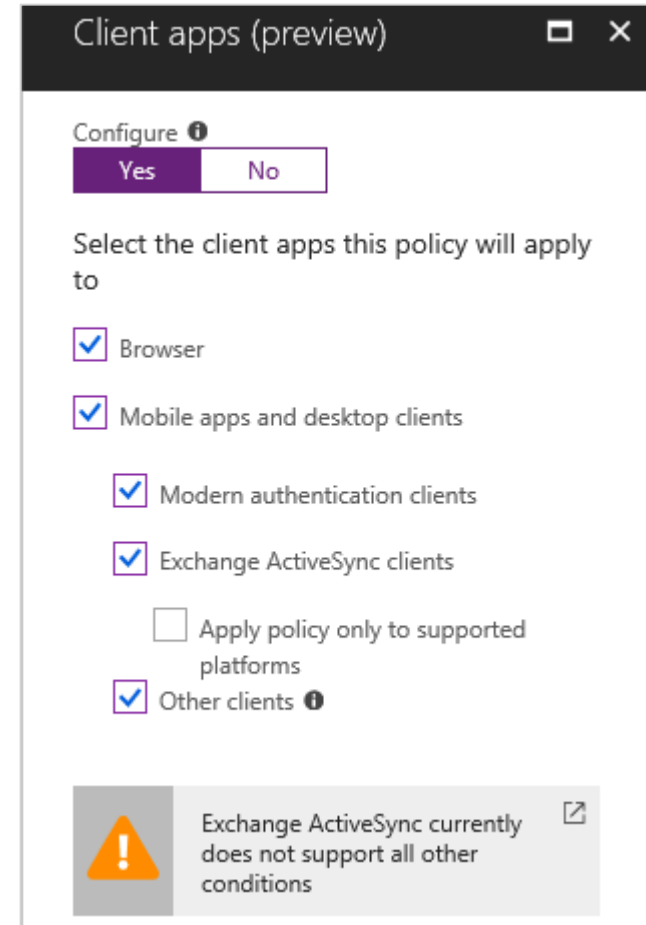
Client apps use different protocols:

- Browser: passive federation clients using a web browser user agent string
- Mobile apps and desktop clients:
 - Modern authentication: uses passive federation, but with a different User Agent String
 - Exchange ActiveSync: EAS
 - Other clients: Legacy Authentication (Basic, WS-Trust, POP/IMAP)

Note: Using Browser condition with device controls requires specific versions of IE, Chrome, Edge and Safari (on Mac/iOS). Chrome requires an extension on Win 10 and registry edits on Win 7/8.1.

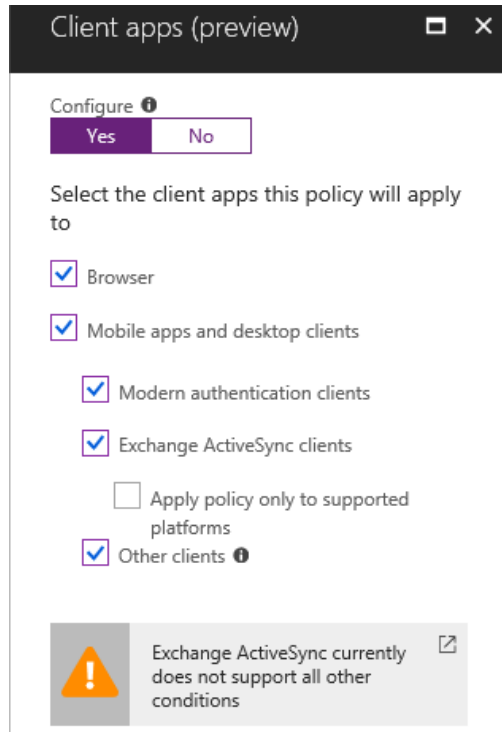
Some typical use cases for this control:

- Enforce device controls on machines using apps that can download offline data
- Force unmanaged devices to use only the browser for access
- Block web access but allow mobile app access.
- **Block legacy protocols**



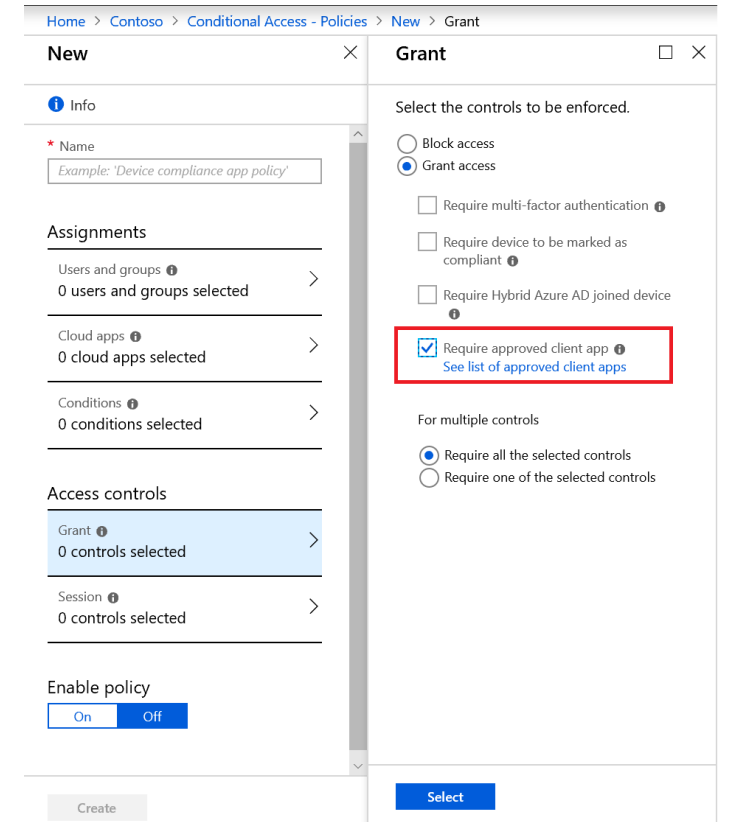
Client Apps – Both a Condition and a Control

Condition



OR

Control (Approved Client Apps)



- For applying different policies to browser or app use.

This control is used to enforce MAM policies.

Conditions: Sign in risk

Azure Active Directory Identity Protection analyzes each sign-in and calculates the likelihood that a sign-in attempt was not performed by the legitimate owner of a user account.

The likelihood (low, medium, high) is indicated in form of a calculated value called sign-in risk levels.

This requires **Azure AD Premium P2 or EMS E5 or M365 E5**

The screenshot shows two side-by-side configuration windows. The left window, titled 'Conditions', lists several criteria that are currently 'Not configured': Sign-in risk, Device platforms, Locations, Client apps (preview), and Device state (preview). The right window, titled 'Sign-in risk', shows a 'Configure' section with 'Yes' selected. Below this, it asks to 'Select the sign-in risk level this policy will apply to' and provides four radio button options: High, Medium, Low, and No risk.

Conditions	Sign-in risk
i Info	i Info
Sign-in risk i Not configured >	Configure i Yes No
Device platforms i Not configured >	Select the sign-in risk level this policy will apply to
Locations i Not configured >	<input type="checkbox"/> High
Client apps (preview) i Not configured >	<input type="checkbox"/> Medium
Device state (preview) i Not configured >	<input type="checkbox"/> Low
	<input type="checkbox"/> No risk

⚙️ Controls



Control types: Grant or Session

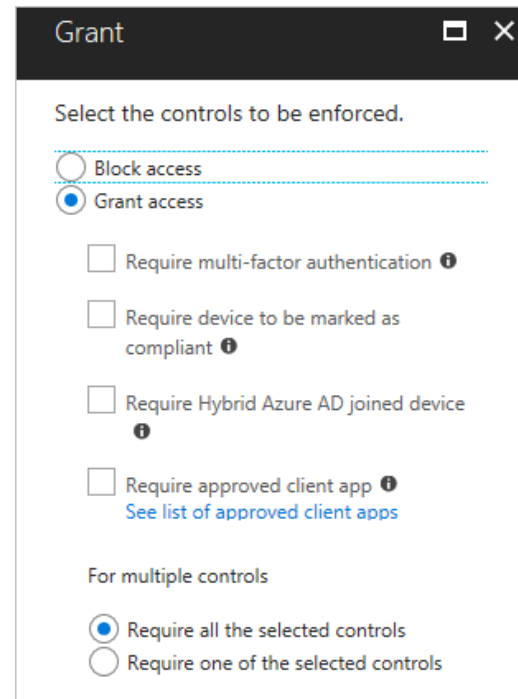
Each control is either a requirement that must be fulfilled by the person or system signing in, or a restriction on what the user can do after signing in.

There are two types of controls:

- **Grant controls** - To gate access or require additional factors of auth
- **Session controls** - To restrict access within a session

Grant controls:

With grant controls, you can either block access altogether or allow access with additional requirements by selecting the desired controls.

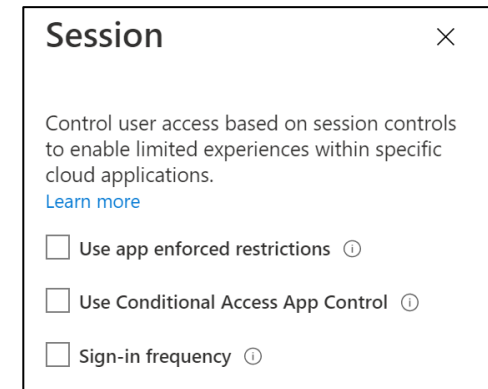


The screenshot shows a dialog box titled "Grant" with a close button. It contains the following elements:

- Header: "Grant" with a close button.
- Instruction: "Select the controls to be enforced."
- Radio buttons for "Block access" (unselected) and "Grant access" (selected).
- Four checkboxes for additional controls, all unselected:
 - Require multi-factor authentication ⓘ
 - Require device to be marked as compliant ⓘ
 - Require Hybrid Azure AD joined device ⓘ
 - Require approved client app ⓘ [See list of approved client apps](#)
- Section: "For multiple controls"
- Radio buttons for "Require all the selected controls" (selected) and "Require one of the selected controls" (unselected).

Session controls:

The session controls are enforced by cloud apps and rely on additional information provided by Azure AD to the app about the session.



The screenshot shows a dialog box titled "Session" with a close button. It contains the following elements:

- Header: "Session" with a close button.
- Text: "Control user access based on session controls to enable limited experiences within specific cloud applications." followed by a [Learn more](#) link.
- Three checkboxes for session controls, all unselected:
 - Use app enforced restrictions ⓘ
 - Use Conditional Access App Control ⓘ
 - Sign-in frequency ⓘ

Identity Demo



Microsoft Security



Identity and access management

Your universal platform to manage and secure identities.



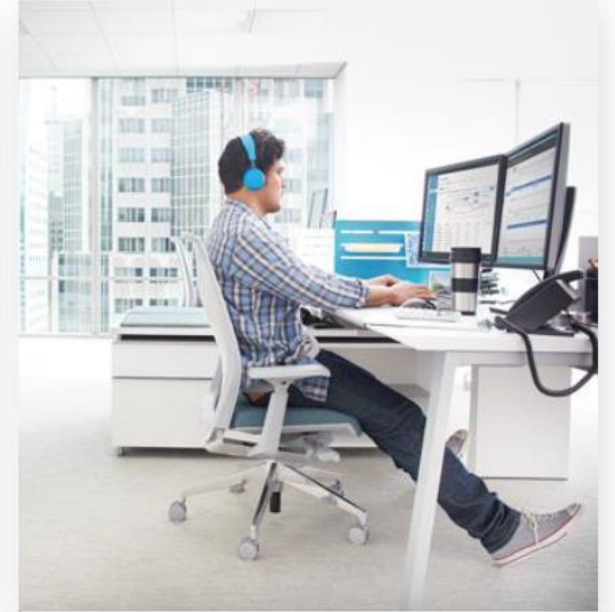
Threat protection

Stop attacks with integrated and automated security.



Information protection

Protect your sensitive data—wherever it lives or travels.



Cloud security

Safeguard your cross-cloud resources.

Stories about phishing and ransomware

“Thankfully, it...didn't jump through the network. We **were able to lock it down quickly** and limit exposure.”

— Barry L, architecture firm, 125 employees

“£4,000 was paid to the wrong account, which we were **very lucky to get back**”

— David L, import/export company, 10 employees

“My sister in law owns a company. They just got hit with one of these cyber terrorist things and **had to shell out like \$40,000 dollars** to get their data back”

— Diane B, meal assembly kitchen, 10 employees

“They **got the CFO to wire \$1.9M** to a bank in southern Idaho, where someone had arranged...to transfer the money from there to Vietnam.”

—Dave C. IT Partner for manufacturing company, 150 employee

Cyberattacks are becoming more sophisticated

"We're getting blasted. Wire transfers. Direct deposit requests. Gift cards."

- Jeff, distribution company, 125 employees

Phishing emails have less grammar errors, formatting problems, and other signs that used to make them easy to recognize

Ransomware has become "easy money" for cybercriminals; successful attacks are becoming more frequent

Zero-day attacks that traditional attachment scanning can't catch are increasing in number and sophistication

Enhanced **spoofing techniques** lead to personalized emails from colleagues that are difficult to spot

Use of **social engineering** techniques are very effective, especially when a password is compromised



Protection against cyber threats in Microsoft 365 Business



Safe
Links



Safe
Attachments



Spoof
Intelligence



Microsoft Defender
Exploit Guard

Office 365 Advanced Threat Protection

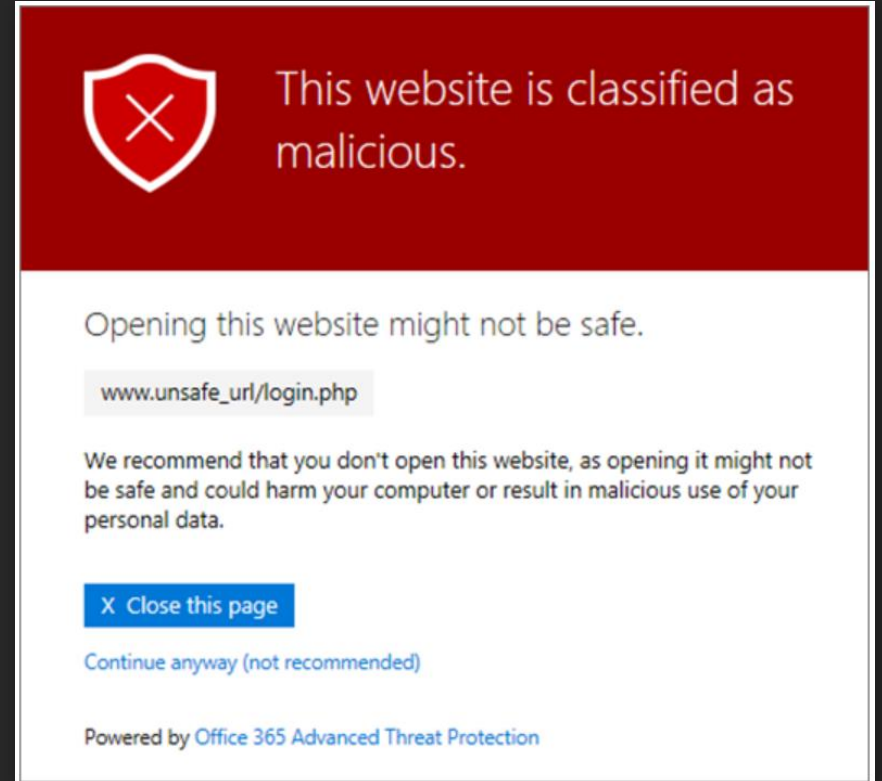
Office 365 ATP Safe Links

What it is


Office 365 ATP Safe Links can help protect your organization by providing time-of-click verification of web addresses (URLs) in **email messages** and **Office documents**.

How it works

When a user clicks on a URL in an email message or in an Office file, the link is checked by ATP Safe Links and is identified as blocked, malicious, or safe before opening the website.



The image shows a warning banner from Office 365 ATP. The top part is a red bar with a white shield icon containing a red 'X'. To the right of the icon, the text reads "This website is classified as malicious." Below the red bar, the text says "Opening this website might not be safe." followed by the URL "www.unsafe_url/login.php" in a grey box. Below the URL, it says "We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data." There are two buttons: a blue "X Close this page" button and a grey "Continue anyway (not recommended)" button. At the bottom, it says "Powered by Office 365 Advanced Threat Protection".

 This website is classified as malicious.

Opening this website might not be safe.

`www.unsafe_url/login.php`

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

[X Close this page](#)

[Continue anyway \(not recommended\)](#)

Powered by [Office 365 Advanced Threat Protection](#)

Enable ATP Safe Links

To enable ATP Safe Links

1. In the [Security & Compliance Center](#), choose **Threat management > Policy > ATP Safe Links**
2. Double-click the **Default** policy
3. In the **Use safe links in** section, select the option **Office 365 ProPlus, Office for iOS and Android**, and then click **Save**
4. In the **Policies that apply to specific recipients** section, click the plus sign (+)
5. Specify the following settings:
 - In the **Name** box, type a name, such as **Safe Links**
 - In the **Select the action** section, choose **On**
 - Select these options:
 - **Use safe attachments to scan downloadable content**
 - **Apply safe links to email messages sent within the organization**
 - **Do not let users click through safe links to original URL**
 - In the **Applied to** section, choose **The recipient domain is**. Then, select your domain, choose **Add**, and then click **OK**
6. Click **Save**

To learn more, see [Set up Office 365 ATP Safe Links policies](#).

The screenshot displays the Office 365 Security & Compliance Center interface. The left-hand navigation pane shows the 'Threat management' section expanded, with 'Policy' selected. The main content area shows a grid of policy tiles. The 'ATP Safe Links' tile is highlighted with a red border. Below this, a 'new safe links policy' dialog box is open, showing the following configuration:

- Name:** Safe Links
- Description:** (empty field)
- Select the action for unknown potentially malicious URLs in messages:**
 - OFF
 - On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.
- Use safe attachments to scan downloadable content.
- Apply safe links to email messages sent within the organization.
- Do not track when users click safe links.
- Do not let users click through safe links to original URL.

Buttons for 'Save' and 'Cancel' are visible at the bottom right of the dialog box.

Office 365 ATP Safe Attachments

What it is:

Office 365 ATP Safe Attachments can help protect your company by checking to see if email attachments are malicious.

How it works:

When an ATP Safe Attachments policy is in place, email attachments are opened and tested in a virtual environment. If determined to be malicious, the attachment will not open.

This protection also applies to attachments shared via SharePoint Online, OneDrive or Teams.

Enable ATP Safe Attachments

To enable ATP Safe Attachments

1. In the [Security & Compliance Center](#), choose **Threat management > Policy > ATP safe attachments**
2. Select the option **Turn on ATP for SharePoint, OneDrive, and Microsoft Teams**
3. In the **Protect email attachments** section, click the plus sign (+)
4. Specify the following settings:
 - In the **Name** box, type **Block malware**
 - In the response section, choose **Block**
 - In the **Redirect attachment** section, select the option **Enable redirect**, and then specify the email address for your organization's security administrator or operator who will review detected files
 - In the **Applied to** section, choose **The recipient domain is**. Then, select your domain, choose **Add**, and then click **OK**
5. Click **Save**
6. (Recommended additional step) As a global administrator or a SharePoint Online administrator run the [Set-SPOTenant](#) cmdlet with the **DisallowInfectedFileDownload** parameter set to true for your Office 365 environment. (This prevents people from opening, moving, copying, or sharing files that are detected as malicious)

The screenshot displays the Office 365 Security & Compliance Center interface. The left-hand navigation pane shows the 'Policy' section under 'Threat management'. The main content area shows several policy tiles: 'ATP anti-phishing', 'ATP safe attachments' (highlighted with a red box), 'ATP Safe Links', 'Anti-spam', 'DKIM', and 'Anti-malware'. The 'ATP safe attachments' tile is selected, and a modal dialog titled 'new safe attachments policy' is open. The dialog shows the following configuration:

- Select the action for unknown malware in attachments:** Block - Block the current and future emails and attachments with detected malware.
- Warning:** Monitor, Replace and Block actions may cause significant delay to email delivery. Dynamic Delivery is only available for recipients with hosted mailboxes.
- Redirect attachment on detection:** Enable redirect. Send the attachment to the following email address:
- Applied To:** Apply the above selection if malware scanning for attachments times out or error occurs.
- Applied To:** Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:
 - *If... The recipient domain is

Buttons for 'Save' and 'Cancel' are visible at the bottom of the dialog.

To learn more, see [Set up Office 365 ATP Safe Attachments policies](#) and [Turn on Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams](#).

Office 365 ATP anti-spoofing

What it is:

Office 365 mitigates against spoofing attacks (emails that use forged sender domains).

Examples:

Ćontoso.com instead of Contoso.com

debbrajghosh@conotos.com instead of debrajghosh@contoso.com)

How it works:

An array of techniques, updated as threats evolve, help block sophisticated impersonation attempts.

- Detection of forgery of the 'From: header'
- Understanding the history of the source's email infrastructure
- Machine learning algorithms that understand a user's normal patterns of contact with others

Emails may be blocked, sent to junk mail, quarantined, or have a Safety Tips displayed.

 Reply  Reply All  Forward



Mon 4/29/2019 2:18 PM

Satya Nadella <satyan@microsoft.com> (Satya Nadella via ceocomm)

End of fiscal

To David Bjurman-Birr

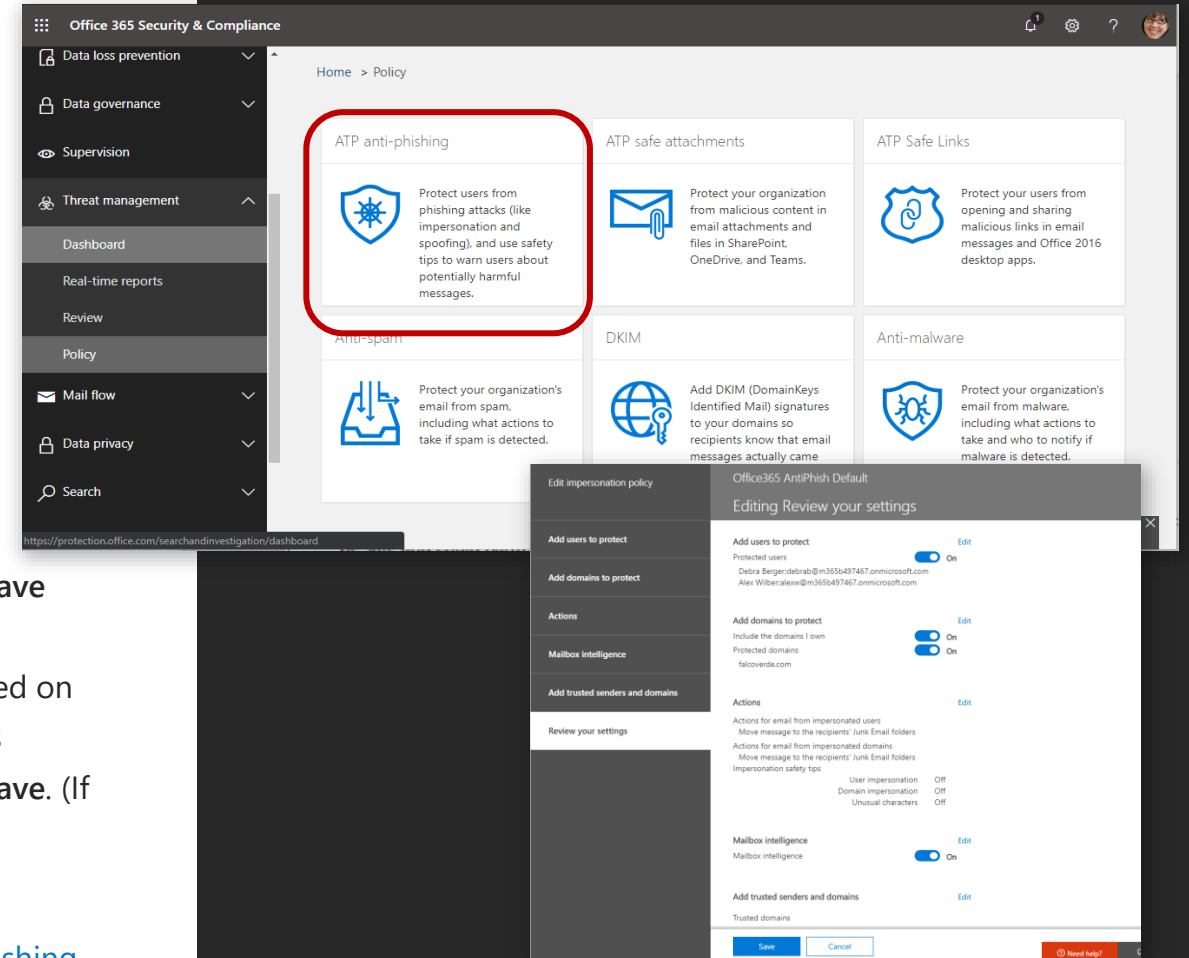
 The actual sender of this message is different than the normal sender. [Click here to learn more.](#)

Enable ATP Anti-phishing

To enable ATP anti-phishing

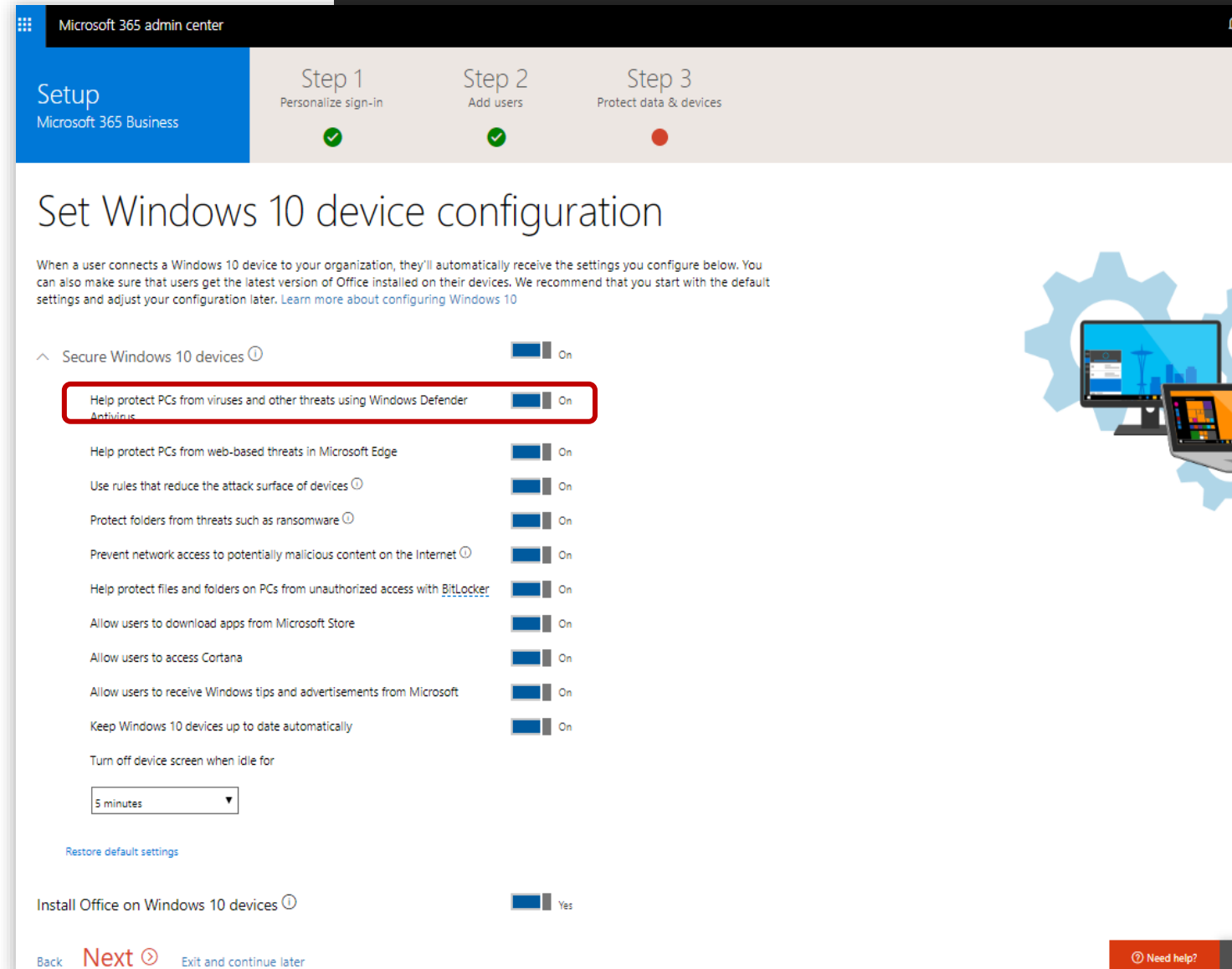
1. In the [Security & Compliance Center](#), choose **Threat management > Policy > ATP anti-phishing**
2. Click **Default policy**
3. In the **Impersonation** section, click **Edit**, and then specify the following settings:
 - a) On the **Add users to protect** tab, turn protection on. Then add users, such as your organization's board members, your CEO, CFO, and other senior leaders. (You can type an individual email address, or click to display a list)
 - b) On the **Add domains to protect** tab, turn on **Automatically include the domains I own**. If you have custom domains, add those as well
 - c) On the **Actions** tab, select **Move message to the recipients' Junk Email folders** for both impersonated user and impersonated domain, and turn on safety tips
 - d) On the **Mailbox intelligence** tab, make sure mailbox intelligence is turned on
 - e) On the **Review your settings** tab, after you have reviewed your settings, click **Save**
4. In the **Spoof** section, click **Edit**, and then specify the following settings:
 - a) On the **Spoofing filter settings** tab, make sure anti-spoofing protection is turned on
 - b) On the **Actions** tab, choose **Move message to the recipients' Junk Email folders**
 - c) On the **Review your settings** tab, after you have reviewed your settings, click **Save**. (If you didn't make any changes, click **Cancel**)
5. Close the default policy settings page

To learn more about your anti-phishing policy options, see [Set up Office 365 ATP anti-phishing and anti-phishing policies](#).



Enforce Microsoft Defender on all your PCs

With Microsoft 365 Business, you can easily enforce the protections of Microsoft Defender on all of your Windows 10 devices, via the Setup Wizard.



The screenshot displays the Microsoft 365 admin center interface during the Setup Wizard. The top navigation bar shows the current step: "Step 3: Protect data & devices", with previous steps "Step 1: Personalize sign-in" and "Step 2: Add users" marked as complete with green checkmarks. The main heading is "Set Windows 10 device configuration". Below this, a descriptive paragraph explains that settings will be applied to Windows 10 devices connected to the organization. The configuration list includes several toggle switches, all of which are currently turned "On". The first option, "Help protect PCs from viruses and other threats using Windows Defender Antivirus", is highlighted with a red rectangular box. Other options include protection for Microsoft Edge, ransomware, network access, BitLocker, Microsoft Store apps, Cortana, Windows tips, and automatic updates. At the bottom, there is a "Turn off device screen when idle for" dropdown menu set to "5 minutes" and a "Restore default settings" link. The footer contains navigation buttons for "Back", "Next", and "Exit and continue later", along with a "Need help?" link.

Microsoft 365 admin center

Setup
Microsoft 365 Business

Step 1
Personalize sign-in

Step 2
Add users

Step 3
Protect data & devices

Set Windows 10 device configuration

When a user connects a Windows 10 device to your organization, they'll automatically receive the settings you configure below. You can also make sure that users get the latest version of Office installed on their devices. We recommend that you start with the default settings and adjust your configuration later. [Learn more about configuring Windows 10](#)

Secure Windows 10 devices [ⓘ] On

- Help protect PCs from viruses and other threats using Windows Defender Antivirus On
- Help protect PCs from web-based threats in Microsoft Edge On
- Use rules that reduce the attack surface of devices [ⓘ] On
- Protect folders from threats such as ransomware [ⓘ] On
- Prevent network access to potentially malicious content on the Internet [ⓘ] On
- Help protect files and folders on PCs from unauthorized access with BitLocker On
- Allow users to download apps from Microsoft Store On
- Allow users to access Cortana On
- Allow users to receive Windows tips and advertisements from Microsoft On
- Keep Windows 10 devices up to date automatically On
- Turn off device screen when idle for
 [ⓘ]

[Restore default settings](#)

Install Office on Windows 10 devices [ⓘ] Yes

[Back](#) [Next](#) [ⓘ] [Exit and continue later](#) [Need help?](#)

Microsoft Security



Identity and access management

Your universal platform to manage and secure identities.



Threat protection

Stop attacks with integrated and automated security.



Information protection

Protect your sensitive data—wherever it lives or travels.



Cloud security

Safeguard your cross-cloud resources.

Protect and control your data and documents



Encrypt
email



Apply restrictions
to email and
documents



Protect against
data leaks



Archive
email data

Examples of sensitive business data

"Prices we pay for products"	"Sales forecasts"	"Protected health information"	"Compensation information"	"Product formulations"	"Phone numbers"
"Credit card and drivers license info sent to us by customers"	"Ingredients that go into our hair care products"	"Bank account and ABA numbers"	"Passport info we collect from our international 1099 contractors"	"Credit applications that people send us"	
"Customer SSN and taxpayer IDs"	"Employee files that HR keeps"	"Company financials"	"Customer lists"	"Home addresses"	"Rates we charge"

Protect and control your data and documents



Encrypt
email



Apply restrictions
to email and
documents



Protect against
data leaks



Archive
email data

Encrypt emails

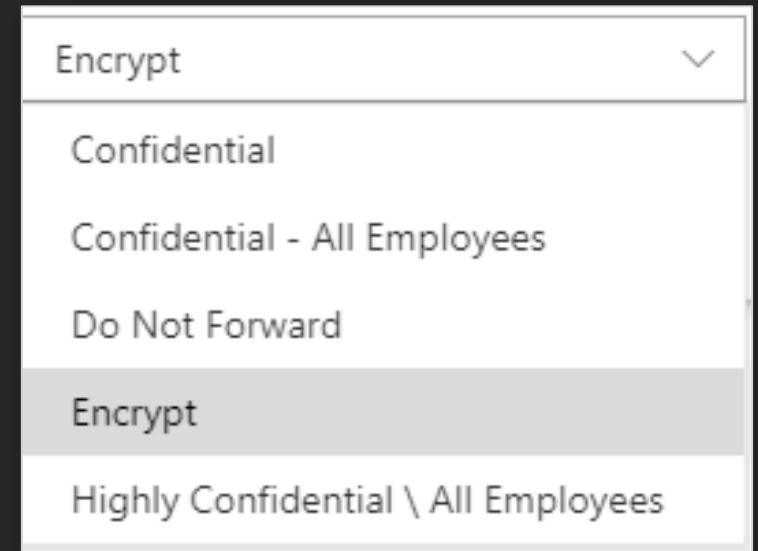
The problem:

Sensitive information is sometimes sent via email

The open nature of email systems means this information is at risk of being read by unauthorized people

The solution:

Encrypt email sent from Microsoft 365 Business, so only the intended recipient can access it.



Email encryption

What it is:

Azure Information Protection provides easy-to-use email encryption capabilities for sending encrypted email

How it works:

The message text and all attachments are encrypted.

Only the recipient can decipher the message for reading.

Anyone else who tries to open the email sees indecipherable text.

Identity verification:

The way the recipient verifies their identity depends on their email system:

- For Office 365 users, authentication happens automatically
- Google, Yahoo, or Outlook.com/Hotmail users sign in with their Google, Yahoo, or Microsoft account
- All others sign in with a one-time passcode

Sending an encrypted email

Note: This demo is most effective if you send an encrypted email to an Outlook.com account, and a separate message to a Gmail account, so the audience can see the two experiences.

To send an encrypted message

To send an encrypted message from Outlook:

- Select **Options > Permissions**
- Select the protection option you need

To send an encrypted message from Outlook on the web:

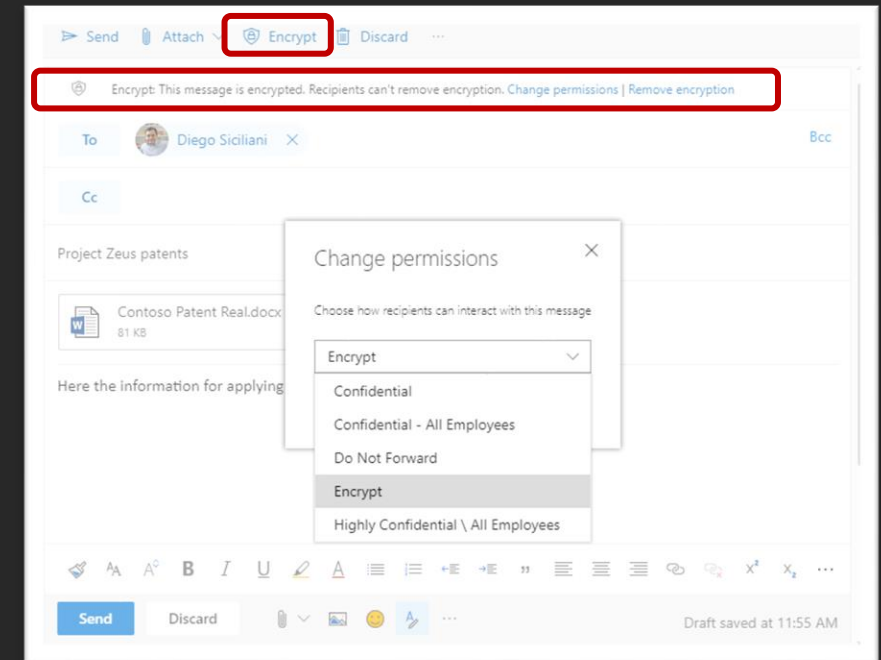
- Select the **Encrypt** button

To view an encrypted message

For email recipients with Office 365, the decryption will happen automatically, and the message will be decrypted upon opening it.

For recipients not using Office 365, the encrypted message will contain a link in the message body.

- Select Read the message
- Select how you'd like to sign in to read the message
 - If your email provider is Google, Yahoo, or Microsoft, you can select Sign in with Google, Yahoo, or Microsoft respectively
 - Otherwise, select sign in with a one-time passcode. Once you receive the passcode in an email message, make a note of the passcode, then return to the web page where you requested the passcode and enter the passcode, and select CONTINUE



Protect and control your data and documents



Encrypt
email



Apply restrictions
to email and
documents



Protect against
data leaks



Archive
email data

Control access to your data and documents

The problem:

Files containing sensitive information often leave the four walls of your business. This puts your data at risk of falling into the wrong hands.

The solution:

Azure Information Protection gives you control over who can access your emails and documents.

You can control whether an email can be forwarded, printed, or viewed by non-employees.

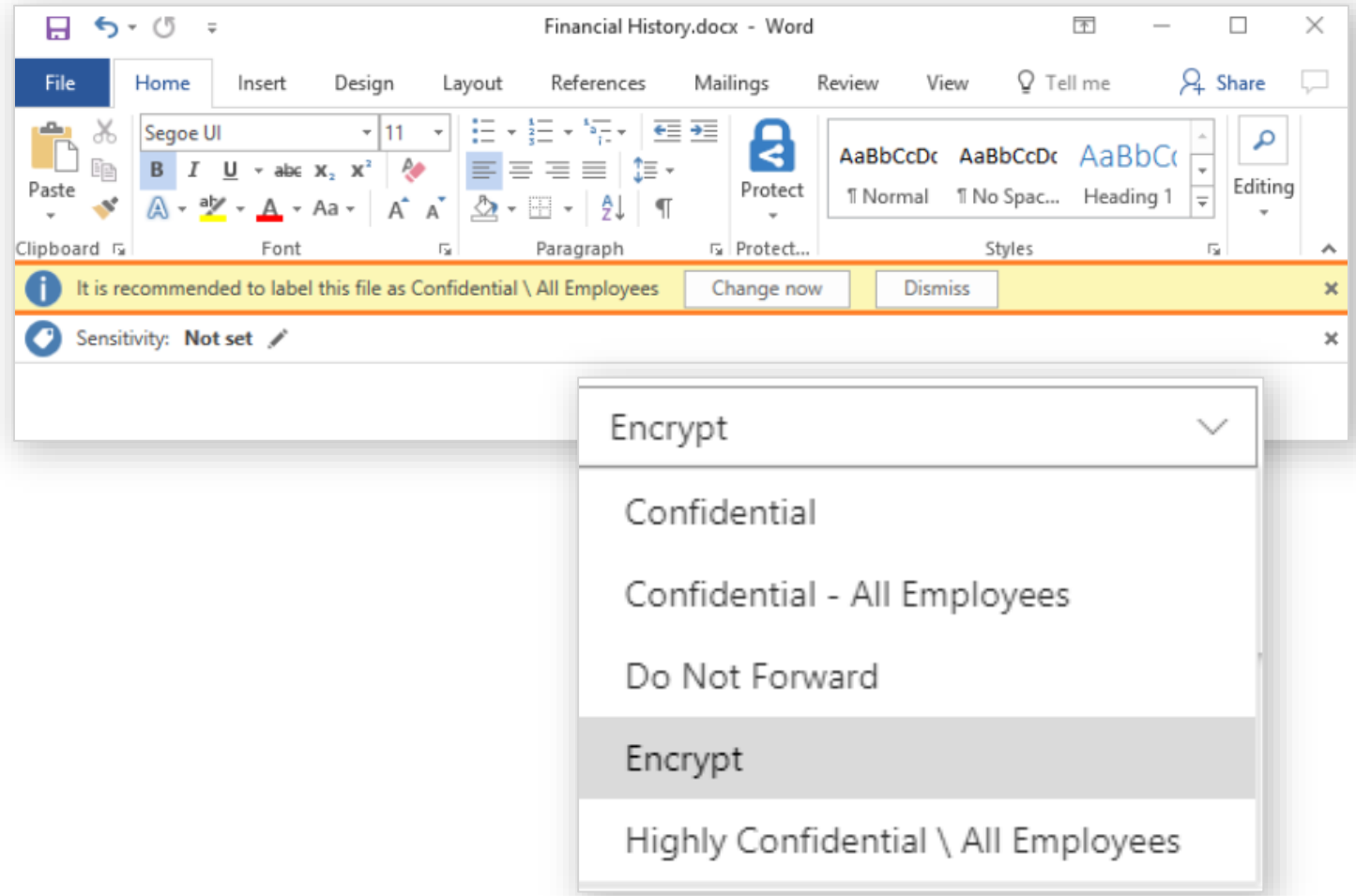
You can control whether a document can be edited, printed, or viewed by non-employees. You can also revoke access.



Azure Information Protection (AIP)

What it is:

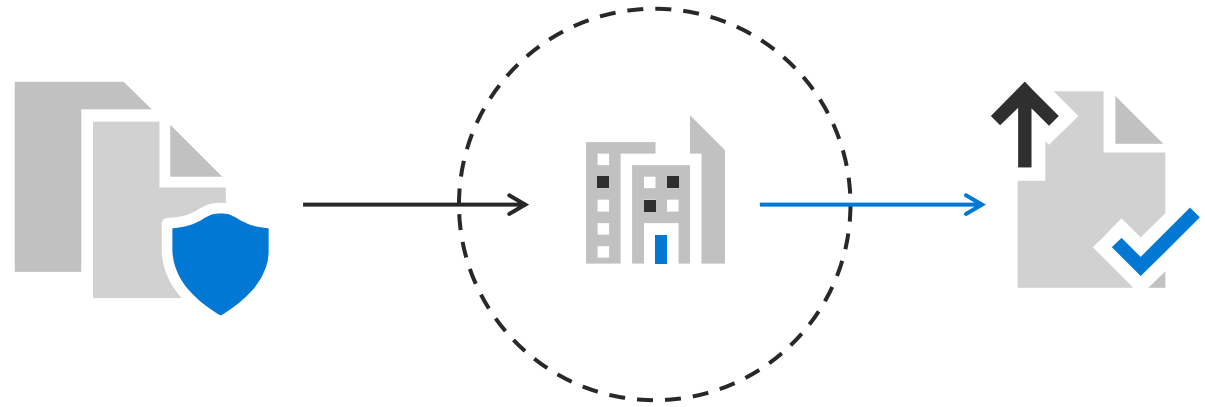
Azure Information Protection helps an organization to classify protect its documents and emails, either by restricting the ability to forward and print, or by applying labels.



Protection follows document, even after it leaves your organization

Restrict access, even if the file is saved outside the company

The restrictions and protections stay with the files and emails regardless of the location. Even if the file is emailed outside the company, or saved to an employee's personal computer, you remain in control of your data.



Azure Information Protection (AIP)

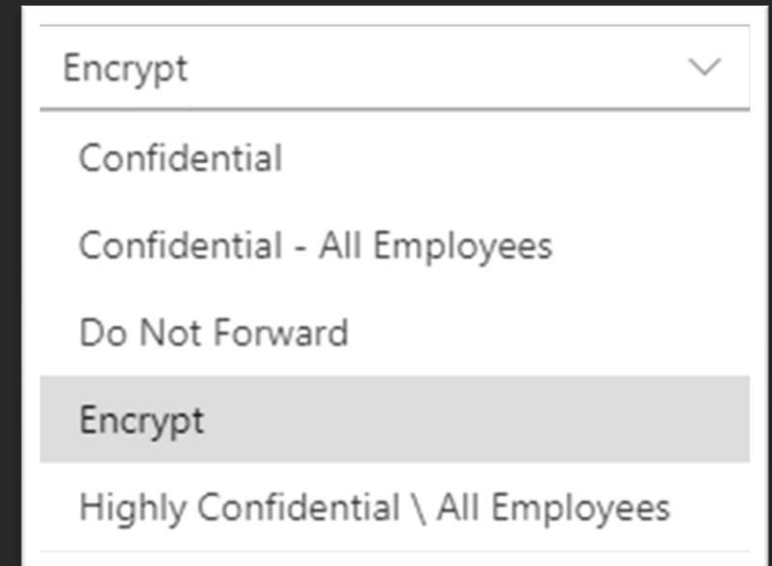
Some examples of how it can be used

You can restrict a sales forecast spreadsheet so that it cannot be accessed by anyone outside your organization.

Your CEO can give managers a heads up about an upcoming reorganization, and mark it "Do Not Forward" so they don't accidentally pass it along.

You can prevent users from sending Reply-All response to a company-wide email.

When an employee leaves your company, you can revoke access to a master list of customers.



Protect and control your data and documents



Encrypt
email



Apply restrictions
to email and
documents



Protect against
data leaks



Archive
email data

Protect against accidental data leaks

The problem:

It is difficult and unrealistic to expect employees to manually check every email or document shared for sensitive information before sharing files outside the company.

The solution:

Enable **Data Loss Prevention (DLP)** policies to automatically identify sensitive information and inform users before sharing this data externally.



Data Loss Prevention

What it is:

The Data Loss Prevention policies help businesses **identify, monitor, and protect sensitive information** through deep content analysis.

Examples of sensitive information that you might want to prevent from leaking outside your organization include personally identifiable information (PII) such as credit card numbers, social security numbers, or health records.

With a DLP policy, you can:

- Identify sensitive information across many locations and apps
- Prevent the accidental sharing of sensitive information
- Monitor and protect sensitive information in the desktop versions of Excel, PowerPoint, and Word
- Help users learn how to stay compliant without interrupting their workflow

Data Loss Prevention

How it works

A DLP policy contains a few basic things:

- Where to protect the content
- When and how to protect the content by enforcing **rules** comprised of:
 - **Conditions** the content must match before the rule is enforced
 - **Actions** that you want the rule to take automatically when content matching the conditions is found
- You can use a rule to meet a specific protection requirement, and then use a DLP policy to group together common protection requirements, such as all of the rules needed to comply with a specific regulation



For example, you might have a DLP policy that helps you detect the presence of information subject to the Health Insurance Portability and Accountability Act (HIPAA). This DLP policy could help protect HIPAA data (the what) across all SharePoint Online sites and all OneDrive for Business sites (the where) by finding any document containing this sensitive information that's shared with people outside your organization (the conditions) and then blocking access to the document and sending a notification (the actions).

Data Loss Prevention

DLP Policy Templates:

DLP comes with templates to save you the work of building a new set of rules from scratch.

You can modify these requirements to fine tune the rule to meet your organization's specific requirements.

Examples of DLP policy templates:

- HIPAA data
- PCI-DSS data
- Gramm-Leach-Bliley Act data
- Locale-specific personally identifiable information



Enable a DLP policy

To enable a DLP policy

- Go to <https://protection.office.com>.
- Sign in to Office 365. You're now in the Office 365 Security & Compliance Center.

In the Security & Compliance Center > left navigation > **Data loss prevention** > **Policy** > **+ Create a policy**.

- Choose the DLP policy template that protects the types of sensitive information that you need > **Next**.

In this example, you'll select **Financial>PCI Data Security Standard (PCI DSS)**.

- Name the policy > **Next**.
- On the **Choose locations** page:
- Choose **All locations in Office 365** > **Next**.
- On the **Customize the type of content you want to protect** page:
 - Click **Find content that contains: Credit Card Number**, and select Detect when this content is shared ... with people outside my organization
 - Click **Next**

On the **What do you want to do if we detect sensitive info** page:

- Select **Show policy tips...**
- Select **Detect when content that's being shared contains: ...** change to 1 instance
- Select **Send incident reports...**
- Click **Next**

On the **Do you want to turn on the policy...** page:

- Select **Yes, turn it on right away**
- Click **Next**

On the **Review your setting** page, click **Create**

Protect and control your data and documents



Encrypt
email



Apply restrictions
to email and
documents



Protect against
data leaks



Archive
email data

Long-term preservation of email

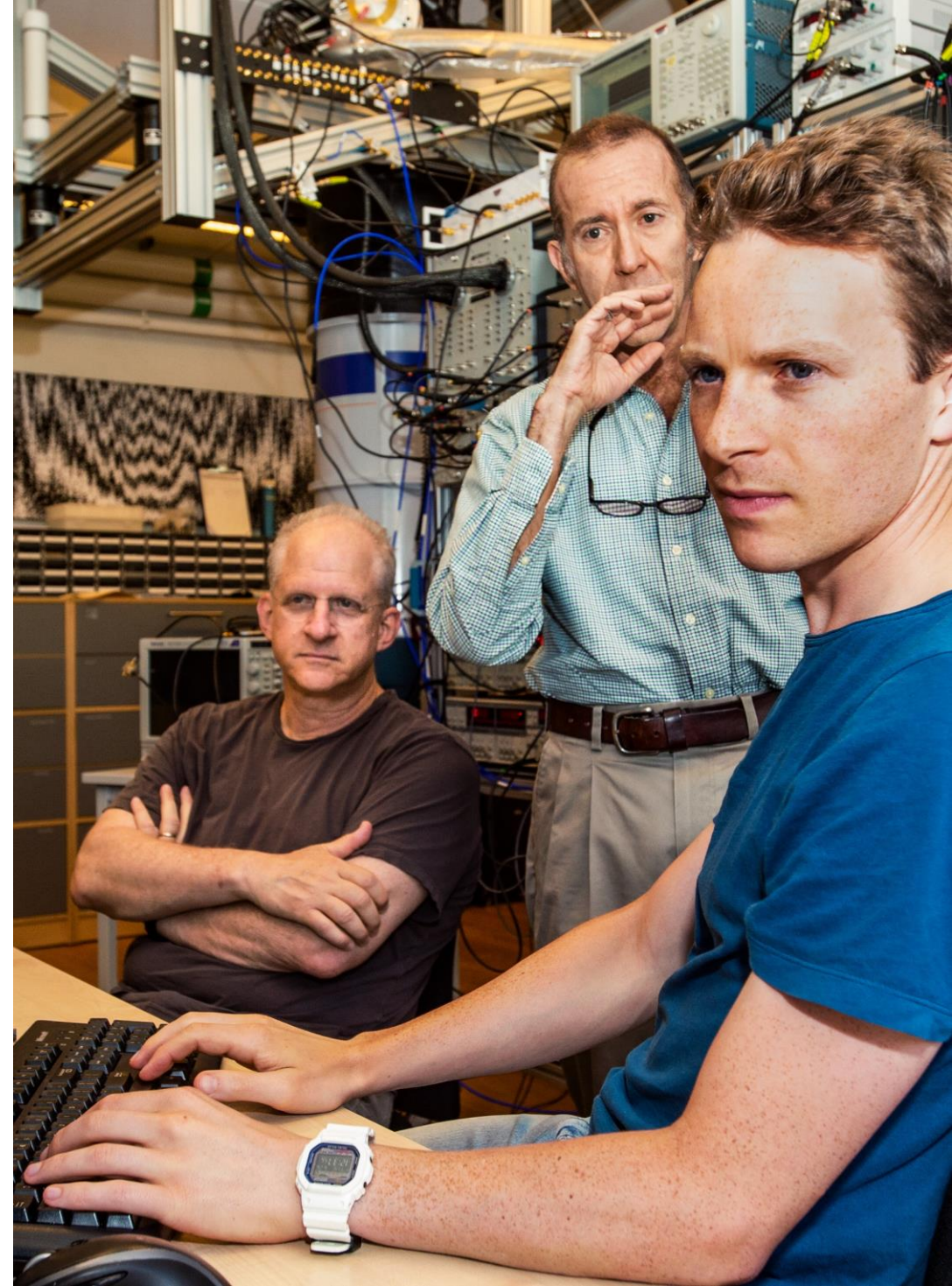
The problem:

After an employee leaves, you may need to access to emails they sent or received.

Or, your company may have a policy of retaining email for a period of time, such as 7 years, to meet regulatory requirements

The solution:

Utilize the capabilities of Exchange Online Archiving to archive and preserve email and other relevant information.



Archiving (In-Place Hold)

What it is:

In-Place Hold and Litigation Hold, part of Exchange Online Archiving, can help companies preserve electronically stored information that could be relevant to a pending or current legal case.

How it works:

You can use In-Place Hold to accomplish the following goals:

- Enable users to be placed on hold and preserve mailbox items immutably
- Preserve mailbox items deleted by users or automatic deletion processes
- Protect mailbox items from tampering, changes by a user, or automatic processes
- Preserve items indefinitely or for a specific duration

Additionally, you can:

- Preserve the entire mailbox of an employee who leaves or is terminated
- Use In-Place eDiscovery to search mailbox items, including items placed on hold

Microsoft Security



Identity and access management

Your universal platform to manage and secure identities.



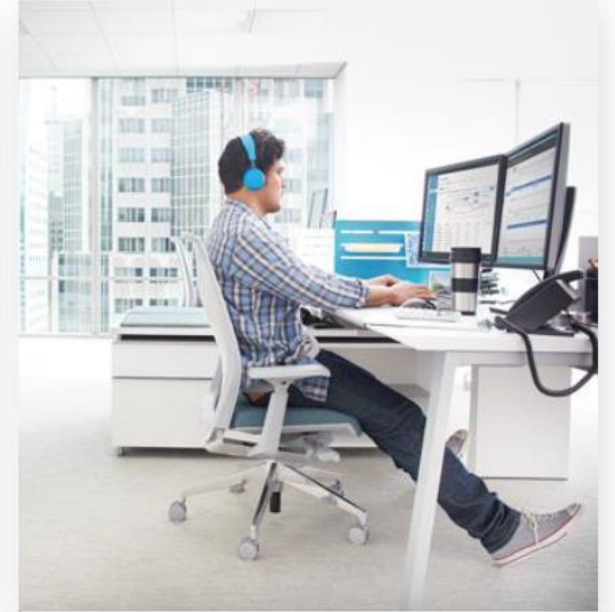
Threat protection

Stop attacks with integrated and automated security.



Information protection

Protect your sensitive data—wherever it lives or travels.



Cloud security

Safeguard your cross-cloud resources.

Questions ?

THANK YOU

For further information please contact
your sales representative or

msftcsp@synnex.com

