1Q48VMiR152XNuDEkfV3khFdiYoBPGH4V4

Support this content
via Bitcoin

Focusing on security with Microsoft 365 Business

June 2018

@directorcia

http://about.me/ciaops

- Security is a journey NOT a destination !

- Security is something that just can’t be turned on

- Nobody ever calls to tell you that everything is working

- Users just want the technology to work

- Security is about reducing risk

- Got access denied ? Good !

- You alone are responsible for your IT security

- The easiest way is not the most secure
- Cost of pro active security is less that post active recovery
- What is your security situation now ?
- Initial entry is everything
- What is the impact of failure ?
- Have you done a security assessment ?

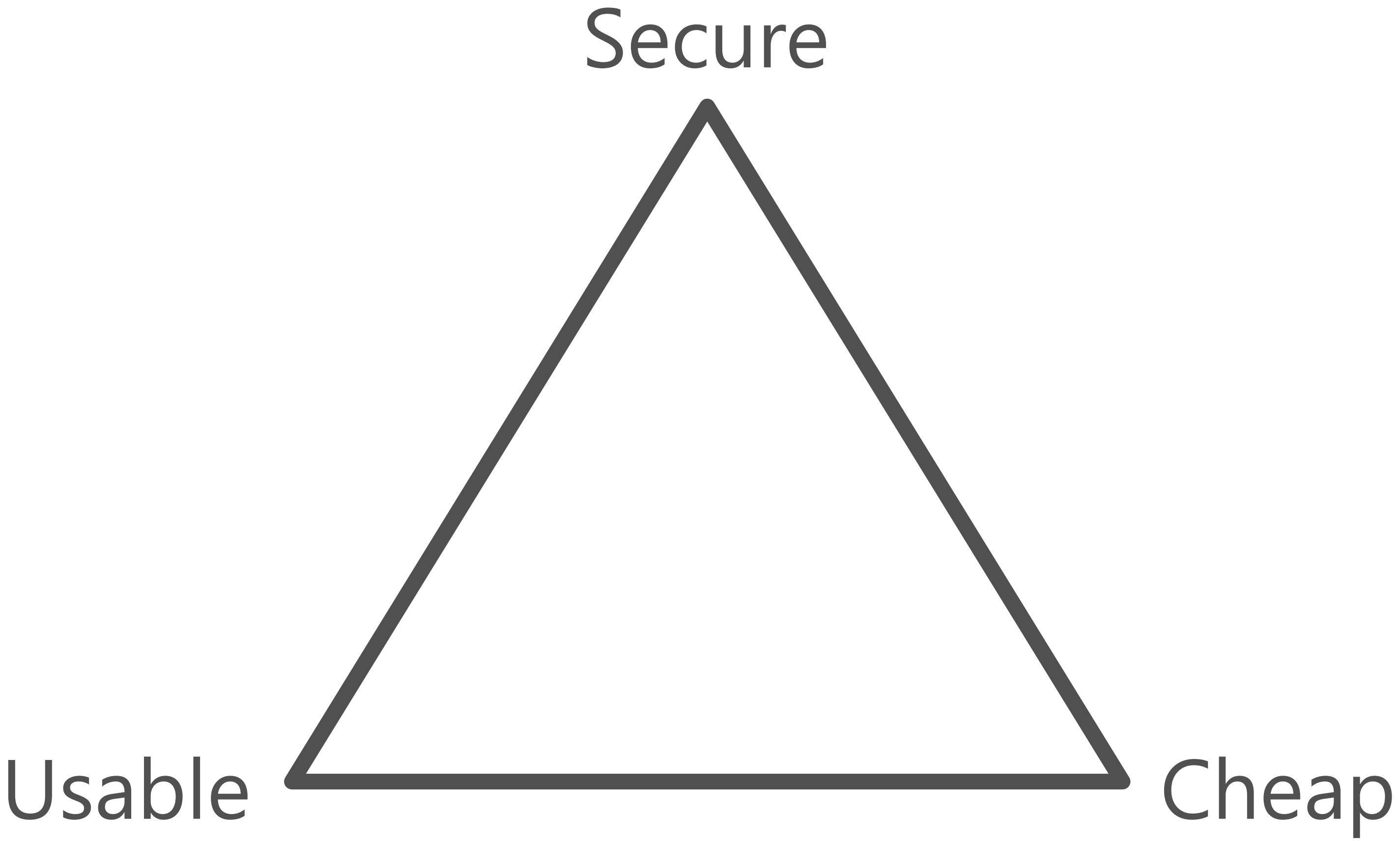
Q. How many exploits do YOU have to defend against ?

A. Every single one

Q. How many exploits does ANYONE need to find ?

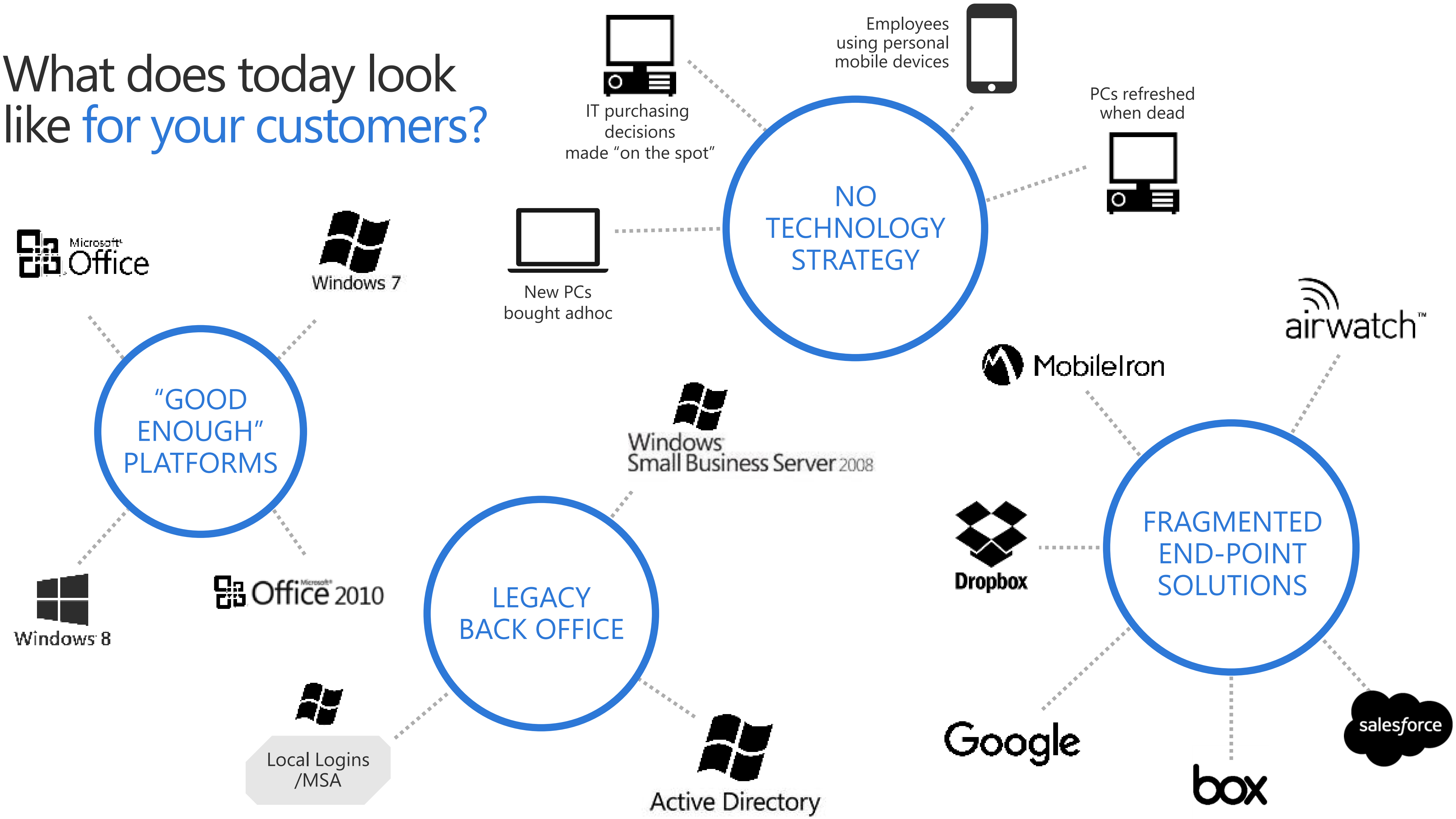
A. Just one !

The Security Dilemma



Complexity is enemy of security

What does today look like for your customers?



NO TECHNOLOGY STRATEGY

IT purchasing decisions made “on the spot”

Employees using personal mobile devices

PCs refreshed when dead

New PCs bought adhoc

“GOOD ENOUGH” PLATFORMS

Microsoft Office

Windows 7

Windows 8

Office 2010

LEGACY BACK OFFICE

Windows Small Business Server 2008

Local Logins /MSA

Active Directory

FRAGMENTED END-POINT SOLUTIONS

airwatch

MobileIron

Dropbox

Google

box

salesforce

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*

Providing clarity and consistency for the protection of personal data

The **General Data Protection Regulation** (GDPR) imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents, no matter where they are located.

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

Microsoft 365 Business

An integrated solution to securely run and grow your business

Office 365 Business Premium

Office Applications:
Word, Excel, PowerPoint, Outlook, OneNote, Publisher, and Access

Online Services:
Exchange, OneDrive (1TB), Skype for Business, SharePoint, Teams

Business Apps:
Bookings, Staff Hub, Outlook Customer Manager

+

Enhanced Security Cross-platform

Consistent Security configuration across Windows 10, Android and iOS devices

Documents encryption and enforced Multi Factor Authentication and restricted copy/paste

Device data encryption with BitLocker and remote wipe for lost or stolen devices

Information Rights Management, Intelligent Labeling and Data Loss Prevention tips

Device protection against ransomware and malicious websites with Windows Exploit Guard

+

Device Management & Simplified Admin

Always up-to-date Office, Windows and Windows Defender anti virus

Streamlined deployment of PCs with Windows AutoPilot

Auto-installation of Office apps on Windows 10 Devices

Mobile Device Management for Windows 10, Android, iOS and Mac with Microsoft Intune

Exchange Online archiving & preservation policies to recover data or remain compliant

*Includes upgrade benefits from **Windows 7 Professional** or **Windows 8.1 Pro** to **Windows 10 Pro** at no additional cost*

New features in Microsoft 365 Business (April 2018)

Cyber Threats

- Office 365 Advanced Threat Protection[1]

  Attachment scanning & ML detection to catch suspicious attachments

  Link Scanning/Checking to prevent users from clicking suspicious links

- Windows Exploit Guard Enforcement

  Preventing devices from ransomware and malicious websites at device end points

Back End

- Hybrid Active Directory Deployment[3]

  To support customers with on premise infrastructure

Safeguard Sensitive Information

- Data Loss Prevention[2]

  Does Deep Content Analysis to easily identify, monitor, and protect sensitive information from leaving org

- Azure Information Protection P1

  Controls & Manages how sensitive content is accessed

- Intune Availability

  Protecting data across devices with E2E Device and app management

- Exchange Online archiving

  100GB Archiving & preservation policies to recover data or remain compliant

- Bitlocker Enforcement

  Encrypt Data on devices to protect data if device lost or stolen

[1] O365 ATP for Email available now. Word, Excel and PowerPoint support coming soon
[2] DLP Policy Tips and IRM in Outlook coming soon

[3] DJ++ guidance and technical documentation coming soon

Microsoft 365 Business

One subscription for Productivity + Security + Device Management

3rd party solutions
(bought separately, expensive & hard to integrate)

- Device Management
- Archiving
- Data Loss Prevention
- Email Threat Protection
- Email Filtering
- Device Anti Virus
- Online Chat & Meetings
- Storage
- Email
- Productivity Software

VS.

- Device & App Management
  PCs, Macs, iOS & Android
- Information Protection
- Archiving + Litigation Hold
- Data Loss Prevention
- Email + Device Threat Protection
- Email Filtering
- Windows Defender AV
- Teams & Skype for Business
- 1 TB File Storage
- 50 GB Cloud Email
- Office
  (Word, PowerPoint, Excel, Outlook, Onenote)

Microsoft 365 Business
(all included, seamlessly integrated)

AU$28 Per user standalone

Detailed comparison of plans

	Features (new in blue)	Office 365 BP	Microsoft 365 Business	Microsoft 365 E3	Microsoft 365 E5
	Estimated retail price per user per month $USD (with annual commitment)	$17.49	$28.07	$49.06	$89.21
	Maximum number of users	300	300	unlimited	unlimited
Office Apps	Install Office on up to 5 PCs/Macs + 5 tablets + 5 smartphones per user (Word, Excel, PowerPoint, OneNote, Access), Office Online	Business	Business	ProPlus	ProPlus
Email & Calendar	Outlook, Exchange Online	50GB	50GB	unlimited	unlimited
Chat-based Workspace, Meetings	Microsoft Teams, Skype For Business	●	●	●	●
File Storage	OneDrive for Business	1 TB	1 TB	unlimited	unlimited
Social, Video, Sites	Yammer, SharePoint Online, Planner	●	●	●	●
	Stream		●	●	●
Business Apps	Scheduling Apps – Booking, StaffHub	●	●	●	●
	Business Apps – Outlook Customer Manager, MileIQ[1] Business center[2], Listings[2], Connections[2], Invoicing[2]	●	●		
Threat Protection	Microsoft Advanced Threat Analytics, Device Guard, Credential Guard, App Locker, Enterprise Data Protection,			●	●
	Office 365 Advanced Threat Protection		●		●
	Windows Defender Advanced Threat Protection				●
	Office 365 Threat Intelligence				●
Identity & Access Management	Azure Active Directory - SSPR Cloud Identities, MFA, SSO >10 Apps		●	●	●
	Azure Active Directory - Conditional Access, SSPR Hybrid Identities, Cloud App Discovery, AAD Connect Health			●	●
	Credential Guard and Direct Access			●	●
	Azure Active Directory Plan 2				●
Device & App Management	Microsoft Intune, Windows AutoPilot		●	●	●
	Microsoft Desktop Optimization Package, VDA			●	●
Information Protection	Unlimited Exchange Archiving[3], Office 365 Data Loss Prevention*, Azure Information Protection Plan 1		●	●	●
	Azure Information Protection Plan 2, Microsoft Cloud App Security, O365 Cloud App Security				●
On-Prem CAL Rights	ECAL Suite (Exchange, SharePoint, Skype, Windows, SCCM, Win. Rights Management)			●	●
Compliance	Litigation Hold, eDiscovery, Compliance Manager, Data Subject Requests		●	●	●
	Advanced eDiscovery, Customer Lockbox, Advanced Data Governance				●
Analytics	Power BI Pro, MyAnalytics				●
Voice	PSTN Conferencing, Cloud PBX				●

[1] Available in US, UK, Canada; [2] Currently in public preview in US, UK, Canada; [3] Unlimited when auto-expanding turned on

*Data Loss Prevention Features will be available summer 2018

Microsoft 365 powered device

The best way to experience Microsoft 365

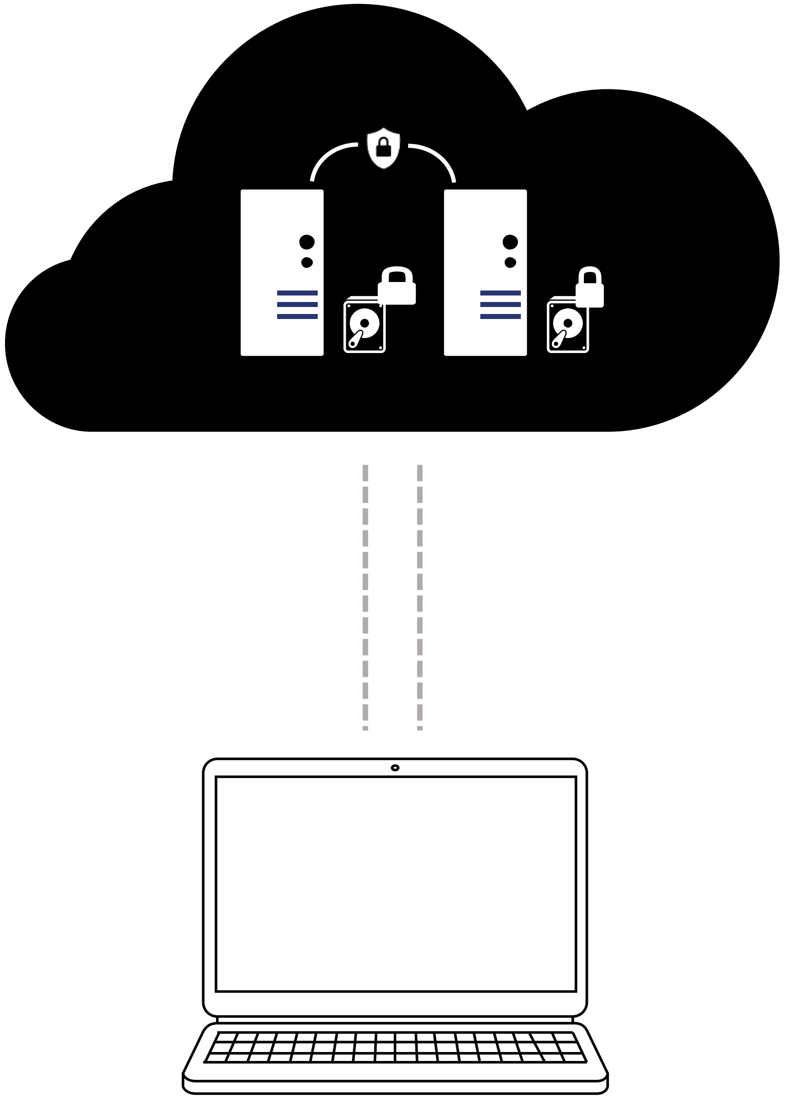
- Intelligent security, built-in
- Easy to deploy and manage
- Always up to date
- Proactive insights

Some Standard Offerings

Default Encryption

- Data in transit
  - Strong SSL/TLS cipher suite
  - Perfect Forward Secrecy
  - Datacenter-to-datacenter encryption

- Data at rest
  - BitLocker disk encryption
  - Per-file encryption for customer content

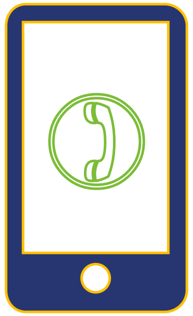


Multi-factor authentication

Mobile Apps

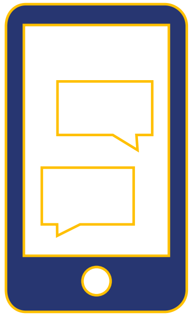
Push Notification
One-Time-Passcode
(OTP) Token

Phone Calls



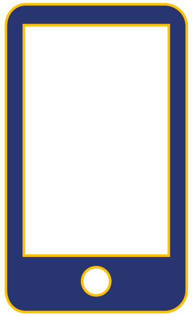
Phone Calls

Text Messages



Text
One-Time Passcode
(OTP) by Text

Code



Code
One-Time app
passcode

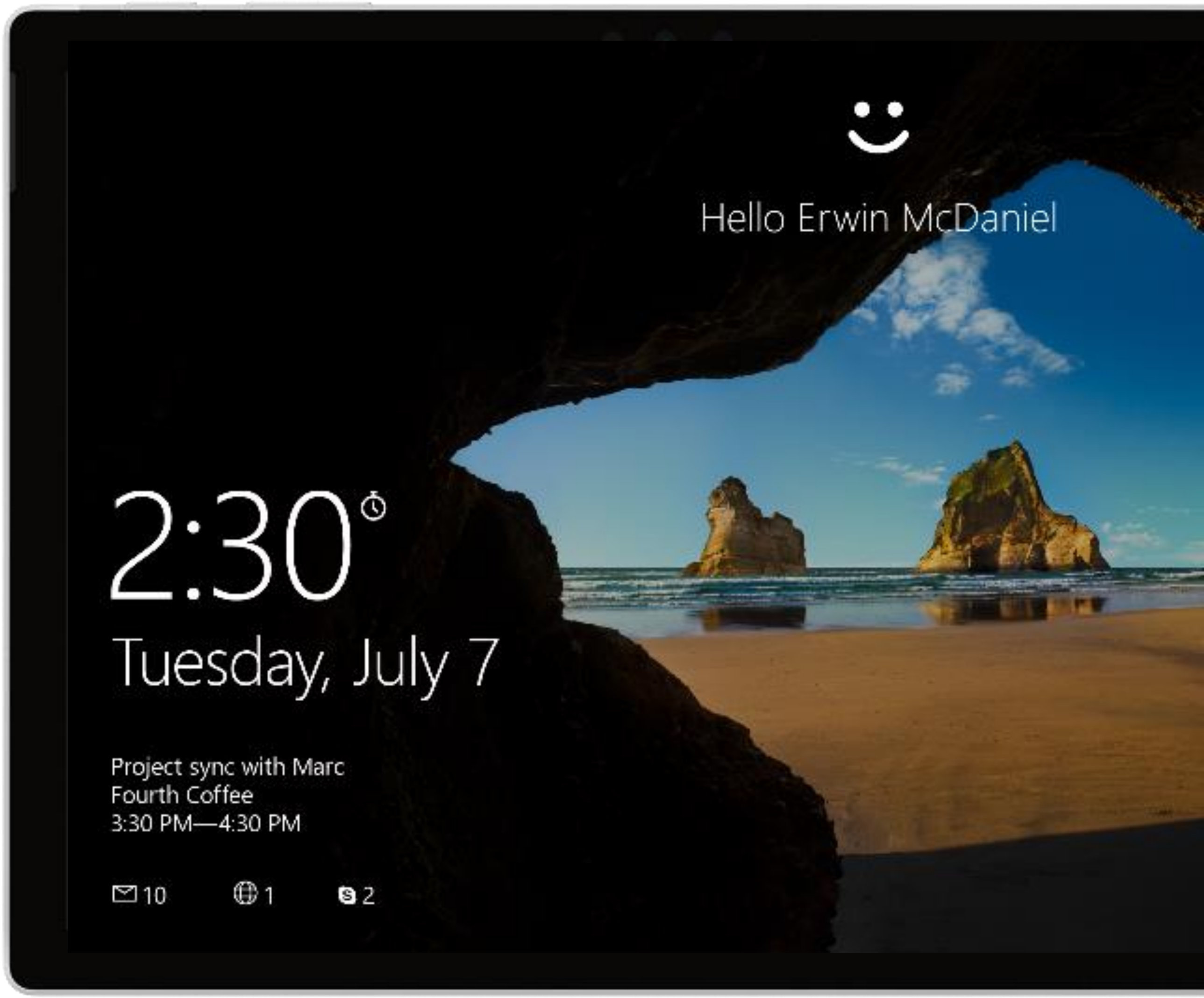
WINDOWS HELLO **FOR BUSINESS**

Passwordless strong authentication via multiple factors

- PC + PIN or Biometrics
- PC + Companion Device
- PC supported Biometrics: fingerprint & facial
- Companion Device can support other biometrics options (e.g.: EKG)

Supported on any Windows 10 device

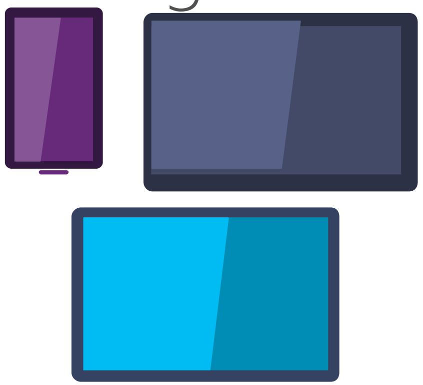
>100 devices supporting biometrics



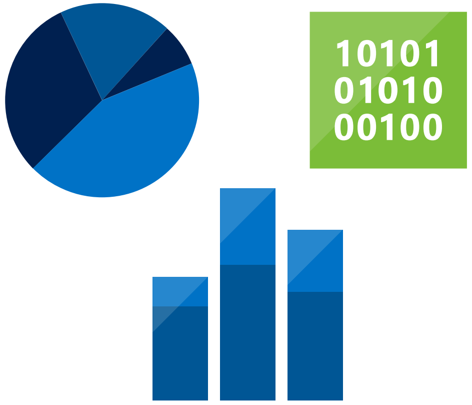
Mobile Device Management

Conditional Access

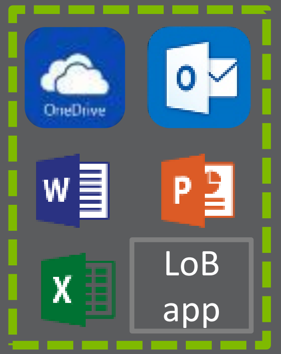
Device Management



Selective Wipe



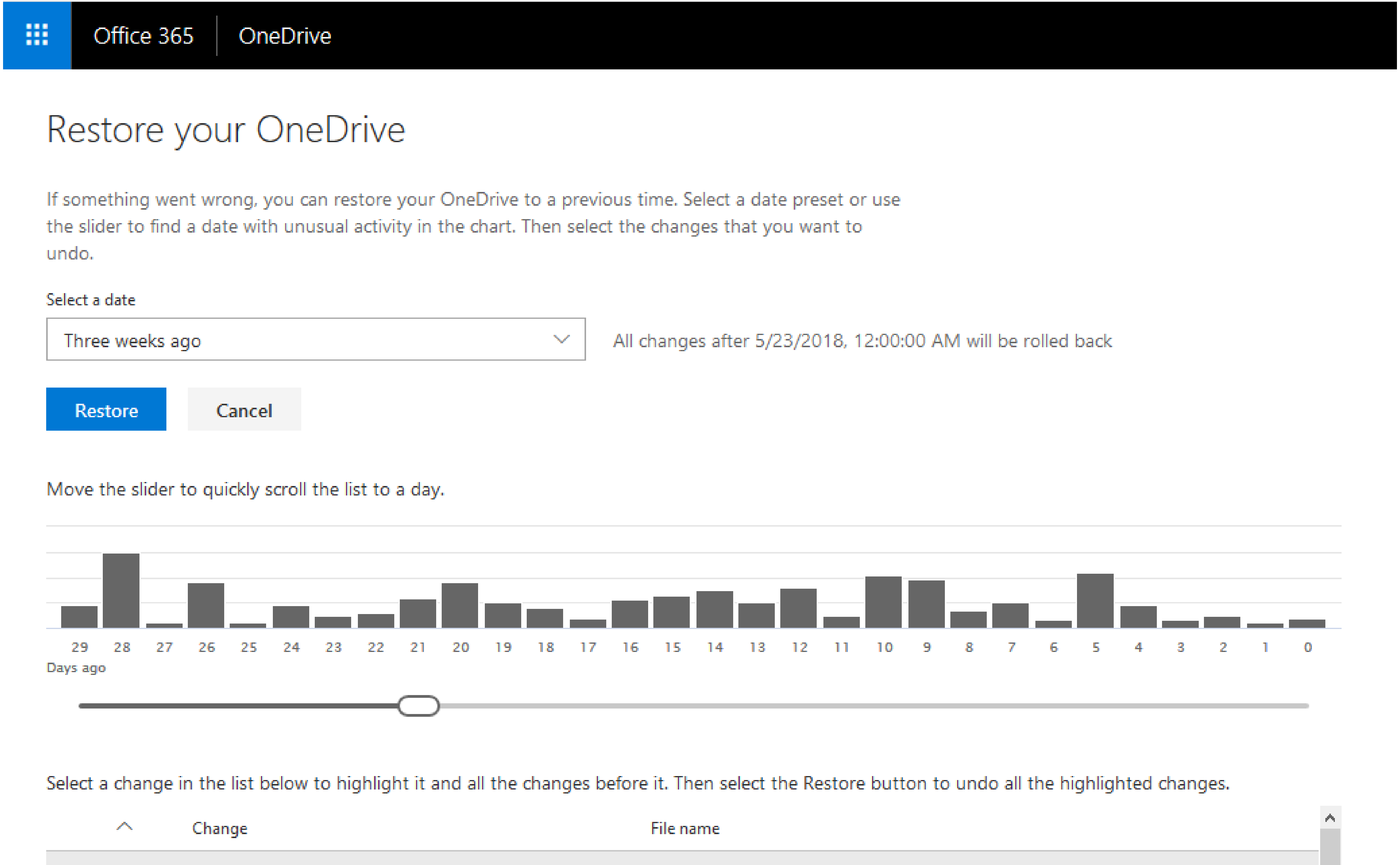
Advanced Application Management



MDM Office 365 Built-in

+

Microsoft Intune



Restore your OneDrive

If something went wrong, you can restore your OneDrive to a previous time. Select a date preset or use the slider to find a date with unusual activity in the chart. Then select the changes that you want to undo.

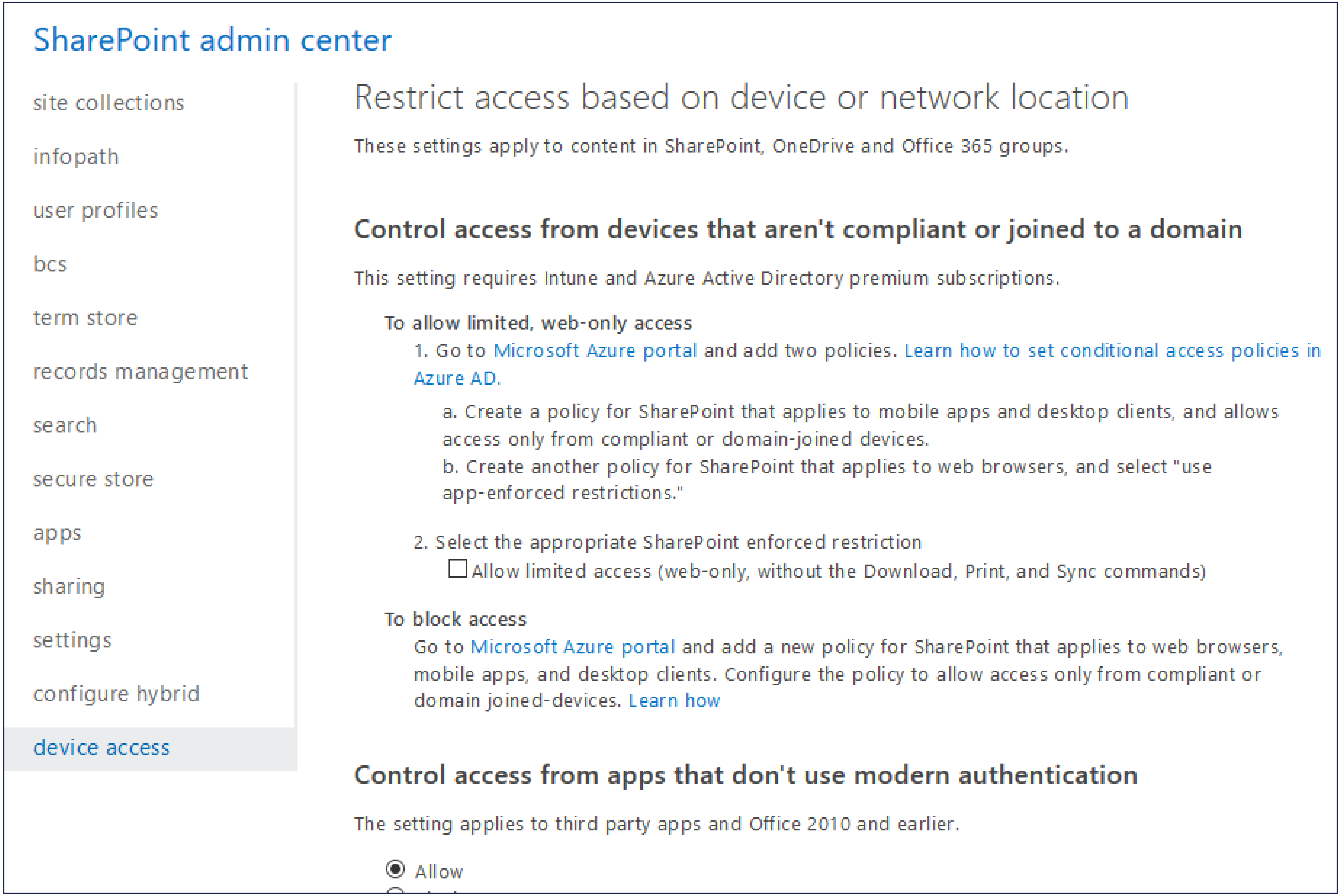
Select a date

Three weeks ago

All changes after 5/23/2018, 12:00:00 AM will be rolled back

Move the slider to quickly scroll the list to a day.

Select a change in the list below to highlight it and all the changes before it. Then select the Restore button to undo all the highlighted changes.



Restrict access based on device or network location

These settings apply to content in SharePoint, OneDrive and Office 365 groups.

Control access from devices that aren't compliant or joined to a domain

This setting requires Intune and Azure Active Directory premium subscriptions.

To allow limited, web-only access

1. Go to Microsoft Azure portal and add two policies. Learn how to set conditional access policies in Azure AD.

   a. Create a policy for SharePoint that applies to mobile apps and desktop clients, and allows access only from compliant or domain-joined devices.

   b. Create another policy for SharePoint that applies to web browsers, and select "use app-enforced restrictions."

2. Select the appropriate SharePoint enforced restriction

   ☐ Allow limited access (web-only, without the Download, Print, and Sync commands)

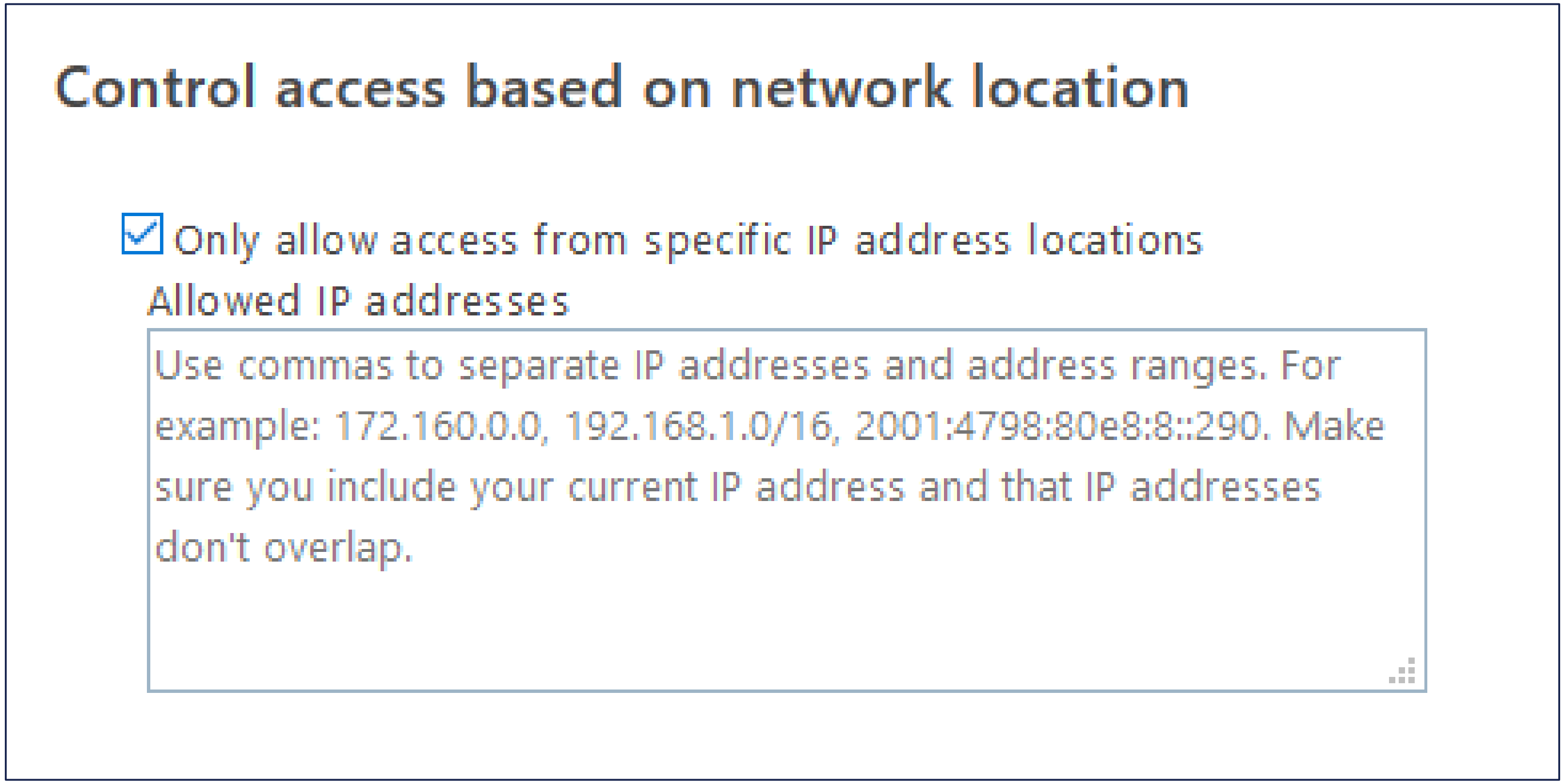
To block access

Go to Microsoft Azure portal and add a new policy for SharePoint that applies to web browsers, mobile apps, and desktop clients. Configure the policy to allow access only from compliant or domain joined-devices. Learn how

Control access from apps that don't use modern authentication

The setting applies to third party apps and Office 2010 and earlier.

● Allow



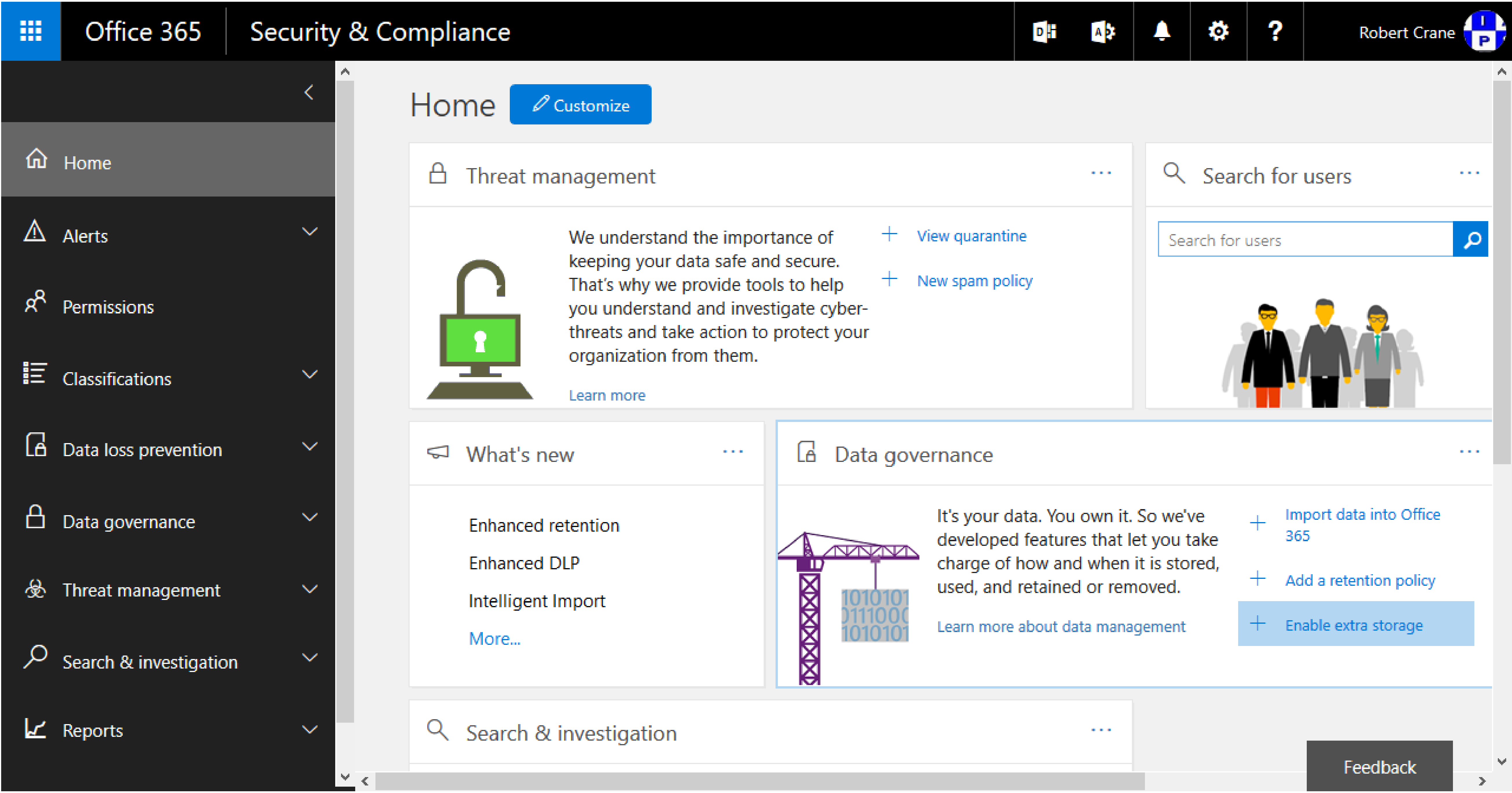
Control access based on network location

☑ Only allow access from specific IP address locations

Allowed IP addresses

Use commas to separate IP addresses and address ranges. For example: 172.160.0.0, 192.168.1.0/16, 2001:4798:80e8:8::290. Make sure you include your current IP address and that IP addresses don't overlap.

Security and Compliance Center



Home

Threat management

We understand the importance of keeping your data safe and secure. That's why we provide tools to help you understand and investigate cyber-threats and take action to protect your organization from them.

Learn more

+ View quarantine

+ New spam policy

Search for users

Search for users

What's new

Enhanced retention

Enhanced DLP

Intelligent Import

More...

Data governance

It's your data. You own it. So we've developed features that let you take charge of how and when it is stored, used, and retained or removed.

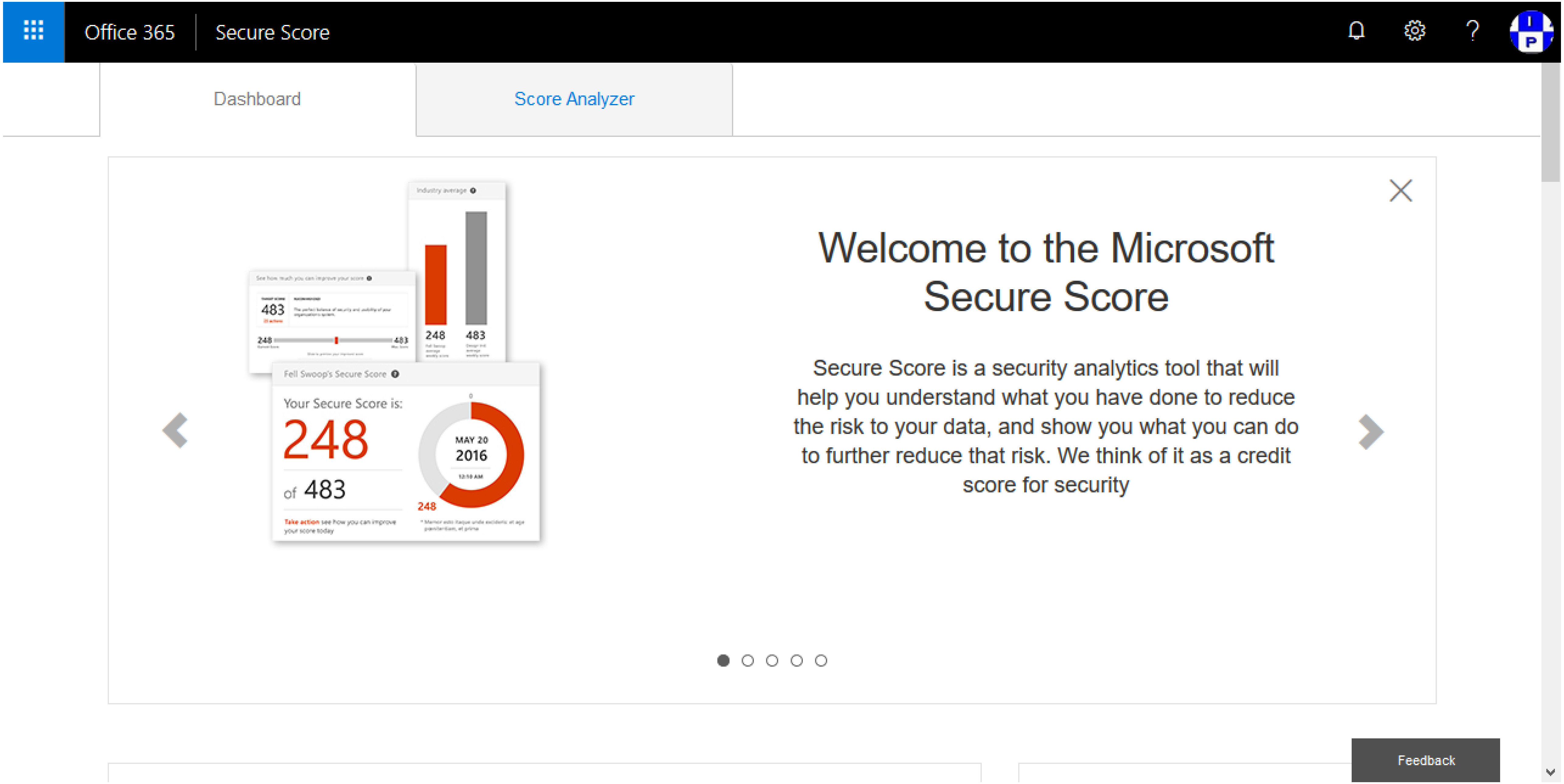
Learn more about data management

+ Import data into Office 365

+ Add a retention policy

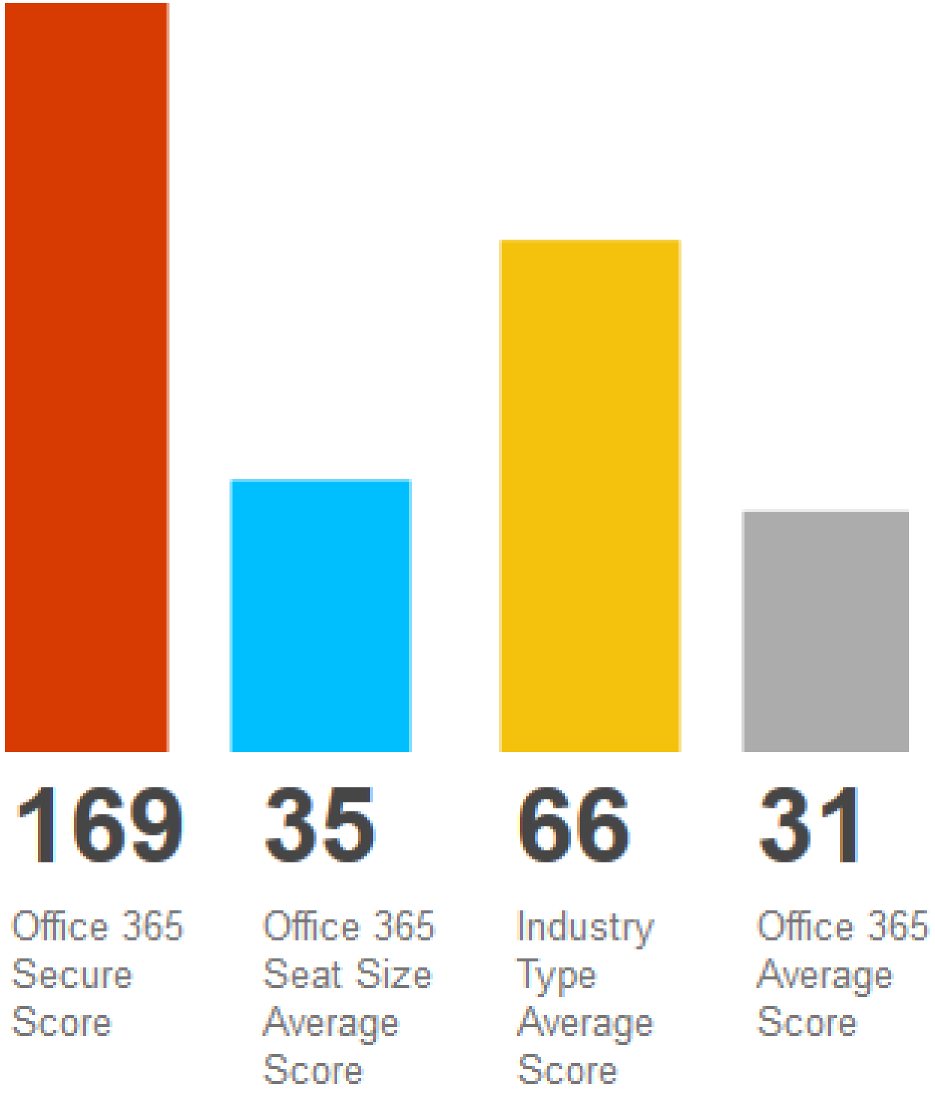
+ Enable extra storage

Search & investigation

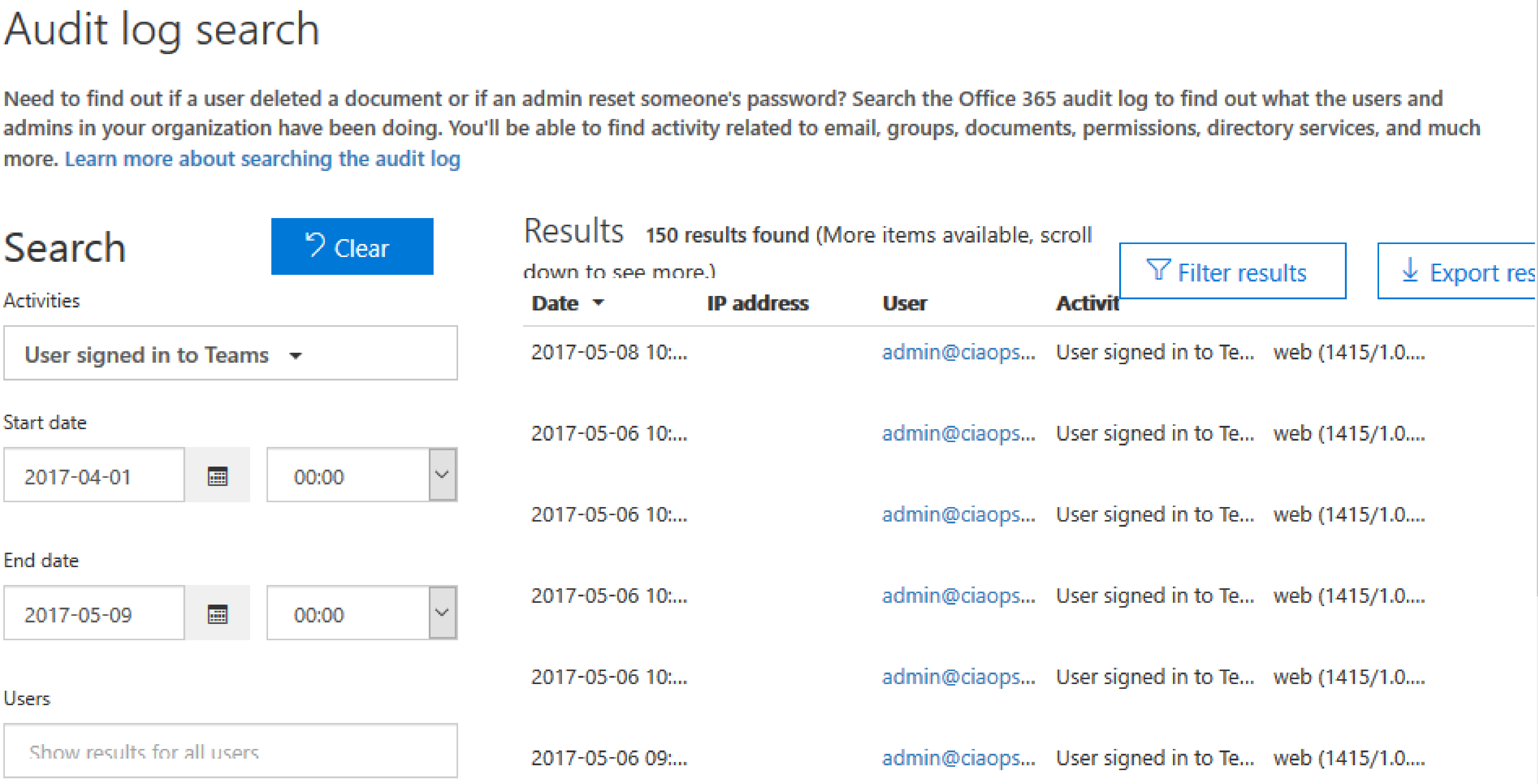


Welcome to the Microsoft Secure Score

Secure Score is a security analytics tool that will help you understand what you have done to reduce the risk to your data, and show you what you can do to further reduce that risk. We think of it as a credit score for security



Seat size this tenant belongs to is 6 - 99 seats
Industry type for this tenant is Technology



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

Activities

User signed in to Teams

Start date

2017-04-01 00:00

End date

2017-05-09 00:00

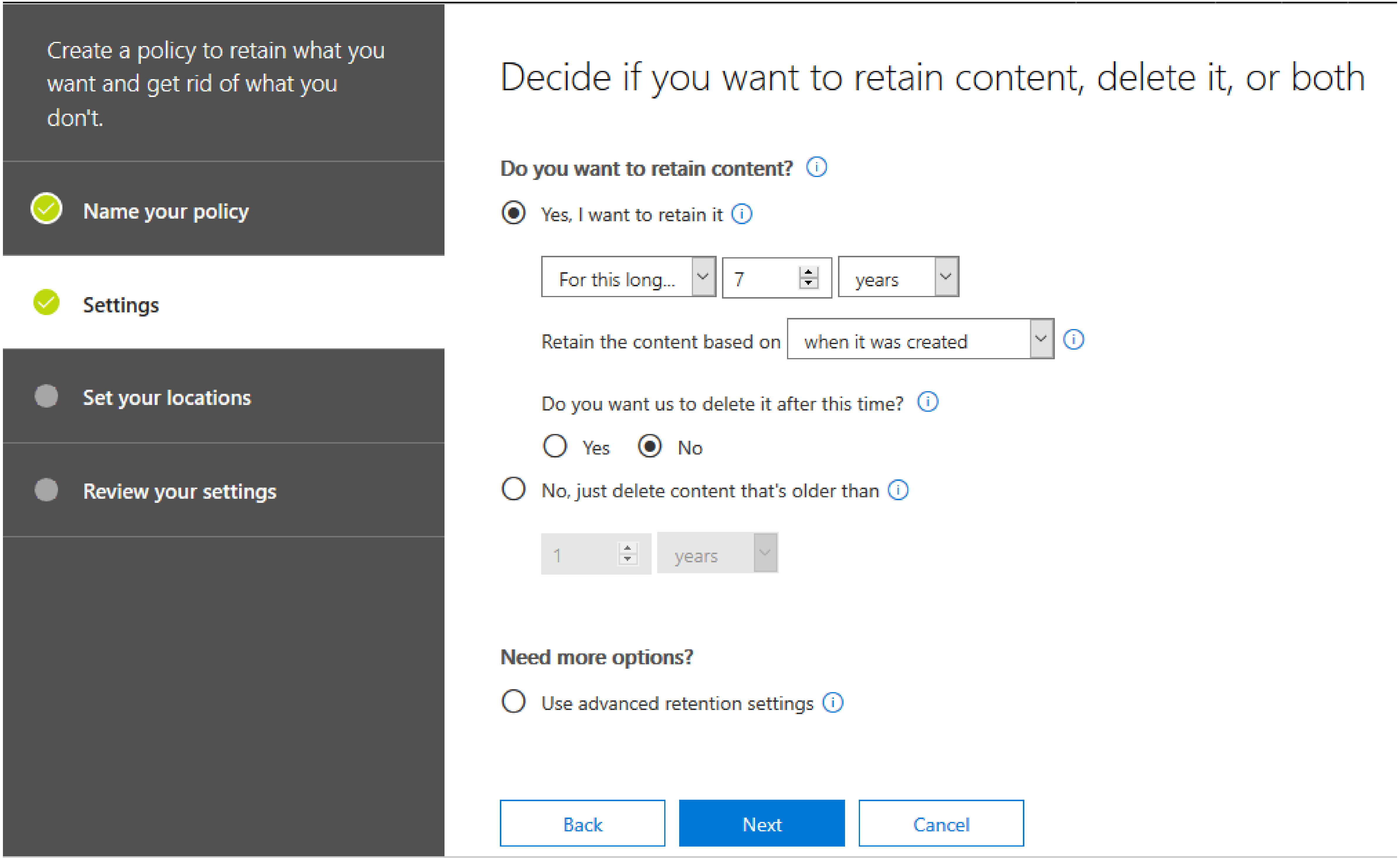
Users

Show results for all users

Results

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

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....



Create a policy to retain what you want and get rid of what you don't.

- ✓ Name your policy
- ✓ Settings
- ● Set your locations
- ● Review your settings

Decide if you want to retain content, delete it, or both

Do you want to retain content?

● Yes, I want to retain it

For this long... | 7 | years

Retain the content based on when it was created

Do you want us to delete it after this time?

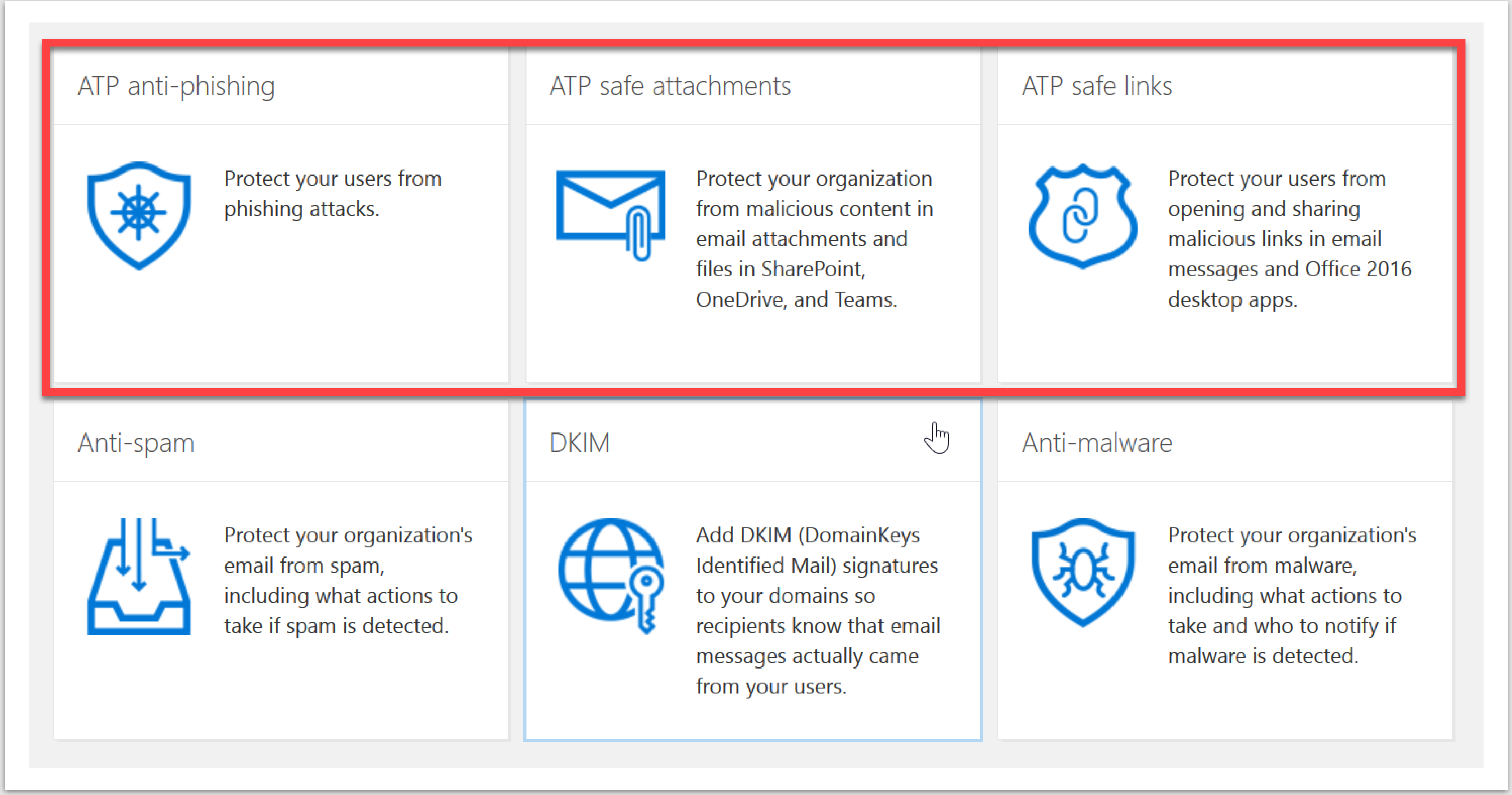
○ Yes ● No

○ No, just delete content that's older than

1 | years

Need more options?

○ Use advanced retention settings



ATP anti-phishing

Protect your users from phishing attacks.

ATP safe attachments

Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.

ATP safe links

Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.

Anti-spam

Protect your organization's email from spam, including what actions to take if spam is detected.

DKIM

Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.

Anti-malware

Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

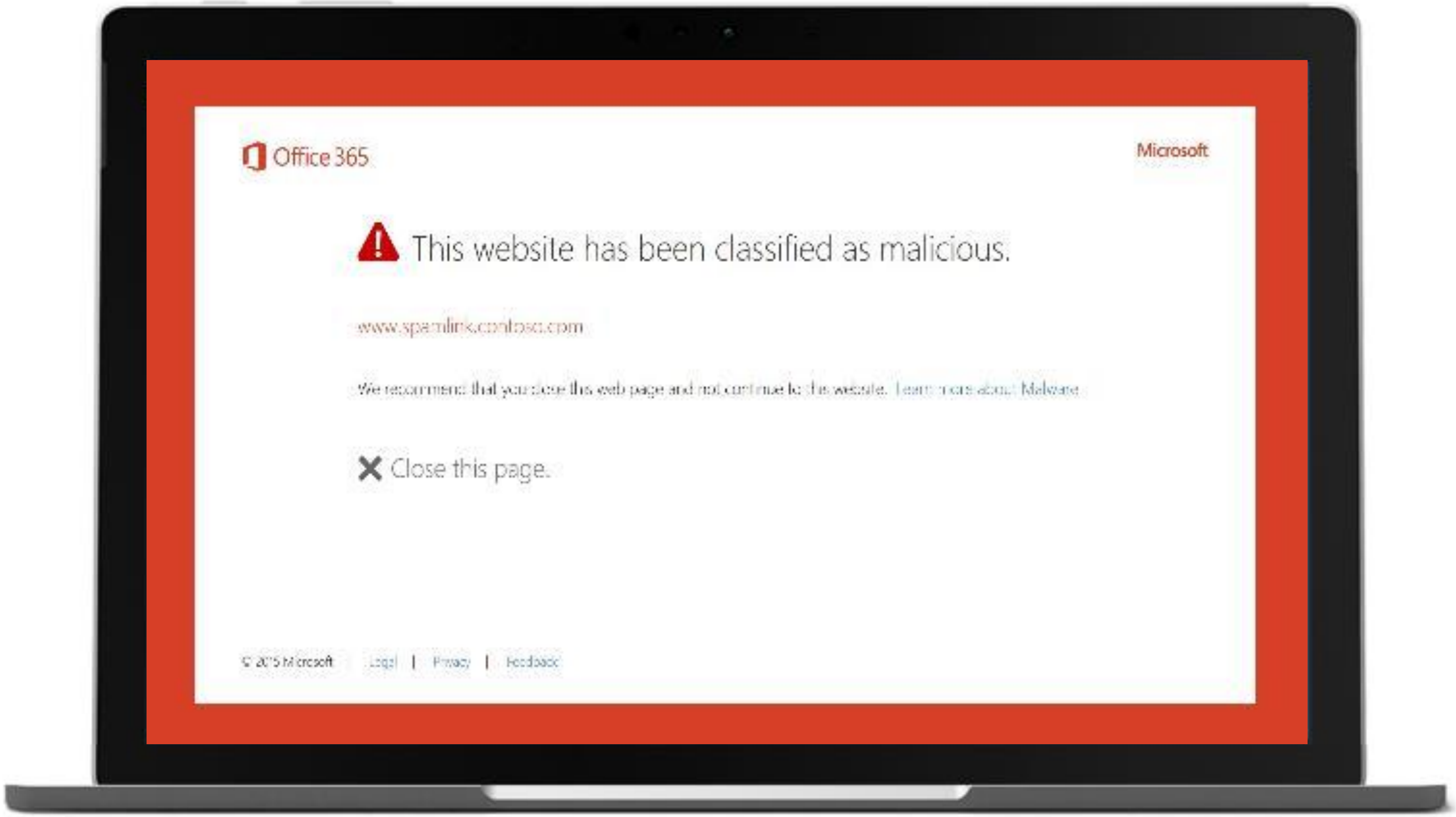
Safeguard your data:

Protection from threats

Links are **checked in real time** to warn you if the destination is a malicious site

AI-powered attachment scanning detects malware previously not seen

Windows devices are **monitored for suspicious processes** like ransomware



Office 365

Microsoft

This website has been classified as malicious.

www.spamlink.contoso.com

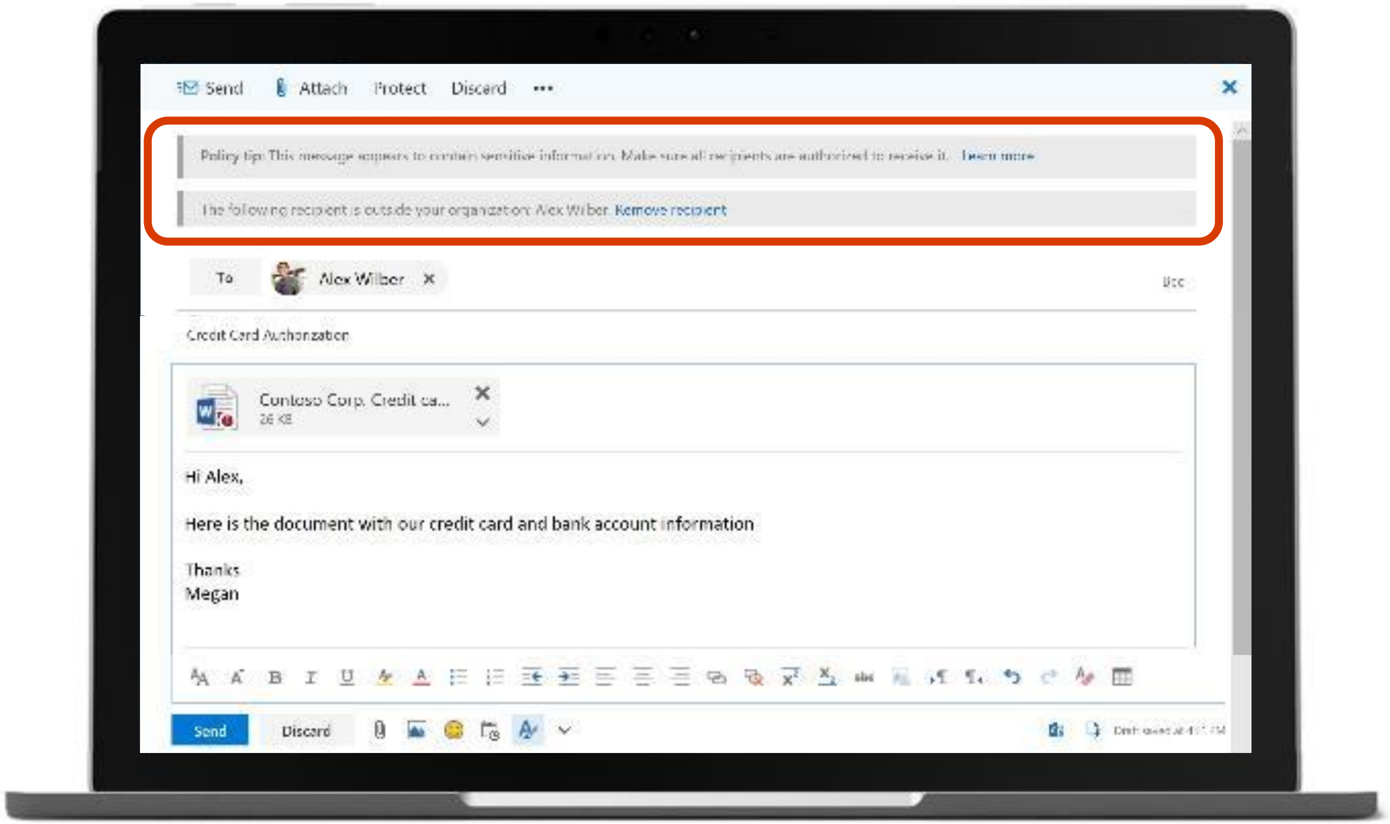
We recommend that you close this web page and not continue to this website. Learn more about Malware

✕ Close this page.

© 2015 Microsoft | Legal | Privacy | Feedback

Safeguard your data:

Protection from data leaks



Policy tip: This message appears to contain sensitive information. Make sure all recipients are authorized to receive it. Learn more

The following recipient is outside your organization: Alex Wilber. Remove recipient

To: Alex Wilber

Credit Card Authorization

Contoso Corp. Credit ca...
26 KB

Hi Alex,

Here is the document with our credit card and bank account information

Thanks
Megan

Apply **data loss prevention policies** to help keep sensitive information from falling into the wrong hands*

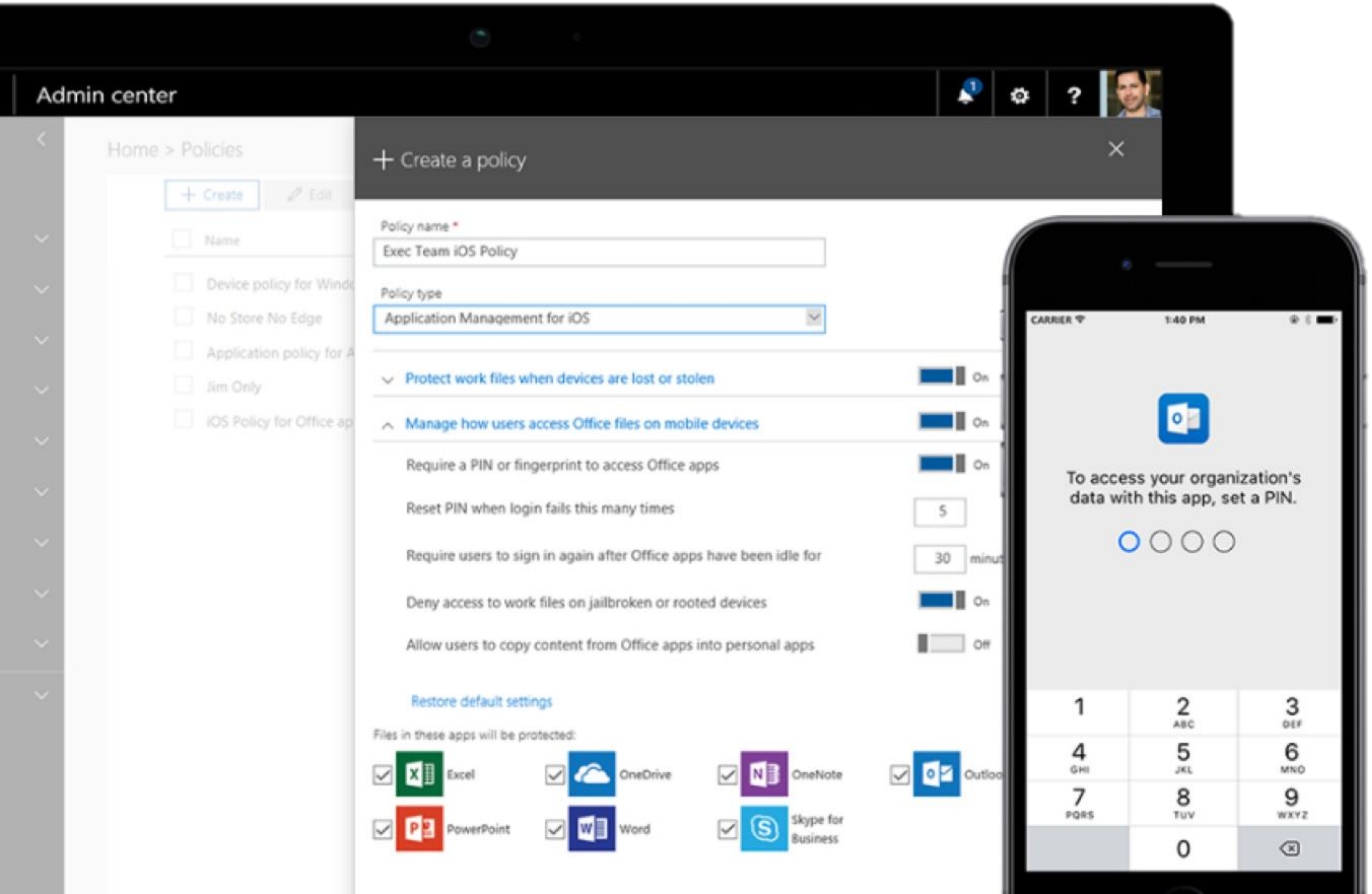
Enforce **BitLocker device encryption to** protect data if a computer is lost or stolen

Manage all your devices—PCs, Mac, iOS, and Android—with full-featured **Intune management**

*Data Loss Prevention will be available in Microsoft 365 Business in summer 2018

Safeguard your data:

Control data access



Admin center

Home > Policies

+ Create / Edit

- □ Name
- □ Device policy for Windo
- □ No Store No Edge
- □ Application policy for A
- □ Jim Only
- □ iOS Policy for Office ap

+ Create a policy

Policy name *: Exec Team iOS Policy

Policy type: Application Management for iOS

Protect work files when devices are lost or stolen — On

Manage how users access Office files on mobile devices — On

Require a PIN or fingerprint to access Office apps — On

Reset PIN when login fails this many times — 5

Require users to sign in again after Office apps have been idle for — 30 minut

Deny access to work files on jailbroken or rooted devices — On

Allow users to copy content from Office apps into personal apps — Off

Restore default settings

Files in these apps will be protected:

- ☑ Excel
- ☑ OneDrive
- ☑ OneNote
- ☑ Outloo
- ☑ PowerPoint
- ☑ Word
- ☑ Skype for Business

CARRIER 1:40 PM

To access your organization's data with this app, set a PIN.

○ ○ ○ ○

Require PIN or fingerprint to access business documents and data

Remotely wipe business data without affecting personal information

Apply **encryption** and restrictions like **do not forward** to emails and documents

Email archiving and retention

Preserve

In-Place Archive

Secondary mailbox with separate quota

Managed through EAC or PowerShell

Available on-premises, online, or through EOA

Governance

Automated and time-based criteria

Set policies at item or folder level

Expiration date shown in email message

Hold

Capture deleted and edited email messages

Time-Based In-Place Hold

Granular Query-Based In-Place Hold

Optional notification

Search

eDiscovery

Web-based eDiscovery Center and multi-mailbox search

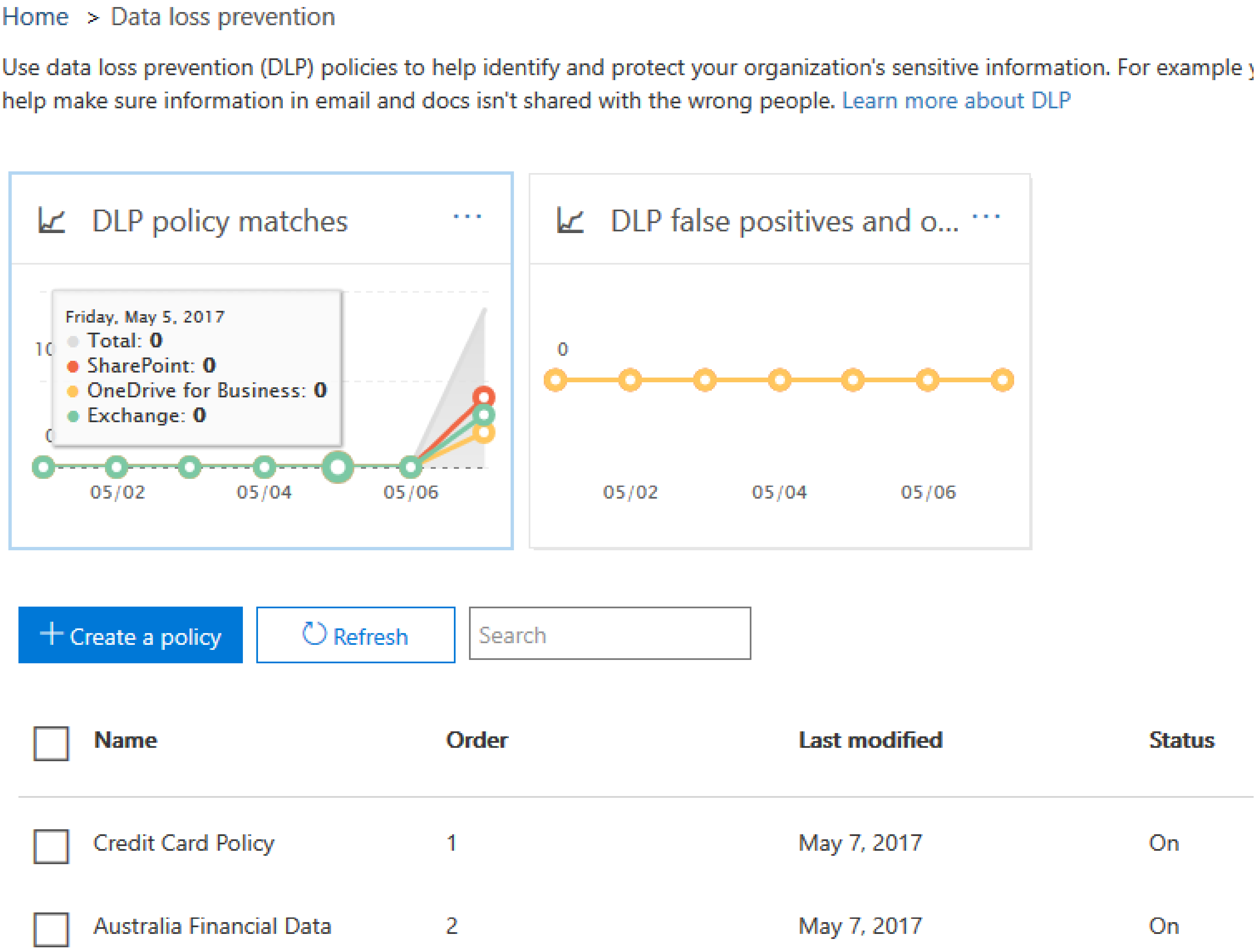
Search primary, In-Place Archive, and recoverable items

Delegate through roles-based administration

De-duplication after discovery

Auditing to ensure controls are met

Data Loss Prevention (DLP)



Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive information. For example y help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP

Friday, May 5, 2017
● Total: **0**
● SharePoint: **0**
● OneDrive for Business: **0**
● Exchange: **0**

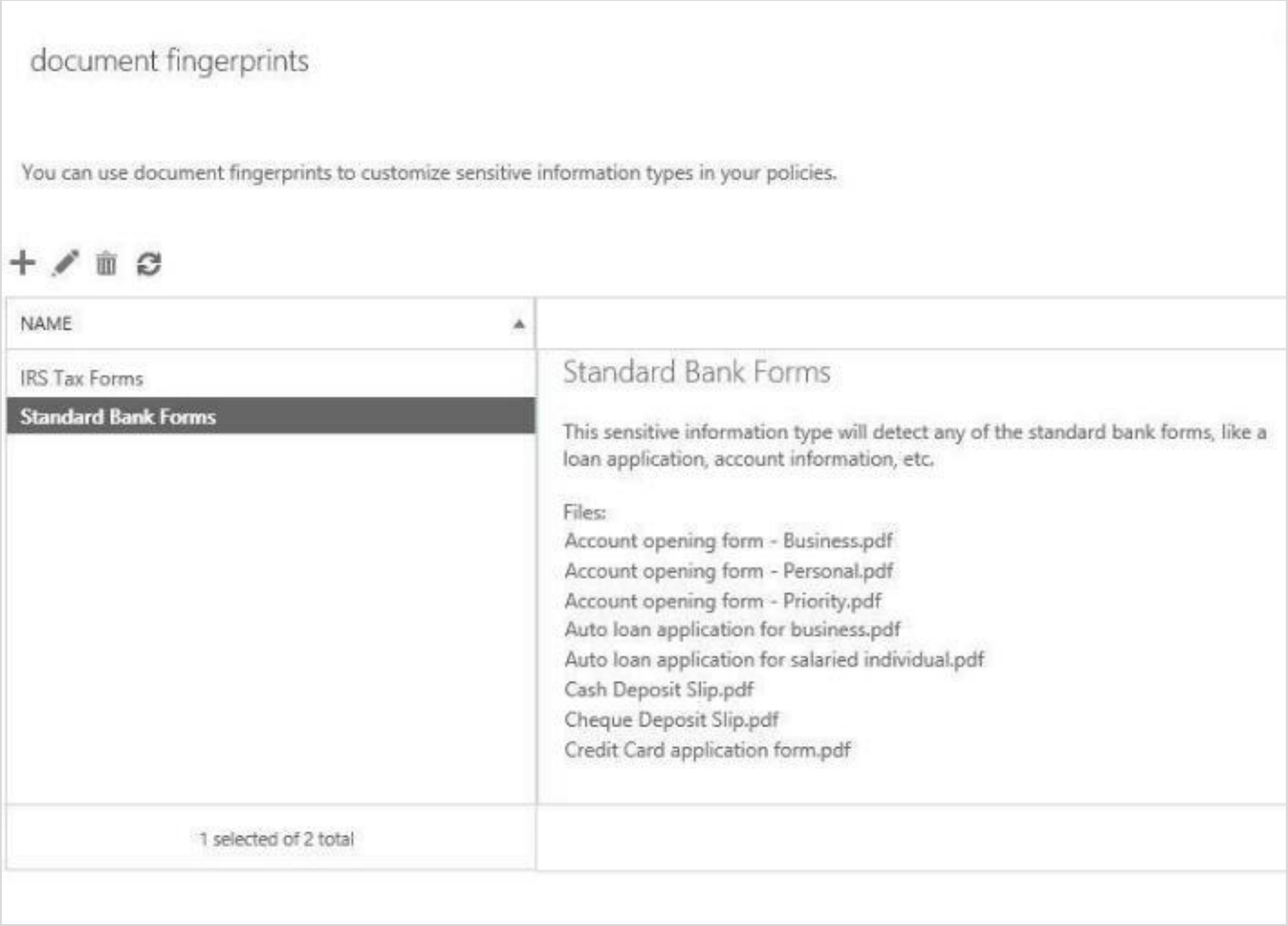
□	Name	Order	Last modified	Status
□	Credit Card Policy	1	May 7, 2017	On
□	Australia Financial Data	2	May 7, 2017	On

DLP document fingerprinting

Scan email and attachments to look for patterns that match document templates

Protect sensitive documents from being accidently shared outside your organization

No coding required; simply upload sample documents to create fingerprints



document fingerprints

You can use document fingerprints to customize sensitive information types in your policies.

NAME
IRS Tax Forms
Standard Bank Forms

1 selected of 2 total

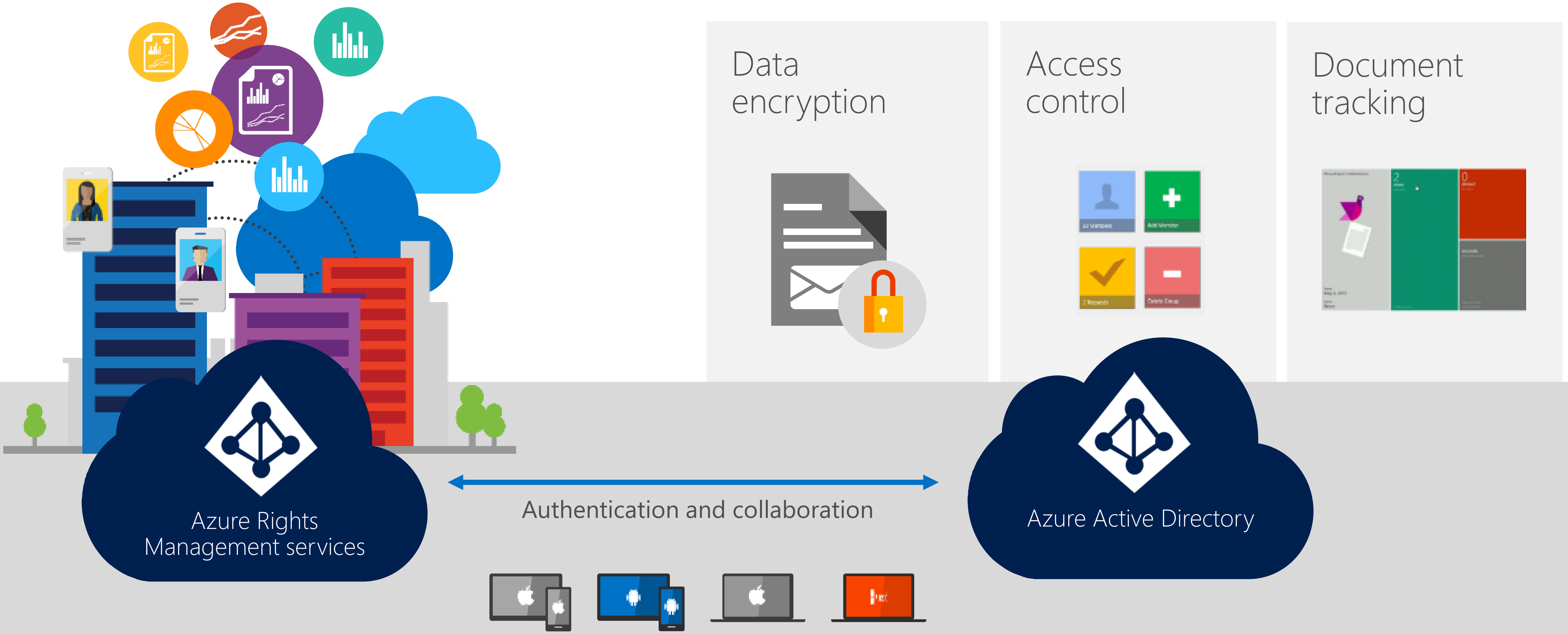
Standard Bank Forms

This sensitive information type will detect any of the standard bank forms, like a loan application, account information, etc.

Files:
Account opening form - Business.pdf
Account opening form - Personal.pdf
Account opening form - Priority.pdf
Auto loan application for business.pdf
Auto loan application for salaried individual.pdf
Cash Deposit Slip.pdf
Cheque Deposit Slip.pdf
Credit Card application form.pdf

Secure collaboration with AIP

Share internally and externally



Data encryption

Access control

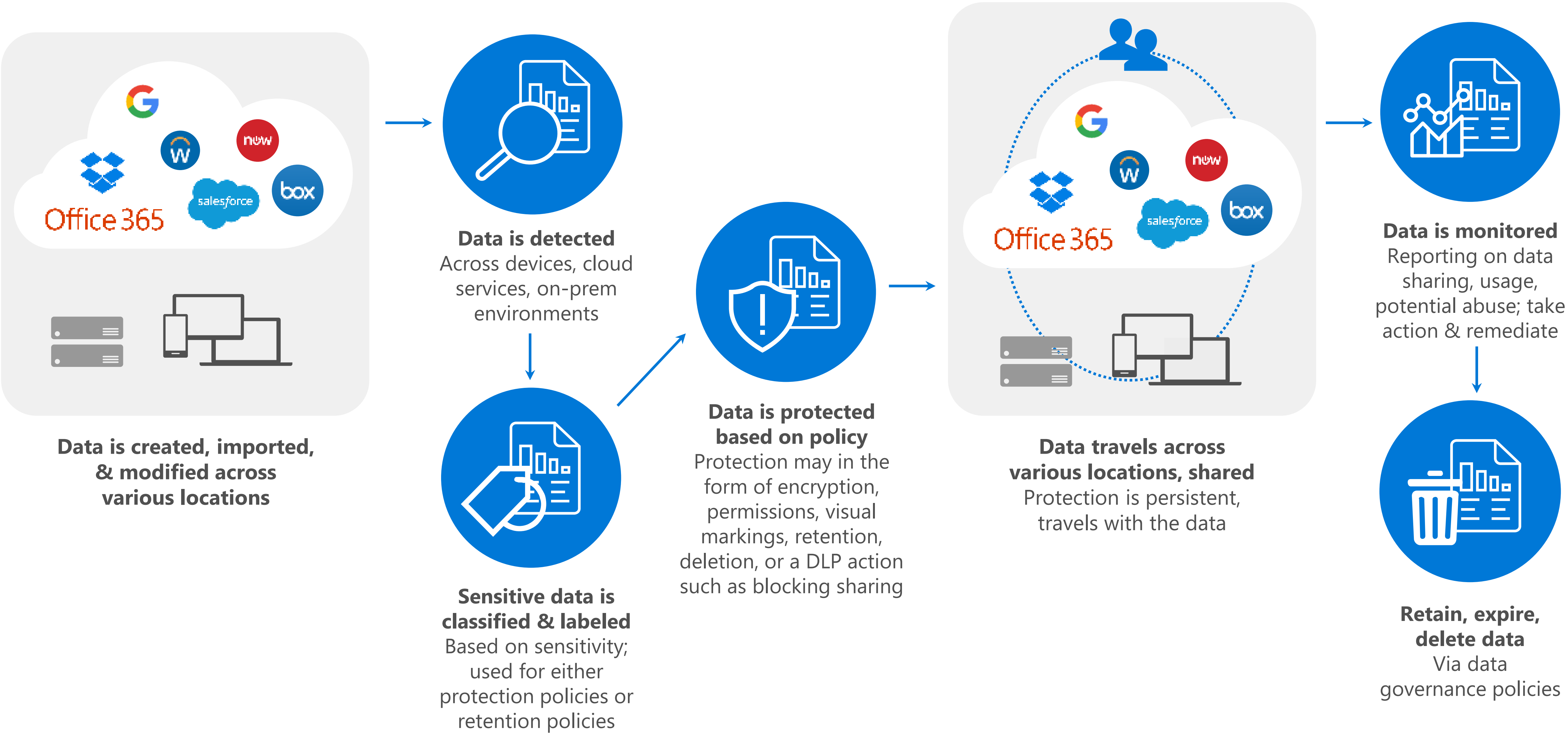
Document tracking

Azure Rights Management services

Authentication and collaboration

Azure Active Directory

Lifecycle of a sensitive document



Data is created, imported, & modified across various locations

Data is detected
Across devices, cloud services, on-prem environments

Sensitive data is classified & labeled
Based on sensitivity; used for either protection policies or retention policies

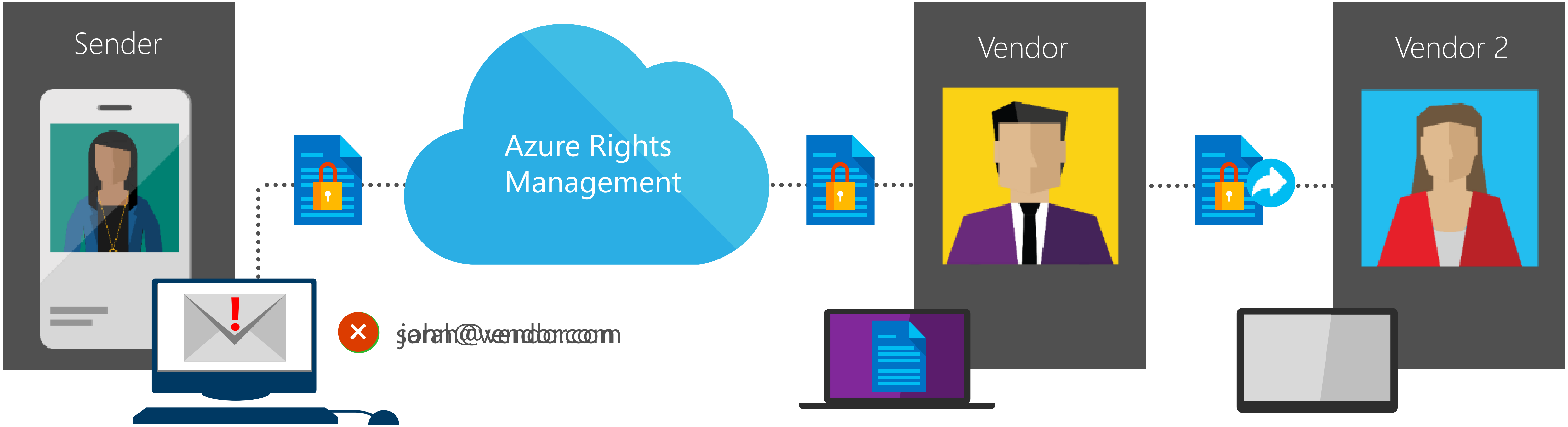
Data is protected based on policy
Protection may in the form of encryption, permissions, visual markings, retention, deletion, or a DLP action such as blocking sharing

Data travels across various locations, shared
Protection is persistent, travels with the data

Data is monitored
Reporting on data sharing, usage, potential abuse; take action & remediate

Retain, expire, delete data
Via data governance policies

Secure collaboration with AIP



☑ Recipient email: john@vendor.com

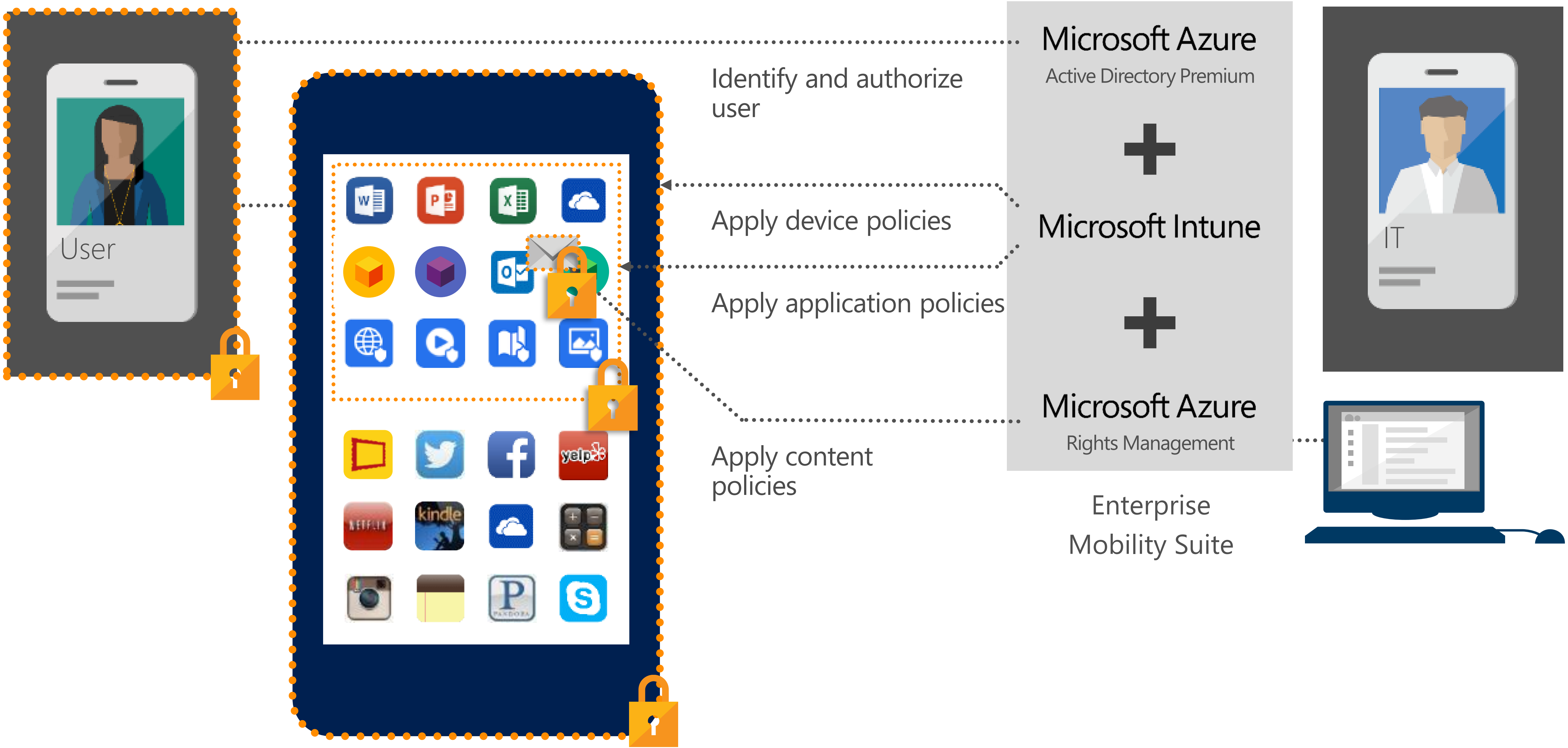
☑ Expiration: 5 days

☑ Email notifications

☑ Permissions: Read only

Mobile Device Management (MDM)

Multiple layers of data protection



Identify and authorize user

Apply device policies

Apply application policies

Apply content policies

Microsoft Azure
Active Directory Premium

+

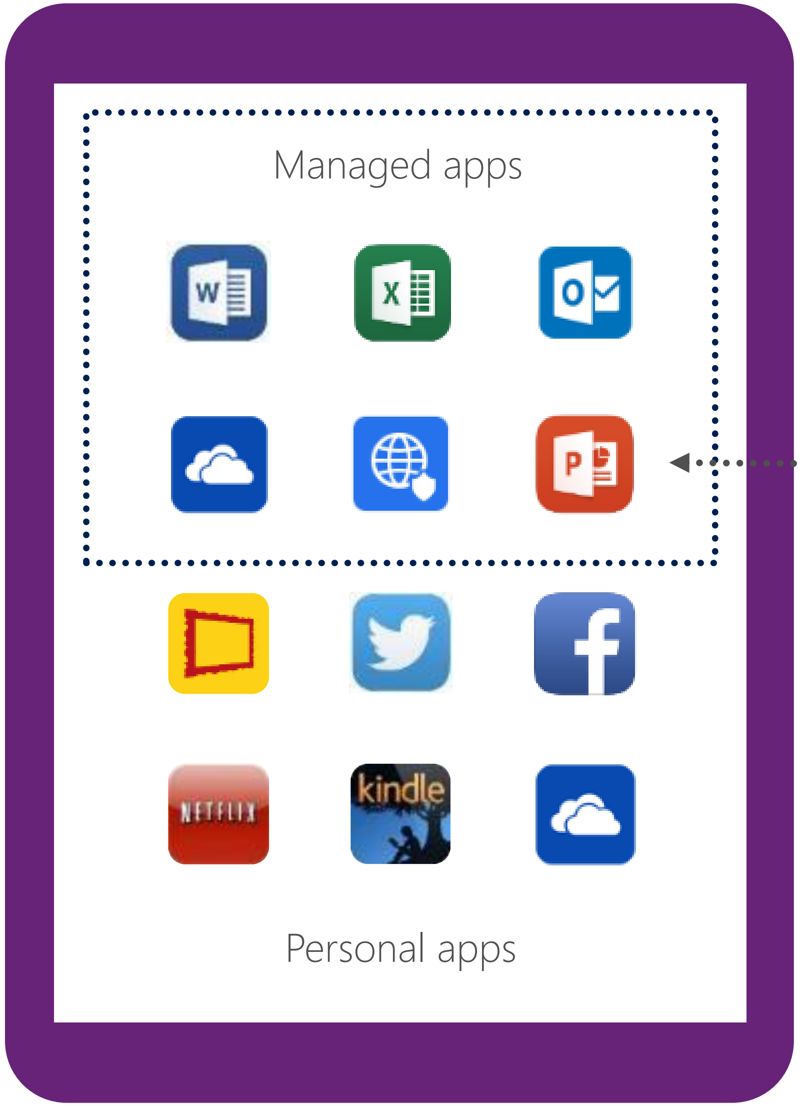
Microsoft Intune

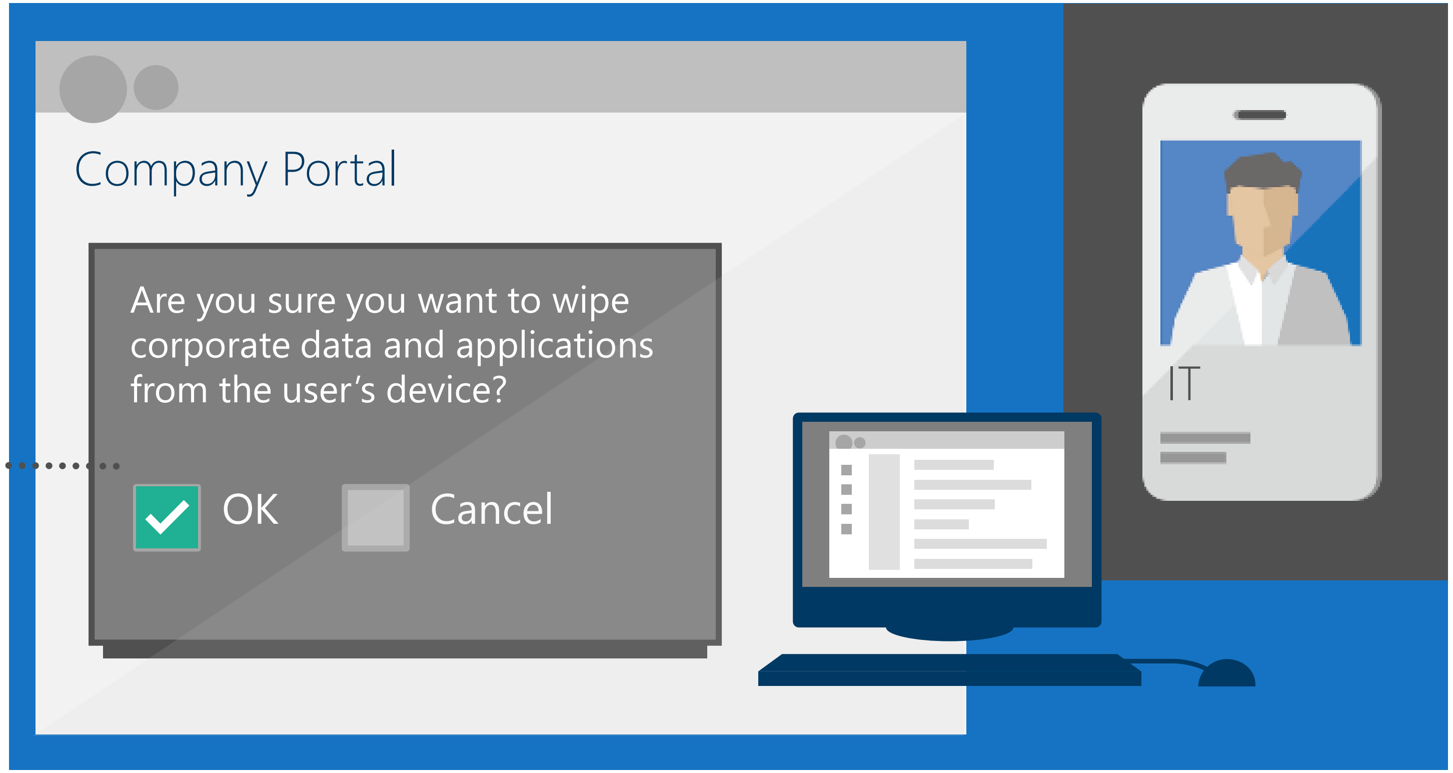
+

Microsoft Azure
Rights Management

Enterprise
Mobility Suite

Selective wipe



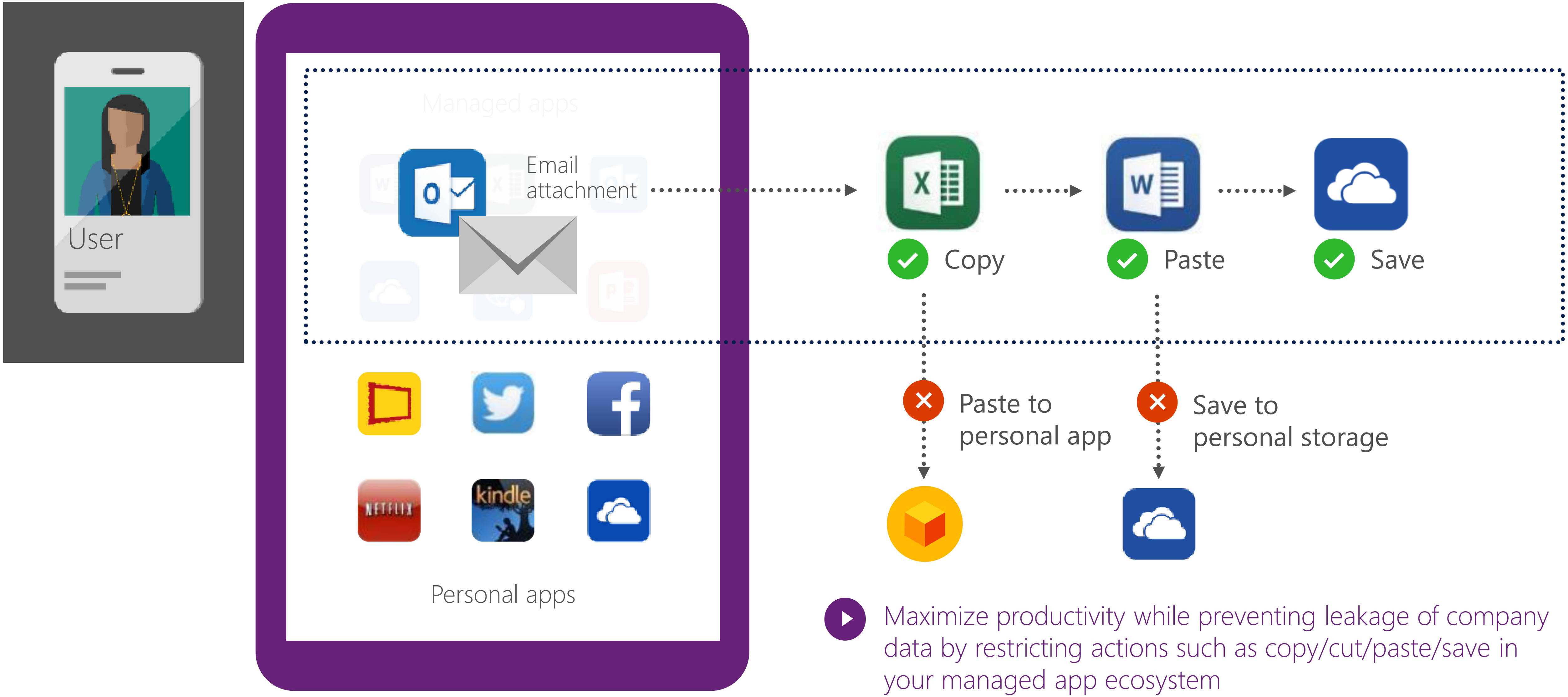


Are you sure you want to wipe corporate data and applications from the user's device?

☑ OK □ Cancel

- Perform selective wipe via self-service company portal or admin console
- Remove managed apps and data
- Keep personal apps and data intact

Mobile application management



User

Managed apps

Email attachment

Copy

Paste

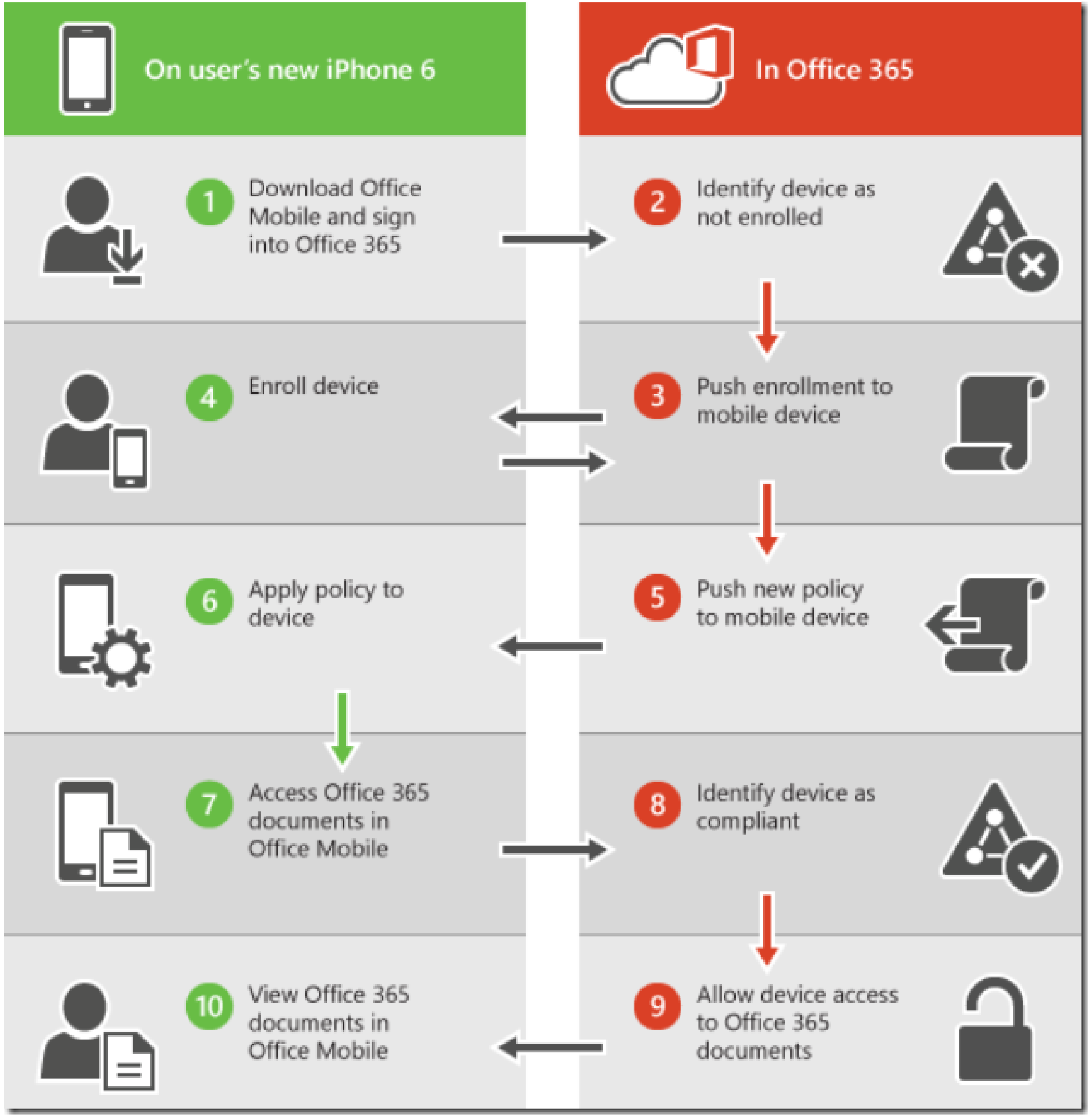
Save

Paste to personal app

Save to personal storage

Personal apps

Maximize productivity while preventing leakage of company data by restricting actions such as copy/cut/paste/save in your managed app ecosystem


On user's new iPhone 6
In Office 365
1 Download Office Mobile and sign into Office 365
2 Identify device as not enrolled
3 Push enrollment to mobile device
4 Enroll device
5 Push new policy to mobile device
6 Apply policy to device
7 Access Office 365 documents in Office Mobile
8 Identify device as compliant
9 Allow device access to Office 365 documents
10 View Office 365 documents in Office Mobile

Hold and eDiscovery

eDiscovery and In-Place Hold in Office 365

Integrated tools to help you preserve, expire, and discover data

Hold

Keep the data you do want

- Data Held In-Place
- Customize holds based on filters
- Hold across multiple products in a single action
- Capture deleted & edited messages

Deletion

Delete the data you don't want

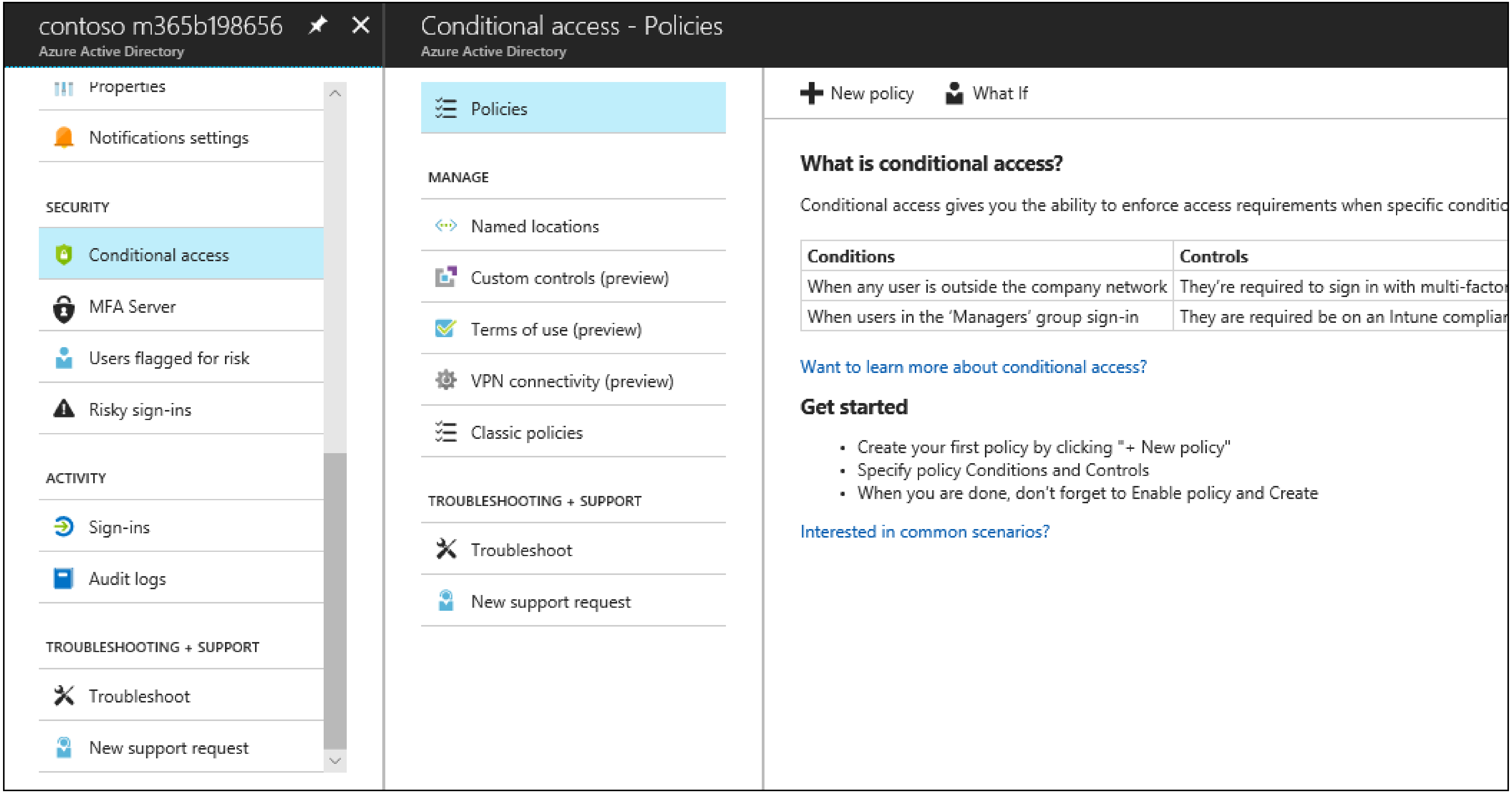
- Automated time-based criteria to delete
- Set policies at item or folder level – admin or user
- Set site level retention polices

Search

Find the data you need

- Search across multiple products
- De-duplication & search statistics
- Case management
- Export search results

Conditional Access



What is conditional access?

Conditional access gives you the ability to enforce access requirements when specific conditio

Conditions	Controls
When any user is outside the company network	They're required to sign in with multi-facto
When users in the 'Managers' group sign-in	They are required be on an Intune complia

Want to learn more about conditional access?

Get started

- Create your first policy by clicking "+ New policy"
- Specify policy Conditions and Controls
- When you are done, don't forget to Enable policy and Create

Interested in common scenarios?

Resources

- Office 365 Trust Center - http://www.abc.net.au/news/2018-03-15/sensitive-data-stolen-from-global-shipping-company-svitzer/9552600
- Office 365 Compliance - https://technet.microsoft.com/en-au/library/office-365-compliance.aspx
- Overview of DLP - https://support.office.com/en-us/article/Overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e
- Create a DLP policy from a template - https://support.office.com/en-us/article/Create-a-DLP-policy-from-a-template-59414438-99f5-488b-975c-5023f2254369
- What the DLP policy template includes - https://support.office.com/en-us/article/What-the-DLP-policy-templates-include-c2e588d3-8f4f-4937-a286-8c399f28953a
- Office 365 Advanced Threat Protection - https://support.office.com/en-us/article/office-365-advanced-threat-protection-e100fe7c-f2a1-4b7d-9e08-622330b83653

CIAOPS Resources

- Blog – http://blog.ciaops.com
- Free SharePoint Training via email – http://bit.ly/cia-gs-spo
- Free Office 365, Azure Administration newsletter – http://bit.ly/cia-o365-tech
- Free Office 365, Azure video tutorials – http://www.youtube.com/directorciaops
- Free documents, presentations, eBooks – http://docs.com/ciaops
- Office 365, Azure, Cloud podcast – http://ciaops.podbean.com
- Office 365, Azure online training courses – http://www.ciaopsacademy.com
- Office 365 and Azure community – http://www.ciaopspatron.com/

Twitter	Facebook	Email	Skype for Business
@directorcia	https://www.facebook.com/ciaops	director@ciaops.com	admin@ciaops365.com

1Q48VMiR152XNuDEkfV3khFdiYoBPGH4V4

Support this content via Bitcoin