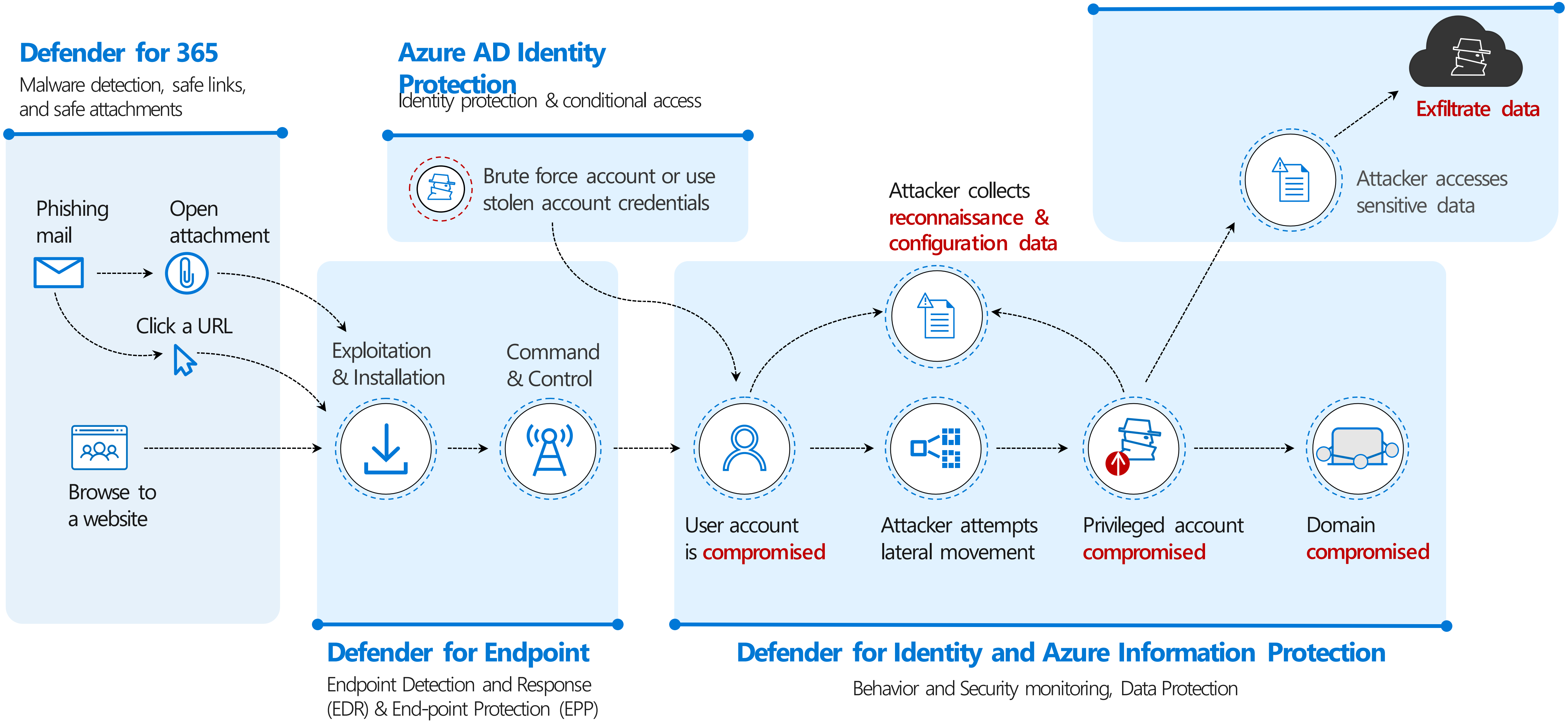
Microsoft 365

Cloud SaaS – A security blind spot?

Terence Lee
Microsoft Hong Kong
Partner Technology Architect

Protection across the attack kill chain



Microsoft Cloud App Security
Extends protection & conditional
access to other cloud apps

Defender for 365
Malware detection, safe links,
and safe attachments

Phishing mail

Open attachment

Click a URL

Browse to a website

Azure AD Identity Protection
Identity protection & conditional access

Brute force account or use stolen account credentials

Exploitation & Installation

Command & Control

User account is compromised

Attacker attempts lateral movement

Privileged account compromised

Domain compromised

Attacker collects reconnaissance & configuration data

Attacker accesses sensitive data

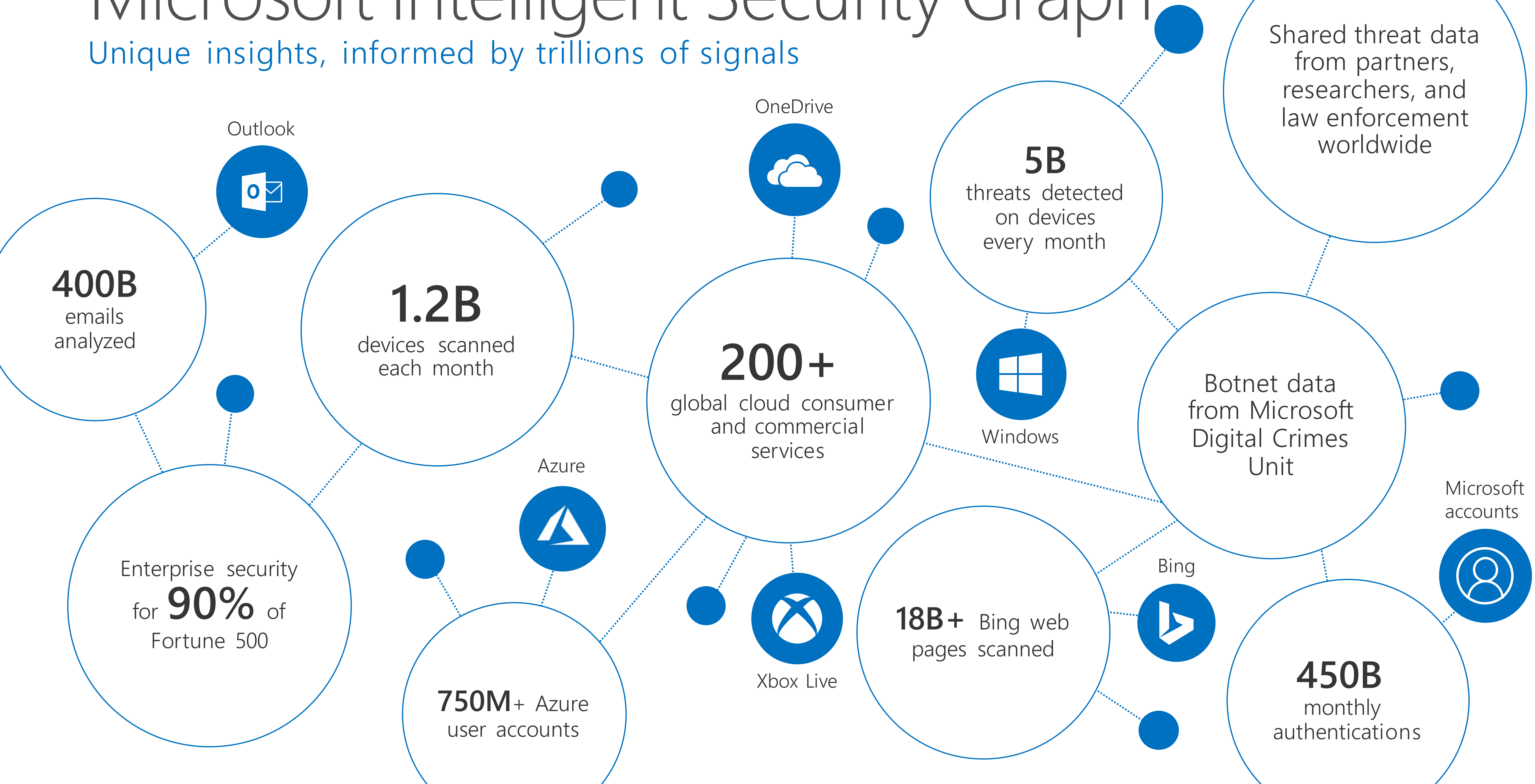
Exfiltrate data

Defender for Endpoint
Endpoint Detection and Response
(EDR) & End-point Protection (EPP)

Defender for Identity and Azure Information Protection
Behavior and Security monitoring, Data Protection

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Outlook

400B emails analyzed

1.2B devices scanned each month

OneDrive

200+ global cloud consumer and commercial services

5B threats detected on devices every month

Shared threat data from partners, researchers, and law enforcement worldwide

Windows

Botnet data from Microsoft Digital Crimes Unit

Enterprise security for **90%** of Fortune 500

Azure

750M+ Azure user accounts

Xbox Live

18B+ Bing web pages scanned

Bing

Microsoft accounts

450B monthly authentications

Gartner Security & Compliance Magic Quadrants

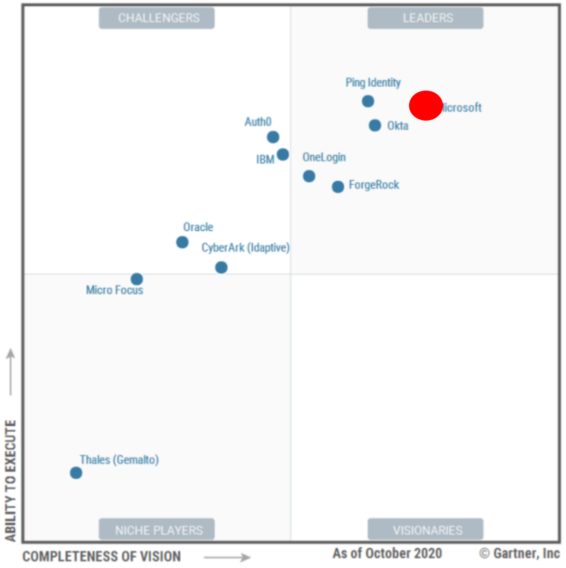
Full Report Links:

- Access Management
- Enterprise Information Archiving
- Unified Endpoint Management Tools
- Endpoint Protection Platforms
- Cloud App Security Brokers

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Microsoft.

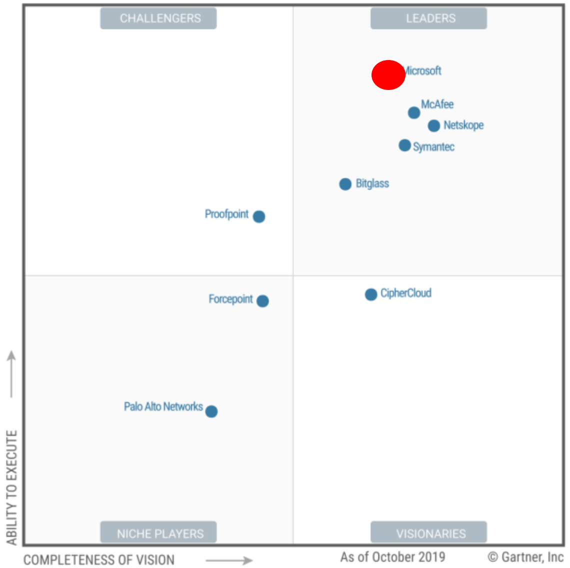
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

ACCESS MANAGEMENT



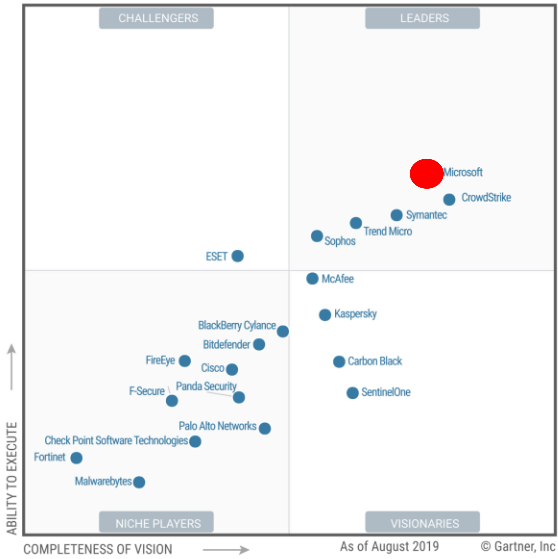
CLOUD ACCESS SECURITY BROKERS

Figure 1. Magic Quadrant for Cloud Access Security Brokers



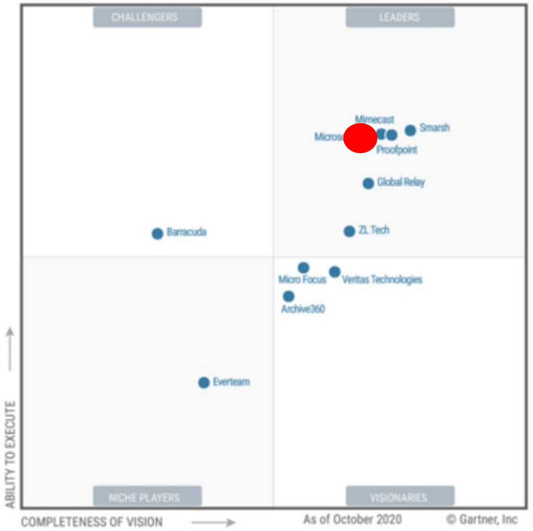
Source: Gartner (October 2019)

ENDPOINT PROTECTION PLATFORMS



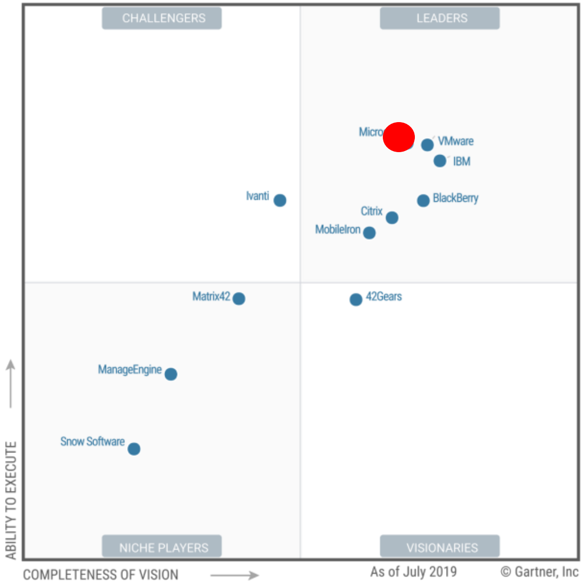
ENTERPRISE INFORMATION ARCHIVING

Figure 1: Magic Quadrant for Enterprise Information Archiving



Source: Gartner (October 2020)

UNIFIED ENDPOINT MANAGEMENT TOOLS



IT challenges of the modern workplace

How do you empower users while
protecting your most important assets?

Employee goals

Collaborate

Easy access

Work
anywhere

IT goals

Protect data

Manage access

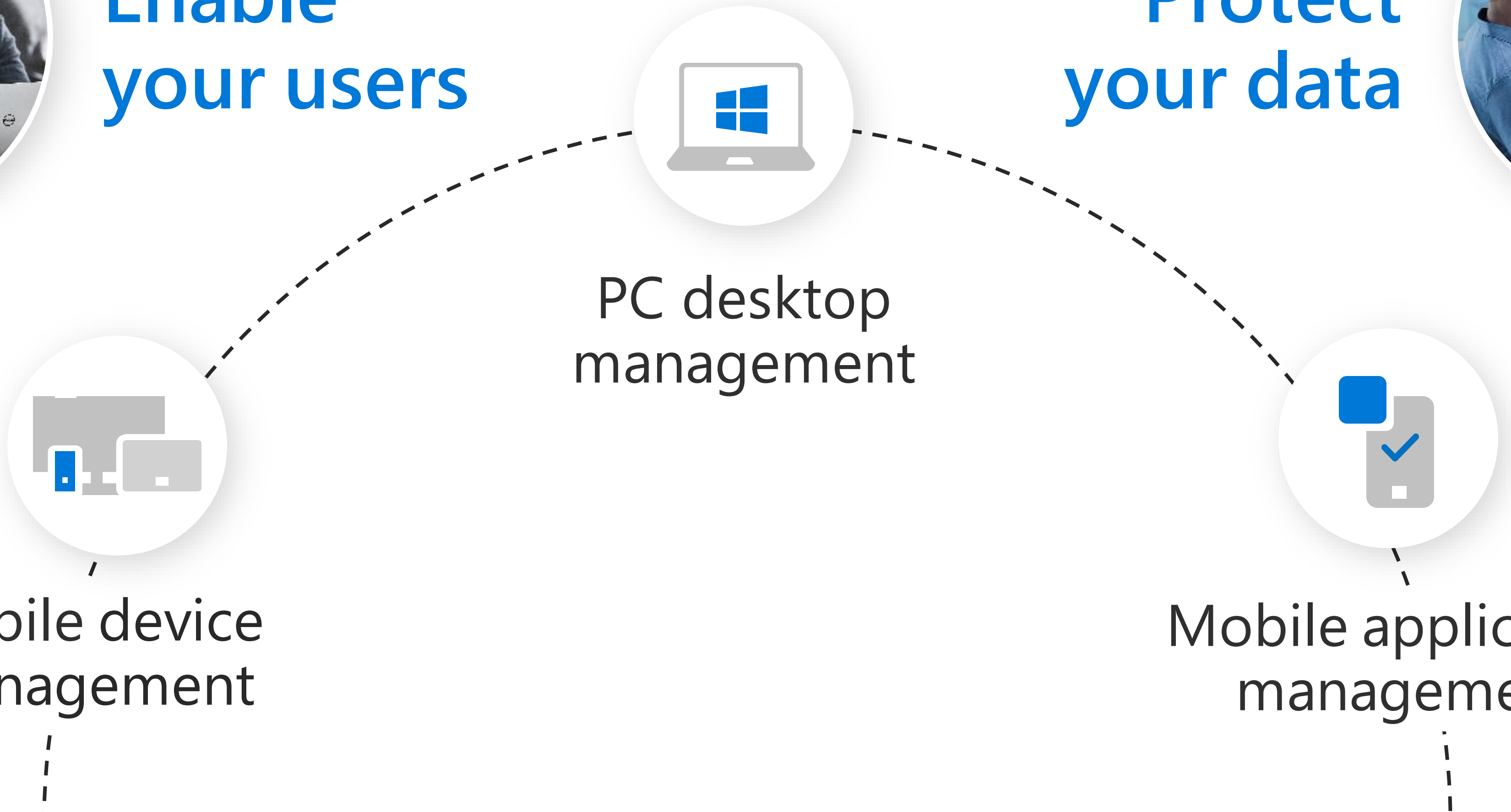
Stay
innovative

Transformative device management and security

Microsoft Unified Endpoint Management

Enable your users

Protect your data



PC desktop management

Mobile device management

Mobile application management

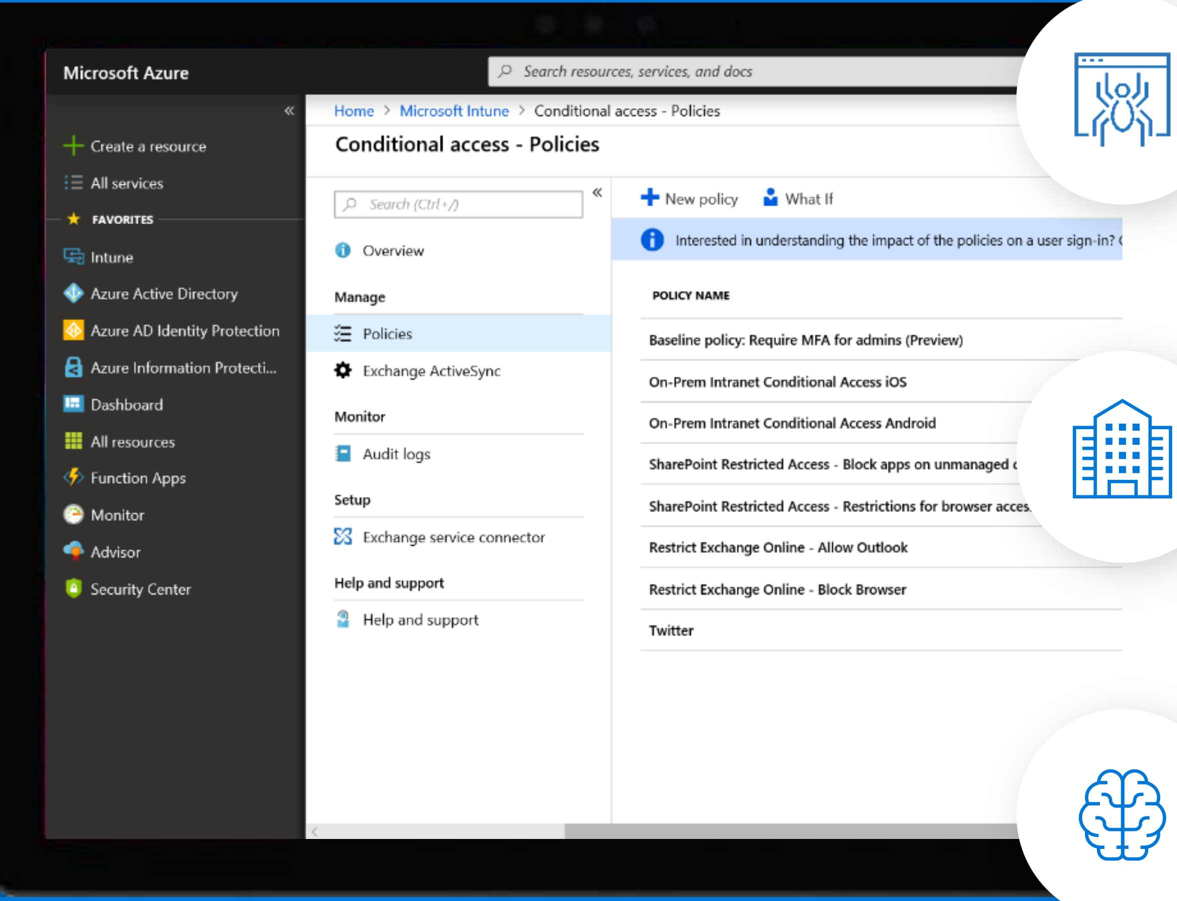
Transform IT delivery and device management

Zero-touch IT provisioning for all devices using Windows Autopilot, Apple Business Manager, or Android Enterprise

App lifecycle management for in-house (LOB) apps, public store apps, and traditional Win32 apps

Depth of **configuration and security controls** across any device

Secure apps and data in the modern workplace



Microsoft Azure

Search resources, services, and docs

Create a resource
All services
FAVORITES
Intune
Azure Active Directory
Azure AD Identity Protection
Azure Information Protecti...
Dashboard
All resources
Function Apps
Monitor
Advisor
Security Center

Home > Microsoft Intune > Conditional access - Policies

Conditional access - Policies

Search (Ctrl+/)

Overview

Manage

Policies

Exchange ActiveSync

Monitor

Audit logs

Setup

Exchange service connector

Help and support

Help and support

New policy   What If

Interested in understanding the impact of the policies on a user sign-in?

POLICY NAME
Baseline policy: Require MFA for admins (Preview)
On-Prem Intranet Conditional Access iOS
On-Prem Intranet Conditional Access Android
SharePoint Restricted Access - Block apps on unmanaged d
SharePoint Restricted Access - Restrictions for browser acces
Restrict Exchange Online - Allow Outlook
Restrict Exchange Online - Block Browser
Twitter

Respond to internal and external threats with **real-time risk-analysis** before access to company data

Protect corporate data before, during and after they are shared, even outside the company

Extensive **visibility and intelligent cloud-powered insights** to improve end-to-end security posture

Maximize user productivity

Secure the **data in Office apps** on mobile devices, without management of the devices

Deliver native **app experiences** that work and feel natural on any platform

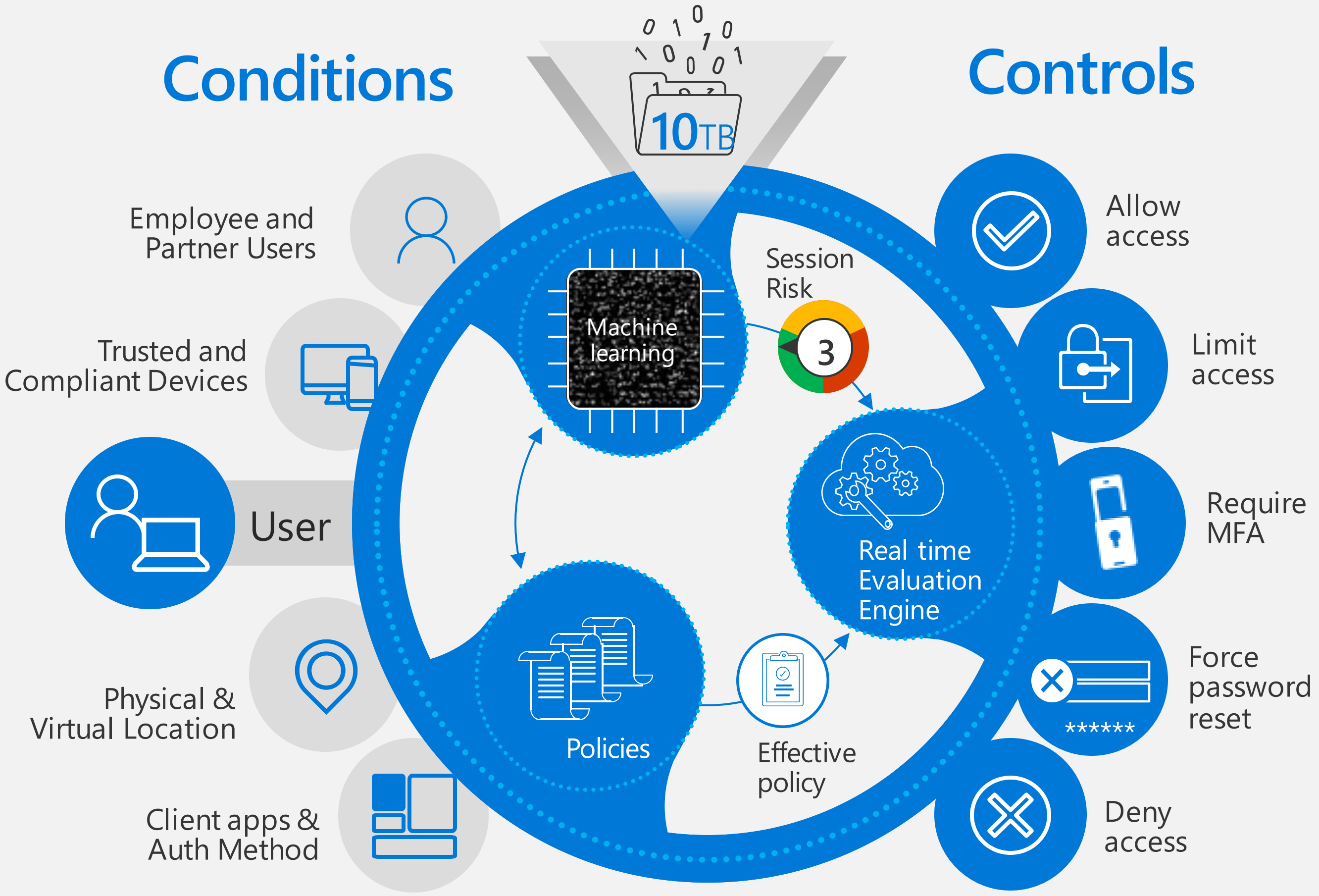
Simplify **access to resources** employees need with single sign-on, for faster service roll-out

Conditional access to data with real-time risk analysis

Define **contextual policies** at the user, location, device, and app levels

Controls adapt to **real time conditions** based on monitoring of perceived risks

Risks calculated based on **advanced Microsoft machine learning**



Manage devices and protect data with Intune

Device security configuration and Remote Actions

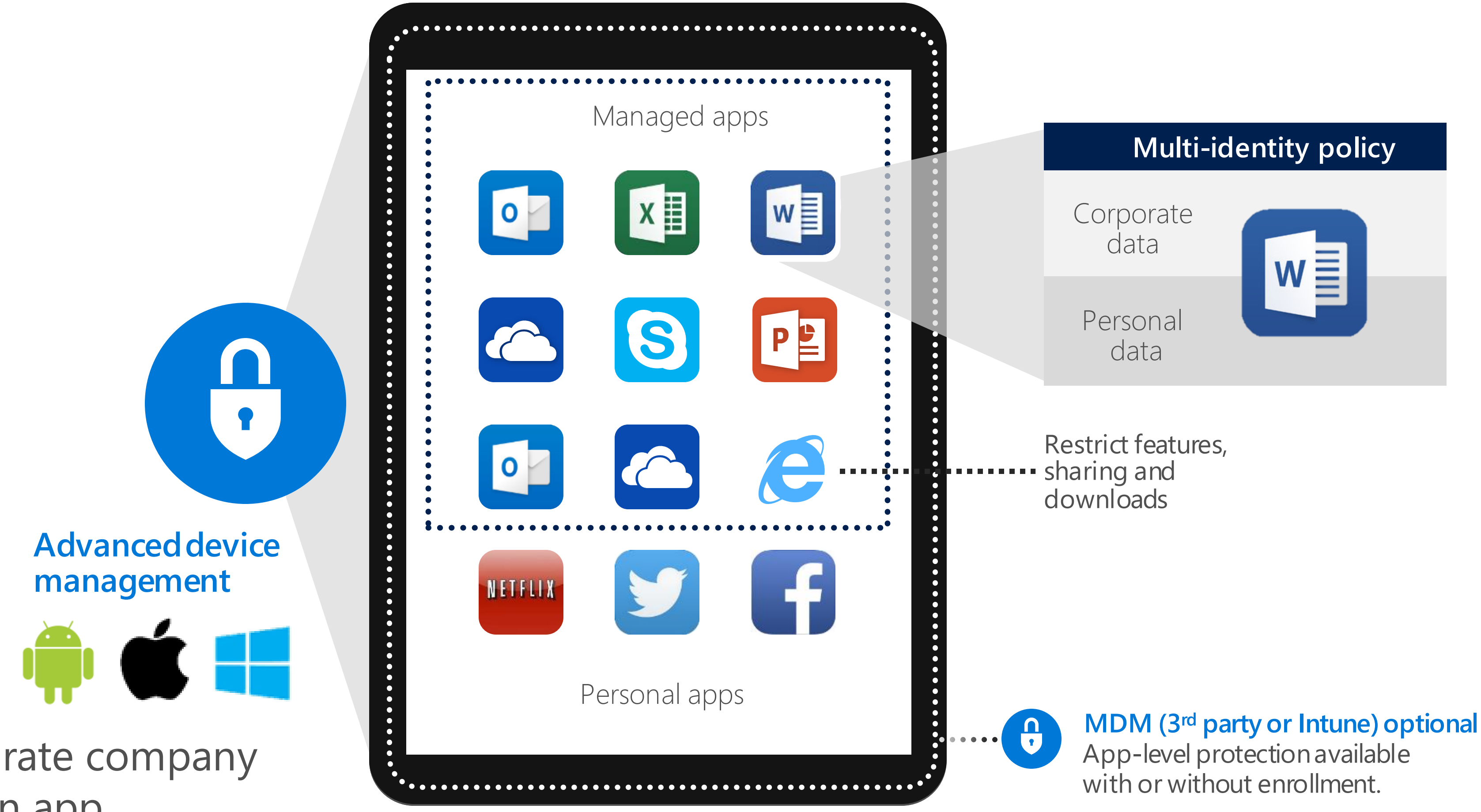
Enforce device encryption, password/PIN requirements, jailbreak/root detection, lock, selective wipe

Data control

Control company data after it has been accessed, and separate it from personal data.

Data separation

Multi-identity allows you to separate company data from personal data within an app.



Advanced device management

Managed apps

Personal apps

Multi-identity policy

Corporate data

Personal data

Restrict features, sharing and downloads

MDM (3rd party or Intune) optional
App-level protection available with or without enrollment.

Microsoft Edge for iOS and Android

Best browser for work and personal

Security

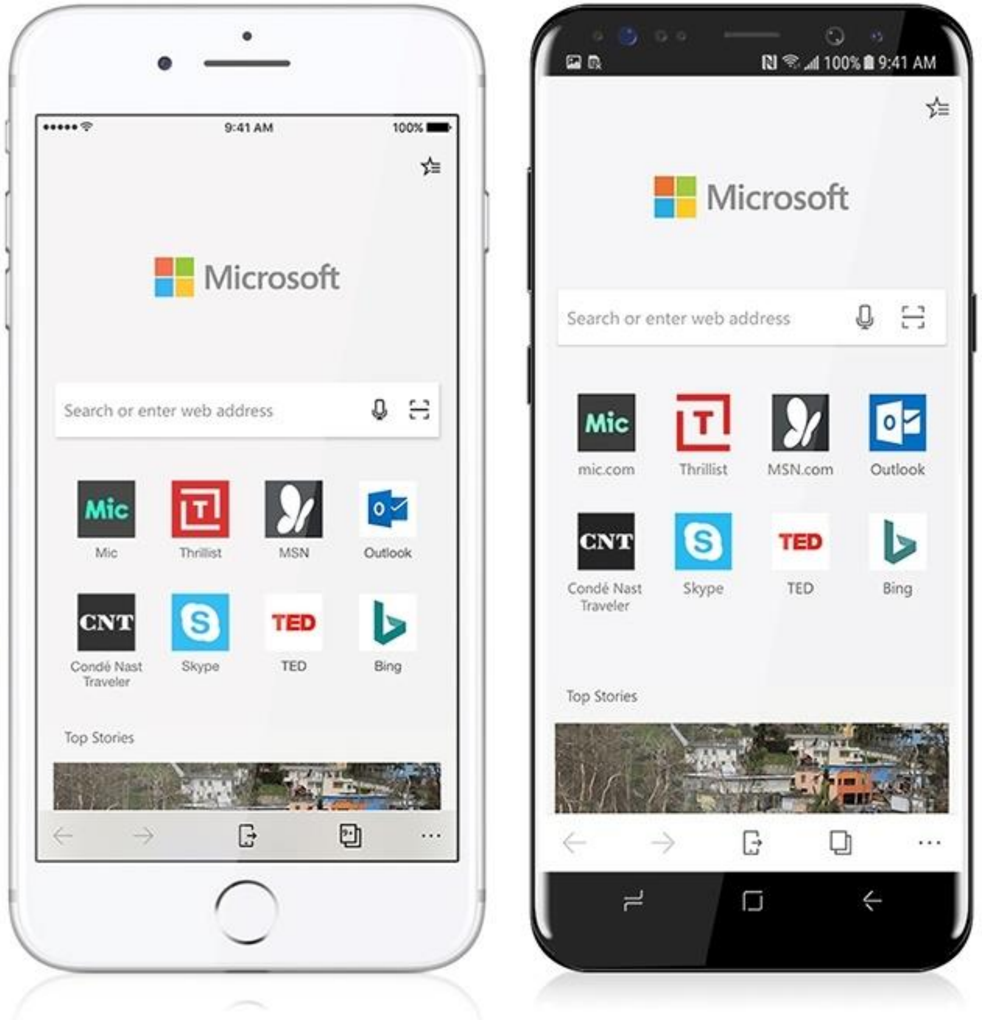
Conditional Access, App Protection Policies

Productivity

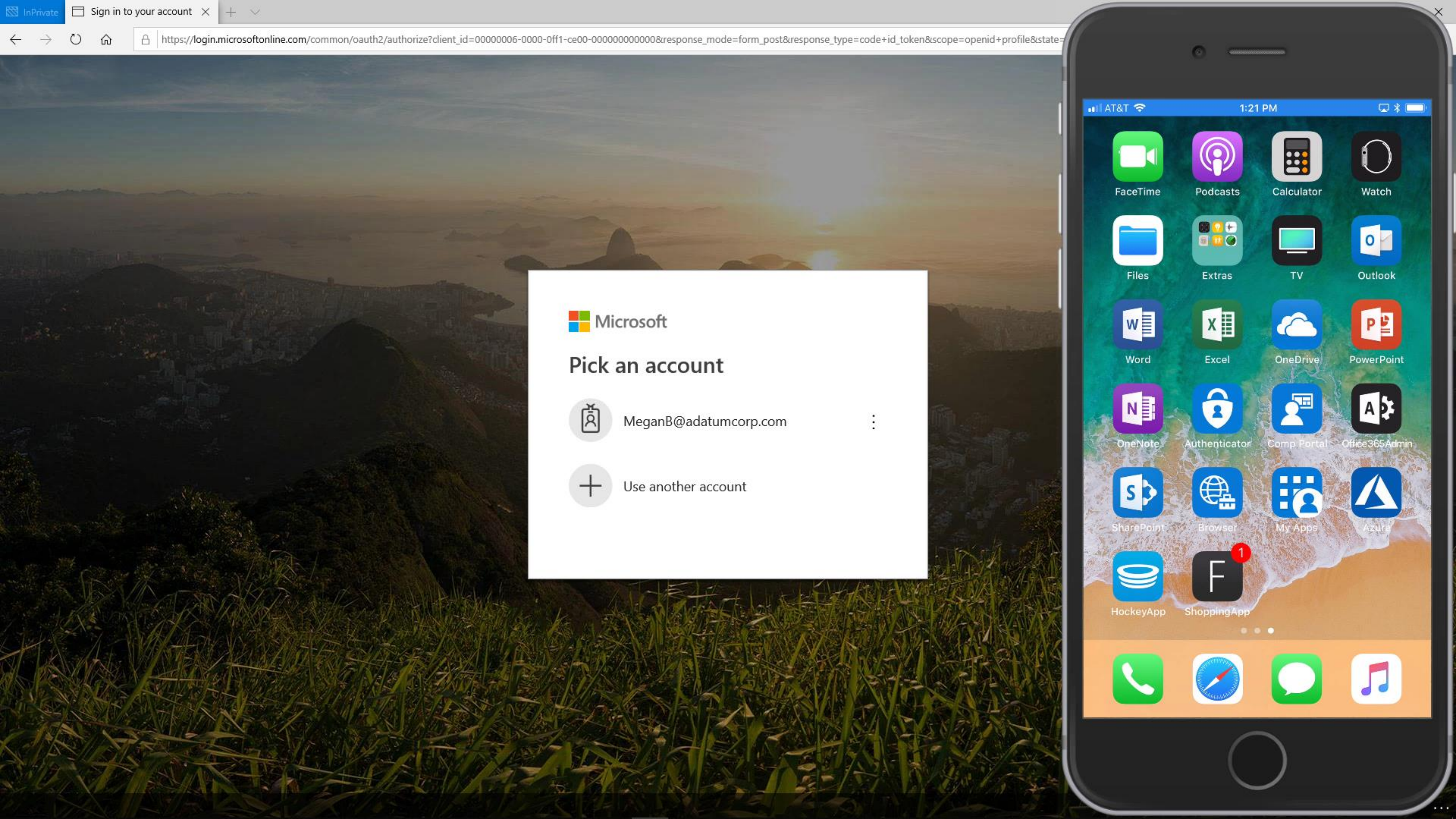
Personal & Corporate Identity Support, App Proxy, SSO

Manageability

Managed Favorites & Home Shortcut, Blocked Sites



Identity Protection



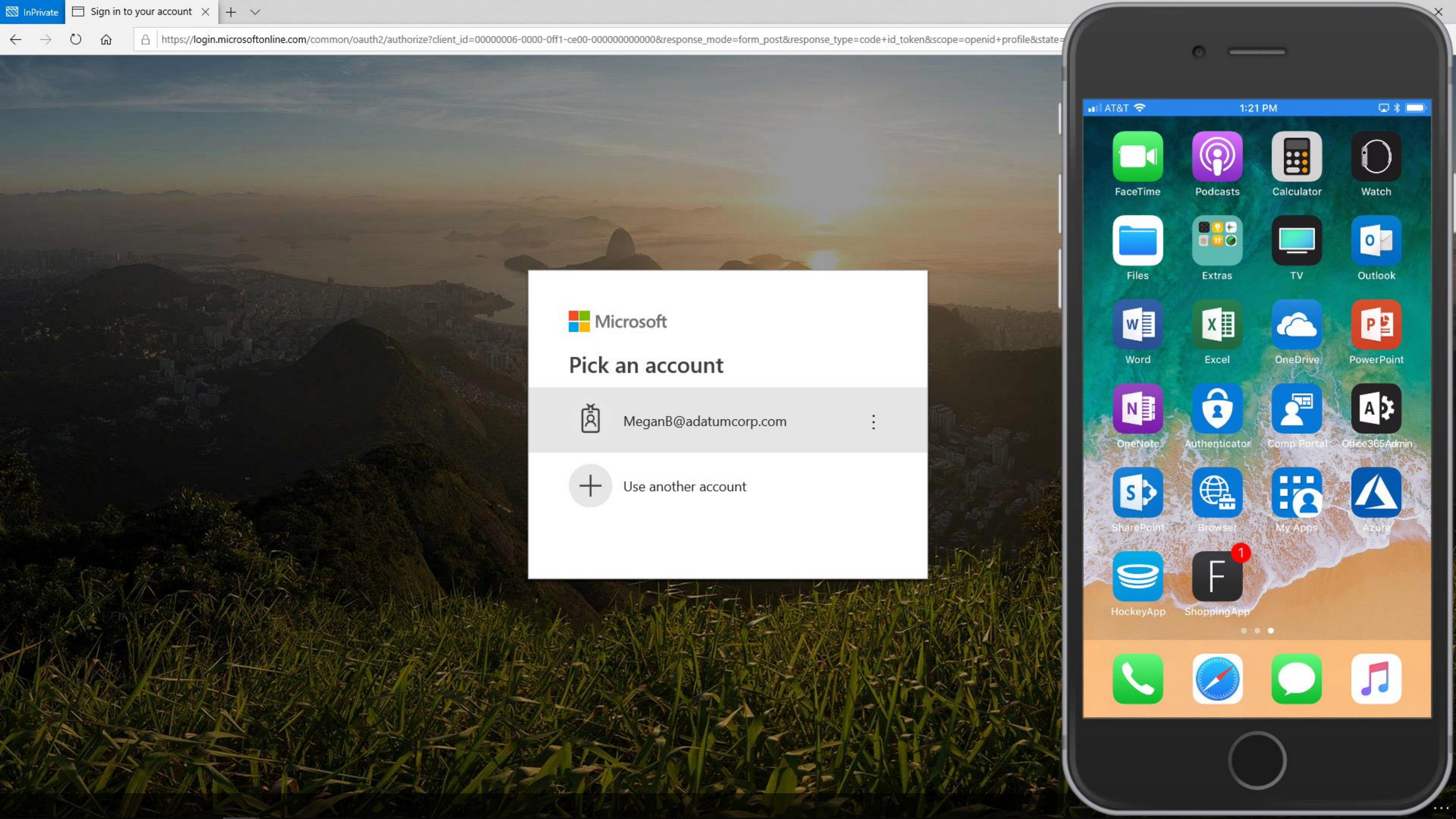
https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000006-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code+id_token&scope=openid+profile&state=

Microsoft

Pick an account

MeganB@adatumcorp.com

Use another account



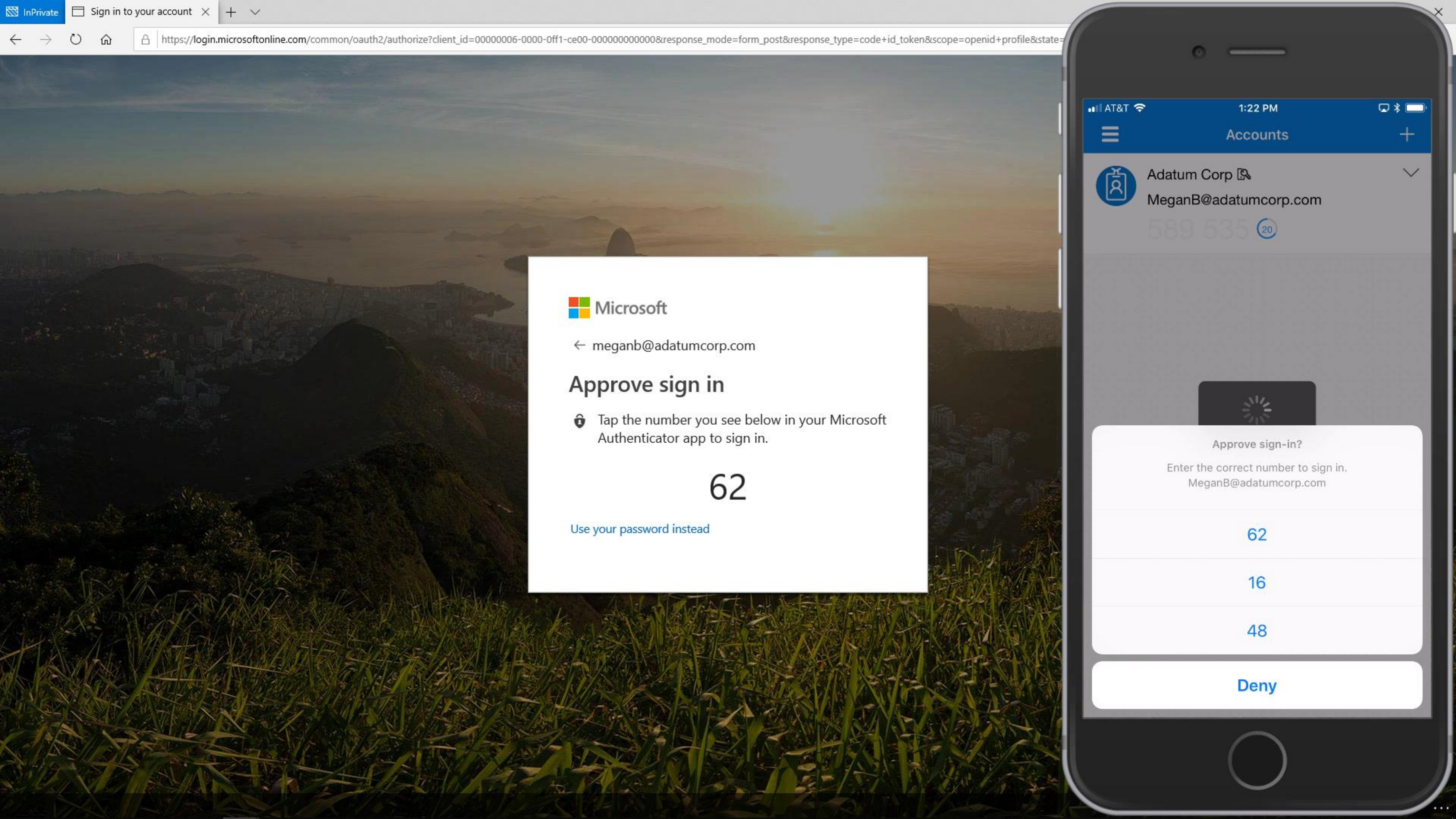
https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000006-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code+id_token&scope=openid+profile&state=

Microsoft

Pick an account

MeganB@adatumcorp.com

Use another account



InPrivate
Sign in to your account
https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000006-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code+id_token&scope=openid+profile&state=
Microsoft
AT&T
1:22 PM
Accounts
Adatum Corp
589 535
20

meganb@adatumcorp.com

Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

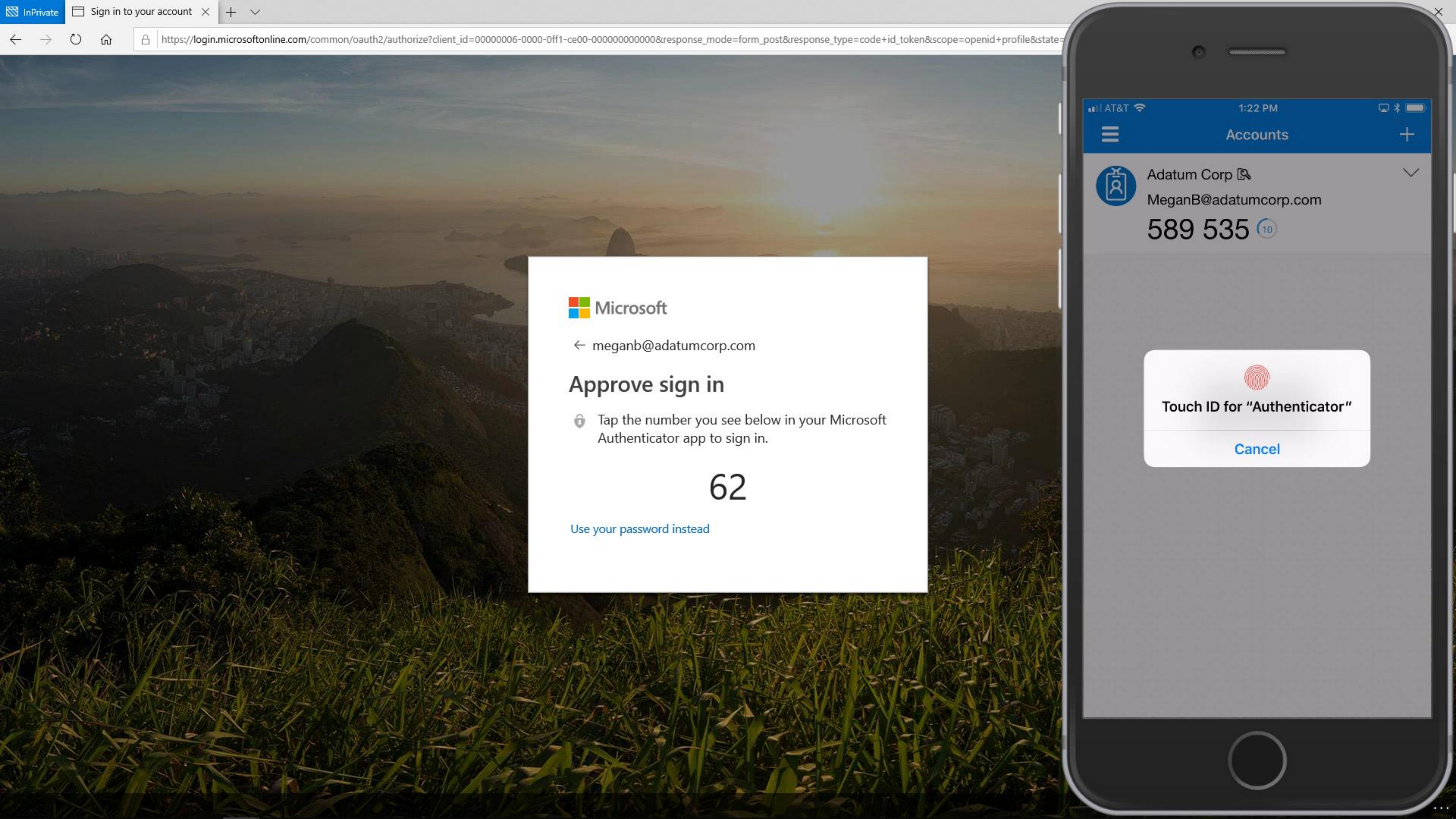
62

Use your password instead

MeganB@adatumcorp.com

Approve sign-in?

Enter the correct number to sign in.
MeganB@adatumcorp.com



https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000006-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code+id_token&scope=openid+profile&state=

← meganb@adatumcorp.com

Approve sign in

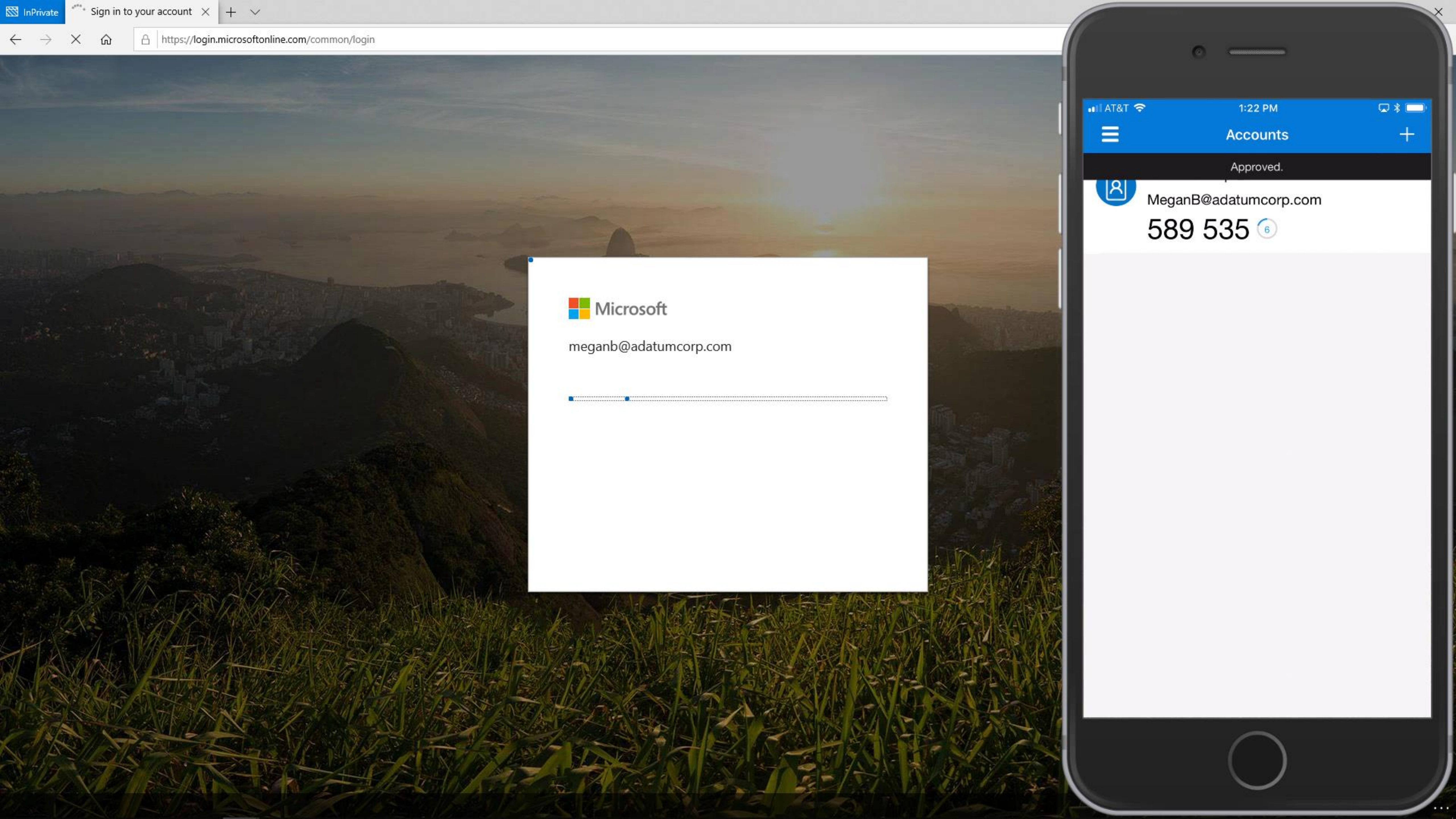
Tap the number you see below in your Microsoft Authenticator app to sign in.

62

Adatum Corp

MeganB@adatumcorp.com

589 535

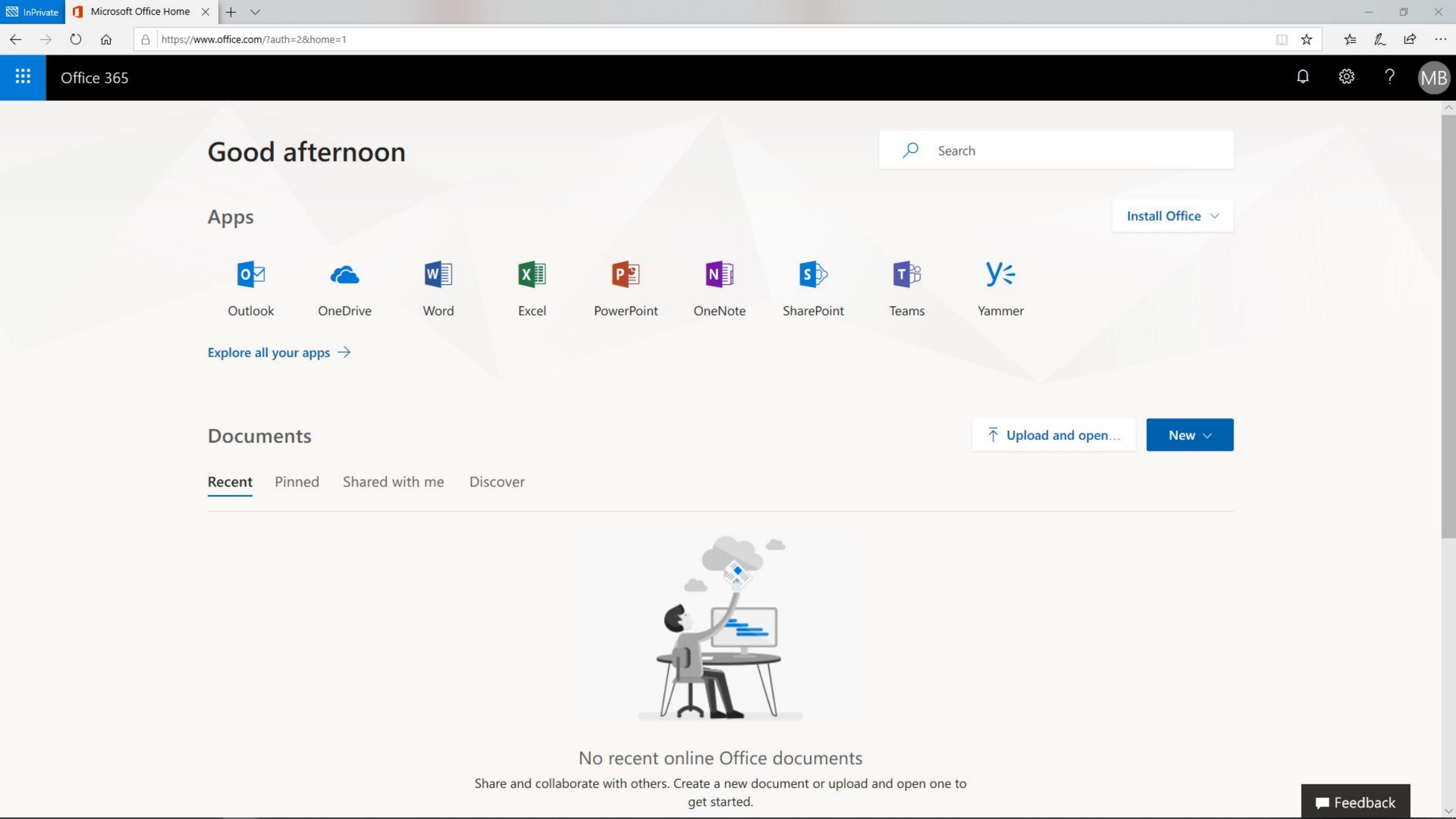


meganb@adatumcorp.com

Approved.

MeganB@adatumcorp.com

589 535



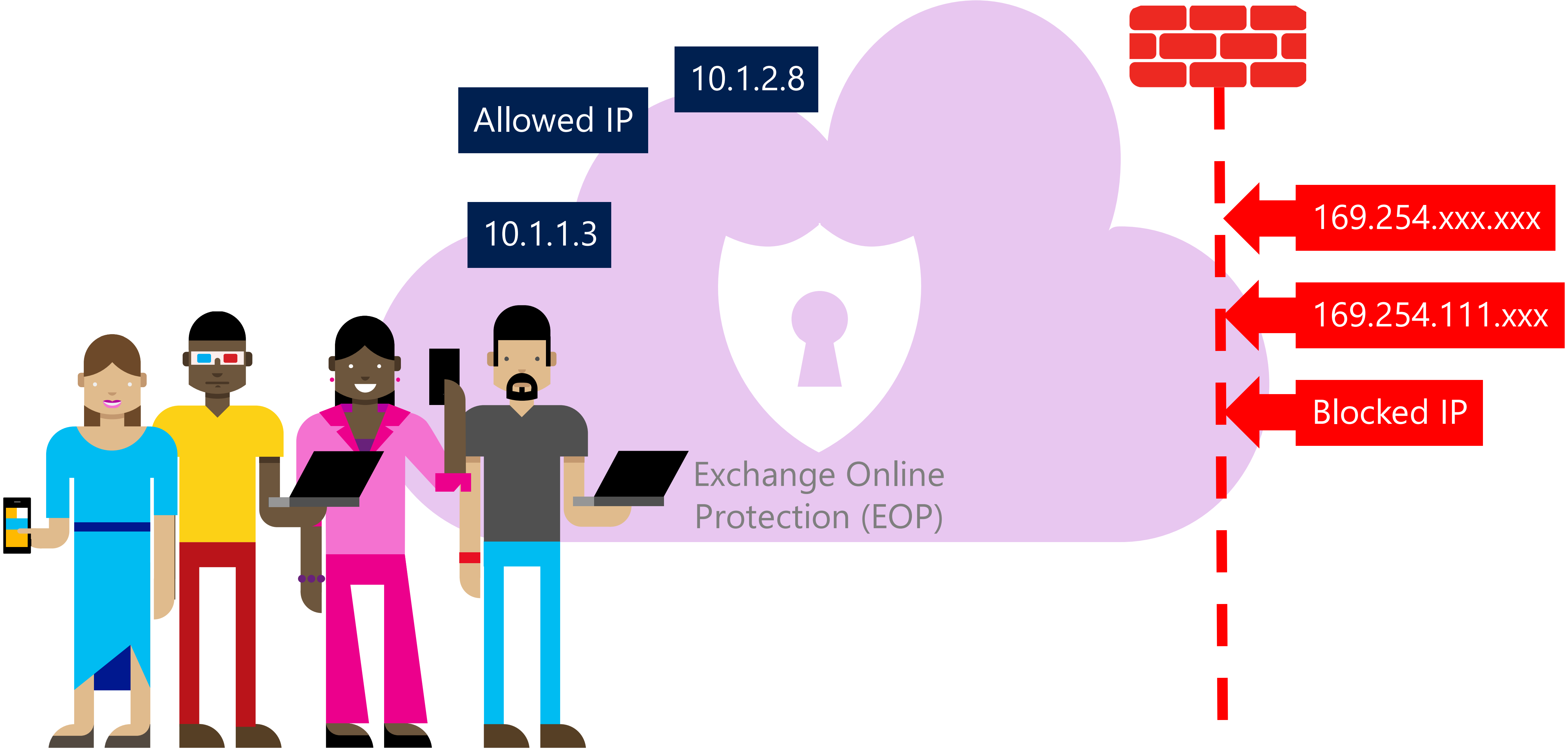
Good afternoon

No recent online Office documents

Share and collaborate with others. Create a new document or upload and open one to get started.

Email Security

Blocking threats at the connection level



Allowed IP

10.1.2.8

10.1.1.3

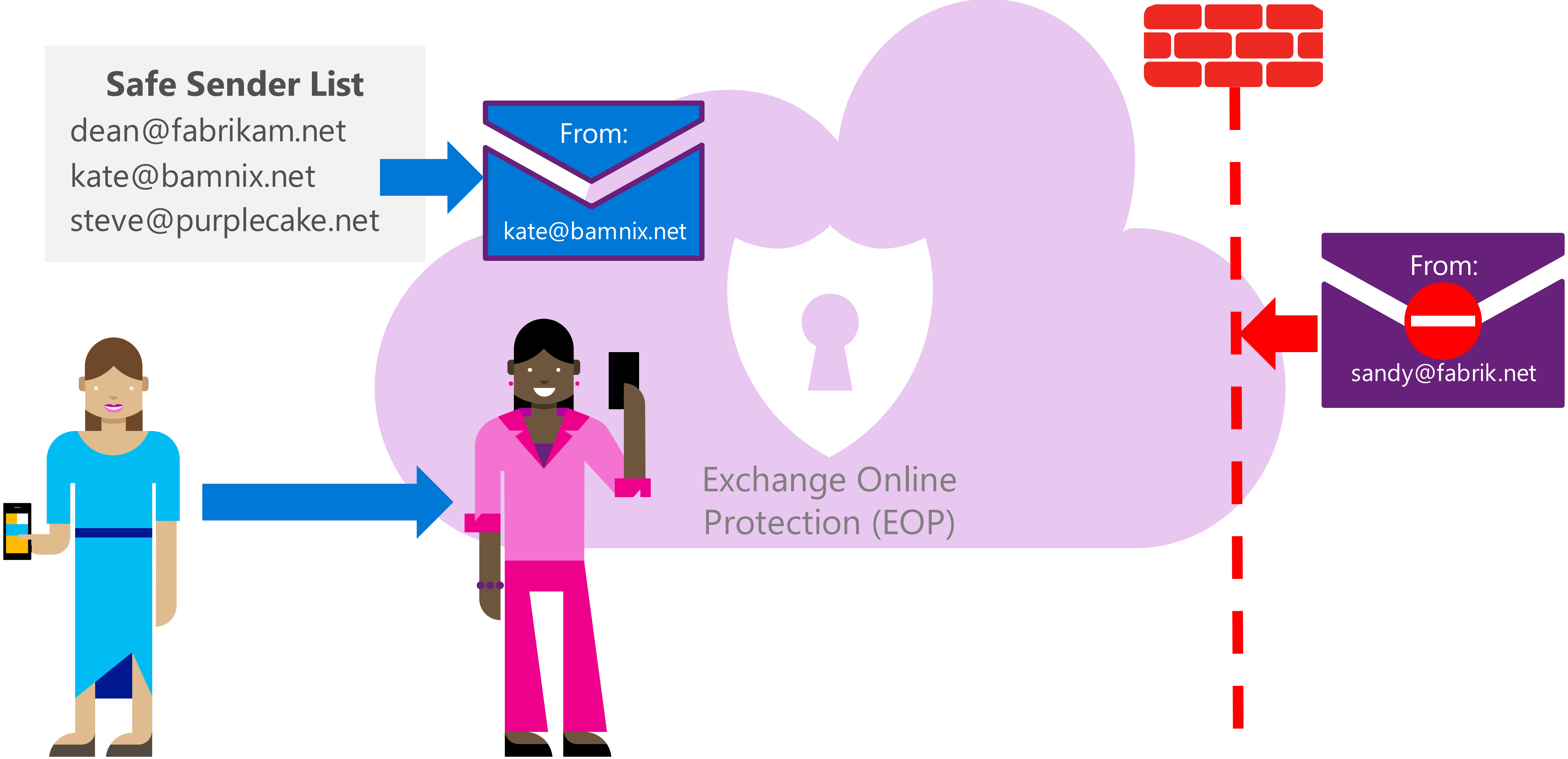
Exchange Online Protection (EOP)

169.254.xxx.xxx

169.254.111.xxx

Blocked IP

Blocking threats at the user level



Safe Sender List

dean@fabrikam.net

kate@bamnix.net

steve@purplecake.net

From:

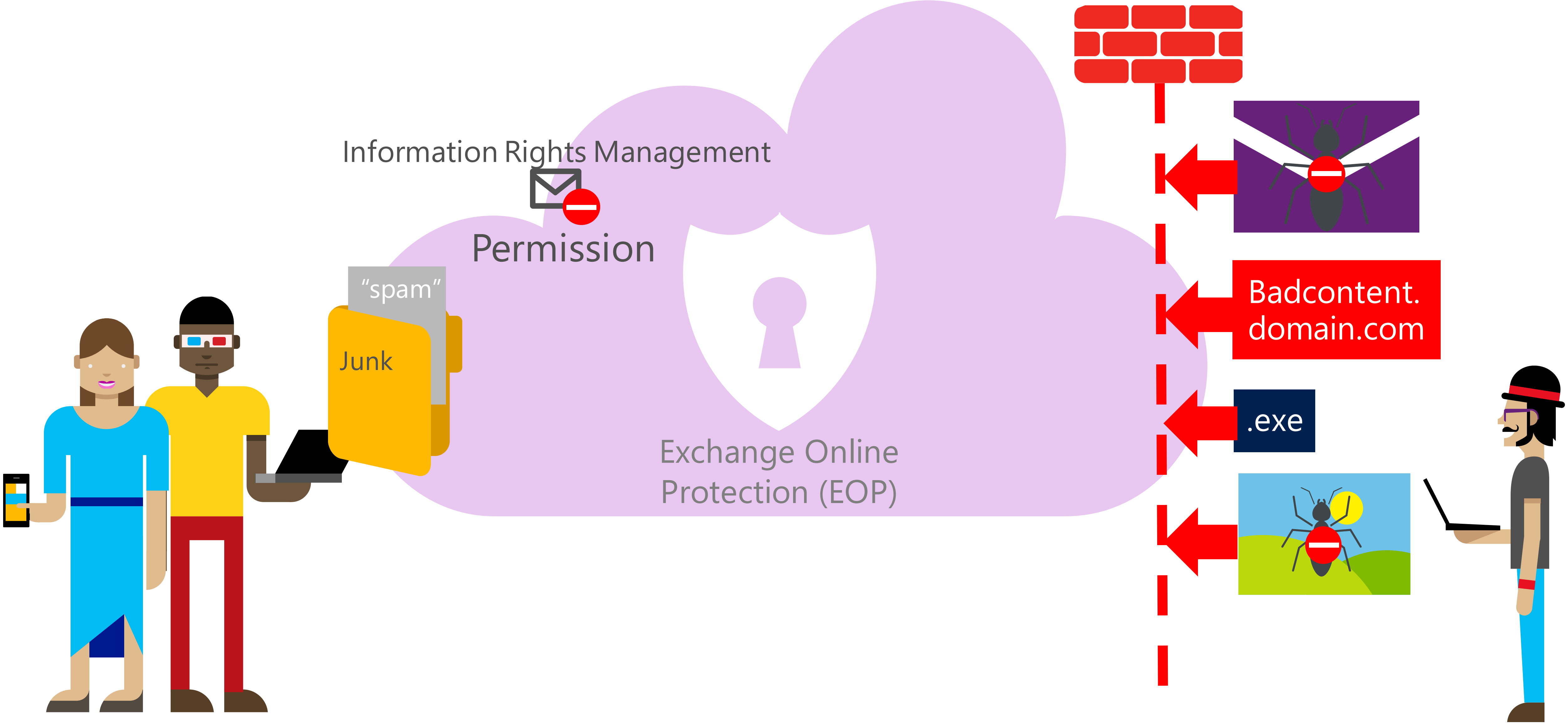
kate@bamnix.net

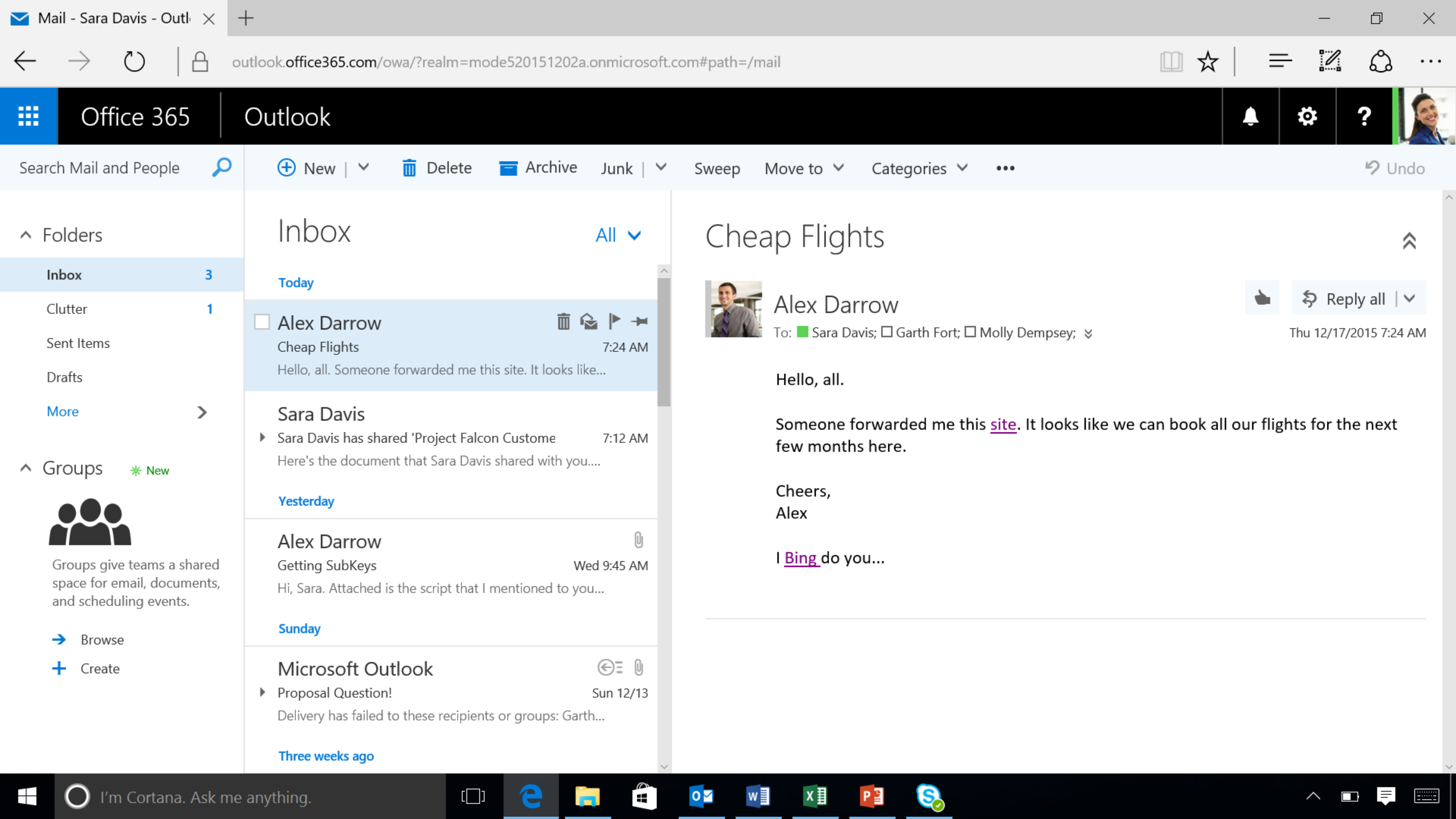
From:

sandy@fabrik.net

Exchange Online Protection (EOP)

Blocking threats at the content level


Information Rights Management
Permission
"spam"
Junk
Exchange Online Protection (EOP)
Badcontent.domain.com
.exe



Groups give teams a shared space for email, documents, and scheduling events.

Today

Alex Darrow
Cheap Flights 7:24 AM
Hello, all. Someone forwarded me this site. It looks like...

Sara Davis
Sara Davis has shared 'Project Falcon Custome 7:12 AM
Here's the document that Sara Davis shared with you....

Yesterday

Alex Darrow
Getting SubKeys Wed 9:45 AM
Hi, Sara. Attached is the script that I mentioned to you...

Sunday

Microsoft Outlook
Proposal Question! Sun 12/13
Delivery has failed to these recipients or groups: Garth...

Three weeks ago

Cheap Flights

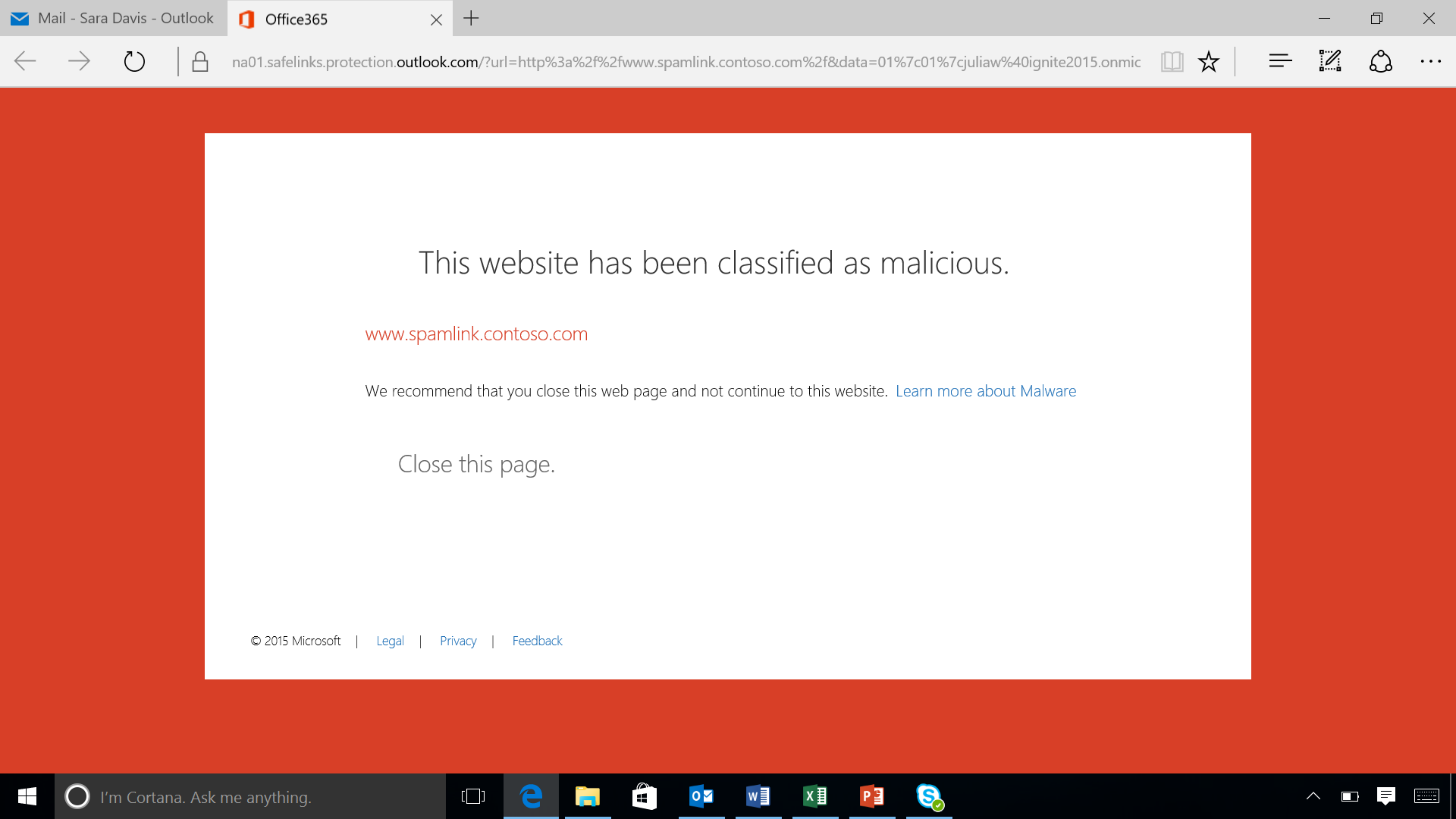
Alex Darrow
To: 🟩 Sara Davis; □ Garth Fort; □ Molly Dempsey;
Thu 12/17/2015 7:24 AM

Hello, all.

Someone forwarded me this site. It looks like we can book all our flights for the next few months here.

Cheers,
Alex

I Bing do you...


Mail - Sara Davis - Outlook
Office365
na01.safelinks.protection.outlook.com/?url=http%3a%2f%2fwww.spamlink.contoso.com%2f&data=01%7c01%7cjuliaw%40ignite2015.onmic
I'm Cortana. Ask me anything.

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

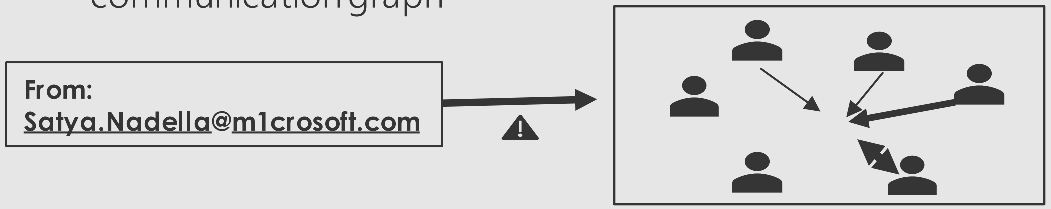
Multi-layered Phishing Defense

Spoof Protection

- ✓ Explicit Authentication Check for domains that enforce DMARC/SPF
- ✓ Intra Org and Cross Domain Spoof Intelligence for domains that don't
  - ❑ Example: DOMAIN: outlook.ms.com SPF=none, DKIM=none, DMARC=None

Impersonation Protection

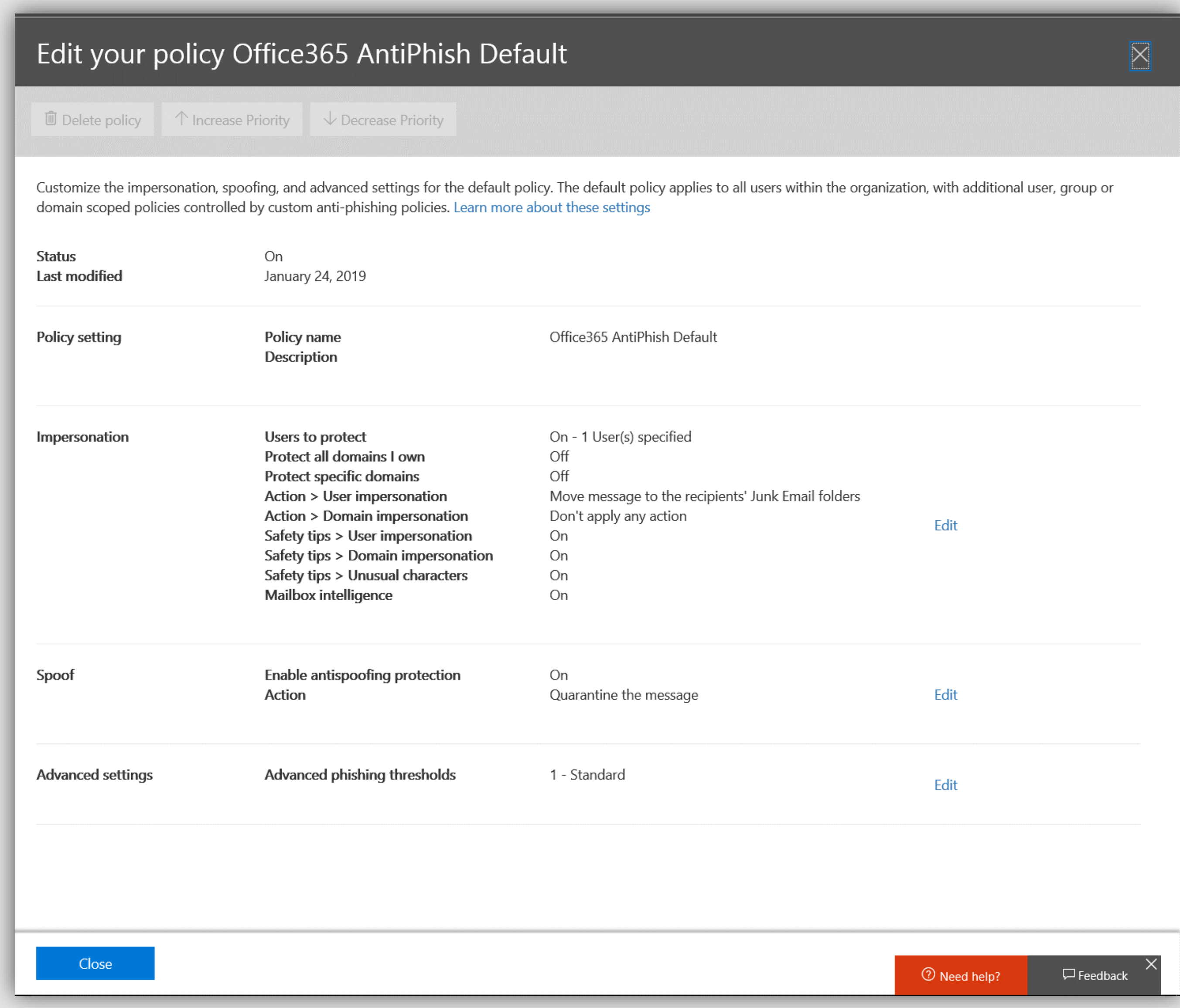
- ✓ Detect Username, Domain and Brand Impersonation
- ✓ Leverage Mailbox Intelligence based on user communication graph



From:
Satya.Nadella@m1crosoft.com

Machine Learning Models

- ✓ Over 10+ ML Models, Analyzing over 500 features for each mail
- ✓ Headers, Sender, Recipient, Content, Mail body, URLs, etc

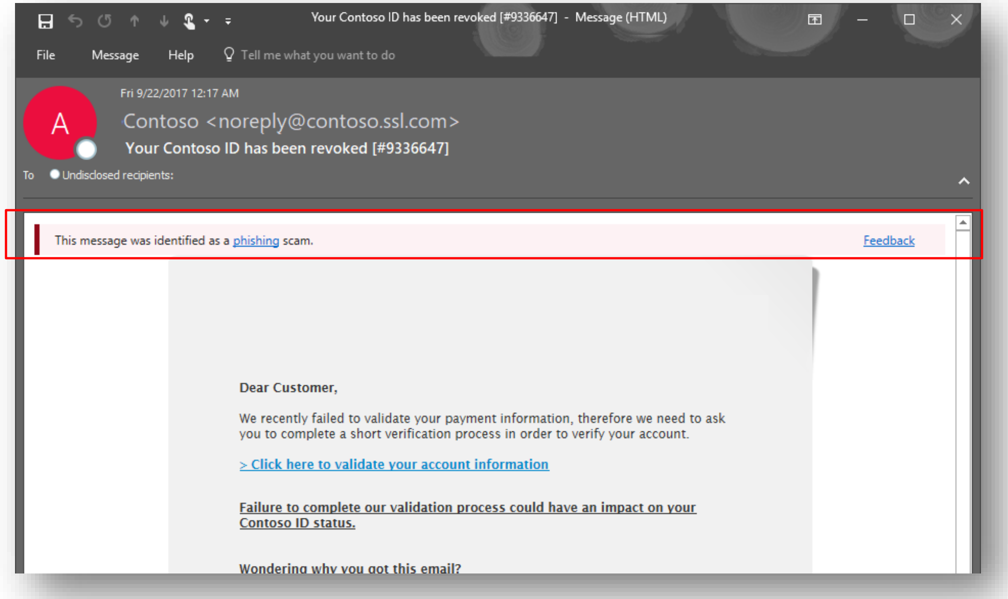


Edit your policy Office365 AntiPhish Default

Customize the impersonation, spoofing, and advanced settings for the default policy. The default policy applies to all users within the organization, with additional user, group or domain scoped policies controlled by custom anti-phishing policies. Learn more about these settings

Status	On		
Last modified	January 24, 2019		
Policy setting	**Policy name**	Office365 AntiPhish Default	
	Description		
Impersonation	**Users to protect**	On - 1 User(s) specified	
	Protect all domains I own	Off	
	Protect specific domains	Off	
	Action > User impersonation	Move message to the recipients' Junk Email folders	
	Action > Domain impersonation	Don't apply any action	Edit
	Safety tips > User impersonation	On	
	Safety tips > Domain impersonation	On	
	Safety tips > Unusual characters	On	
	Mailbox intelligence	On	
Spoof	**Enable antispoofing protection**	On	
	Action	Quarantine the message	Edit
Advanced settings	**Advanced phishing thresholds**	1 - Standard	Edit

Intelligent Client Tips & Warnings for Suspicious Mails


Your Contoso ID has been revoked [#9336647] - Message (HTML)
File
Message
Help
Tell me what you want to do
A
Feedback

Fri 9/22/2017 12:17 AM

Contoso <noreply@contoso.ssl.com>

Your Contoso ID has been revoked [#9336647]

To Undisclosed recipients:

This message was identified as a phishing scam.

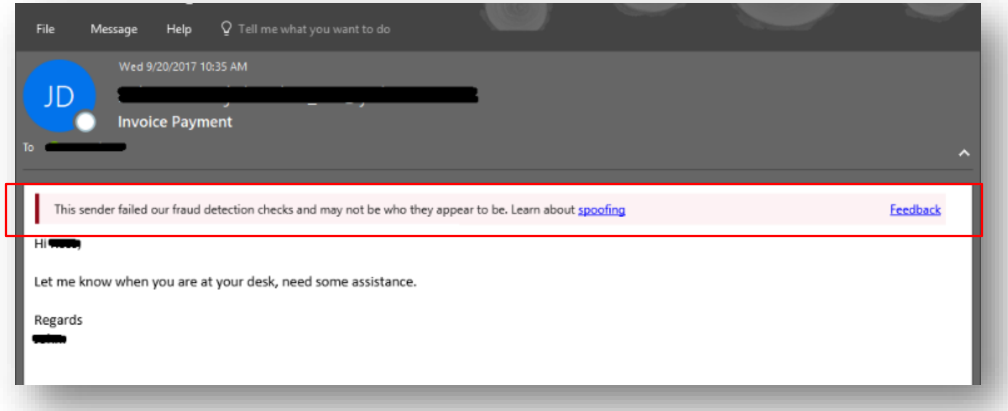
Dear Customer,

We recently failed to validate your payment information, therefore we need to ask you to complete a short verification process in order to verify your account.

> Click here to validate your account information

Failure to complete our validation process could have an impact on your Contoso ID status.

Wondering why you got this email?



Wed 9/20/2017 10:35 AM

[redacted]

Invoice Payment

To [redacted]

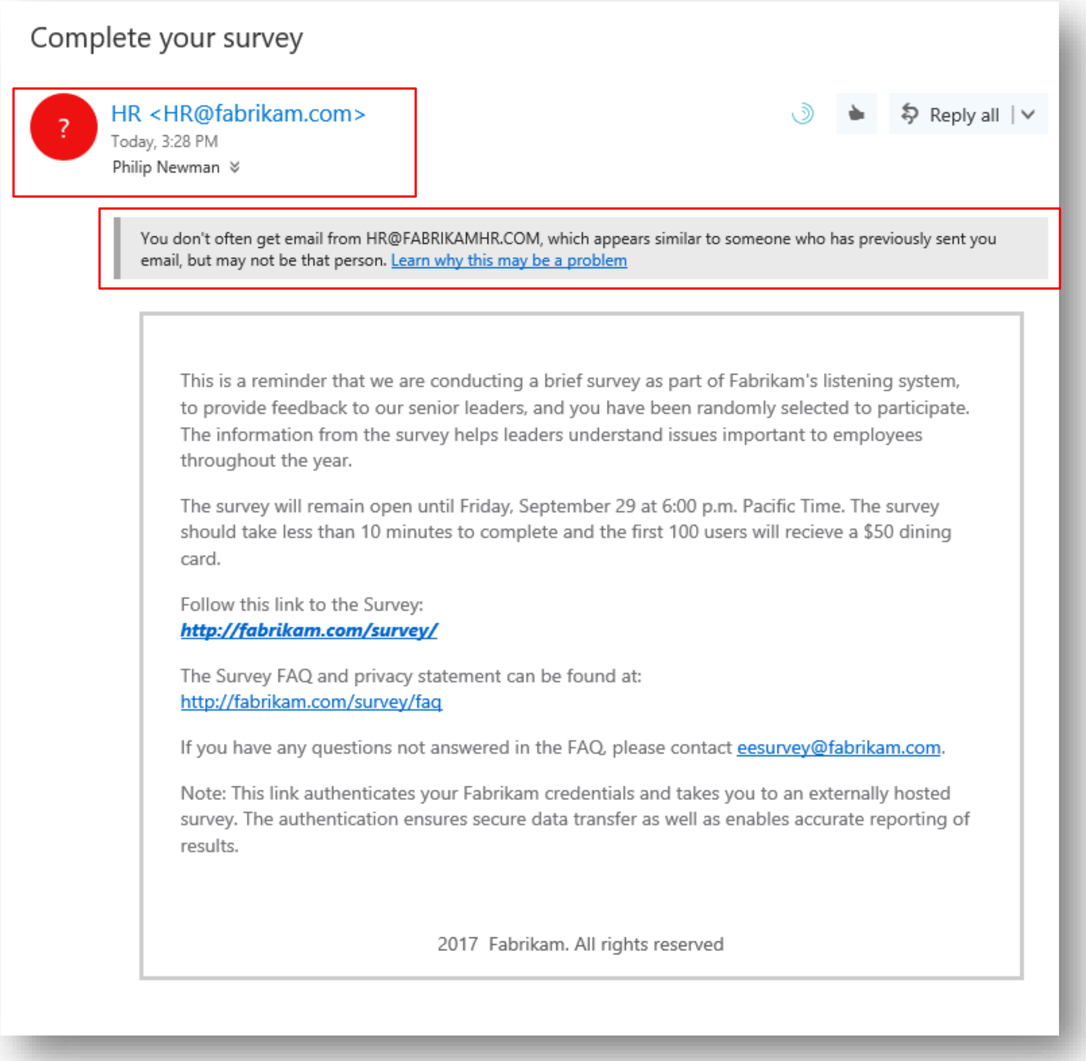
This sender failed our fraud detection checks and may not be who they appear to be. Learn about spoofing

Hi [redacted]

Let me know when you are at your desk, need some assistance.

Regards

[redacted]



Complete your survey

HR <HR@fabrikam.com>

Today, 3:28 PM

Philip Newman

You don't often get email from HR@FABRIKAMHR.COM, which appears similar to someone who has previously sent you email, but may not be that person. Learn why this may be a problem

This is a reminder that we are conducting a brief survey as part of Fabrikam's listening system, to provide feedback to our senior leaders, and you have been randomly selected to participate. The information from the survey helps leaders understand issues important to employees throughout the year.

The survey will remain open until Friday, September 29 at 6:00 p.m. Pacific Time. The survey should take less than 10 minutes to complete and the first 100 users will recieve a $50 dining card.

Follow this link to the Survey:
http://fabrikam.com/survey/

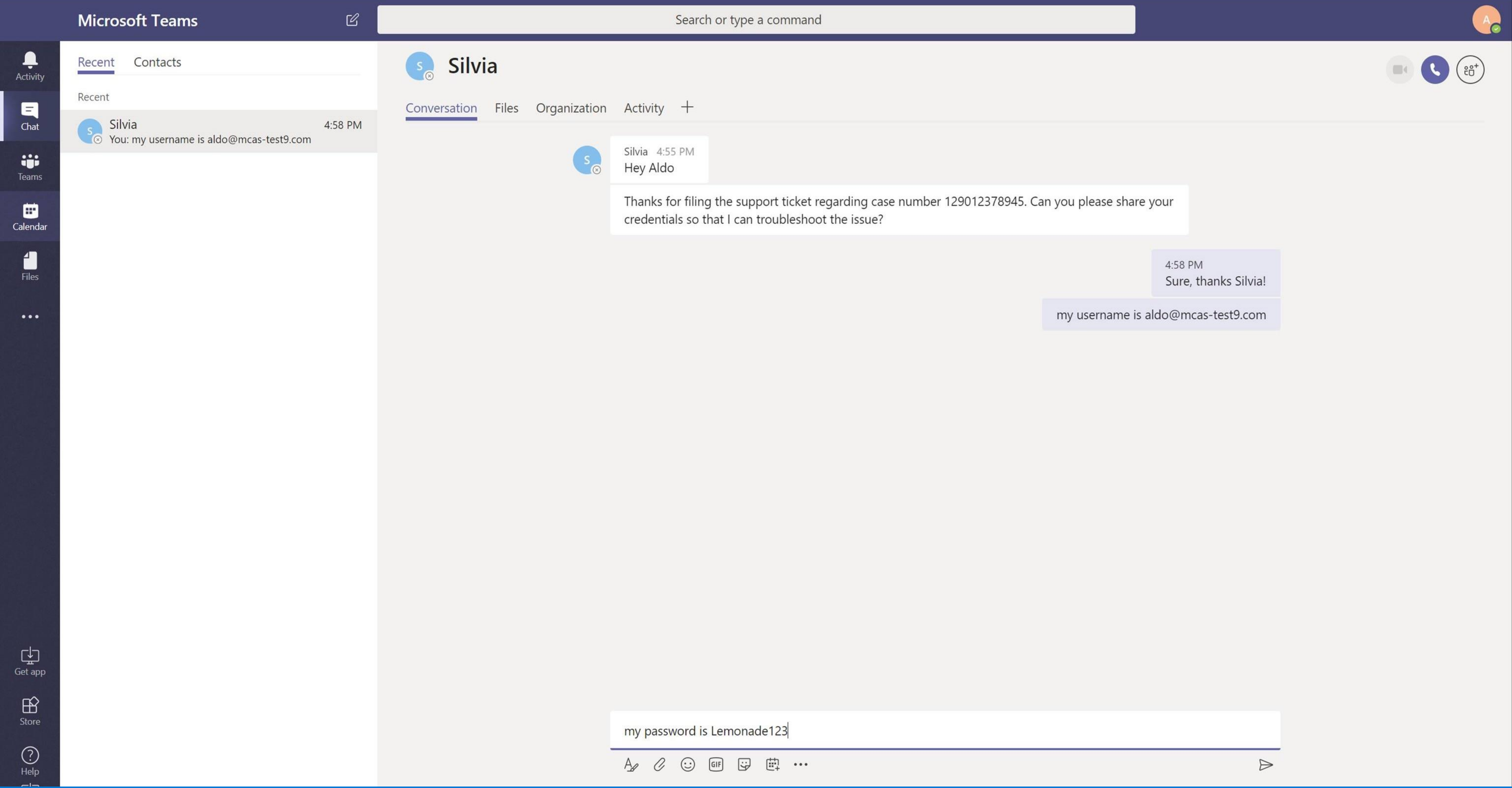
The Survey FAQ and privacy statement can be found at:
http://fabrikam.com/survey/faq

If you have any questions not answered in the FAQ, please contact eesurvey@fabrikam.com.

Note: This link authenticates your Fabrikam credentials and takes you to an externally hosted survey. The authentication ensures secure data transfer as well as enables accurate reporting of results.

2017 Fabrikam. All rights reserved

Mobile Device Control



Recent

Silvia 4:58 PM
You: my username is aldo@mcas-test9.com

Silvia

Silvia 4:55 PM
Hey Aldo

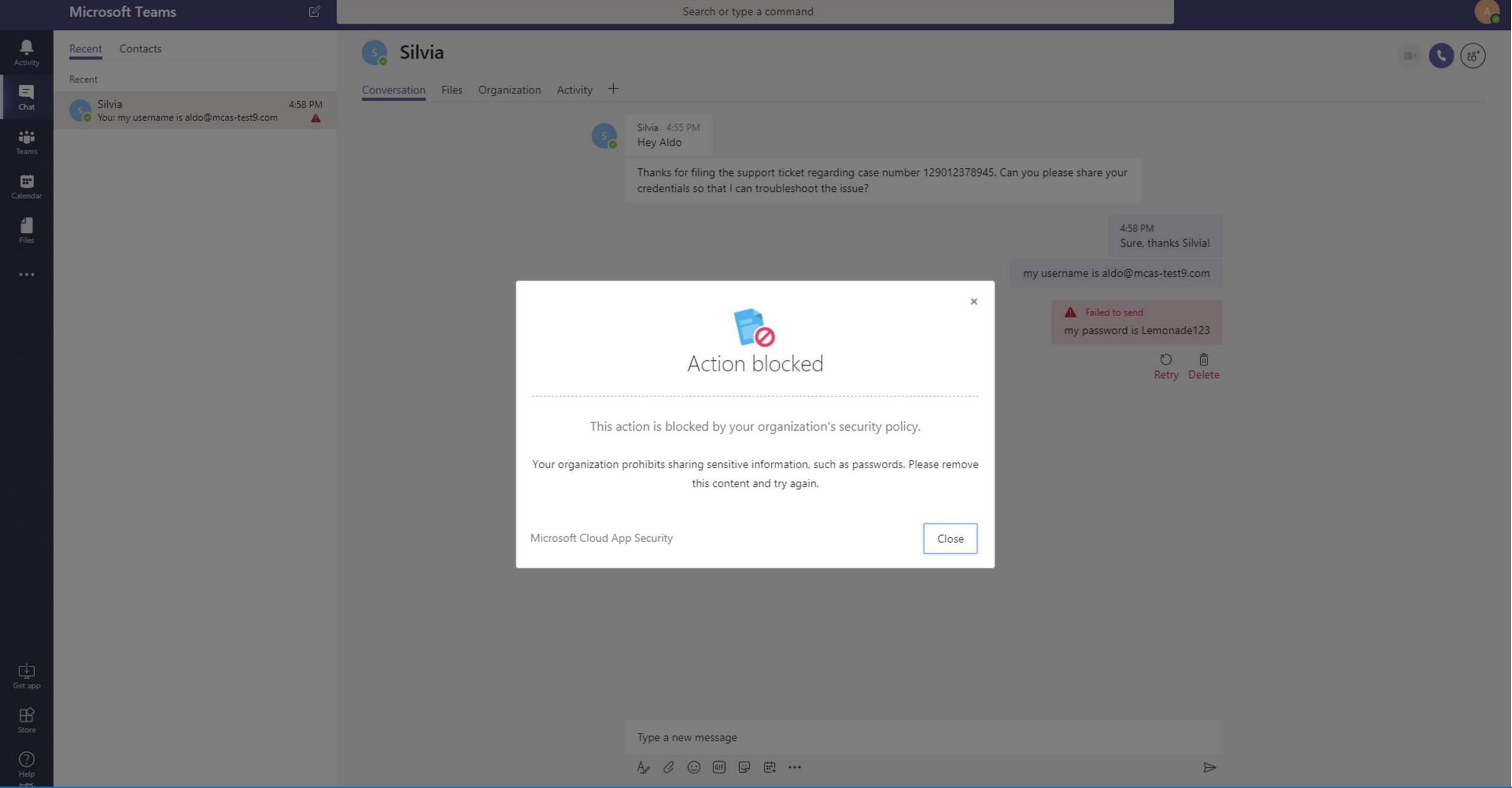
Thanks for filing the support ticket regarding case number 129012378945. Can you please share your credentials so that I can troubleshoot the issue?

4:58 PM
Sure, thanks Silvia!

my username is aldo@mcas-test9.com

my password is Lemonade123

End user attempts to send sensitive information (password) via IM message



Recent

Silvia 4:58 PM
You: my username is aldo@mcas-test9.com

Silvia

Silvia 4:55 PM
Hey Aldo

Thanks for filing the support ticket regarding case number 129012378945. Can you please share your credentials so that I can troubleshoot the issue?

4:58 PM
Sure, thanks Silvia!

my username is aldo@mcas-test9.com

Failed to send
my password is Lemonade123

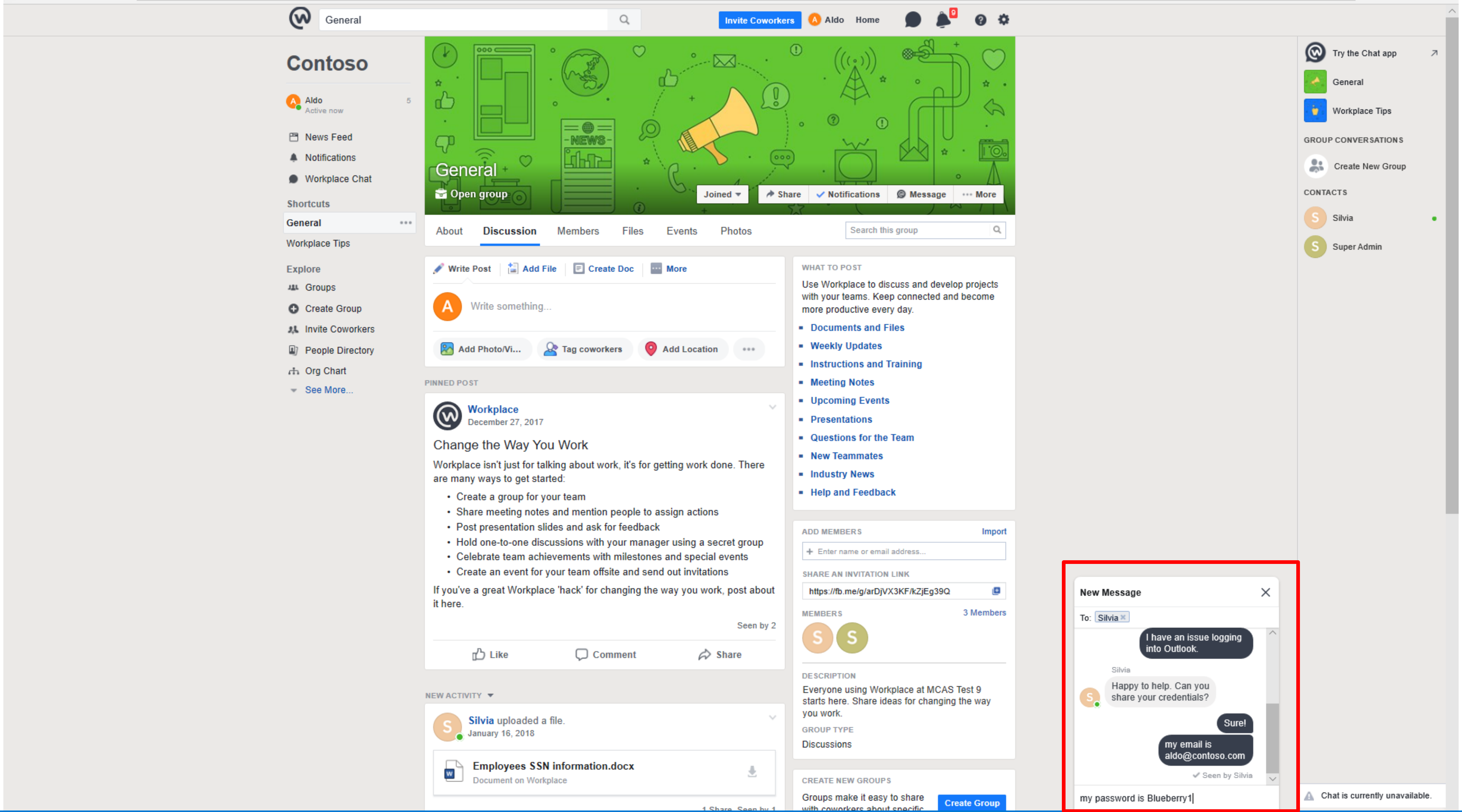
Action blocked

This action is blocked by your organization's security policy.

Your organization prohibits sharing sensitive information, such as passwords. Please remove this content and try again.

Microsoft Cloud App Security

The IM message is blocked in real-time and not delivered



General

Invite Coworkers · Aldo · Home

Contoso

Aldo
Active now

- News Feed
- Notifications
- Workplace Chat

Shortcuts

- General
- Workplace Tips

Explore

- Groups
- Create Group
- Invite Coworkers
- People Directory
- Org Chart
- See More...

General
Open group

Joined · Share · Notifications · Message · More

About · Discussion · Members · Files · Events · Photos · Search this group

Write Post · Add File · Create Doc · More

Write something...

Add Photo/Vi... · Tag coworkers · Add Location

PINNED POST

Workplace
December 27, 2017

Change the Way You Work

Workplace isn't just for talking about work, it's for getting work done. There are many ways to get started:

- Create a group for your team
- Share meeting notes and mention people to assign actions
- Post presentation slides and ask for feedback
- Hold one-to-one discussions with your manager using a secret group
- Celebrate team achievements with milestones and special events
- Create an event for your team offsite and send out invitations

If you've a great Workplace 'hack' for changing the way you work, post about it here.

Seen by 2

Like · Comment · Share

NEW ACTIVITY

Silvia uploaded a file.
January 16, 2018

Employees SSN information.docx
Document on Workplace

WHAT TO POST

Use Workplace to discuss and develop projects with your teams. Keep connected and become more productive every day.

- Documents and Files
- Weekly Updates
- Instructions and Training
- Meeting Notes
- Upcoming Events
- Presentations
- Questions for the Team
- New Teammates
- Industry News
- Help and Feedback

ADD MEMBERS · Import

Enter name or email address...

SHARE AN INVITATION LINK

https://fb.me/g/arDjVX3KF/kZjEg39Q

MEMBERS · 3 Members

DESCRIPTION

Everyone using Workplace at MCAS Test 9 starts here. Share ideas for changing the way you work.

GROUP TYPE

Discussions

CREATE NEW GROUPS

Groups make it easy to share with coworkers about specific

Create Group

Try the Chat app

General

Workplace Tips

GROUP CONVERSATIONS

Create New Group

CONTACTS

Silvia

Super Admin

New Message

To: Silvia

I have an issue logging into Outlook.

Silvia

Happy to help. Can you share your credentials?

Sure!

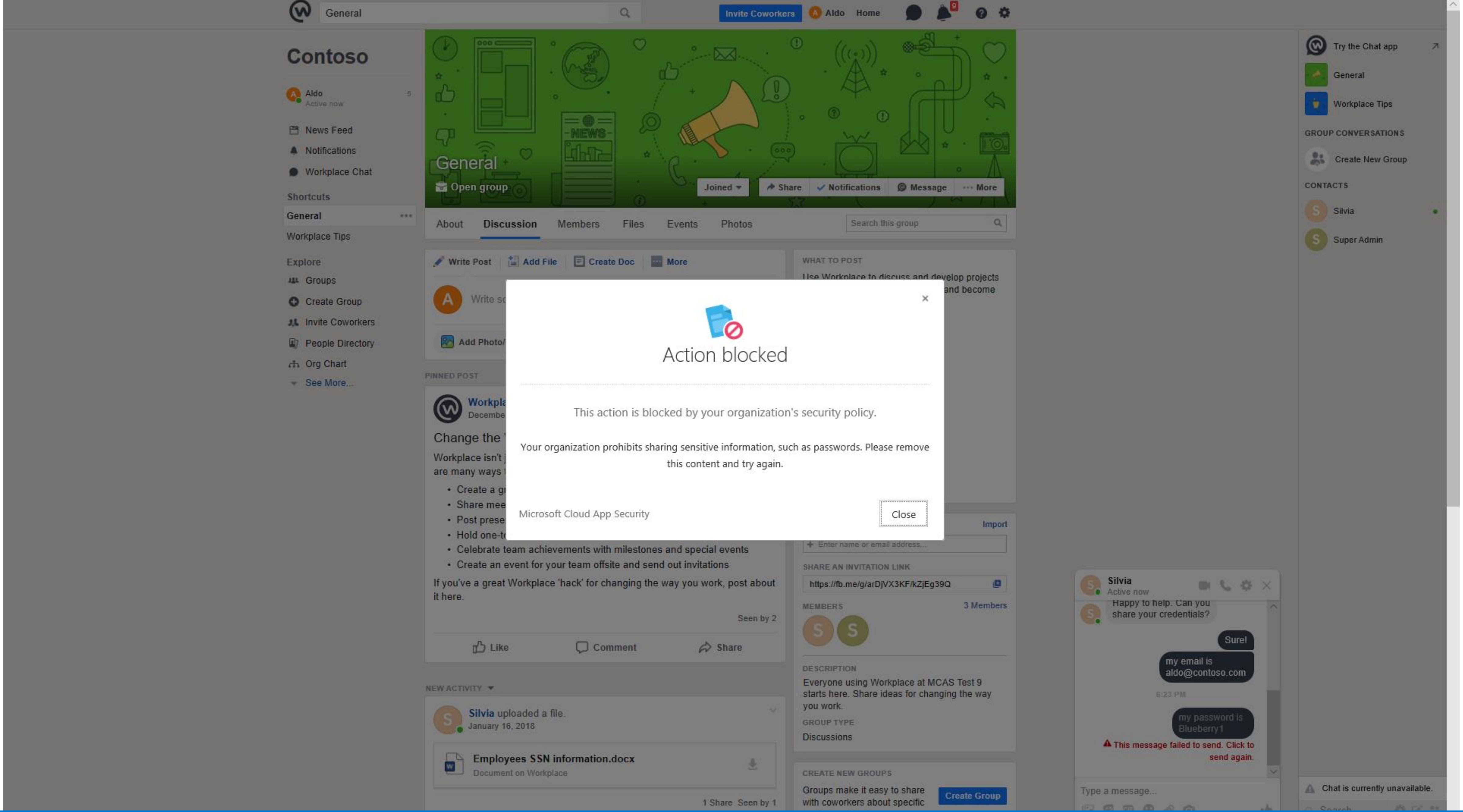
my email is aldo@contoso.com

✓ Seen by Silvia

my password is Blueberry1

Chat is currently unavailable.

End user attempts to send sensitive information (password) via IM message



Action blocked

This action is blocked by your organization's security policy.

Your organization prohibits sharing sensitive information, such as passwords. Please remove this content and try again.

Microsoft Cloud App Security

Close

WHAT TO POST

Use Workplace to discuss and develop projects ... and become

Workpla...
Decembe...

Change the ...

Workplace isn't j... are many ways ...

- Create a g...
- Share mee...
- Post prese...
- Hold one-t...
- Celebrate team achievements with milestones and special events
- Create an event for your team offsite and send out invitations

If you've a great Workplace 'hack' for changing the way you work, post about it here.

Seen by 2

Silvia uploaded a file.
January 16, 2018

Employees SSN information.docx
Document on Workplace

1 Share Seen by 1

https://fb.me/g/arDjVX3KF/kZjEg39Q

Everyone using Workplace at MCAS Test 9 starts here. Share ideas for changing the way you work.

Discussions

Groups make it easy to share with coworkers about specific

Silvia
Active now

Happy to help. Can you share your credentials?

Sure!

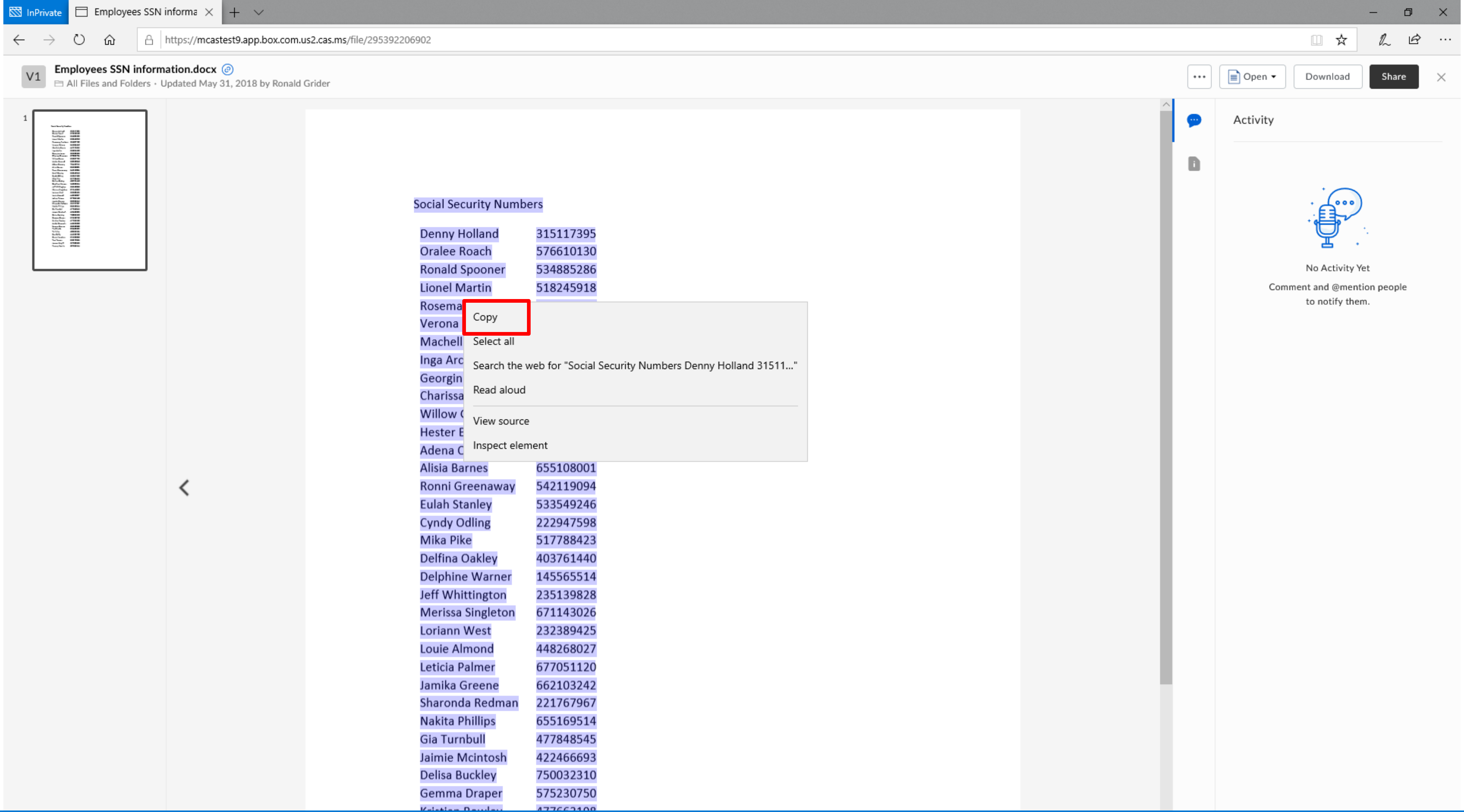
my email is aldo@contoso.com

6:23 PM

my password is Blueberry1

This message failed to send. Click to send again.

The IM message is blocked in real-time and not delivered


InPrivate
Employees SSN informa
https://mcastest9.app.box.com.us2.cas.ms/file/295392206902
V1
Open
Download
Share
1
Activity
No Activity Yet
Comment and @mention people to notify them.
Copy
Select all
Search the web for "Social Security Numbers Denny Holland 31511..."
Read aloud
View source
Inspect element

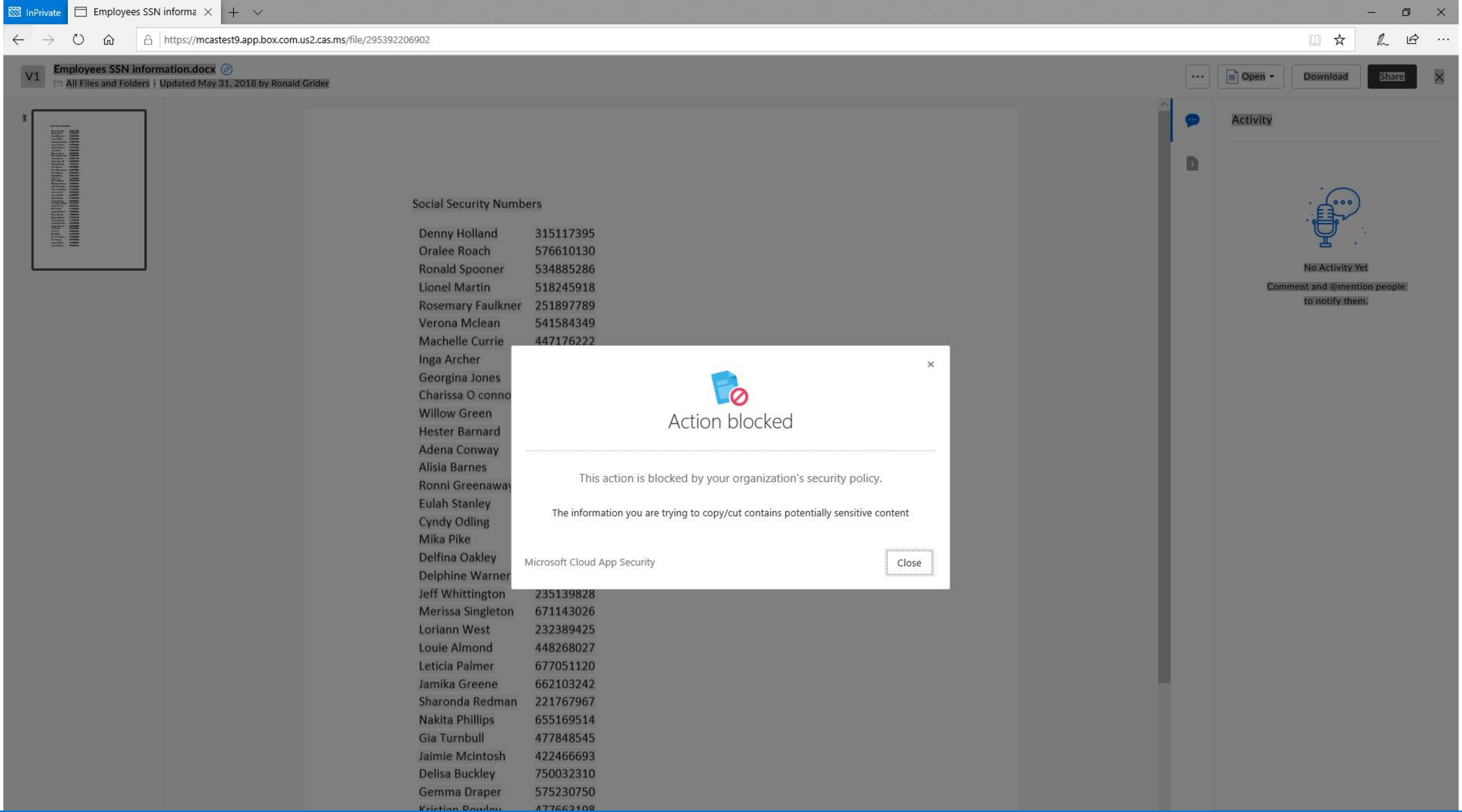
Employees SSN information.docx

All Files and Folders · Updated May 31, 2018 by Ronald Grider

Social Security Numbers

Denny Holland	315117395
Oralee Roach	576610130
Ronald Spooner	534885286
Lionel Martin	518245918
Rosema	
Verona	
Machell	
Inga Arc	
Georgin	
Charissa	
Willow (	
Hester E	
Adena C	
Alisia Barnes	655108001
Ronni Greenaway	542119094
Eulah Stanley	533549246
Cyndy Odling	222947598
Mika Pike	517788423
Delfina Oakley	403761440
Delphine Warner	145565514
Jeff Whittington	235139828
Merissa Singleton	671143026
Loriann West	232389425
Louie Almond	448268027
Leticia Palmer	677051120
Jamika Greene	662103242
Sharonda Redman	221767967
Nakita Phillips	655169514
Gia Turnbull	477848545
Jaimie Mcintosh	422466693
Delisa Buckley	750032310
Gemma Draper	575230750

End user attempts to copy sensitive information (Social Security numbers)



https://mcastest9.app.box.com.us2.cas.ms/file/295392206902

Employees SSN information.docx

All Files and Folders · Updated May 31, 2018 by Ronald Grider

No Activity Yet

Comment and @mention people to notify them.

Social Security Numbers

Denny Holland	315117395
Oralee Roach	576610130
Ronald Spooner	534885286
Lionel Martin	518245918
Rosemary Faulkner	251897789
Verona Mclean	541584349
Machelle Currie	447176222
Inga Archer	
Georgina Jones	
Charissa O conno	
Willow Green	
Hester Barnard	
Adena Conway	
Alisia Barnes	
Ronni Greenaway	
Eulah Stanley	
Cyndy Odling	
Mika Pike	
Delfina Oakley	
Delphine Warner	
Jeff Whittington	235139828
Merissa Singleton	671143026
Loriann West	232389425
Louie Almond	448268027
Leticia Palmer	677051120
Jamika Greene	662103242
Sharonda Redman	221767967
Nakita Phillips	655169514
Gia Turnbull	477848545
Jaimie Mcintosh	422466693
Delisa Buckley	750032310
Gemma Draper	575230750
Kristian Rowley	477663198

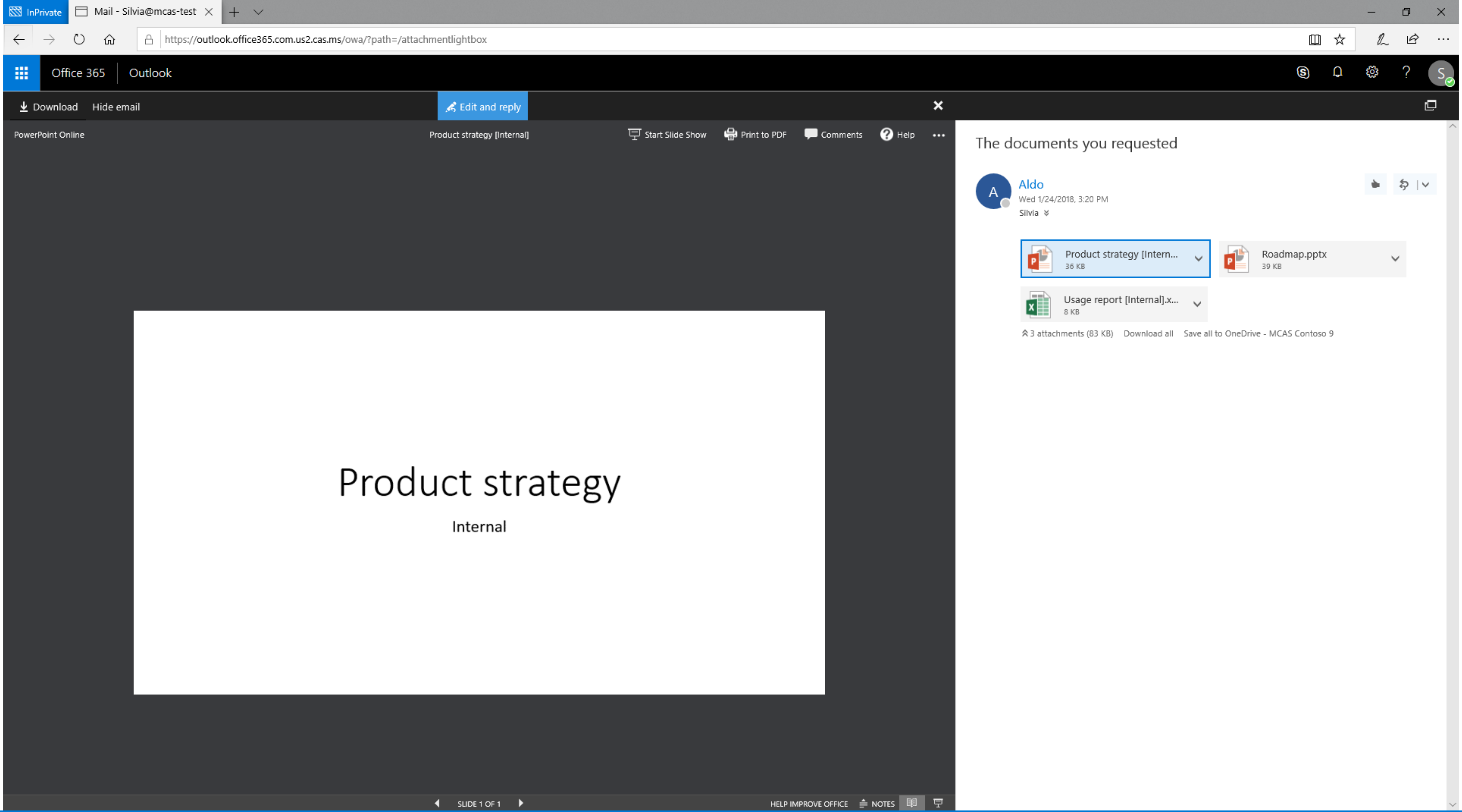
Action blocked

This action is blocked by your organization's security policy.

The information you are trying to copy/cut contains potentially sensitive content

Microsoft Cloud App Security

End user receives a notification that his action was blocked



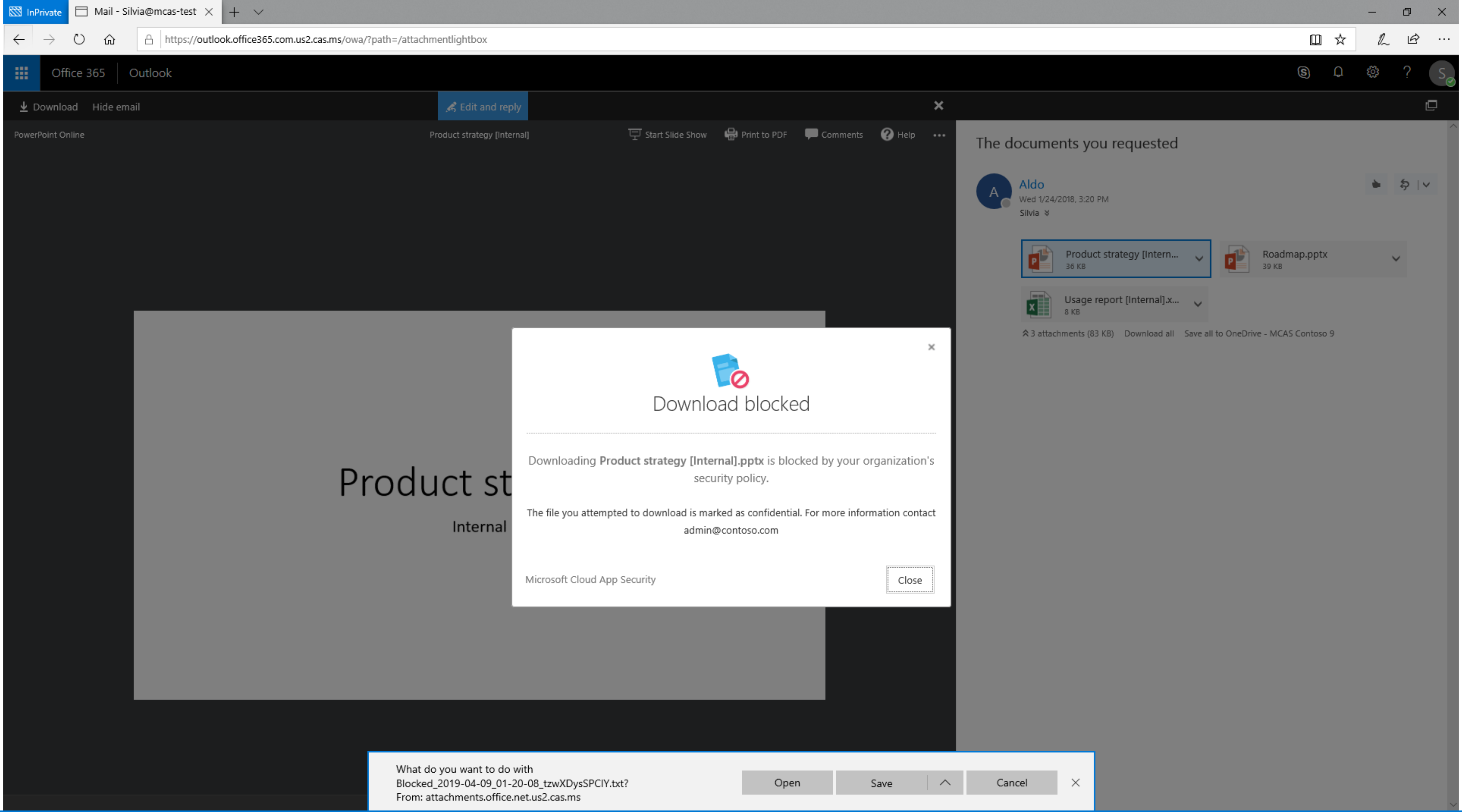
The documents you requested

Aldo
Wed 1/24/2018, 3:20 PM
Silvia

Product strategy [Intern... 36 KB
Roadmap.pptx 39 KB
Usage report [Internal].x... 8 KB

3 attachments (83 KB) Download all Save all to OneDrive - MCAS Contoso 9

End user attempts to download an email attachment containing sensitive, internal information



Download blocked

Downloading **Product strategy [Internal].pptx** is blocked by your organization's security policy.

The file you attempted to download is marked as confidential. For more information contact admin@contoso.com

Microsoft Cloud App Security

Close

What do you want to do with Blocked_2019-04-09_01-20-08_tzwXDysSPCIY.txt?
From: attachments.office.net.us2.cas.ms

Open Save Cancel

End user is notified that the download to his personal device was blocked

Microsoft

© 2017 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.