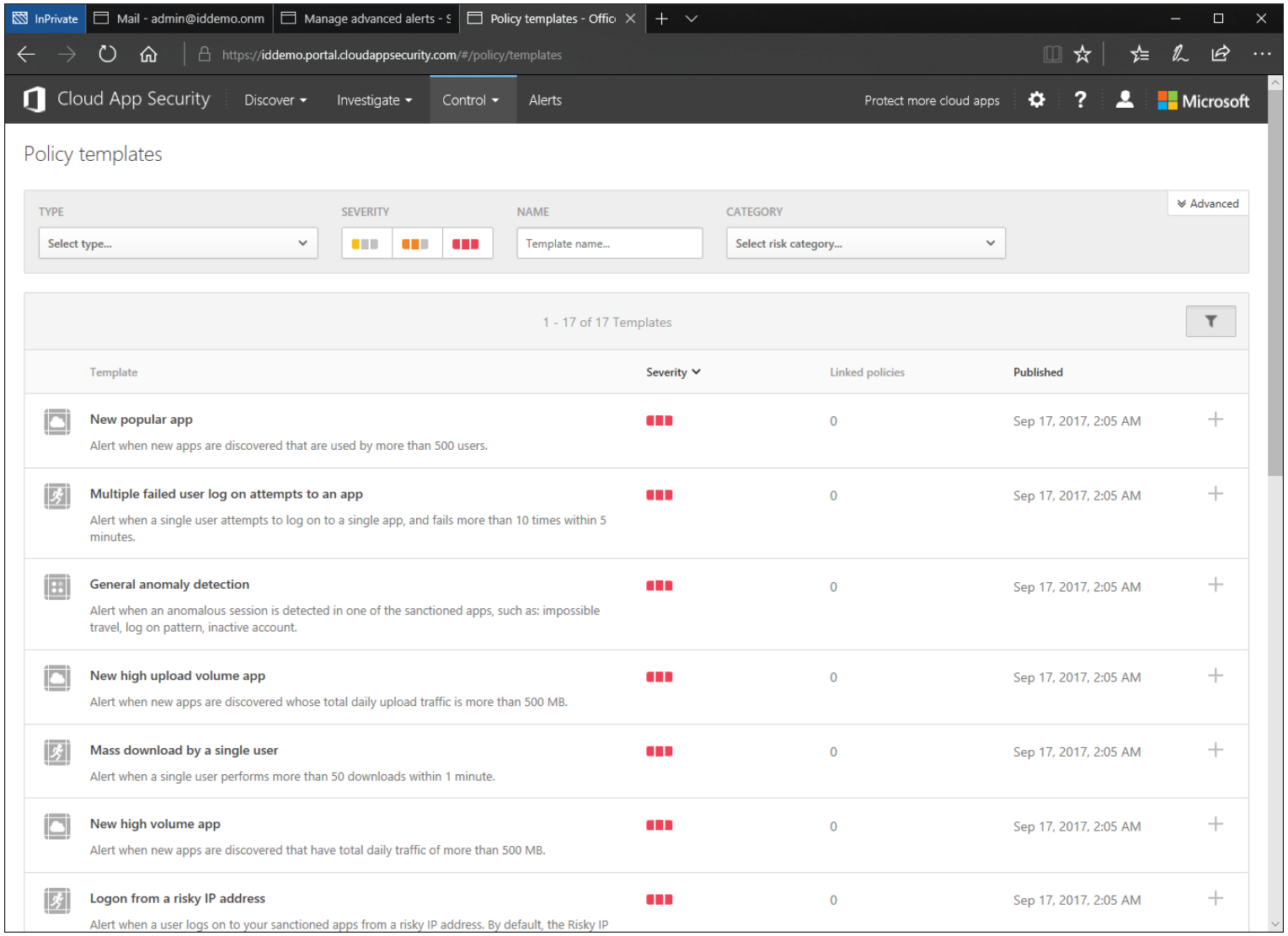
Microsoft 365

# CSP Masters Program in person series
## Technical training

# Detect & Respond: Cloud App Security

## Defender for Cloud Apps

- ✓ Suspicious user activity
- ✓ New OAuth applications
- ✓ Addition of mail forwarding rules



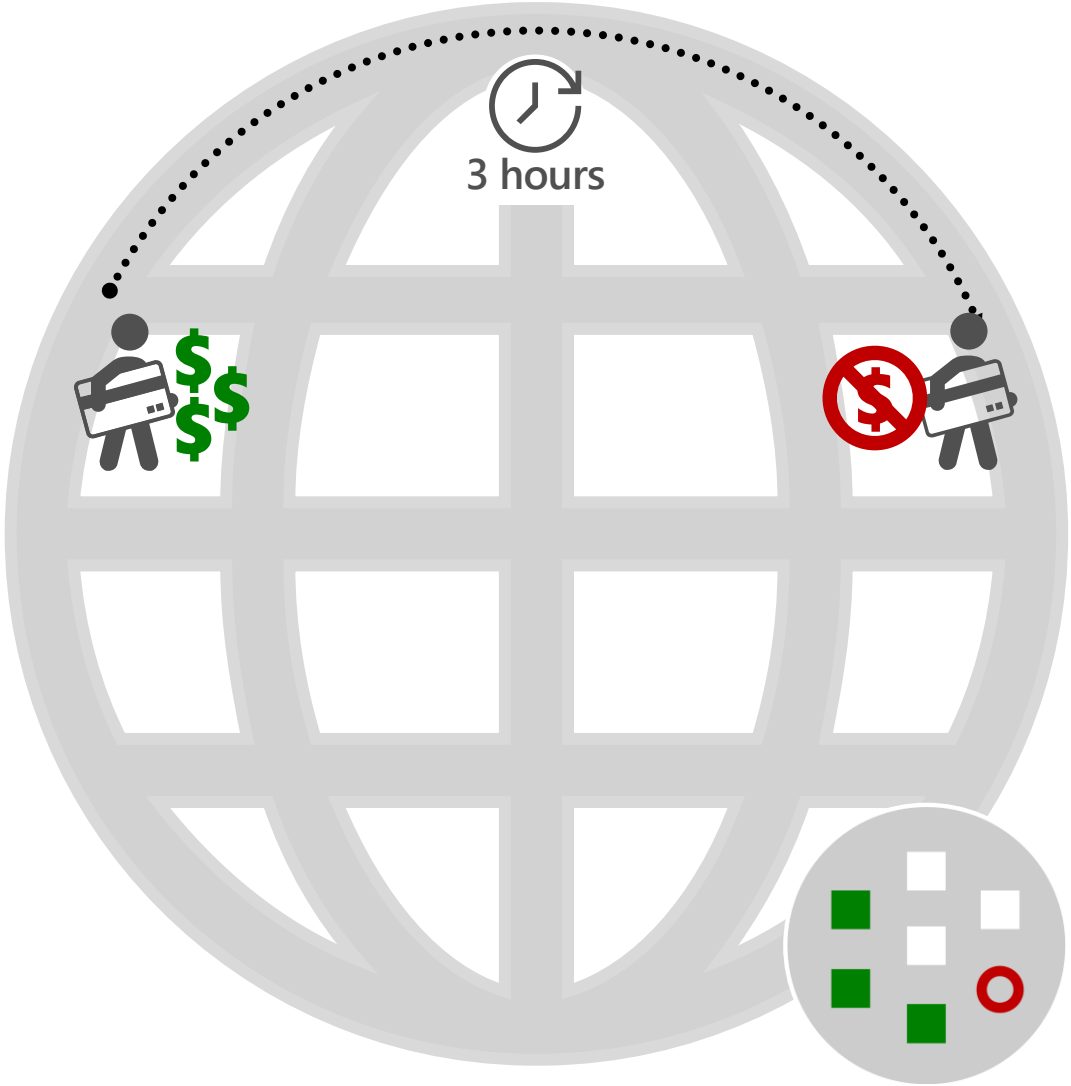

Personal laptop
Home office
Personal device
Personal wearable
Company-owned device
Customer wearable
Partners
Customers
Partner device
Customer device
On-premises
Mobile device
Mobile device

# User and entity behavioral analytics

Monitors behaviors of users and other entities by using **multiple data-sources**

Profiles behavior and detects anomalies by using **machine learning** algorithms

Evaluates the activity of users and other entities to detect **advanced attacks**

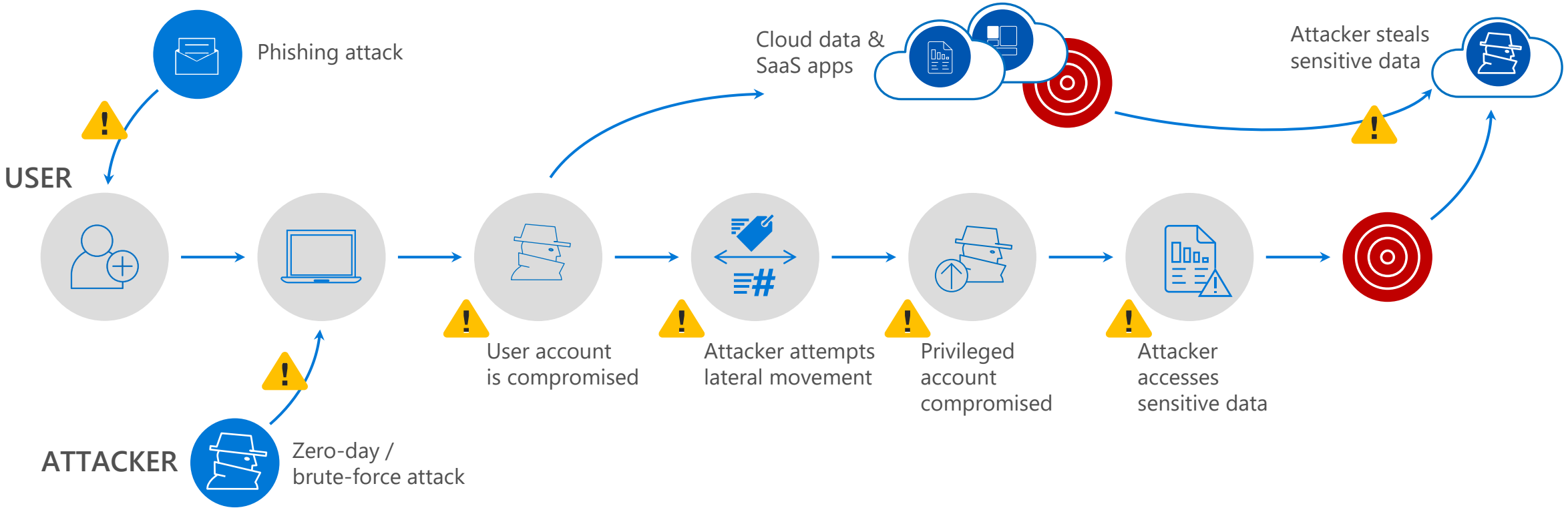



**Credit card companies monitor cardholders' behavior.**

**By observing purchases, behavioral analytics learn what behavior is typical for each buyer.**

**If there is any abnormal activity, they will notify the cardholder to verify charge.**

# I want to shorten the attack timeline




Anonymous user behavior

Lateral movement attacks

Data exfiltration

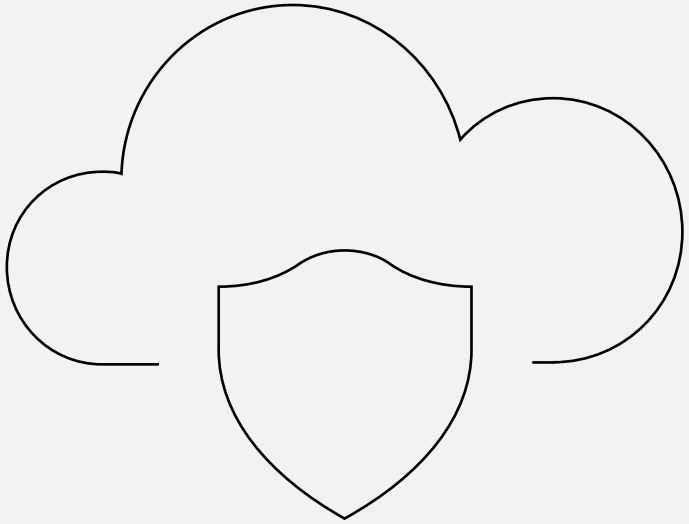
Unfamiliar sign-in location

Escalation of privileges

Anonymous user behavior

Account impersonation

# Microsoft Defender for Cloud Apps Security



## What is Microsoft Defender for Cloud Apps ?

A multi-mode Cloud Access Security Broker

## Insights into threats to identity and data

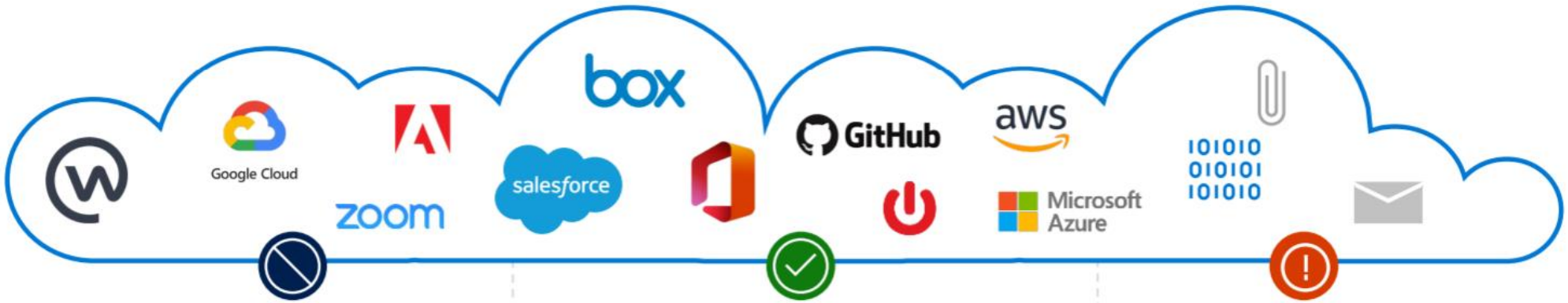
Raise alerts on user or file behavior anomalies in cloud apps leveraging their API connectors

## Ability to respond to detected threats, discover shadow IT usage and configure application monitoring and control

## Requirements

Available to organizations with an Azure tenant or a Microsoft 365 commercial subscription and who are in the multi-tenant and Microsoft 365 U.S. Government Community cloud

# Microsoft Cloud App Security addresses multiple use cases




Unsanctioned apps

Discover and govern

Sanctioned apps

Protect information

Control user sessions

Cloud Threats

Detect and block threats

Home

Office

Internal / External Users

Unmanaged Devices

# Monitor and control activities and data across apps

**1,181**

different cloud services are used by the average enterprise

**75%**

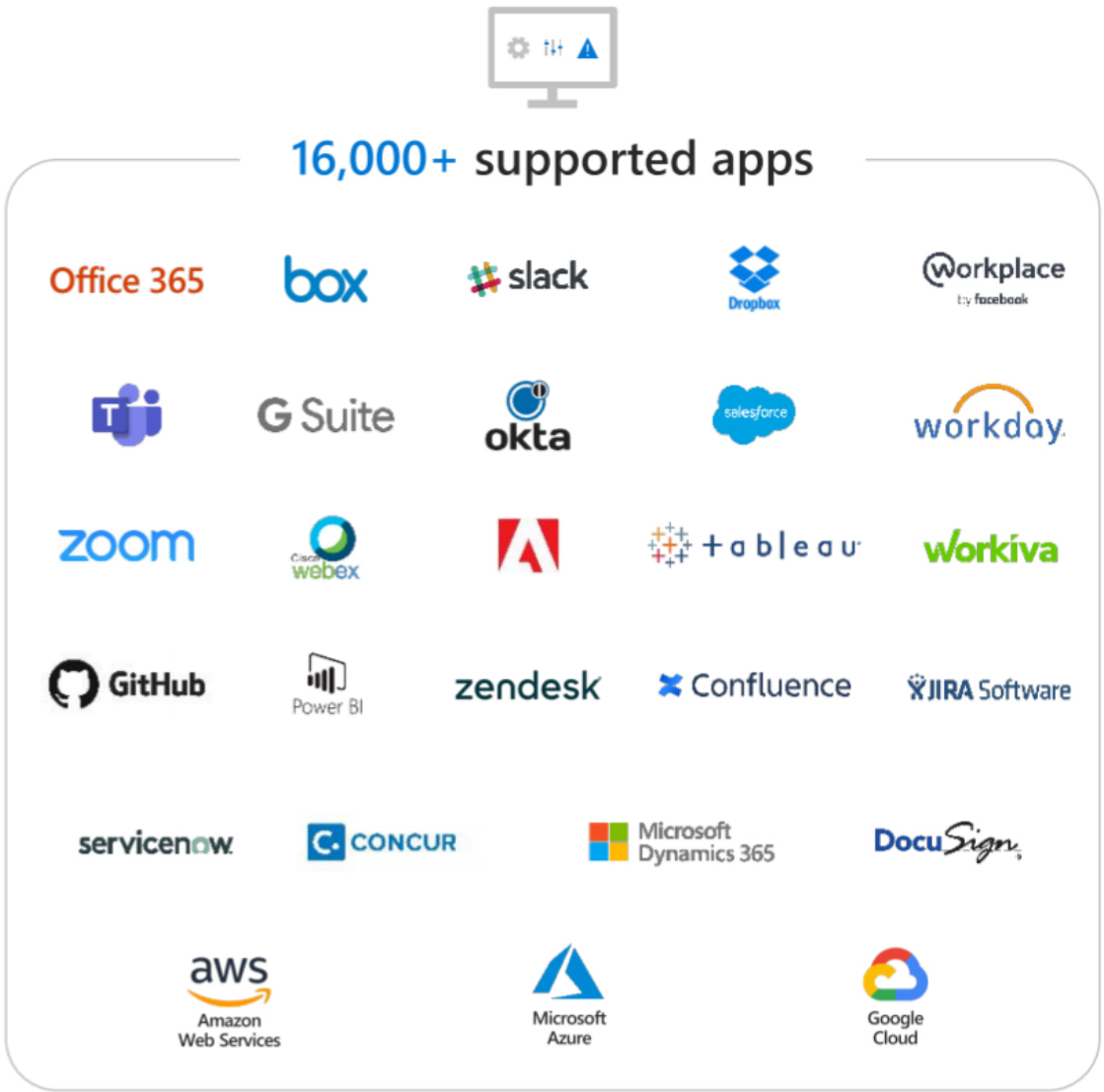
of companies consider SaaS tools essential to their business

**61%**

of cloud applications IT isn't aware of

**80%**

of workers use non-sanctioned cloud apps



# What is Defender for Cloud Apps Security?

## Cloud discovery

Discover all cloud usage in your organization

## Information protection

Monitor and control your data in the cloud

## Threat detection

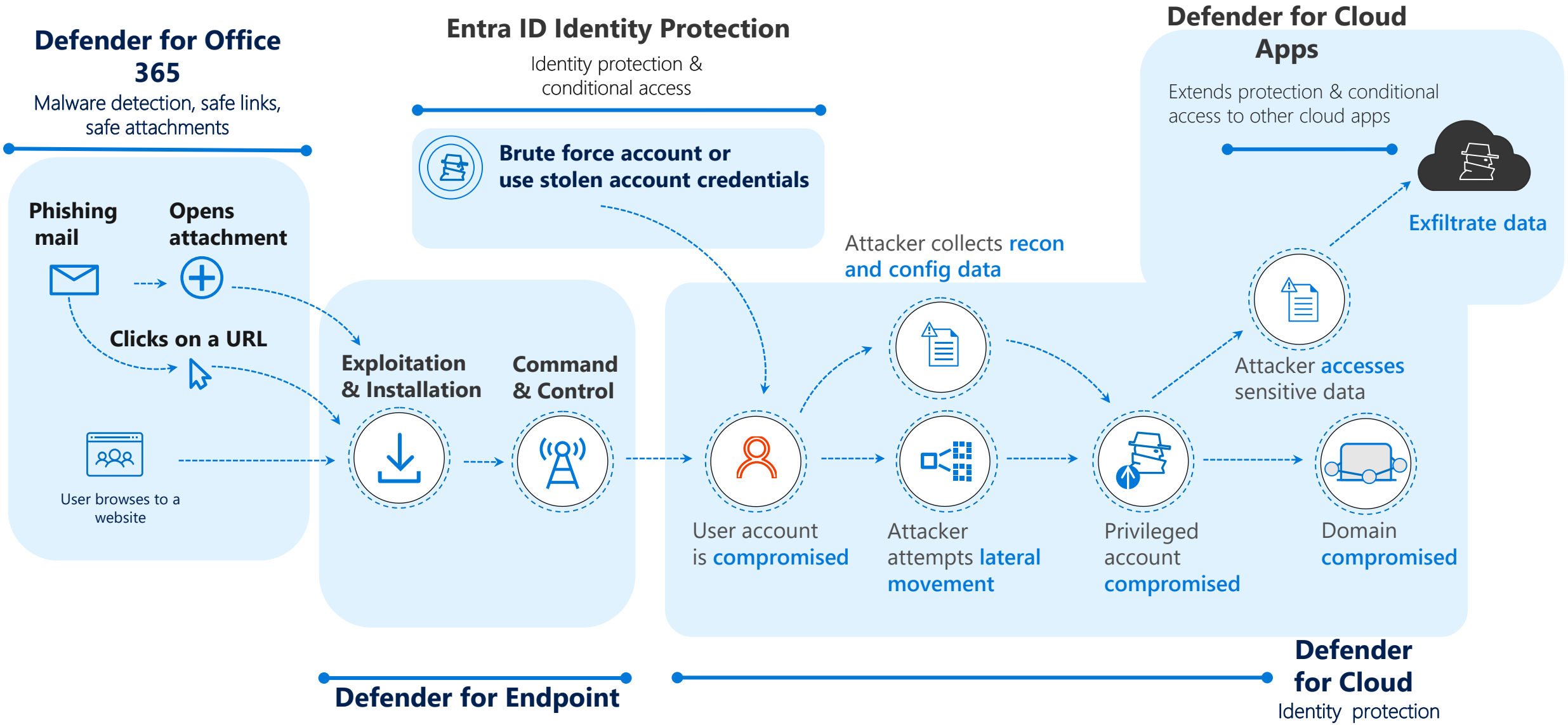
Detect usage anomalies and security incidents

## In-session control

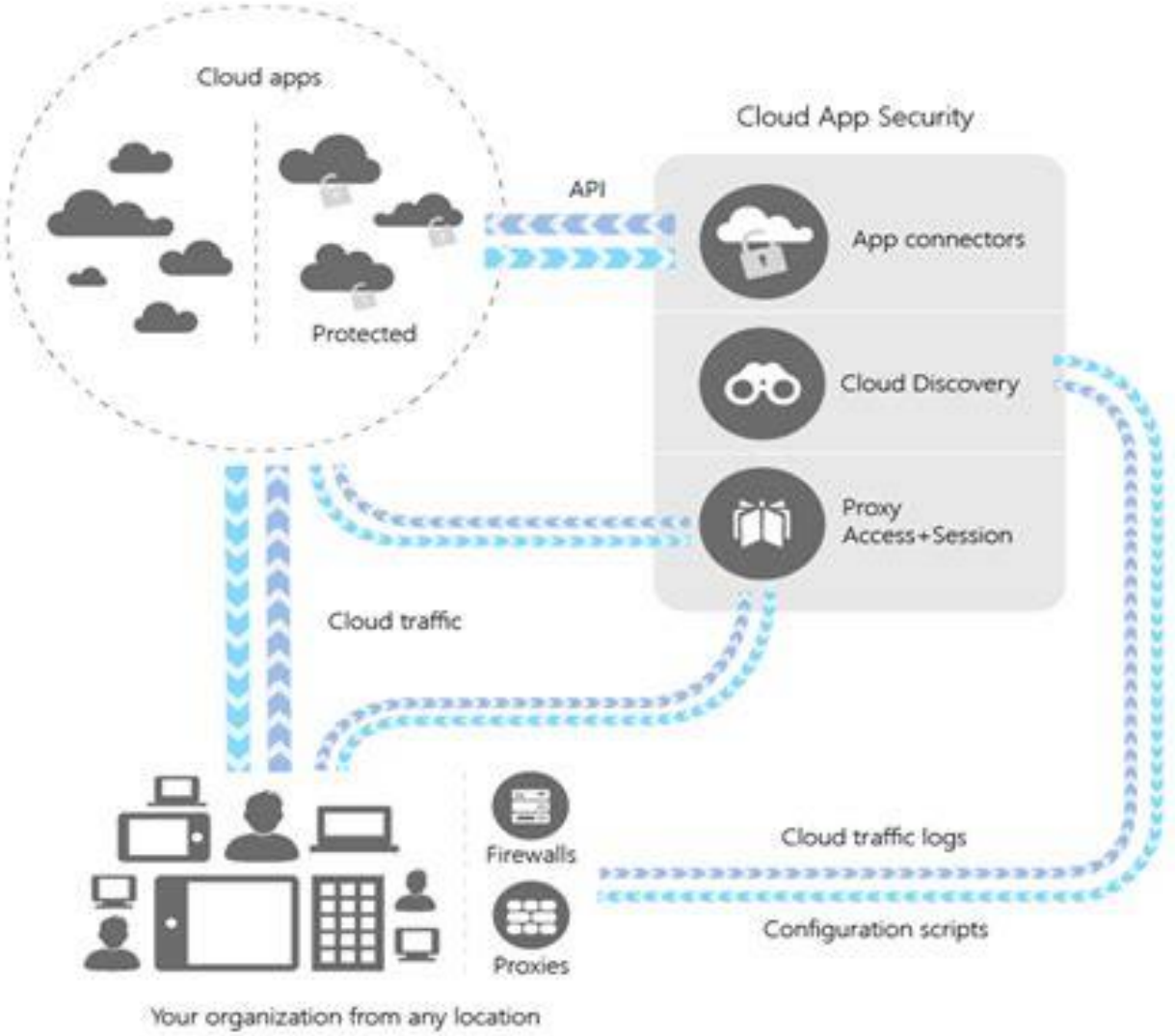
Control and limit user access based on session context

DISCOVER > INVESTIGATE > CONTROL > PROTECT

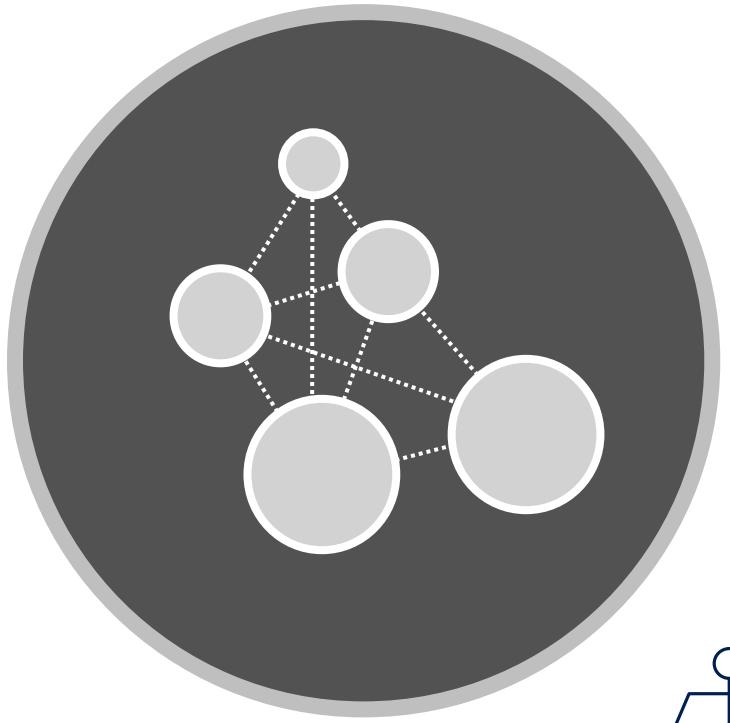
# Protection across the attack kill chain



# Architecture



# Defender for Cloud Apps protects the application session



### Malicious Insider

Protect against disgruntled employees before they cause damage

### Malware

Detect malware in cloud storage as soon as it's uploaded

### Ransomware

Identify ransomware using sophisticated behavioral analytics technology

### Rogue Application

Identify rouge applications that access your data

### Data exfiltration

Detect unusual flow of data outside of your organization

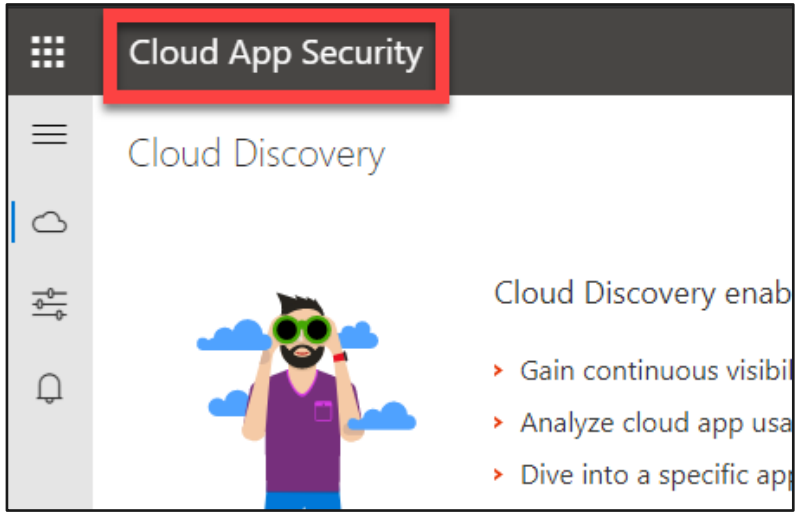
### Compromised Accounts

Combat advanced attackers that leverage compromise user credentials

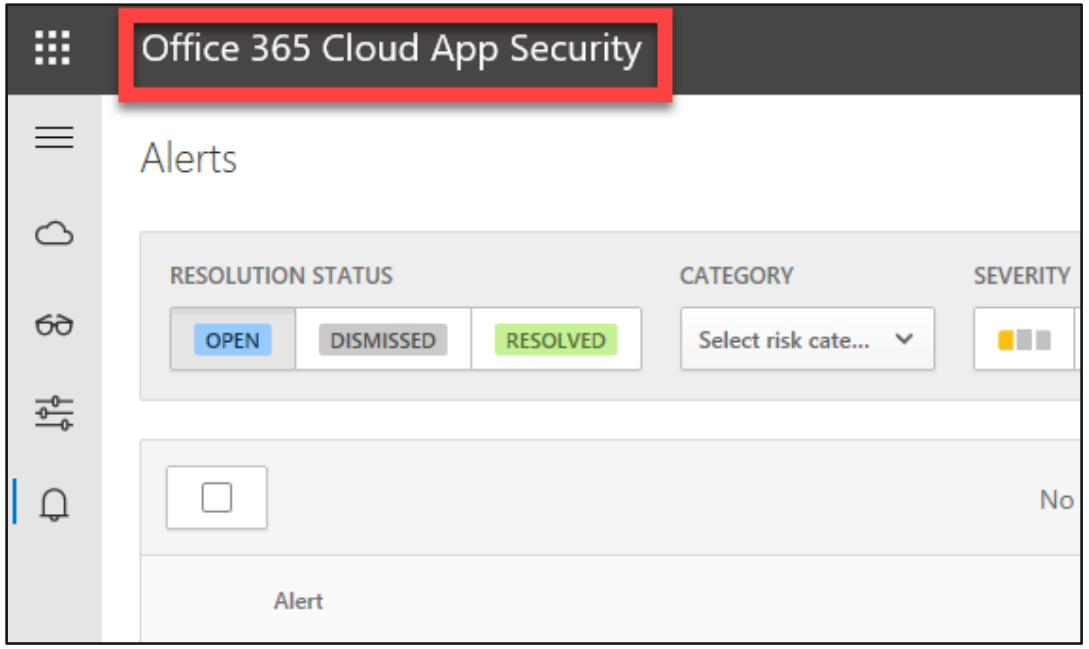
Microsoft Cloud App Security licensing datasheet - https://aka.ms/mcaslicensing

| Capability | Feature | Microsoft Cloud App Security | Azure AD Cloud App Discovery | Office 365 Cloud App Security |
|---|---|---|---|---|
| Cloud Discovery | Discovered apps | 16,000 + cloud apps | 16,000 + cloud apps | 750+ cloud apps with similar functionality to Office 365 |
| | Deployment for discovery analysis | Manual and automatic log upload | Manual and automatic log upload | Manual log upload |
| | Log anonymization for user privacy | Yes | Yes | |
| | Access to full Cloud App Catalog | Yes | Yes | |
| | Cloud app risk assessment | Yes | Yes | |
| | Cloud usage analytics per app, user, IP address | Yes | Yes | |
| | Ongoing analytics & reporting | Yes | Yes | |
| | Anomaly detection for discovered apps | Yes | | |
| Information Protection | Data Loss Prevention (DLP) support | Cross-SaaS DLP and data sharing control | | Uses existing Office DLP (available in Office E3 and above) |
| | App permissions and ability to revoke access | Yes | | Yes |
| | Policy setting and enforcement | Yes | | |
| | Integration with Azure Information Protection | Yes | | |
| | Integration with third-party DLP solutions | Yes | | |
| Threat Detection | Anomaly detection and behavioral analytics | For Cross-SaaS apps including Office 365 | | For Office 365 apps |
| | Manual and automatic alert remediation | Yes | | Yes |
| | SIEM connector | Yes. Alerts and activity logs for cross-SaaS apps. | | Yes. Office 365 alerts only. |
| | Integration to Microsoft Intelligent Security Graph | Yes | | Yes |
| | Activity policies | Yes | | Yes |

# Cloud App Security versions




Azure AD Cloud App Discover y- included with Azure AD P1

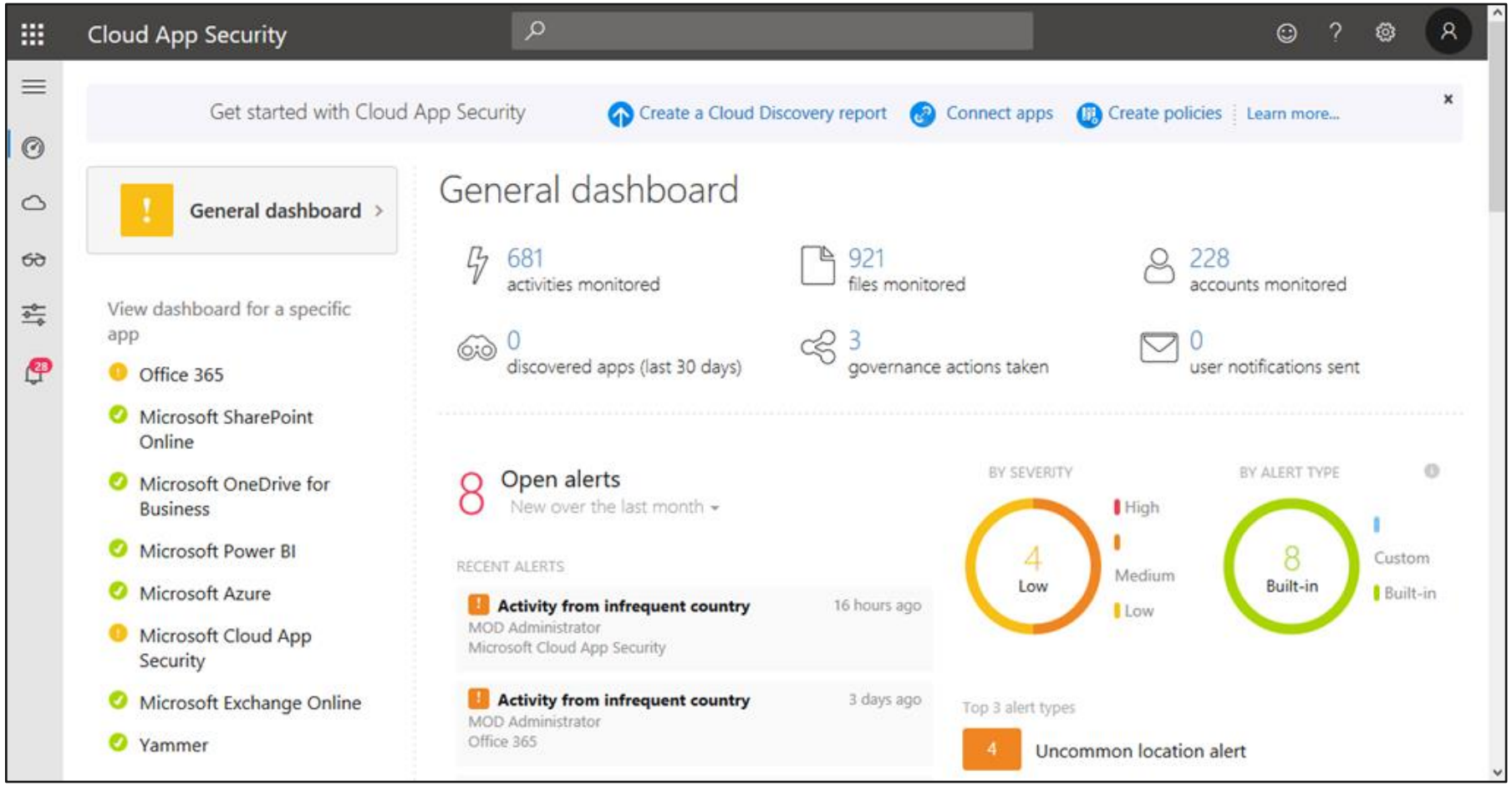



Office 365 Cloud App Security

$3.80 user/month

Enhanced visibility and control into your Office 365 environment.

# Cloud App Security Versions

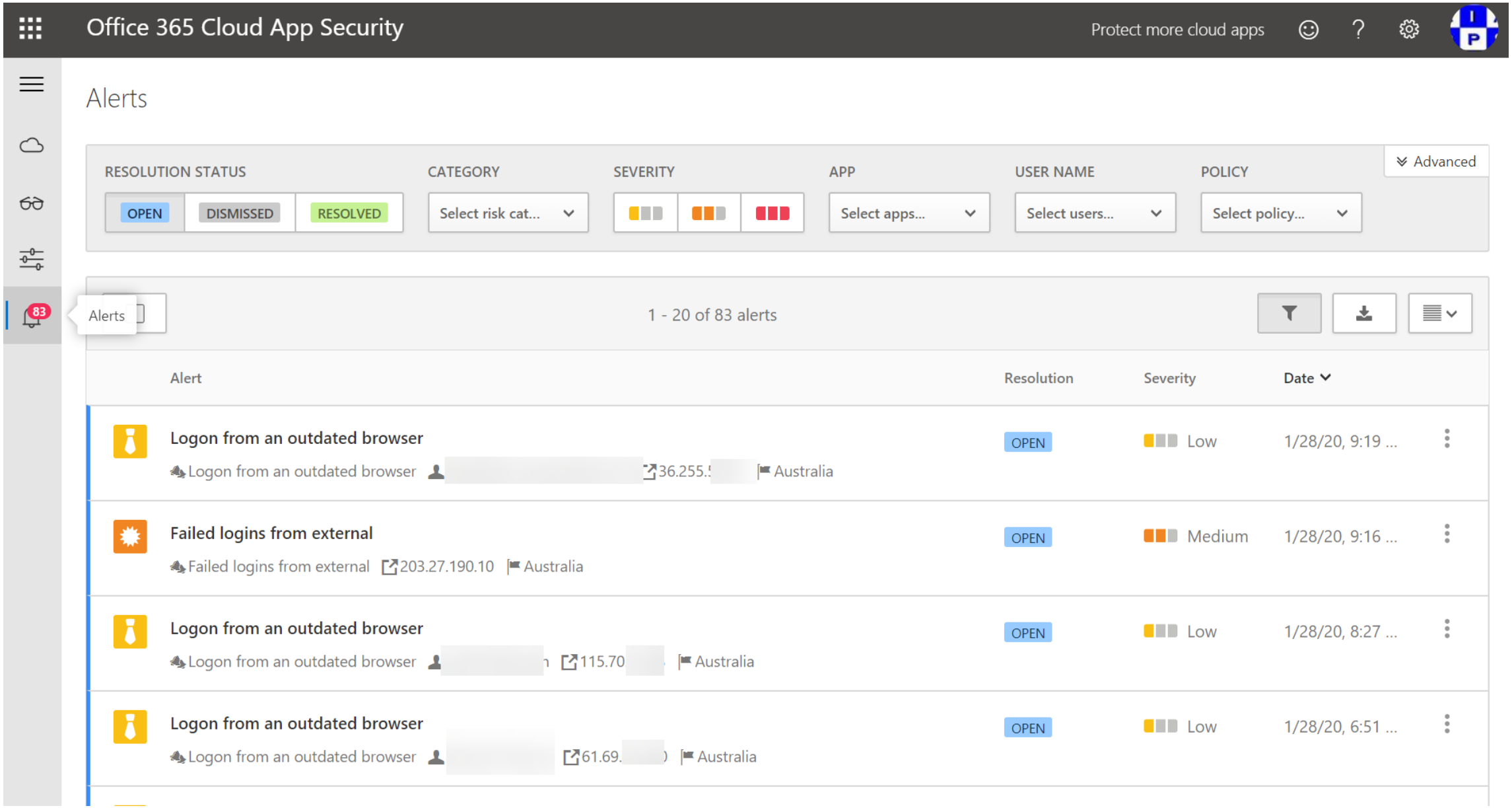



## Microsoft Cloud App Security

$4.50 user/month

A cross-platform cloud solution extending IT visibility, governance and control to the cloud applications.

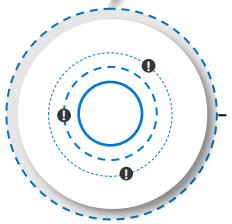
# Cloud App Security Alerts




https://portal.cloudappsecurity.com/#/alerts

# Microsoft Cloud App Security – Cross apps detections

Suspicious inbox rules (delete, forward)
Malware implanted in cloud apps
Malicious OAuth application
Multiple failed login attempts to app

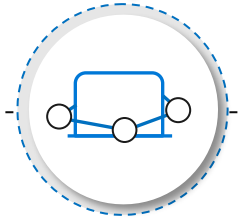


Threat delivery and persistence

Indicators of a compromised session

Activity from suspicious IP addresses
Activity from anonymous IP addresses
Activity from an infrequent country
Impossible travel between sessions
Logon attempt from a suspicious user agent

Unusual file share activity
Unusual file download
Unusual file deletion activity
Ransomware activity
Data exfiltration to unsanctioned apps
Activity by a terminated employee

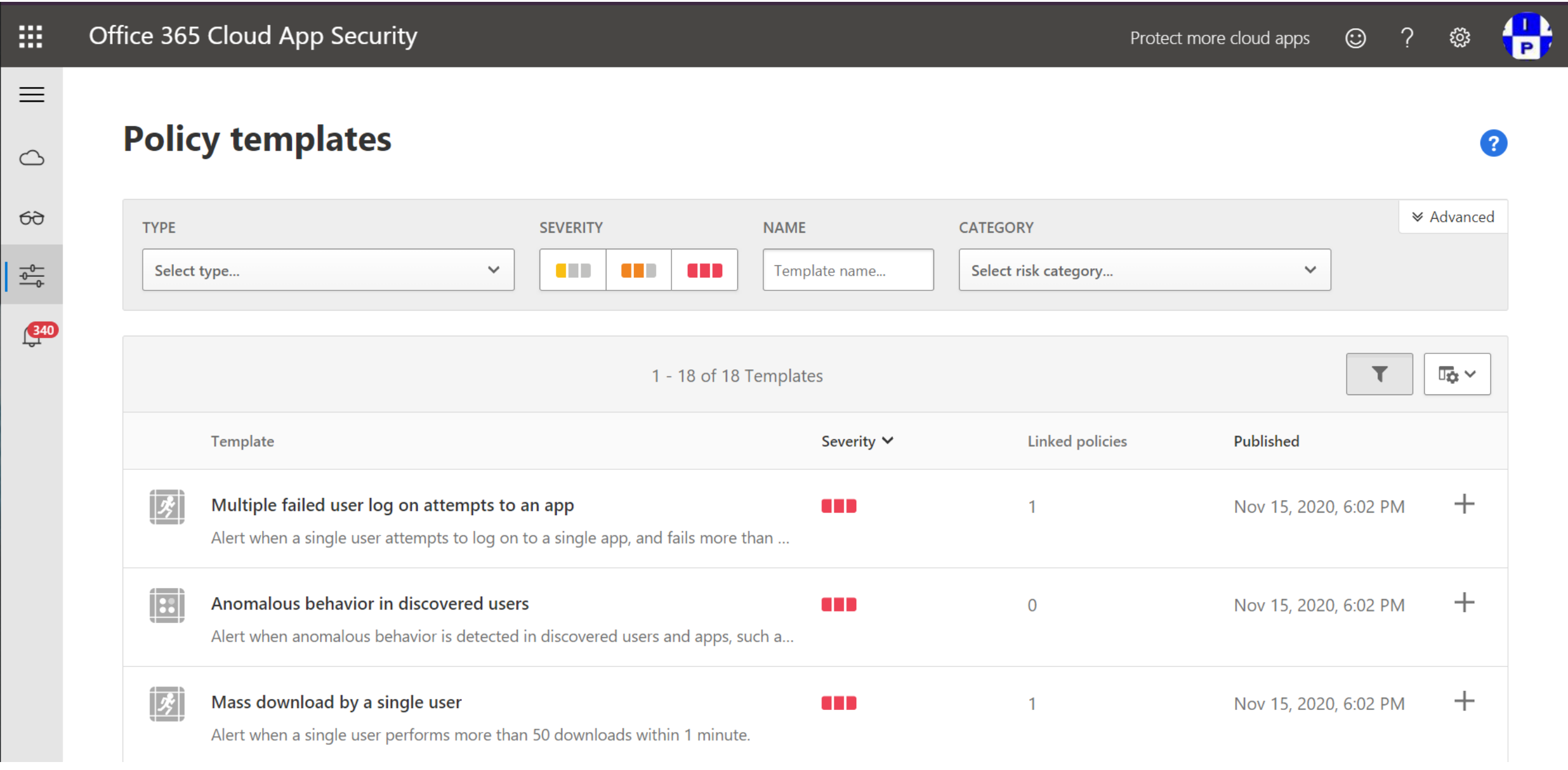


Malicious use of an end-user account

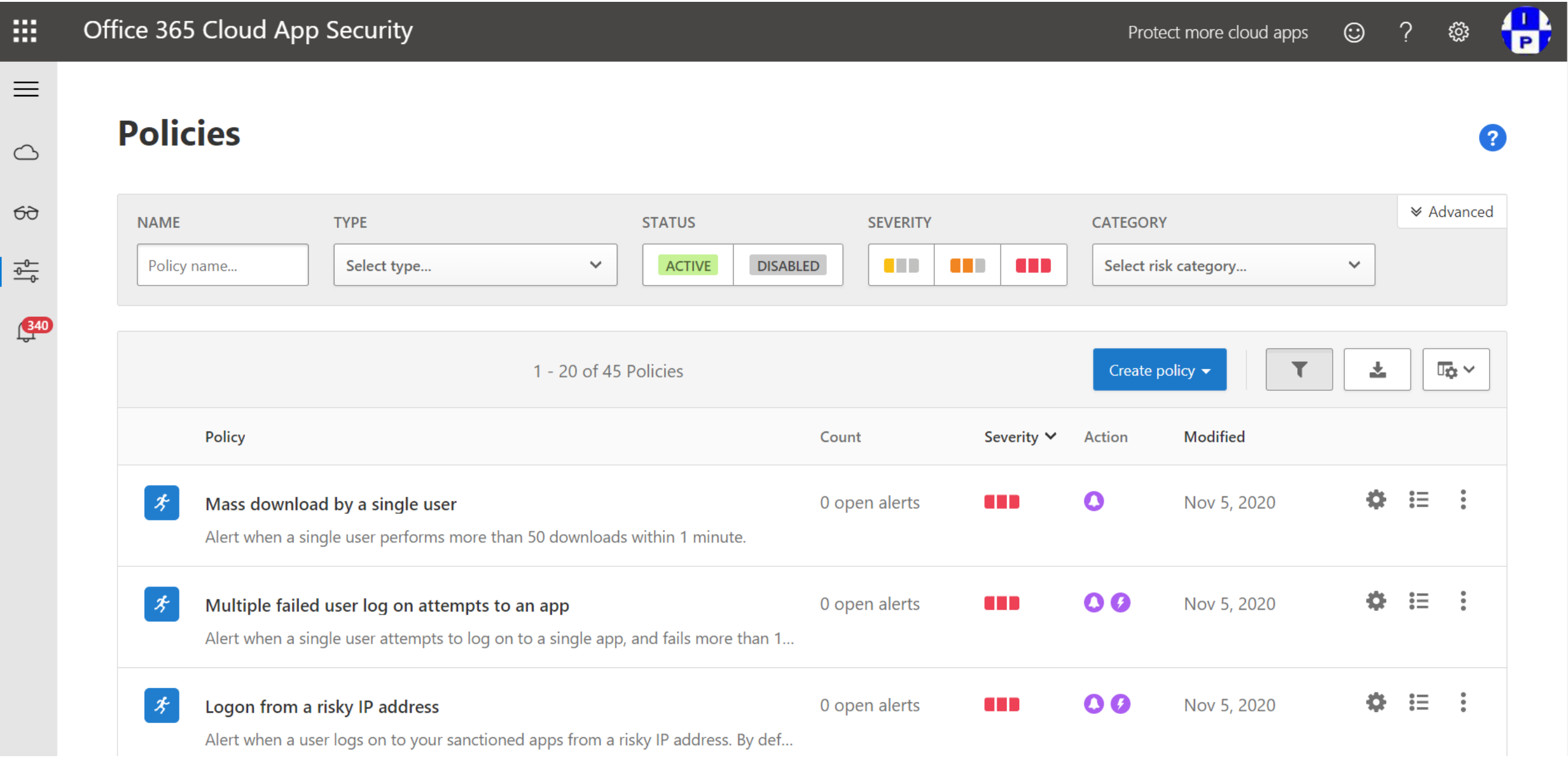
Malicious use of a privileged user

Unusual impersonated activity
Unusual administrative activity
Unusual multiple delete VM activity

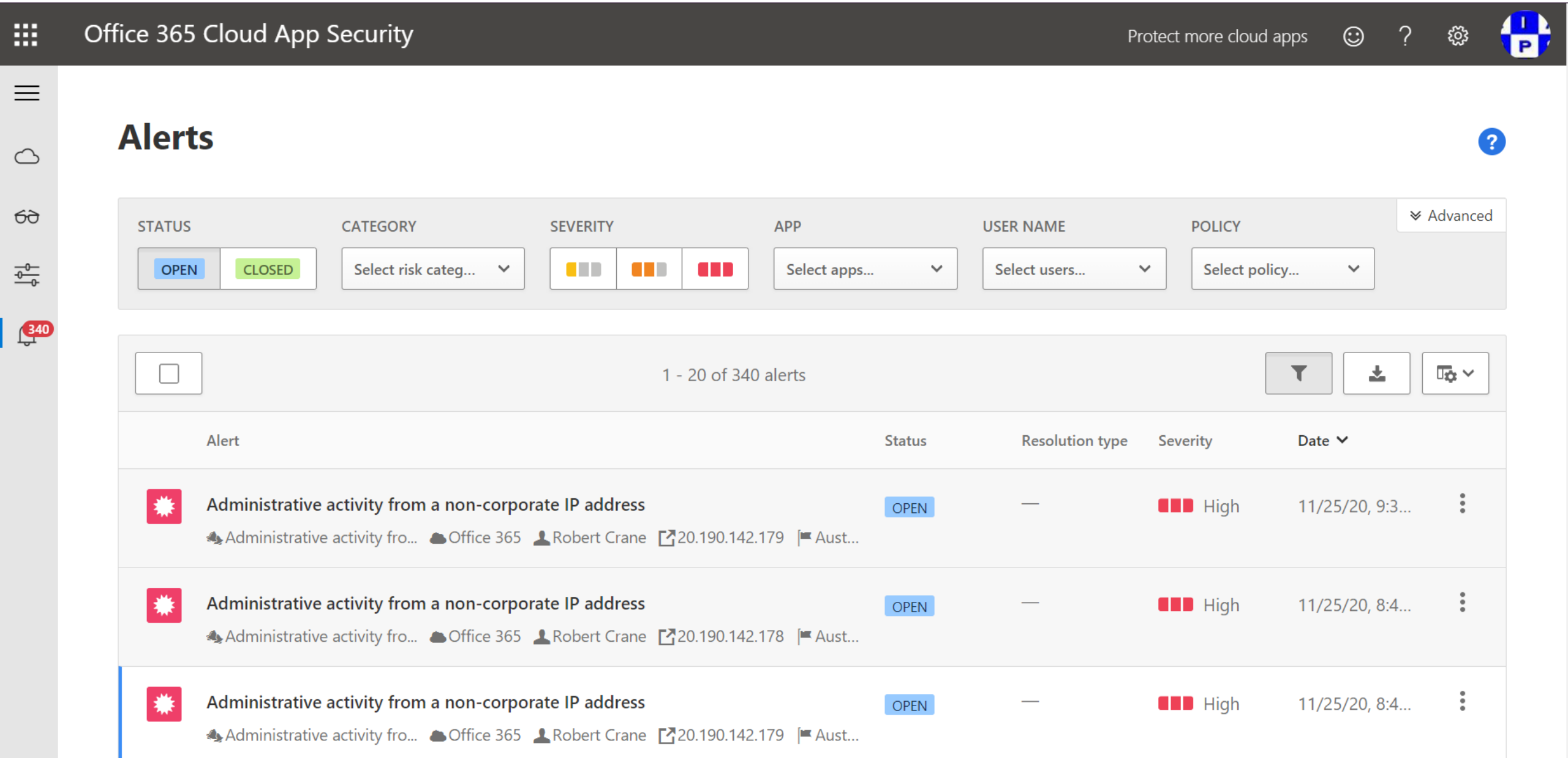
# Policy Templates



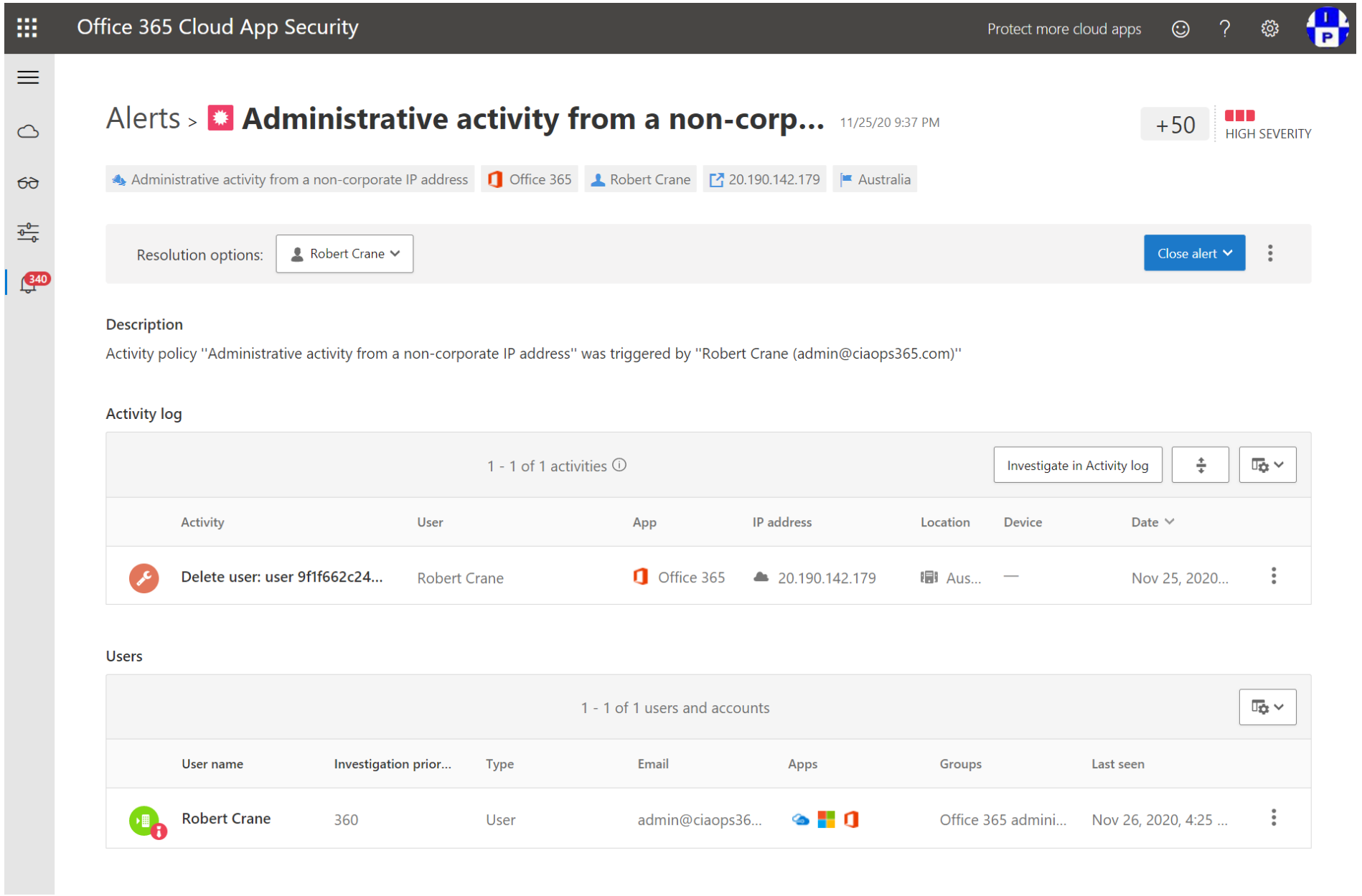
# Policies

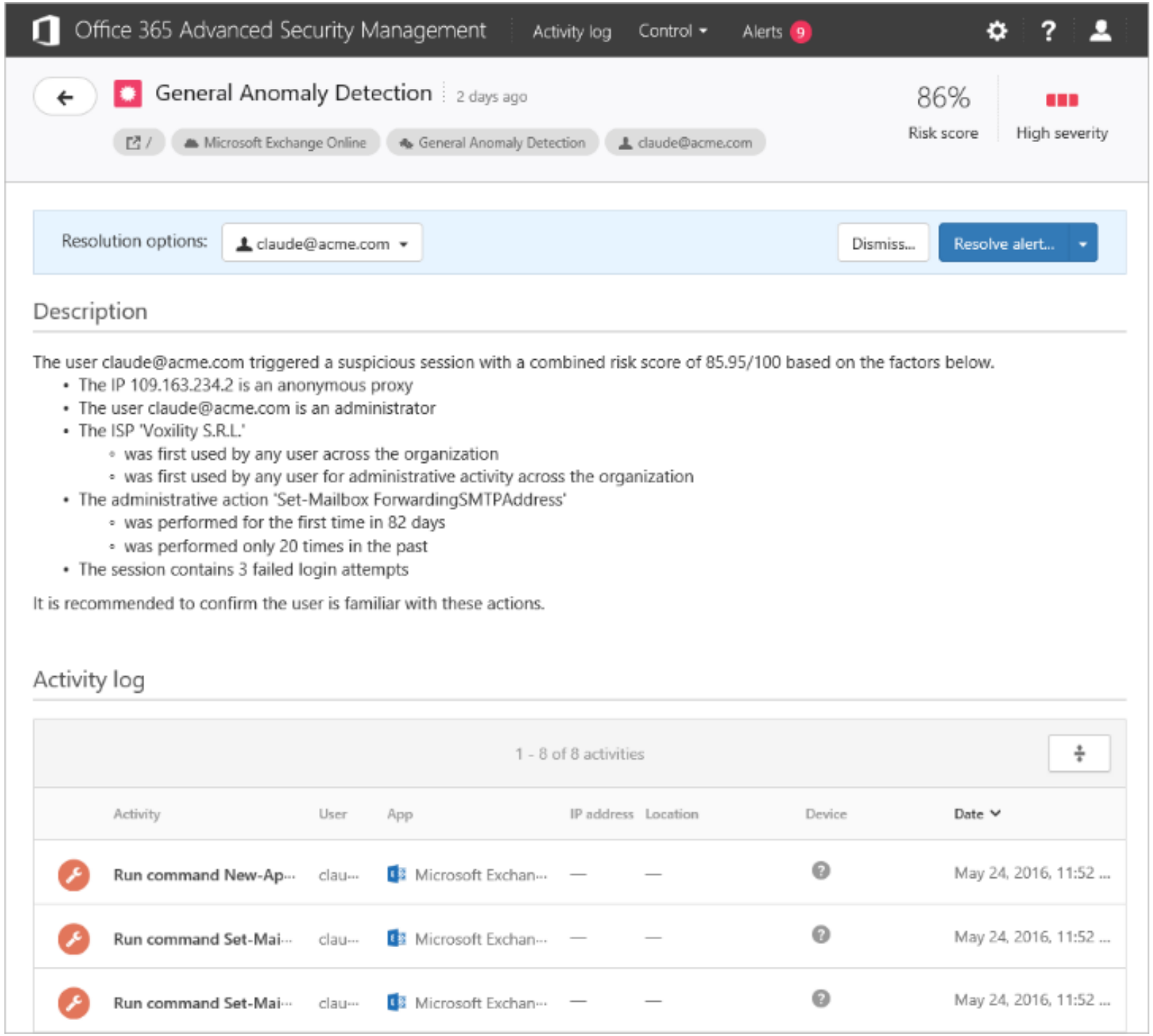

Office 365 Cloud App Security
Protect more cloud apps
340
Policies
NAME
Policy name...
TYPE
Select type...
STATUS
ACTIVE
DISABLED
SEVERITY
CATEGORY
Select risk category...
Advanced
1 - 20 of 45 Policies
Create policy
Policy
Count
Severity
Action
Modified
Mass download by a single user
0 open alerts
Nov 5, 2020
Alert when a single user performs more than 50 downloads within 1 minute.
Multiple failed user log on attempts to an app
0 open alerts
Nov 5, 2020
Alert when a single user attempts to log on to a single app, and fails more than 1...
Logon from a risky IP address
0 open alerts
Nov 5, 2020
Alert when a user logs on to your sanctioned apps from a risky IP address. By def...

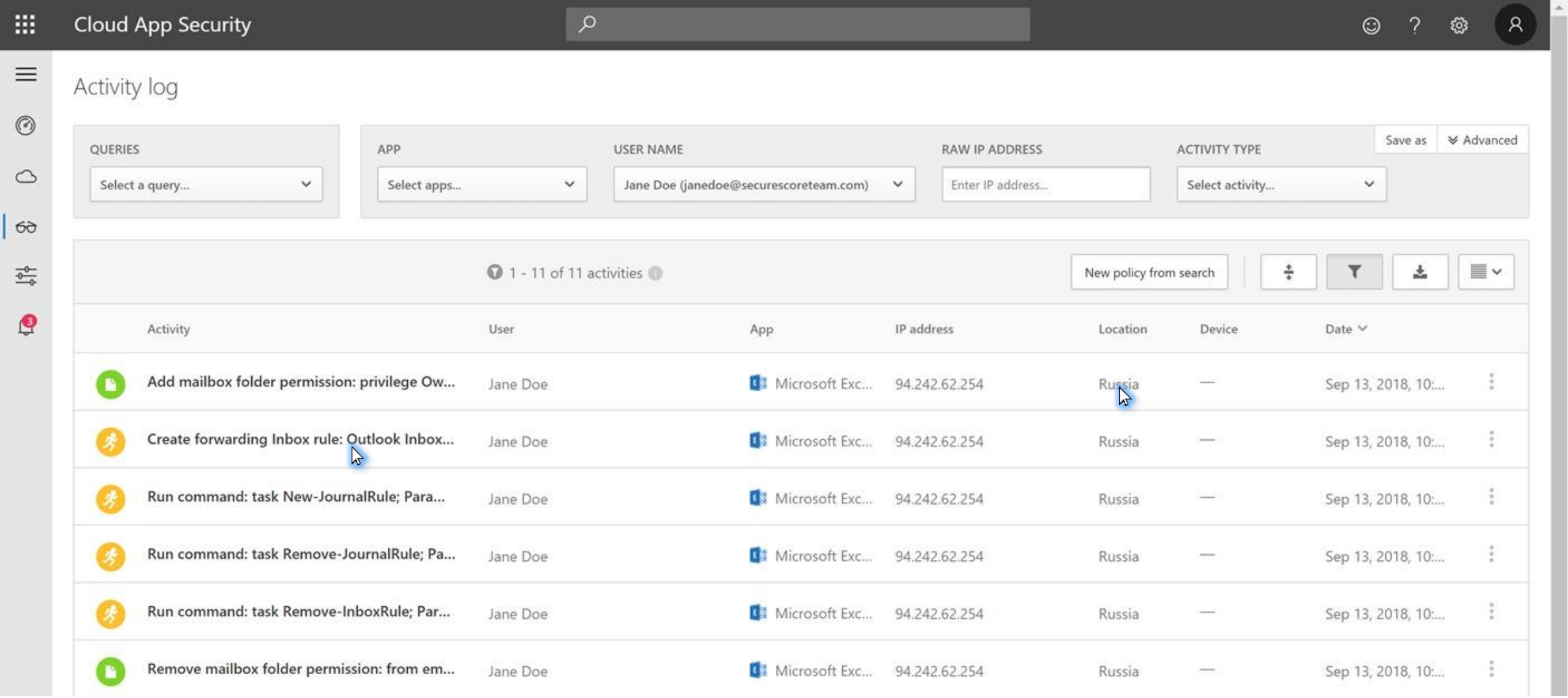
# Alerts

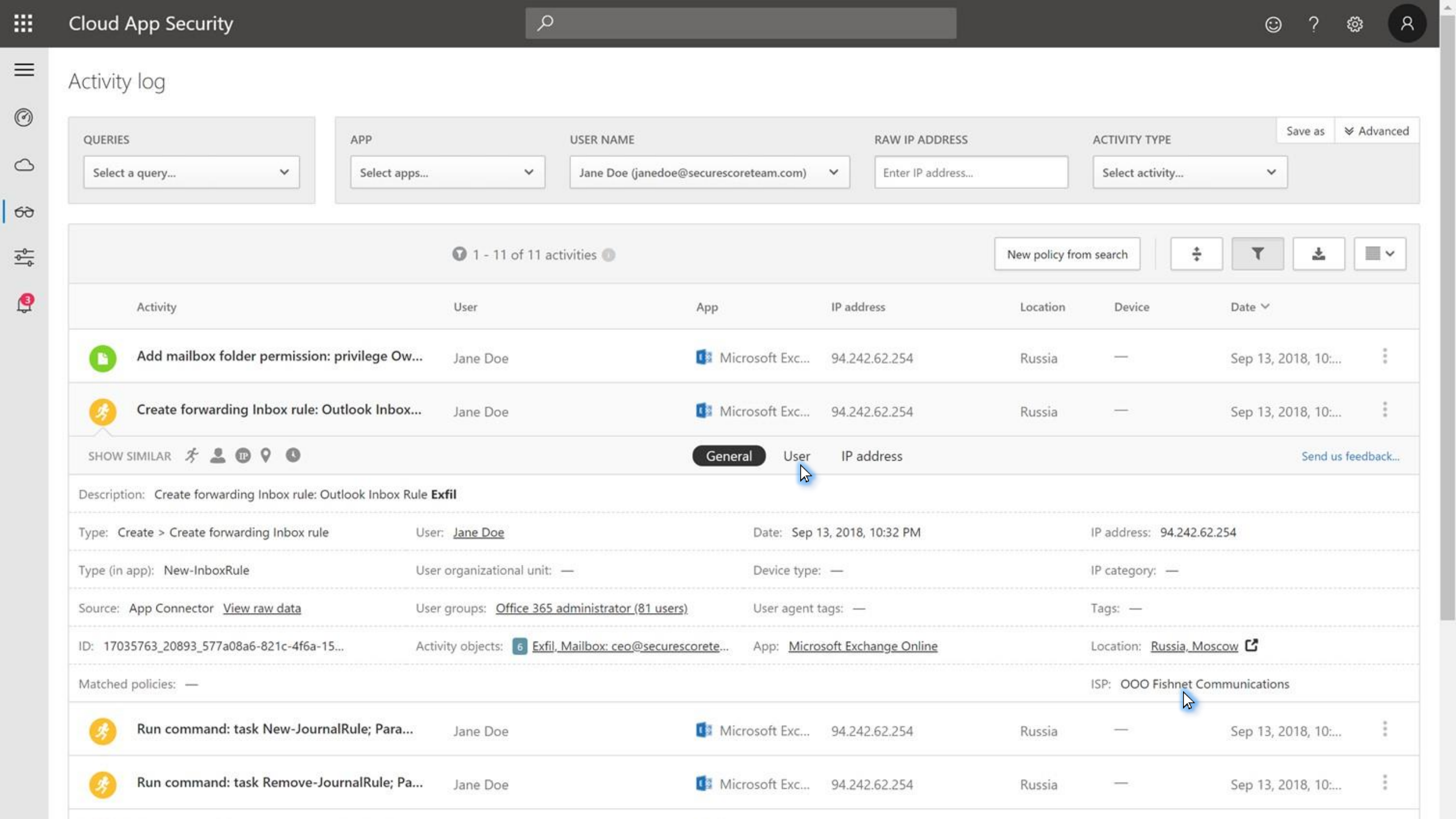

Office 365 Cloud App Security
Protect more cloud apps
340
Alerts
STATUS
OPEN
CLOSED
CATEGORY
Select risk categ...
SEVERITY
APP
Select apps...
USER NAME
Select users...
POLICY
Select policy...
Advanced
1 - 20 of 340 alerts
Alert
Status
Resolution type
Severity
Date
Administrative activity from a non-corporate IP address
Administrative activity fro... Office 365 Robert Crane 20.190.142.179 Aust...
OPEN
—
High
11/25/20, 9:3...
Administrative activity from a non-corporate IP address
Administrative activity fro... Office 365 Robert Crane 20.190.142.178 Aust...
OPEN
—
High
11/25/20, 8:4...
Administrative activity from a non-corporate IP address
Administrative activity fro... Office 365 Robert Crane 20.190.142.179 Aust...
OPEN
—
High
11/25/20, 8:4...

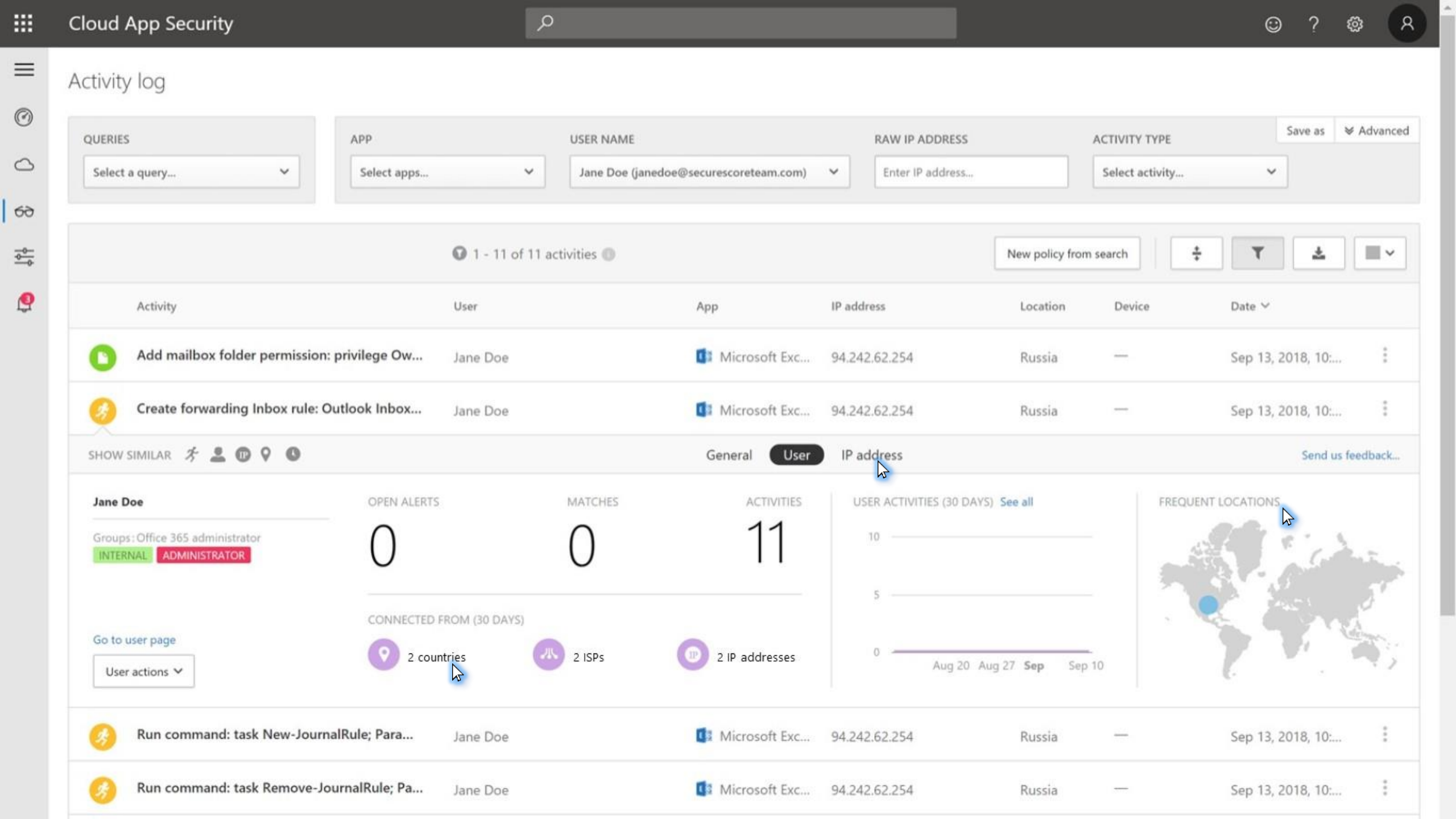
# Alerts - Detail




Office 365 Advanced Security Management
Activity log
Control
Alerts 9
General Anomaly Detection
2 days ago
/
Microsoft Exchange Online
General Anomaly Detection
claude@acme.com
86%
Risk score
High severity
Resolution options:
claude@acme.com
Dismiss...
Resolve alert...
Description
The user claude@acme.com triggered a suspicious session with a combined risk score of 85.95/100 based on the factors below.
• The IP 109.163.234.2 is an anonymous proxy
• The user claude@acme.com is an administrator
• The ISP 'Voxility S.R.L.'
◦ was first used by any user across the organization
◦ was first used by any user for administrative activity across the organization
• The administrative action 'Set-Mailbox ForwardingSMTPAddress'
◦ was performed for the first time in 82 days
◦ was performed only 20 times in the past
• The session contains 3 failed login attempts
It is recommended to confirm the user is familiar with these actions.
Activity log
1 - 8 of 8 activities
Activity
User
App
IP address
Location
Device
Date
Run command New-Ap···
clau···
Microsoft Exchan···
—
—
May 24, 2016, 11:52 ...
Run command Set-Mai···
clau···
Microsoft Exchan···
—
—
May 24, 2016, 11:52 ...
Run command Set-Mai···
clau···
Microsoft Exchan···
—
—
May 24, 2016, 11:52 ...


Cloud App Security
Activity log
QUERIES
Select a query...
APP
Select apps...
USER NAME
Jane Doe (janedoe@securescoreteam.com)
RAW IP ADDRESS
Enter IP address...
ACTIVITY TYPE
Select activity...
Save as
Advanced
1 - 11 of 11 activities
New policy from search
Activity
User
App
IP address
Location
Device
Date
Add mailbox folder permission: privilege Ow...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
—
Sep 13, 2018, 10:...
Create forwarding Inbox rule: Outlook Inbox...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
—
Sep 13, 2018, 10:...
Run command: task New-JournalRule; Para...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
—
Sep 13, 2018, 10:...
Run command: task Remove-JournalRule; Pa...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
—
Sep 13, 2018, 10:...
Run command: task Remove-InboxRule; Par...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
—
Sep 13, 2018, 10:...
Remove mailbox folder permission: from em...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
—
Sep 13, 2018, 10:...


Cloud App Security
Activity log
QUERIES
Select a query...
APP
Select apps...
USER NAME
Jane Doe (janedoe@securescoreteam.com)
RAW IP ADDRESS
Enter IP address...
ACTIVITY TYPE
Select activity...
Save as
Advanced
1 - 11 of 11 activities
New policy from search
Activity
User
App
IP address
Location
Device
Date
Add mailbox folder permission: privilege Ow...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
—
Sep 13, 2018, 10:...
Create forwarding Inbox rule: Outlook Inbox...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
—
Sep 13, 2018, 10:...
SHOW SIMILAR
General
User
IP address
Send us feedback...
Description: Create forwarding Inbox rule: Outlook Inbox Rule Exfil
Type: Create > Create forwarding Inbox rule
User: Jane Doe
Date: Sep 13, 2018, 10:32 PM
IP address: 94.242.62.254
Type (in app): New-InboxRule
User organizational unit: —
Device type: —
IP category: —
Source: App Connector View raw data
User groups: Office 365 administrator (81 users)
User agent tags: —
Tags: —
ID: 17035763_20893_577a08a6-821c-4f6a-15...
Activity objects: 6 Exfil, Mailbox: ceo@securescorete...
App: Microsoft Exchange Online
Location: Russia, Moscow
Matched policies: —
ISP: OOO Fishnet Communications
Run command: task New-JournalRule; Para...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
—
Sep 13, 2018, 10:...
Run command: task Remove-JournalRule; Pa...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
—
Sep 13, 2018, 10:...


Cloud App Security
Activity log
QUERIES
Select a query...
APP
Select apps...
USER NAME
Jane Doe (janedoe@securescoreteam.com)
RAW IP ADDRESS
Enter IP address...
ACTIVITY TYPE
Select activity...
Save as
Advanced
1 - 11 of 11 activities
New policy from search
Activity
User
App
IP address
Location
Device
Date
Add mailbox folder permission: privilege Ow...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
Sep 13, 2018, 10:...
Create forwarding Inbox rule: Outlook Inbox...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
Sep 13, 2018, 10:...
SHOW SIMILAR
General
User
IP address
Send us feedback...
Jane Doe
Groups: Office 365 administrator
INTERNAL
ADMINISTRATOR
Go to user page
User actions
OPEN ALERTS
0
MATCHES
0
ACTIVITIES
11
CONNECTED FROM (30 DAYS)
2 countries
2 ISPs
2 IP addresses
USER ACTIVITIES (30 DAYS)
See all
10
5
0
Aug 20
Aug 27
Sep
Sep 10
FREQUENT LOCATIONS
Run command: task New-JournalRule; Para...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
Sep 13, 2018, 10:...
Run command: task Remove-JournalRule; Pa...
Jane Doe
Microsoft Exc...
94.242.62.254
Russia
Sep 13, 2018, 10:...

Cloud App Security

# Activity log

QUERIES: Select a query...

APP: Select apps...

USER NAME: Jane Doe (janedoe@securescoreteam.com)

RAW IP ADDRESS: Enter IP address...

ACTIVITY TYPE: Select activity...

Save as | Advanced

1 - 11 of 11 activities

New policy from search

| Activity | User | App | IP address | Location | Device | Date |
|---|---|---|---|---|---|---|
| Add mailbox folder permission: privilege Ow... | Jane Doe | Microsoft Exc... | 94.242.62.254 | Russia | — | Sep 13, 2018, 10:... |
| Create forwarding Inbox rule: Outlook Inbox... | Jane Doe | Microsoft Exc... | 94.242.62.254 | Russia | — | Sep 13, 2018, 10:... |

SHOW SIMILAR

General | User | IP address

Send us feedback...

94.242.62.254

Russia, Moscow

ISP: OOO Fi[illegible]et Communications

OPEN ALERTS: 0

ACTIVITIES: 8

ADMIN ACTIVITIES: 0

IP ACTIVITIES (30 DAYS) See all

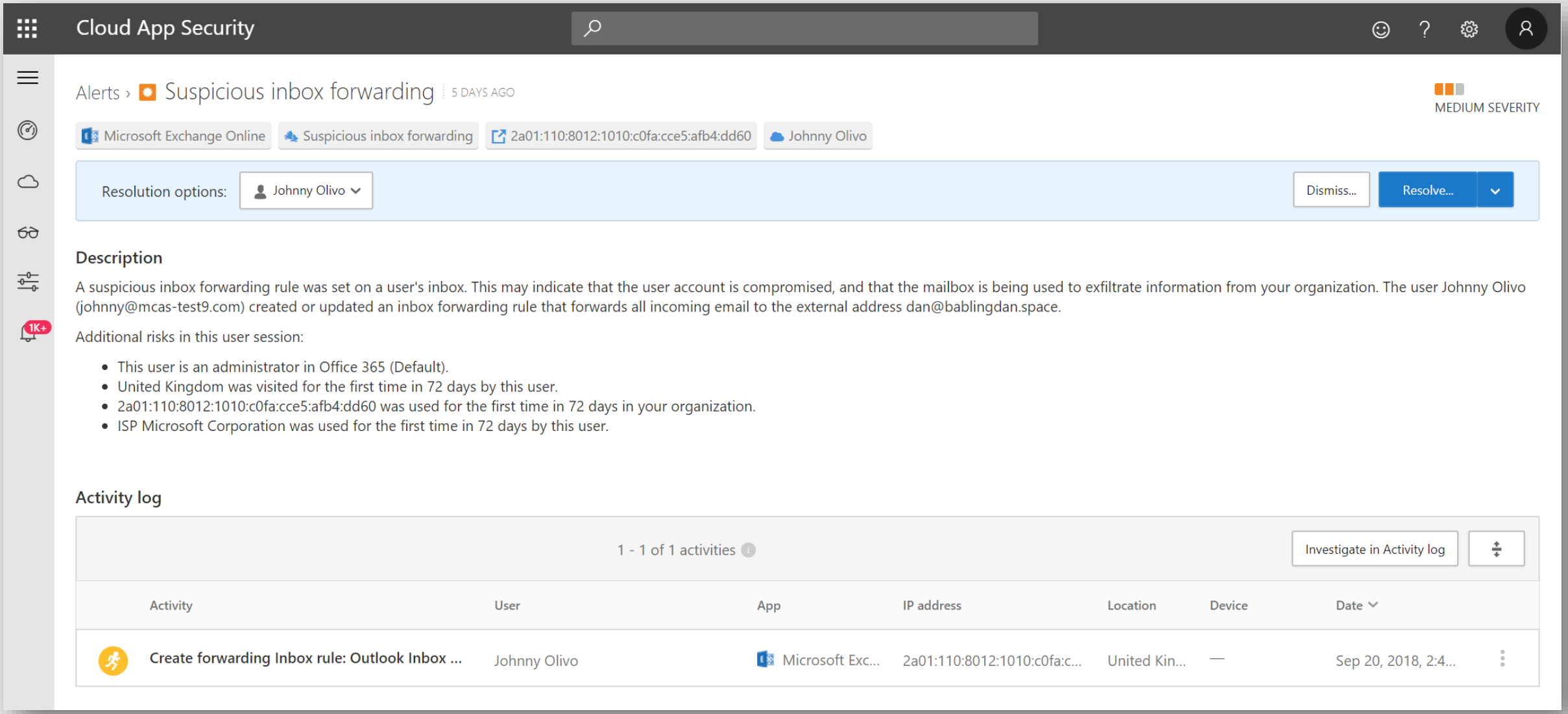

IP LOCATION

Filter by this IP address

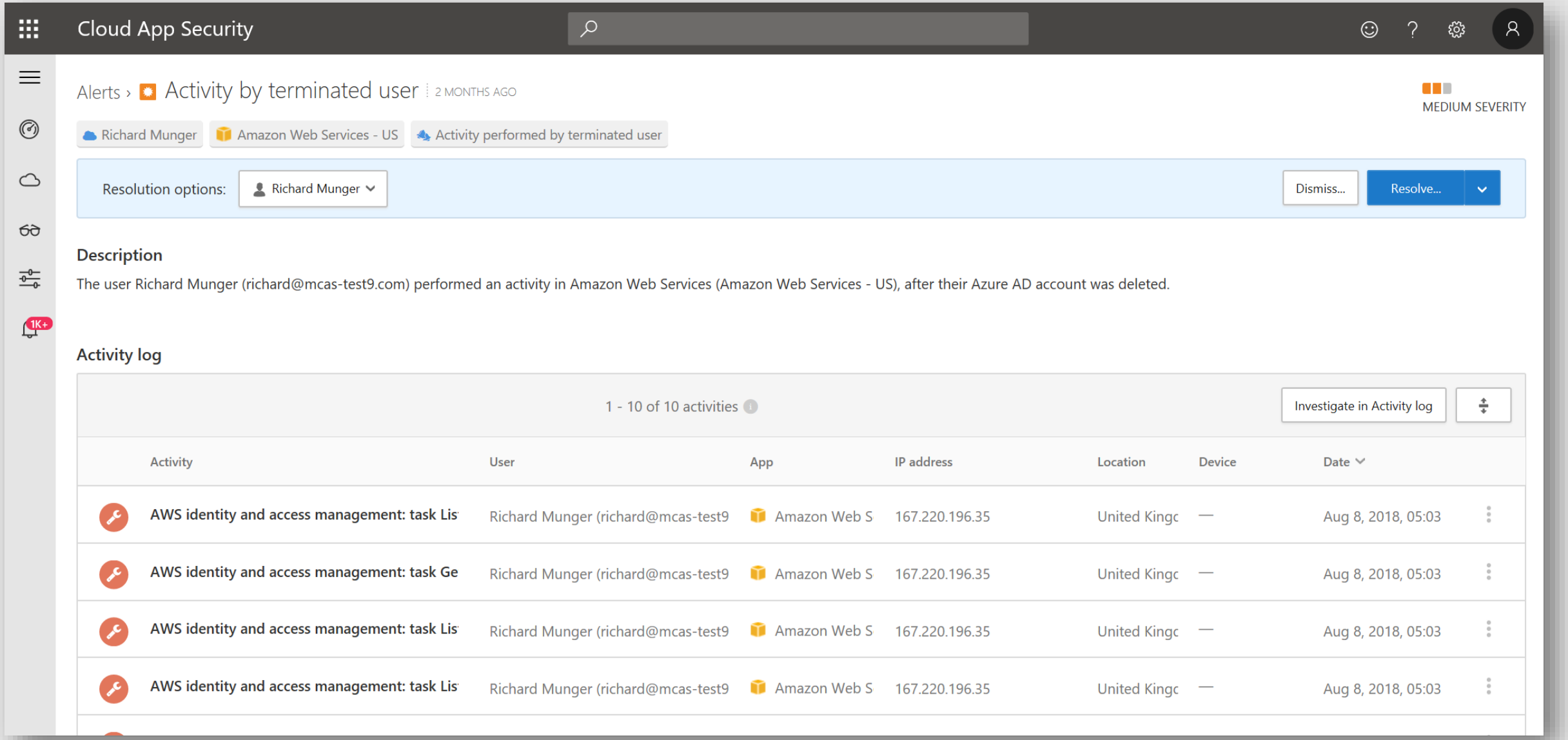
IP address actions

| | | | | | | |
|---|---|---|---|---|---|---|
| Run command: task New-JournalRule; Para... | Jane Doe | Microsoft Exc... | 94.242.62.254 | Russia | — | Sep 13, 2018, 10:... |
| Run command: task Remove-JournalRule; Pa... | Jane Doe | Microsoft Exc... | 94.242.62.254 | Russia | — | Sep 13, 2018, 10:... |

# Suspicious mailbox rules



# Activity by a terminated employee



Policy name

Shields up

Description

Alert if Jane Doe sets a journal rule

Policy severity

Low

Category

Threat detection

## Create filters for the policy

Act on:

- Single activity
  Every activity that matches the filters
- Repeated activity:
  Repeated activity by a single user

Edit and preview results

ACTIVITIES MATCHING ALL OF THE FOLLOWING

Activity type | equals | Set-JournalRule

## Alerts

Create alert Use your organization's default settings

Daily alert limit 5

Send alert as email

Send alert as text message

Save these alert settings as the default for your organization

## Governance

All apps - 1 selected

Notify user

CC additional users

exchangeadmin@securescoreteam.com

Suspend user
For Azure Active Directory users

Require user to sign in again
For Azure Active Directory users

Office 365

Suspend user

Require user to sign in again

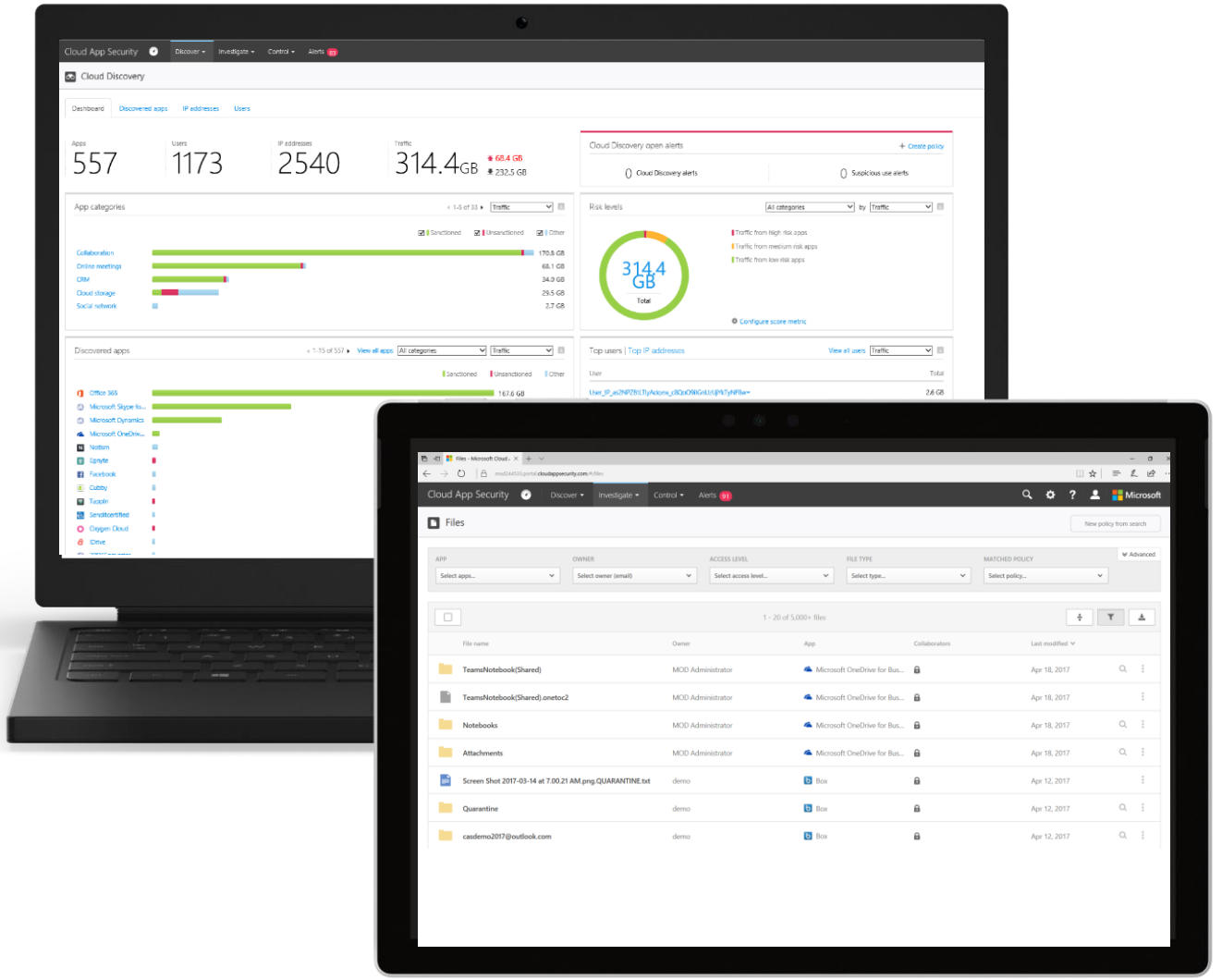
# MONITOR **CLOUD APP USAGE**

**Advanced incident investigation tools**
Investigate on users, file, activities, locations and managed apps, quantify exposure and risk

**Cloud data visibility**
Identify how data – both classified and not classified – is shared across cloud apps and identify risk

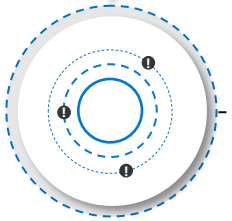
**Cloud app risk assessment**
Assess risk cloud apps based on ~60 security and compliance risk factors.

**On-going analytics & anomaly detection**
Get anomalous usage alerts, new app and trending apps alerts



# Microsoft Cloud App Security – Cross apps detections

Suspicious inbox rules (delete, forward)
Malware implanted in cloud apps
Malicious OAuth application
Multiple failed login attempts to app

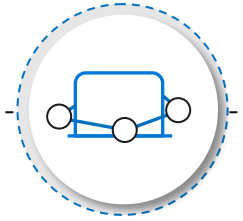


Threat delivery and persistence

Indicators of a compromised session

Activity from suspicious IP addresses
Activity from anonymous IP addresses
Activity from an infrequent country
Impossible travel between sessions
Logon attempt from a suspicious user agent

Unusual file share activity
Unusual file download
Unusual file deletion activity
Ransomware activity
Data exfiltration to unsanctioned apps
Activity by a terminated employee



Malicious use of an end-user account

Malicious use of a privileged user

Unusual impersonated activity
Unusual administrative activity
Unusual multiple delete VM activity

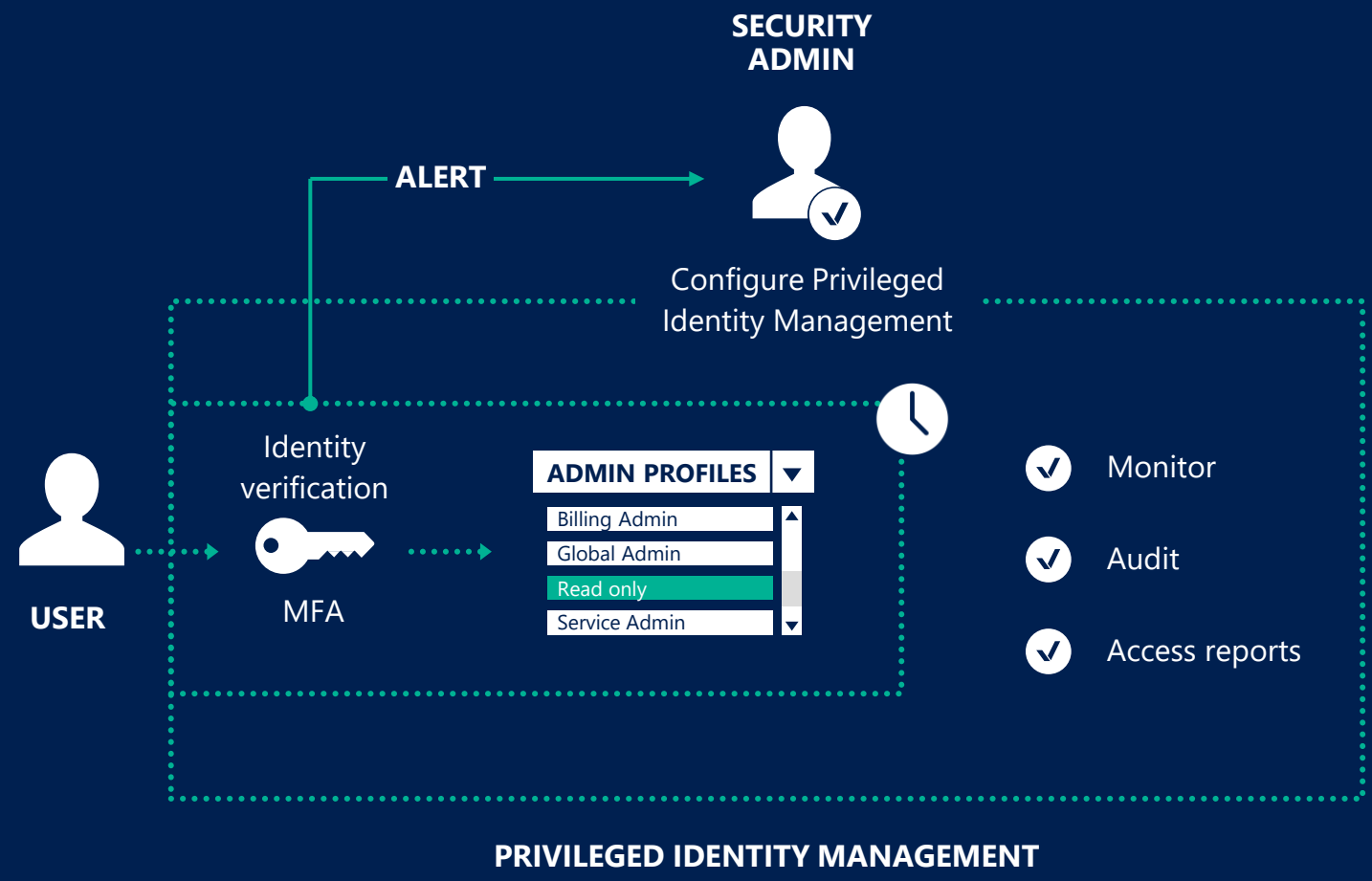
# DEMO

CLOUD-POWERED PROTECTION

# Privileged Identity Management

## How time-limited activation of privileged roles works

- Users need to activate their privileges to perform a task
- MFA is enforced during the activation process
- Alerts inform administrators about out-of-band changes
- Users will retain their privileges for a pre-configured amount of time
- Security admins can discover all privileged identities, view audit reports and review everyone who has is eligible to activate via access reviews

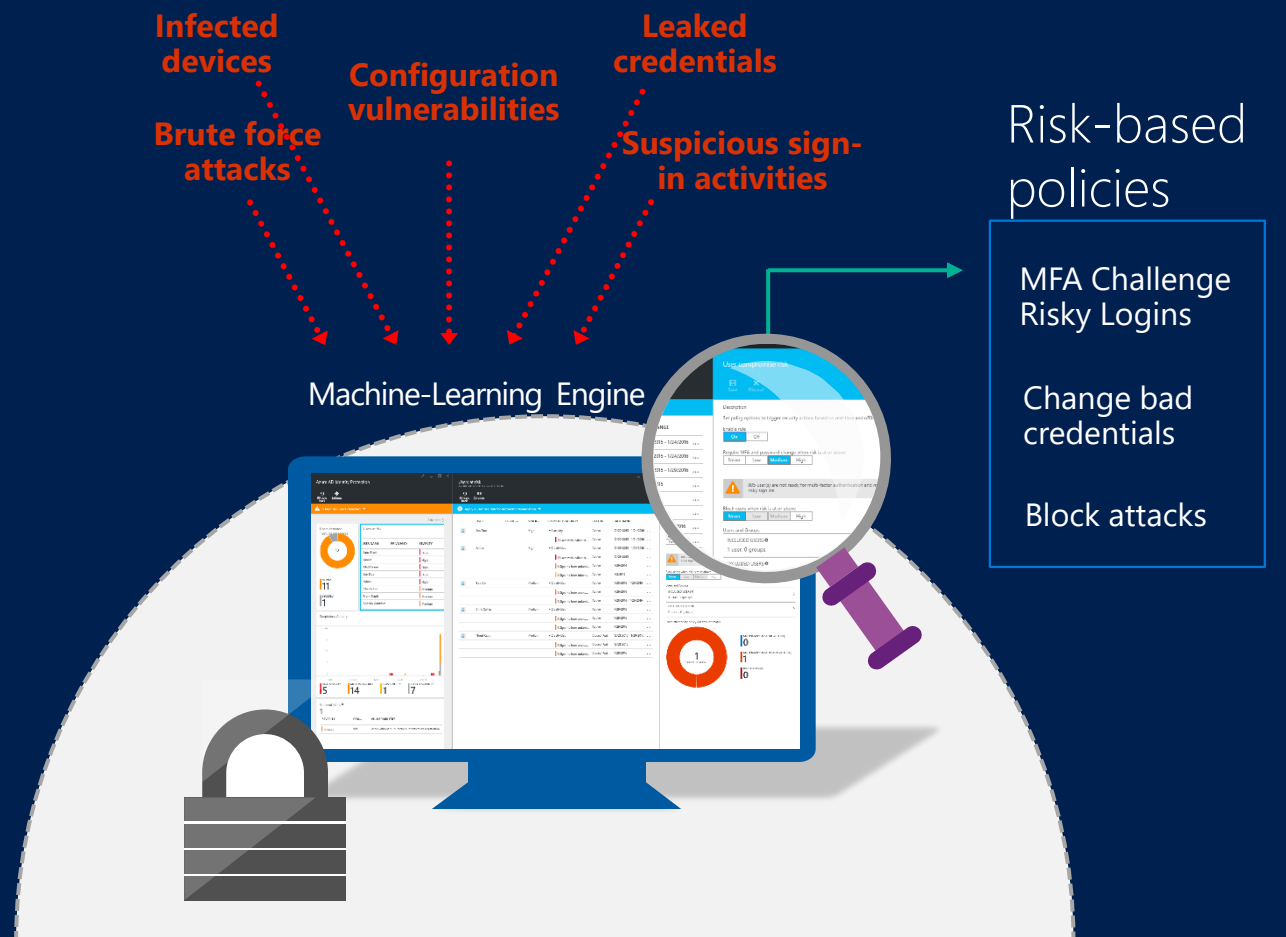


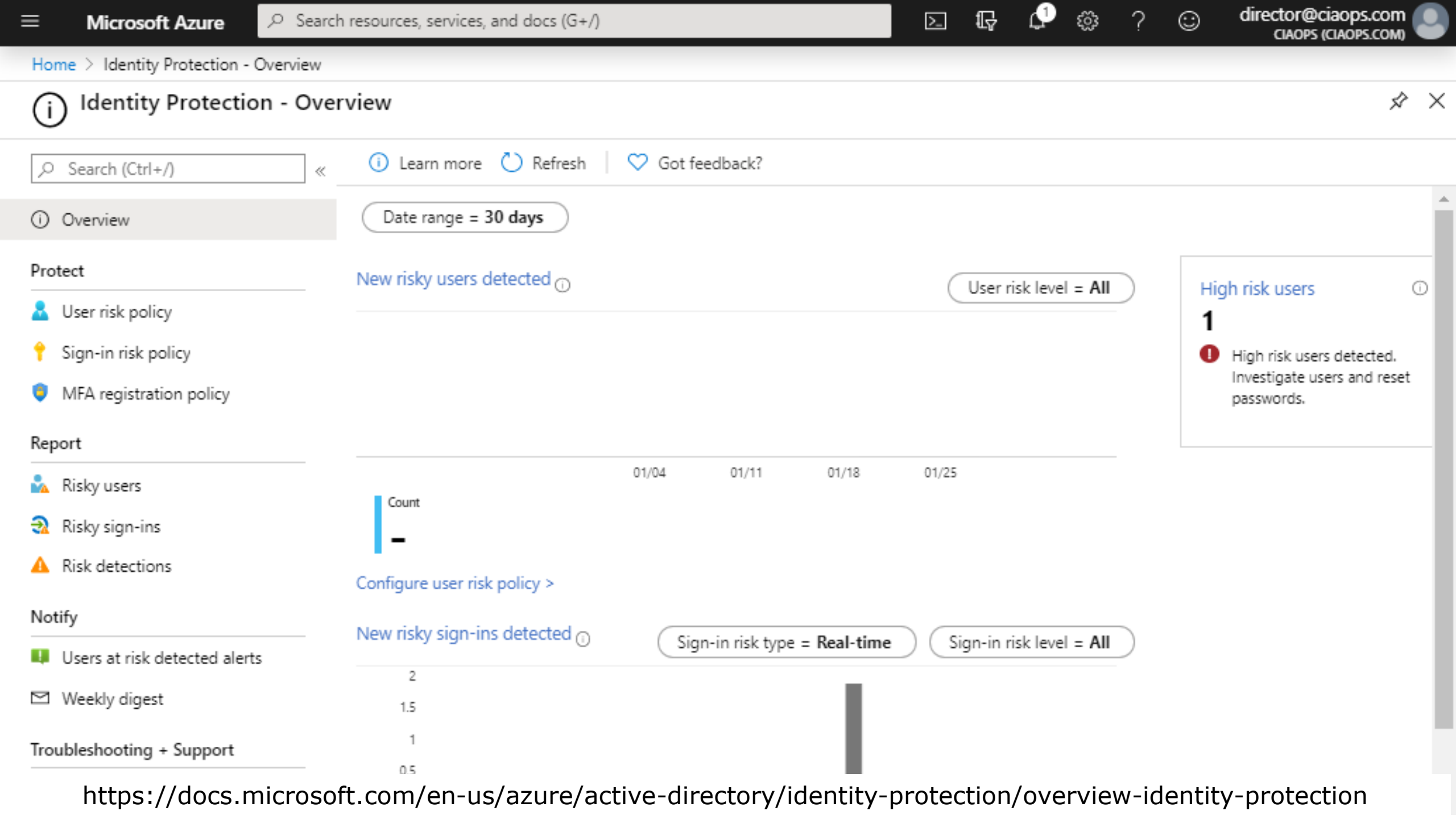
CLOUD-POWERED PROTECTION

# Azure Active Directory Identity Protection

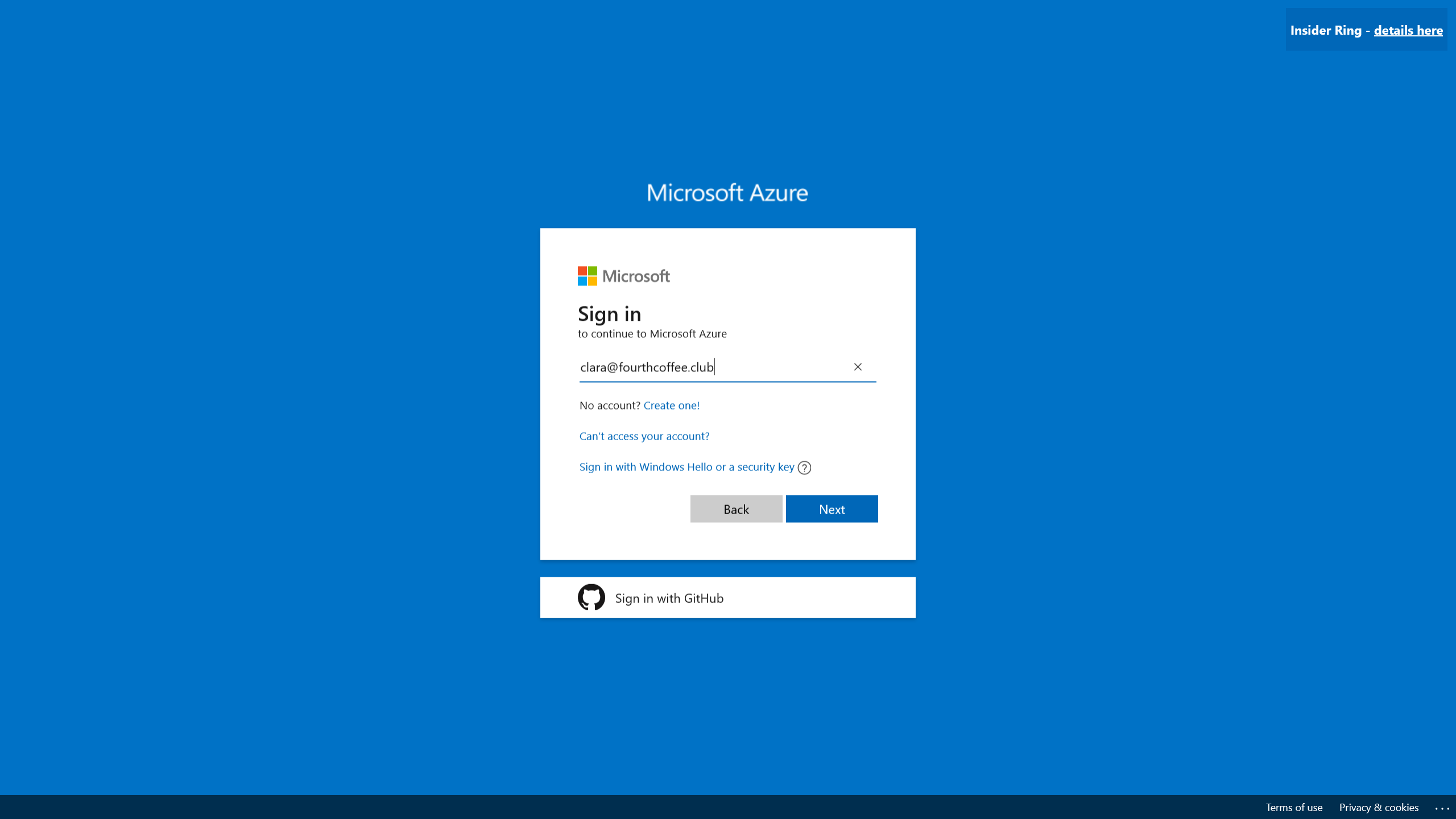
## Identity Protection at its best

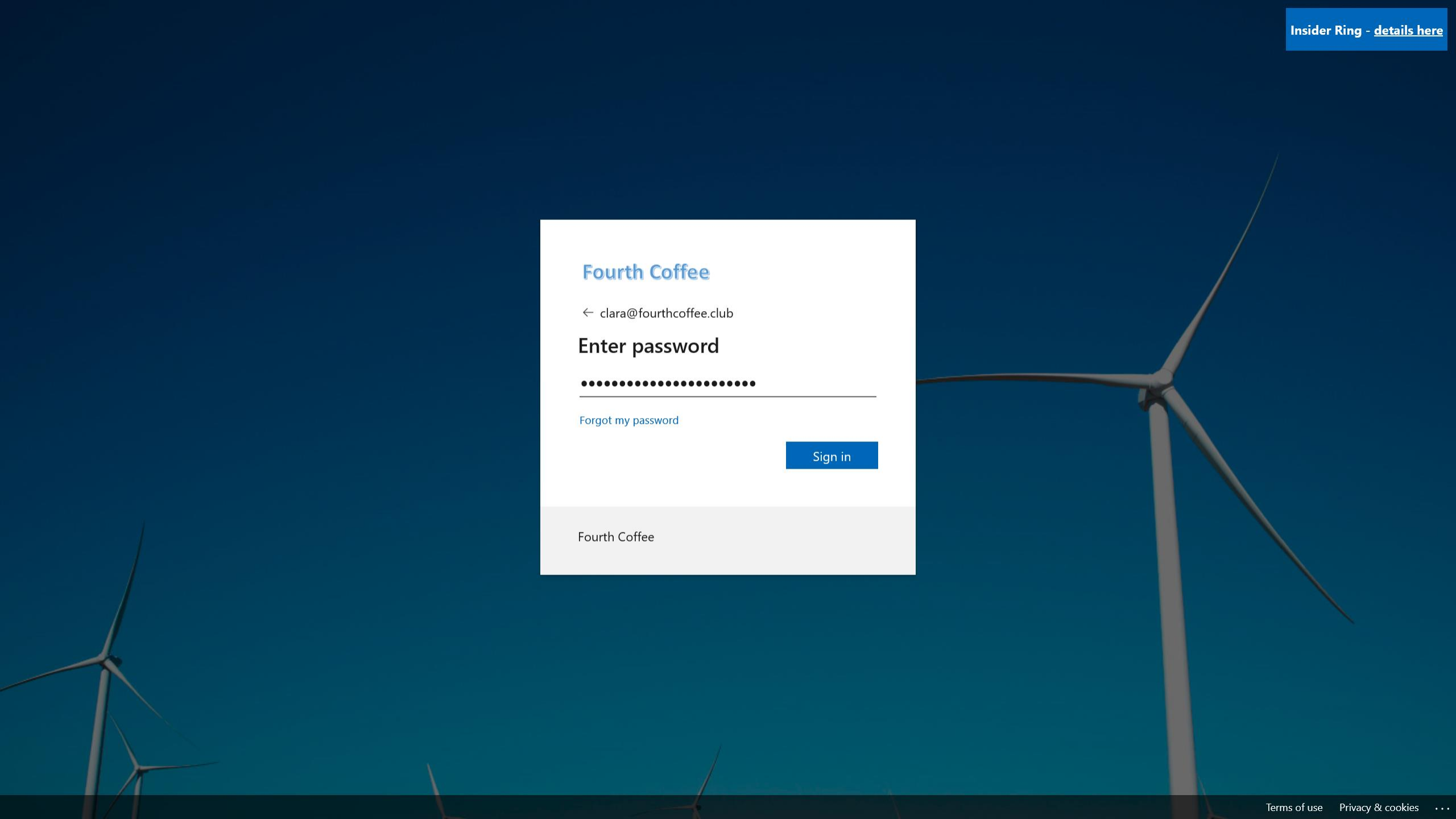
- Gain insights from a consolidated view of machine learning based threat detection
- Remediation recommendations
- Risk severity calculation
- Risk-based conditional access automatically protects against suspicious logins and compromised credentials

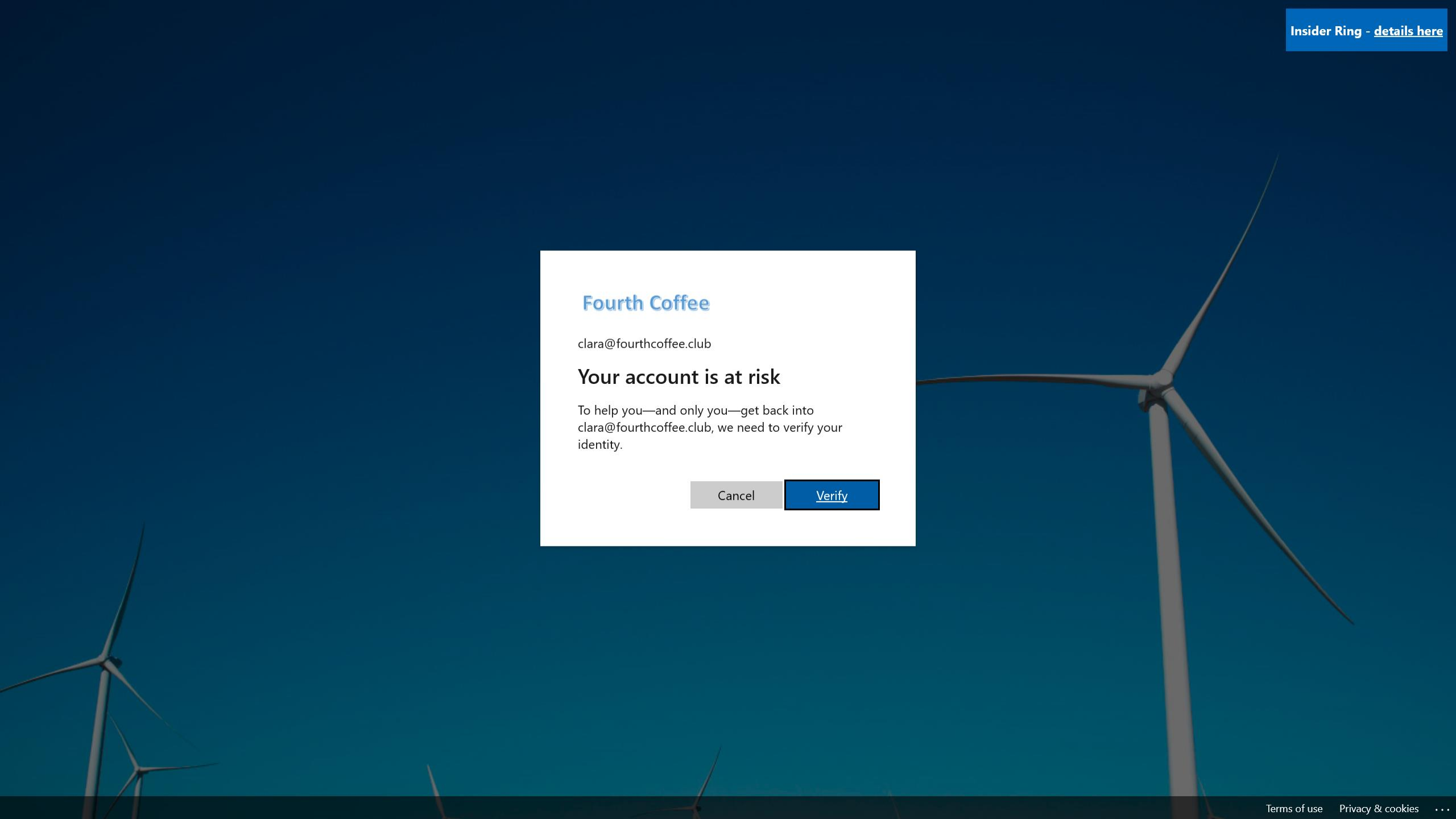


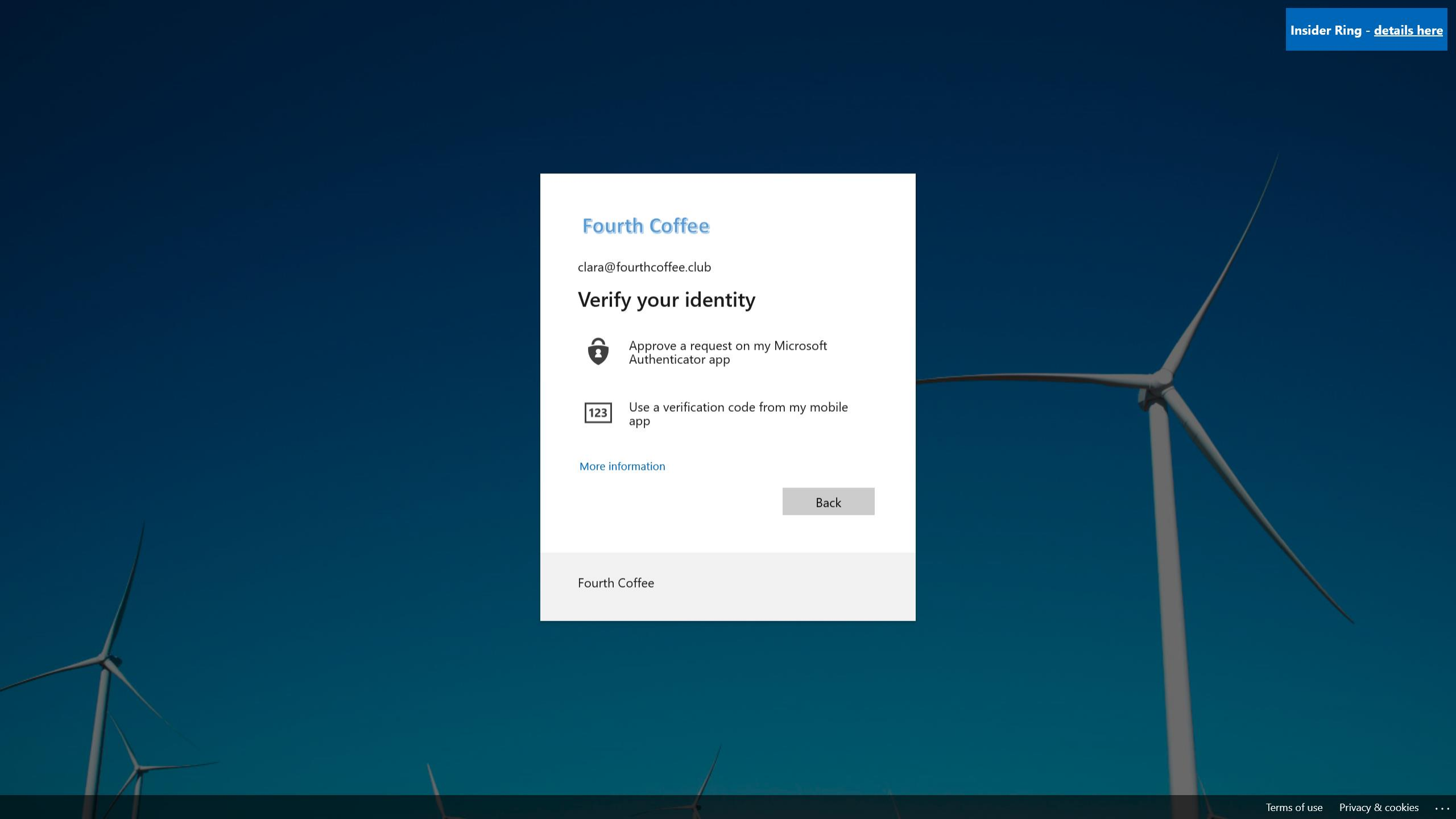


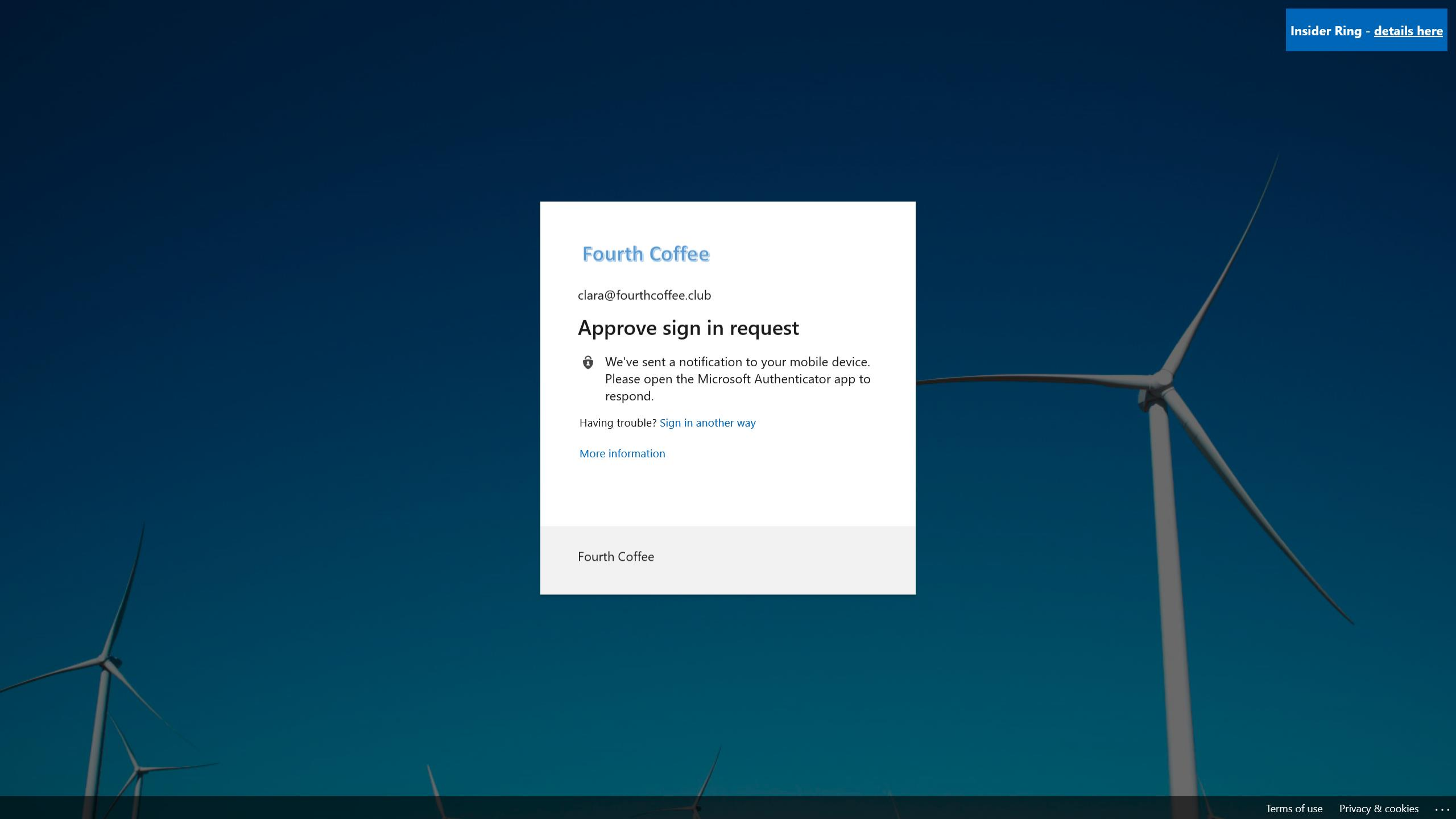

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

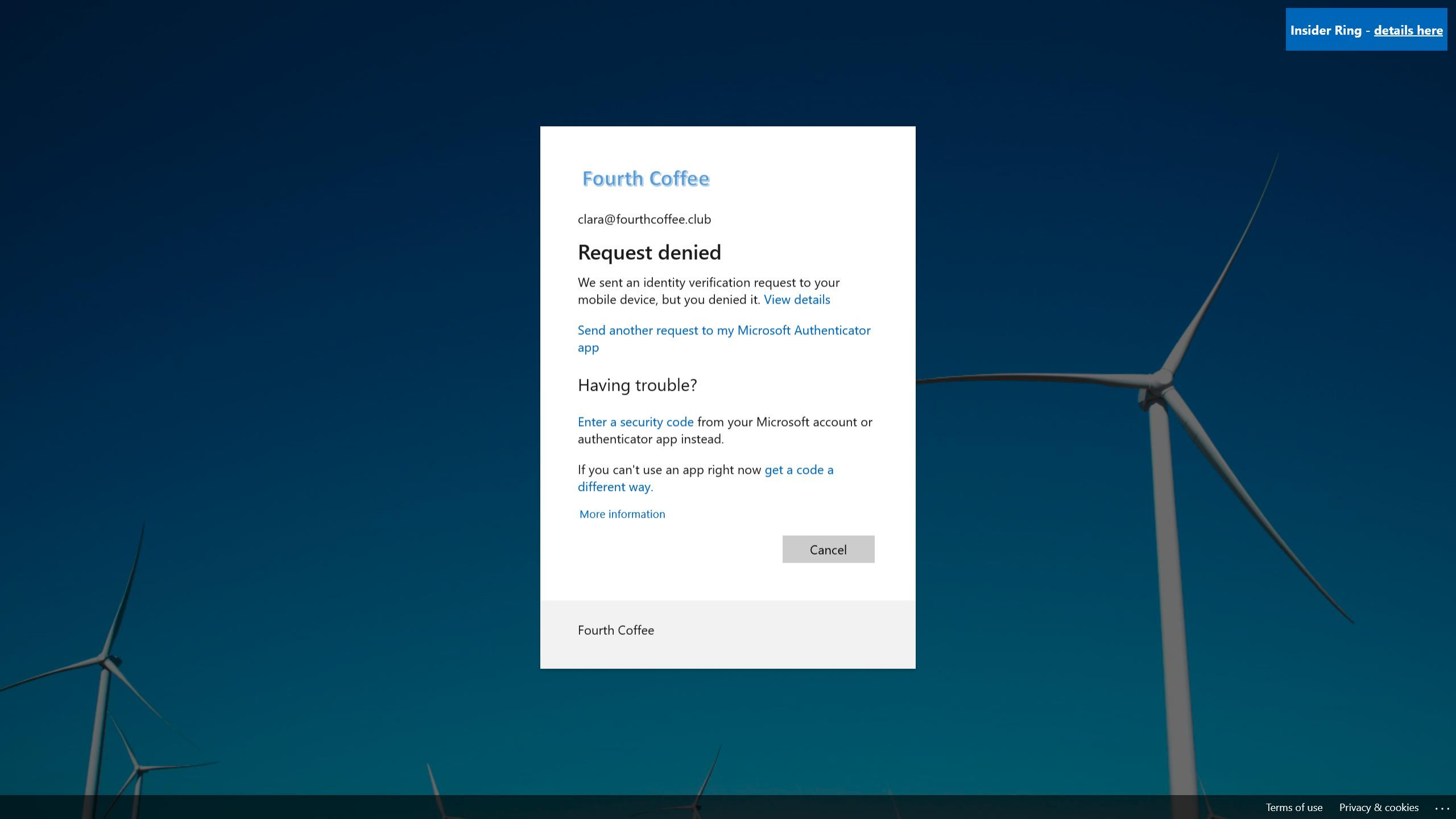

Insider Ring - details here
Microsoft Azure
Microsoft
Sign in
to continue to Microsoft Azure
clara@fourthcoffee.club
No account? Create one!
Can't access your account?
Sign in with Windows Hello or a security key
Back
Next
Sign in with GitHub
Terms of use
Privacy & cookies
...

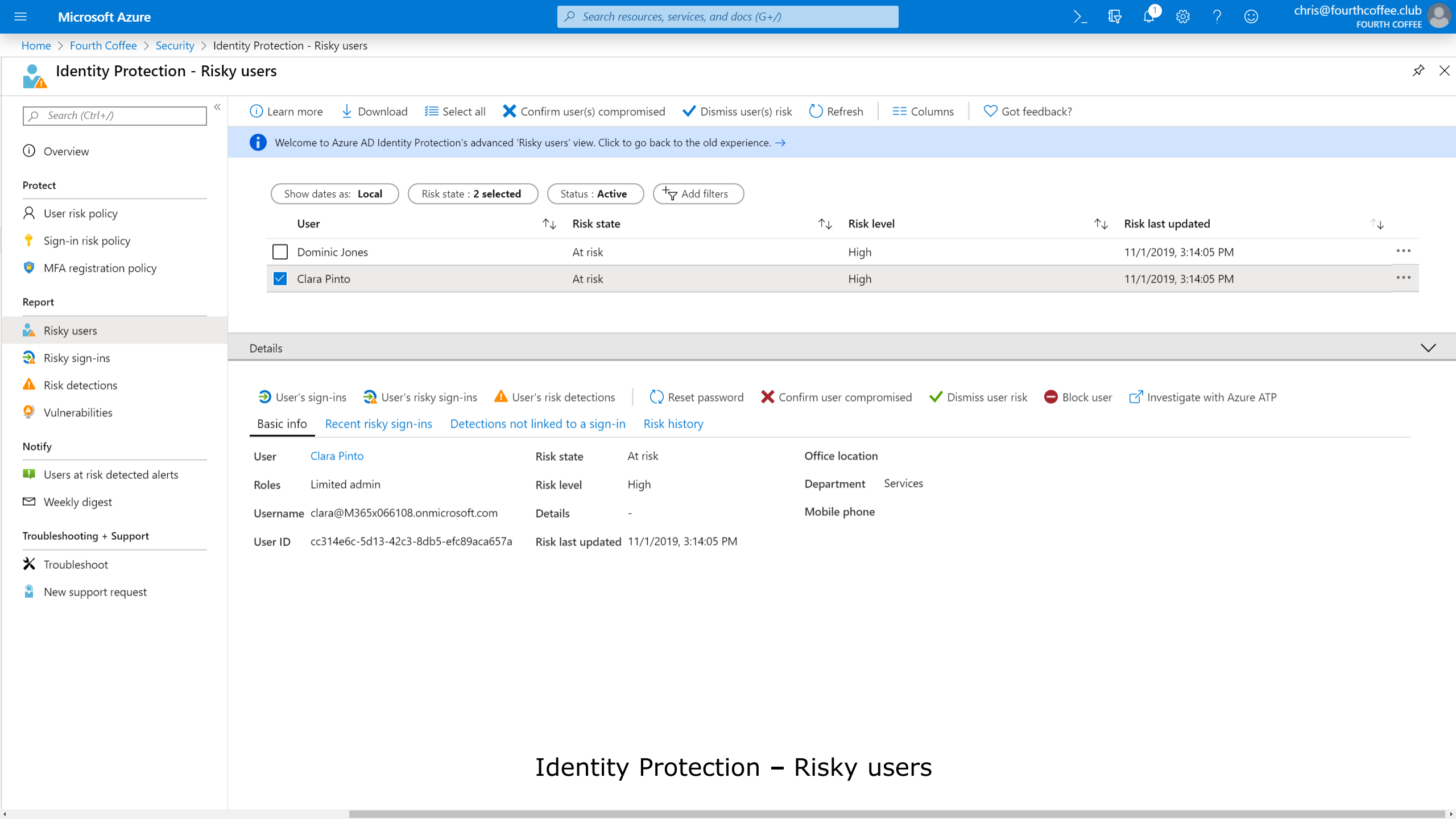

Insider Ring - details here
Fourth Coffee
clara@fourthcoffee.club
Enter password
Forgot my password
Sign in
Fourth Coffee
Terms of use
Privacy & cookies


Insider Ring - details here
Fourth Coffee
clara@fourthcoffee.club
Your account is at risk
To help you—and only you—get back into clara@fourthcoffee.club, we need to verify your identity.
Cancel
Verify
Terms of use
Privacy & cookies
...


Insider Ring - details here
Fourth Coffee
clara@fourthcoffee.club
Verify your identity
Approve a request on my Microsoft Authenticator app
123
Use a verification code from my mobile app
More information
Back
Fourth Coffee
Terms of use
Privacy & cookies
...


Insider Ring - details here
Fourth Coffee
clara@fourthcoffee.club
Approve sign in request
We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.
Having trouble? Sign in another way
More information
Fourth Coffee
Terms of use
Privacy & cookies
...


Insider Ring - details here
Fourth Coffee
clara@fourthcoffee.club
Request denied
We sent an identity verification request to your mobile device, but you denied it. View details
Send another request to my Microsoft Authenticator app
Having trouble?
Enter a security code from your Microsoft account or authenticator app instead.
If you can't use an app right now get a code a different way.
More information
Cancel
Fourth Coffee
Terms of use
Privacy & cookies
...




# Identity Protection – Risky users

# Identity Protection - Risky users

Search (Ctrl+/)
Overview
Protect
User risk policy
Sign-in risk policy
MFA registration policy
Report
Risky users
Risky sign-ins
Risk detections
Vulnerabilities
Notify
Users at risk detected alerts
Weekly digest
Troubleshooting + Support
Troubleshoot
New support request

Learn more | Download | Select all | Confirm user(s) compromised | Dismiss user(s) risk | Refresh | Columns | Got feedback?

Welcome to Azure AD Identity Protection's advanced 'Risky users' view. Click to go back to the old experience. →

Show dates as: **Local** | Risk state : **2 selected** | Status : **Active** | Add filters

| User | Risk state | Risk level | Risk last updated |
|---|---|---|---|
| Dominic Jones | At risk | High | 11/1/2019, 3:14:05 PM |
| Clara Pinto | At risk | High | 11/1/2019, 3:14:05 PM |

Details

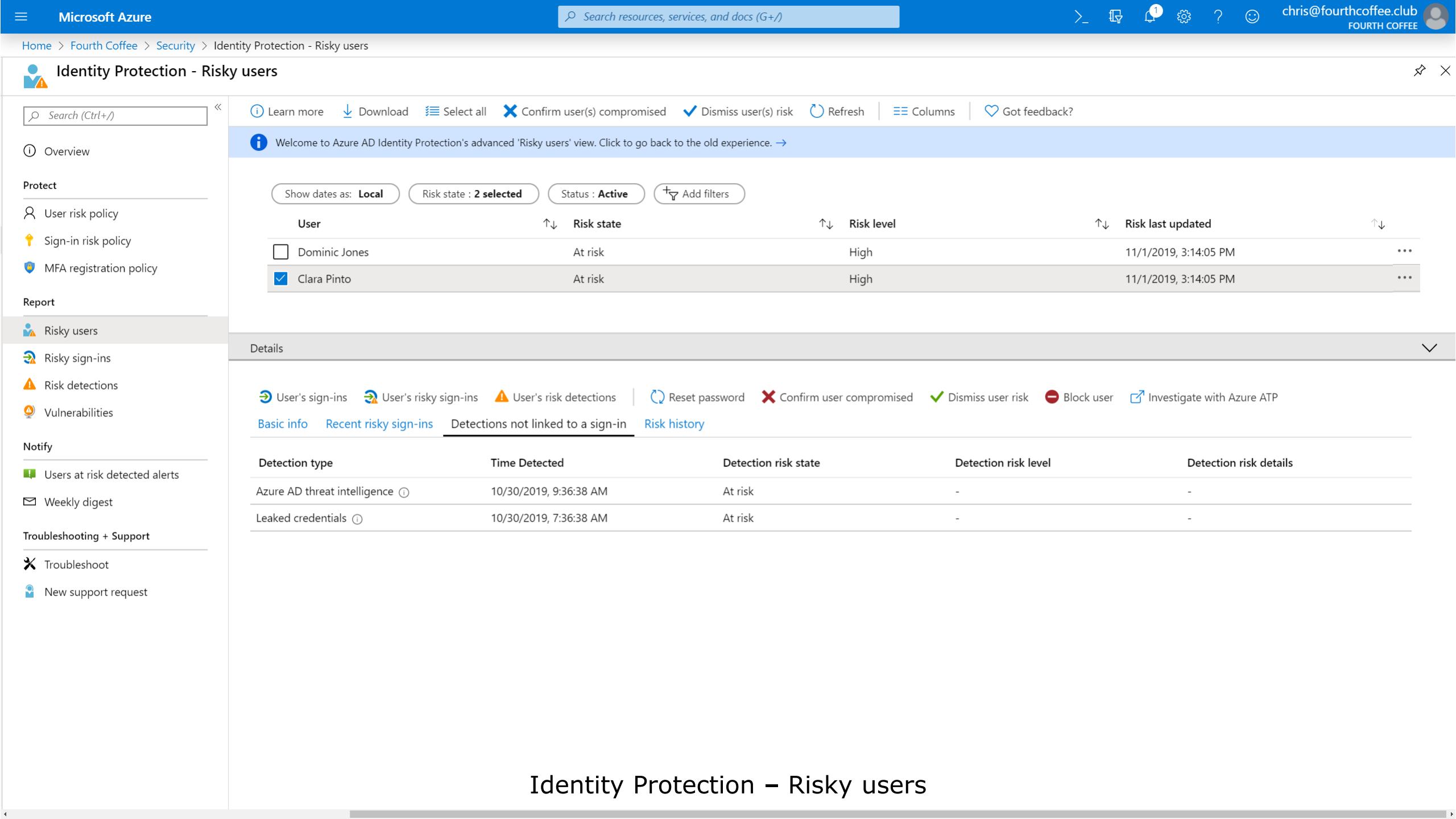
User's sign-ins | User's risky sign-ins | User's risk detections | Reset password | Confirm user compromised | Dismiss user risk | Block user | Investigate with Azure ATP

Basic info | Recent risky sign-ins | Detections not linked to a sign-in | Risk history

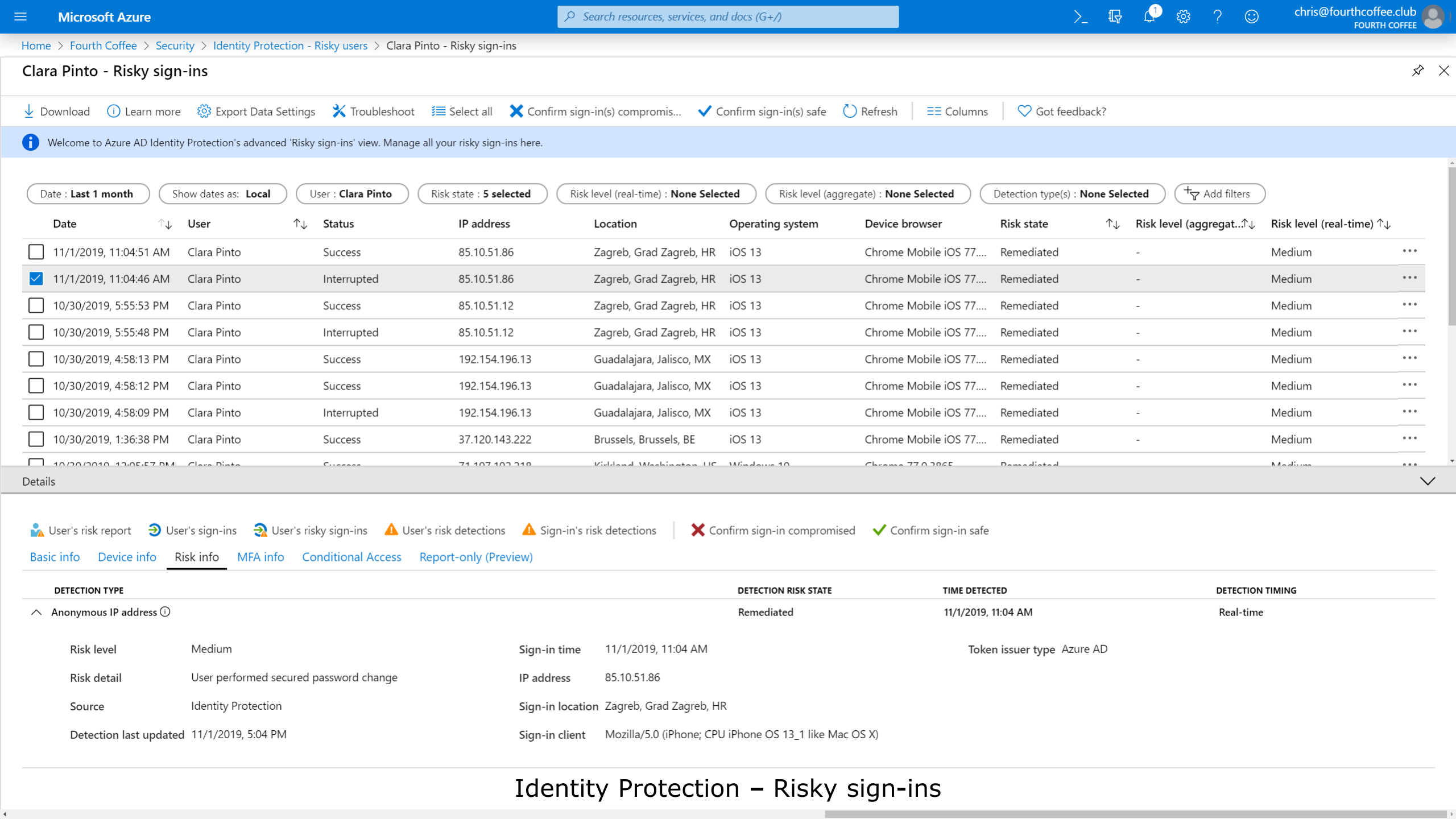
| Application | Status | Date | IP address | Location | Risk state | Risk level (aggregate) | Risk level (real-time) | Conditional access |
|---|---|---|---|---|---|---|---|---|
| Azure Portal | Success | 11/1/2019, 11:04:51 AM | 85.10.51.86 | Zagreb, Grad Zagreb, ... | Confirmed compromis... | High | Medium | Not Applied |
| Azure Portal | Interrupted | 11/1/2019, 11:04:46 AM | 85.10.51.86 | Zagreb, Grad Zagreb, ... | At risk | Low | Medium | Not Applied |
| Azure Portal | Success | 10/30/2019, 5:55:53 PM | 85.10.51.12 | Zagreb, Grad Zagreb, ... | At risk | Medium | Medium | Not Applied |
| Azure Portal | Interrupted | 10/30/2019, 5:55:48 PM | 85.10.51.12 | Zagreb, Grad Zagreb, ... | At risk | High | Medium | Not Applied |
| Azure Portal | Success | 10/30/2019, 4:58:13 PM | 192.154.196.13 | Guadalajara, Jalisco, MX | At risk | Medium | Medium | Not Applied |
| Azure Portal | Success | 10/30/2019, 4:58:12 PM | 192.154.196.13 | Guadalajara, Jalisco, MX | At risk | Medium | Medium | Not Applied |
| Azure Portal | Interrupted | 10/30/2019, 4:58:09 PM | 192.154.196.13 | Guadalajara, Jalisco, MX | At risk | Medium | Medium | Not Applied |
| Azure Portal | Success | 10/30/2019, 1:36:38 PM | 37.120.143.222 | Brussels, Brussels, BE | At risk | High | Medium | Not Applied |
| Azure Portal | Success | 10/30/2019, 12:05:57 P... | 71.197.192.218 | Kirkland, Washington, ... | At risk | Medium | Medium | Not Applied |
| Azure Portal | Success | 10/30/2019, 12:03:27 P... | 71.197.192.218 | Kirkland, Washington, ... | At risk | Low | - | Not Applied |

Users can have detections on sign-ins that are currently not supported in the Sign-ins report. Such risky sign-ins do not appear here. To see all the detections in the last 90 days, please go to the 'Risk history' tab.

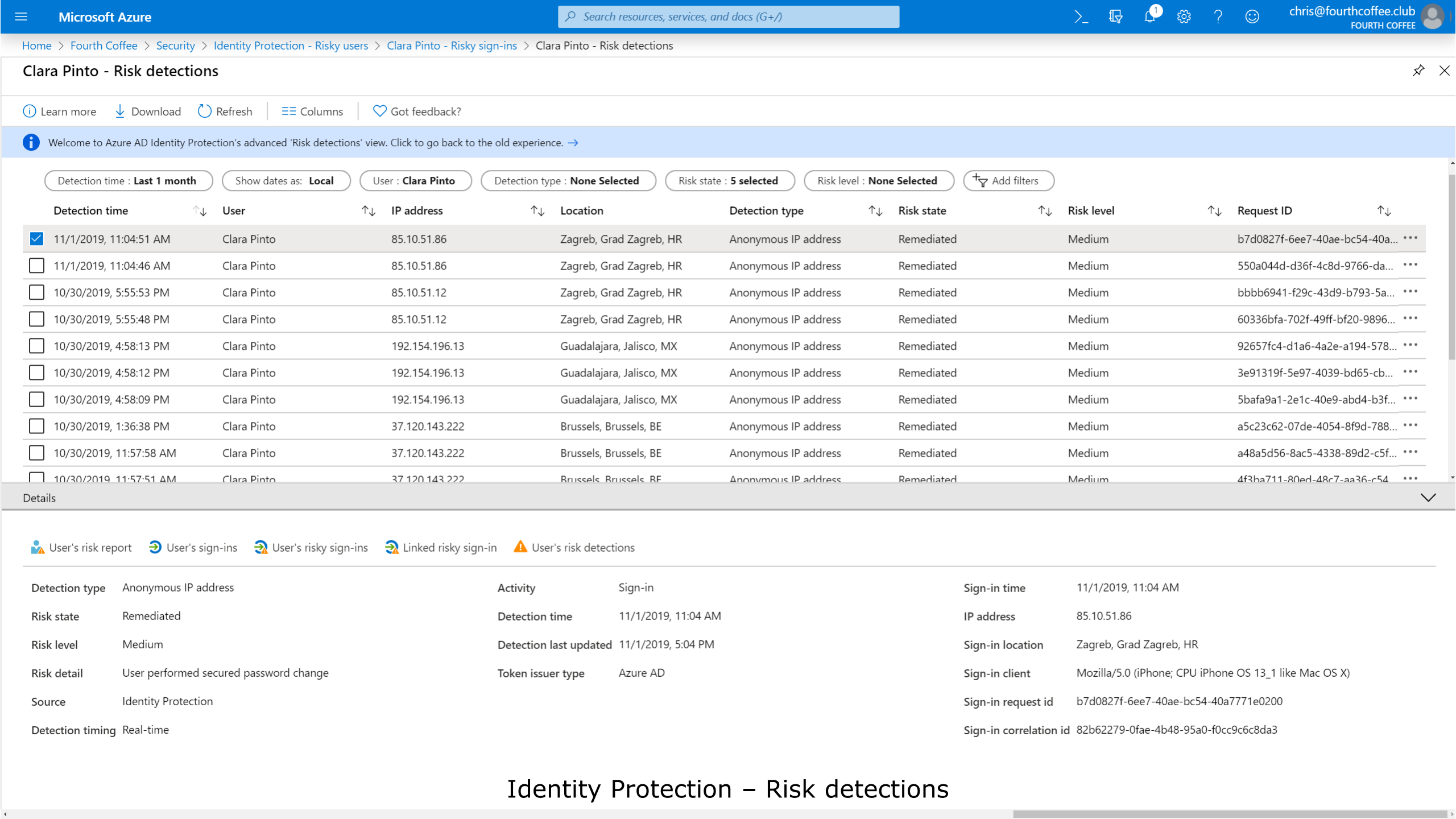
Identity Protection – Risky users




Identity Protection – Risky users

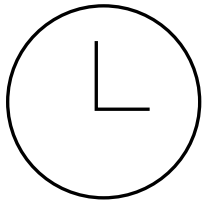



# Identity Protection – Risky sign-ins



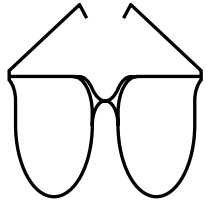

# Identity Protection – Risk detections

# Privileged Identity Management

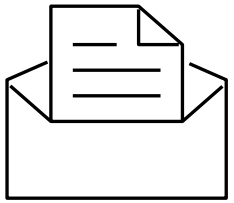


Privileged role membership only granted for a limited amount of time

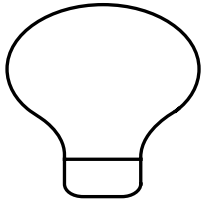
Roles can be configured to require staff to perform MFA prior to elevation of privilege



Roles can be granted automatically or after review by one or more approvers



All role requests for and role approvals are automatically recorded in logs or by email



Almost all roles should be managed by PIM, with a “break glass” permanent account for critical roles just in case

Microsoft Azure | Search resources, services, and docs (G+/) | director@ciaops.com CIAOPS (CIAOPS.COM)

Home > Privileged Identity Management - Quick start

# Privileged Identity Management - Quick start

Privileged Identity Management

- Quick start
- Consent to PIM

**Tasks**

- My roles
- My requests
- Approve requests
- Review access

**Manage**

- Azure AD roles
- Azure AD custom roles (Prev...
- Azure resources

**Activity**

- My audit history

**Troubleshooting + Support**

What's new | Get started

## Manage your privileged access

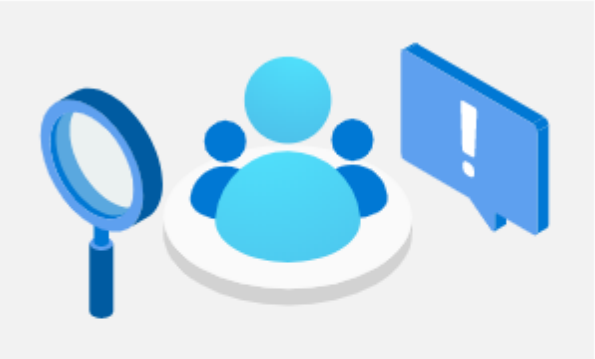
Use Privileged Identity Management to manage the lifecycle of role assignments, enforce just-in-time access policy, and discover who has what roles. Learn more

### Manage access

Users with excessive access are vulnerable in the event of account compromise. Ensure your organization manages to least privilege by periodically reviewing, renewing, or extending

### Activate just in time

Reduce the potential for lateral movement in the event of account compromise by eliminating persistent access to privileged roles and resources. Enforce just in time access to critical



### Discover and monitor

It is common for access to critical resources to go undetected. Ensure you know who has access to what, and receive notifications when new assignments are granted to accounts in your

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

## Global Administrator
Role activation details

Activate | Deactivate

Verify your identity before proceeding →

NAME
Vance Brown

EMAIL
vance@fourthcoffee.club

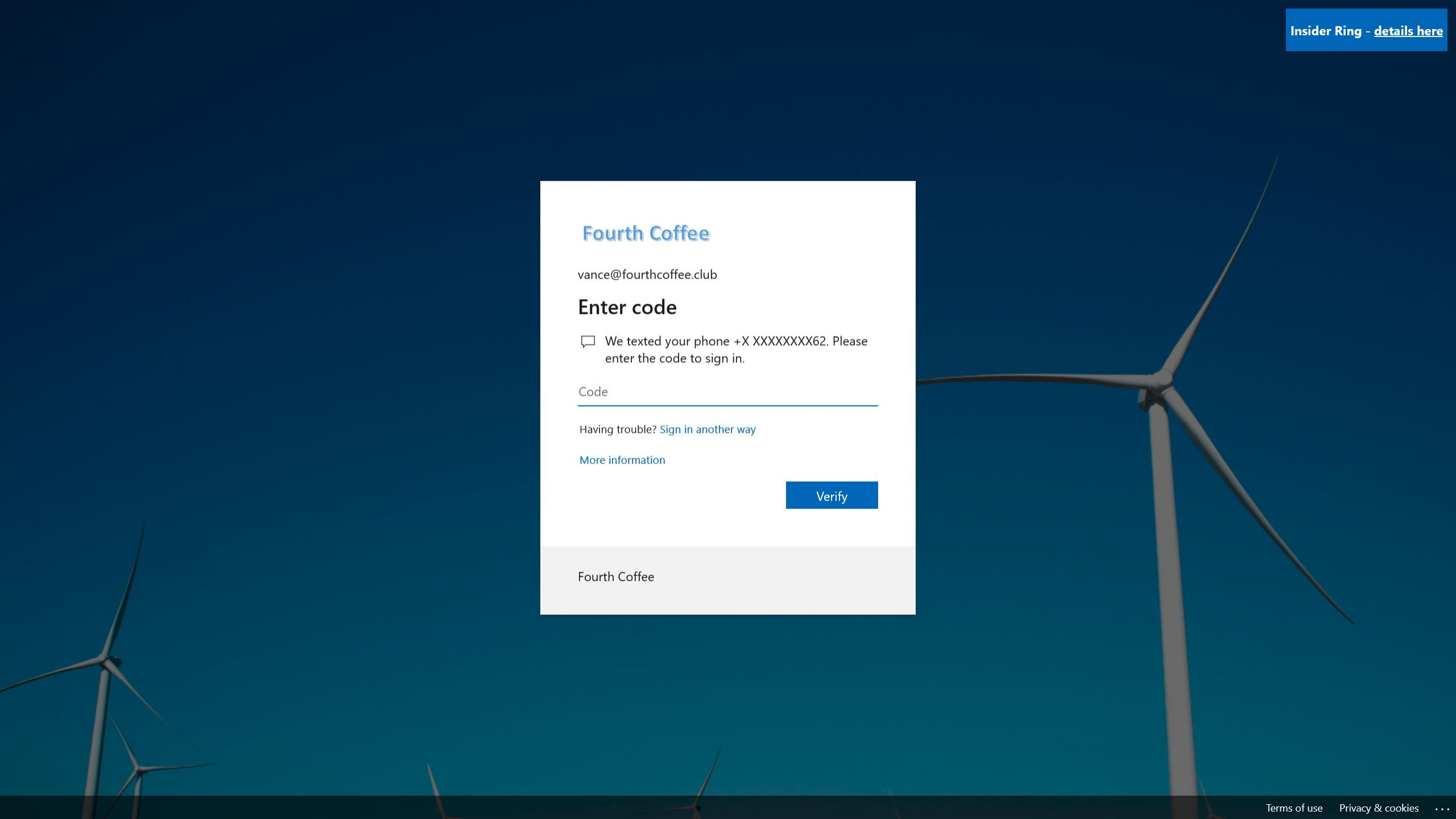
ACTIVATION
Eligible

EXPIRATION
-

## Verify my identity
Global Administrator

Before you activate this role, verify your identity with Azure Multi-Factor Authentication. If you haven't registered with Azure MFA yet, we'll help you do that.

Verify my identity


Insider Ring - details here
Fourth Coffee
vance@fourthcoffee.club
Enter code
We texted your phone +X XXXXXXXX62. Please enter the code to sign in.
Code
Having trouble? Sign in another way
More information
Verify
Fourth Coffee
Terms of use
Privacy & cookies
...

# Global Administrator

Role activation details

Activate | Deactivate

NAME
Vance Brown

EMAIL
vance@fourthcoffee.club

ACTIVATION
Eligible

EXPIRATION
-

# Activation

Role activation details

Custom activation start time

**Activation duration (hours)**

1

**Ticket number** *

85739

**Ticket system**

ServiceNow

**Activation reason (max 500 characters)** *

I need to access a privileged app for CAPN project.

Activate

## Activation
Role activation details

Custom activation start time

Activation duration (hours)
1

Ticket number * ⓘ
85739

Ticket system
ServiceNow

Activation reason (max 500 characters) *
I need to access a privileged app for CAPN project.

Activate

## Activation status

**Stage 1**
Processing your request and activating your role.

**Stage 2**
Validating that your activation is successful.

**Stage 3**
Activation complete, use the link below to sign out and log back in to start using your newly activated role.

Sign out

## Activation
Role activation details

Custom activation start time

Activation duration (hours)

1

Ticket number * ⓘ

85739

Ticket system

ServiceNow

Activation reason (max 500 characters) *

I need to access a privileged app for CAPN project.

Activate

## Activation status

**Stage 1**
Processing your request and activating your role.

**Stage 2**
Validating that your activation is successful.

**Stage 3**
Activation complete, use the link below to sign out and log back in to start using your newly activated role.

Sign out

## Activation
Role activation details

Custom activation start time

Activation duration (hours)
1

Ticket number * ⓘ
85739

Ticket system
ServiceNow

Activation reason (max 500 characters) *
I need to access a privileged app for CAPN project.

Activate

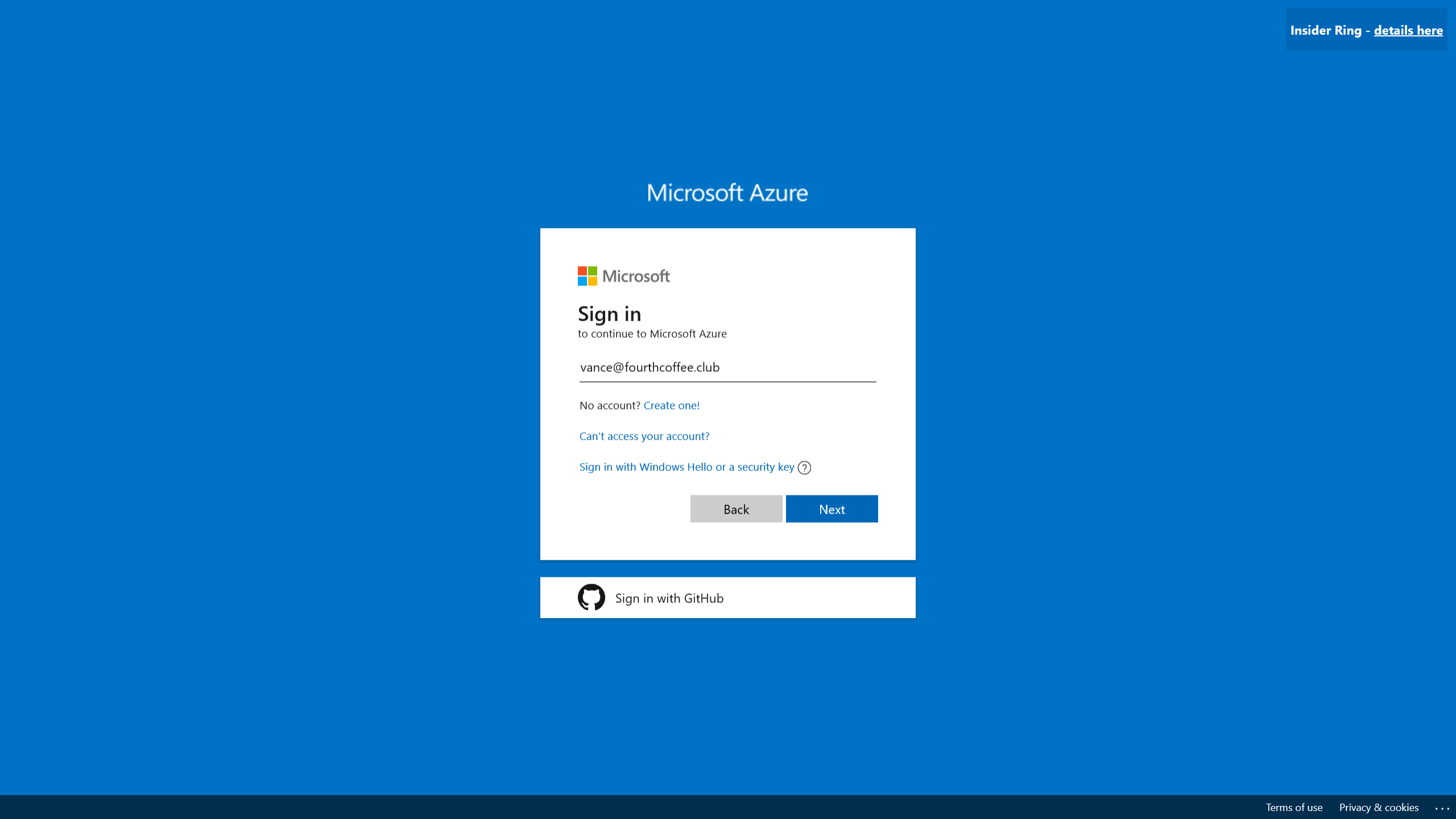
## Activation status

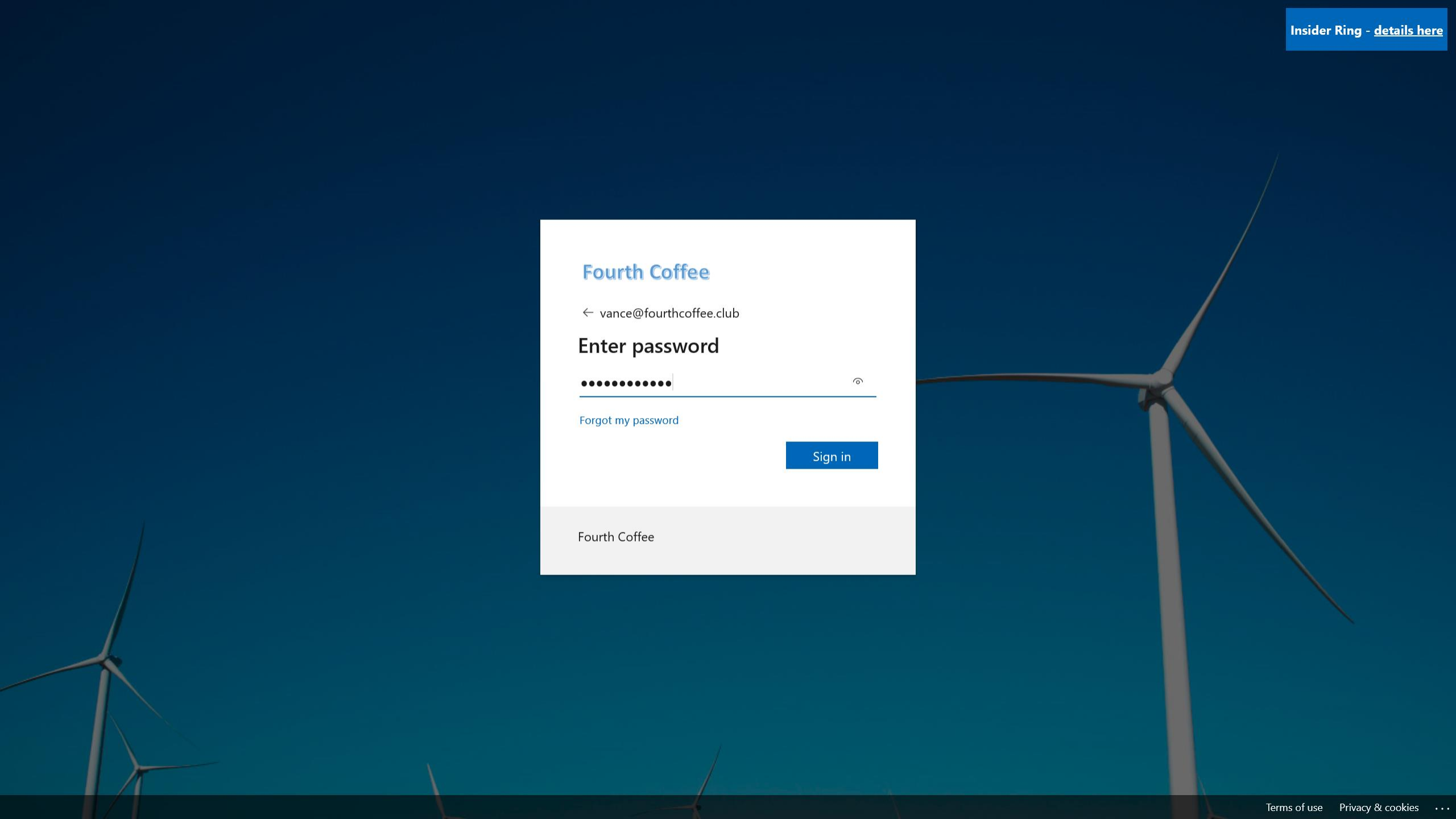
**Stage 1**
Processing your request and activating your role.

**Stage 2**
Validating that your activation is successful.

**Stage 3**
Activation complete, use the link below to sign out and log back in to start using your newly activated role.

Sign out


Insider Ring - details here
Microsoft Azure
Microsoft
Sign in
to continue to Microsoft Azure
vance@fourthcoffee.club
No account? Create one!
Can't access your account?
Sign in with Windows Hello or a security key
Back
Next
Sign in with GitHub
Terms of use
Privacy & cookies
...


Insider Ring - details here
Fourth Coffee
vance@fourthcoffee.club
Enter password
Forgot my password
Sign in
Fourth Coffee
Terms of use
Privacy & cookies

# Demo