RSAConference2019

San Francisco | March 4–8 | Moscone Center

SESSION ID: IDY-W10

No More Firewalls! How Zero Trust Networks are Reshaping Cyber Security

Matt Soseman

Security Architect
Microsoft
@SosemanMatt
http://aka.ms/MattsBlog

Session Objectives

- Understand what Zero Trust is and why it is important.
- Understand how identity, device health and trustworthiness contribute to overall security posture.
- Learn considerations for automated access to resources via device and identity conditions.
- Discover how to apply these conditions to line of business SaaS apps or on-premises web apps.

RSAConference2019

The challenge with perimeter-based networks…

It was a walled garden (castle/moat approach)

- Perimeter-based networks operate on the assumption that all systems (and users) within a network can be trusted.
- Not able to accommodate modern work styles such as Bring Your Own Device (BYOD) and Bring Your Own Cloud (BYOC)
- Attacker can compromise single endpoint within trusted boundary and quickly expand foothold across entire network.

Users cannot be trusted! (Neither can the network!)

4%

Of end-users will click on anything[1]

28%

of attacks involved inside actors[1]

17%

Of breaches had errors as casual events[1]

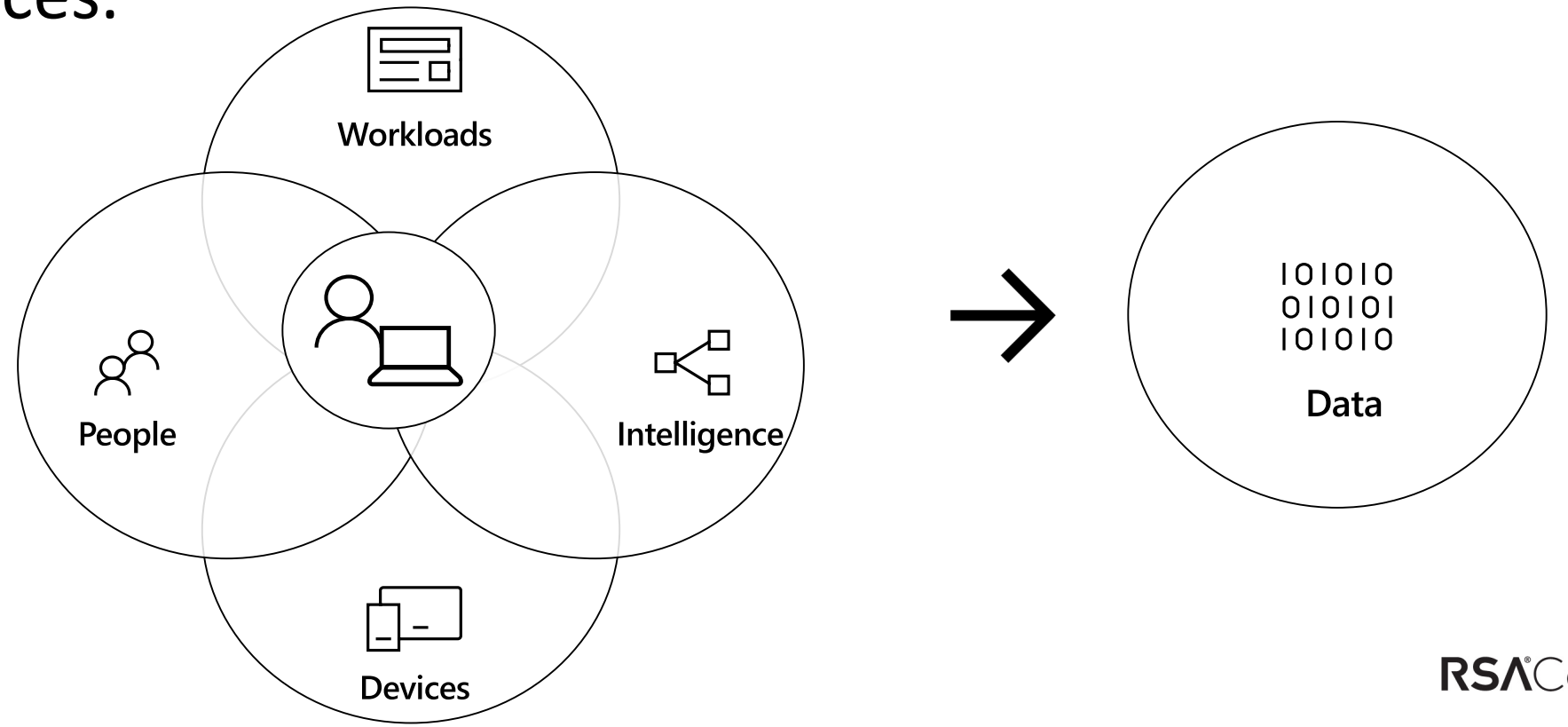
1. Verizon DBIR Report 2018 https://enterprise.verizon.com/resources/reports/dbir/

RSAConference2019

Zero Trust to the rescue!

What is a Zero Trust network?

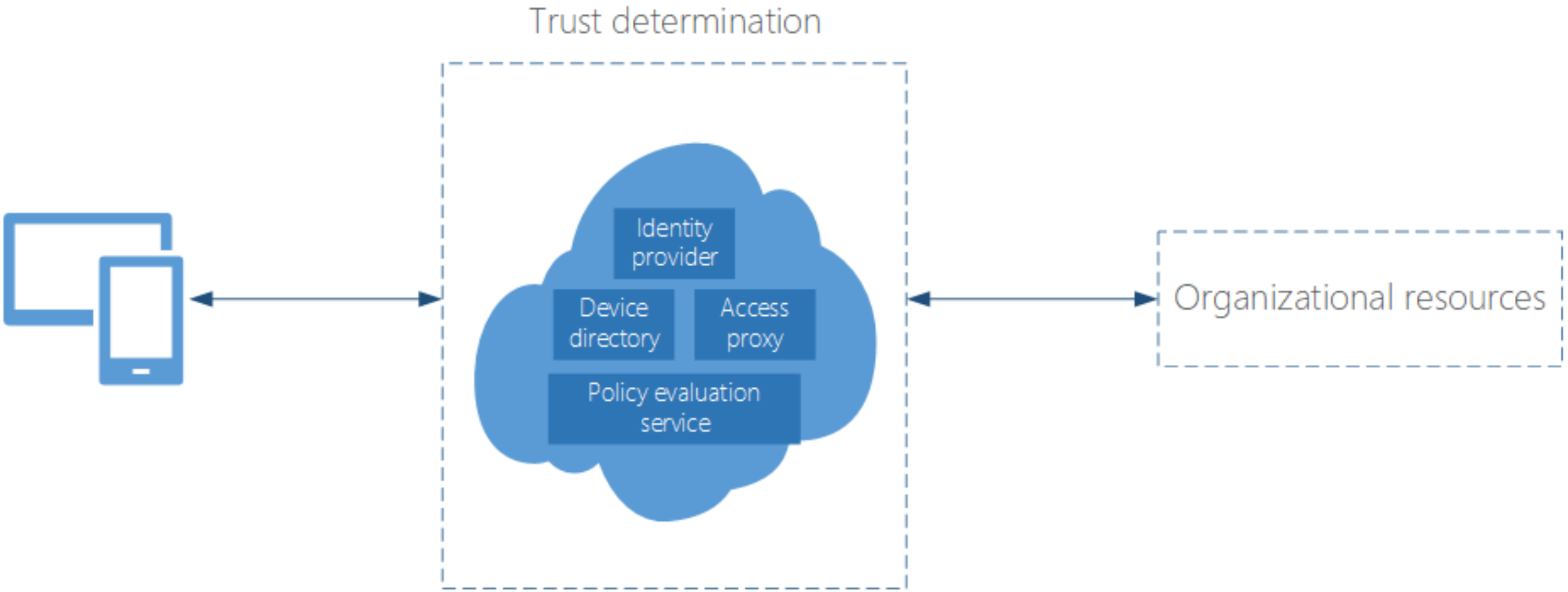
- Eliminates the concept of trust based on network location within a perimeter.
- Leverages device and user trust claims to gate access to data and resources.



What comprises a Zero Trust network?

- Identity provider to keep track of users and user-related information.
- Device directory to maintain a list of devices that have access to corporate resources, along with their corresponding device information (e.g., type of device, integrity etc.)
- Policy evaluation service to determine if a user or device conforms to the policy set forth by security admins
- Access proxy that utilizes the above signals to grant or deny access to an organizational resource
- Anomaly detection and machine learning

Example: Basic components of a Zero Trust network model



Benefits of a Zero Trust model

- Allow conditional access to certain resources while restricting access to high-value resources on managed/compliant devices.
- Prevent network access and lateral movement using stolen credentials and compromised device.
- Enables users to be more productive by working however they want, where they want, when they want.

RSAConference2019

Designing a Zero Trust architecture

Approach: Start with asking questions

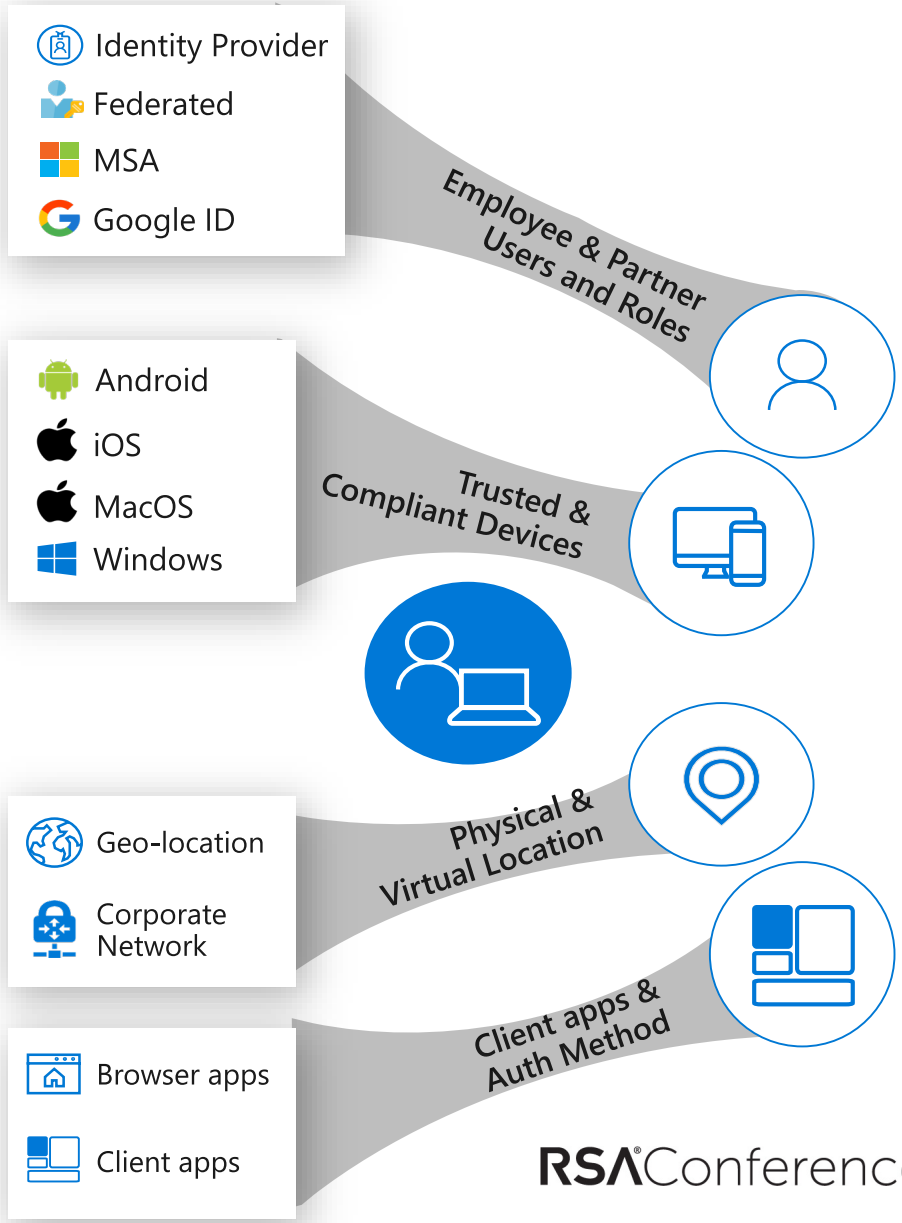
Who are your users? What apps are they trying to access? How are they doing it? Why are they doing it that way?

What conditions are required to access a corporate resource?

What controls are required based on the condition?

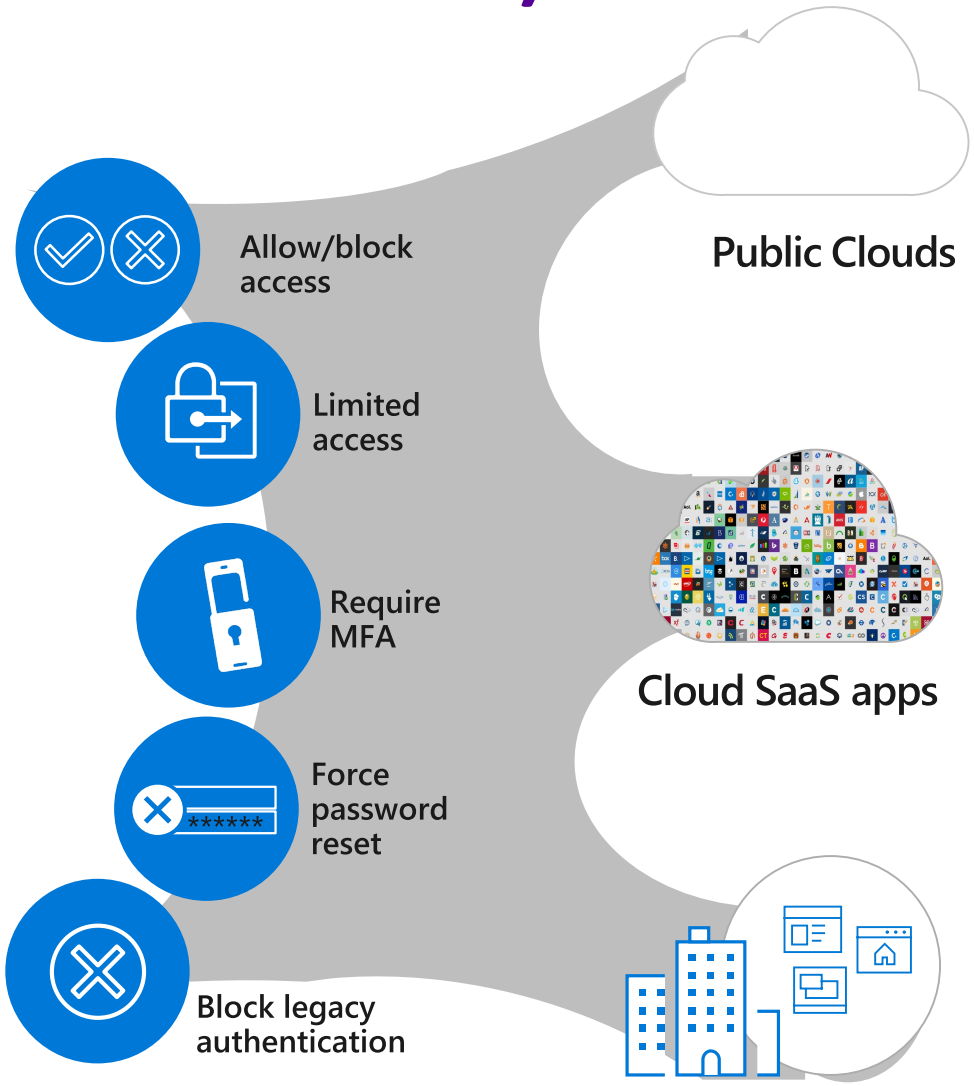
Consider an approach based on set of conditions

- What is the user's role and group membership?
- What is the device health and compliance state?
- What is the SaaS, on-prem or mobile app being accessed?
- What is the user's physical location?
- What is the time of sign-in?
- What is the sign-in risk of the user's identity? (i.e. probability it isn't authorized by the identity owner)
- What is the user risk? (i.e. probability a bad actor has compromised the account?

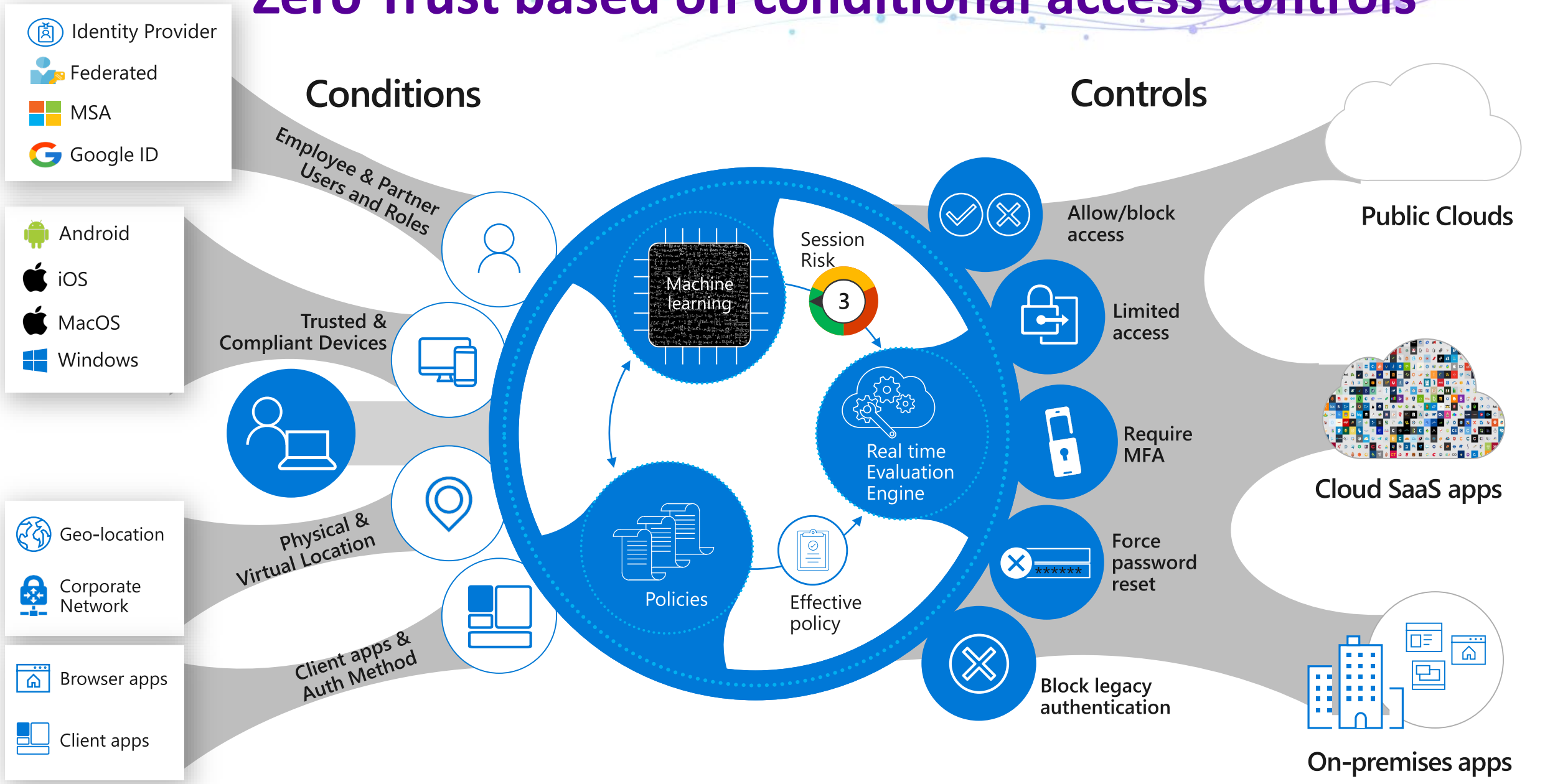


Followed by a set of controls (if/then statement)

- Allow/deny access
- Require MFA
- Force password reset
- Control session access to the app (i.e. allow read but not download, etc)

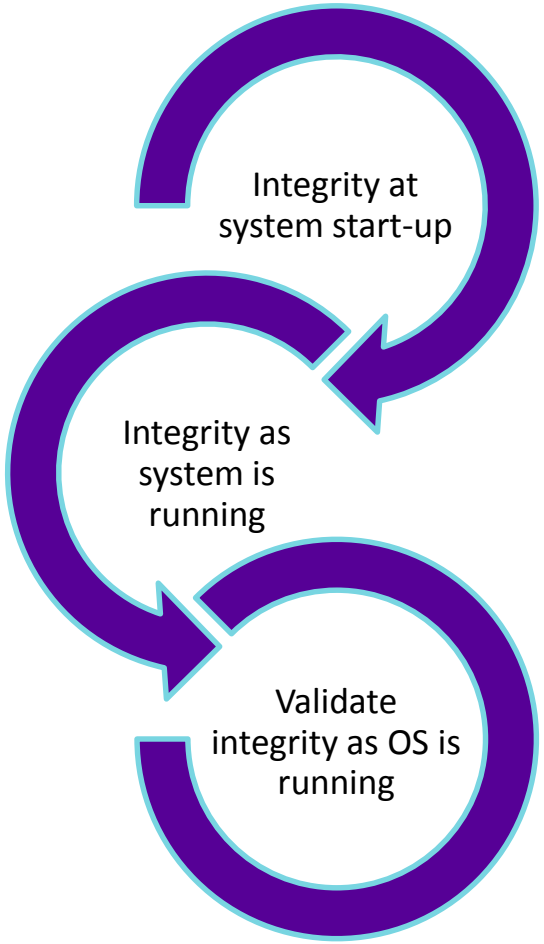


Zero Trust based on conditional access controls

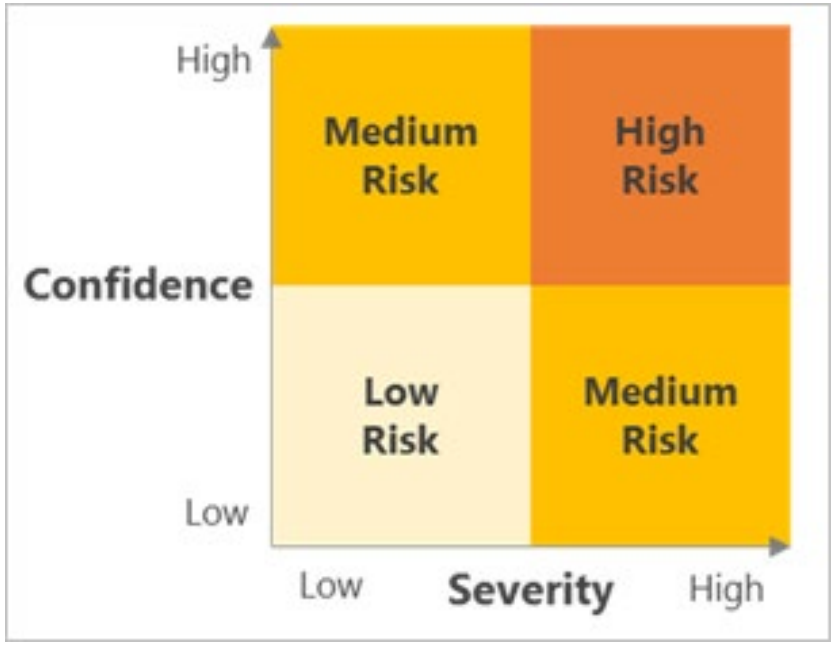


Device Health Conditions

- Determine the machine risk level (i.e. is it compromised by malware, Pass-the-Hash (PtH), etc)
- Determine the system integrity and posture (i.e. hardware-rooted boot-time and runtime checks)
- Integrity checks:
  - Drivers
  - Kernel
  - Firmware
  - Peripheral firmware
  - Antimalware driver code
- Verify boot state of machine
- Compliance policy checks (i.e. is an OS security setting missing/not configured?)



Identity Conditions



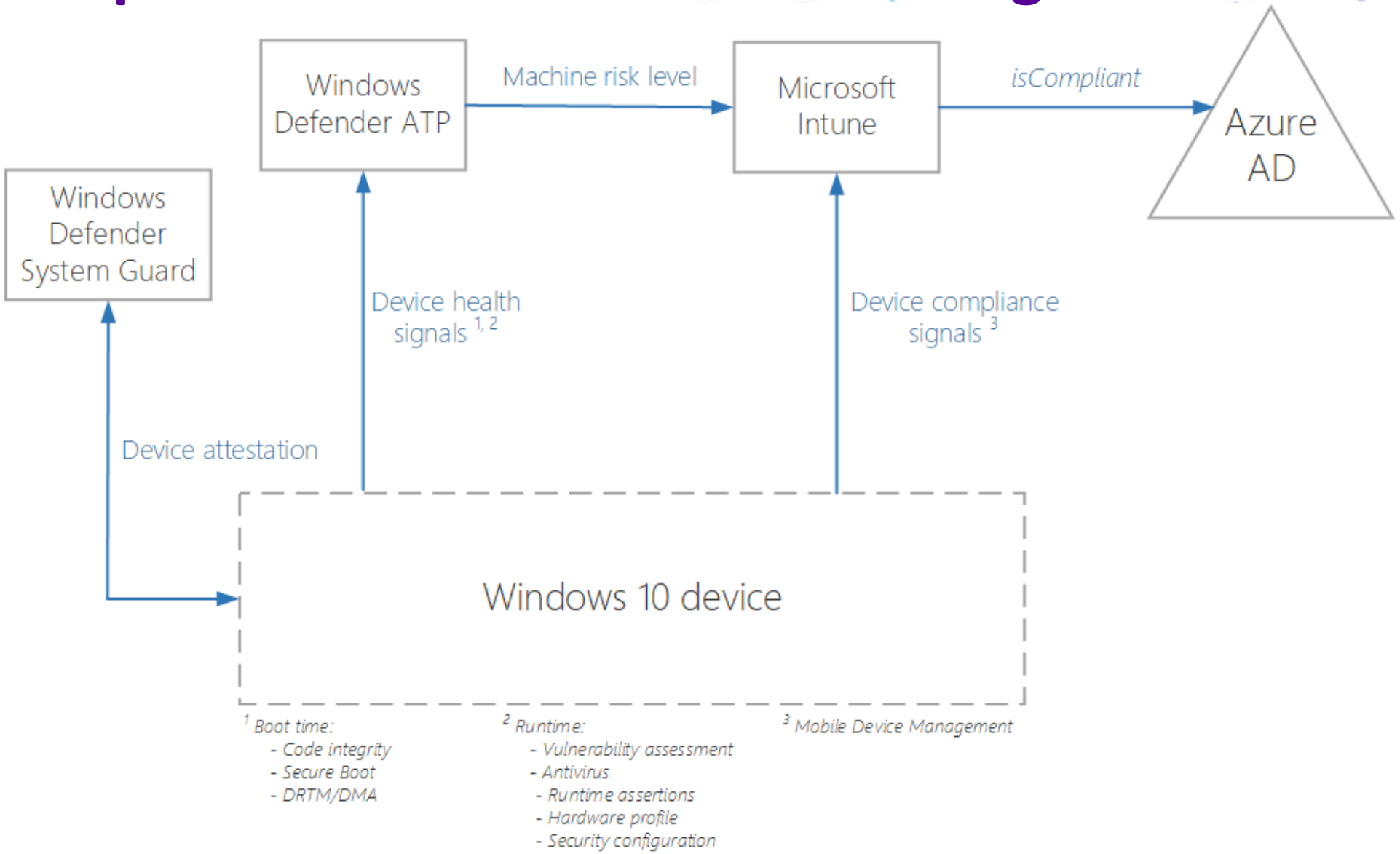
What is the user's risk level?

- Is the sign in coming from:
  - A known botnet IP address?
  - An anonymous IP address?
  - Unauthorized browser? (i.e. Tor)
  - An unfamiliar location?
  - Impossible travel to atypical locations?
- Is the sign in suspicious?
  - High number of failed attempts across multiple accounts over a short period of time
  - Matches traffic patterns of IP addresses used by attackers
- Are the user's credentials (username/password pair) leaked?
  - Up for sale on the dark web / black sites

RSAConference2019

Example Zero Trust Architectures

Example Zero Trust architecture using conditional access



Operations in a Zero Trust model

- Automatic gating to applications is key.
- Automatic remediation based on device health (not rely on user intervention).
- Monitoring for policy violations (signal from the noise).
- Prioritizing alerts correlated with sensitive data access.
- Reporting on state of Identity, Device, SaaS app and data.

Making it real with demos

- Demonstrate how a Zero Trust model behaves in the real world using key scenarios
- Tying the key Zero Trust components together with conditional access policies
- See example reports of policy violations
- Understand the user experience in a Zero Trust model

Download this deck and these click thru demos!
http://aka.ms/ZeroTrustDemos

RSAConference2019

Demo

Challenge with Multi-Factor Authentication, w/ Apple Watch and Terms of Use to an app when using a non-managed device

Chrome File Edit View History Bookmarks People Window Help

100% Sat Mar 2 7:54 PM

New Tab

mail.google.com/a/soseman.org

mail.google.com/a/soseman.org

mail.google.com/a/soseman.org - Google Search

You've gone incognito

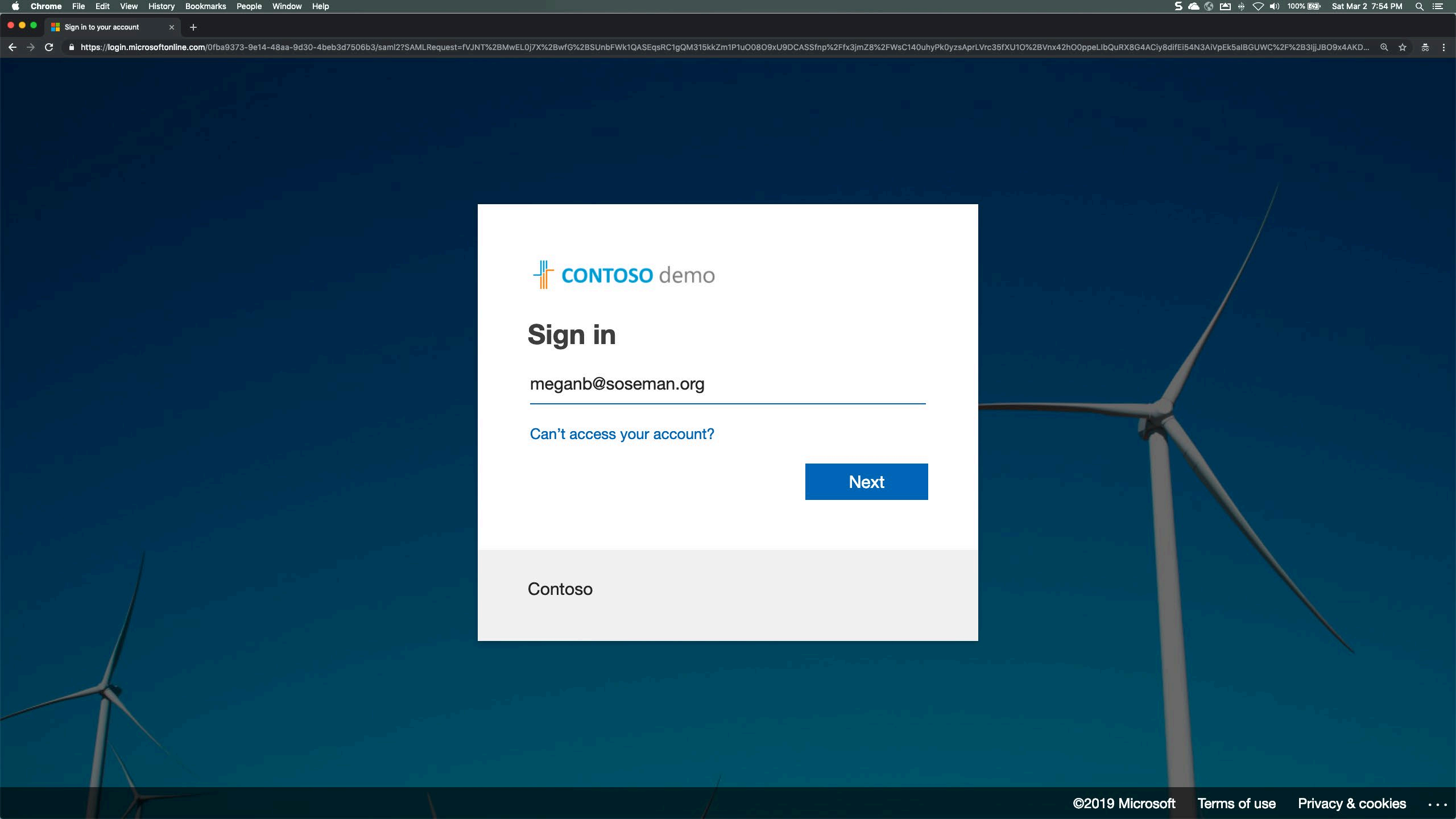
Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

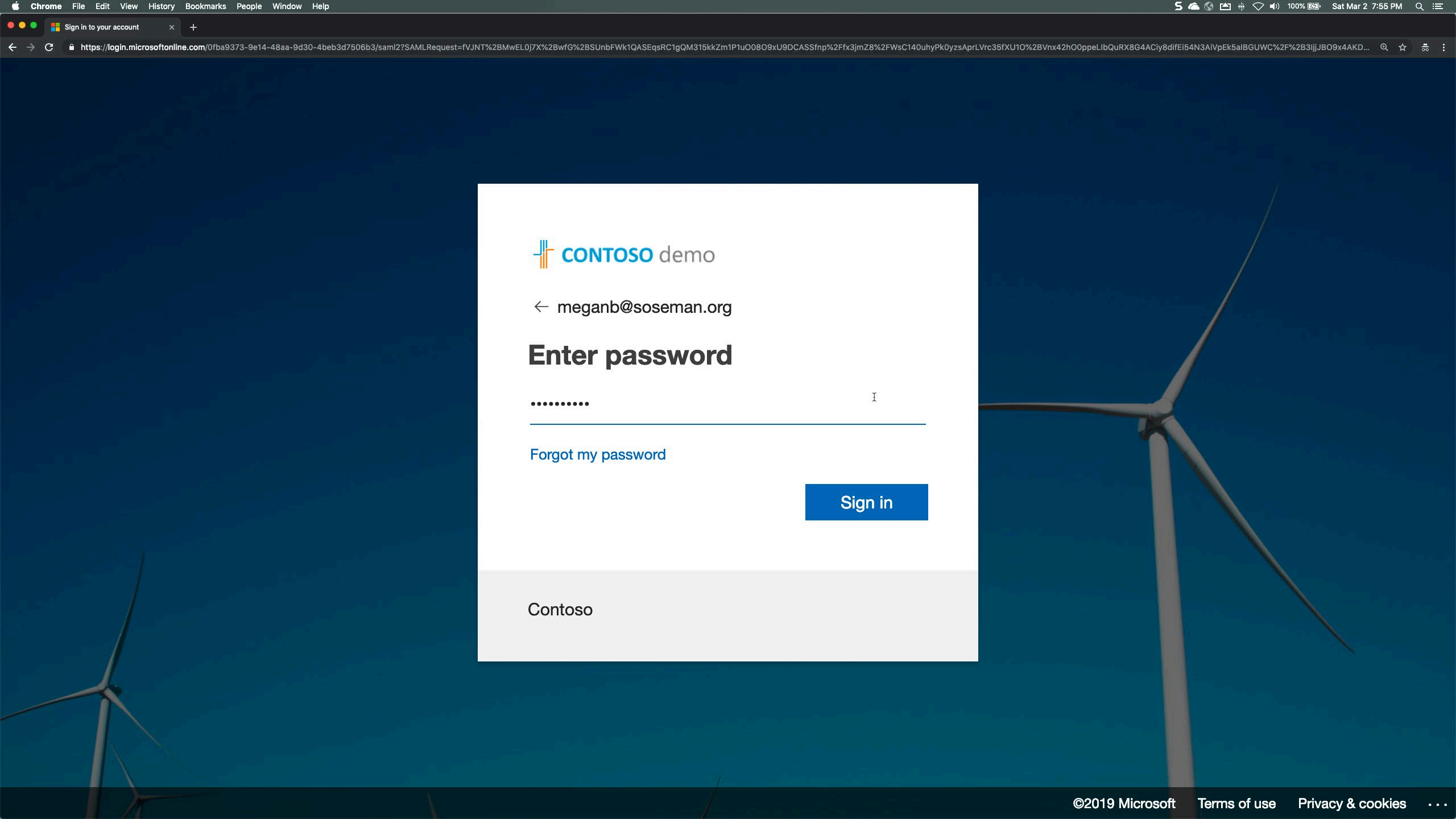
Chrome won't save the following information:

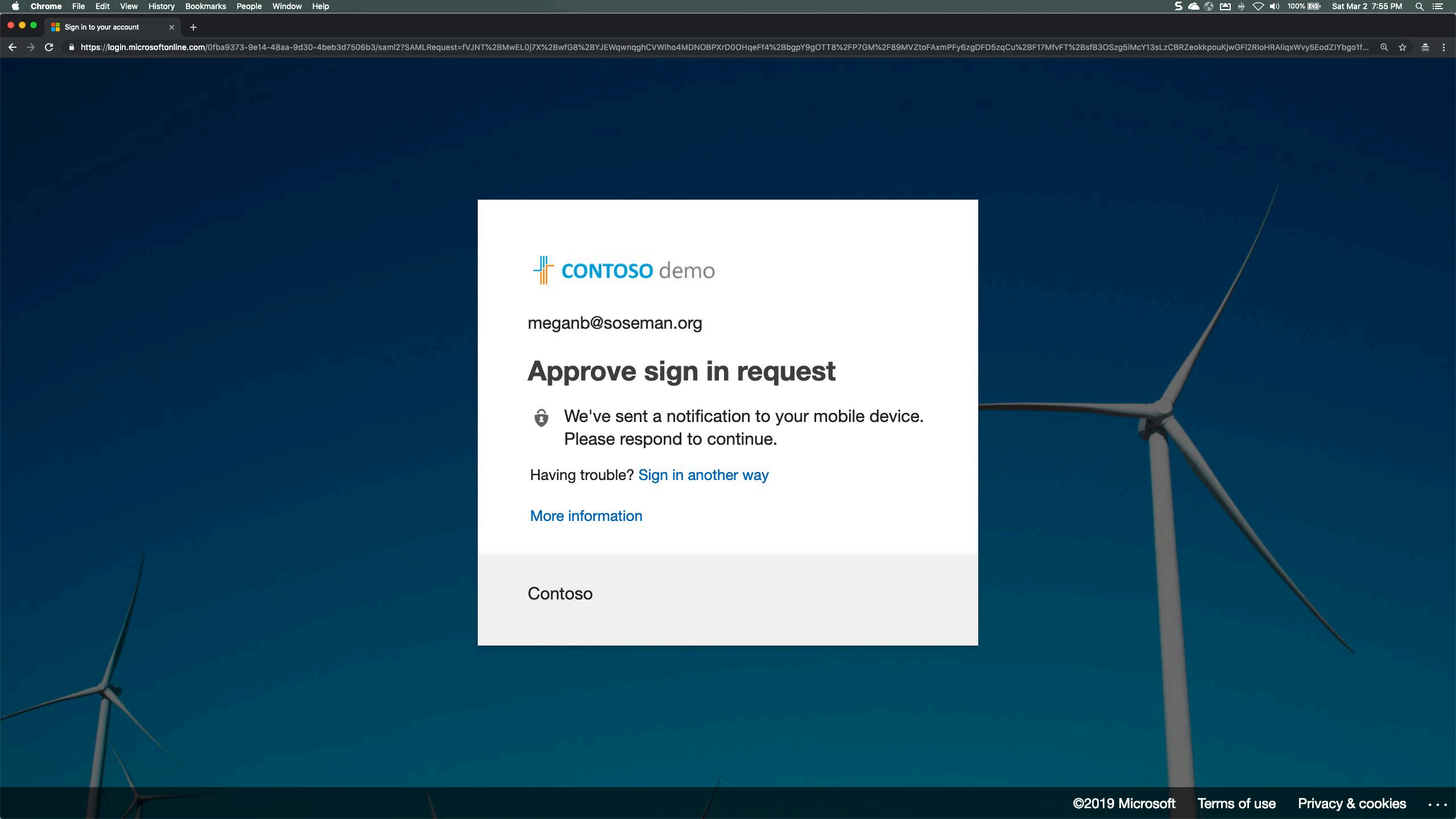
- Your browsing history
- Cookies and site data
- Information entered in forms

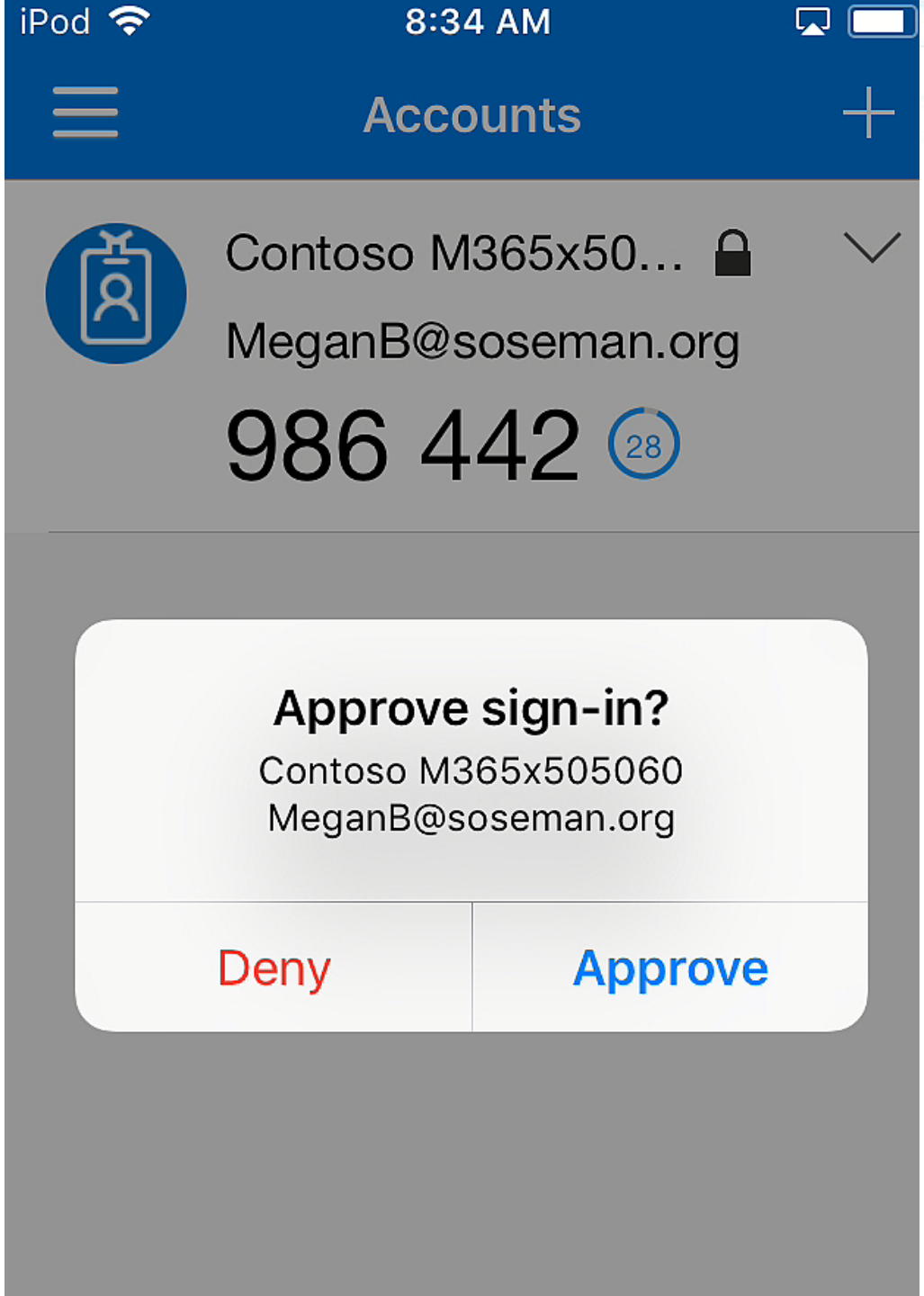
Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

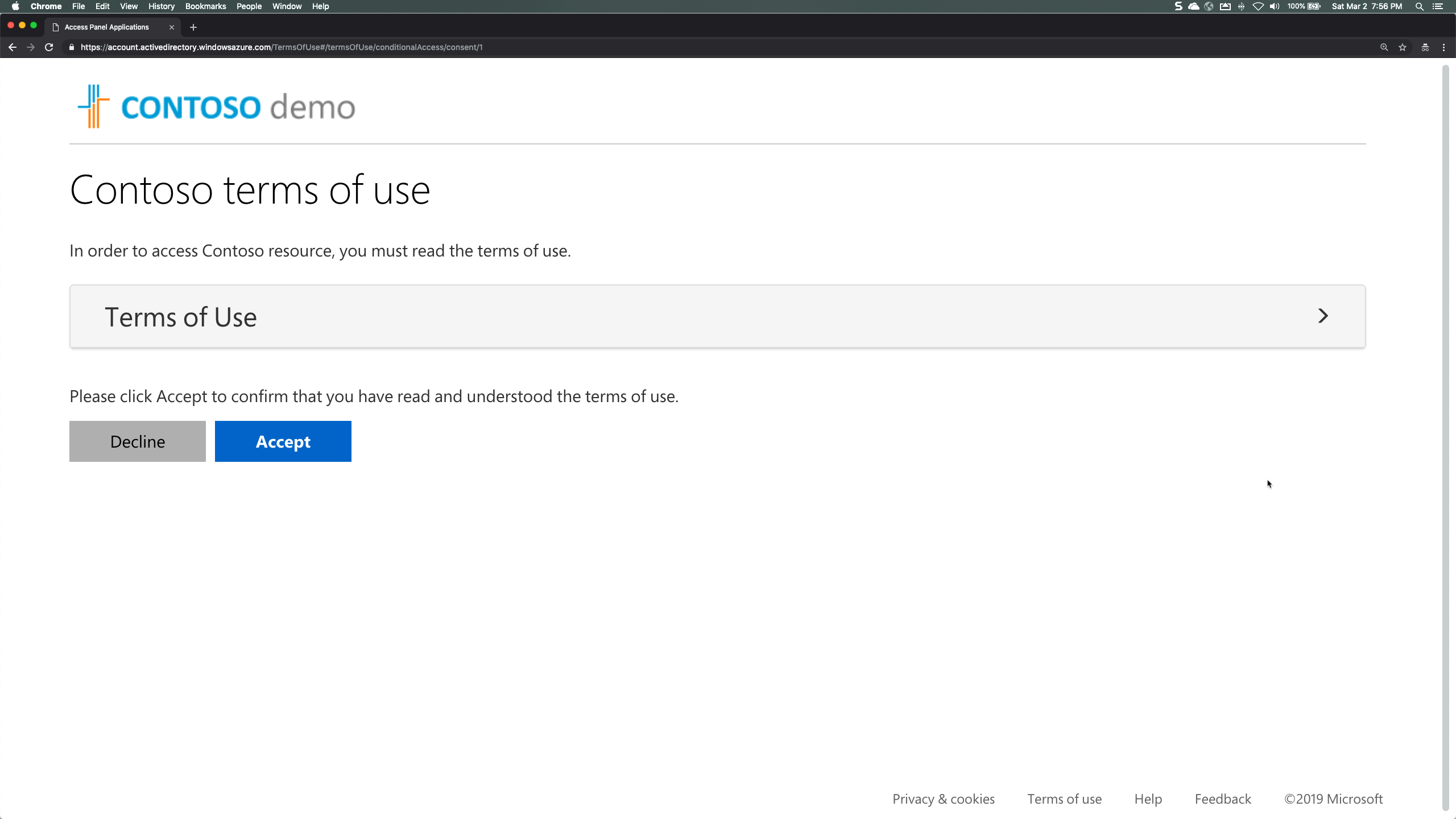

Chrome File Edit View History Bookmarks People Window Help
100% Sat Mar 2 7:54 PM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVJNT%2BMwEL0j7X%2BwfG%2BSUnbFWk1QASEqsRC1gQM315kkZm1P1uO08O9xU9DCASSfnp%2Ffx3jmZ8%2FWsC140uhyPk0yzsAprLVrc35fXU1O%2BVnx42hO0ppeLIbQuRX8G4ACiy8difEi54N3AiVpEk5aIBGUWC%2F%2B3IjJBO9x4AKD...
CONTOSO demo
Sign in
meganb@soseman.org
Can’t access your account?
Next
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies
. . .

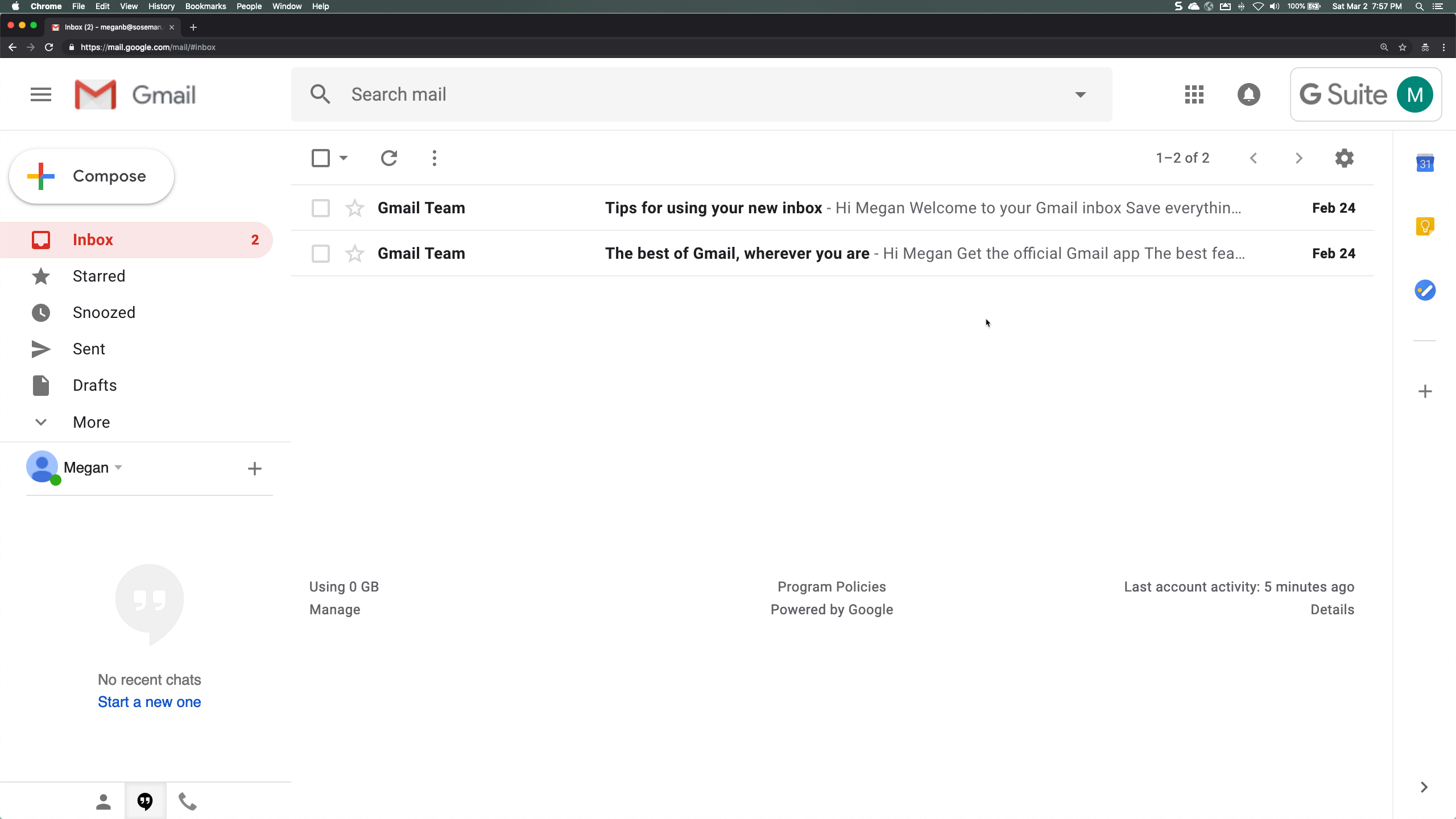

Chrome File Edit View History Bookmarks People Window Help
100% Sat Mar 2 7:55 PM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVJNT%2BMwEL0j7X%2BwfG%2BSUnbFWk1QASEqsRC1gQM315kkZm1P1uO08O9xU9DCASSfnp%2Ffx3jmZ8%2FWsC140uhyPk0yzsAprLVrc35fXU1O%2BVnx42hO0ppeLIbQuRX8G4ACiy8difEi54N3AiVpEk5aIBGUWC%2F%2B3IjJBO9x4AKD...
CONTOSO demo
meganb@soseman.org
Enter password
Forgot my password
Sign in
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies


Chrome File Edit View History Bookmarks People Window Help
100% Sat Mar 2 7:55 PM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVJNT%2BMwEL0j7X%2BwfG8%2BYJEWqwnqghCVWIho4MDNOBPXrD0OHqeFf4%2BbgpY9gOTT8%2FP7GM%2F89MVZtoFAxmPFy6zgDFD5zqCu%2BF17MfvFT%2BsfB3OSzg5iMcY13sLzCBRZeokkpouKjwGFl2RIoHRAliqxWvy5EodZIYbgo1f...
CONTOSO demo
meganb@soseman.org
Approve sign in request
We've sent a notification to your mobile device.
Please respond to continue.
Having trouble? Sign in another way
More information
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies


iPod
8:34 AM
Accounts
Contoso M365x50...
MeganB@soseman.org
986 442
28
Approve sign-in?
Contoso M365x505060
MeganB@soseman.org
Deny
Approve


AUTHENTICATOR
You have received a sign in verification request.
Approve
Deny

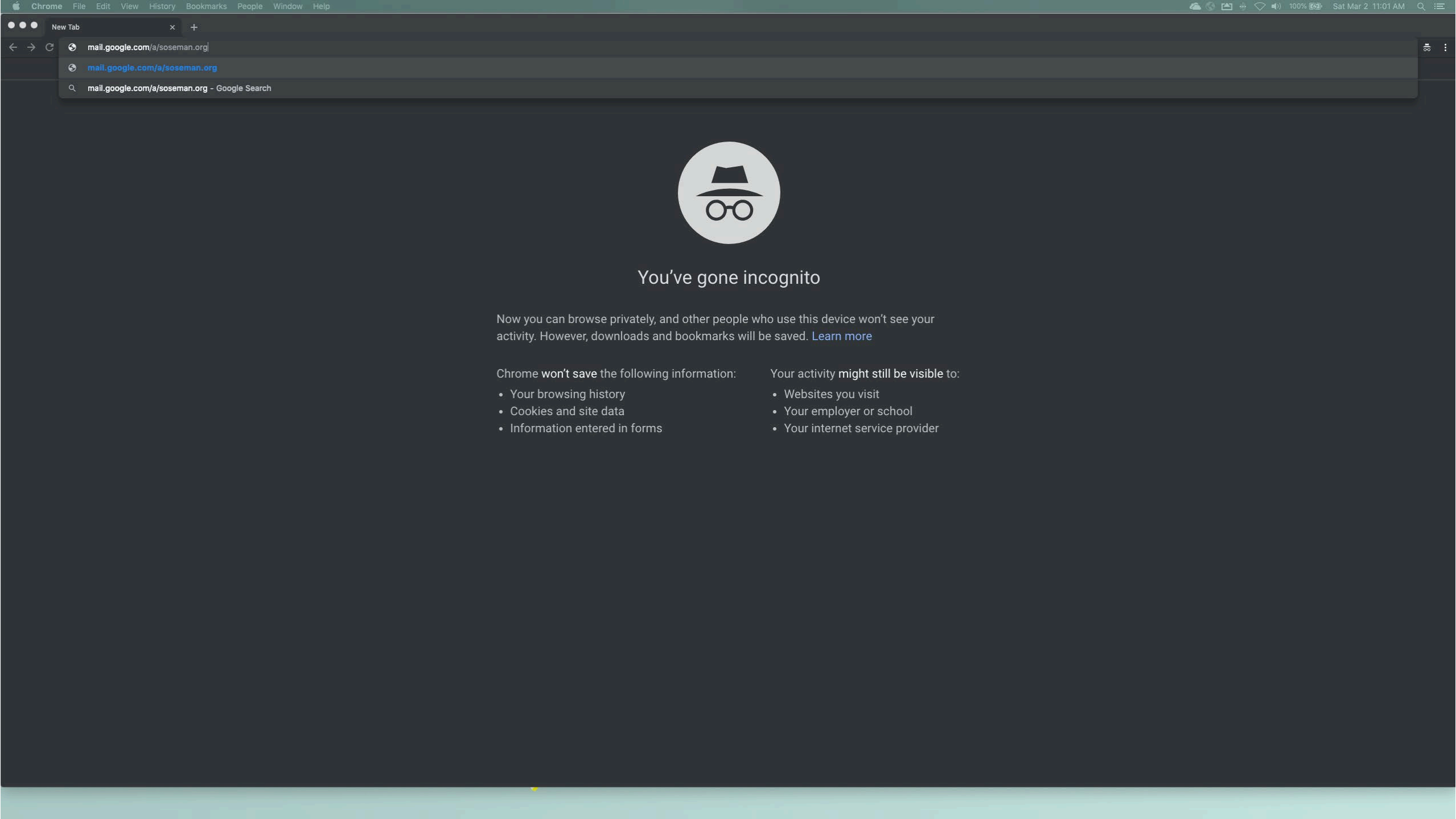

Chrome File Edit View History Bookmarks People Window Help
100% Sat Mar 2 7:56 PM
Access Panel Applications
https://account.activedirectory.windowsazure.com/TermsOfUse#/termsOfUse/conditionalAccess/consent/1
CONTOSO demo
Contoso terms of use
In order to access Contoso resource, you must read the terms of use.
Terms of Use
Please click Accept to confirm that you have read and understood the terms of use.
Decline
Accept
Privacy & cookies
Terms of use
Help
Feedback
©2019 Microsoft

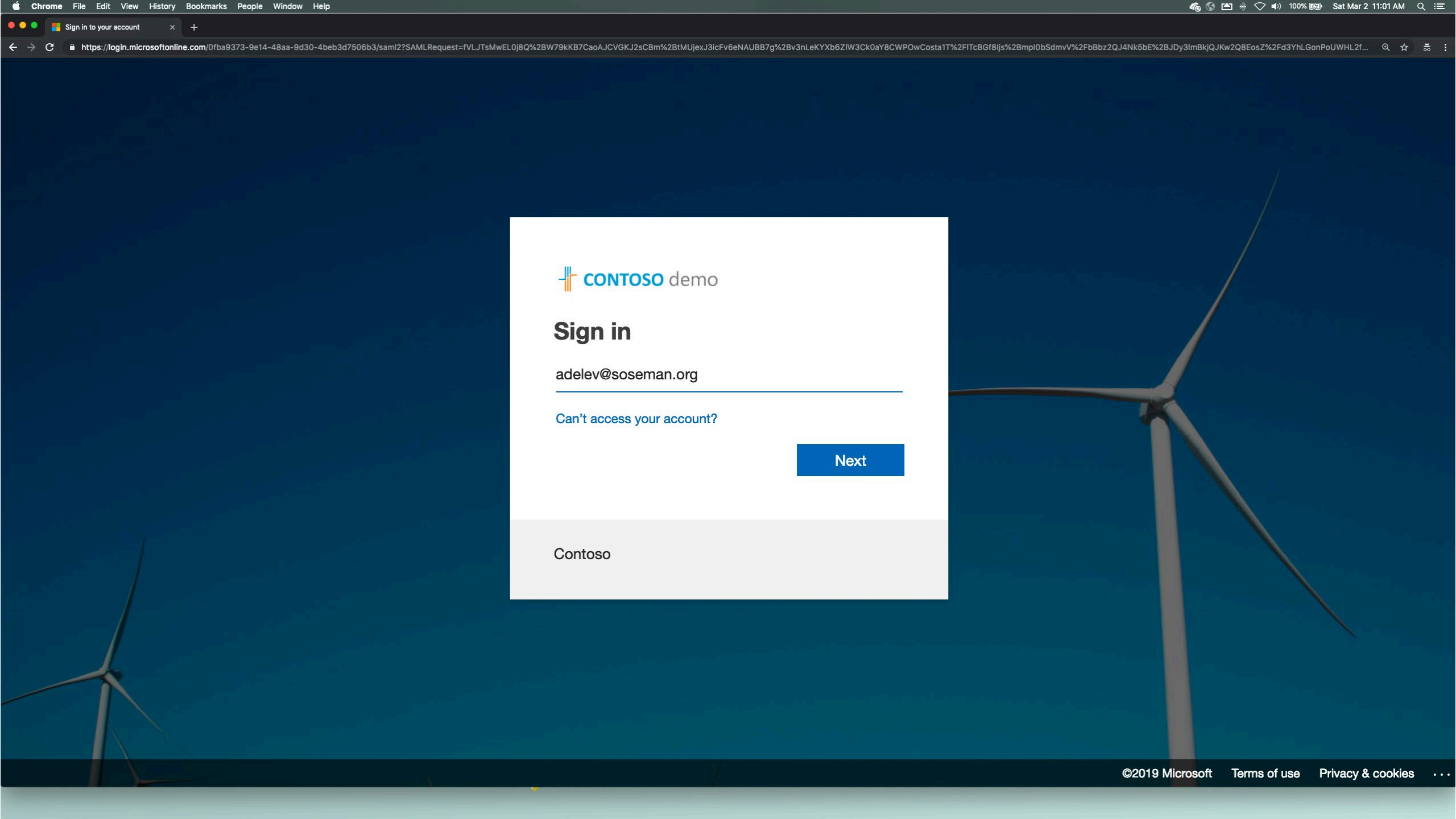

Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 7:57 PM
Inbox (2) - meganb@soseman
https://mail.google.com/mail/#inbox
Gmail
Search mail
G Suite
M
Compose
Inbox 2
Starred
Snoozed
Sent
Drafts
More
Megan
1–2 of 2
Gmail Team Tips for using your new inbox - Hi Megan Welcome to your Gmail inbox Save everythin... Feb 24
Gmail Team The best of Gmail, wherever you are - Hi Megan Get the official Gmail app The best fea... Feb 24
Using 0 GB
Manage
Program Policies
Powered by Google
Last account activity: 5 minutes ago
Details
No recent chats
Start a new one

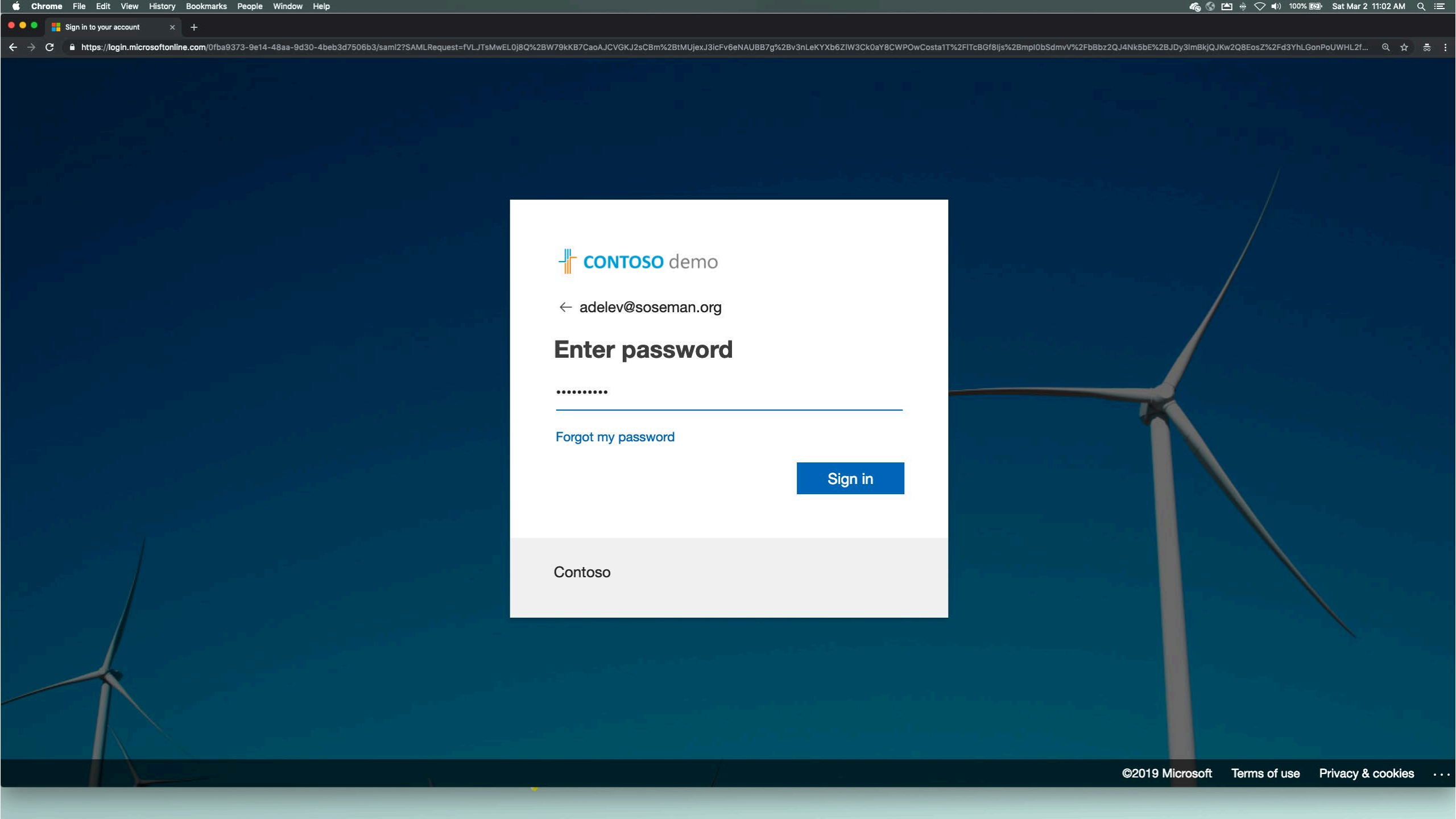
RSAConference2019

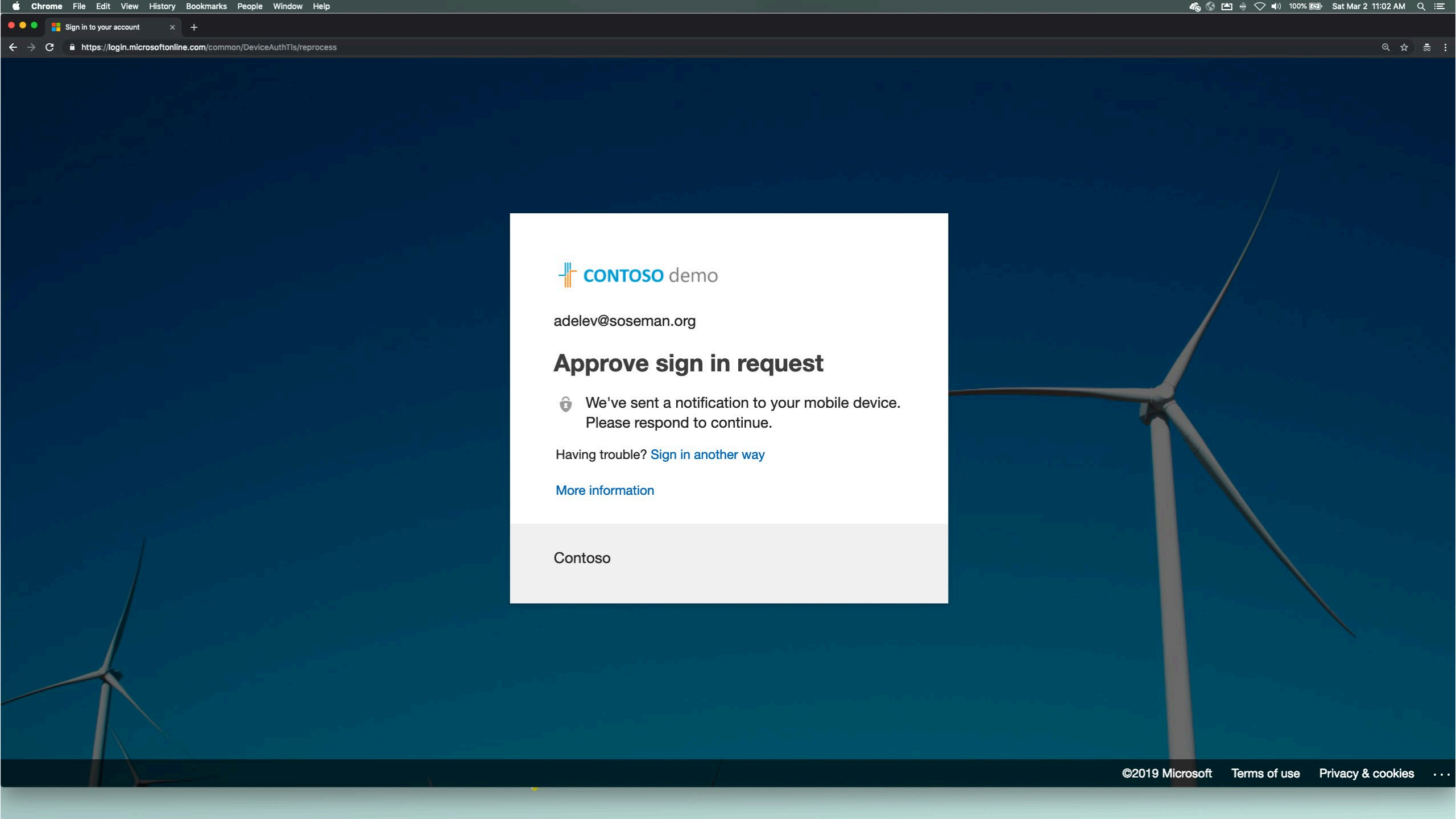
Demo

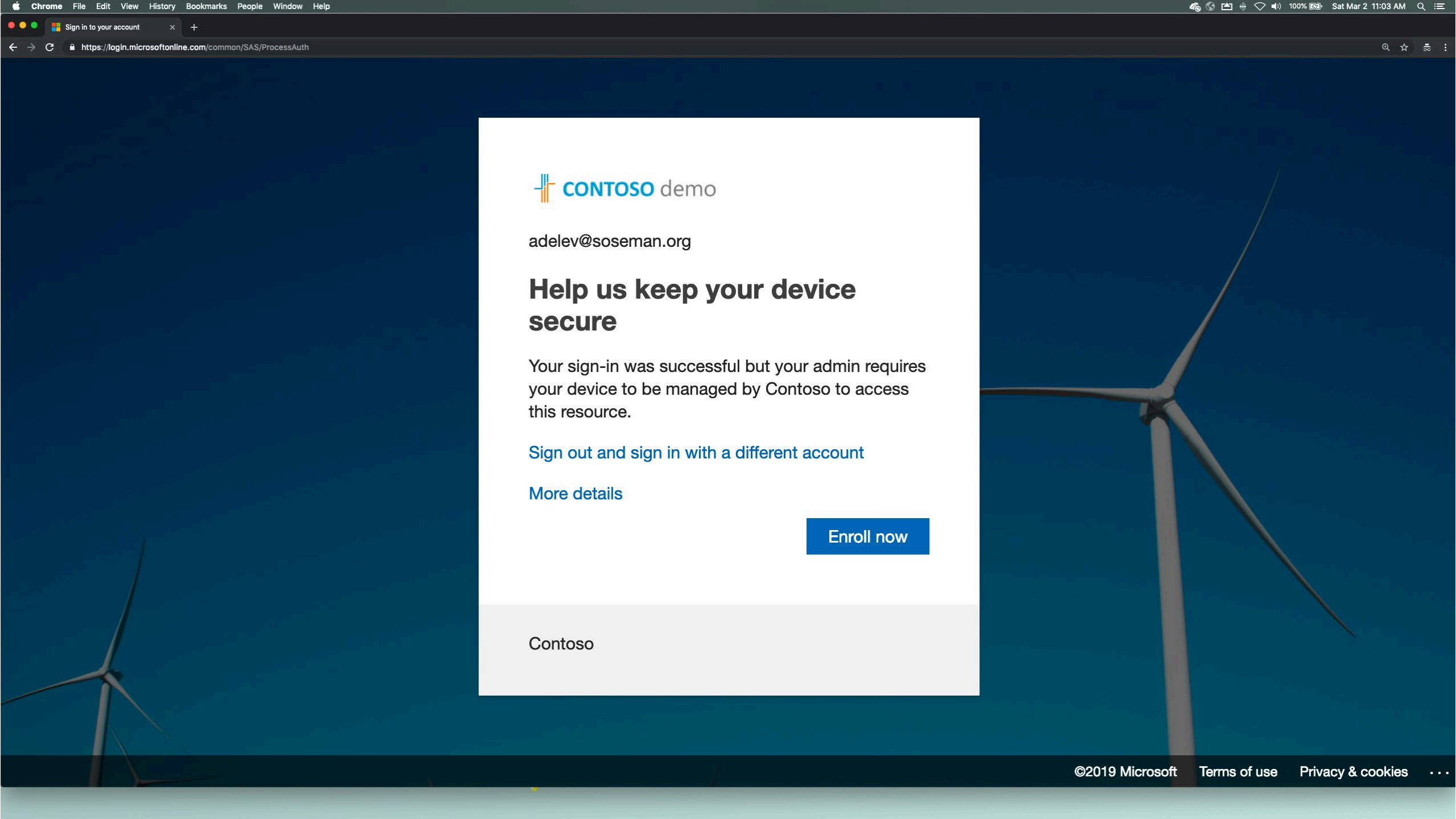
Require device is managed and compliant to access corporate resources


Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 11:01 AM
New Tab
mail.google.com/a/soseman.org
mail.google.com/a/soseman.org
mail.google.com/a/soseman.org - Google Search
You've gone incognito
Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more
Chrome won't save the following information:
Your browsing history
Cookies and site data
Information entered in forms
Your activity might still be visible to:
Websites you visit
Your employer or school
Your internet service provider


Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 11:01 AM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVLJTsMwEL0j8Q%2BW79kKB7CaoAJCVGKJ2sCBm%2BtMUjexJ3icFv6eNAUBB7g%2Bv3nLeKYXb6ZlW3Ck0aY8CWPOwCosta1T%2FITcBGf8Ijs%2BmpI0bSdmvV%2FbBbz2QJ4Nk5bE%2BJDy3lmBkjQJKw2Q8EosZ%2Fd3YhLGonPoUWHL2f...
CONTOSO demo
Sign in
adelev@soseman.org
Can't access your account?
Next
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies
...


Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 11:02 AM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVLJTsMwEL0j8Q%2BW79kKB7CaoAJCVGKJ2sCBm%2BtMUjexJ3icFv6eNAUBB7g%2Bv3nLeKYXb6ZlW3Ck0aY8CWPOwCosta1T%2FITcBGf8Ijs%2BmpI0bSdmvV%2FbBbz2QJ4Nk5bE%2BJDy3ImBkjQJKw2Q8EosZ%2Fd3YhLGonPoUWHL2f...
CONTOSO demo
adelev@soseman.org
Enter password
Forgot my password
Sign in
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies

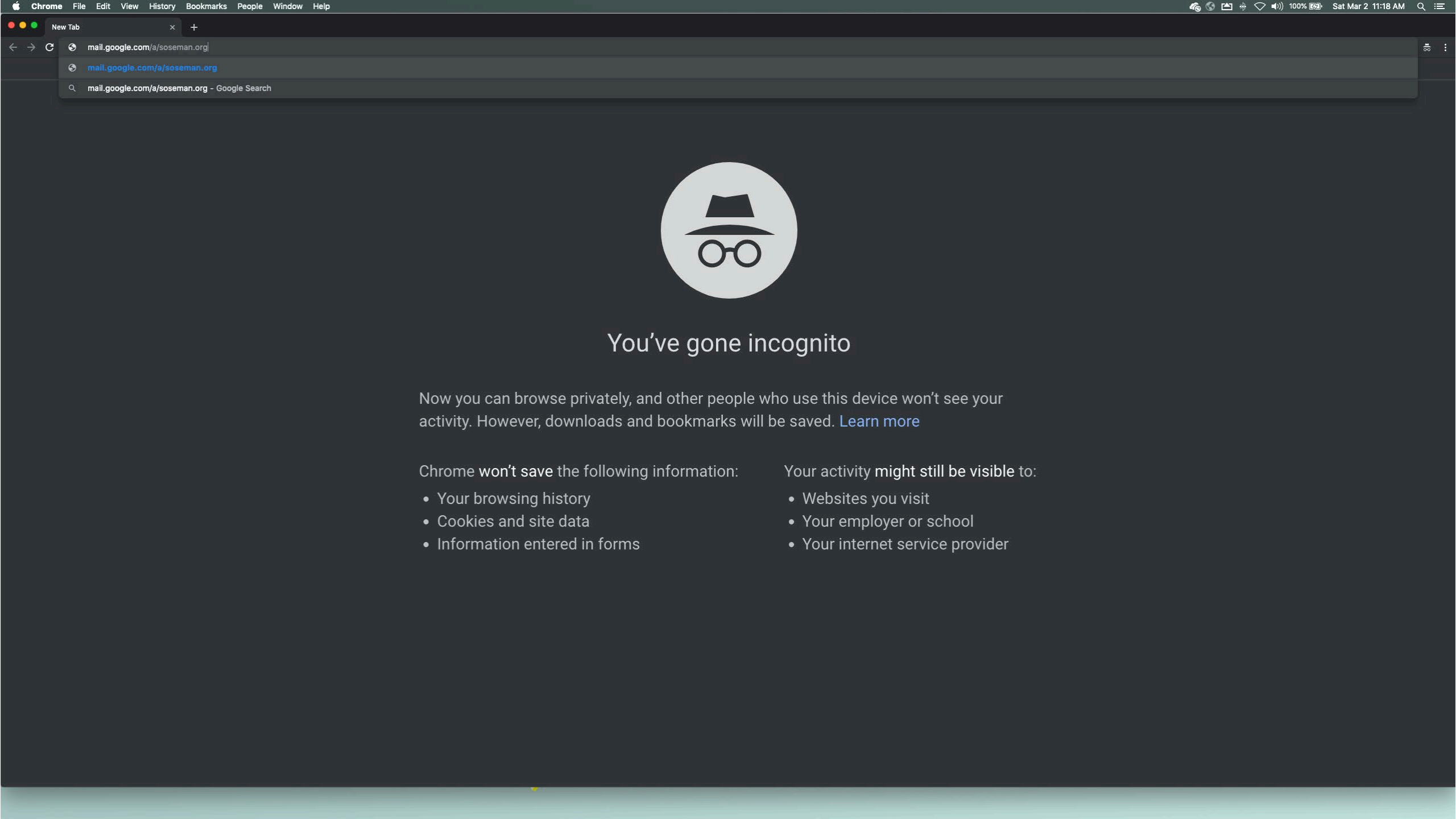

Chrome File Edit View History Bookmarks People Window Help
100% Sat Mar 2 11:02 AM
Sign in to your account
https://login.microsoftonline.com/common/DeviceAuthTls/reprocess
CONTOSO demo
adelev@soseman.org
Approve sign in request
We've sent a notification to your mobile device. Please respond to continue.
Having trouble? Sign in another way
More information
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies

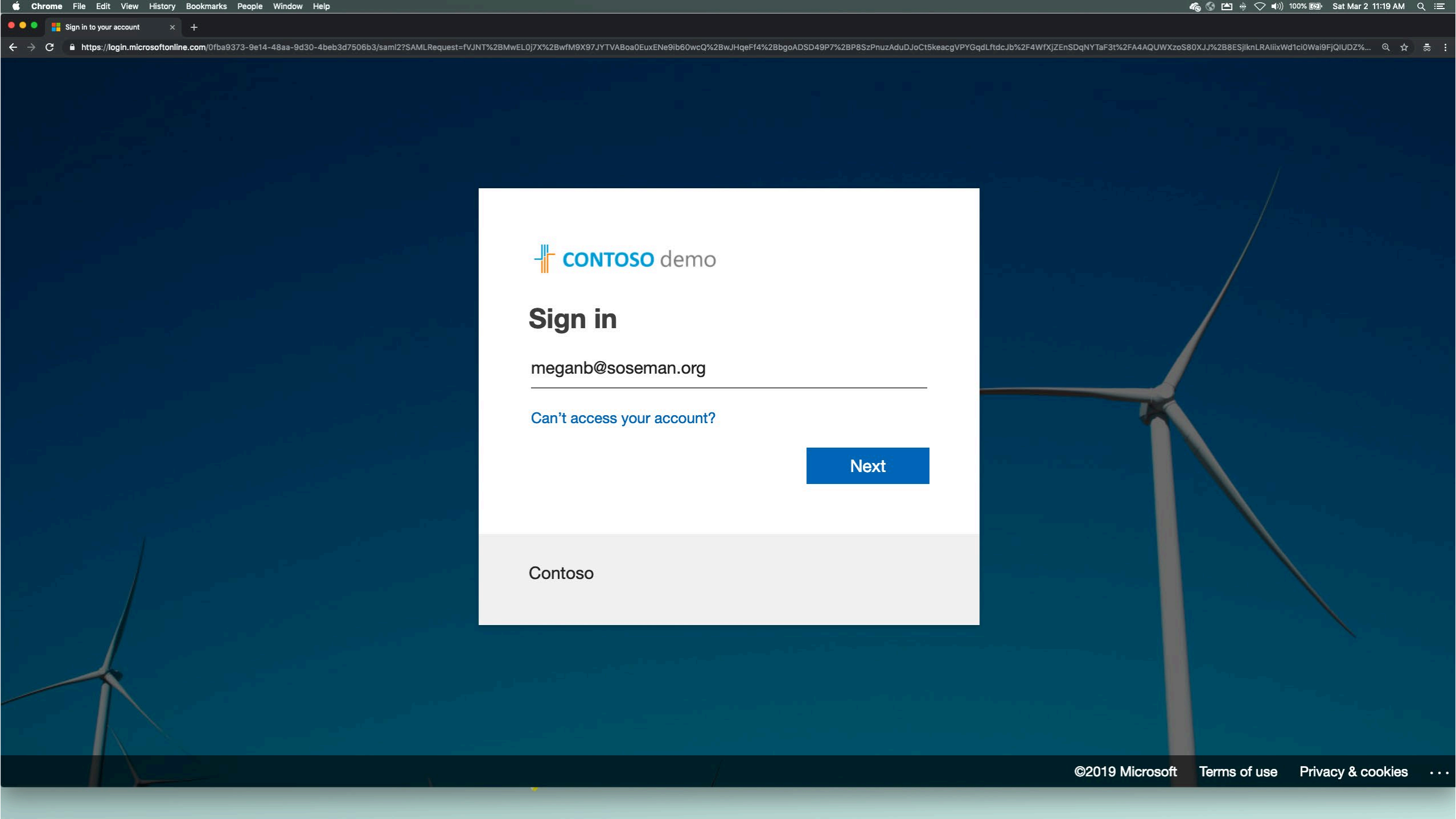

Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 11:03 AM
Sign in to your account
https://login.microsoftonline.com/common/SAS/ProcessAuth
CONTOSO demo
adelev@soseman.org
Help us keep your device secure
Your sign-in was successful but your admin requires your device to be managed by Contoso to access this resource.
Sign out and sign in with a different account
More details
Enroll now
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies

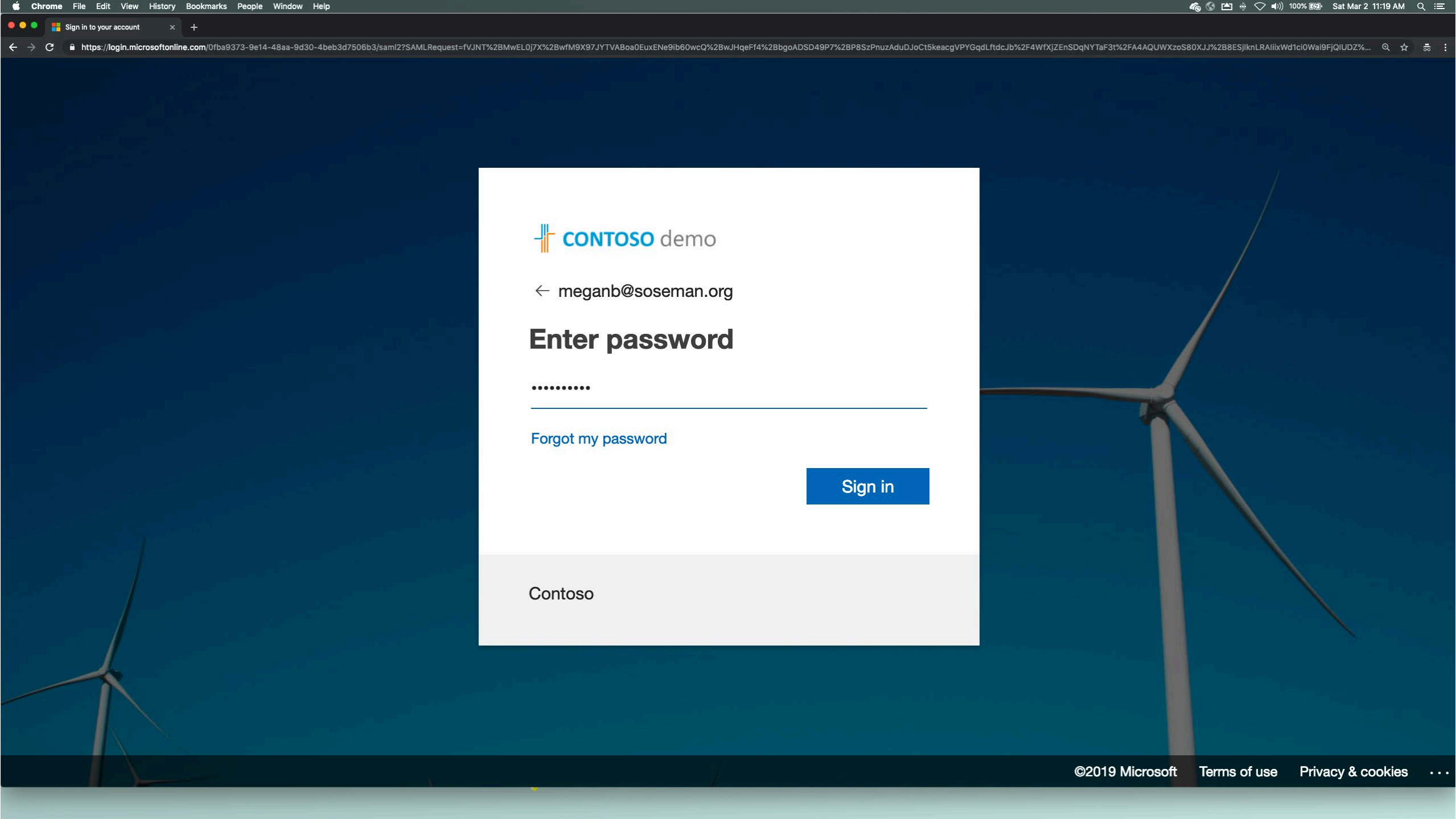
RSAConference2019

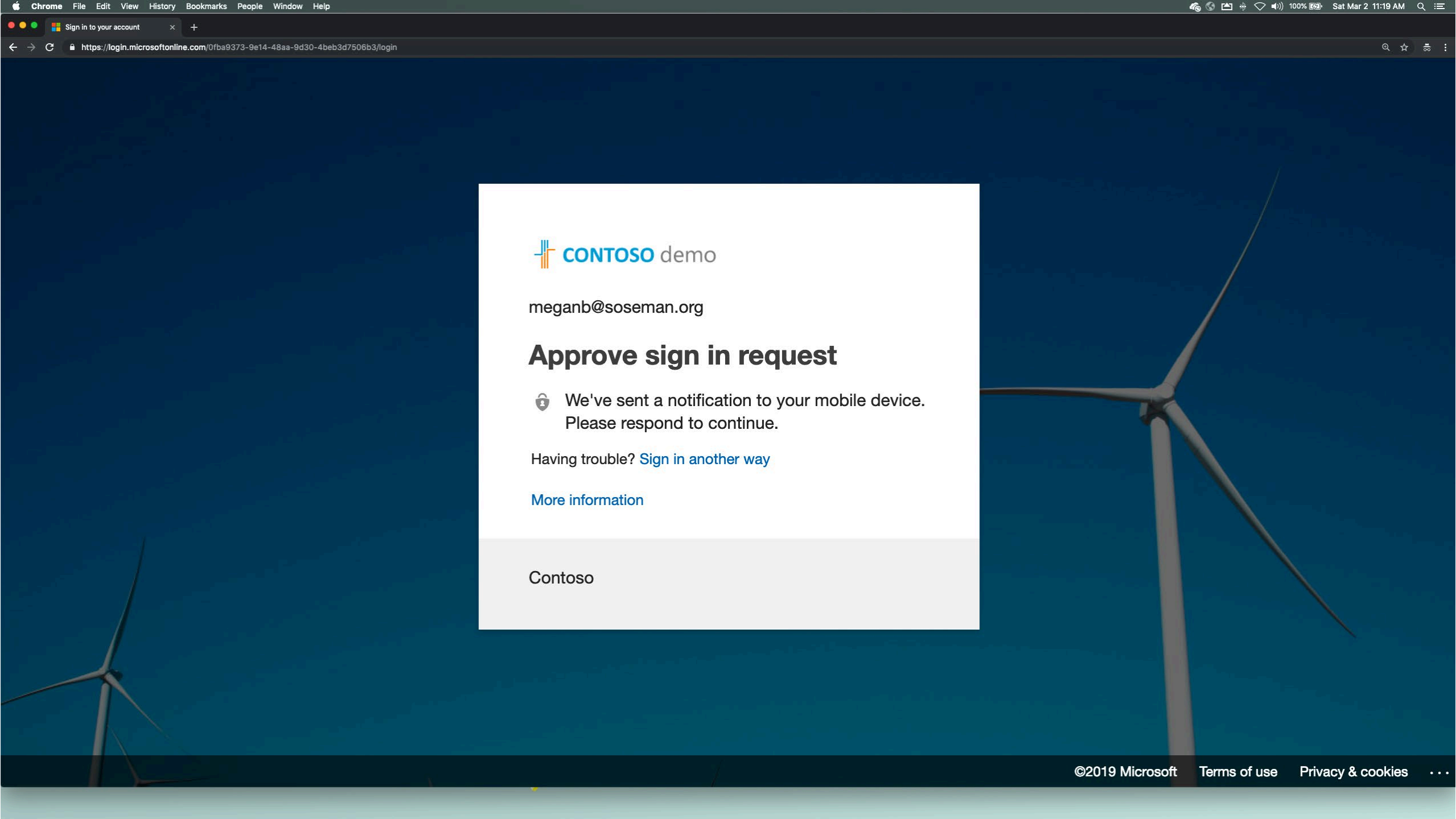
Demo

Limiting and auditing session access from a non-managed device (i.e. prevent download from app or apply DLP to downloaded files)


Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 11:18 AM
New Tab
mail.google.com/a/soseman.org
mail.google.com/a/soseman.org
mail.google.com/a/soseman.org - Google Search
You've gone incognito
Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more
Chrome won't save the following information:
Your browsing history
Cookies and site data
Information entered in forms
Your activity might still be visible to:
Websites you visit
Your employer or school
Your internet service provider


Chrome File Edit View History Bookmarks People Window Help
100% Sat Mar 2 11:19 AM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVJNT%2BMwEL0j7X%2BwfM9X97JYTVABoa0EuxENe9ib60wcQ%2BwJHqeFf4%2BbgoADSD49P7%2BP8SzPnuzAduDJoCt5keacgVPYGqdLftdcJb%2F4WfXjZEnSDqNYTaF3t%2FA4AQUWXzoS80XJJ%2B8ESjiknLRAIixWd1ci0Wai9FjQIUDZ%...
CONTOSO demo
Sign in
meganb@soseman.org
Can't access your account?
Next
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies
. . .

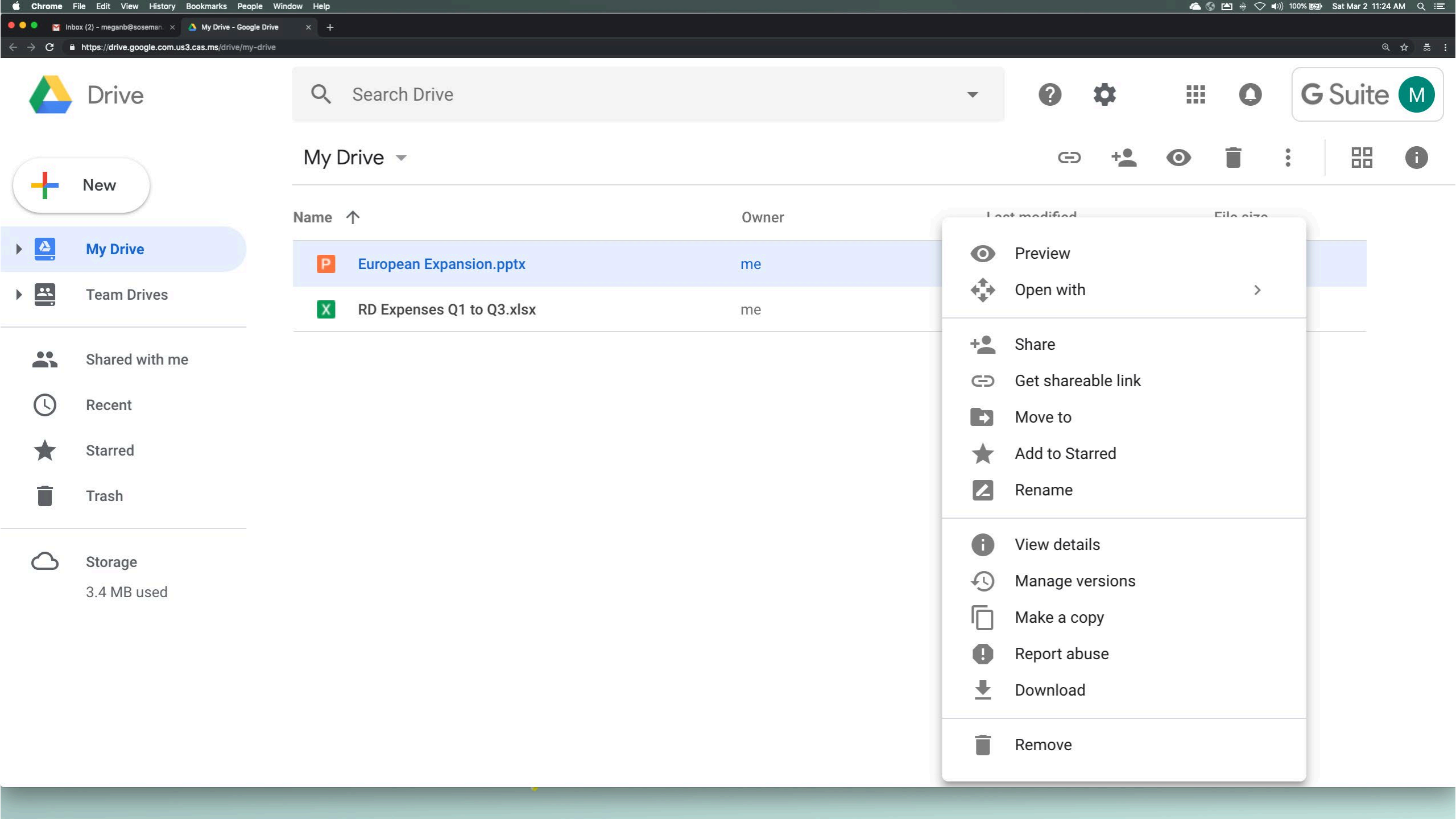

Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 11:19 AM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVJNT%2BMwEL0j7X%2BwfM9X97JYTVABoa0EuxENe9ib60wcQ%2BwJHqeFf4%2BbgoADSD49P7%2BP8SzPnuzAduDJoCt5keacgVPYGqdLftdcJb%2F4WfXjZEnSDqNYTaF3t%2FA4AQUWXzoS80XJJ%2B8ESjiknLRAIixWd1ci0Wai9FjQIUDZ%...
CONTOSO demo
meganb@soseman.org
Enter password
Forgot my password
Sign in
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies

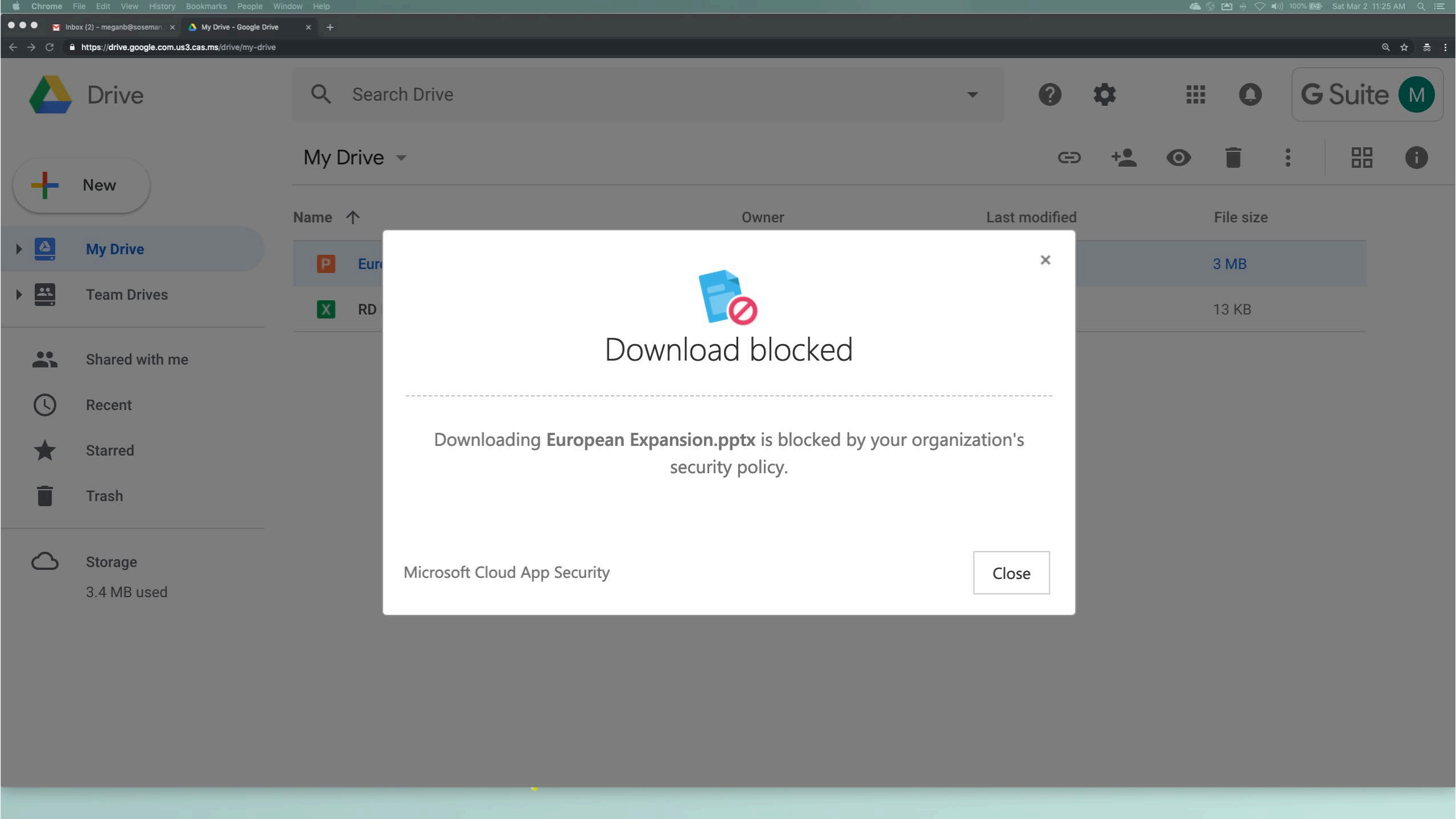

Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 11:19 AM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/login
CONTOSO demo
meganb@soseman.org
Approve sign in request
We've sent a notification to your mobile device.
Please respond to continue.
Having trouble? Sign in another way
More information
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies

Access to G Suite is monitored

For improved security, your organization allows access to **G Suite** in monitor mode.
Access is only available from a web browser.

Continue to G Suite


Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 11:24 AM
Inbox (2) - meganb@soseman
My Drive - Google Drive
https://drive.google.com.us3.cas.ms/drive/my-drive
Drive
Search Drive
G Suite
M
My Drive
New
My Drive
Team Drives
Shared with me
Recent
Starred
Trash
Storage
3.4 MB used
Name
Owner
European Expansion.pptx
me
RD Expenses Q1 to Q3.xlsx
me
Preview
Open with
Share
Get shareable link
Move to
Add to Starred
Rename
View details
Manage versions
Make a copy
Report abuse
Download
Remove


Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 11:25 AM
Inbox (2) - meganb@soseman
My Drive - Google Drive
https://drive.google.com.us3.cas.ms/drive/my-drive
Drive
Search Drive
G Suite
M
New
My Drive
Team Drives
Shared with me
Recent
Starred
Trash
Storage
3.4 MB used
My Drive
Name
Owner
Last modified
File size
Eur
3 MB
RD
13 KB
Download blocked
Downloading European Expansion.pptx is blocked by your organization's security policy.
Microsoft Cloud App Security
Close

Cloud App Security

Discovered apps
IP addresses
Users
Machines
Cloud app catalog
Create snapshot report

Investigate
Activity log
Files
Users and accounts
Security configuration
OAuth apps
Connected apps (5)

Control
Policies
Templates

Alerts 34

Activity log

QUERIES: Select a query...

APP: G Suite, ... | USER NAME: Select u... | RAW IP ADDRESS: Enter IP address... | ACTIVITY TYPE: Select a... | LOCATION: Select c...

Save as | Advanced

1 - 20 of 122 activities

New policy from search

Activity	User	App	IP address	Location	Device	Date
Download file: file Eur...	Megan Bowen (meganb@s...	—	70.95.74.144	United ...		Mar 2, 2019, ...

SHOW SIMILAR

General | User | IP address

Send us feedback...

Description: Download file: file **European Expansion.pptx**

Type: Download > Download file
User: Megan Bowen (meganb@so...
Date: Mar 2, 2019, 11:24 AM
IP address: 70.95.74.144

Type (in app): Download File
User organizational unit: —
Device type: PC, OS X, Chrome 72.0
IP category: —

Source: Session control
User groups: Office 365 administrator...
User agent tags: —
Tags: —

ID: 1551554684249_29f6e320-c73...
Activity objects: 2 European Expansion.pp...
App: —
Location: United States, California,...

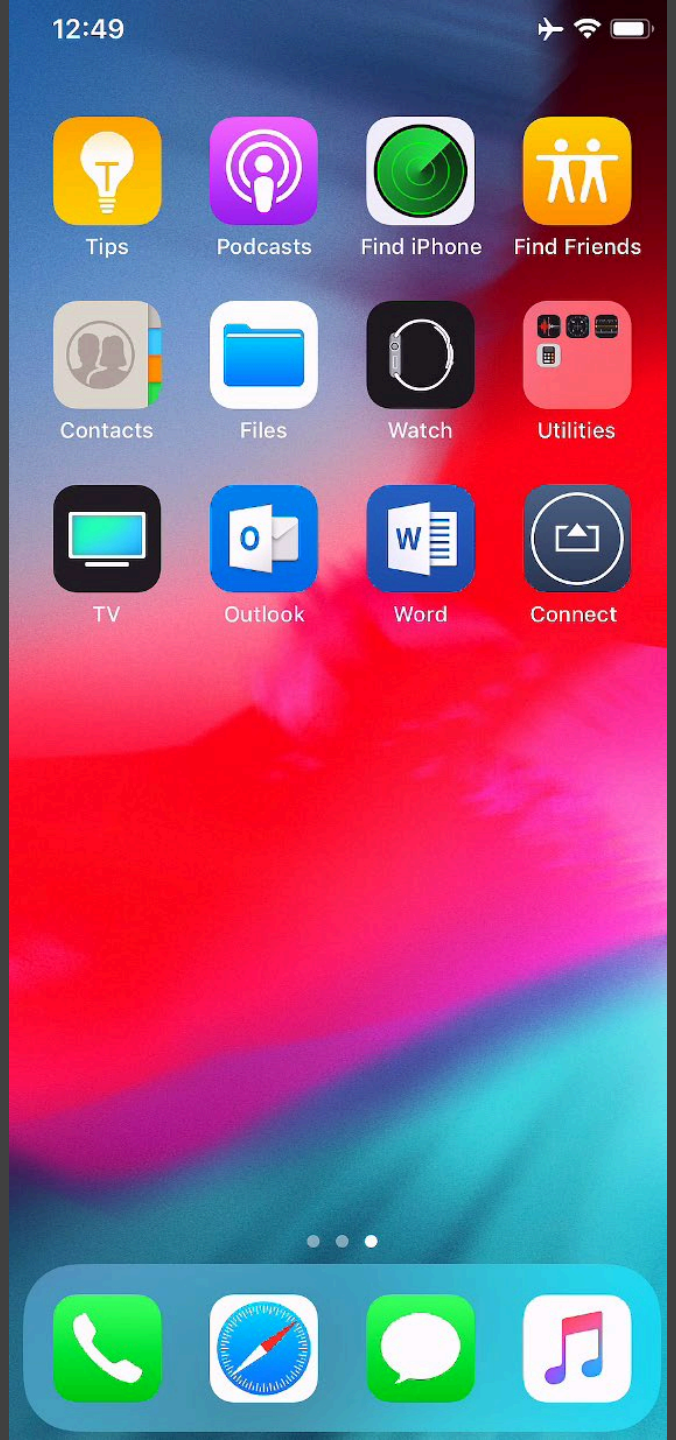
Matched policies: Megan Session Control ...
ISP: Spectrum

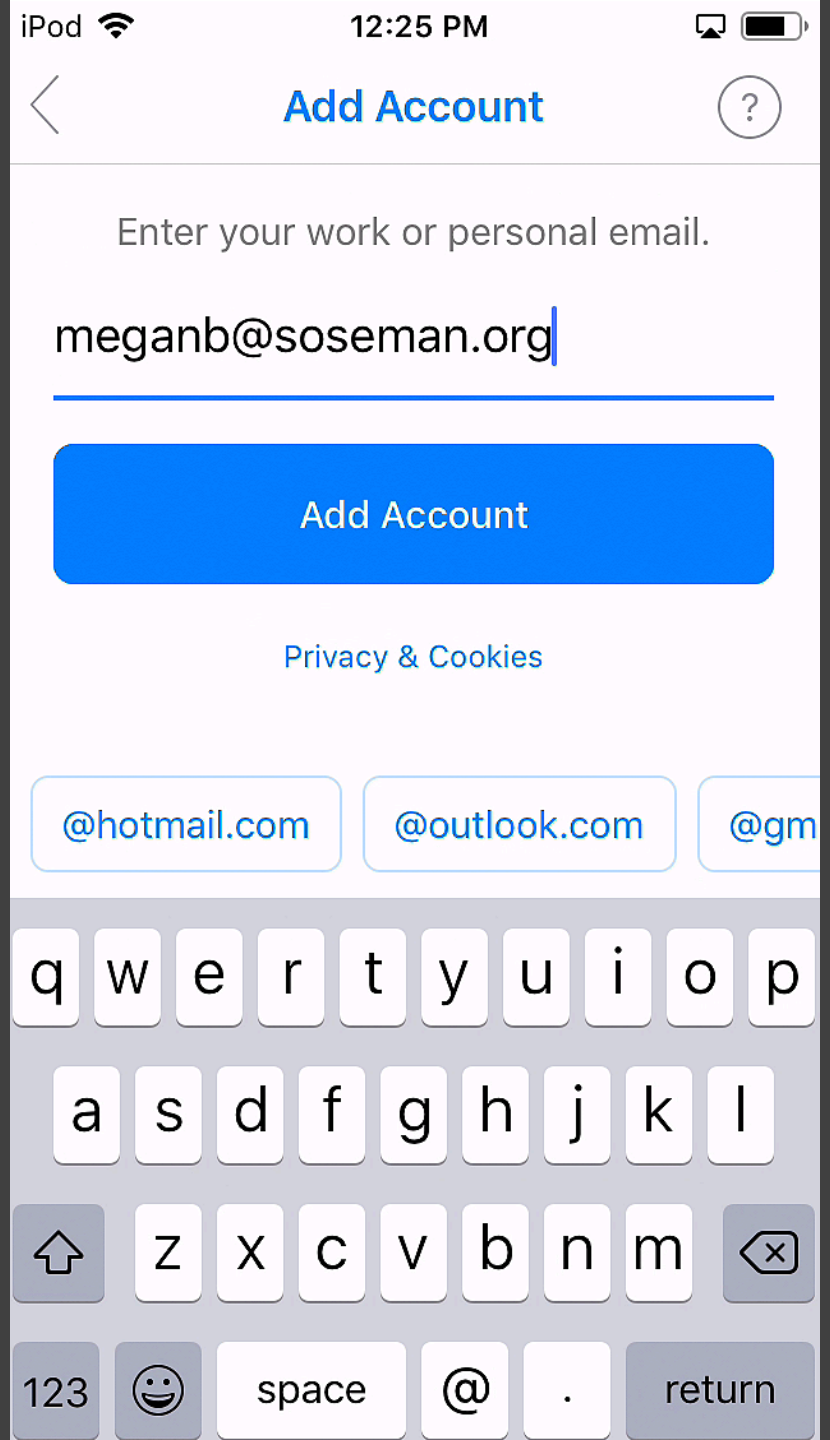
Trash file: file Getting started	Megan Bowen (meganb@s...	G-Suite	104.45.170.180	Uni...	—	Mar 2, 2019, ...
Upload file: file European Ex	Megan Bowen (meganb@s...	G-Suite	104.45.170.70	Uni...	—	Mar 2, 2019

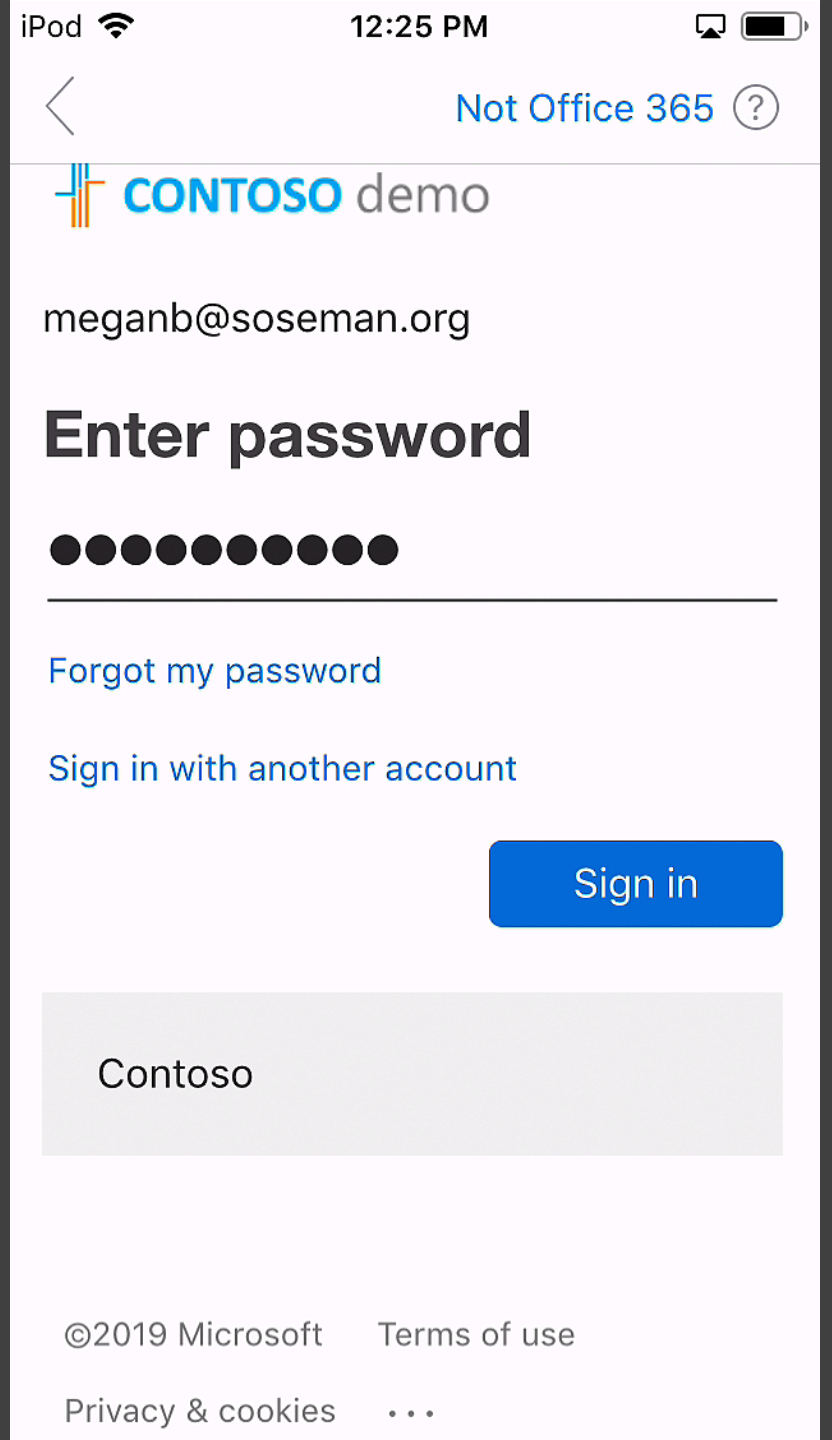
RSAConference2019

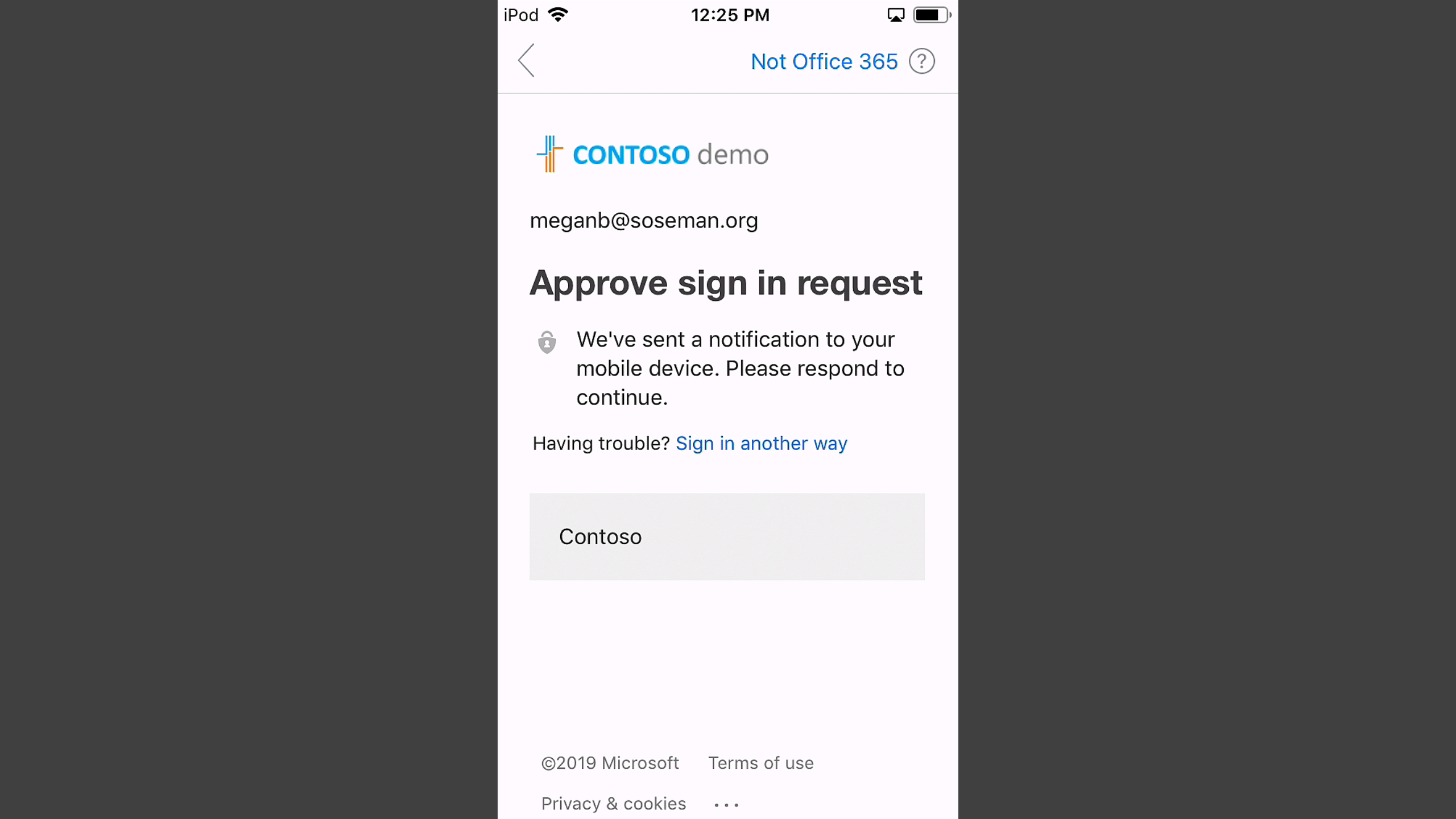
Demo

Govern data access on unmanaged device by protecting data in the managed app

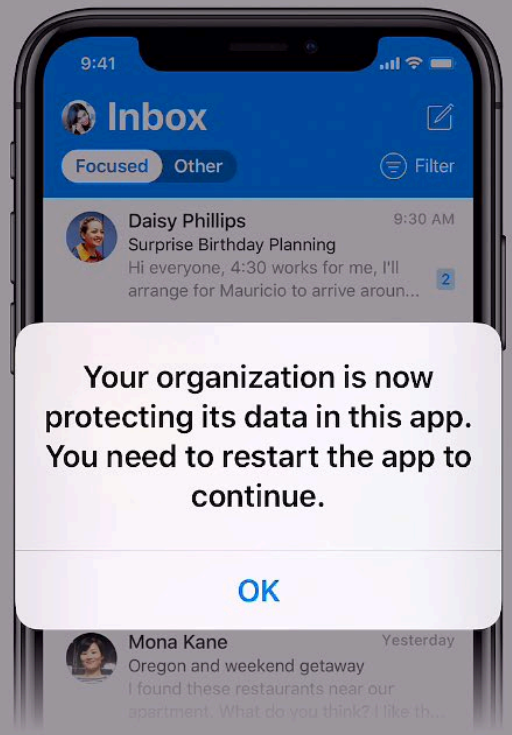

12:49
Tips
Podcasts
Find iPhone
Find Friends
Contacts
Files
Watch
Utilities
TV
Outlook
Word
Connect


iPod
12:25 PM
Add Account
Enter your work or personal email.
meganb@soseman.org
Add Account
Privacy & Cookies
@hotmail.com
@outlook.com
@gm
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
@
.
return


iPod
12:25 PM
Not Office 365
CONTOSO demo
meganb@soseman.org
Enter password
Forgot my password
Sign in with another account
Sign in
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies


iPod
12:25 PM
Not Office 365
CONTOSO demo
meganb@soseman.org
Approve sign in request
We've sent a notification to your mobile device. Please respond to continue.
Having trouble? Sign in another way
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies
• • •

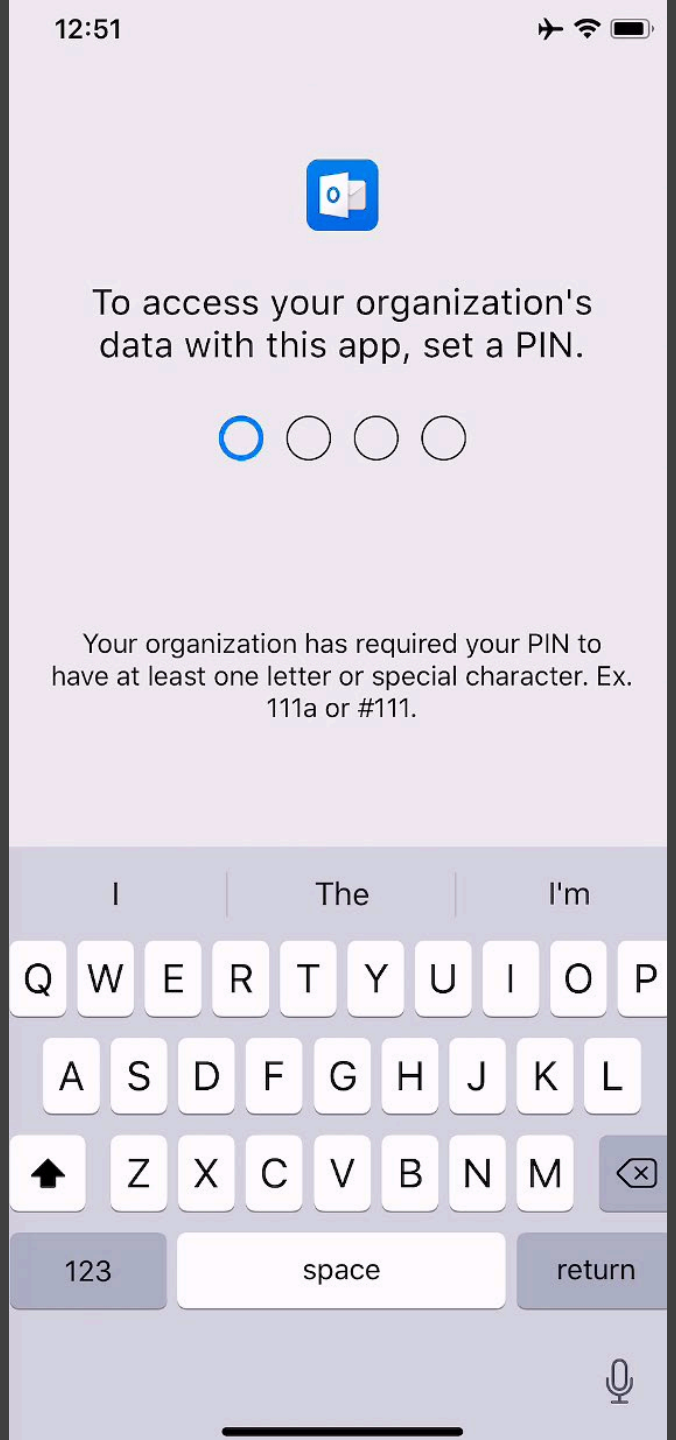
12:50

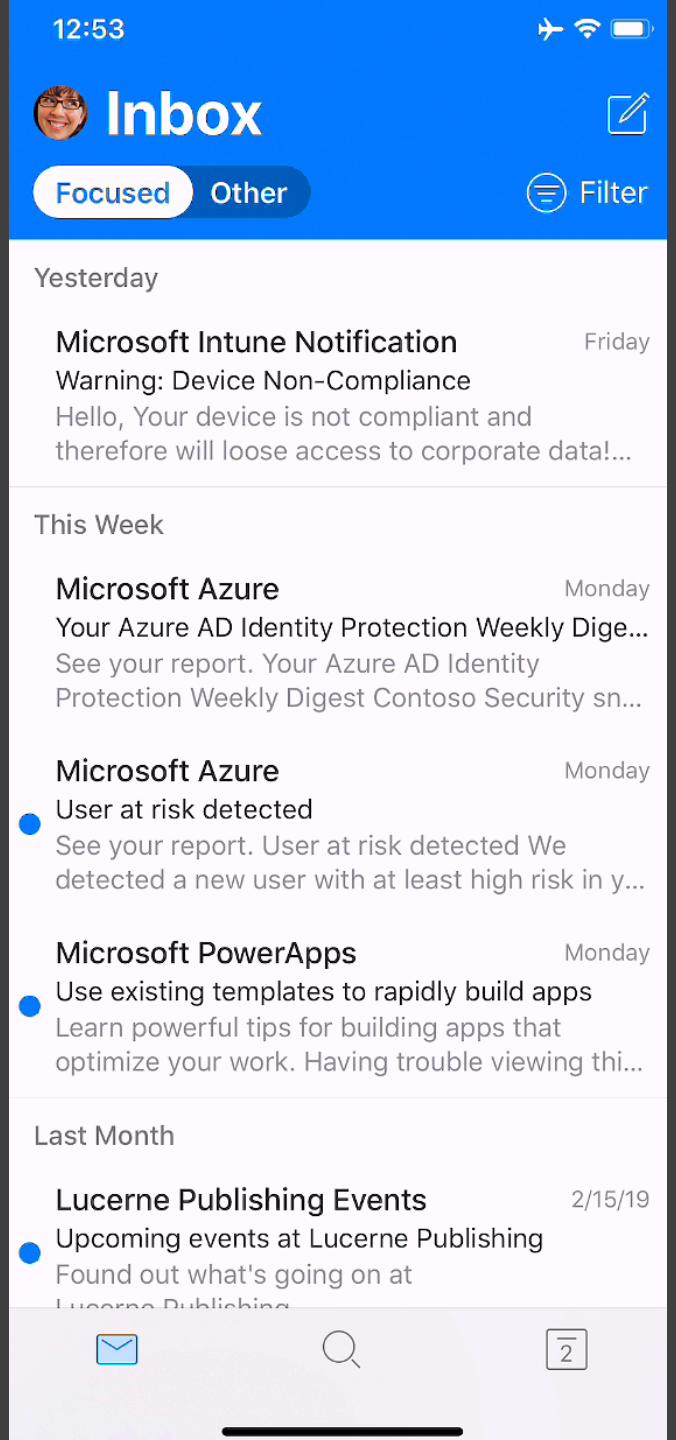


Focused Inbox

Find the email you need to act on right here.

Skip


12:51
To access your organization's data with this app, set a PIN.
Your organization has required your PIN to have at least one letter or special character. Ex. 111a or #111.
I
The
I'm
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return


12:53
Inbox
Focused
Other
Filter
Yesterday
Microsoft Intune Notification
Friday
Warning: Device Non-Compliance
Hello, Your device is not compliant and therefore will loose access to corporate data!...
This Week
Microsoft Azure
Monday
Your Azure AD Identity Protection Weekly Dige...
See your report. Your Azure AD Identity Protection Weekly Digest Contoso Security sn...
Microsoft Azure
Monday
User at risk detected
See your report. User at risk detected We detected a new user with at least high risk in y...
Microsoft PowerApps
Monday
Use existing templates to rapidly build apps
Learn powerful tips for building apps that optimize your work. Having trouble viewing thi...
Last Month
Lucerne Publishing Events
2/15/19
Upcoming events at Lucerne Publishing
Found out what's going on at
2

12:53

Please Forward Contoso patent document

Isaiah Langer
To You

Feb 15

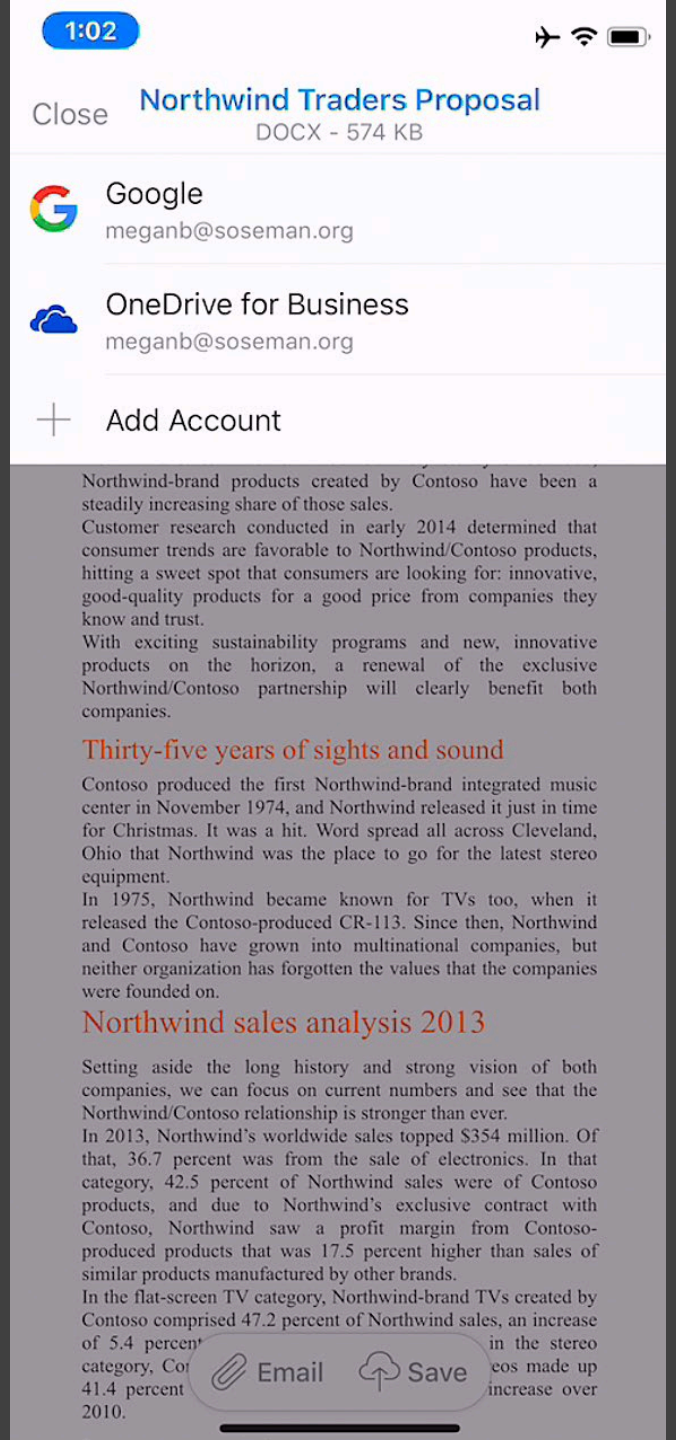
Contoso Patent Real
DOCX - 81 KB

Hi Megan,

I don't have Alex Darrow's email address, please forward Contoso patent document to him please.

Thank you,
Isaiah Langer

Reply


1:02
Close
Northwind Traders Proposal
DOCX - 574 KB
Google
meganb@soseman.org
OneDrive for Business
meganb@soseman.org
Add Account
Northwind-brand products created by Contoso have been a steadily increasing share of those sales.
Customer research conducted in early 2014 determined that consumer trends are favorable to Northwind/Contoso products, hitting a sweet spot that consumers are looking for: innovative, good-quality products for a good price from companies they know and trust.
With exciting sustainability programs and new, innovative products on the horizon, a renewal of the exclusive Northwind/Contoso partnership will clearly benefit both companies.
Thirty-five years of sights and sound
Contoso produced the first Northwind-brand integrated music center in November 1974, and Northwind released it just in time for Christmas. It was a hit. Word spread all across Cleveland, Ohio that Northwind was the place to go for the latest stereo equipment.
In 1975, Northwind became known for TVs too, when it released the Contoso-produced CR-113. Since then, Northwind and Contoso have grown into multinational companies, but neither organization has forgotten the values that the companies were founded on.
Northwind sales analysis 2013
Setting aside the long history and strong vision of both companies, we can focus on current numbers and see that the Northwind/Contoso relationship is stronger than ever.
In 2013, Northwind's worldwide sales topped $354 million. Of that, 36.7 percent was from the sale of electronics. In that category, 42.5 percent of Northwind sales were of Contoso products, and due to Northwind's exclusive contract with Contoso, Northwind saw a profit margin from Contoso-produced products that was 17.5 percent higher than sales of similar products manufactured by other brands.
In the flat-screen TV category, Northwind-brand TVs created by Contoso comprised 47.2 percent of Northwind sales, an increase
of 5.4 percent
in the stereo
category, Co
eos made up
41.4 percent
increase over
2010.
Email
Save

Executive summary

Contoso and Northwind have a long and trusted relationship that spans more than three decades. Their shared core values and a vision of the future has benefited both companies over the years and will continue to do so in the future.

A sales analysis from 2013 showed that 42.5 percent of Northwind electronics sales were of Northwind-brand products created by Contoso. A multiyear analysis showed that while Northwind sales have remained relatively steady since 2007, Northwind-brand products created by Contoso have been a steadily increasing share of those sales.

Customer research conducted in early 2014 determined that consumer trends are favorable to Northwind/Contoso products, hitting a sweet spot that consumers are looking for: innovative, good quality products for a good price from companies they kn

W

pr

N

co

T

C

ce

fo

Ohio that Northwind was the place to go for the latest stereo equipment.

In 1975, Northwind became known for TVs too, when it released the Contoso-produced CR-113. Since then, Northwind and Contoso have grown into multinational companies, but neither organization has forgotten the values that the companies were founded on.

Northwind sales analysis 2013

Setting aside the long history and strong vision of both companies, we can focus on current numbers and see that the Northwind/Contoso relationship is stronger than ever.

In 2013, Northwind's worldwide sales topped $354 million. Of that, 36.7 percent was from the sale of electronics. In that category, 42.5 percent of Northwind sales were of Contoso products, and due to Northwind's exclusive contract with Contoso, Northwind saw a profit margin from Contoso-produced products that was 17.5 percent higher than sales of similar products manufactured by other brands.

In the flat-screen TV category, Northwind-brand TVs created by Contoso comprised 47.2 percent of Northwind sales, an increase of 5.4 percent

in the stereo category, Co

eos made up 41.4 percent

increase over 2010.

Executive summary

Copy | Look Up | Share...

Contoso ...onship
spans n... ...alues a
...ision of the future has benefited both companies over the y
and will continue to do so in the future.

A sales analysis from 2013 showed that 42.5 percen
Northwind electronics sales were of Northwind-brand proc
created by Contoso. A multiyear analysis showed that w
Northwind sales have remained relatively steady since 2
Northwind-brand products created by Contoso have be
steadily increasing share of those sales.

Customer research conducted in early 2014 determined
consumer trends are favorable to Northwind/Contoso prod
hitting a sweet spot that consumers are looking for: innova
good-quality products for a good price from companies
know and trust.

With exciting sustainability programs and new, innov
products on the horizon, a renewal of the exclu
Northwind/Contoso partnership will clearly benefit
companies.

Thirty-five years of sights and sound

Contoso produced the first Northwind-brand integrated n
center in November 1974, and Northwind released it just in
for Christmas. It was a hit. Word spread all across Clevel
Ohio that Northwind was the place to go for the latest s
equipment.

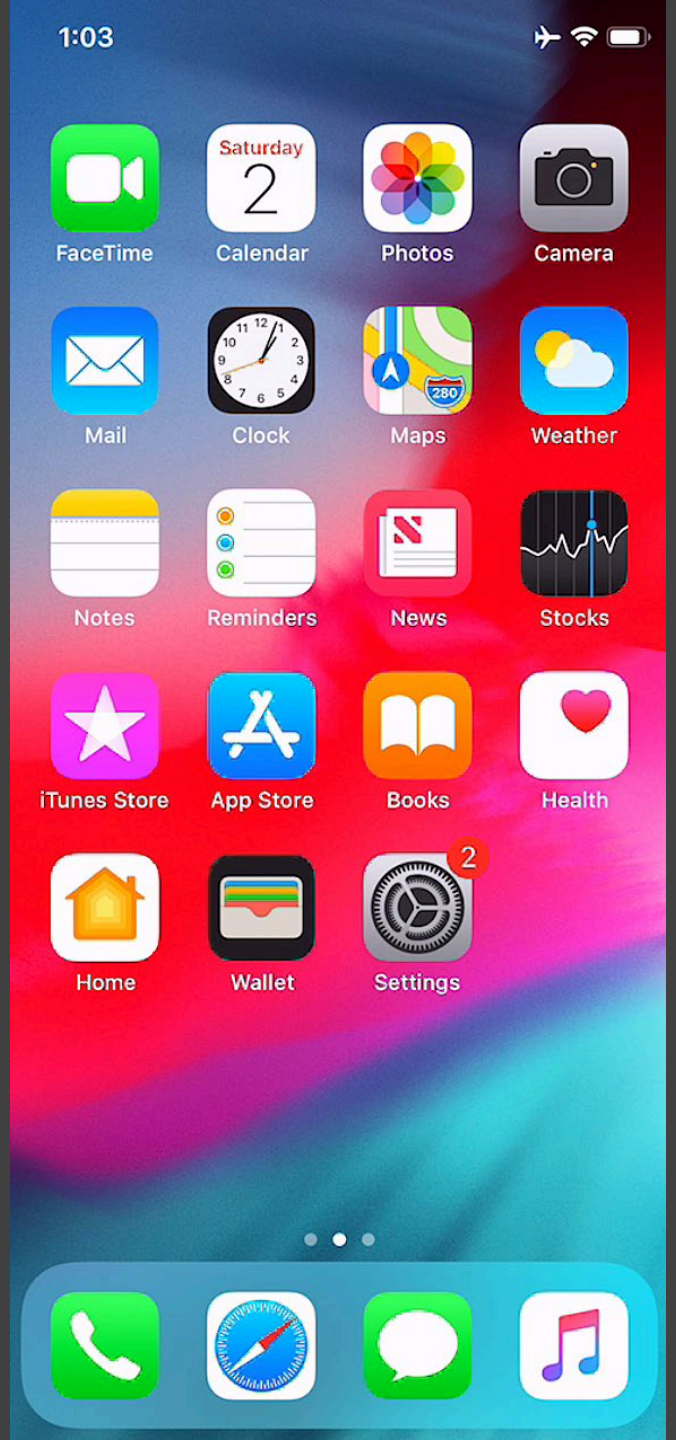
In 1975, Northwind became known for TVs too, whe
released the Contoso-produced CR-113. Since then, North
and Contoso have grown into multinational companies,
neither organization has forgotten the values that the compa
were founded on.

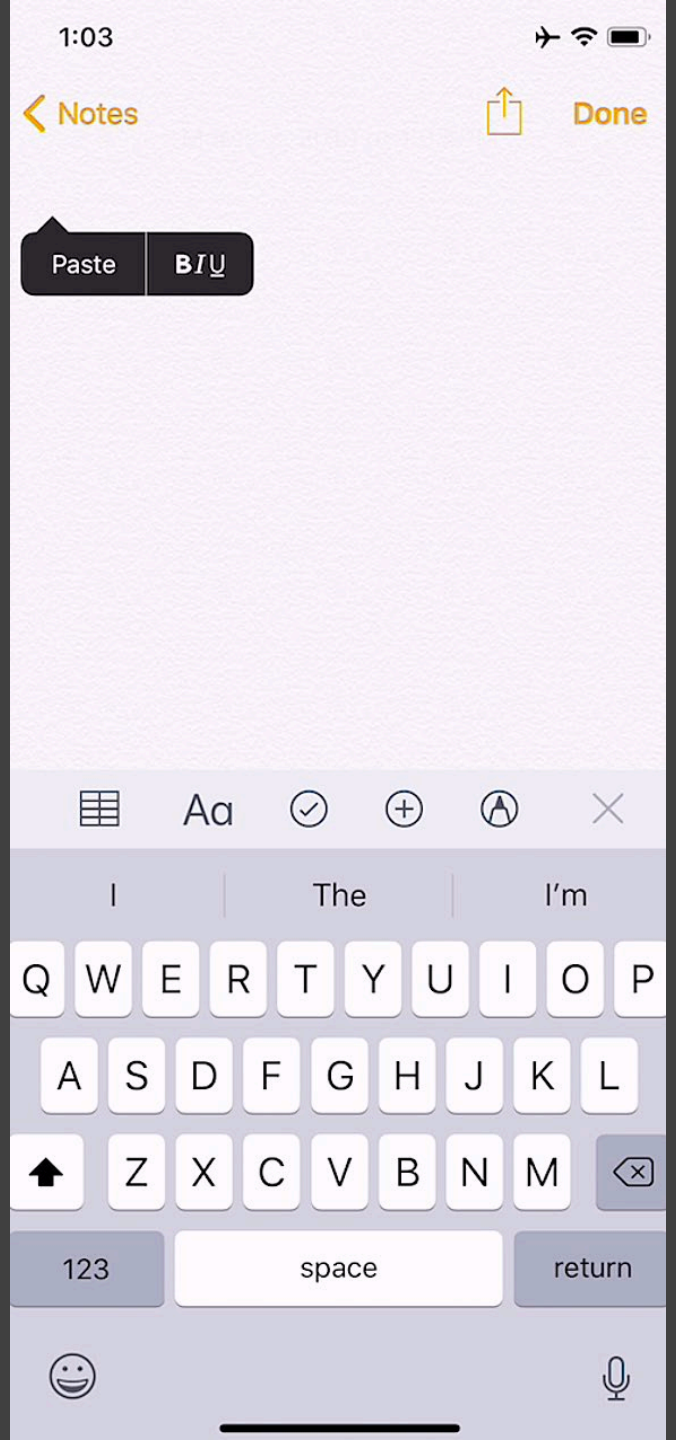
Northwind sales analysis 2013

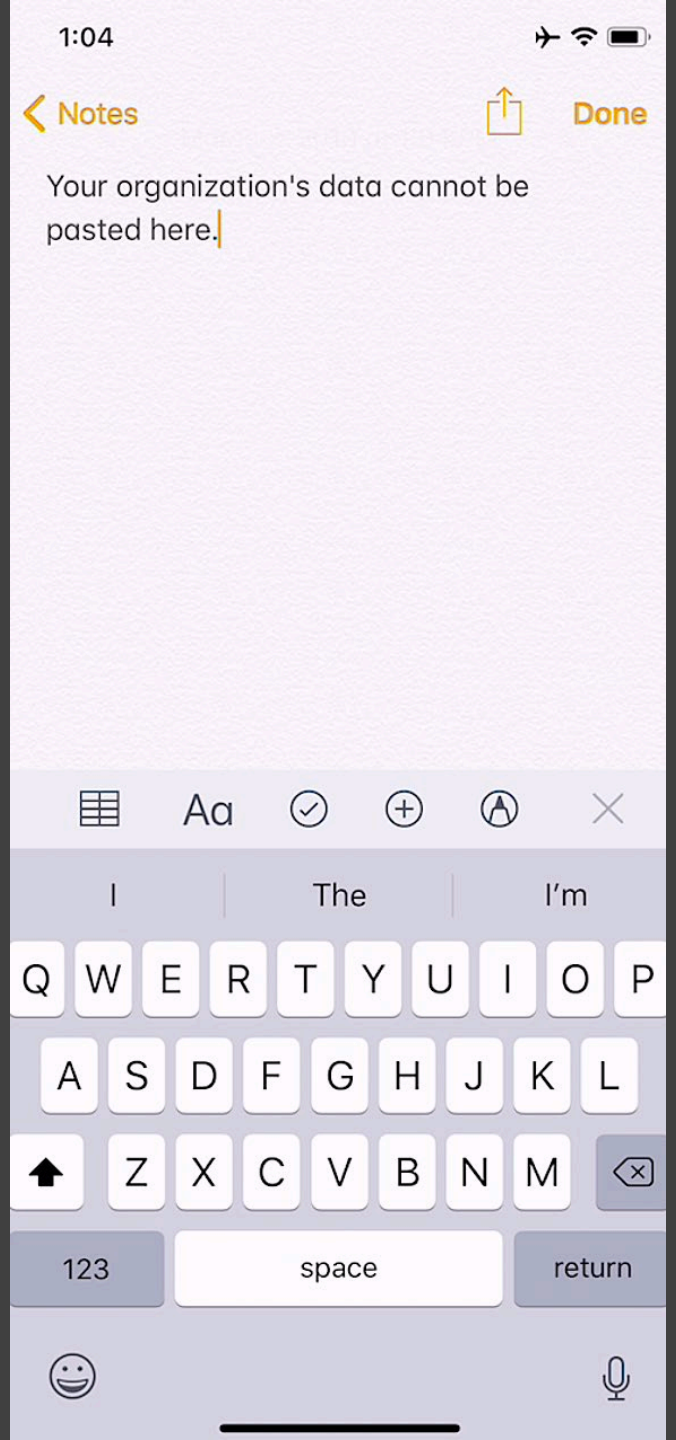
Setting aside the long history and strong vision of
companies, we can focus on current numbers and see tha
Northwind/Contoso relationship is stronger than ever.

In 2013, Northwind's worldwide sales topped $354 millio
that, 36.7 ...of electronics. In
category, ...ales were of Cor
products, a... ...exclusive contract
Contoso, Northwind saw a profit margin from Cont

Email | Save


1:03
FaceTime
Saturday
2
Calendar
Photos
Camera
Mail
Clock
Maps
Weather
Notes
Reminders
News
Stocks
iTunes Store
App Store
Books
Health
Home
Wallet
2
Settings

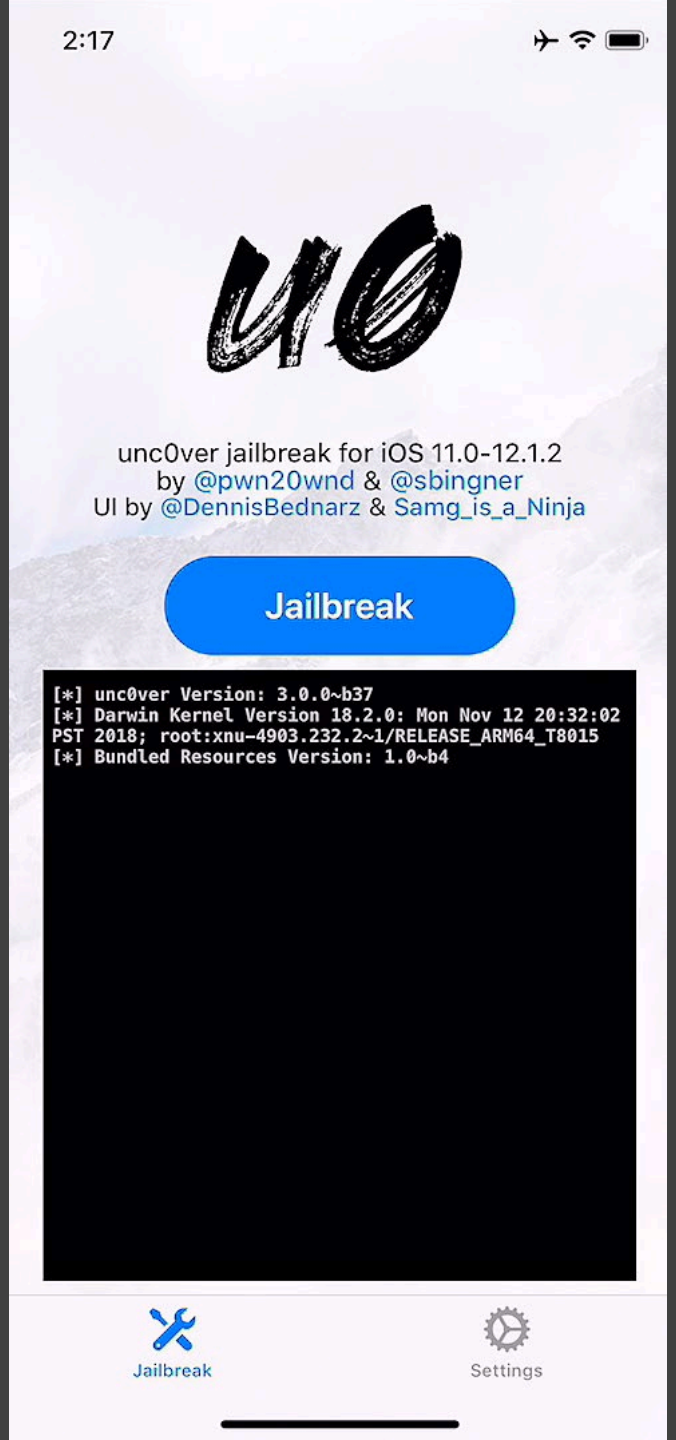

1:03
Notes
Done
Paste
B I U
Aa
I
The
I'm
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return

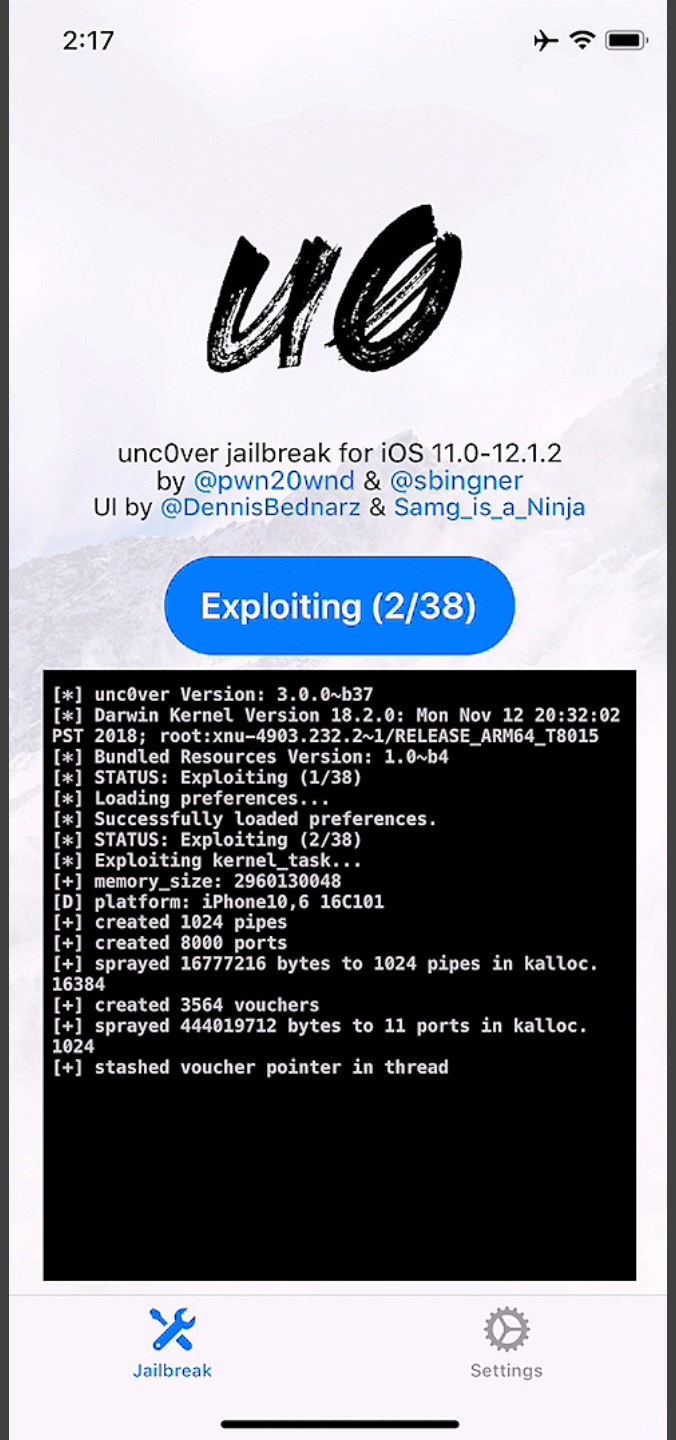

1:04
Notes
Done
Your organization's data cannot be pasted here.
Aa
I
The
I'm
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return

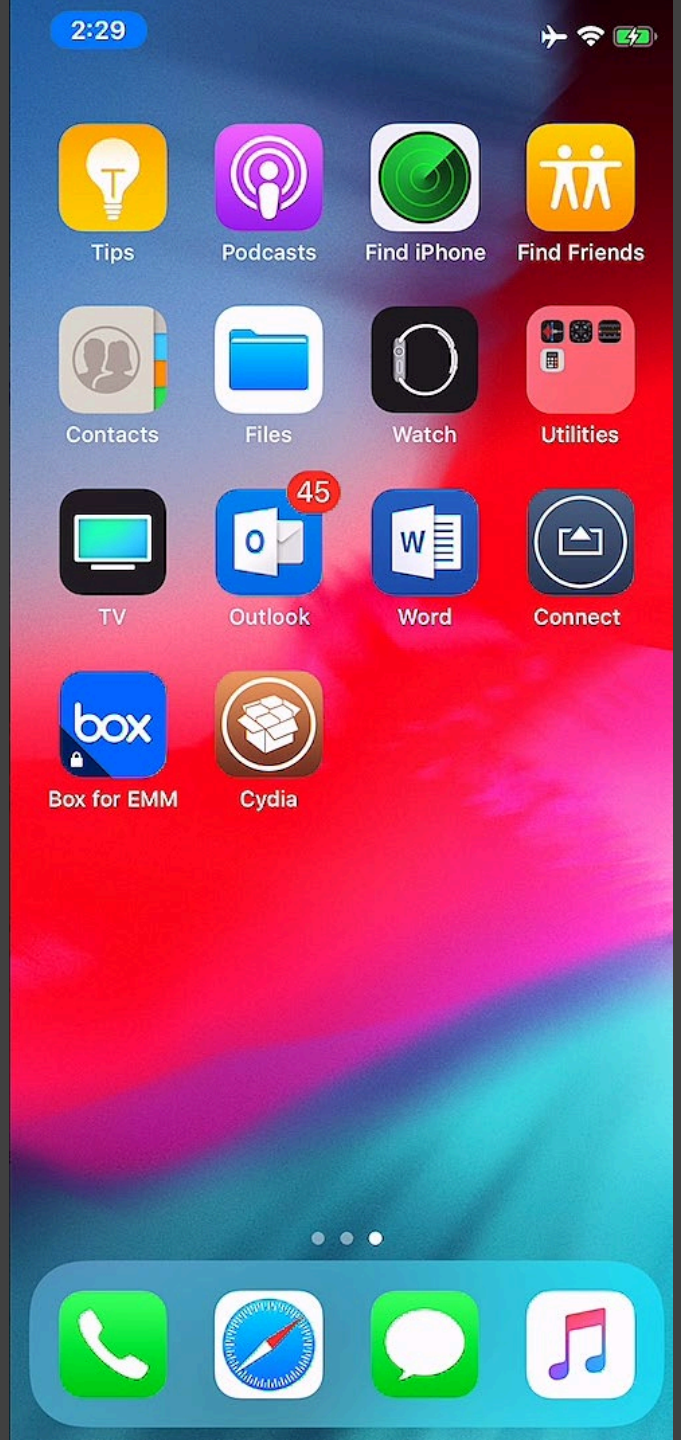
RSAConference2019

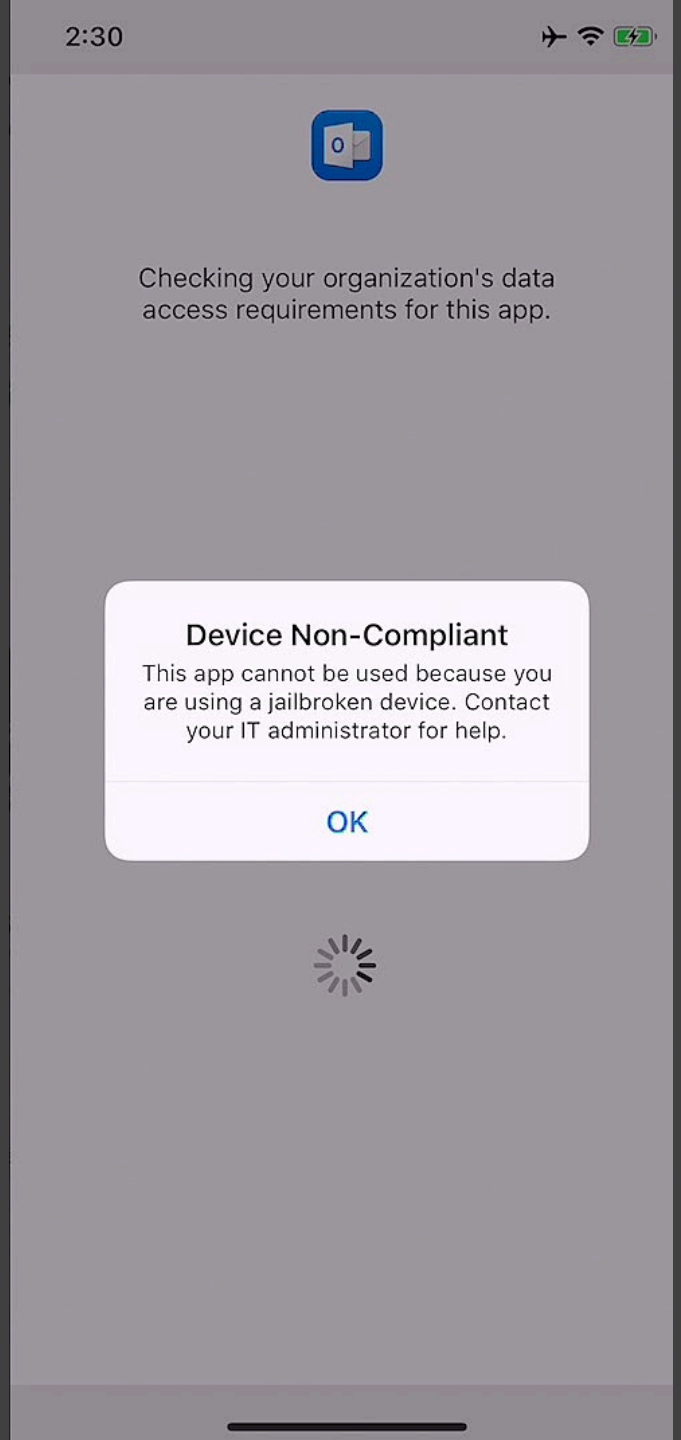
Demo

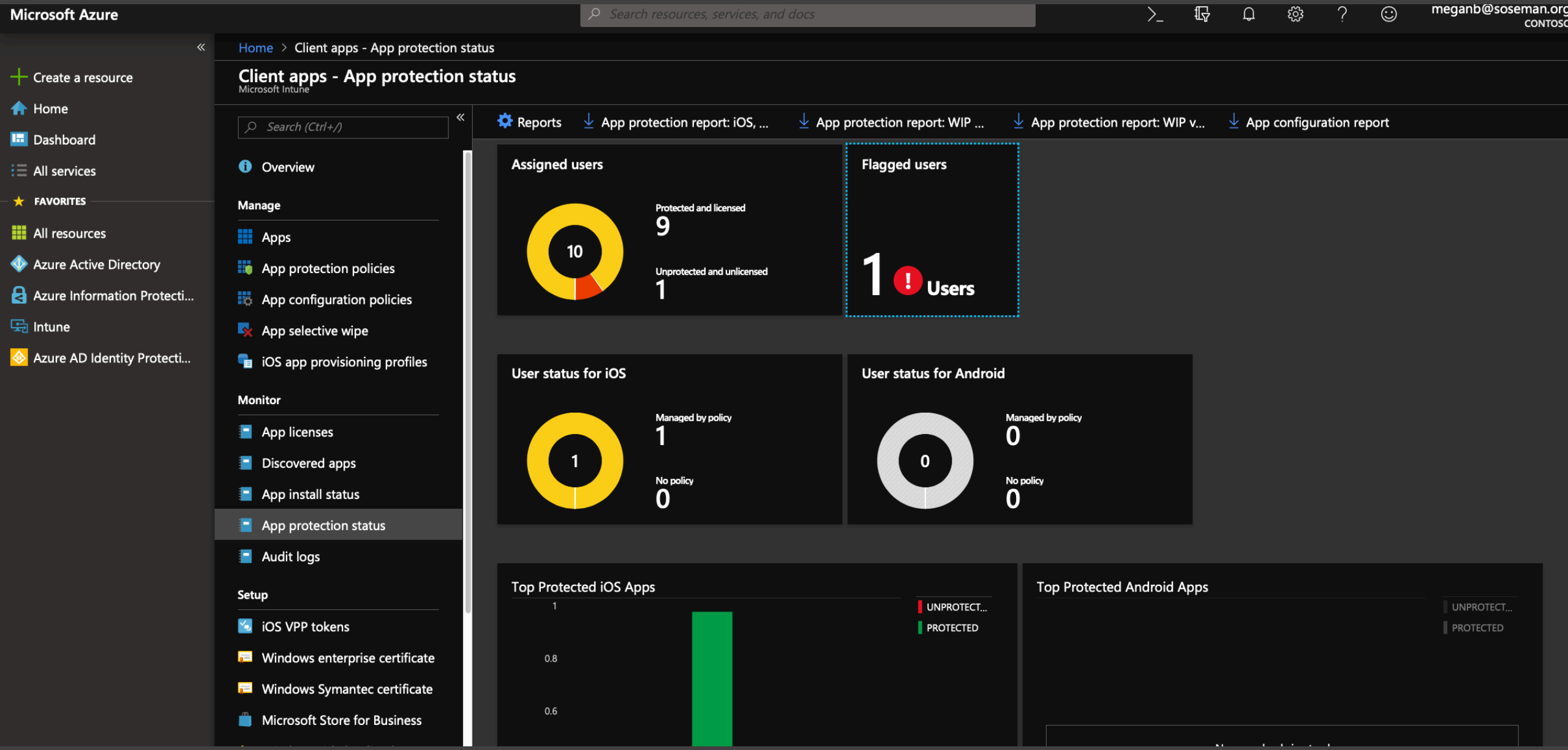
Deny access to applications when device “jailbroken” or “rooted”

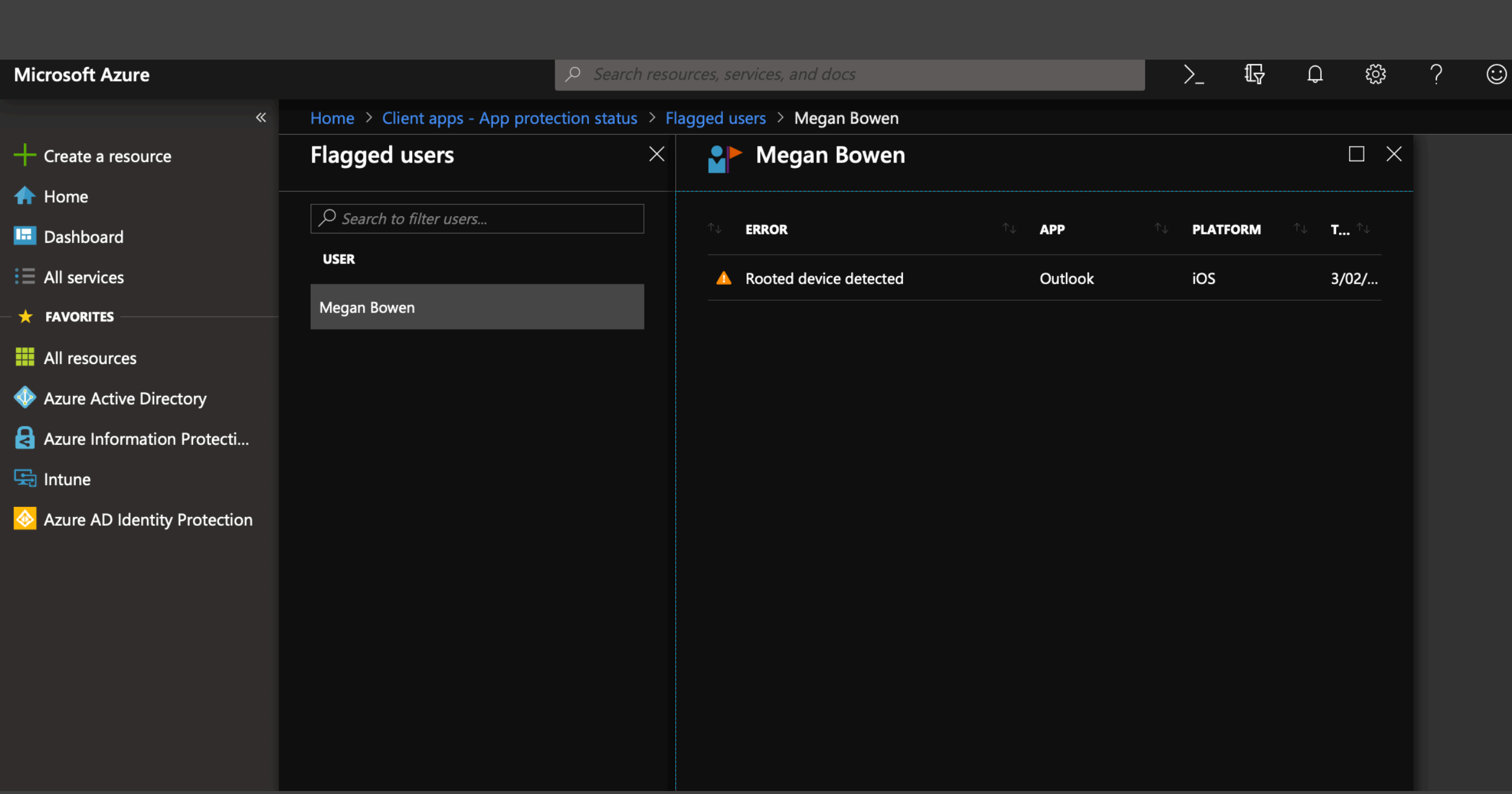

2:17
unc0ver jailbreak for iOS 11.0-12.1.2
by @pwn20wnd & @sbingner
UI by @DennisBednarz & Samg_is_a_Ninja
Jailbreak
[*] unc0ver Version: 3.0.0~b37
[*] Darwin Kernel Version 18.2.0: Mon Nov 12 20:32:02 PST 2018; root:xnu-4903.232.2~1/RELEASE_ARM64_T8015
[*] Bundled Resources Version: 1.0~b4
Jailbreak
Settings


2:17
unc0ver jailbreak for iOS 11.0-12.1.2
by @pwn20wnd & @sbingner
UI by @DennisBednarz & Samg_is_a_Ninja
Exploiting (2/38)
[*] unc0ver Version: 3.0.0~b37
[*] Darwin Kernel Version 18.2.0: Mon Nov 12 20:32:02 PST 2018; root:xnu-4903.232.2~1/RELEASE_ARM64_T8015
[*] Bundled Resources Version: 1.0~b4
[*] STATUS: Exploiting (1/38)
[*] Loading preferences...
[*] Successfully loaded preferences.
[*] STATUS: Exploiting (2/38)
[*] Exploiting kernel_task...
[+] memory_size: 2960130048
[D] platform: iPhone10,6 16C101
[+] created 1024 pipes
[+] created 8000 ports
[+] sprayed 16777216 bytes to 1024 pipes in kalloc. 16384
[+] created 3564 vouchers
[+] sprayed 444019712 bytes to 11 ports in kalloc. 1024
[+] stashed voucher pointer in thread
Jailbreak
Settings


2:29
Tips
Podcasts
Find iPhone
Find Friends
Contacts
Files
Watch
Utilities
45
TV
Outlook
Word
Connect
Box for EMM
Cydia


2:30
Checking your organization's data access requirements for this app.
Device Non-Compliant
This app cannot be used because you are using a jailbroken device. Contact your IT administrator for help.
OK

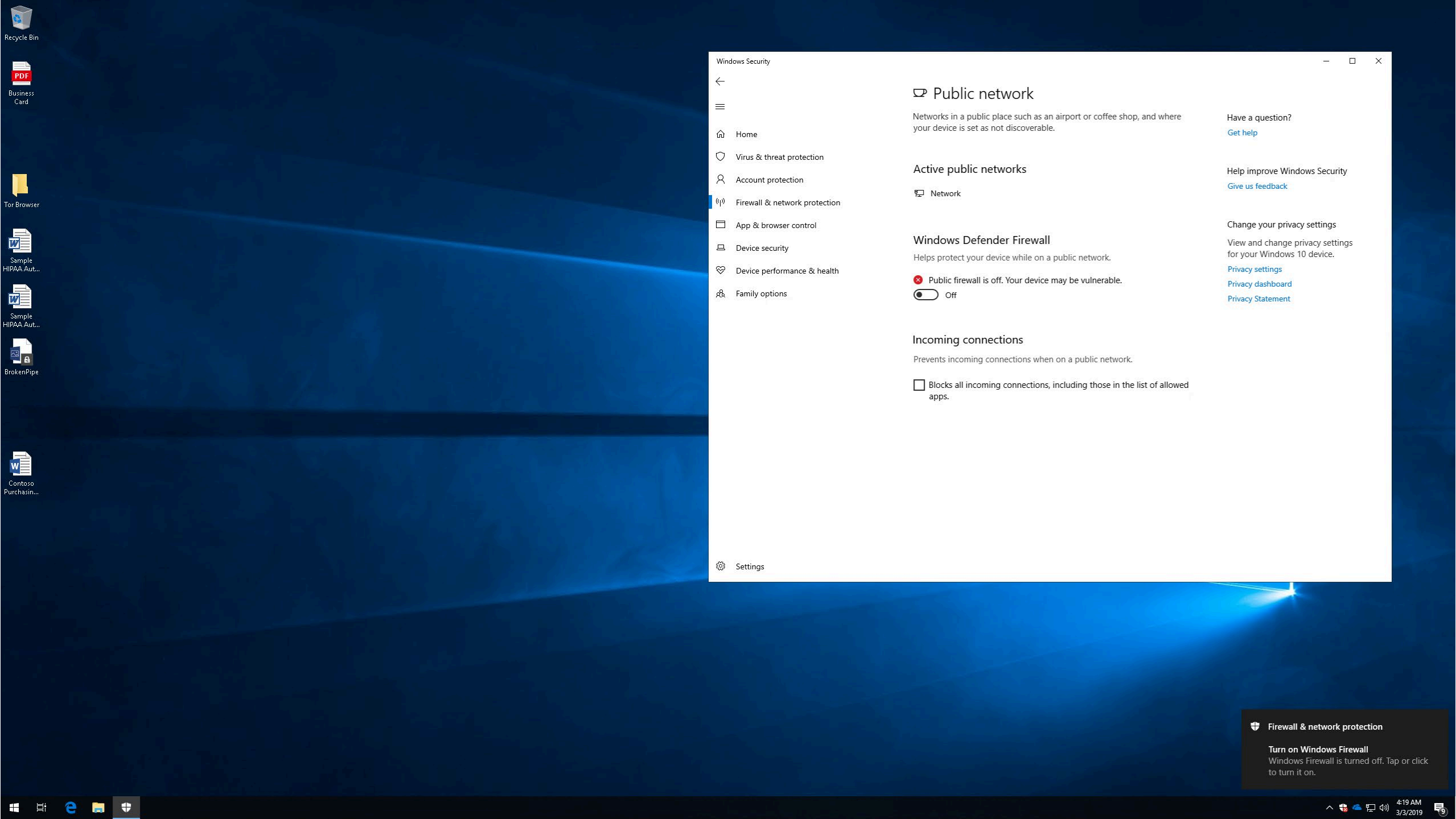

Microsoft Azure
Search resources, services, and docs
meganb@soseman.org
CONTOSO
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Azure Active Directory
Azure Information Protecti...
Intune
Azure AD Identity Protecti...
Home > Client apps - App protection status
Client apps - App protection status
Microsoft Intune
Search (Ctrl+/)
Overview
Manage
Apps
App protection policies
App configuration policies
App selective wipe
iOS app provisioning profiles
Monitor
App licenses
Discovered apps
App install status
App protection status
Audit logs
Setup
iOS VPP tokens
Windows enterprise certificate
Windows Symantec certificate
Microsoft Store for Business
Reports
App protection report: iOS, ...
App protection report: WIP ...
App protection report: WIP v...
App configuration report
Assigned users
10
Protected and licensed
9
Unprotected and unlicensed
1
Flagged users
1
Users
User status for iOS
1
Managed by policy
1
No policy
0
User status for Android
0
Managed by policy
0
No policy
0
Top Protected iOS Apps
1
0.8
0.6
UNPROTECT...
PROTECTED
Top Protected Android Apps
UNPROTECT...
PROTECTED

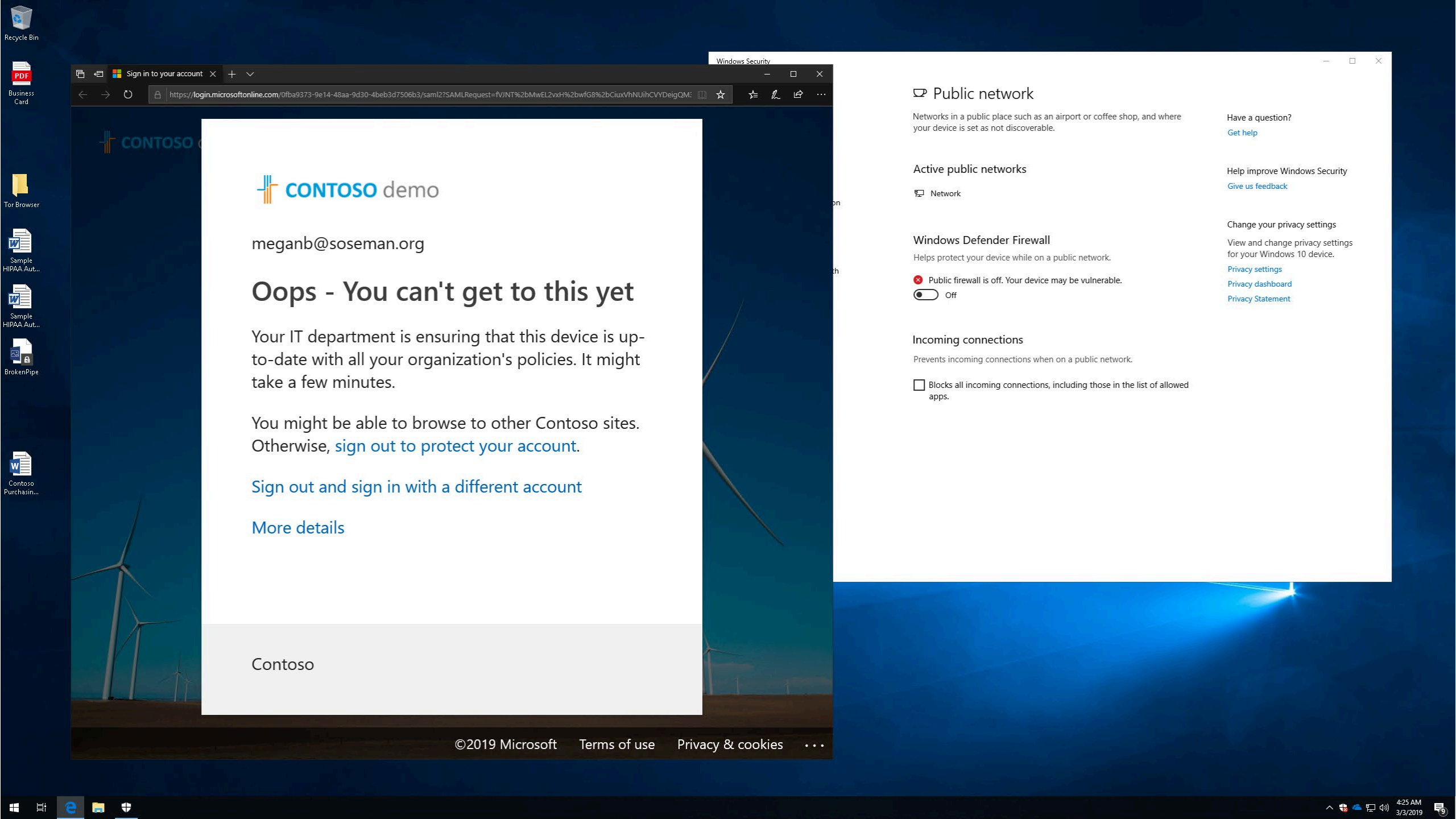

Microsoft Azure
Search resources, services, and docs
Home > Client apps - App protection status > Flagged users > Megan Bowen
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Azure Active Directory
Azure Information Protecti...
Intune
Azure AD Identity Protection
Flagged users
Search to filter users...
USER
Megan Bowen
Megan Bowen
ERROR
APP
PLATFORM
T...
Rooted device detected
Outlook
iOS
3/02/...

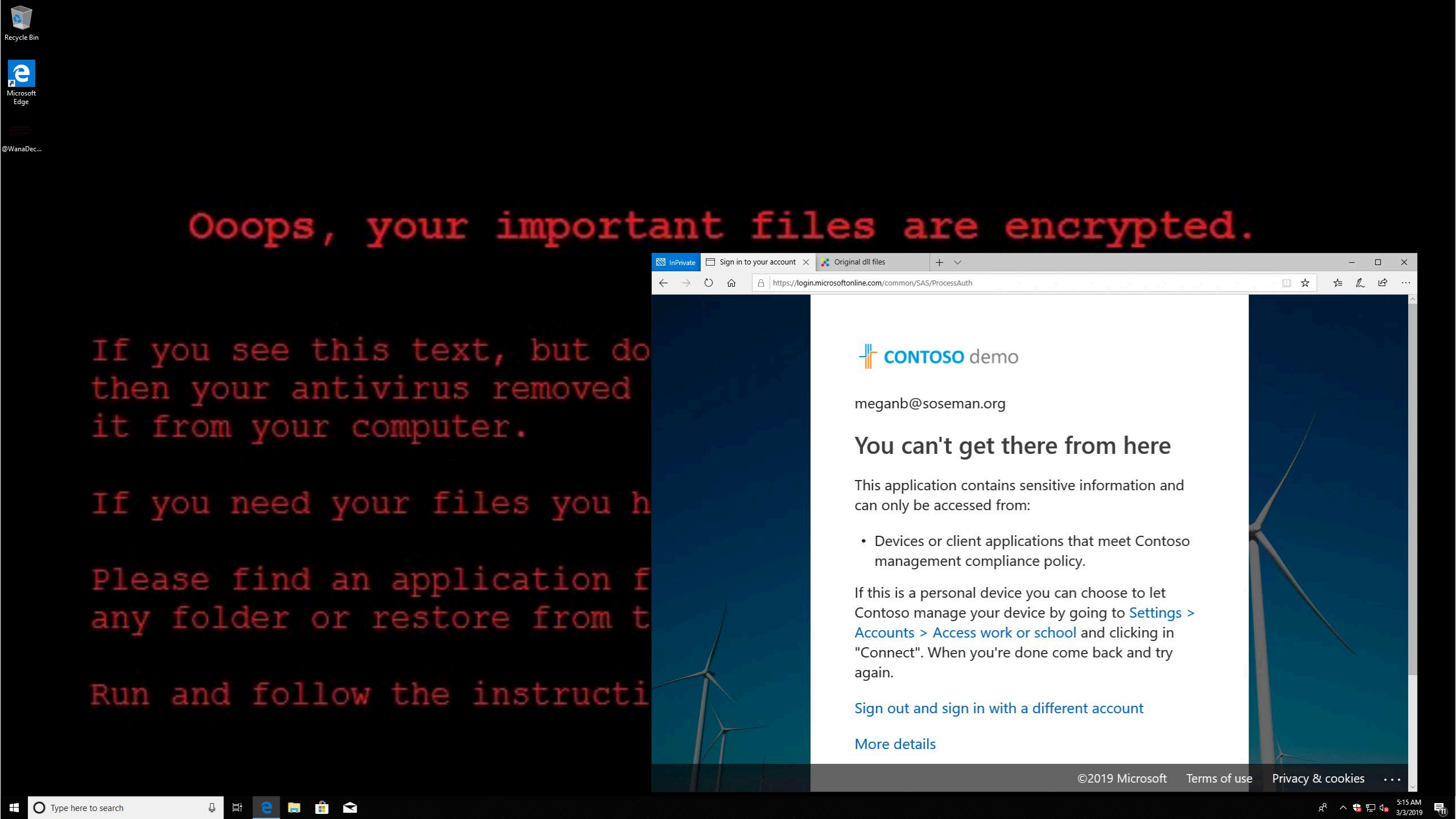
RSAConference2019

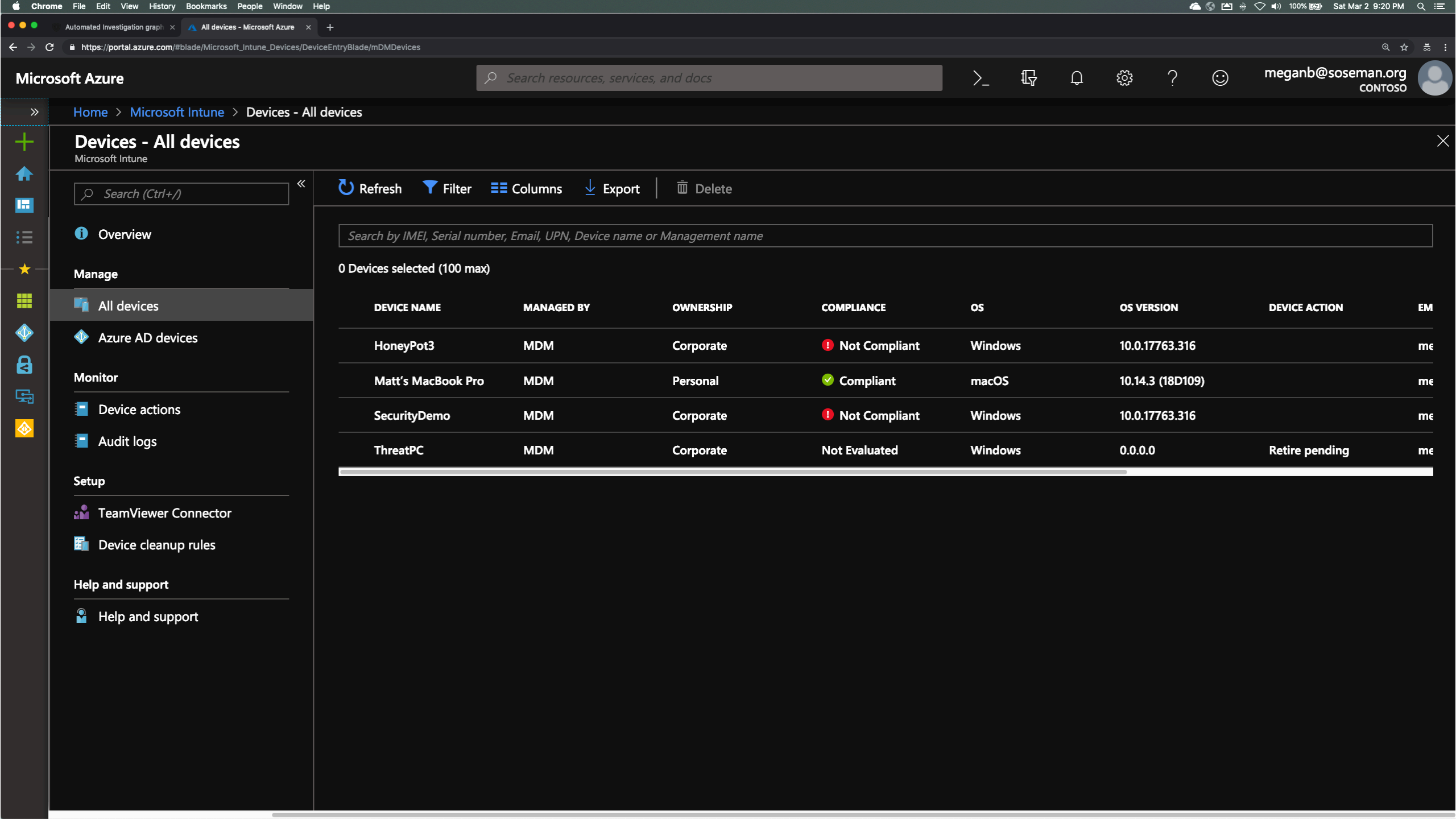
Demo

Deny access to applications when device is not compliant (i.e. a policy is violated or a threat exists)


Recycle Bin
Business Card
Tor Browser
Sample HIPAA Aut...
Sample HIPAA Aut...
BrokenPipe
Contoso Purchasin...
Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Public network
Networks in a public place such as an airport or coffee shop, and where your device is set as not discoverable.
Active public networks
Network
Windows Defender Firewall
Helps protect your device while on a public network.
Public firewall is off. Your device may be vulnerable.
Off
Incoming connections
Prevents incoming connections when on a public network.
Blocks all incoming connections, including those in the list of allowed apps.
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Firewall & network protection
Turn on Windows Firewall
Windows Firewall is turned off. Tap or click to turn it on.
4:19 AM
3/3/2019


Recycle Bin
Business Card
Tor Browser
Sample HIPAA Aut...
Sample HIPAA Aut...
BrokenPipe
Contoso Purchasin...
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVJNT%2bMwEL2vxH%2bwfG8%2bCiuxVhNUihCVYDeigQM:
CONTOSO demo
meganb@soseman.org
Oops - You can't get to this yet
Your IT department is ensuring that this device is up-to-date with all your organization's policies. It might take a few minutes.
You might be able to browse to other Contoso sites. Otherwise, sign out to protect your account.
Sign out and sign in with a different account
More details
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies
Windows Security
Public network
Networks in a public place such as an airport or coffee shop, and where your device is set as not discoverable.
Active public networks
Network
Windows Defender Firewall
Helps protect your device while on a public network.
Public firewall is off. Your device may be vulnerable.
Off
Incoming connections
Prevents incoming connections when on a public network.
Blocks all incoming connections, including those in the list of allowed apps.
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
4:25 AM
3/3/2019


Recycle Bin
Microsoft Edge
@WanaDec...
Ooops, your important files are encrypted.
If you see this text, but do
then your antivirus removed
it from your computer.
If you need your files you h
Please find an application f
any folder or restore from t
Run and follow the instructi
InPrivate
Sign in to your account
Original dll files
https://login.microsoftonline.com/common/SAS/ProcessAuth
CONTOSO demo
meganb@soseman.org
You can't get there from here
This application contains sensitive information and can only be accessed from:
Devices or client applications that meet Contoso management compliance policy.
If this is a personal device you can choose to let Contoso manage your device by going to Settings > Accounts > Access work or school and clicking in "Connect". When you're done come back and try again.
Sign out and sign in with a different account
More details
©2019 Microsoft
Terms of use
Privacy & cookies
Type here to search
5:15 AM
3/3/2019


Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 9:20 PM
Automated Investigation graph
All devices - Microsoft Azure
https://portal.azure.com/#blade/Microsoft_Intune_Devices/DeviceEntryBlade/mDMDevices
Microsoft Azure
Search resources, services, and docs
meganb@soseman.org
CONTOSO
Home > Microsoft Intune > Devices - All devices
Devices - All devices
Microsoft Intune
Search (Ctrl+/)
Overview
Manage
All devices
Azure AD devices
Monitor
Device actions
Audit logs
Setup
TeamViewer Connector
Device cleanup rules
Help and support
Help and support
Refresh
Filter
Columns
Export
Delete
Search by IMEI, Serial number, Email, UPN, Device name or Management name
0 Devices selected (100 max)
DEVICE NAME
MANAGED BY
OWNERSHIP
COMPLIANCE
OS
OS VERSION
DEVICE ACTION
EM
HoneyPot3
MDM
Corporate
Not Compliant
Windows
10.0.17763.316
Matt's MacBook Pro
MDM
Personal
Compliant
macOS
10.14.3 (18D109)
SecurityDemo
MDM
Corporate
Not Compliant
Windows
10.0.17763.316
ThreatPC
MDM
Corporate
Not Evaluated
Windows
0.0.0.0
Retire pending

Suspicious process injection observed

Investigation #1 is running - Waiting for machine

Started
Mar 1, 2019, 4:36:22 AM

Total pending time: 1:14h

2:00:43:39
Waiting for machine

Cancel Investigation

Comments (0)

Investigation details

Status
Waiting for machine

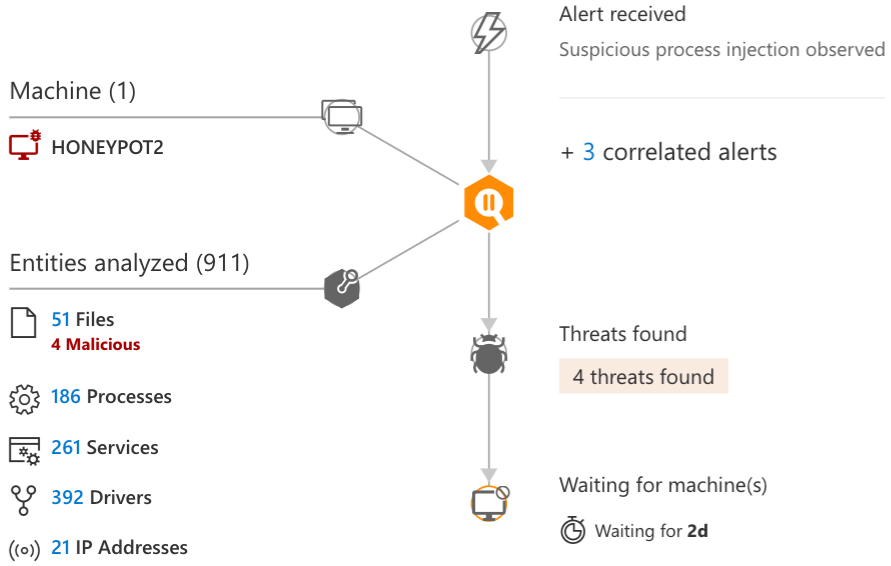
Investigation paused. The investigation will resume as soon as the machine is available.

Alert severity
Medium

Category
Installation

Detection source
EDR

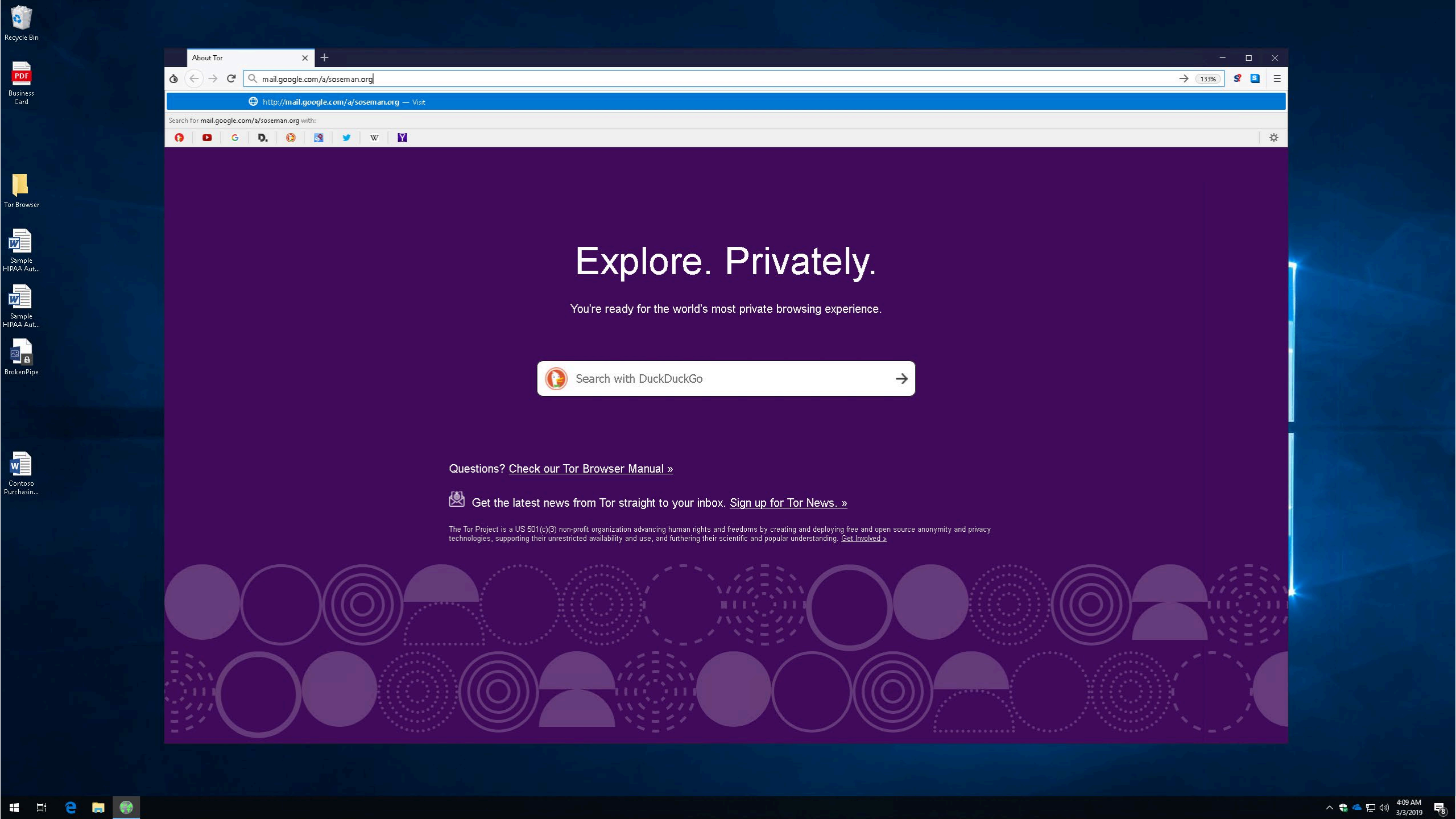
Investigation graph | Alerts (4) | Machines (1) | Key findings (4) | Entities (911) | Log (59)

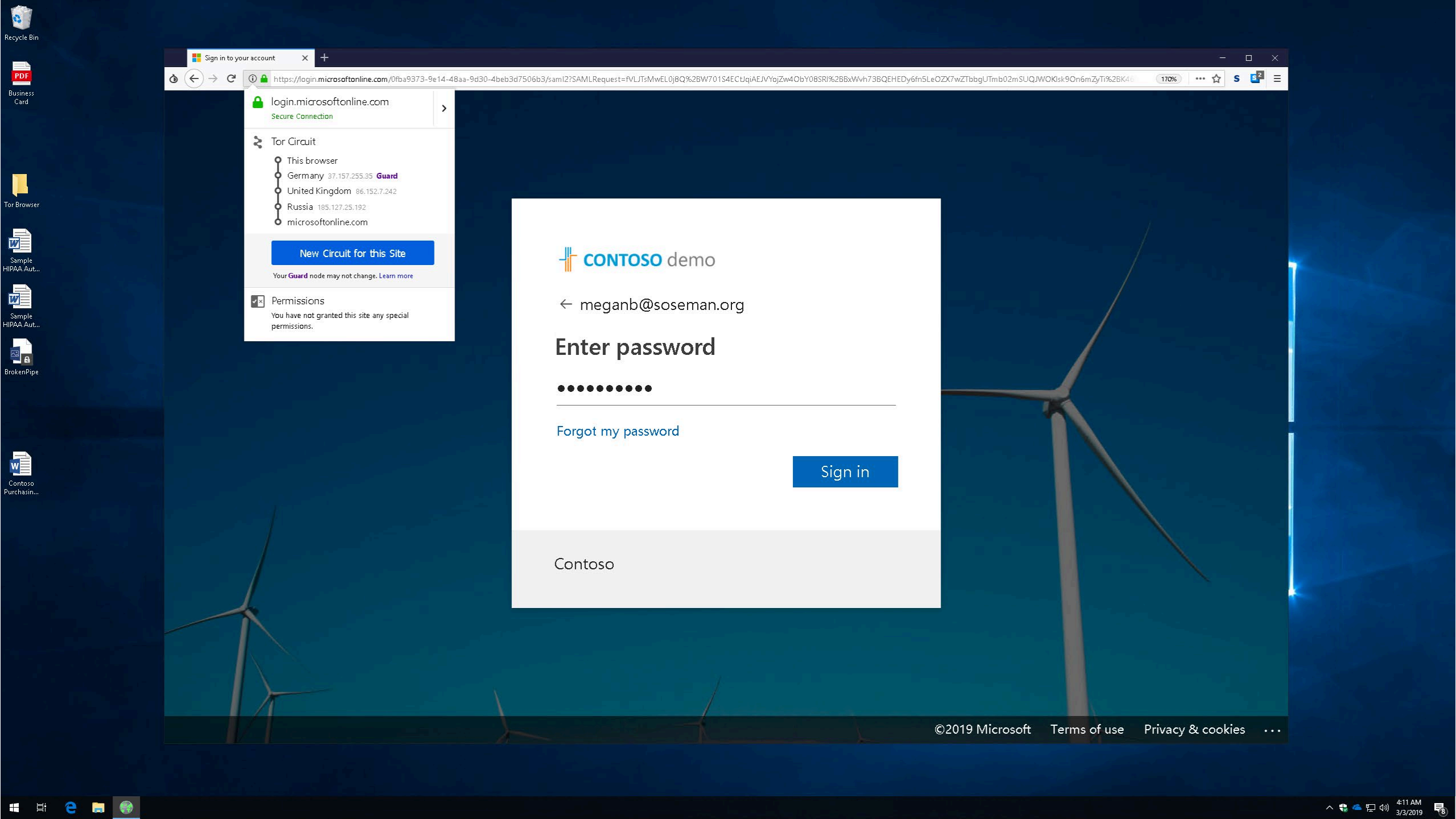


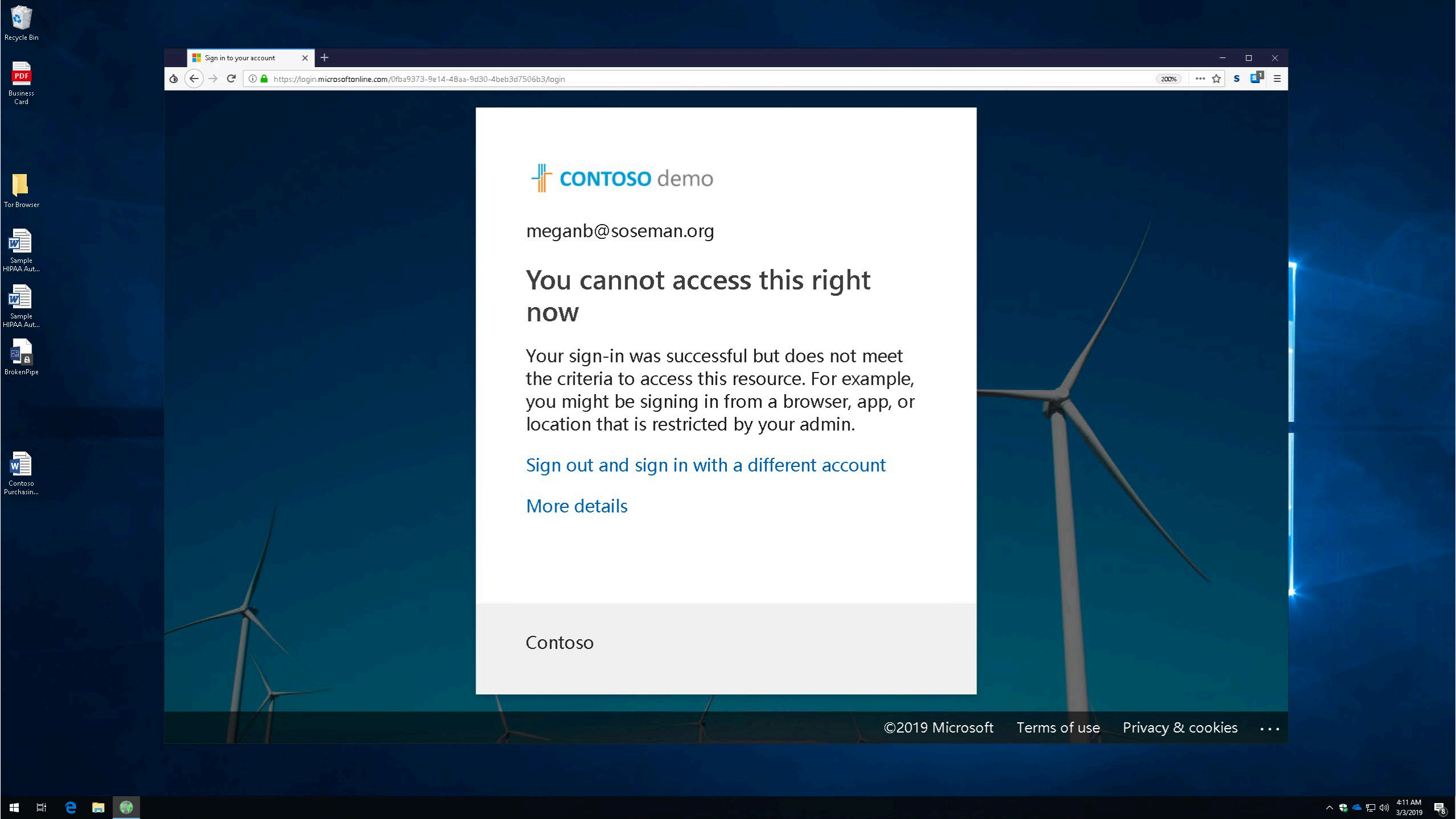
RSAConference2019

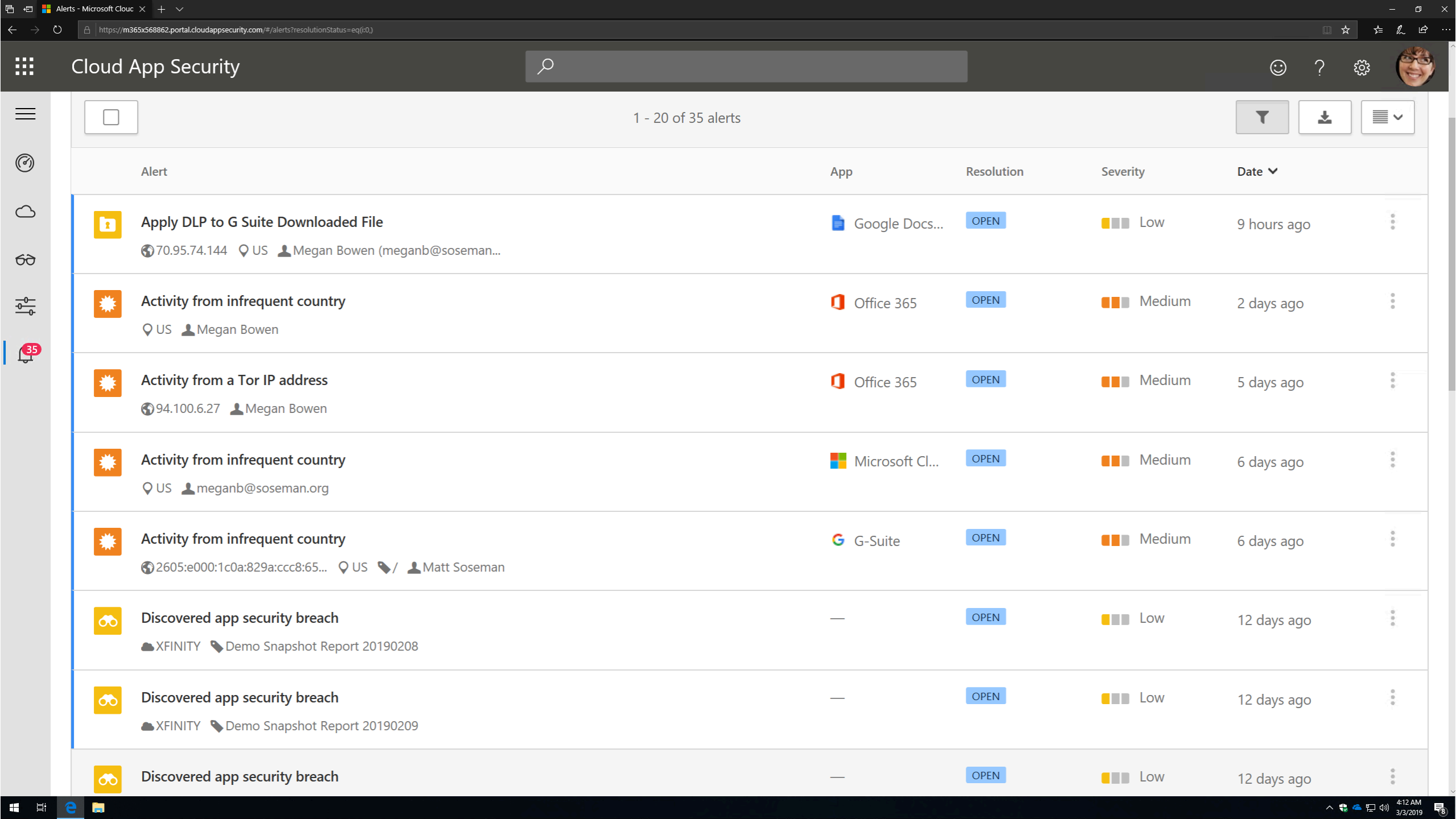
Demo

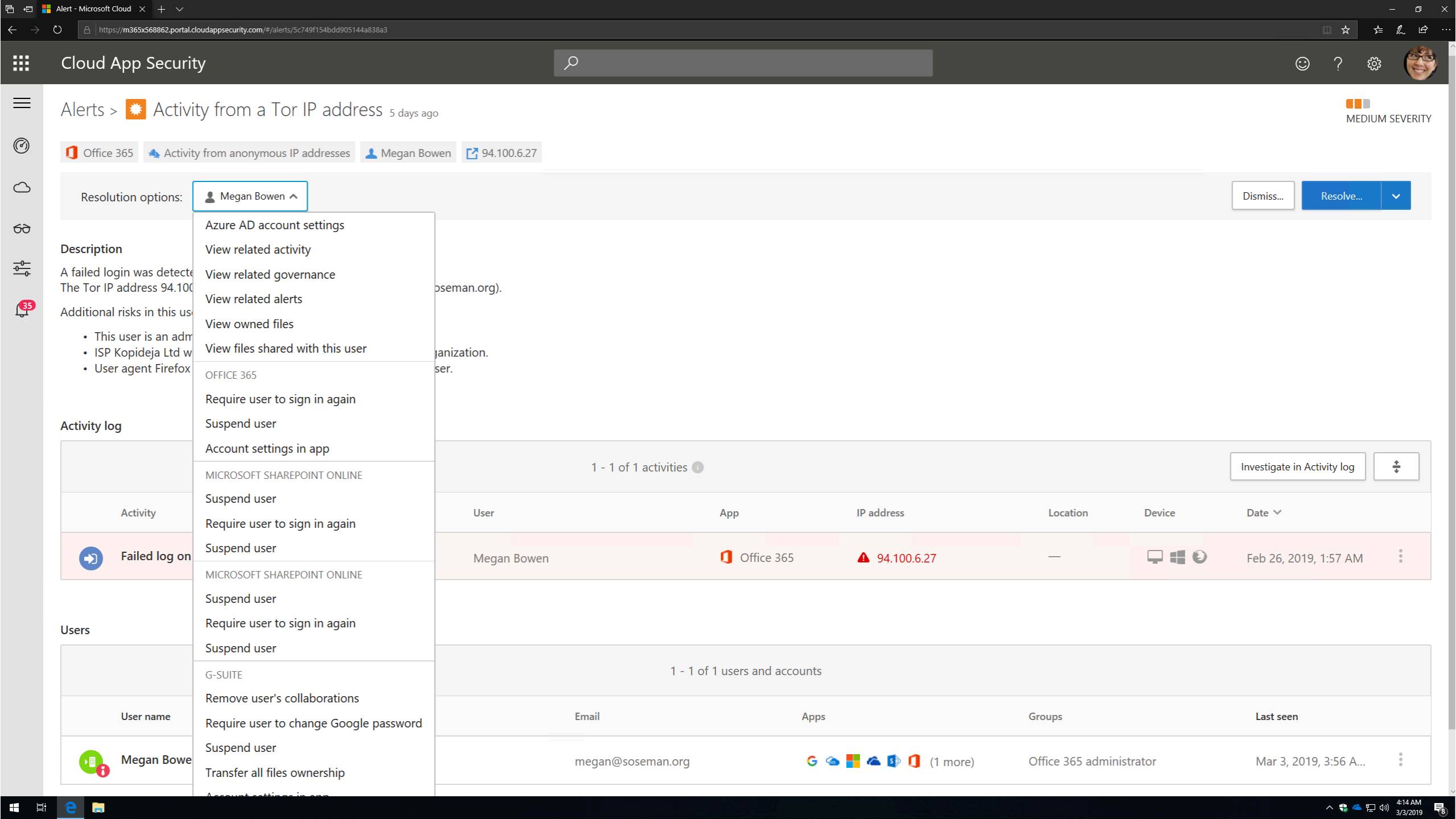
Denying access to an app using an unauthorized app or anonymous IP address


Recycle Bin
Business Card
Tor Browser
Sample HIPAA Aut...
Sample HIPAA Aut...
BrokenPipe
Contoso Purchasin...
About Tor
mail.google.com/a/soseman.org
133%
http://mail.google.com/a/soseman.org — Visit
Search for mail.google.com/a/soseman.org with:
Explore. Privately.
You're ready for the world's most private browsing experience.
Search with DuckDuckGo
Questions? Check our Tor Browser Manual »
Get the latest news from Tor straight to your inbox. Sign up for Tor News. »
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »
4:09 AM
3/3/2019

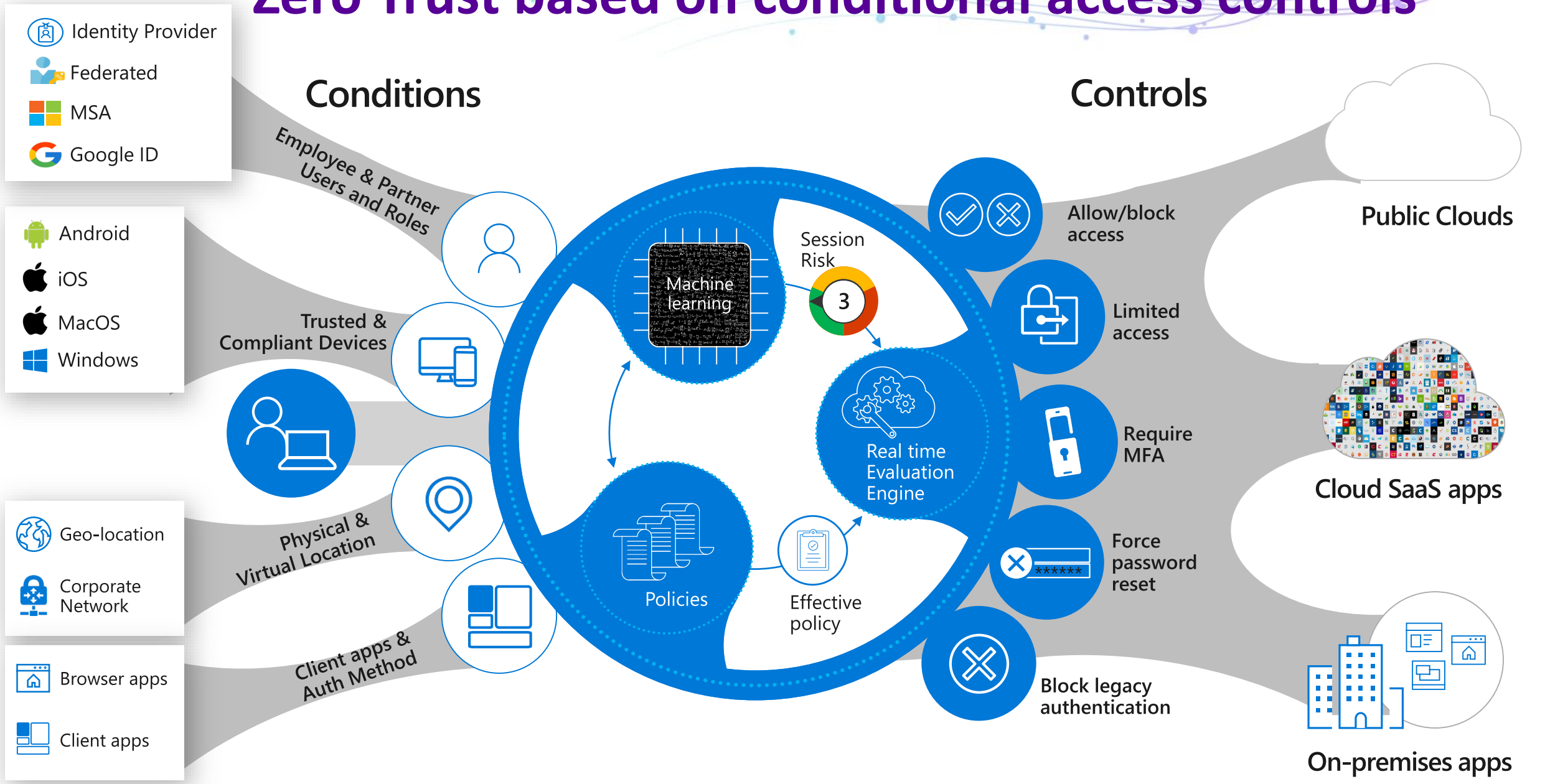

Recycle Bin
Business Card
Tor Browser
Sample HIPAA Aut...
Sample HIPAA Aut...
BrokenPipe
Contoso Purchasin...
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVLJTsMwEL0j8Q%2BW701S4ECtJqiAEJVYojZw4ObY08SRI%2BBxWvh73BQEHEDy6fn5LeOZX7wZTbbgUTmb02mSUQJWOKlsk9On6mZyTi%2BK4
170%
login.microsoftonline.com
Secure Connection
Tor Circuit
This browser
Germany 37.157.255.35 Guard
United Kingdom 86.152.7.242
Russia 185.127.25.192
microsoftonline.com
New Circuit for this Site
Your Guard node may not change. Learn more
Permissions
You have not granted this site any special permissions.
CONTOSO demo
meganb@soseman.org
Enter password
Forgot my password
Sign in
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies
4:11 AM
3/3/2019


Recycle Bin
Business Card
Tor Browser
Sample HIPAA Aut...
Sample HIPAA Aut...
BrokenPipe
Contoso Purchasin...
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/login
200%
CONTOSO demo
meganb@soseman.org
You cannot access this right now
Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.
Sign out and sign in with a different account
More details
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies
4:11 AM
3/3/2019


Alerts - Microsoft Clouc
https://m365x568862.portal.cloudappsecurity.com/#/alerts?resolutionStatus=eq(i:0,)
Cloud App Security
1 - 20 of 35 alerts
Alert
App
Resolution
Severity
Date
Apply DLP to G Suite Downloaded File
70.95.74.144 US Megan Bowen (meganb@soseman...
Google Docs...
OPEN
Low
9 hours ago
Activity from infrequent country
US Megan Bowen
Office 365
OPEN
Medium
2 days ago
Activity from a Tor IP address
94.100.6.27 Megan Bowen
Office 365
OPEN
Medium
5 days ago
Activity from infrequent country
US meganb@soseman.org
Microsoft Cl...
OPEN
Medium
6 days ago
Activity from infrequent country
2605:e000:1c0a:829a:ccc8:65... US / Matt Soseman
G-Suite
OPEN
Medium
6 days ago
Discovered app security breach
XFINITY Demo Snapshot Report 20190208
—
OPEN
Low
12 days ago
Discovered app security breach
XFINITY Demo Snapshot Report 20190209
—
OPEN
Low
12 days ago
Discovered app security breach
—
OPEN
Low
12 days ago
35
4:12 AM
3/3/2019


Alert - Microsoft Cloud
https://m365x568862.portal.cloudappsecurity.com/#/alerts/5c749f154bdd905144a838a3
Cloud App Security
Alerts > Activity from a Tor IP address 5 days ago
MEDIUM SEVERITY
Office 365
Activity from anonymous IP addresses
Megan Bowen
94.100.6.27
Resolution options:
Megan Bowen
Azure AD account settings
View related activity
View related governance
View related alerts
View owned files
View files shared with this user
OFFICE 365
Require user to sign in again
Suspend user
Account settings in app
MICROSOFT SHAREPOINT ONLINE
Suspend user
Require user to sign in again
Suspend user
MICROSOFT SHAREPOINT ONLINE
Suspend user
Require user to sign in again
Suspend user
G-SUITE
Remove user's collaborations
Require user to change Google password
Suspend user
Transfer all files ownership
Dismiss...
Resolve...
Description
A failed login was detecte
The Tor IP address 94.100
oseman.org).
Additional risks in this us
This user is an adm
ISP Kopideja Ltd w
User agent Firefox
ganization.
ser.
Activity log
1 - 1 of 1 activities
Investigate in Activity log
Activity
User
App
IP address
Location
Device
Date
Failed log on
Megan Bowen
Office 365
94.100.6.27
—
Feb 26, 2019, 1:57 AM
Users
1 - 1 of 1 users and accounts
User name
Email
Apps
Groups
Last seen
Megan Bowe
megan@soseman.org
(1 more)
Office 365 administrator
Mar 3, 2019, 3:56 A...
4:14 AM
3/3/2019

Zero Trust based on conditional access controls



Key Takeaways

- Networks that fail to evolve from traditional defenses are vulnerable to breaches. We must assume breach.
- Zero Trust *can* enable new business outcomes that were not possible before.
- Technology has evolved to now make these scenarios possible, and you may already own it.
- Consider an "*if-this-then-that*" automated approach to Zero Trust.
- Identity is everything, make it the control plane.

Apply what you have learned today

Apply what you have learned today – detailed view (take a photo of this slide!)

- Next week you should:
  - Download this deck.
  - Understand what “zero trust controls” your identity solution provides.
  - Discover what products in your environment can integrate with your identity solution to help you create a zero trust story for your organization. (i.e. firewall, VPN, MDM, EDR, DLP, etc)
- In the first three months following this presentation you should:
  - Build a persona profile (set of conditions) required for your end users with an understanding of who they are, where they are going, and what they want.
    - i.e. The state of the identity (verified or compromised), what types of devices they are using, from which locations, and to what applications.
  - Identify what controls are required to respond to those specific conditions
    - i.e. If accessing an app (e.g. SharePoint or G-Suite) from an untrusted device, do I need to challenge with multi-factor authentication? Or require to first enroll the device into MDM/Domain *then* allow access? If the identity is compromised and credentials in public, block access.
- Within six months to one year you should:
  - Identify two “zero trust” controls from above to conduct a production proof of concept. Develop a test plan to effectively test controls. Gather datapoints and effectiveness of policies. Fine tune if needed.
  - Consider a limited production pilot with group of “friendlies” (business users). Study their behavior, gather feedback/datapoints, and understand if/how the policies impact their productivity. Fine tune if needed.
  - Develop an architecture and project plan to roll out those two controls out to the organization with a roadmap of future controls. **Become a rockstar.**