Microsoft

CSP Masters Program in person series
Technical training

Microsoft

Security

Security

- ✓ Security foundation
- ✓ Identity security
- ✓ Email protection
- ✓ Information governance
- ✓ Endpoint / Device security
- ✓ Bringing it all together

Microsoft

Security foundations

Cyberthreats– overview

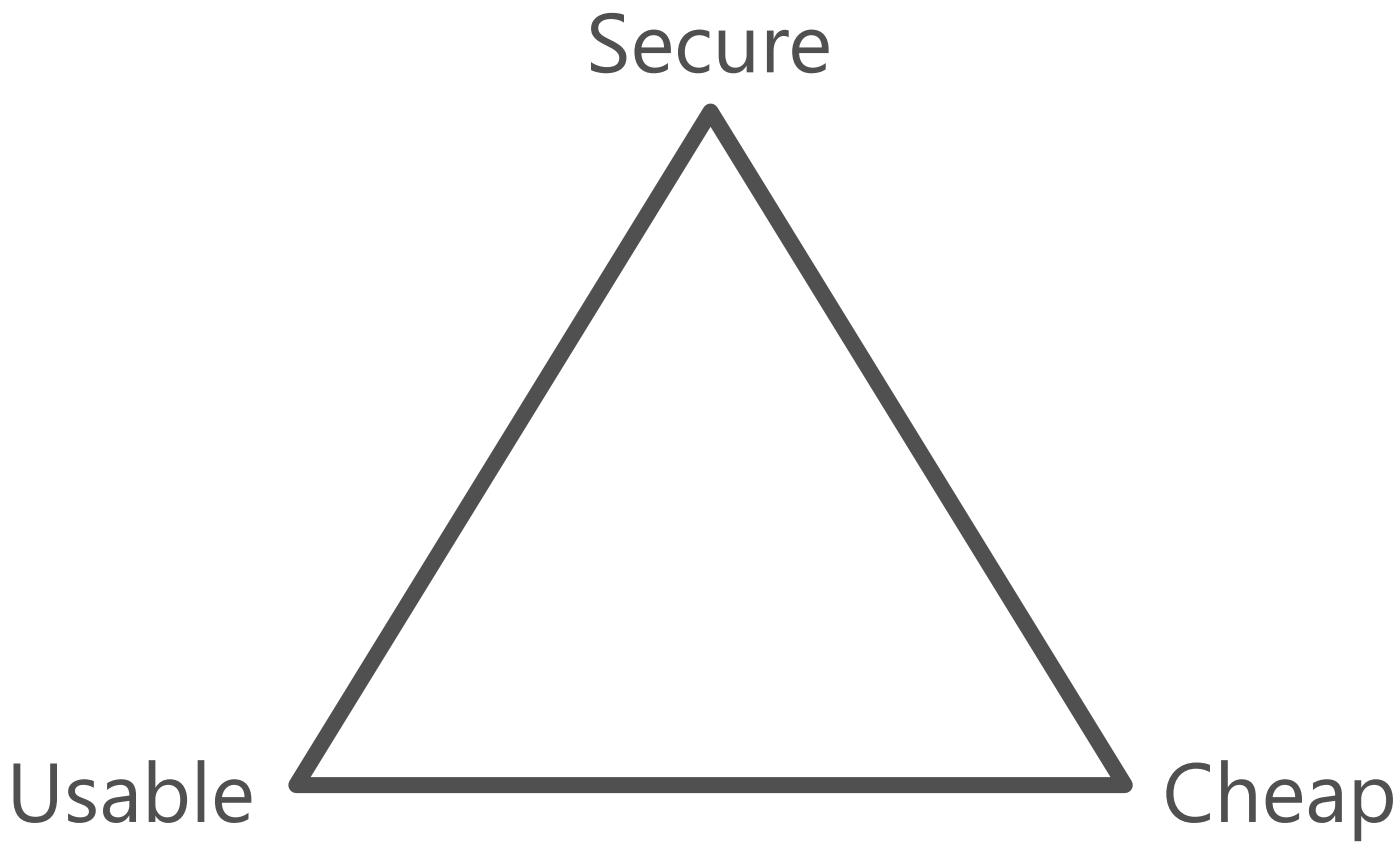
Phishing Fraud in which an attacker masquerades as a reputable person. It's often easier to trick someone than to hack in.

Ransomware Malicious encryption software that blocks access to systems and demands a sum of money to unlock. An infected PC can spread the ransomware to other computers on your network.

Fileless attacks use malicious scripts that hijack legitimate software and load malware into memory, without saving to the file system. This makes the malware harder to detect.

Live off the land attacks use trusted software and system tools to carry out their work. Examples are administrative shells, antivirus programs, RMM software, etc. This makes it difficult to detect and/or determine who is behind the activity.

The Security Dilemma



Perception

I am too small a business for hackers to attack me…only large enterprises need to worry about security…

Reality

"Someone was **fooled by the email from the CEO** and used his Corp card to send the iTunes gift cards. We lost about $5,000."

—Adam A., equipment rentals, 150 employees

"The only reason **we caught it** was that it was a 6-digit sales order and our sales orders are 7 digits."

— Joe B, food distribution, 250 employees

"They **got someone's password**, and sent an email to our CFO, who sent the $40,000 wire transfer."

— Bob K., property management, 150 employees

Australian Government

Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches (NDB) scheme in Australia

- Starting on 22nd February 2018
- Australian organisations are required to notify any individuals likely to be at risk of serious harm by a data breach.
- Examples of a data breach include when:
  - a device containing customers' personal information is lost or stolen
  - a database containing personal information is hacked
  - personal information is mistakenly provided to the wrong person.
- For more information visit *https://oaic.gov.au*

Data breaches involving managed service providers

A failure by both the MSP and its clients to notify the OAIC and individuals at risk of serious harm from a data breach will represent a breach of the provisions of Part IIIC of the Privacy Act, and will likely constitute an interference with privacy by all.

https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020/

SMBs and Security

80% of SMBs

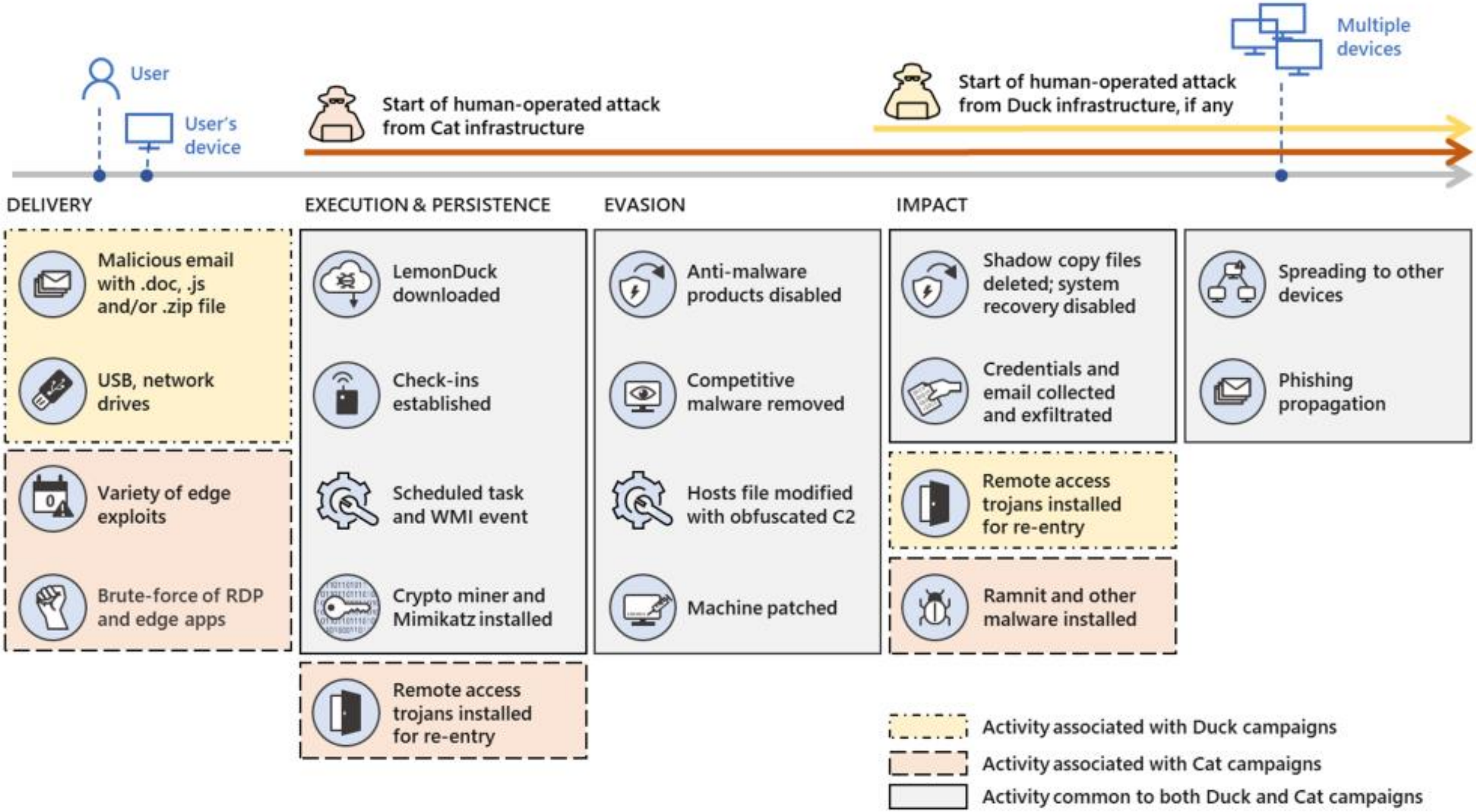
have antivirus in place, but 93% still have Security concerns

70% of SMBs

believes security is becoming more of a risk

Nearly 1 in 4

have experienced a cyber attack


User
User's device
Start of human-operated attack from Cat infrastructure
Start of human-operated attack from Duck infrastructure, if any
Multiple devices
DELIVERY
EXECUTION & PERSISTENCE
EVASION
IMPACT
Malicious email with .doc, .js and/or .zip file
USB, network drives
Variety of edge exploits
Brute-force of RDP and edge apps
LemonDuck downloaded
Check-ins established
Scheduled task and WMI event
Crypto miner and Mimikatz installed
Remote access trojans installed for re-entry
Anti-malware products disabled
Competitive malware removed
Hosts file modified with obfuscated C2
Machine patched
Shadow copy files deleted; system recovery disabled
Credentials and email collected and exfiltrated
Remote access trojans installed for re-entry
Ramnit and other malware installed
Spreading to other devices
Phishing propagation
Activity associated with Duck campaigns
Activity associated with Cat campaigns
Activity common to both Duck and Cat campaigns

Business Premium partner opportunity

85%

of partners see **security** as biggest area of growth[1]

How do we expand security services beyond basic AV?

How do we deliver services at scale?

How do we do so without increasing cost?

Sources: [1]Channel Futures | 2020 MSP 501 Full Report

Microsoft

Zero trust

What is Zero Trust and how does it help me protect my customer?

Name: Bob D

Role: Technical Consultant

Company: Partner

The increasingly complex state of cybersecurity

Attack surface is expanding due to hybrid work

Rapid acceleration and increasing sophistication of cybercrime

Rising cost of cybersecurity risk mitigation and remediation

Common challenges with access security today

Rapid increase of identities
(employees, partners, customers, digital workloads) that **need to be protected**

Hybrid work requires seamless, flexible experiences while **keeping access secure**

Evolving regulations with data privacy and security implications

Accelerated growth of apps, on and off the corporate network, **requiring secure access**

Identity attacks are on the rise—
921 password attacks per second[1]
and new attack vectors (e.g., token theft)

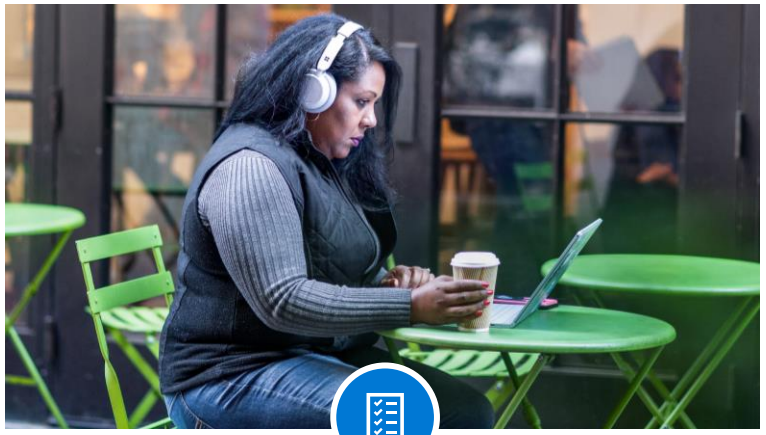
1. "This World Password Day consider ditching passwords altogether". May 5, 2022, Microsoft Security

Solve secure access challenges with a Zero Trust approach

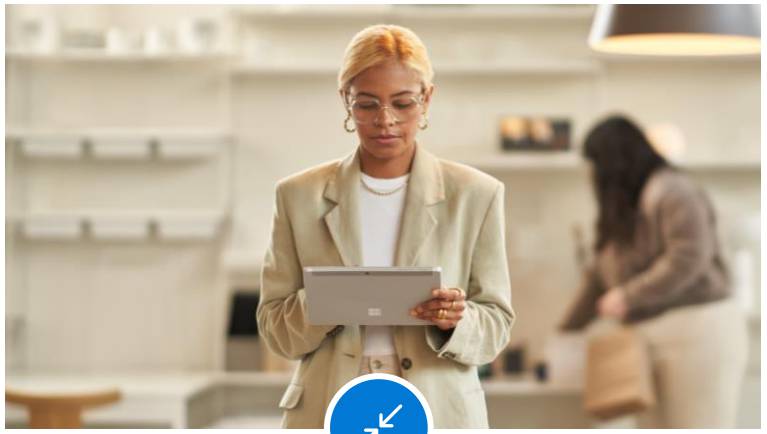
Zero Trust defined

A proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to respond to threats

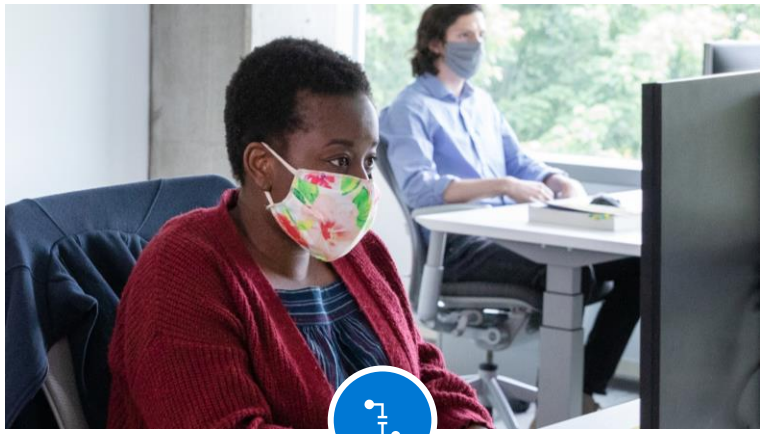
Zero Trust principles



Verify explicitly

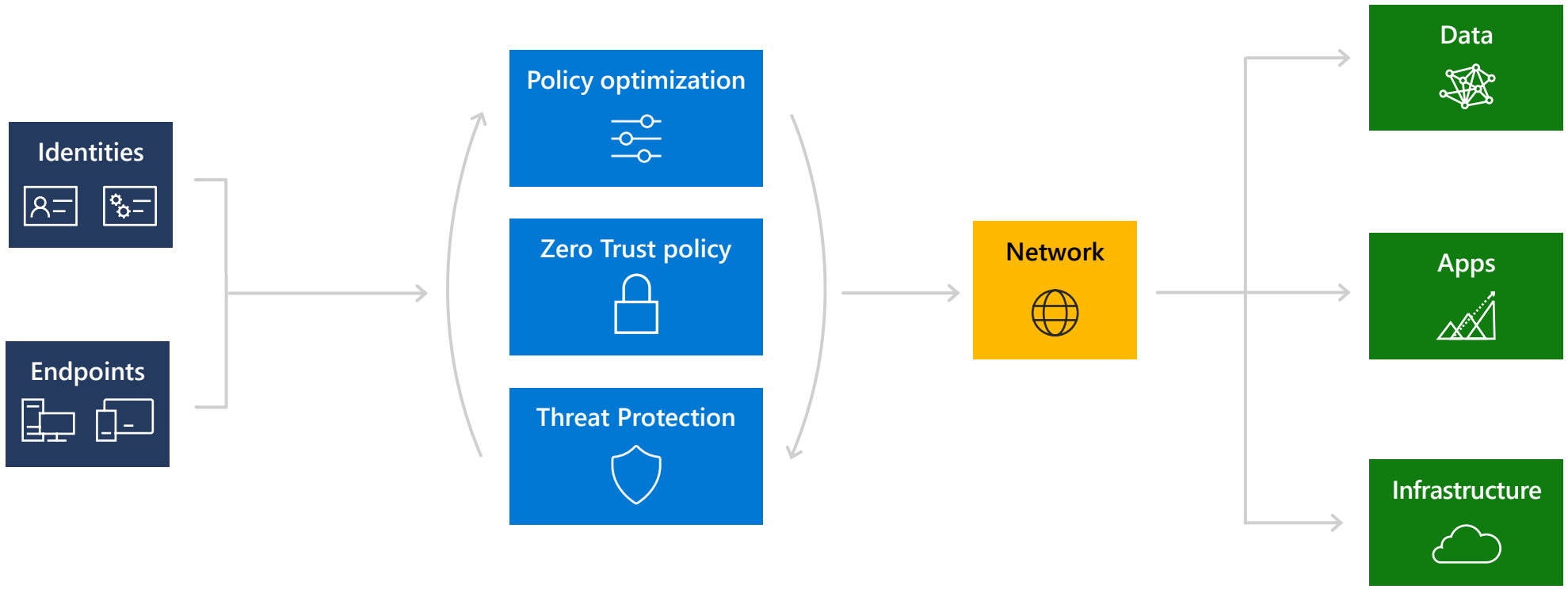


Use least privilege access

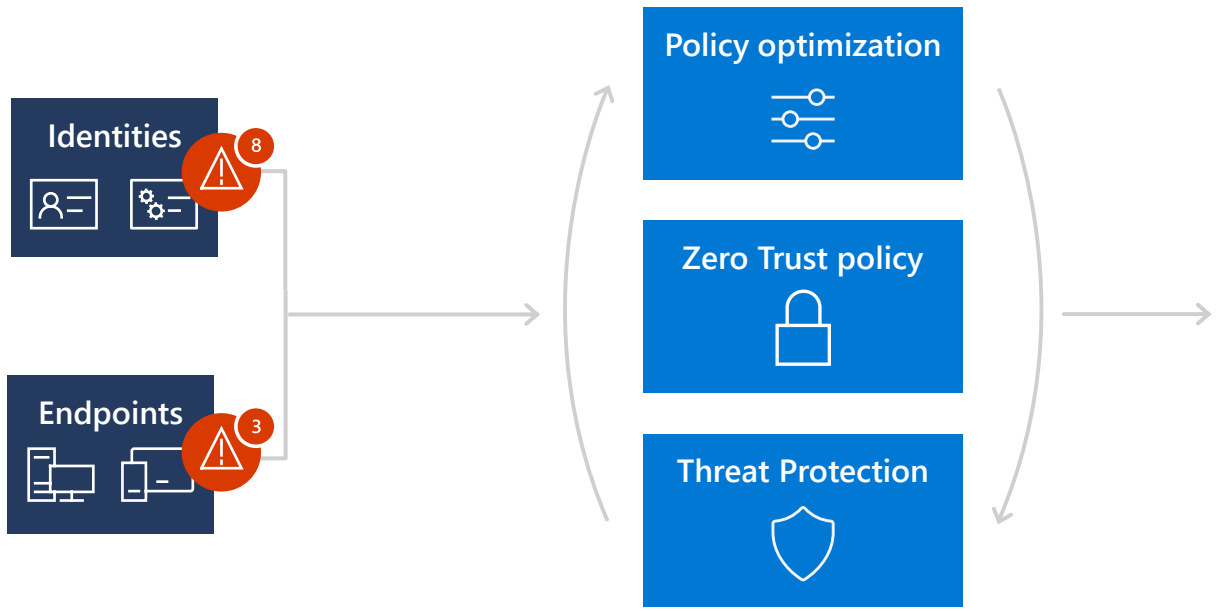


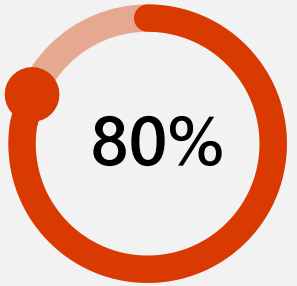
Assume breach

Zero Trust starts with secure identities and endpoints



Identities and endpoints are your first line of defense





of breaches involve the use of lost or stolen passwords.[1]

of BYO devices are not secured by IT.[2]

Monitoring and analytics

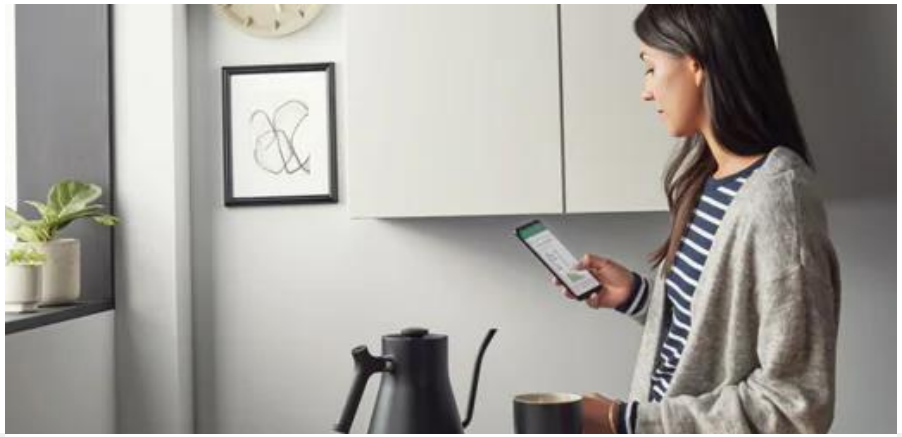
1. "Verizon 2020 Data Breach Investigations Report"
2. "Mobile security—the 60 percent problem" Brian Peck, Zimperium, April 7, 2020

An integrated and complete solution for securing access and identities

Secure identities and access

Azure Active Directory P1

Secure Endpoints



Microsoft Endpoint Manager

Microsoft Defender for Defender for Business

Endpoint security for Zero Trust is a team sport

Microsoft Endpoint Manager

simplifies management workflows across cloud and on premises endpoints for Zero Trust security.

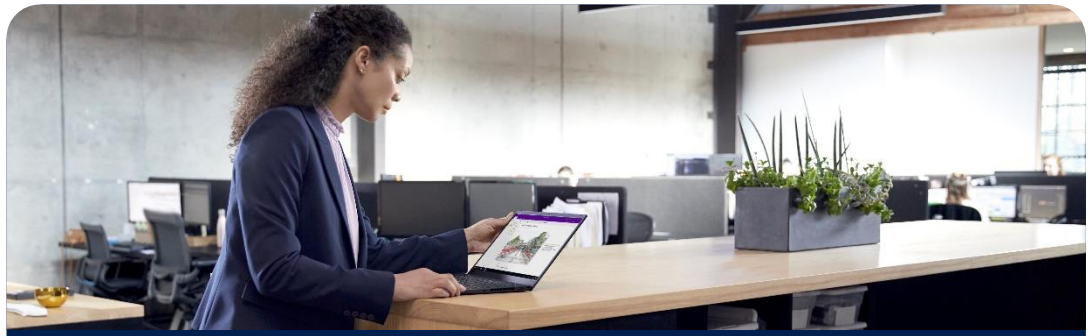
- Visibility and control with continuous health, compliance, and security signaling
- Set policies and manage company and employee-owned device compliance
- Zero touch deployment, and non-intrusive app management supports seamless user experiences

Microsoft Defender for Business

provides visibility into endpoints accessing corporate resources, one of the first steps in a Zero Trust device strategy.

- Monitor and gain visibility into configuration profiles while exposing security anomalies
- Evaluate every endpoint for risks and employ granular access controls to devices
- Discover unmanaged and unauthorized endpoints and network devices

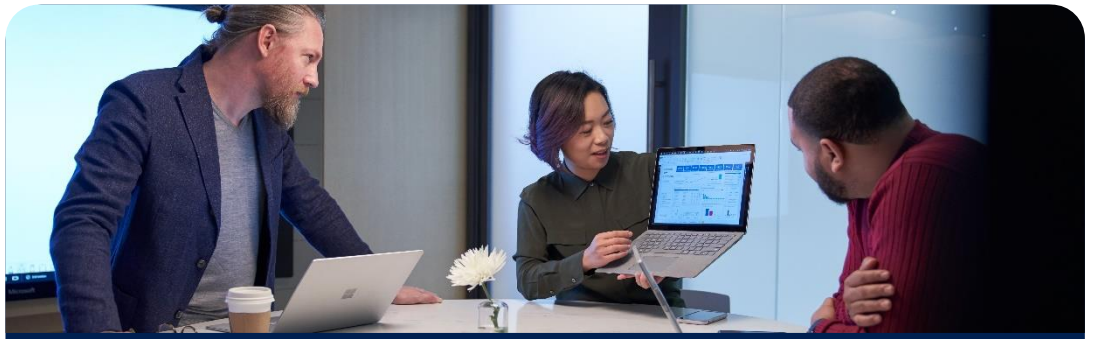
Two key offers for SMBs



01

Business Premium

Comprehensive Security with device management and productivity



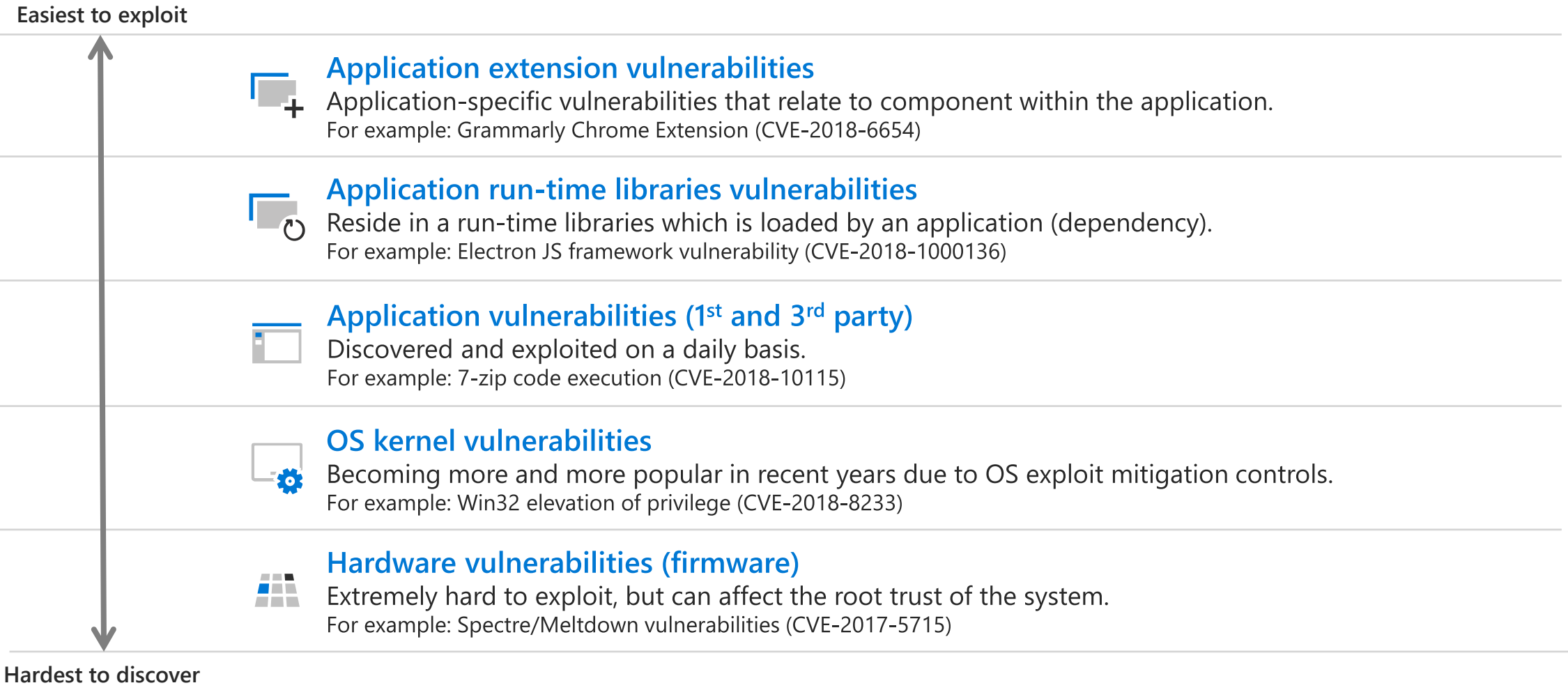
02

Microsoft Defender for Business

Standalone endpoint Security to protect customers devices and endpoints

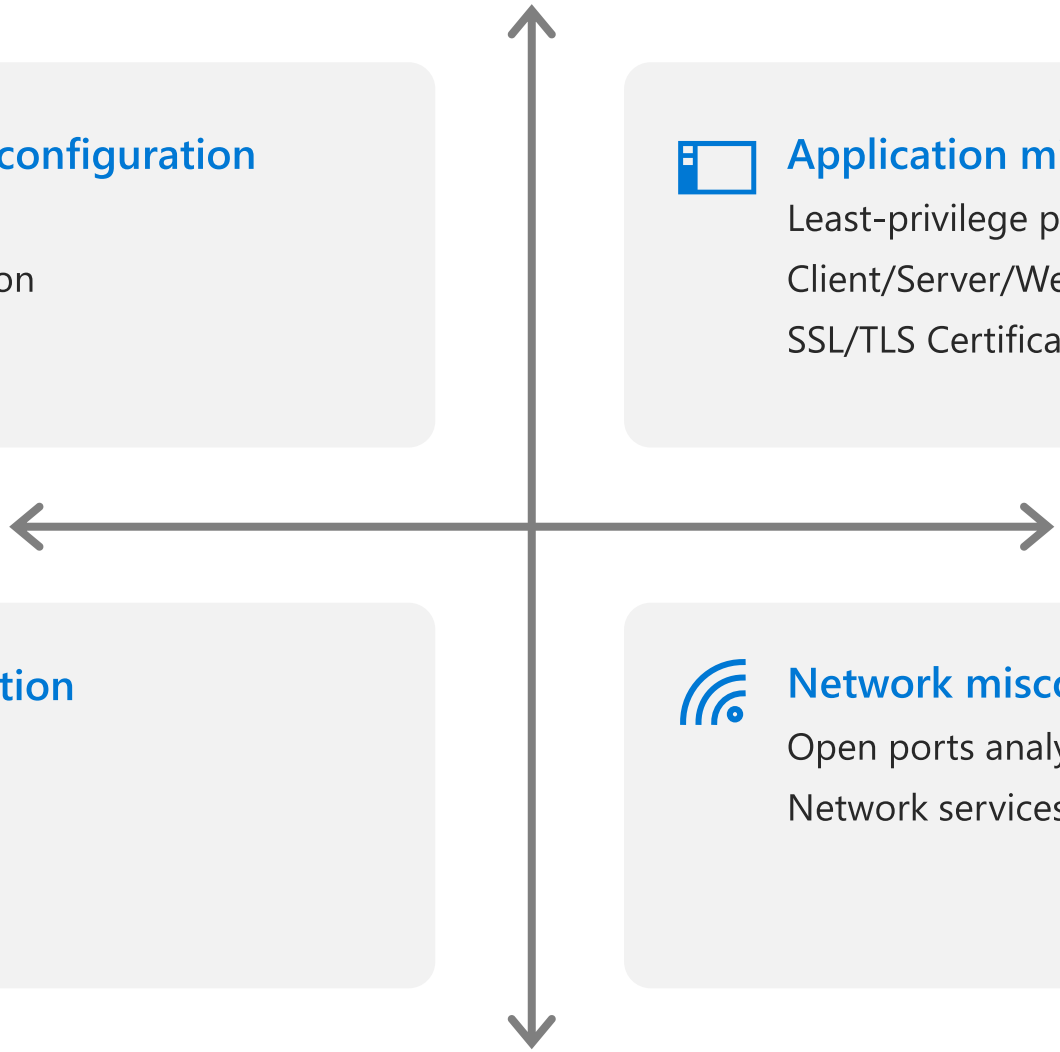
Extensive vulnerability assessment across the entire stack

Continuous real-time discovery



Broad secure configuration assessment

Continuous real-time discovery



Operation system misconfiguration

File Share Analysis

Security Stack configuration

OS baseline

Application misconfiguration

Least-privilege principle

Client/Server/Web application analysis

SSL/TLS Certificate assessment

Account misconfiguration

Password Policy

Permission Analysis

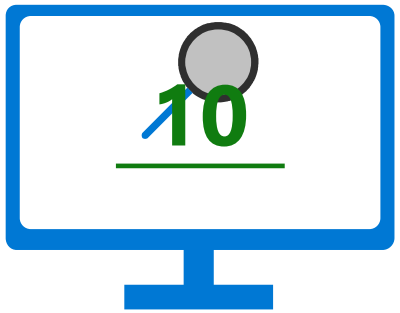
Network misconfiguration

Open ports analysis

Network services analysis

Helping customers focus on the right things at the right time

Threat & Business Prioritization (“TLV”)



T

Threat Landscape

Vulnerability characteristics (CVSS score, days vulnerable)

Exploit characteristics (public exploit & difficulty, bundle)

EDR security alerts (Active alerts, breach history)

Threat analytics (live campaigns, threat actors)

L

Breach Likelihood

Current security posture

Internet facing

Exploit attempts in the org

V

Business Value

HVA analysis (WIP, HVU, critical process)

Run-time & Dependency analysis

Home > Audit log search

Audit log search

! To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a report.

Turn on auditing

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search

Clear

Activities

Show results for all activities

Start date

2020-02-11 00:00

End date

Results

Date	IP address	User	Activity	Item	Detail

Run a search to view results

https://protection.office.com/unifiedauditlog

Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search

Clear

Activities

User signed in to Teams

Start date

2017-04-01 00:00

End date

2017-05-09 00:00

Users

Show results for all users

Results

150 results found (More items available, scroll down to see more.)

Filter results

Export res

Date	IP address	User	Activit	
2017-05-08 10:...		admin@ciaops...	User signed in to Te...	web (1415/1.0....
2017-05-06 10:...		admin@ciaops...	User signed in to Te...	web (1415/1.0....
2017-05-06 10:...		admin@ciaops...	User signed in to Te...	web (1415/1.0....
2017-05-06 10:...		admin@ciaops...	User signed in to Te...	web (1415/1.0....
2017-05-06 10:...		admin@ciaops...	User signed in to Te...	web (1415/1.0....
2017-05-06 09:...		admin@ciaops...	User signed in to Te...	web (1415/1.0....

ciaopslabs | Overview

Azure Active Directory

Overview
Preview features
Diagnose and solve problems

Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security

Monitoring
Sign-ins
Audit logs
Provisioning logs
Logs
Diagnostic settings
Workbooks
Usage & insights

Troubleshooting + Support
Virtual assistant (Preview)
New support request

Add | Manage tenants | What's new | Preview features | Got feedback?

Overview | Monitoring | Tutorials

Search your tenant

Basic information

Name	ciaopslabs	Users	2
Tenant ID	[redacted]	Groups	3
Primary domain	ciaopslabs.com.au	Applications	2
License	Azure AD Premium P2	Devices	1

My feed

RC **Robert Crane** [redacted]

Global administrator
More info

TLS 1.0, 1.1 and 3DES deprecation
Upcoming TLS 1.0, 1.1 and 3DES deprecation for Azure AD. Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

Secure Score for Identity
67.31%
Secure score updates can take up to 48 hours.

Azure AD Connect
Not enabled
Sync has never run

Feature highlights

Access reviews
Make sure only the right people have continued access.

Authentication methods
Configure your users in the authentication methods policy to enable passwordless authentication.

Azure AD Domain Services
Lift-and-shift legacy applications running on-premises into Azure.

Tenant restrictions
Specify the list of tenants that their users are permitted to access.

Privileged Identity Management
Manage, control, and monitor access to important resources in your organization.

Conditional Access
Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

Quick actions

ciaopslabs | Sign-ins

Azure Active Directory

- Overview
- Preview features
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations

Download | Export Data Settings | Troubleshoot | Refresh | Columns | Got feedback?

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 24 hours** | Show dates as : **Local** | Add filters

User sign-ins (interactive) | User sign-ins (non-interactive) | Service principal sign-ins | Managed identity sign-ins

Date	Request ID	User	Application	Status	IP address	Location
8/2/2021, 1:42:19 PM	89d68567-99e9-4fb...	09dabc45-a14b-47a...	Azure Portal	Interrupted	203.129.21.57	
8/2/2021, 1:39:58 PM	37a89011-e1c3-477...	Robert Crane	Microsoft App Acces...	Success	203.129.21.57	Coogee, New South
8/2/2021, 1:39:50 PM	ca294ba3-5859-49d...	Robert Crane	My Profile	Success	203.129.21.57	Morwell, Victoria, AU
8/2/2021, 1:39:39 PM	a231f36d-f776-4c7e...	Robert Crane	Azure Portal	Success	203.129.21.57	Morwell, Victoria, AU
8/2/2021, 1:39:37 PM	bfc6db96-ab38-47bf...	Robert Crane	Azure Portal	Interrupted	203.129.21.57	Coogee, New South

How long does Azure AD store the data?

Activity reports

Report	Azure AD Free	Azure AD Premium P1	Azure AD Premium P2
Audit logs	7 days	30 days	30 days
Sign-ins	7 days	30 days	30 days
Azure AD MFA usage	30 days	30 days	30 days

Security signals

Report	Azure AD Free	Azure AD Premium P1	Azure AD Premium P2
Users at risk	7 days	30 days	90 days
Risky sign-ins	7 days	30 days	90 days

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention

Mailbox actions logged by mailbox audit logging

When you enable mailbox audit logging for a mailbox, access to the mailbox and certain administrator and delegate actions are logged by default. To log actions taken by the mailbox owner, you must specify which owner actions should be audited.

Action	Description	Admin	Delegate	Owner
Copy	An item is copied to another folder.	Yes	No	No
Create	An item is created in the Calendar, Contacts, Notes, or Tasks folder in the mailbox; for example, a new meeting request is created. Note that message or folder creation isn't audited.	Yes[1]	Yes[1]	Yes
FolderBind	A mailbox folder is accessed.	Yes[1]	Yes[2]	No
HardDelete	An item is deleted permanently from the Recoverable Items folder.	Yes[1]	Yes[1]	Yes
MailboxLogin	The user signed in to their mailbox.	No	No	Yes[3]
MessageBind	An item is accessed in the reading pane or opened.	Yes	No	No
Move	An item is moved to another folder.	Yes[1]	Yes	Yes
MoveToDeletedItems	An item is moved to the Deleted Items folder.	Yes[1]	Yes	Yes
SendAs	A message is sent using Send As permissions.	Yes[1]	Yes[1]	No
SendOnBehalf	A message is sent using Send on Behalf permissions.	Yes[1]	Yes	No
SoftDelete	An item is deleted from the Deleted Items folder.	Yes[1]	Yes[1]	Yes
Update	An item's properties are updated.	Yes[1]	Yes[1]	Yes

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention

Demo

Alerts

Reply all | Delete Junk | ...

Low-severity alert: Creation of forwarding/redirect rule

Office365Alerts@microsoft.com
Today, 10:21 PM
sunil kadam; Ileana Olivares; Stuart Clanker; Angel Madera; Vidya Paygude; Woo Lin; Jose Cardenas; Berthold Heinrich; Exchange Admin; Braydon Rigby; Raviv Tamir; Avital Lange; Rob McCarthy; +49 more

Reply all

Office 365

A low-severity alert has been triggered

Creation of forwarding/redirect rule

Severity: Low
Time: 9/14/2018 5:19:00 AM (UTC)
Activity: MailRedirect
User: janedoe@securescoreteam.com
Details: MailRedirect. This alert is triggered whenever someone gets access to read your user's email.

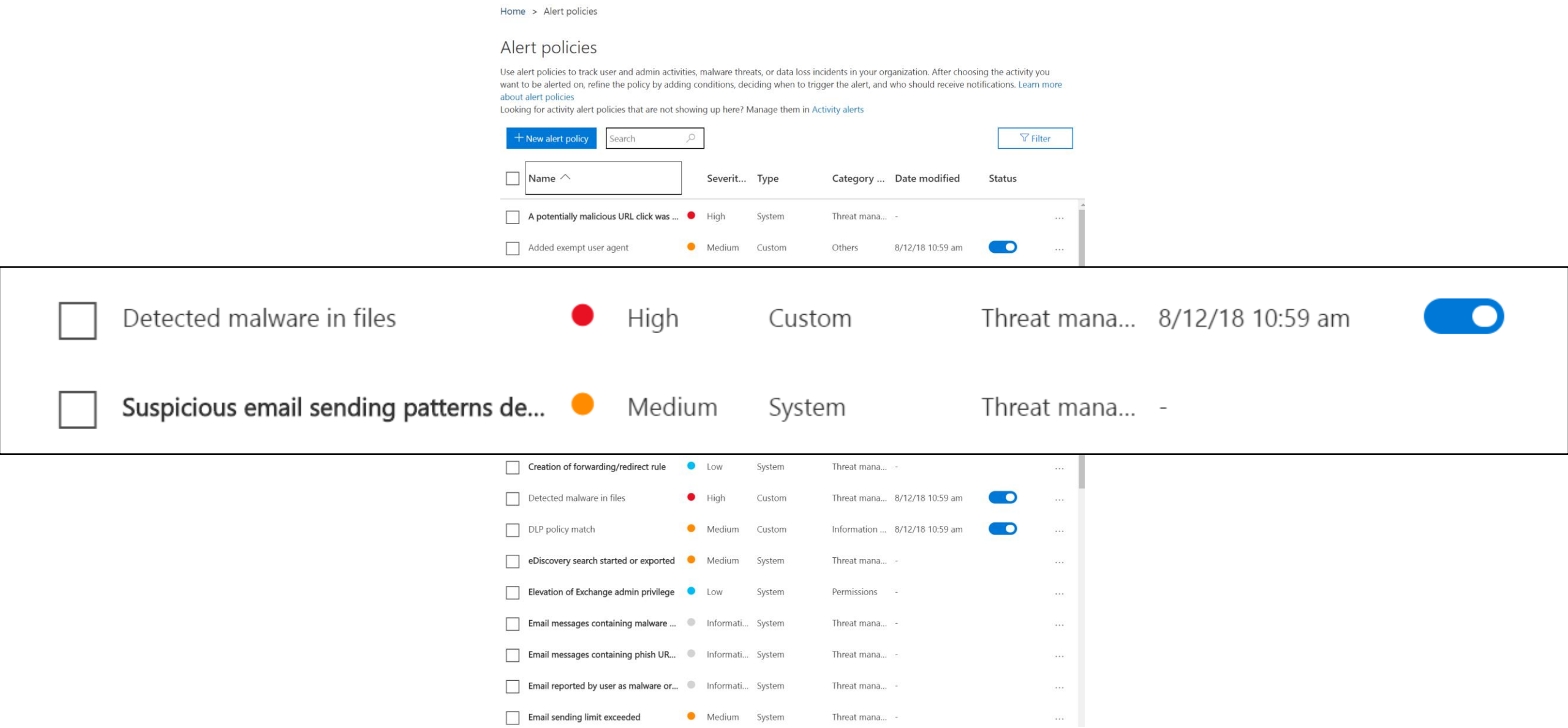
Investigate

Thank you,
The Office 365 Team

Microsoft

One Microsoft Way
Redmond, WA

Protection Alerts



https://protection.office.com/alertpolicies

Activity Alerts

Home > Manage alerts

Activity alerts

! We are working on a better experience for you to manage and view security and compliance alerts. Go to Alert policies

+ New alert policy

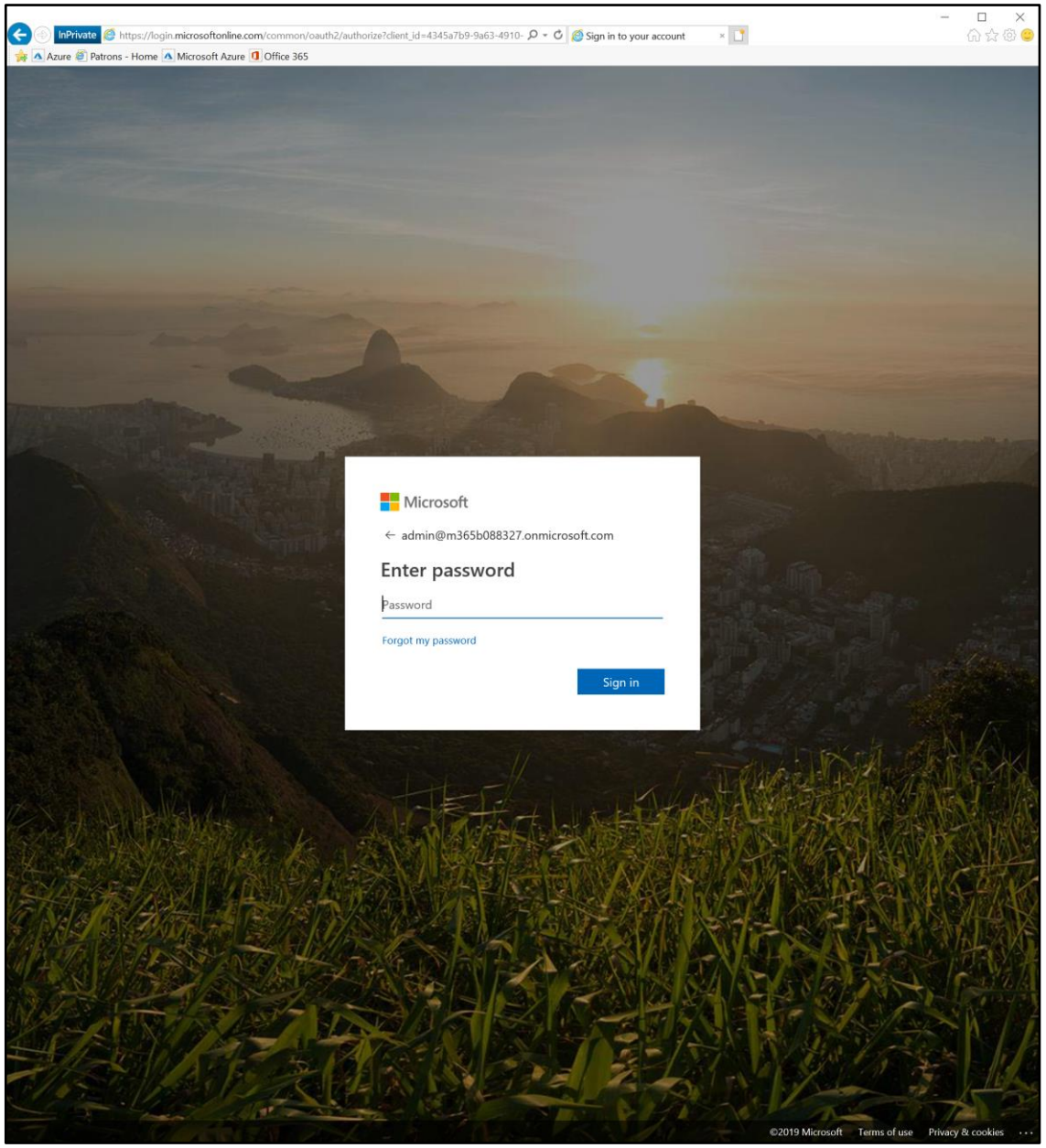
Name	Recipients	Status	Date modified
Role Alert	admin@ciaops365.com	On	2018-07-03 13:01:37
Administrator Password change	director@ciaops.com	On	2017-10-03 18:17:45
Company Information Alert	admin@ciaops365.com	On	2018-07-03 13:01:37
File and Page Alert	admin@ciaops365.com	On	2018-07-03 13:01:29
Site Alert	admin@ciaops365.com	On	2018-07-03 13:01:32
Domain Alert	admin@ciaops365.com	On	2018-07-03 13:01:38
Sharing Alert	admin@ciaops365.com	On	2018-07-03 13:01:30
Access Alert	admin@ciaops365.com	On	2018-07-03 13:01:32
OneDrive sharing	admin@ciaops365.com	On	2017-05-07 10:51:06
Anonymous Links Alert	admin@ciaops365.com	On	2018-07-03 13:01:30
Office Alert	admin@ciaops365.com	On	2018-07-03 13:01:33
Password Alert	admin@ciaops365.com	On	2018-07-03 13:01:36
Mailbox Alert	admin@ciaops365.com	On	2018-07-03 13:01:34

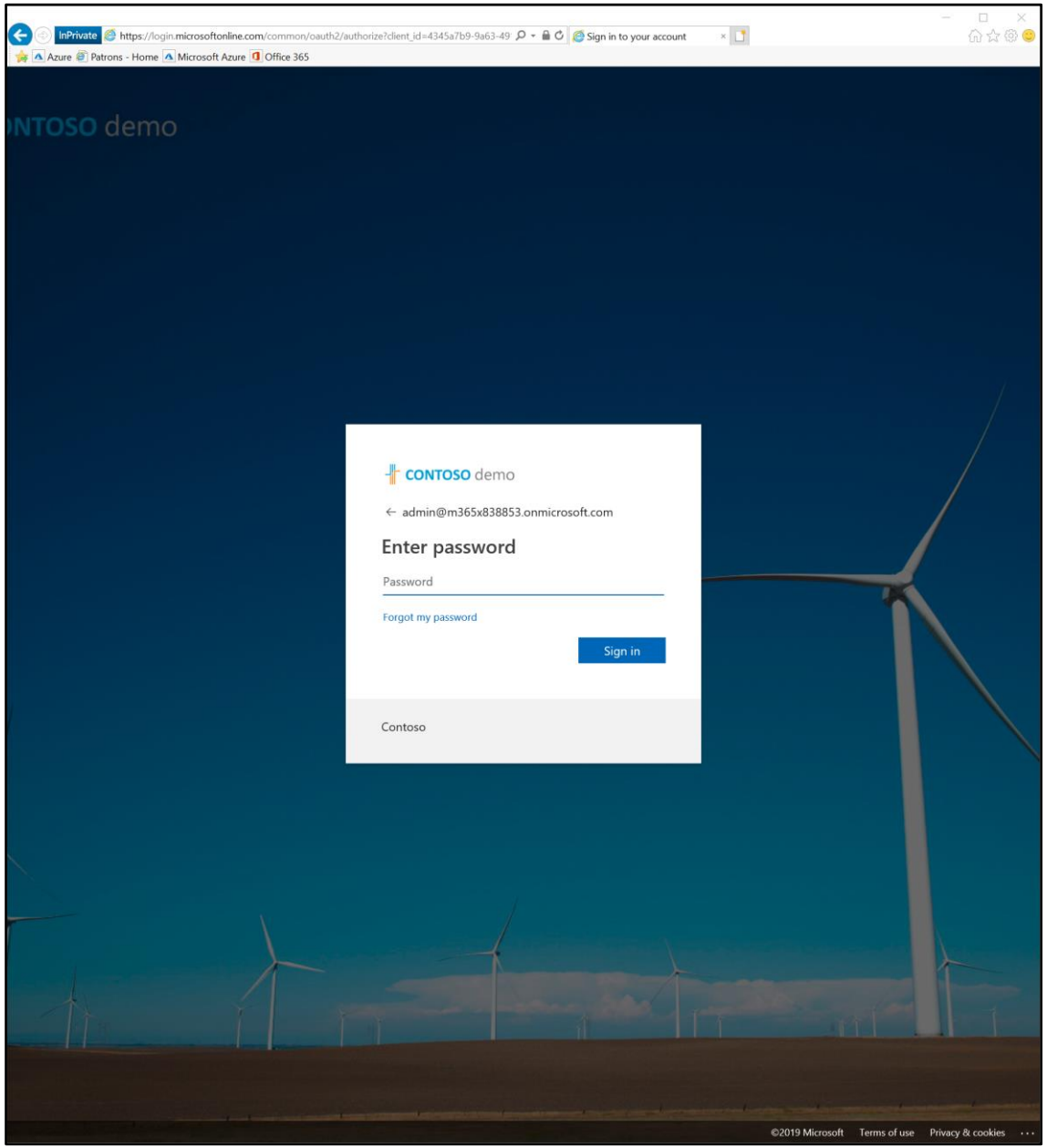
https://protection.office.com/managealerts

Demo

Branding

Tenant branding





CIAOPS - Company branding
Azure Active Directory

Search (Ctrl+/)

- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Notifications settings
- Security

Monitoring

- Sign-ins
- Audit logs
- Provisioning logs (Preview)
- Logs
- Diagnostic settings
- Workbooks
- Usage & insights

New language | Delete

Locale
Default

Edit company branding
Azure Active Directory

Save | Discard

Sign-in page background image
Image size: 1920x1080px
File size: <300KB
File type: PNG, JPG, or JPEG

Remove
Select a file

Banner logo
Image size: 280x60px
File size: 10KB
File type: Transparent PNG, JPG, or JPEG

Remove
Select a file

Username hint

Sign-in page text
Need to Know

Advanced settings

Sign-in page background color #FFFFFF

https://docs.microsoft.com/en-us/microsoft-365/admin/setup/customize-sign-in-page?view=o365-worldwide

Microsoft

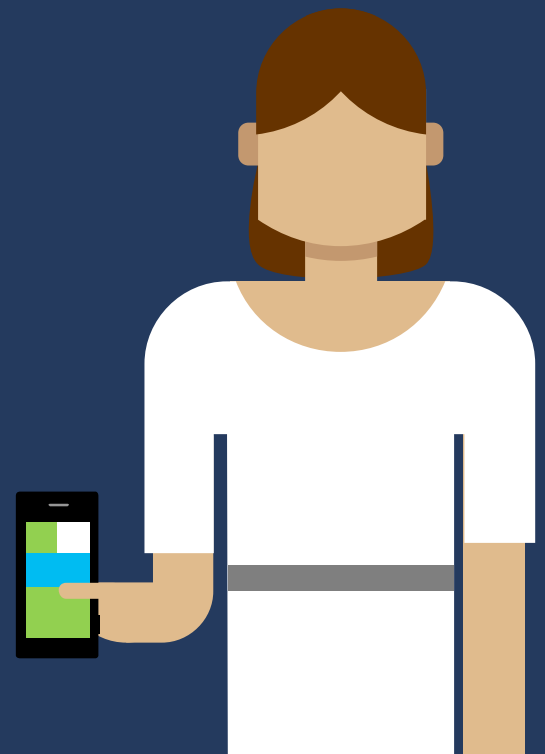
Microsoft 365 Business Premium

What security features are there in Microsoft 365 Business Premium?

Name: Adele V

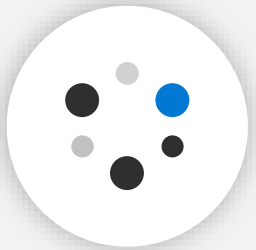
Role: Partner Resource

Company: Partner



Microsoft 365 Business Premium

One solution to run your business securely, from anywhere



Collaborate in real time

Enable secure access to work apps

Protect against cyberthreats and safeguard data

Secure company owned and personal devices

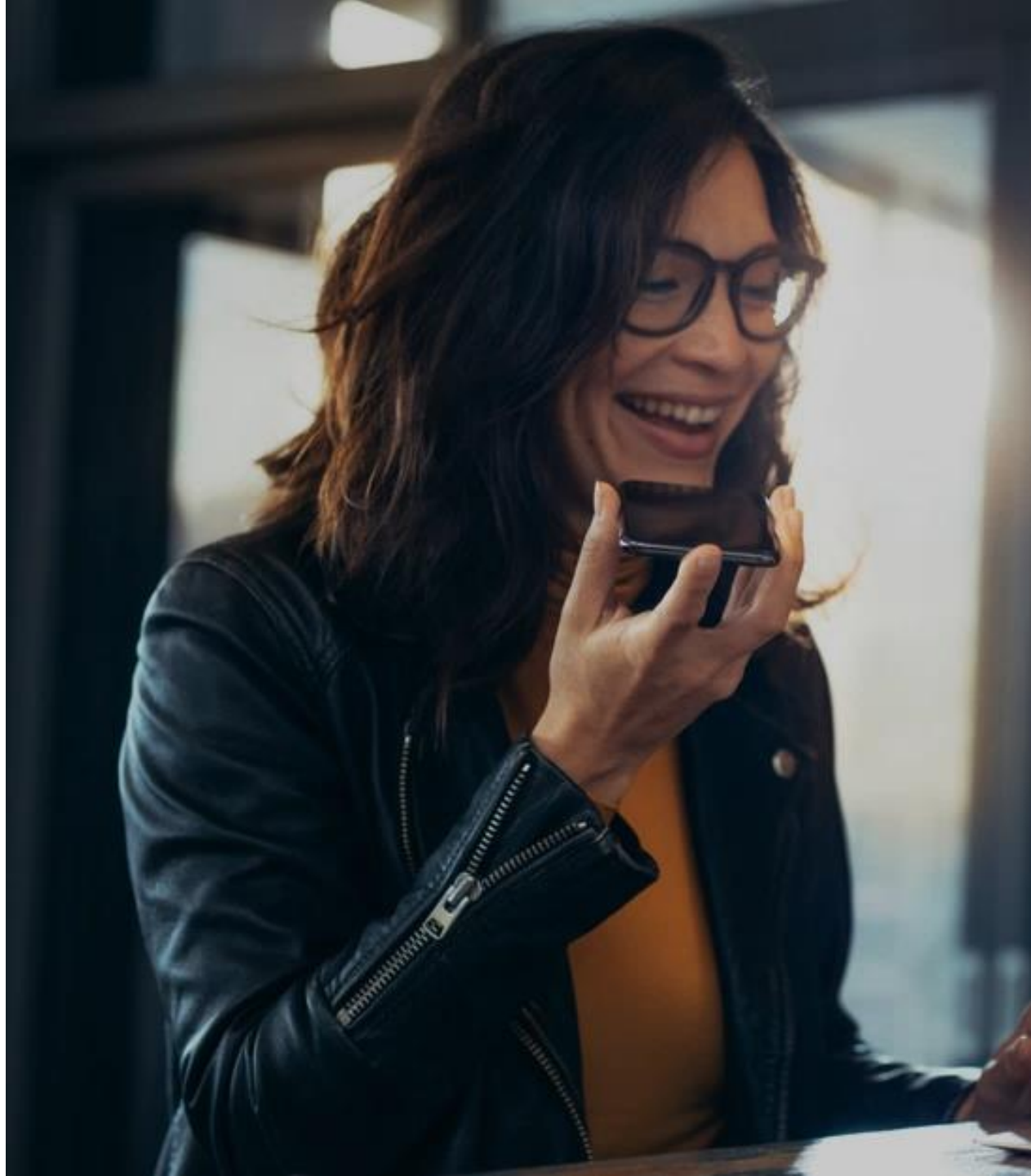
Microsoft 365 Business Premium

Your path to increasing profitability

- Meet customer needs for increased security
- Manage with ease with Lighthouse/RMM
- Standardize on one solution across the SMB stack
- Create ongoing revenue with managed services

"Since basing a managed service offering on Microsoft 365 Business Premium, **profitability per employee has shot up by 250 percent.**"

-- Martin Liljenberg: CTO and Cofounder, WeSafe



Microsoft 365 Business Premium

Comprehensive security and productivity solution, designed for businesses with 1-300 employees

Collaborate in real time

Enable secure access and protect identity

Defend against cyberthreats and data loss

Easily secure and manage devices

"Having a best-in-class platform like Microsoft 365 addresses multiple challenges in one go, something that was missing earlier. Today, I can say that we have all the tools in place for significantly improving business productivity and collaboration while providing a much higher level of security."

—Praveen Vashishta, Chairman and CEO at Howden India

Today's sophisticated attacks call for Layered security

Microsoft 365 Business Premium

Identity Security

User

Azure AD features like MFA

Self Service Password Reset

Conditional Access

Dynamic Groups

Device Security

Device

Full Centralized Management of Mobile and Laptops with Intune

Remote wipe of data of lost & stolen devices

BitLocker Encryption

Enforce Strong Pin requirements along with Wi-Fi, VPN profiles

Microsoft Defender for Business

Application Security

Application

Restrict copy/paste/save corp data to personal apps using Intune App Protection Policies

Defender for Office 365 for protection against malware and zero day attacks

Data Loss Prevention to monitor sensitive data from being transmitted

Email restrictions like "Do Not Forward" or "Encrypt Email"

Document Security

Document

Azure Information Protection protects, classifies Documents for secure sharing including in Teams

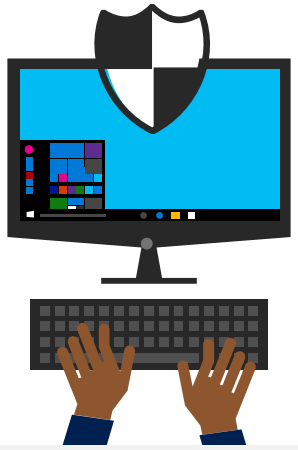
Revoke access to Documents

Track Sensitive documents

Microsoft

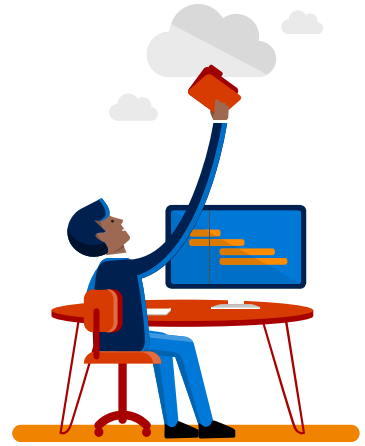
Enable secure access from anywhere and protect identity

Start with securing identity and access



Protect against lost and stolen passwords

Secure access to work apps



Enable remote desktop access

Enable remote desktop access with Windows Virtual Desktop

Deliver the only multi-session Windows 10 experience that's highly scalable and stays up to date

Enable optimizations for Office

Migrate RDS desktops and apps and simplify licensing and reduce costs

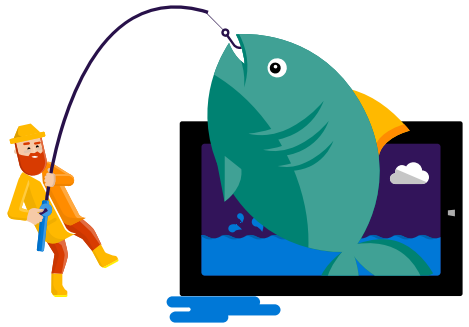
Deploy and scale in minutes. Manage with unified admin interface in Azure Portal

Support any end-user device platform including Windows, Android, Mac, iOS, and HTML 5

Microsoft

Protect against cyber threats and data loss

Defend against cyberthreats and safeguard business data



Protect users against cyberthreats like phishing

Safeguard confidential business data

Get visibility into cloud app use

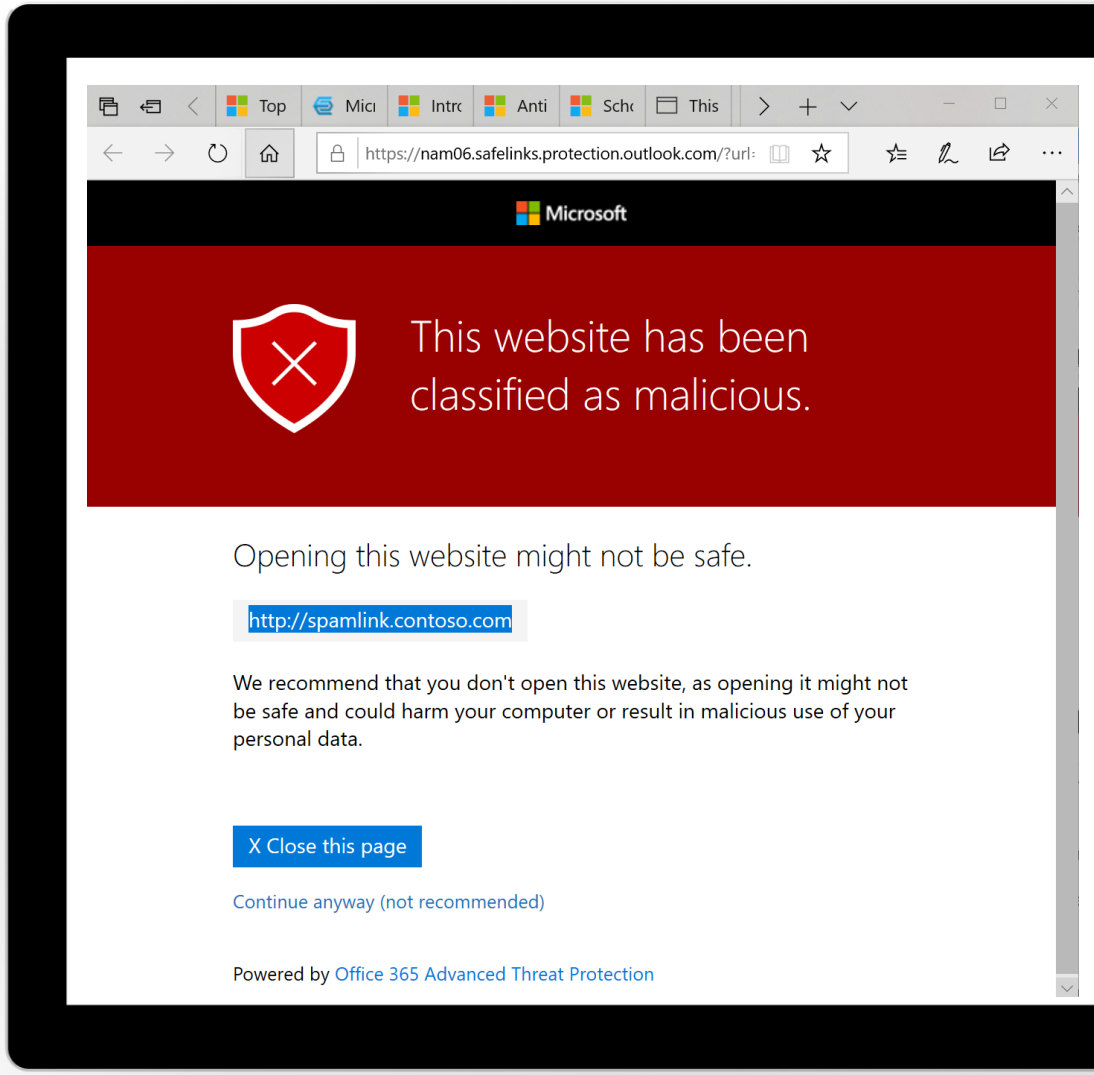
Protect against cyberthreats with Microsoft Defender for Office 365

Protect against malicious links in email or Teams with real time scanning using Microsoft Defender for Office 365 Safe Links

Get AI-powered malware scanning for attachments in email and shared document links in Teams and OneDrive with Safe Attachments

Defend against impersonation and spoofing with anti-phishing

Get better protection on Windows devices against suspicious processes like ransomware with Microsoft Defender AV

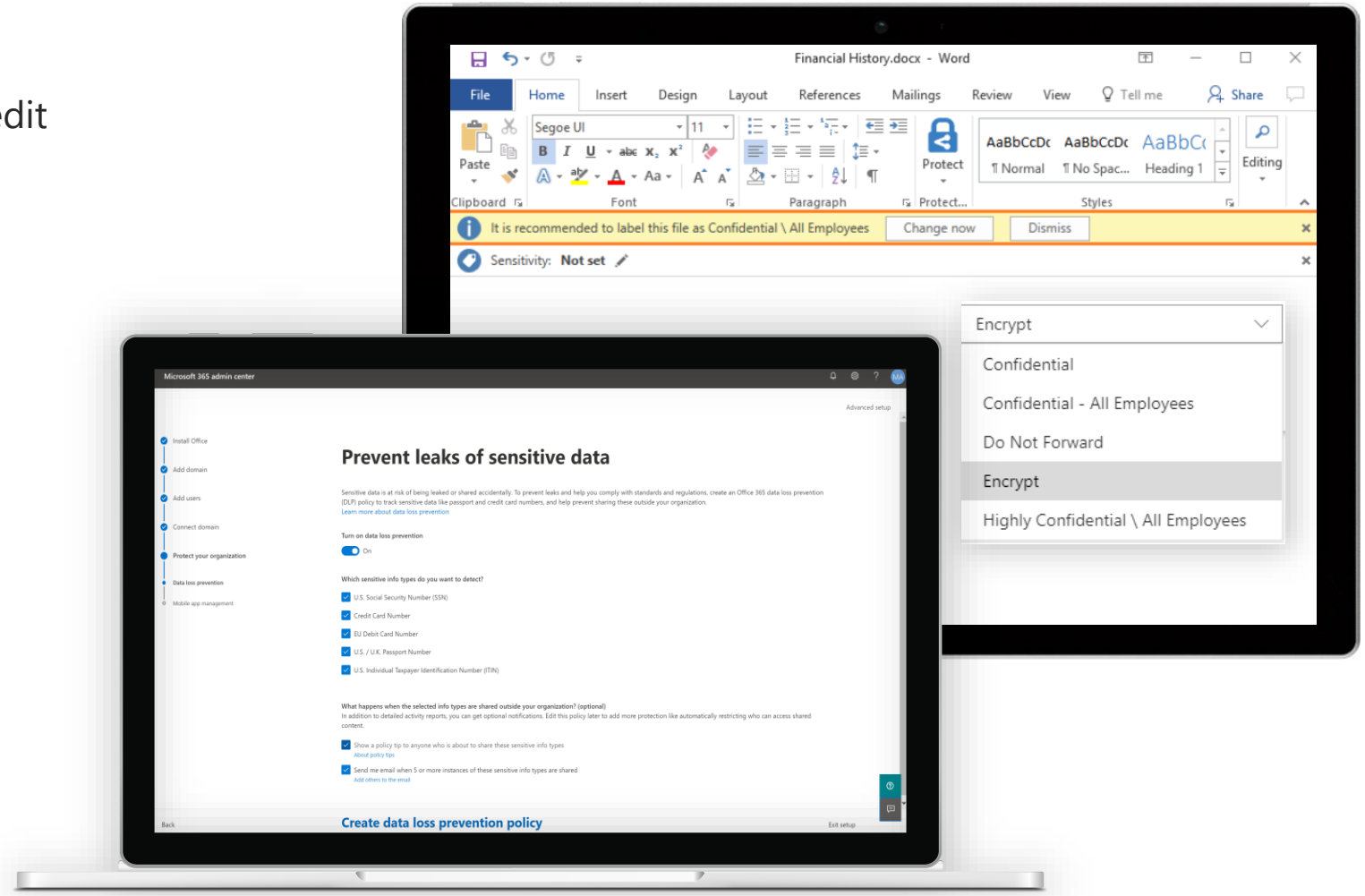


Safeguard business data with DLP and Azure Information Protection

Prevent sharing of sensitive information like credit card numbers using preconfigured DLP policy templates for HIPAA, PCI_DSS, SSN etc

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

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



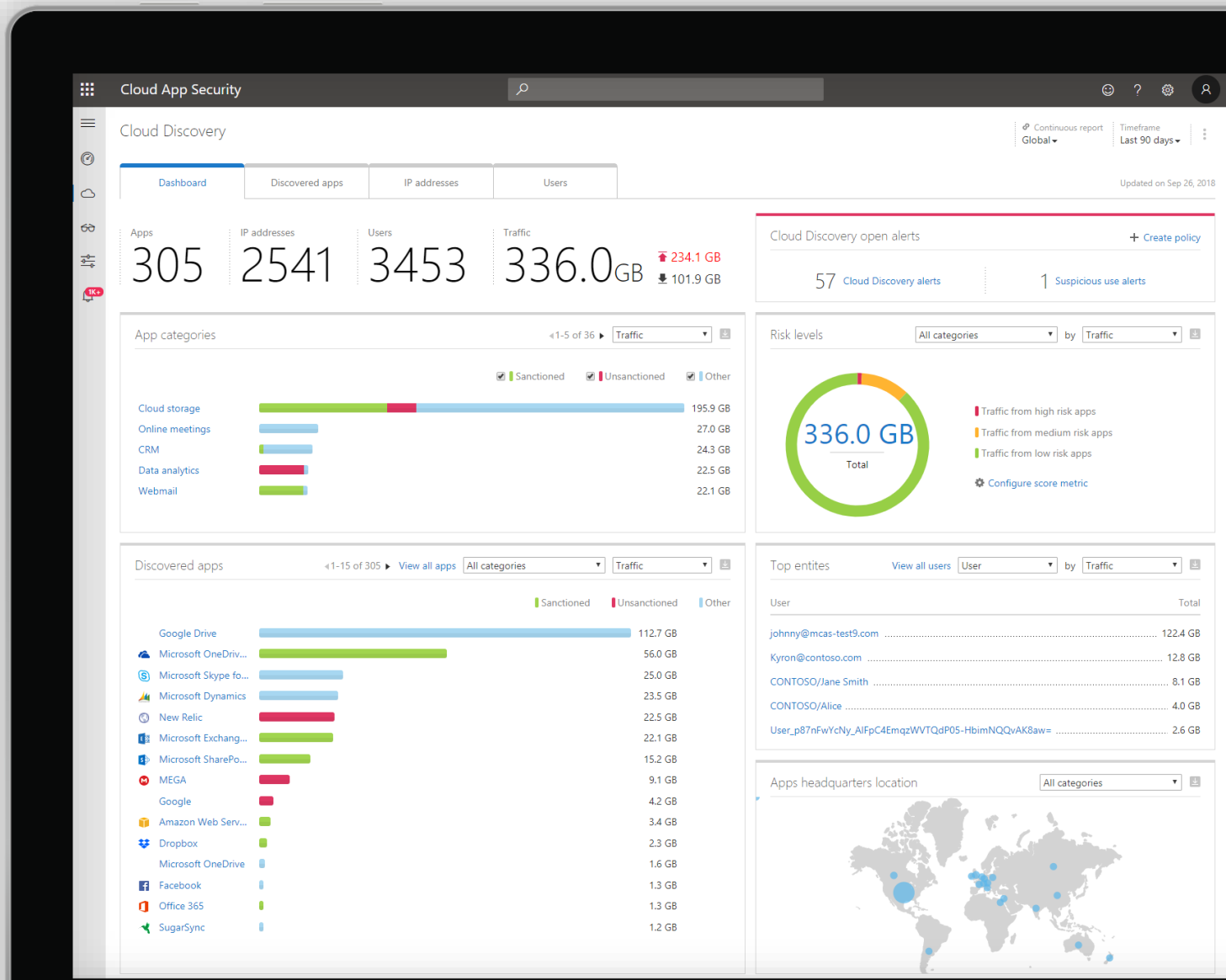
Get visibility into cloud app use with Cloud App Discovery

Discover cloud app usage to understand shadow IT risk

Understand the security of your cloud apps with risk assessment for 16,000+ cloud apps

Understand usage patterns and identify high risk users. Export data for additional analysis

Prioritize applications to bring under IT control and integrate applications to enable single sign-on and user management



Check your Secure Score

The problem:

You want to improve your customer's security, but don't know where to start

The solution:

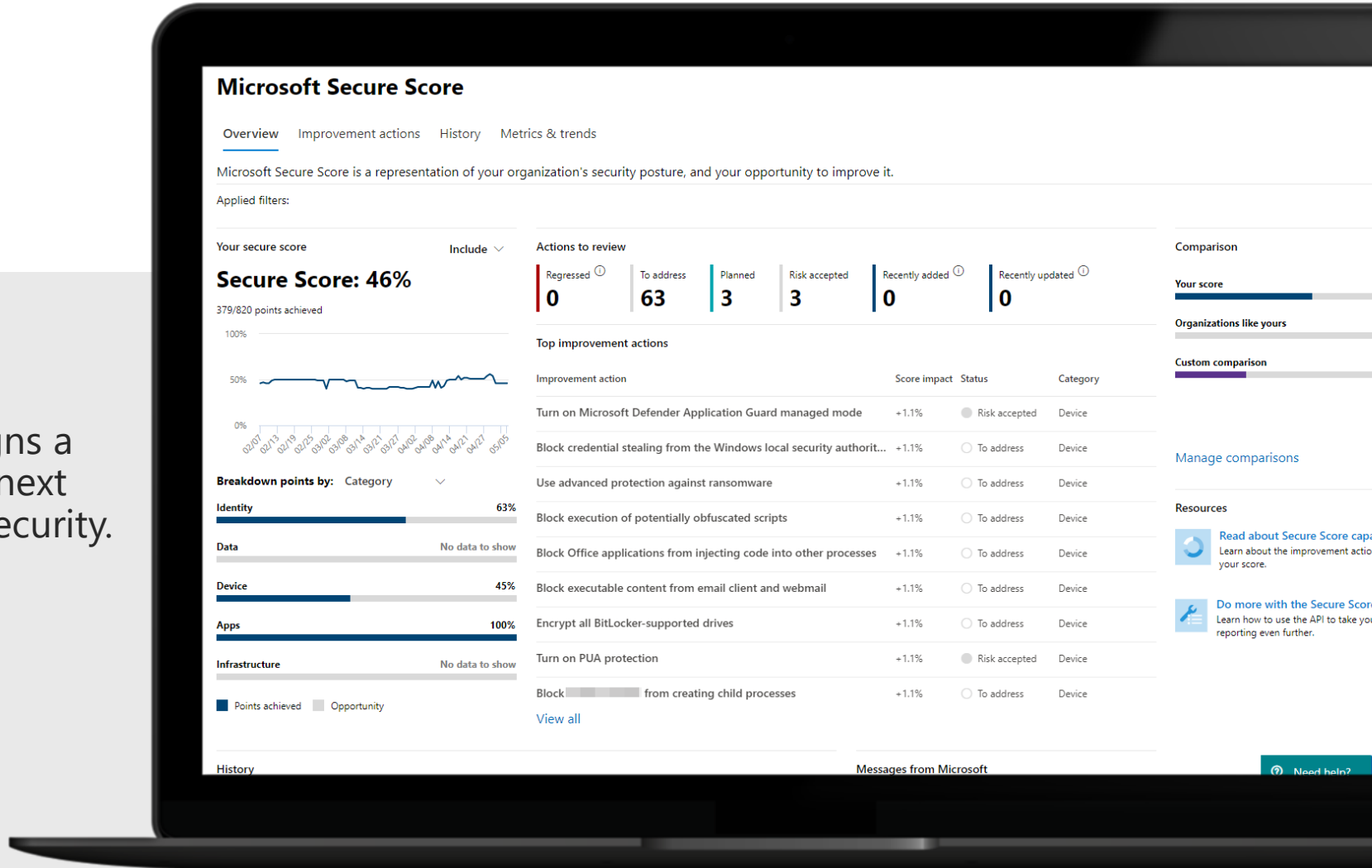
Check Microsoft Secure Score

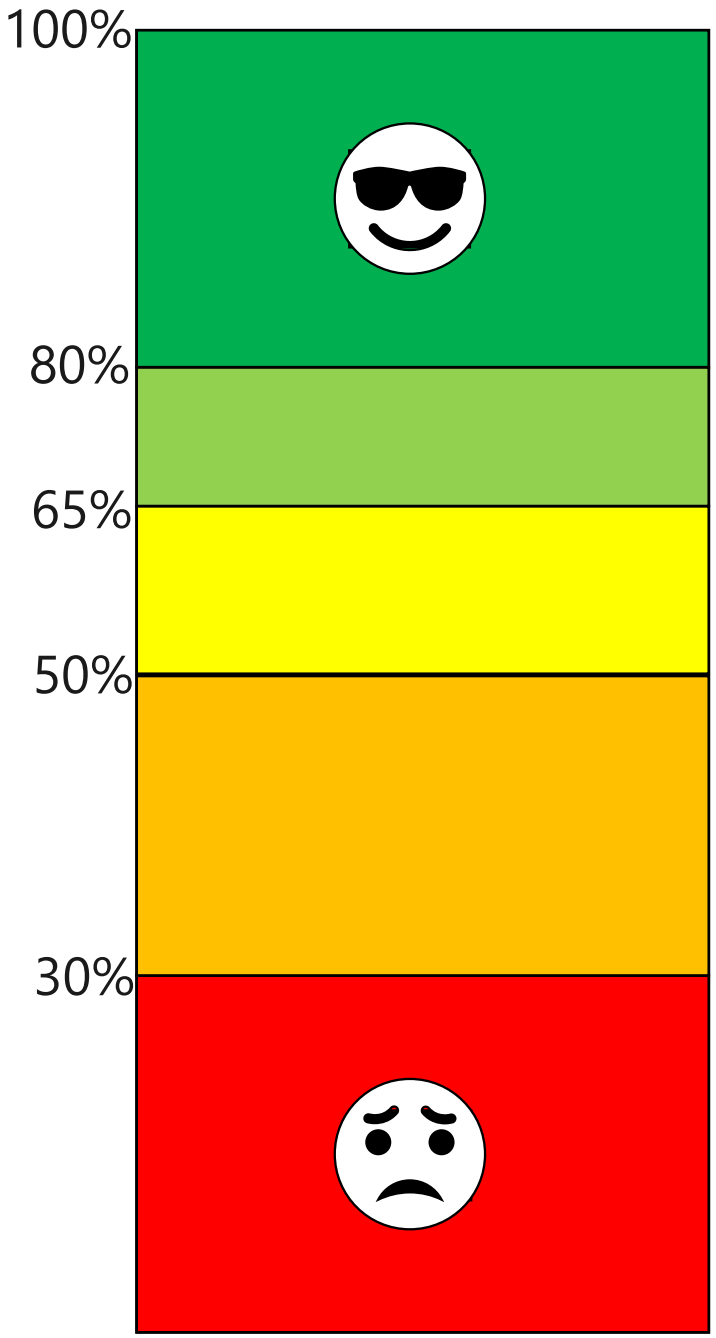
What it is:

Microsoft Secure Score analyzes your Microsoft 365 overall security and assigns a score. Secure Score also recommends next steps to consider in order to improve security.

How to access:

http://securescore.microsoft.com





Your secure score

Include

Planned score
Show projected score when planned actions are completed

Current license score
Show score that can be achieved with your current Microsoft license

Achievable score
Show score that can be achieved with your Microsoft licenses and current risk acceptance

50%

0%

02/04 02/09 02/14 02/19 02/24 03/01 03/06 03/11 03/16 03/21 03/26 04/01 04/10 04/15 04/20 04/25 05/03

Breakdown points by: Category

Identity 10.71%

Apps 25%

Points achieved | Opportunity | Achievable score

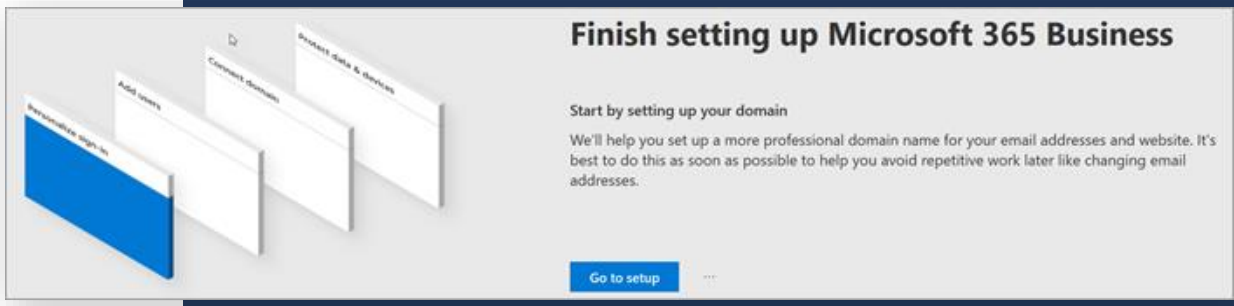
Microsoft

Exercise: Complete the setup wizard & check O365 SecureScore

Complete Setup Wizard

To complete the M365 BP setup wizard:

1. Log into your hands-on lab (HOL) and retrieve admin credentials.
2. Sign in to Microsoft 365 admin center by using your global admin credentials.
3. Choose Go to setup to start the wizard.
4. Skip the option to Install your Office apps
5. Add your m365master.com lab domain
6. Demo users are already added; however, add yourself to the tenant
7. On the Protect data in Office for mobile page, leave mobile app management on, expand the settings and review them, and then select Create mobile app management policy.



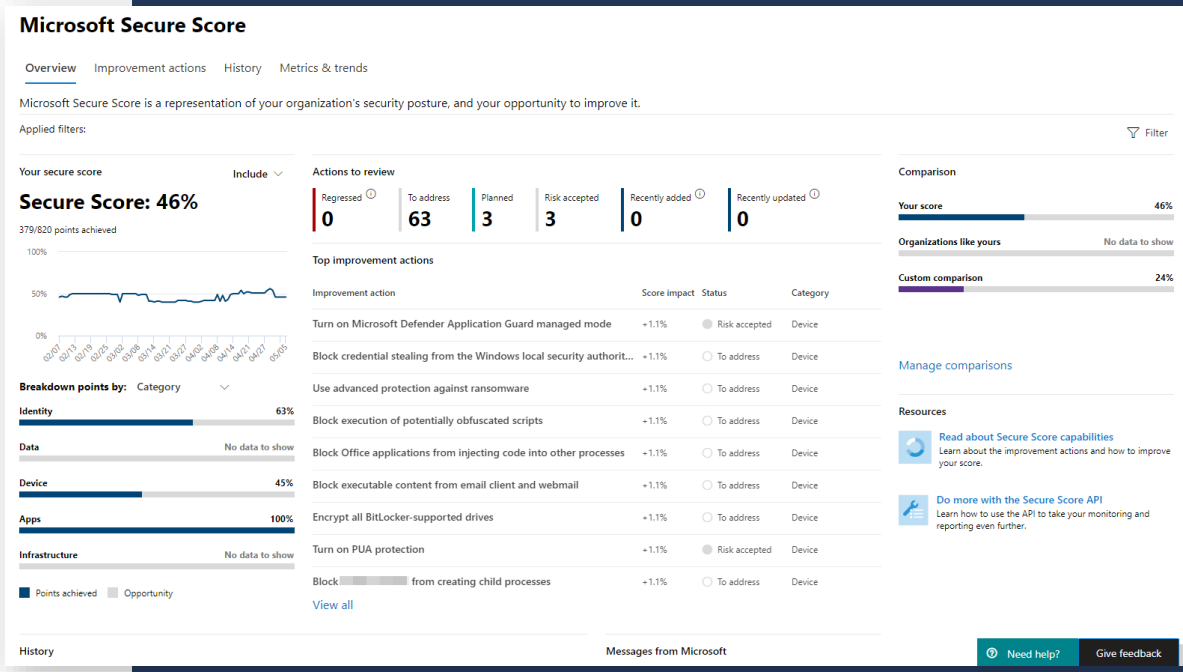
To learn more, see Set up Microsoft 365 Business Premium in the setup wizard

Check Secure Score

To check Secure Score:

1. In the Microsoft Admin Center, choose **Security** in the left-hand navigation under **Admin Centers.** This will open the Microsoft 365 Security Center in a new tab
2. Click on **Secure Score** in left hand naviation.
3. Review Secure Score
4. Review Improvement Actions (We'll do these later)
    1. Enable MFA for administrative roles
    2. Ensure all users can complete multi-factor authentication for secure access
5. Review History

To learn more, see Microsoft Secure Score



M365 Security at a glance

Set up tenant

Configure identity protection

Configure endpoint protection

Configure email protection

Corporate data containment

Advanced Security

Device management & security

Secure remote access

Checklist: https://aka.ms/smbchecklist

How to use the checklist

Review the guidance

Download the checklist

Determine your customer's risk scenario

- Typical customer
- Higher risk / lower tolerance for risk

Checklist: https://aka.ms/smbchecklist

Microsoft

Securing identities with Azure AD P1

How can I secure identities with Azure AD P1?

Name: Bob D

Role: Partner Resource

Company: Partner

Azure AD P1

Secure access for a connected world.

Azure Active Directory

Protect your users, apps, workloads, and devices.

- User directory
- Single sign-on to any app
- User self service
- Multifactor and passwordless authentication
- Conditional Access and Identity Protection
- Hybrid identity management
- Core identity governance
- External and frontline identities

What Is The Issue Enabling MFA?

A new report published by CoreView has revealed:

- Majority of Microsoft 365 admins have not enabled multi-factor authentication to protect their accounts from unauthorized remote access and are failing to implement other basic security practices.

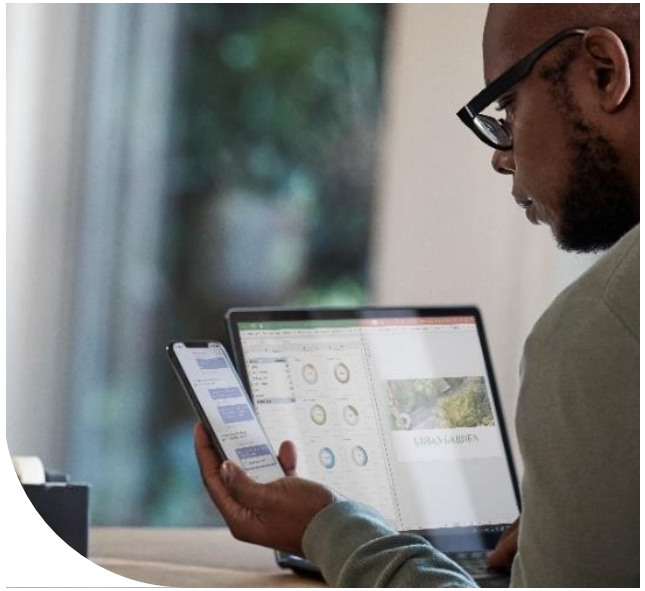
- 78% of Microsoft 365 administrators have not activated multi-factor authentication and 97% of Microsoft 365 users are not using MFA.

- 57% Microsoft 365 administrators are given excessive control and have access to a treasure trove of sensitive information

https://www.coreview.com/resources/whitepaper/microsoft-365-app-security-governance-shadow-it-report/

Enforce Multi-factor authentication

Verify user identities with strong authentication



We support a **broad range of multi-factor authentication options**

Including passwordless technology

- Microsoft Authenticator
- Windows Hello
- FIDO2 Security key
- Biometrics
- Push Notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, Voice

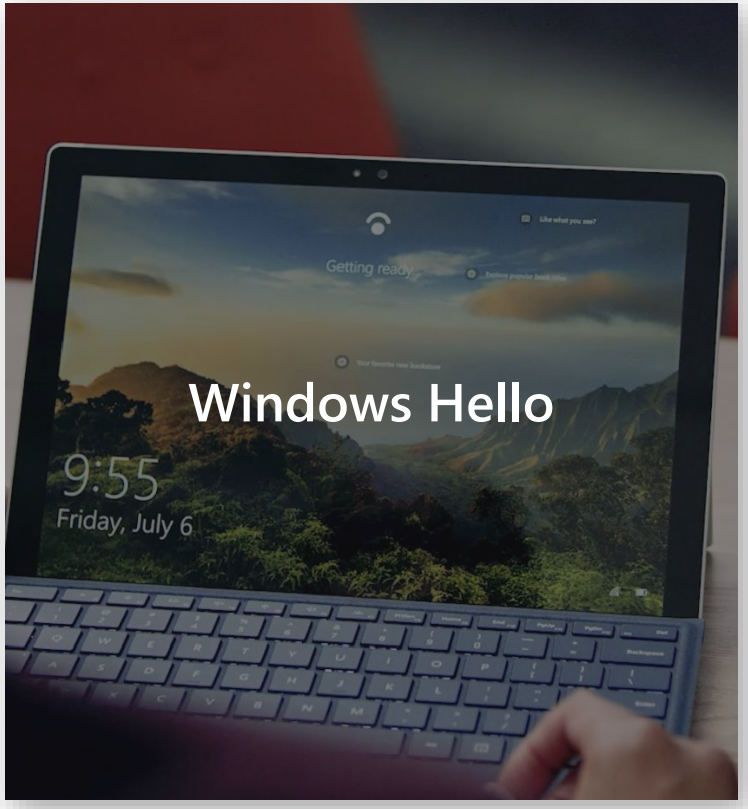
Multi-factor authentication **prevents 99.9% of identity attacks**[1]

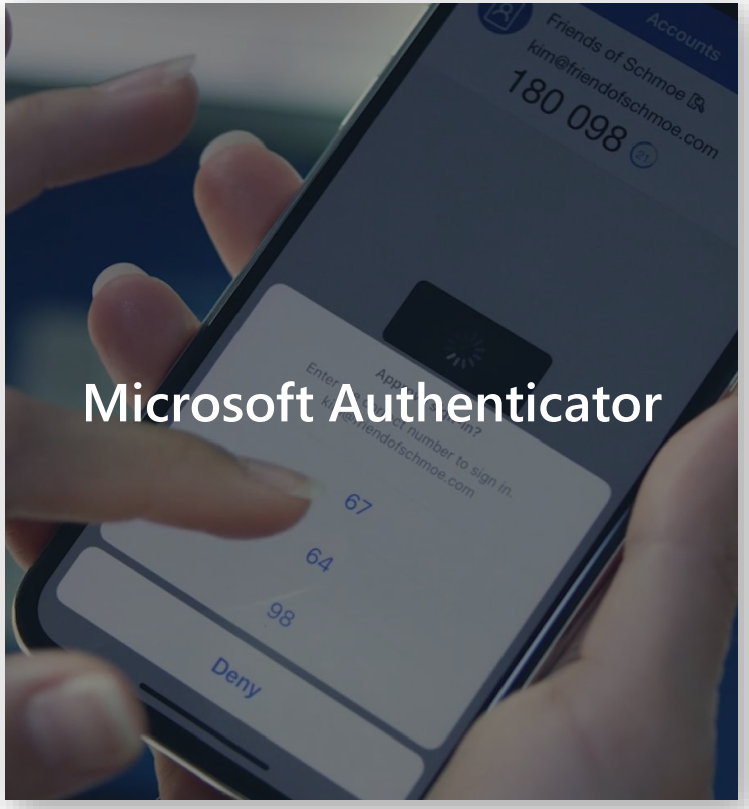
1. "Your Password Doesn't Matter" July 2019, Microsoft Tech Community Research Article

MFA and Password-less

Secure authentication

Getting to a world without passwords





Secure authentication

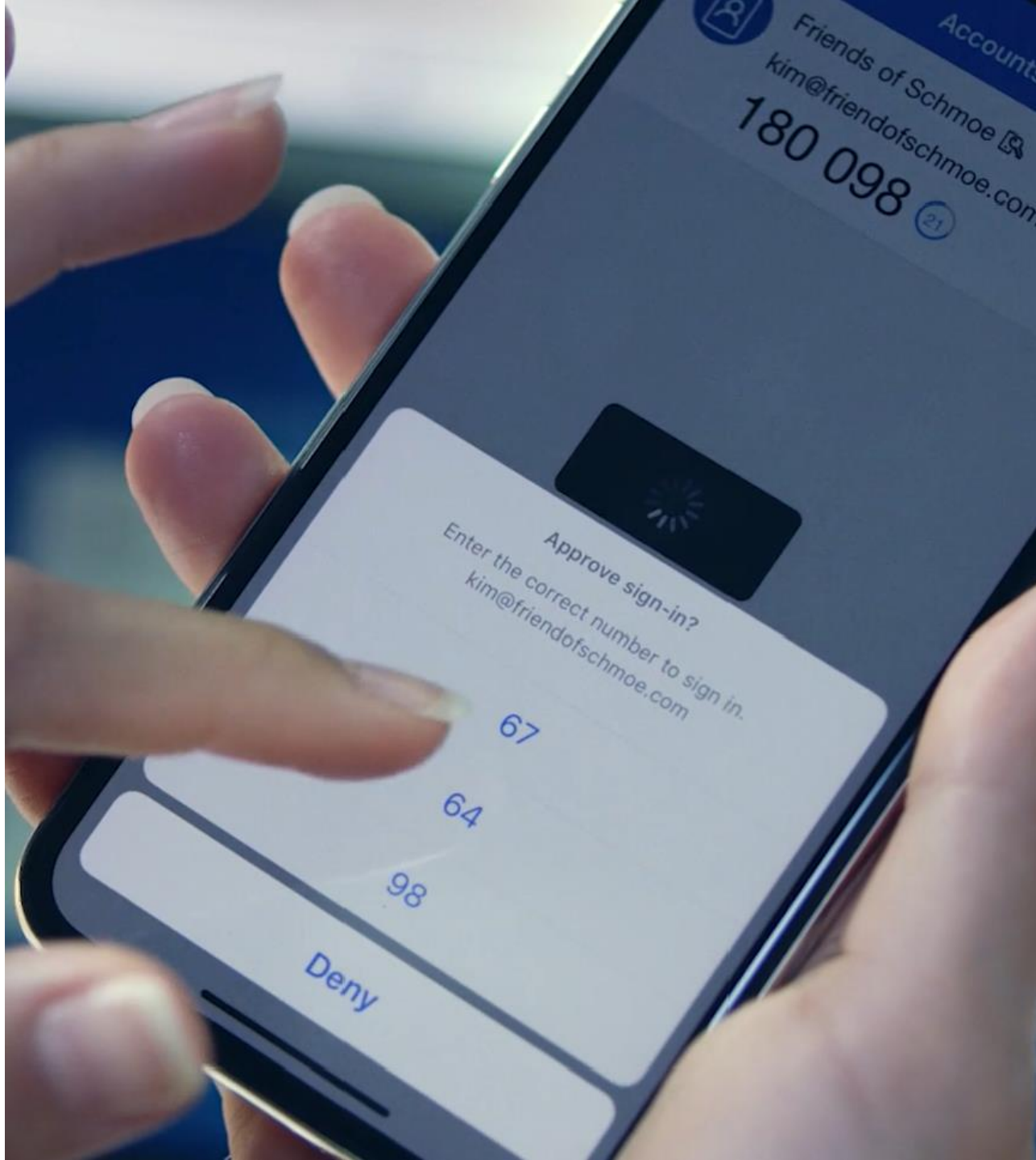
Microsoft Authenticator

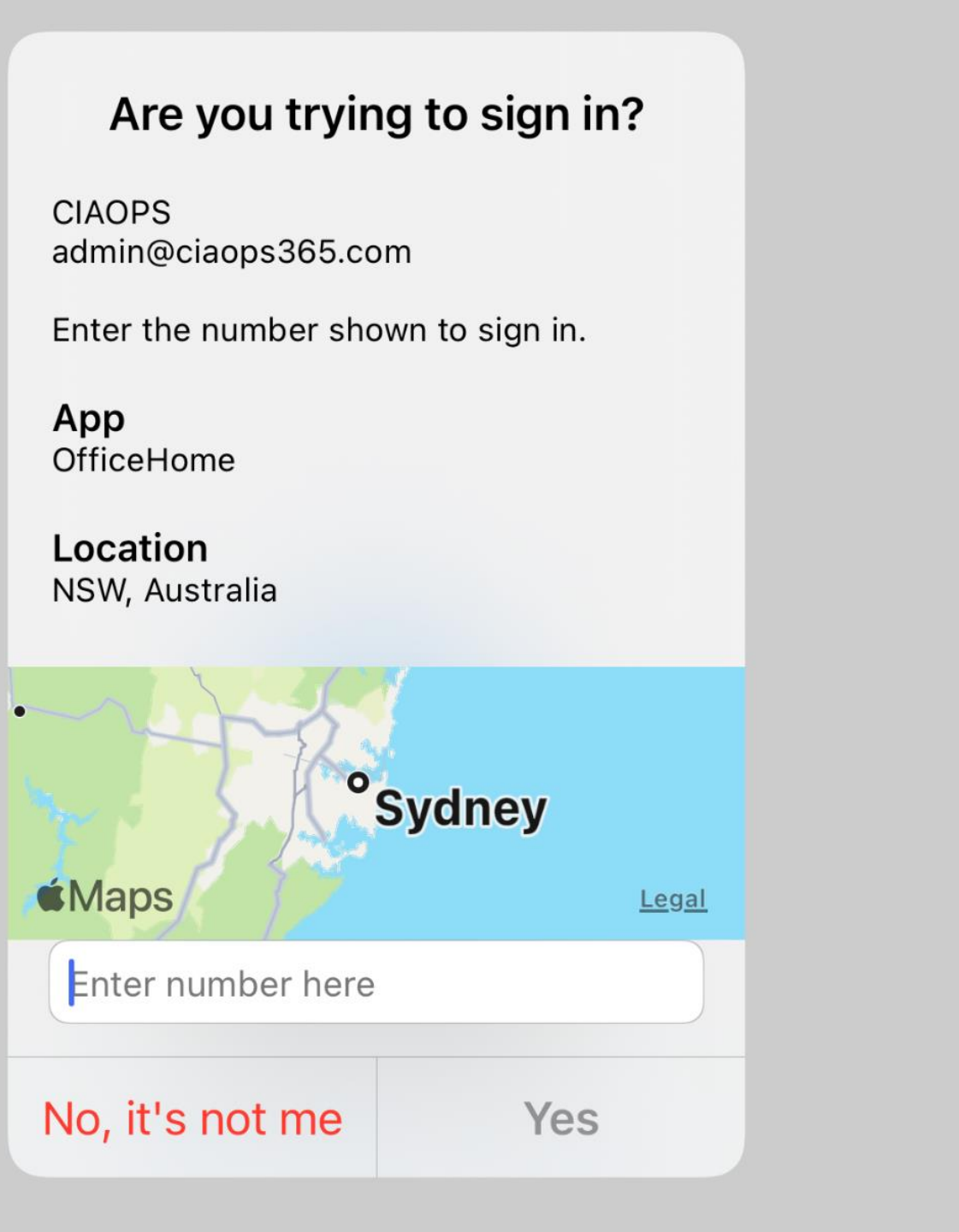
MFA for enterprise and consumer accounts and applications

Device registration (workplace join)

Single sign-on to native mobile apps

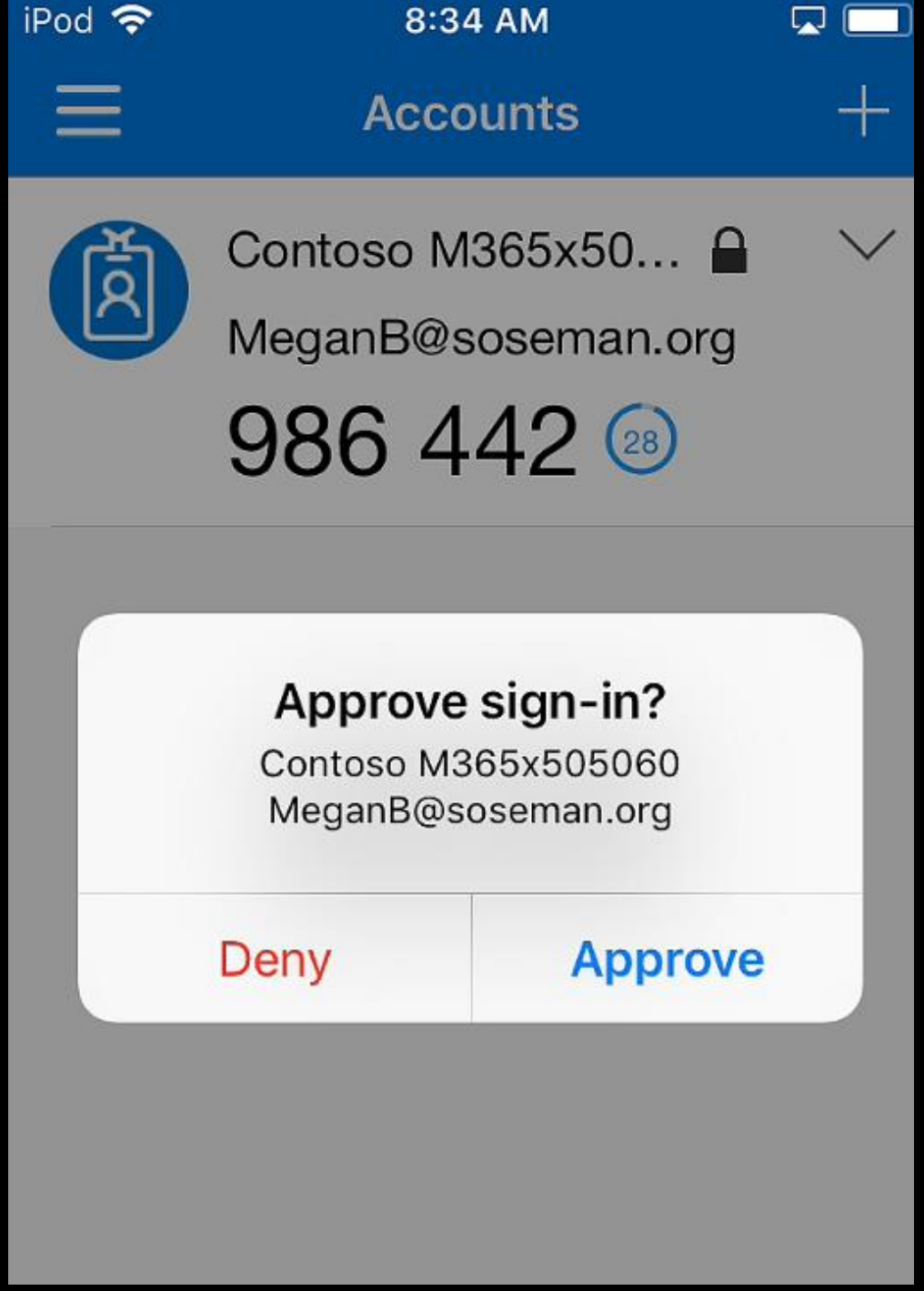
Certificate-based SSO

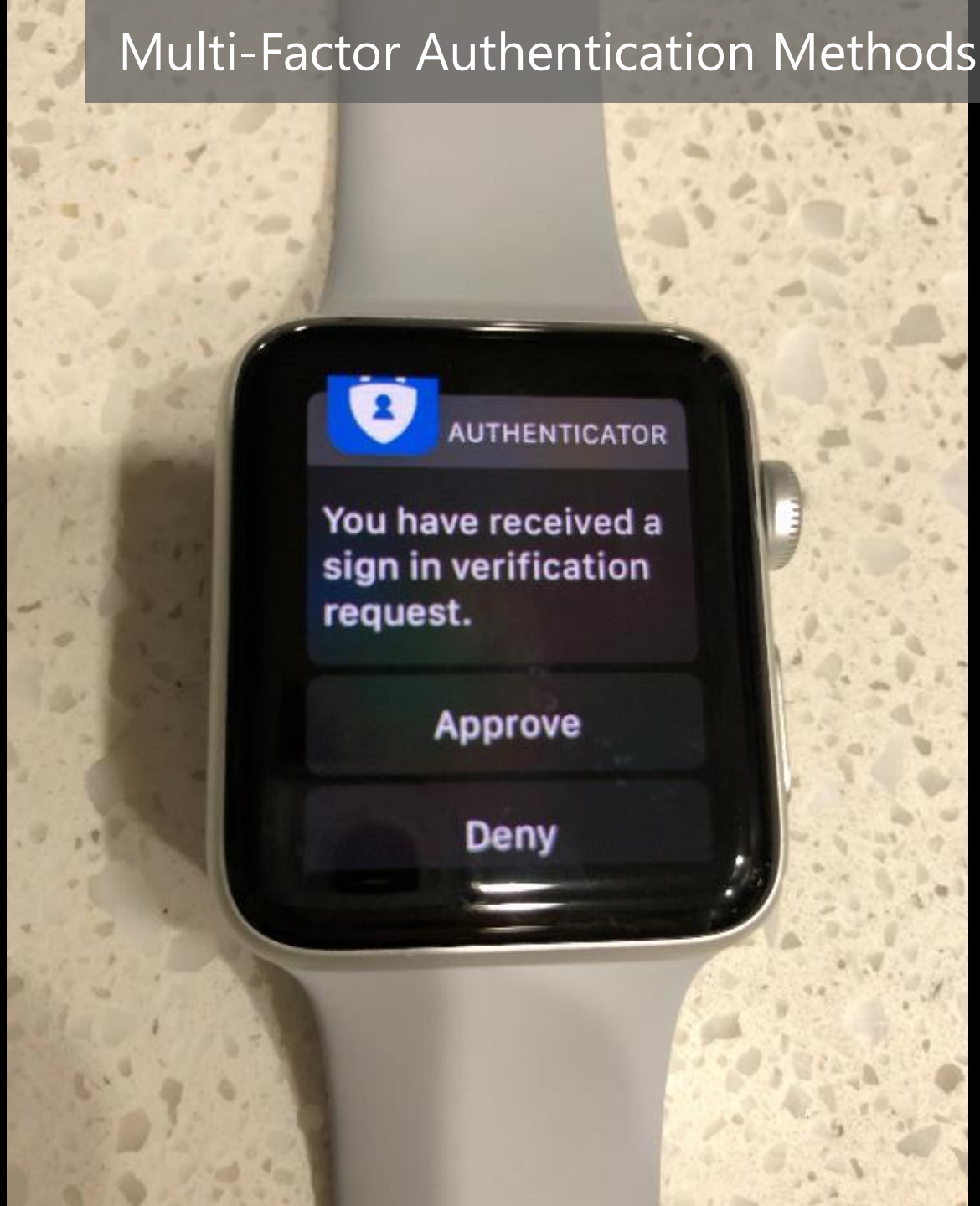




https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context

Multi-Factor Authentication Methods





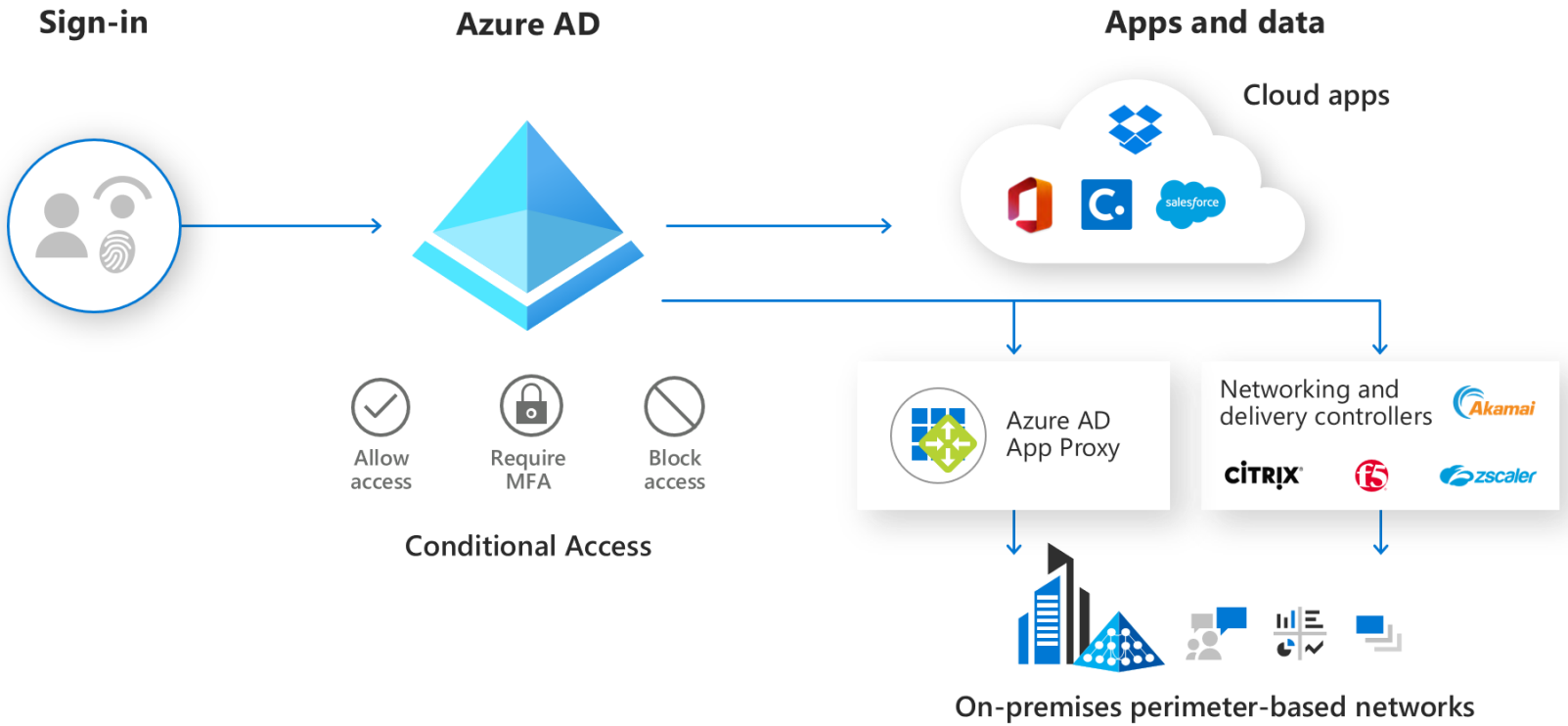
Secure access to work apps – with Azure Active Directory

Azure AD Premium P1 is now included with Microsoft 365 Business Premium

Enable your employees to remotely access on-premises apps without opening broad access to your network with App Proxy[1]

Control “where, when and who” connects to Office apps with Conditional Access

Automatically add/remove users to security groups and reduce IT overhead with Dynamic Groups



Set up identity security with MFA

The problem:

Passwords are vulnerable [1]

- 90% of passwords can be cracked in less than six hours [1]
- Two-thirds of people use the same password everywhere [1]
- Criminals are getting more effective in stealing passwords through phishing and social engineering

The solution:

Multi-factor authentication (MFA)

MFA is enabled by default any Microsoft 365 customer using security defaults

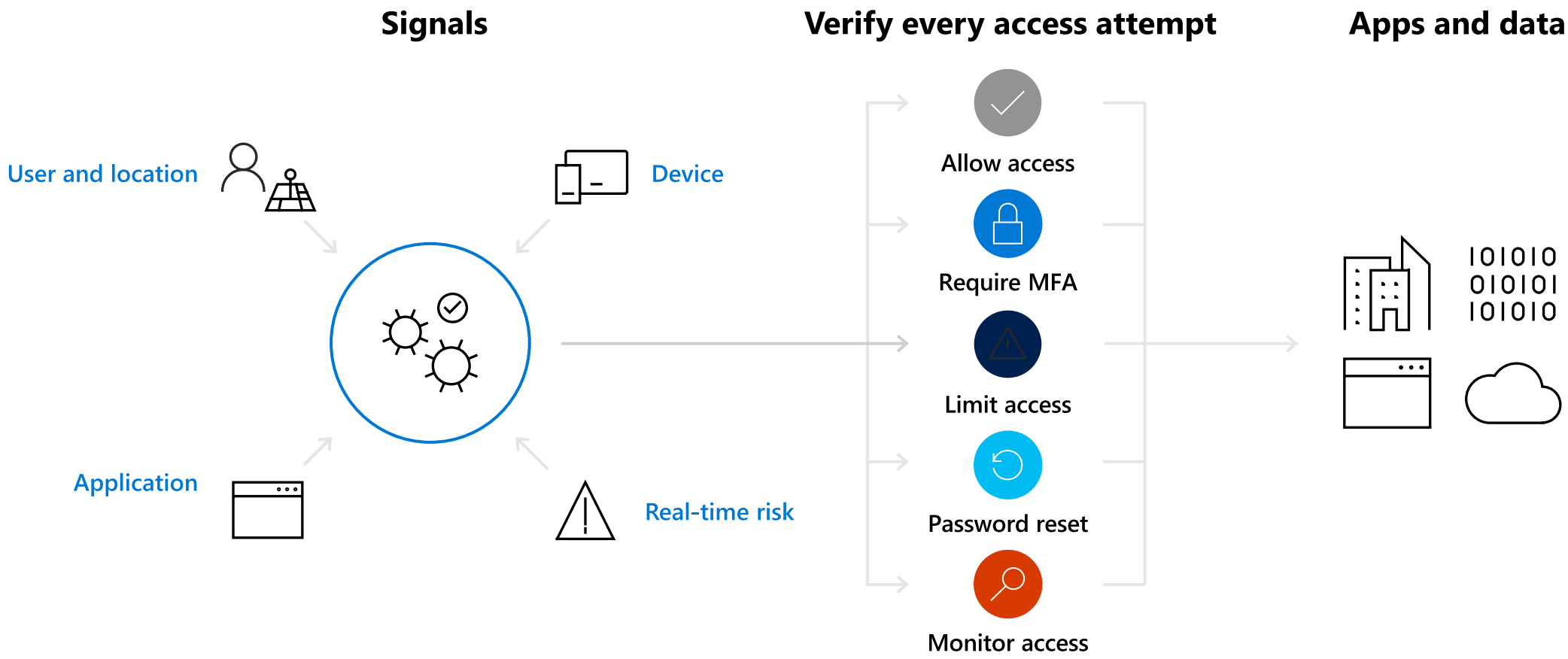
Partners **should** enable MFA for Microsoft 365 Business Premium customers by using conditional access policies

Partners **should** use passwordless MFA authentication methods when possible

[1] https://secureswissdata.com/two-factor-authentication-importance/

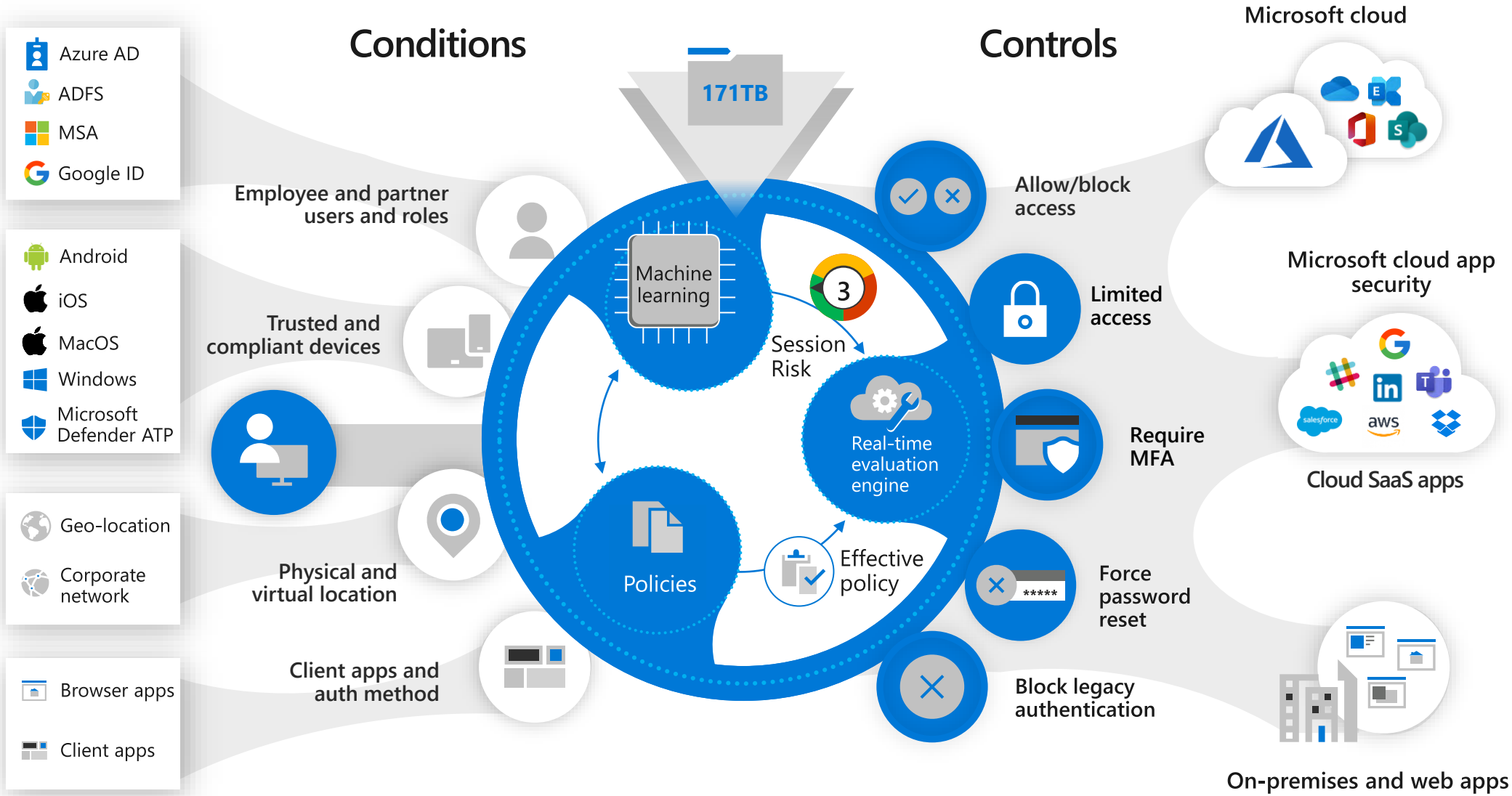
Protect resources with Conditional Access

Configure adaptive access policies based on context and risk



Conditional access and identity protection

Real-time risk-based access control



Microsoft

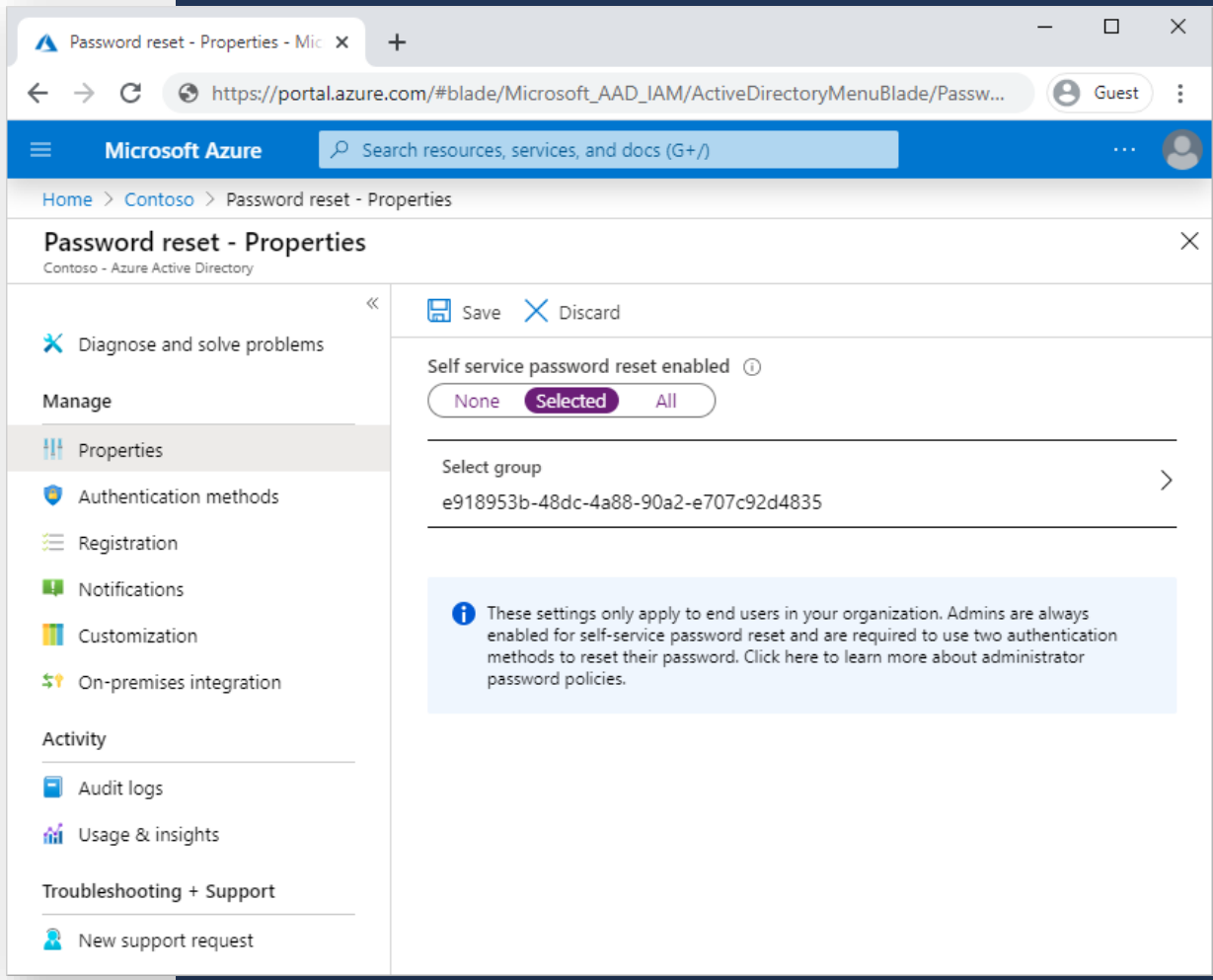
Exercise: Enable MFA with conditional access & self service password reset

Configure Azure AD

Enable Self Service Password Reset:

1. Sign in to the Azure portal using an account with global administrator permissions.
2. Search for and select **Azure Active Directory**, then choose **Password reset** from the menu on the left-hand side.
3. From the Properties page, under the option Self service password reset enabled, choose **All**
4. Select **Save**.

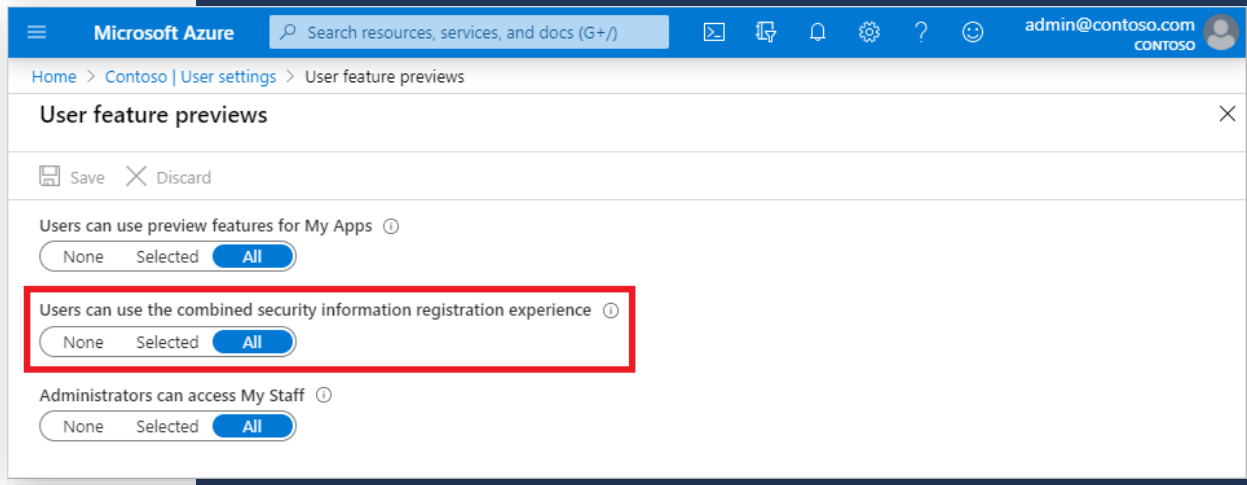
To learn more, see [Tutorial: Enable users to unlock their account or reset passwords using Azure Active Directory self-service password reset]



Configure Azure AD

Enable combined security information registration:

1. In the Microsoft Admin Center, choose **Azure Active Directory** in the left-hand navigation under **Admin Centers.** This will open the Azure Active Directory admin center in a new tab
2. Go to **Azure Active Directory** > **User settings** > **Manage user feature preview settings**.
3. Under Users can use the combined security information registration experience, **All**.
4. Click **Save**.



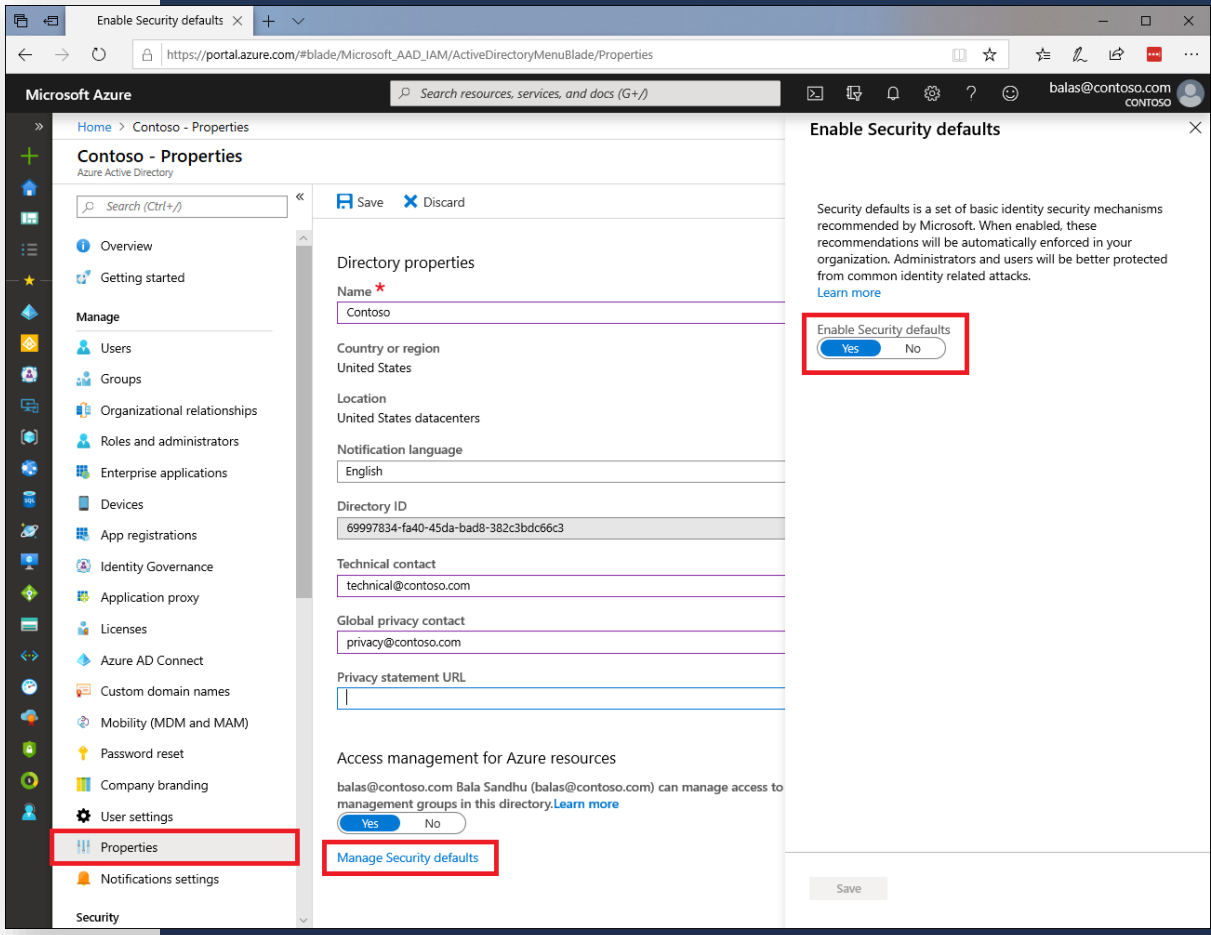
To learn more, see Combined security information registration overview

Configure Azure AD

Enable MFA using Security Defaults:

1. In the Microsoft Admin Center, choose **Azure Active Directory** in the left-hand navigation under **Admin Centers.** This will open the Azure Active Directory admin center in a new tab
2. In the **Azure Active Directory admin center**, click **Azure Active Directory -> Properties** in the left-hand navigation
3. Click **Manage Security Defaults** at the bottom of the Properties pane
4. Select **Yes** under Enable Security Defaults and click **Save**.

To learn more, see What are security defaults?

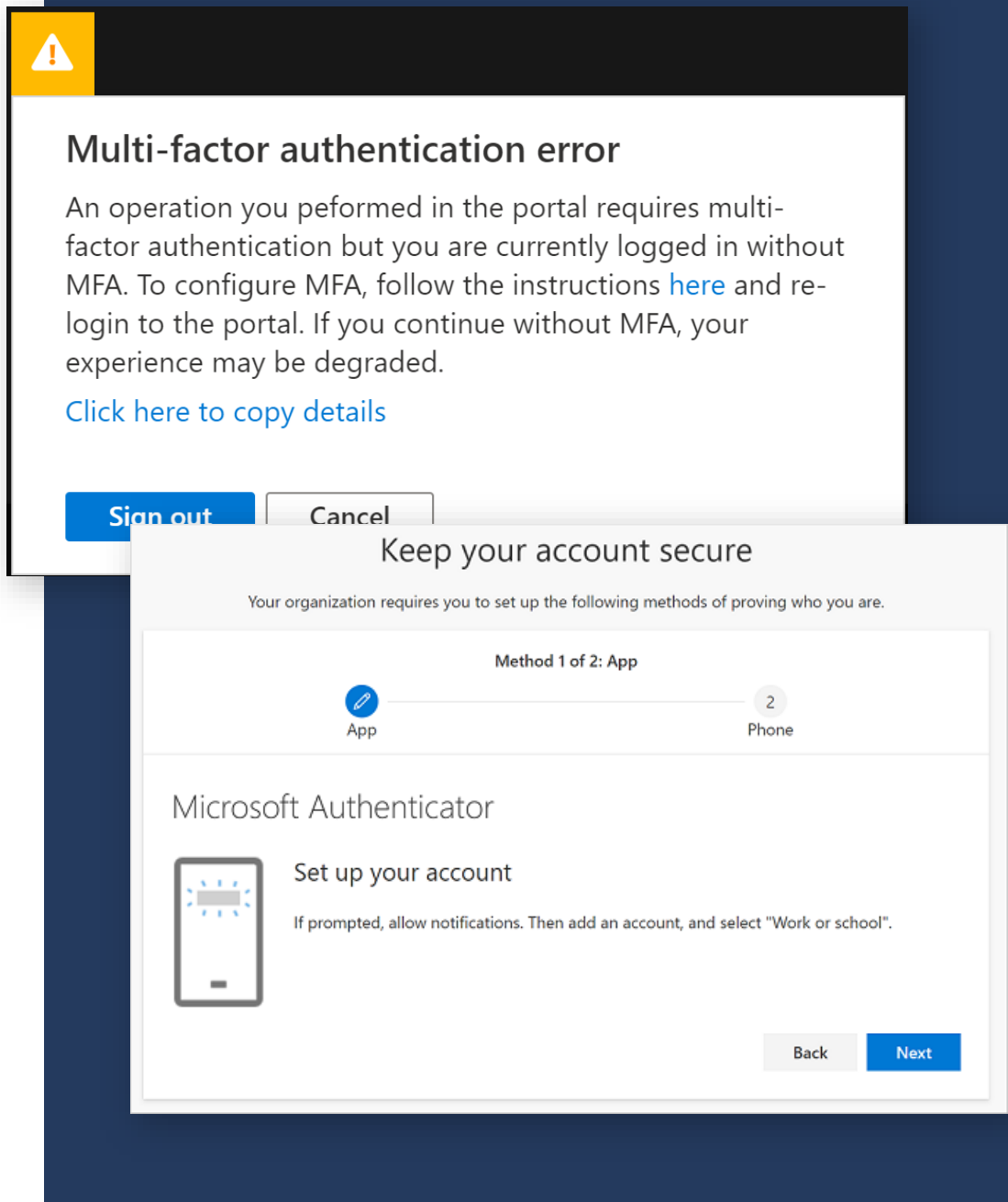


Configure Azure AD

Set up Microsoft Authenticator for your admin account

1. Close all other browser tabs and **sign out** of the Microsoft Admin Center
2. Sign-In the Microsoft Admin Center
3. One the keep your account secure dialog click **Next.**
4. On the Start by getting the app page, select **Download now** to download and install the Microsoft Authenticator app on your mobile device, and then select **Next**.
5. Remain on the Set up your account page while you set up the Microsoft Authenticator app on your mobile device.
6. Open the Microsoft Authenticator app, select to allow notifications (if prompted), select **Add account** from the Customize and control icon on the upper-right, and then select **Work or school account.**
7. Return to the Set up your account page on your computer, and then select **Next**.
8. Scan the provided code with the Microsoft Authenticator app QR code reader, which appeared on your mobile device after you created your work or school account in Step 6.
9. Select **Next** on the Scan the QR code page on your computer.
10. **Approve** the notification in the Microsoft Authenticator app, and then select **Next**.

To learn more, see Set up the Microsoft Authenticator app as your verification method

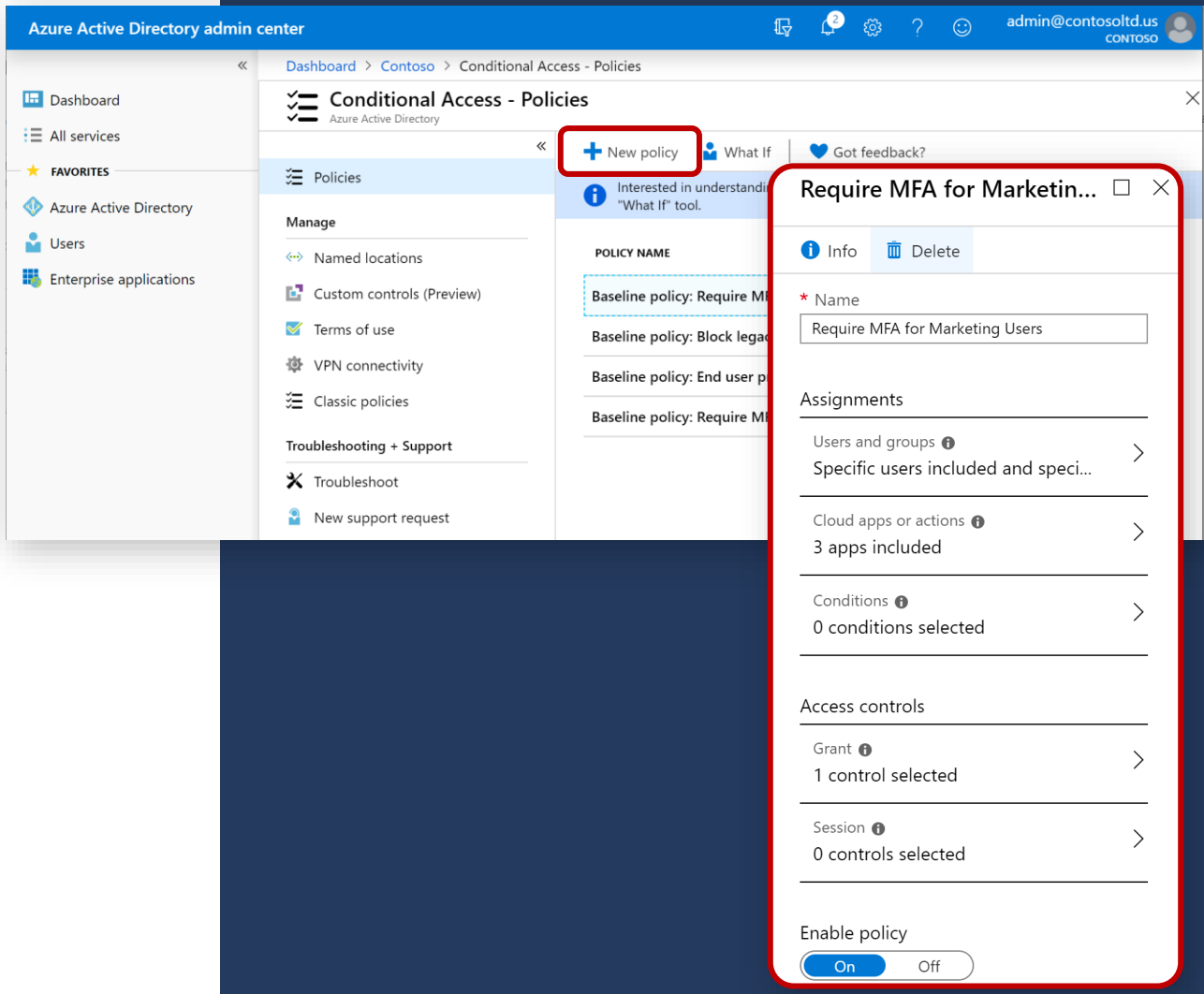


Configure Azure AD

To set up MFA for admins:

1. In the Microsoft Admin Center, choose **Azure Active Directory** in the left-hand navigation under **Admin Centers.** This will open the Azure Active Directory admin center in a new tab
2. In the **Azure Active Directory admin center**, click **Azure Active Directory -> Security -> Conditional Access** in the left-hand navigation
3. Click **+New Policy** and name the policy Require MFA for Admins
4. **Assignments | Directory Roles:** Include the Global Administrators
5. **Assignments | Cloud apps or actions:** All cloud apps
6. **Access Controls | Grant | Require multi-factor authentication:** Checked

To learn more, see Conditional Access: Require MFA for administrators

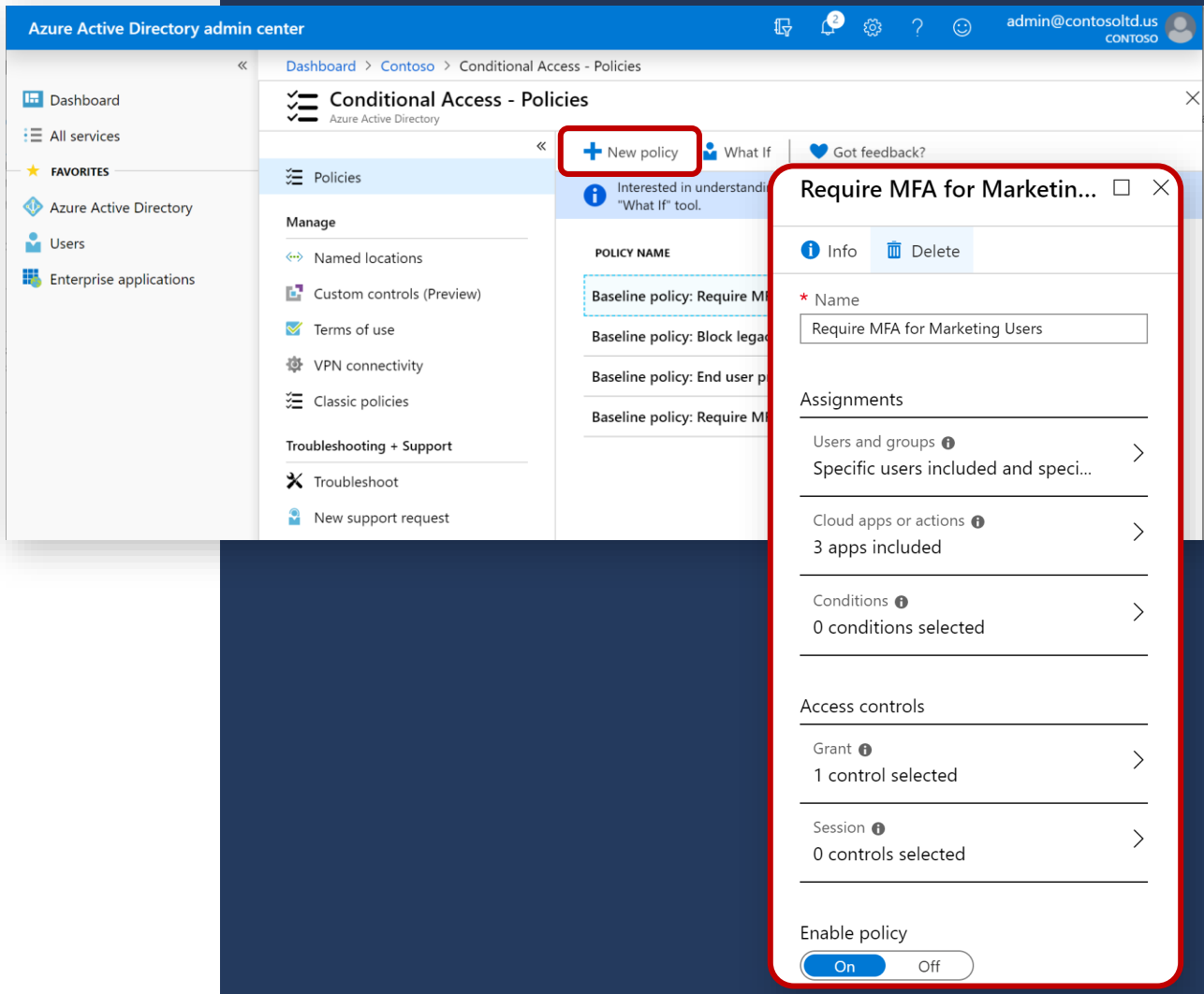


Configure Azure AD

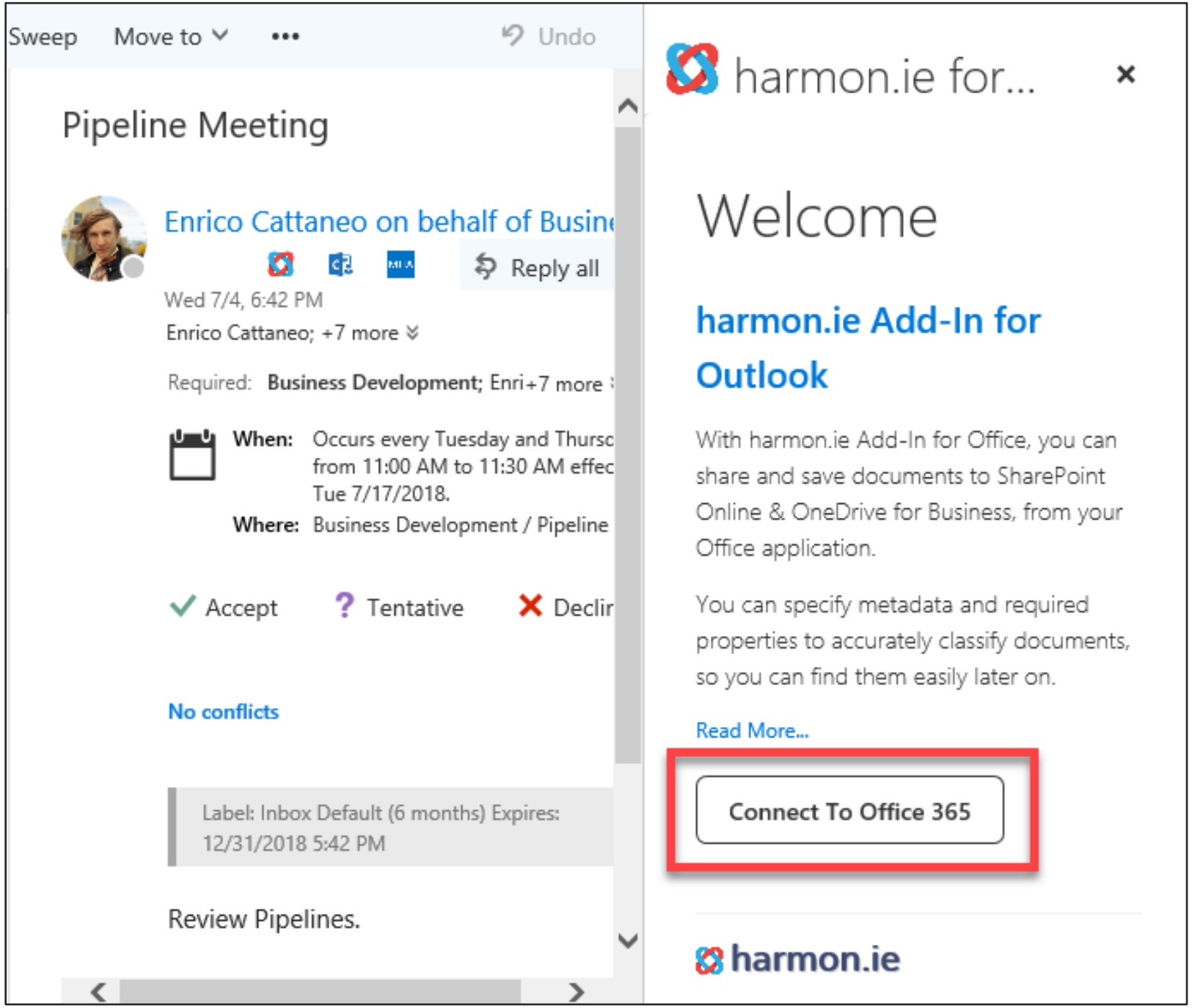
To set up MFA for all users:

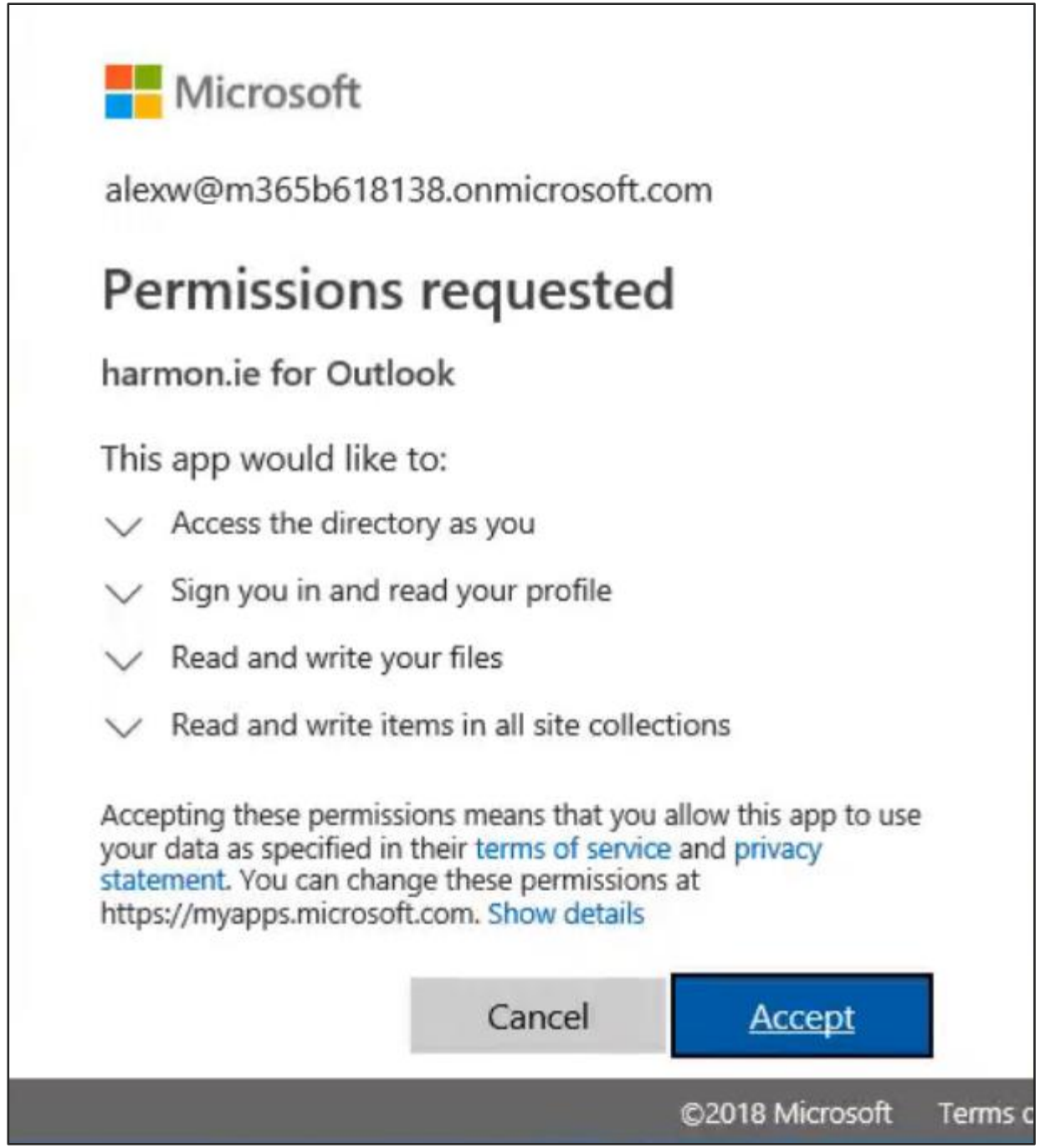
1. In the Microsoft Admin Center, choose **Azure Active Directory** in the left-hand navigation under **Admin Centers.** This will open the Azure Active Directory admin center in a new tab
2. In the **Azure Active Directory admin center**, click **Azure Active Directory -> Security -> Conditional Access** in the left-hand navigation
3. Click **+New Policy** and name the policy Require MFA for Marketing Users
4. **Assignments | Users and Groups:** Include the Marketing group, exclude your admin account
5. **Assignments | Cloud apps or actions:** Office 365 Exchange Online and Office 365 SharePoint Online, and Microsoft Teams
6. **Access Controls | Grant | Require multi-factor authentication:** Checked

To learn more, see Conditional Access: Require MFA for all users

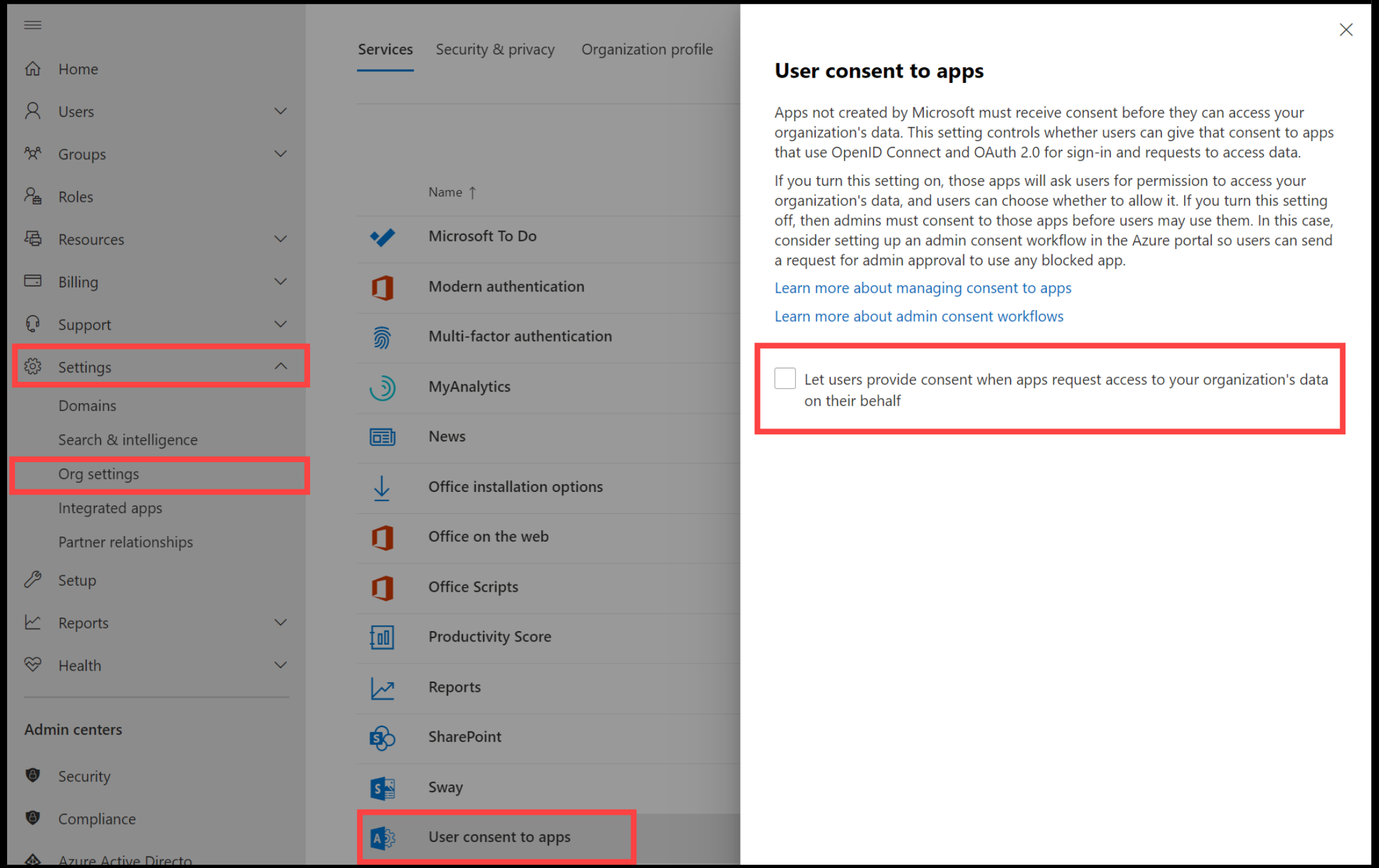


Oauth Apps


Sweep
Move to
Undo
Pipeline Meeting
Enrico Cattaneo on behalf of Busine
Reply all
Wed 7/4, 6:42 PM
Enrico Cattaneo; +7 more
Required: Business Development; Enri+7 more
When: Occurs every Tuesday and Thursc
from 11:00 AM to 11:30 AM effec
Tue 7/17/2018.
Where: Business Development / Pipeline
Accept
Tentative
Declir
No conflicts
Label: Inbox Default (6 months) Expires:
12/31/2018 5:42 PM
Review Pipelines.
harmon.ie for...
Welcome
harmon.ie Add-In for Outlook
With harmon.ie Add-In for Office, you can share and save documents to SharePoint Online & OneDrive for Business, from your Office application.
You can specify metadata and required properties to accurately classify documents, so you can find them easily later on.
Read More...
Connect To Office 365
harmon.ie


Microsoft
alexw@m365b618138.onmicrosoft.com
Permissions requested
harmon.ie for Outlook
This app would like to:
Access the directory as you
Sign you in and read your profile
Read and write your files
Read and write items in all site collections
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details
Cancel
Accept
©2018 Microsoft
Terms o

```
set-MsolCompanysettings -UsersPermissionToUserConsentToAppEnabled $false
```


Microsoft 365 admin center
Search
RC
Home
Users
Groups
Roles
Resources
Billing
Support
Settings
Domains
Search & intelligence
Org settings
Integrated apps
Partner relationships
Setup
Reports
Health
Admin centers
Security
Compliance
Azure Active Directo
Services
Security & privacy
Organization profile
Name
Microsoft To Do
Modern authentication
Multi-factor authentication
MyAnalytics
News
Office installation options
Office on the web
Office Scripts
Productivity Score
Reports
SharePoint
Sway
User consent to apps
User consent to apps
Apps not created by Microsoft must receive consent before they can access your organization's data. This setting controls whether users can give that consent to apps that use OpenID Connect and OAuth 2.0 for sign-in and requests to access data.
If you turn this setting on, those apps will ask users for permission to access your organization's data, and users can choose whether to allow it. If you turn this setting off, then admins must consent to those apps before users may use them. In this case, consider setting up an admin consent workflow in the Azure portal so users can send a request for admin approval to use any blocked app.
Learn more about managing consent to apps
Learn more about admin consent workflows
Let users provide consent when apps request access to your organization's data on their behalf

Manage OAuth apps

Filters:

Advanced filters

App: **Select apps...** | User name: **Select users...** | App state: **Select value...** | Community use: **Select value...** | Permissions: **Select permission...**

Permission level:

Bulk selection | New policy from search | Export

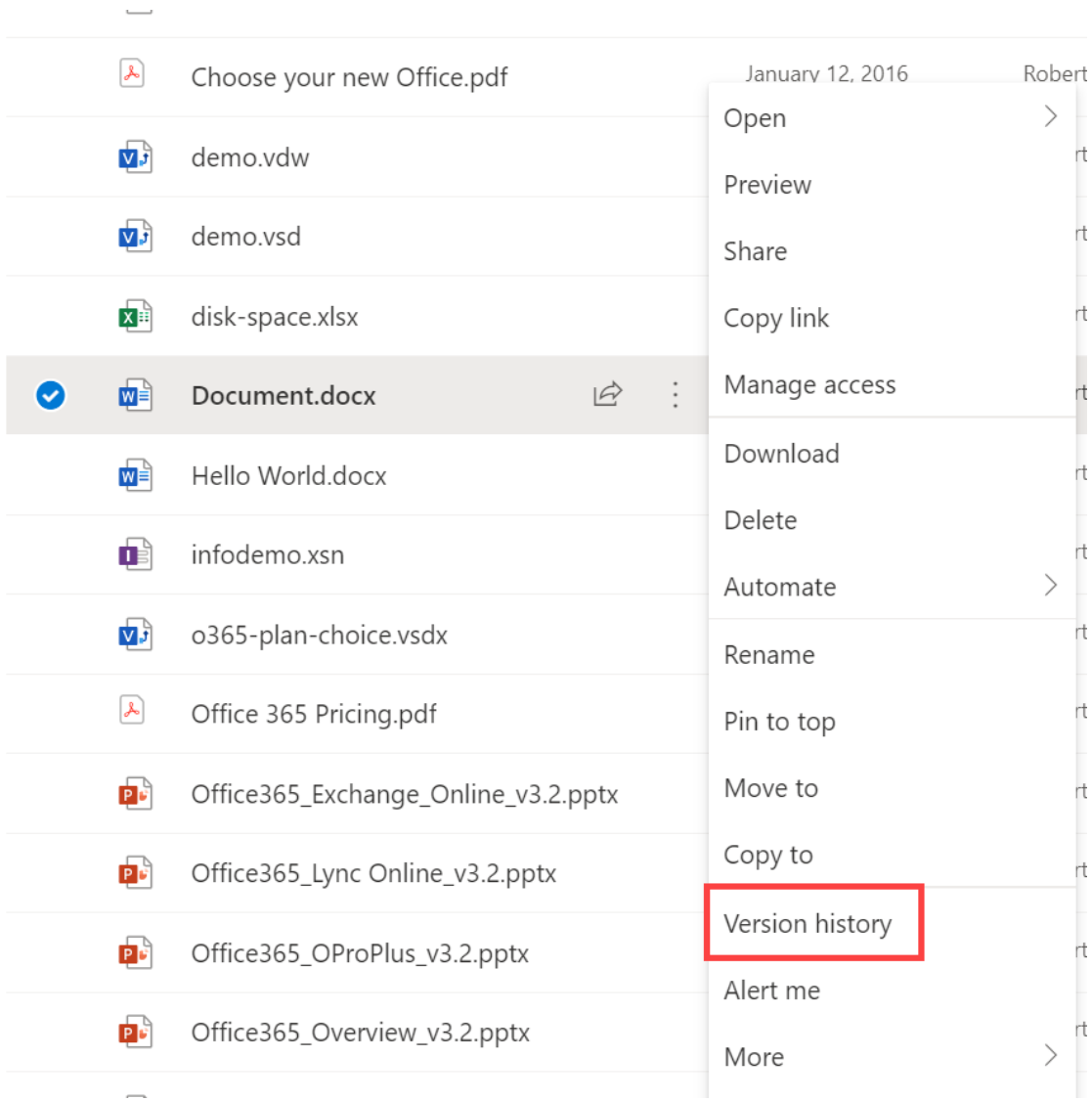
1 - 20 of 62 apps | Show details | Table settings

Name	Authorized by	Permission level	Last authorized	Actions
Polly	13 users	Low	Feb 3, 2021, 11:14 PM	
Polly	5 users	Medium	Aug 4, 2021, 1:16 AM	
Graph Explorer	2 users	High	Nov 25, 2020, 8:05 PM	
WD Antivirus Testground	2 users	Medium	Jul 6, 2021, 10:07 AM	
OneDrive for Business	1 user	High	Aug 5, 2021, 10:31 AM	
Microsoft Docs.com	1 user	High	Jun 9, 2017, 3:41 PM	
Microsoft Tech Community	1 user	Medium	Sep 28, 2016, 6:10 AM	
Office 365	1 user	Low	Sep 30, 2016, 4:56 PM	

Demo

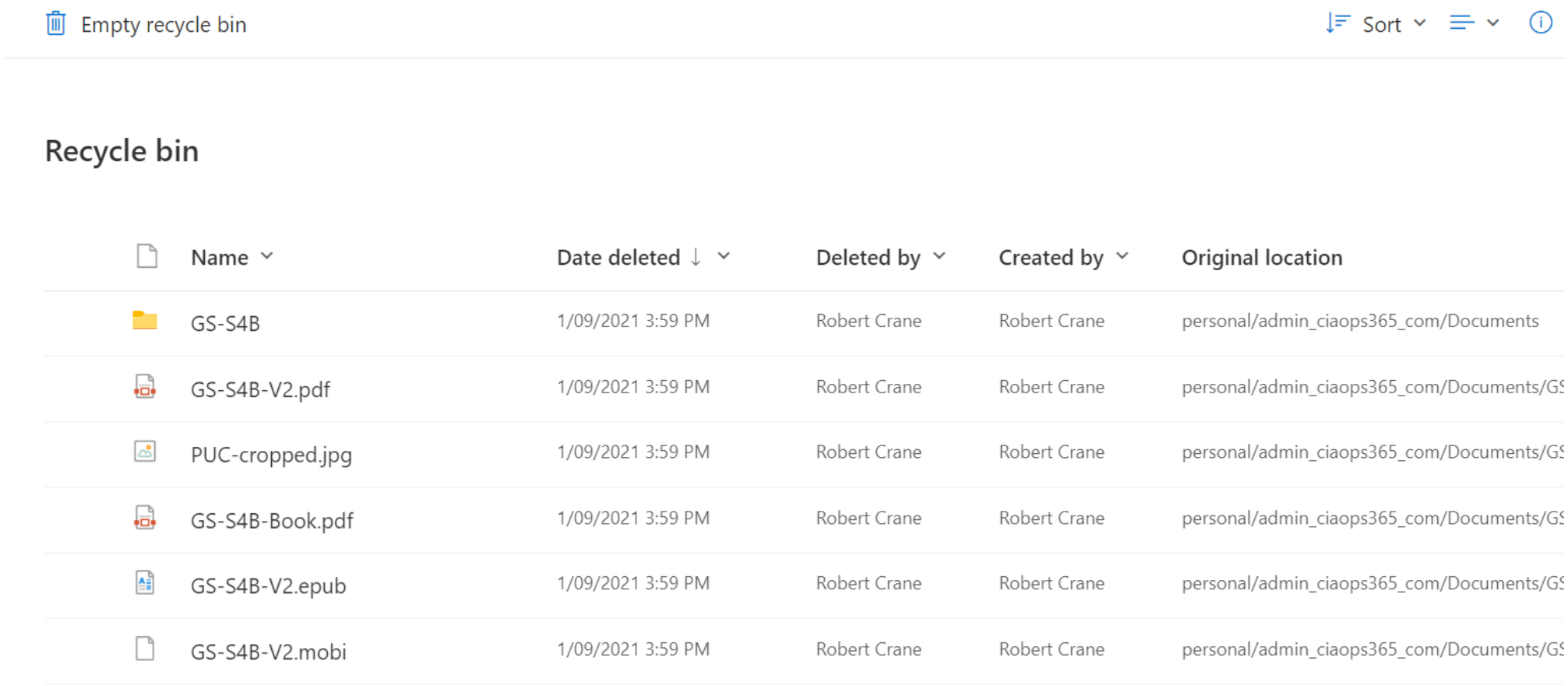
File Security

Automatic versioning

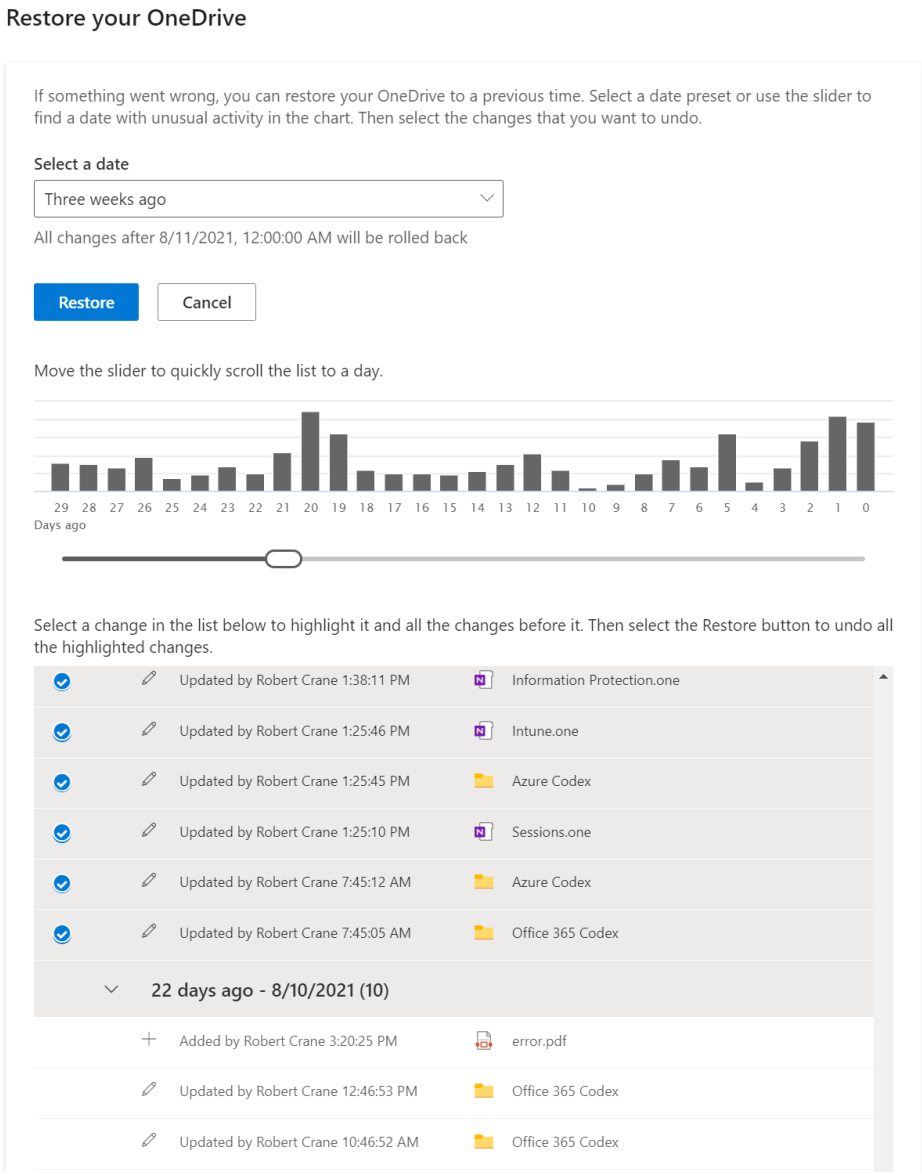


Automatic versioning

Recycle Bin


Empty recycle bin
Sort
Recycle bin
Name
Date deleted
Deleted by
Created by
Original location
GS-S4B
1/09/2021 3:59 PM
Robert Crane
Robert Crane
personal/admin_ciaops365_com/Documents
GS-S4B-V2.pdf
1/09/2021 3:59 PM
Robert Crane
Robert Crane
personal/admin_ciaops365_com/Documents/GS
PUC-cropped.jpg
1/09/2021 3:59 PM
Robert Crane
Robert Crane
personal/admin_ciaops365_com/Documents/GS
GS-S4B-Book.pdf
1/09/2021 3:59 PM
Robert Crane
Robert Crane
personal/admin_ciaops365_com/Documents/GS
GS-S4B-V2.epub
1/09/2021 3:59 PM
Robert Crane
Robert Crane
personal/admin_ciaops365_com/Documents/GS
GS-S4B-V2.mobi
1/09/2021 3:59 PM
Robert Crane
Robert Crane
personal/admin_ciaops365_com/Documents/GS

Restore this Library



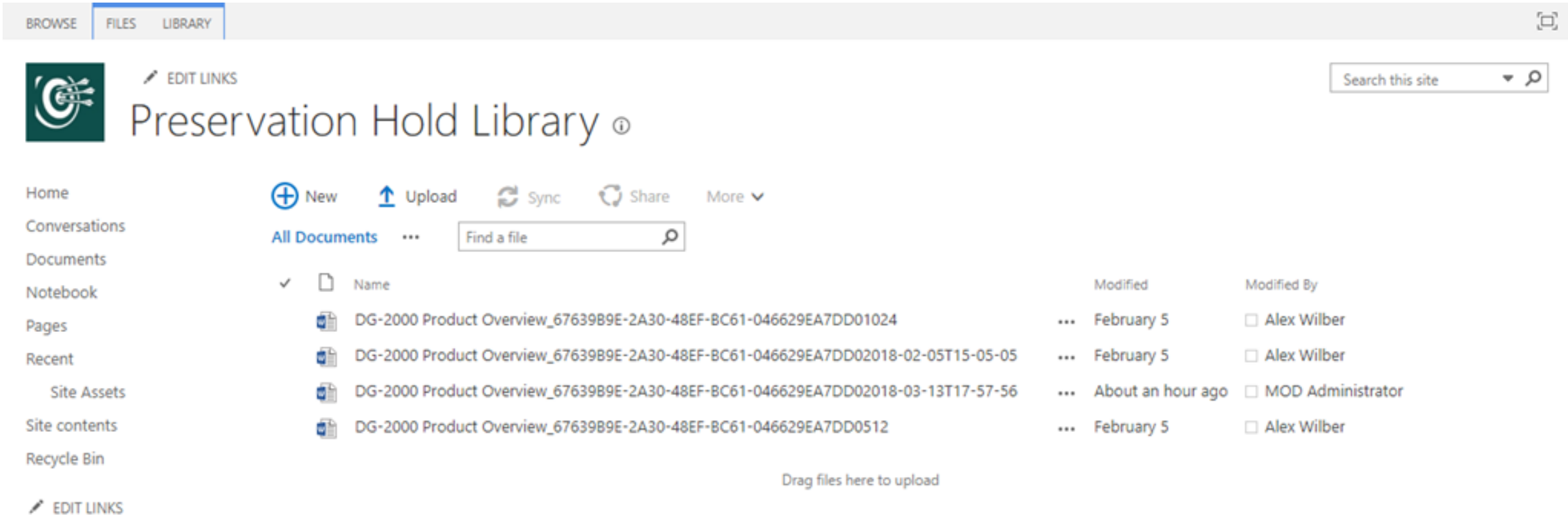
ODFB Retention

2. Enter the number of days you want to retain OneDrive files in the **Days to retain files in OneDrive after a user account is marked for deletion** box.

   The setting takes effect for the next user that is deleted as well as any users that are in the process of being deleted. The count begins as soon as the user account was deleted in the Microsoft 365 admin center, even though the deletion process takes time. The minimum value is 30 days and the maximum value is 3650 days (ten years).

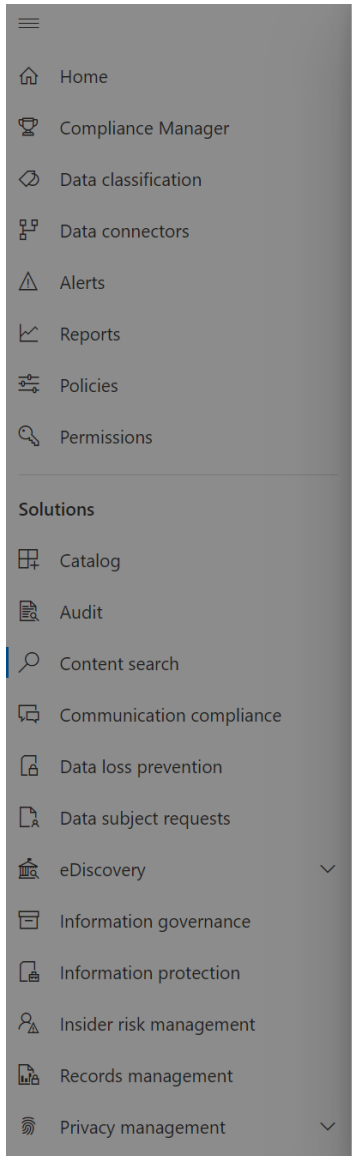
https://blog.ciaops.com/2020/10/13/revisiting-some-facts-around-microsoft-365-backup/

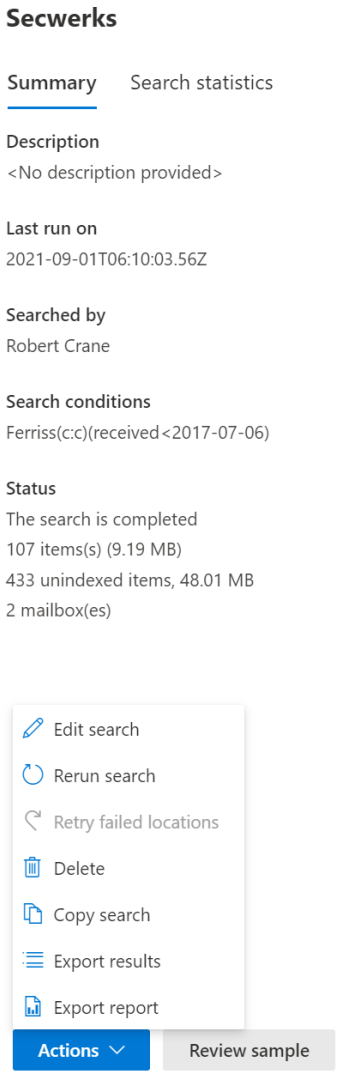
Preservation Hold Library

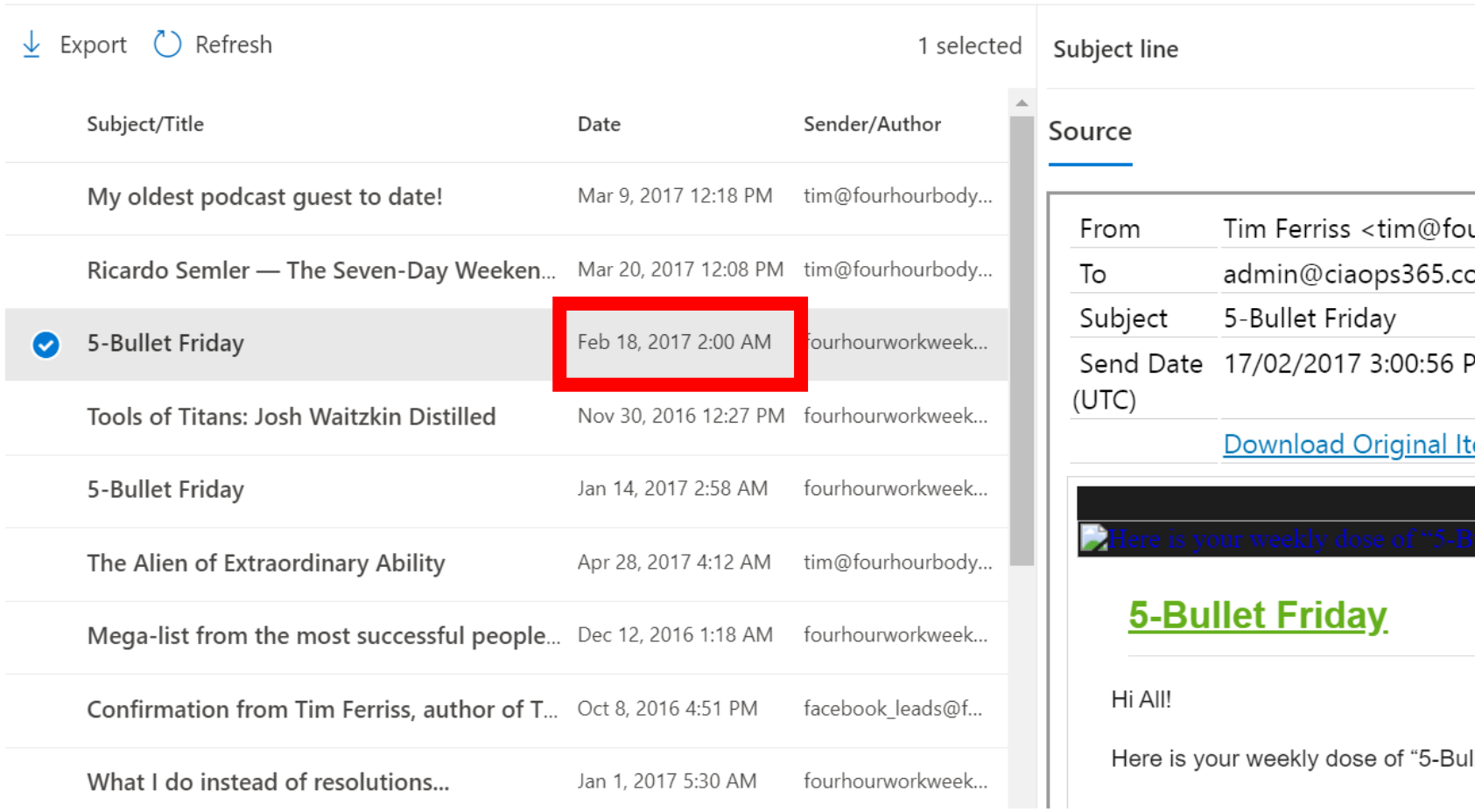


https://blog.ciaops.com/2018/03/14/using-retention-policies-in-office-365/

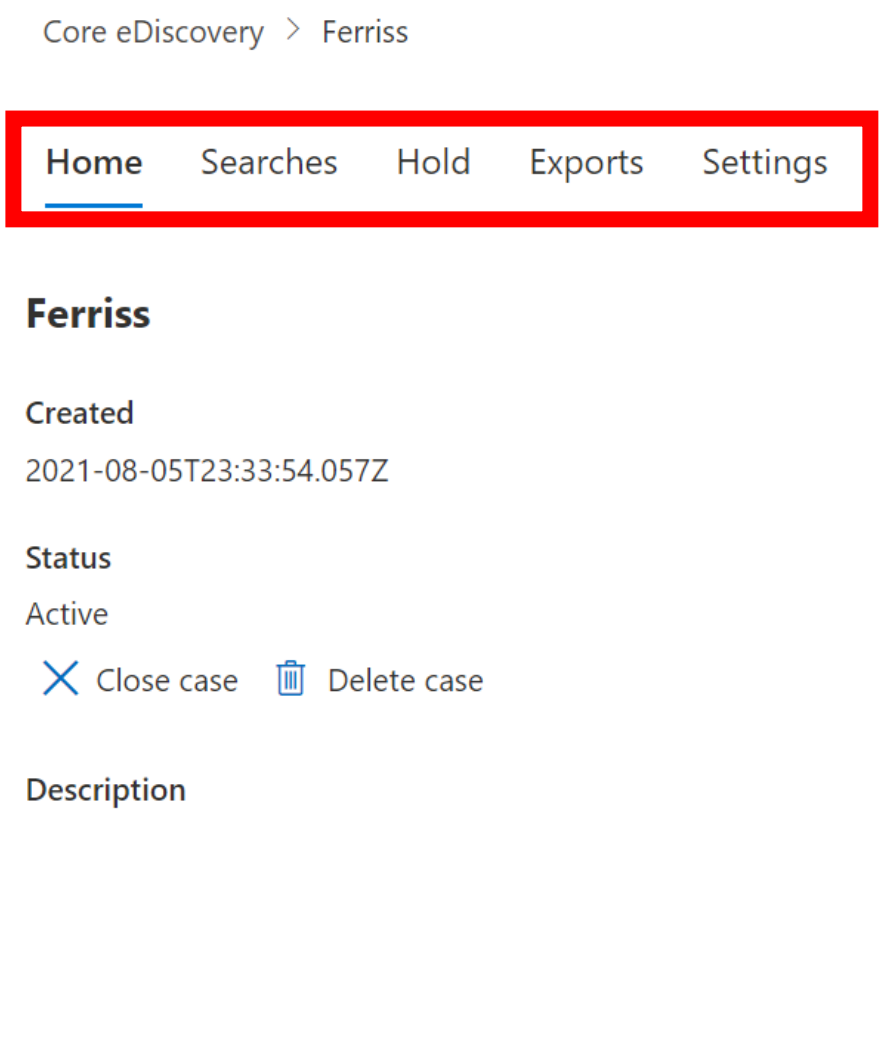
Content Search







eDiscovery


Core eDiscovery > Ferriss
Home
Searches
Hold
Exports
Settings
Ferriss
Created
2021-08-05T23:33:54.057Z
Status
Active
Close case
Delete case
Description

Demo

Best practices

Use Conditional Access for MFA

Do not enable MFA on a per user basis

Always exclude an admin account from the policies to ensure you can correct a mistake

Start with one target group of users

Ensure your users know what to expect

Test your policies before rolling out

Common tasks

Enable SSPR in Azure AD

Create an Conditional Access Exclusion group

Enable common conditional access policies

- Block Legacy Authentication
- Require MFA for admins
- Require MFA for all users
- Secure security info registration
- Block access by location
- Require compliant devices

Microsoft

Security summary

Resources

All content that is linked through out this document can be found at these sites.

Microsoft 365 Business Premium Partner Playbook (aka.ms/m365bppartnerplaybook):
The place to answer all your questions on the product and what is included from a licensing perspective.

Microsoft Defender for Business Partner Kit (aka.ms/mdbpartnerkit):
The place to get deep dive information on core SMB partner opportunities including partner playbooks, customer marketing material & tele sales scripts.

Microsoft 365 Business Partner Page (https://www.microsoft.com/microsoft-365/partners/business):
The one stop show for all product content related to Microsoft 365 Business, including product pitch material, licensing and deployment kits.

Microsoft SMB Tech Community (aka.ms/smbtc):
Forum for technical discussion & questions. The place for the experts.

Practical security resources

Microsoft Secure Score
https://securescore.microsoft.com

Microsoft 365 Business Premium security guide
https://aka.ms/m365bpguide

IT ProMentor CIS based Security Assessment tool
https://www.itpromentor.com/cis-controls-4m365