



# CSP Masters Program in person series

## Technical training

# Detect & Respond: Cloud App Security

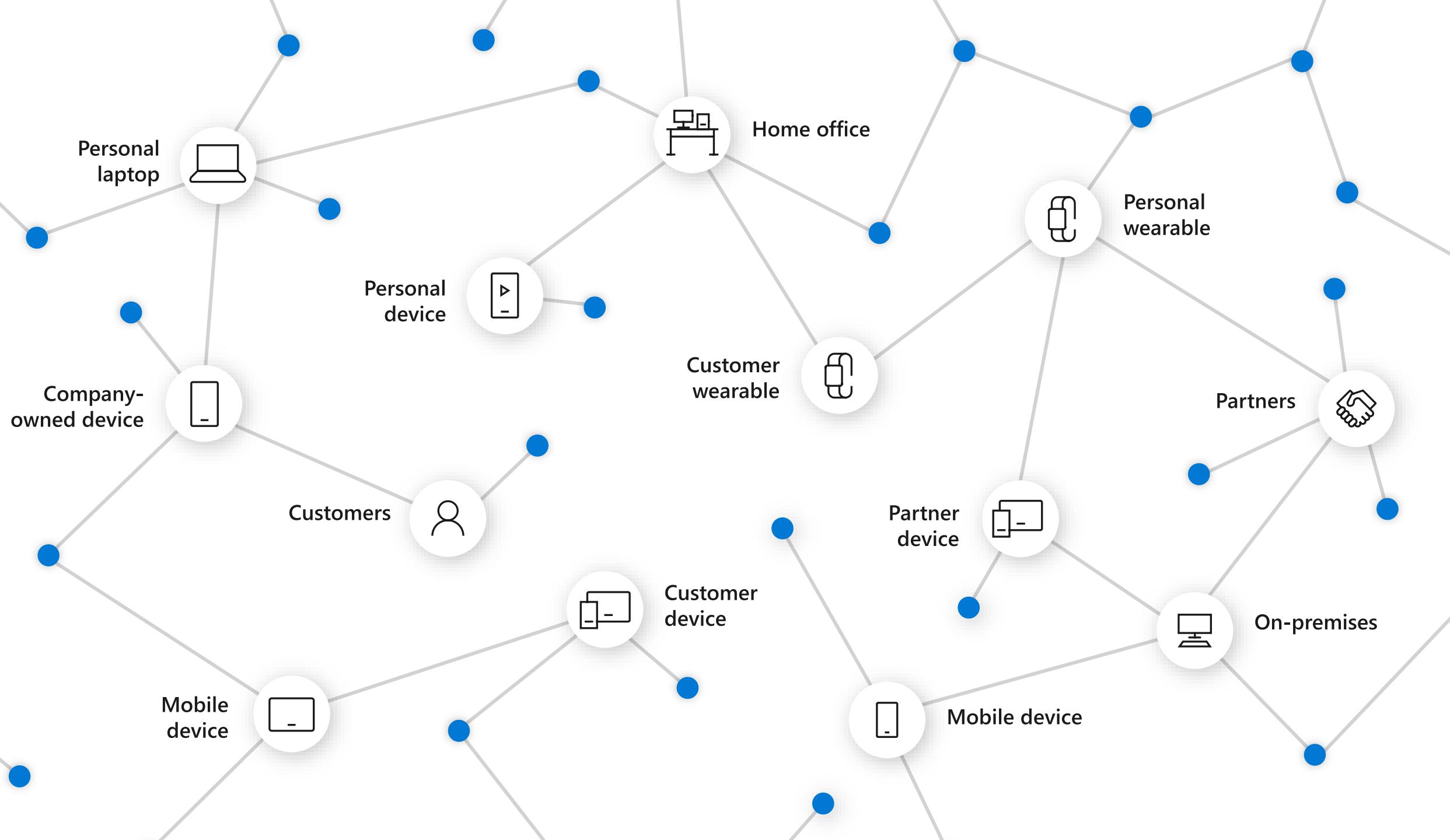


## Defender for Cloud Apps

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

The screenshot shows the 'Policy templates' section of the Microsoft Cloud App Security interface. It includes a search bar and filters for Type, Severity, Name, and Category. A table lists 17 templates, each with a preview, severity level (red), linked policies (0), and publish date (Sep 17, 2017, 2:05 AM). Each row also has a '+' button.

Template	Severity	Linked policies	Published
New popular app Alert when new apps are discovered that are used by more than 500 users.	High (3 red)	0	Sep 17, 2017, 2:05 AM
Multiple failed user log on attempts to an app Alert when a single user attempts to log on to a single app, and fails more than 10 times within 5 minutes.	High (3 red)	0	Sep 17, 2017, 2:05 AM
General anomaly detection Alert when an anomalous session is detected in one of the sanctioned apps, such as: impossible travel, log on pattern, inactive account.	High (3 red)	0	Sep 17, 2017, 2:05 AM
New high upload volume app Alert when new apps are discovered whose total daily upload traffic is more than 500 MB.	High (3 red)	0	Sep 17, 2017, 2:05 AM
Mass download by a single user Alert when a single user performs more than 50 downloads within 1 minute.	High (3 red)	0	Sep 17, 2017, 2:05 AM
New high volume app Alert when new apps are discovered that have total daily traffic of more than 500 MB.	High (3 red)	0	Sep 17, 2017, 2:05 AM
Logon from a risky IP address Alert when a user logs on to your sanctioned apps from a risky IP address. By default, the Risky IP	High (3 red)	0	Sep 17, 2017, 2:05 AM



# User and entity behavioral analytics

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

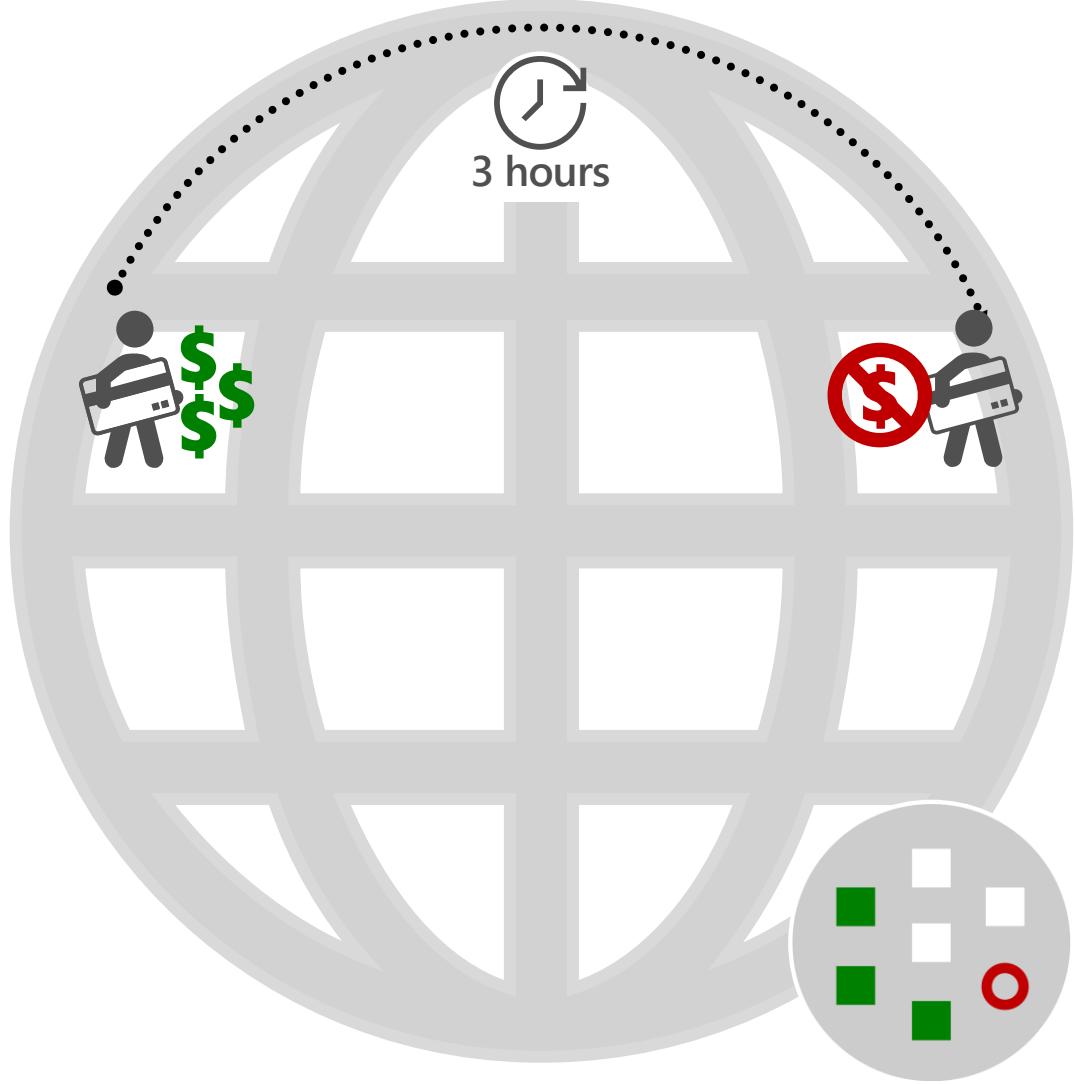
Profiles behavior and detects anomalies by using **machine learning** algorithms

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

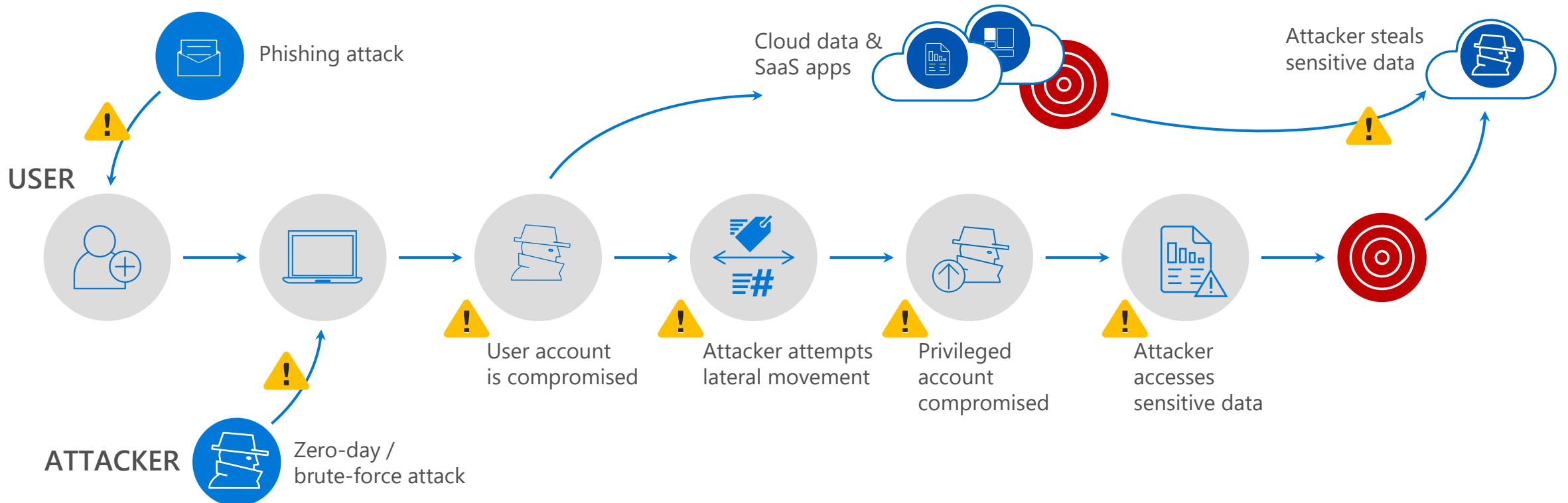
Credit card companies monitor cardholders' behavior.

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

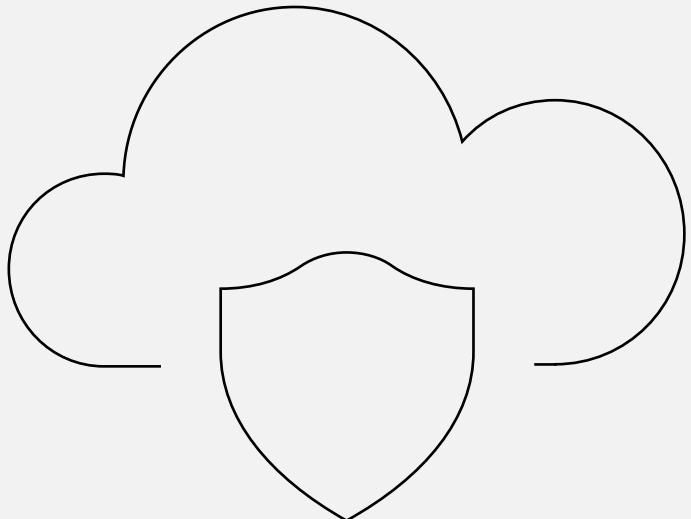
! Unfamiliar sign-in location

! 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

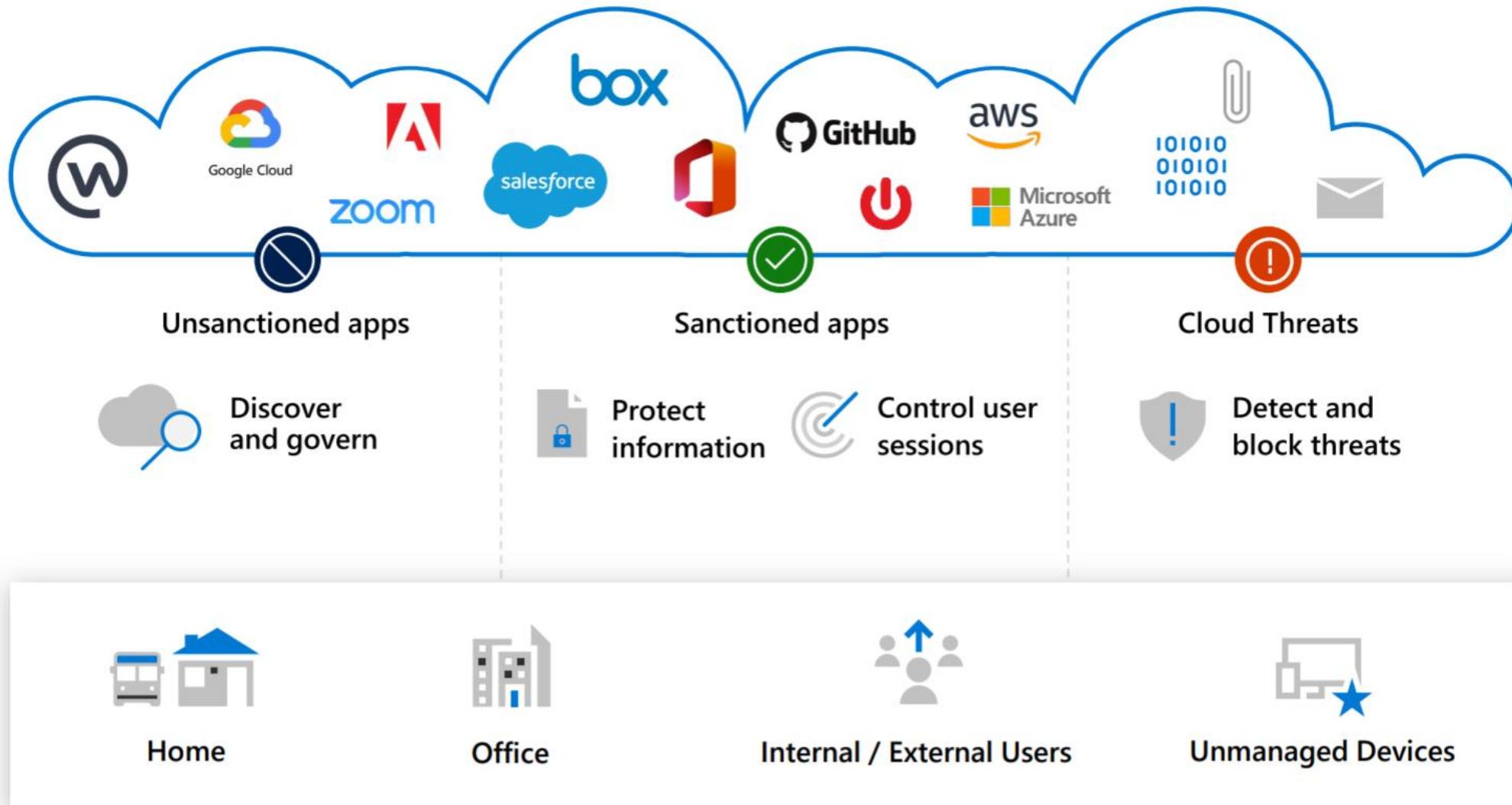
Raise alerts on user or file behavior anomalies in cloud apps leveraging their API connectors

### 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



# 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



**16,000+ supported apps**

Office 365



zoom



servicenow

aws  
Amazon Web Services

box



Okta



Power BI



CONCUR

Microsoft Azure

slack



Tableau



zendesk



Microsoft Dynamics 365



Dropbox



workday



workiva

JIRA Software



Workplace  
by facebook



aws



Google Cloud

# 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

## Defender for Office 365

Malware detection, safe links, safe attachments

Phishing mail      Opens attachment



Clicks on a URL



User browses to a website

## Entra ID Identity Protection

Identity protection & conditional access



Brute force account or use stolen account credentials

Attacker collects recon and config data

Exploitation & Installation



Command & Control



User account is compromised



Attacker attempts lateral movement

Privileged account compromised

Domain compromised

## Defender for Cloud Apps

Extends protection & conditional access to other cloud apps



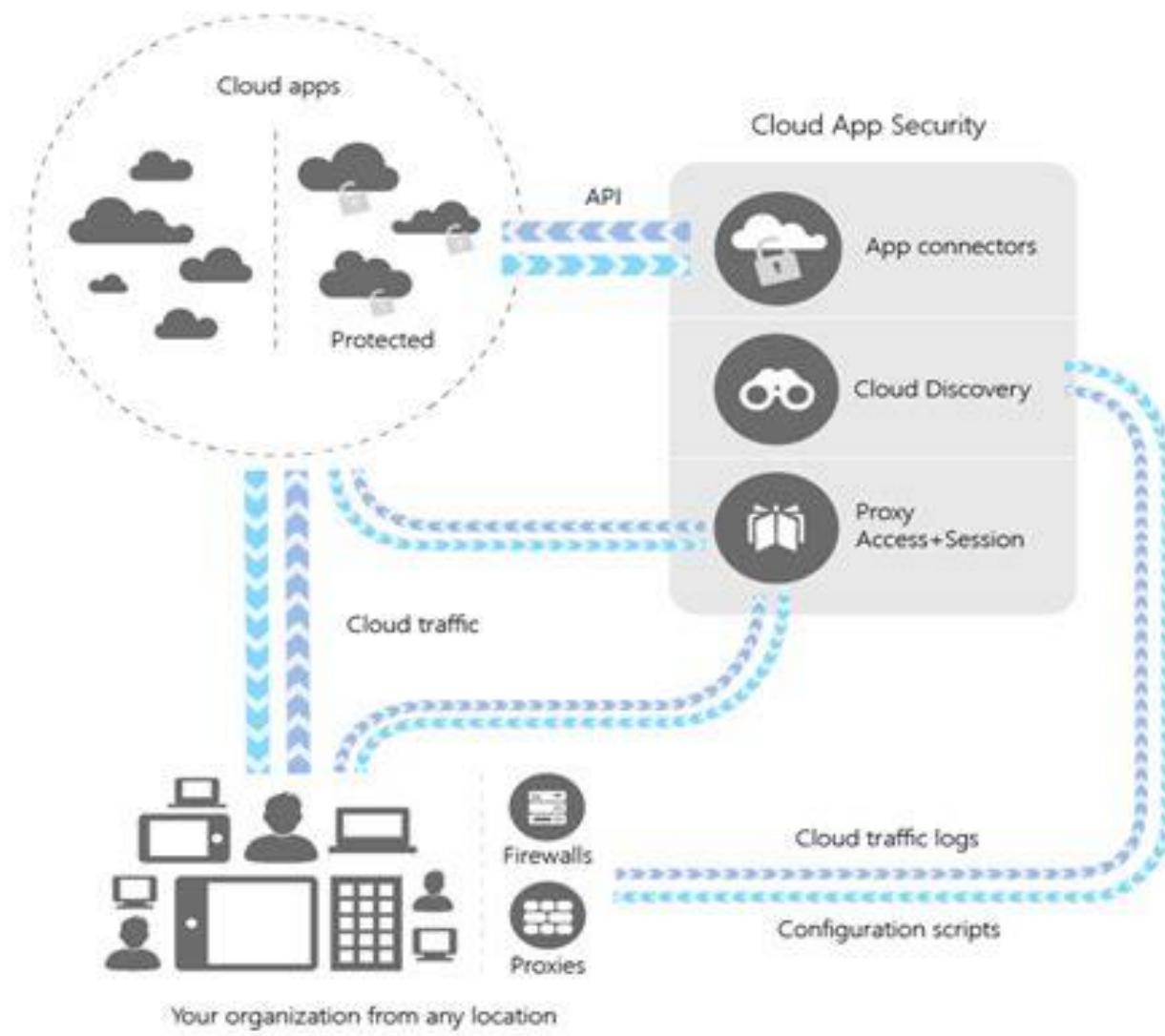
Exfiltrate data

## Defender for Endpoint

Endpoint protection

Defender for Cloud Identity protection

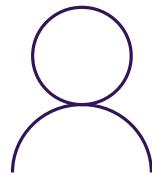
# Architecture



# 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



## Compromised Accounts

Combat advanced attackers that leverage compromise user credentials



## Rogue Application

Identify rogue applications that access your data



## Data exfiltration

Detect unusual flow of data outside of your organization

## 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	
Information Protection	Anomaly detection for discovered apps	Yes		
	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		
Threat Detection	Integration with third-party DLP solutions	Yes		
	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.
Activity policies	Integration to Microsoft Intelligent Security Graph	Yes		Yes
	Activity policies	Yes		Yes

# Cloud App Security versions

Cloud App Security

Cloud Discovery

Cloud Discovery enabled

- Gain continuous visibility
- Analyze cloud app usage
- Dive into a specific app

Azure AD Cloud App Discovery - included with Azure AD P1

Office 365 Cloud App Security

Alerts

RESOLUTION STATUS	CATEGORY	SEVERITY
<button>OPEN</button> <button>DISMISSED</button> <button>RESOLVED</button>	Select risk category...	Low
No		

Alert

Office 365 Cloud App Security

\$3.80 user/month

Enhanced visibility and control into your Office 365 environment.

# Cloud App Security Versions

Cloud App Security

Get started with Cloud App Security    Create a Cloud Discovery report    Connect apps    Create policies    Learn more...

## General dashboard

681 activities monitored    921 files monitored    228 accounts monitored

0 discovered apps (last 30 days)    3 governance actions taken    0 user notifications sent

8 Open alerts    New over the last month

RECENT ALERTS

**Activity from infrequent country**  
MOD Administrator  
Microsoft Cloud App Security    16 hours ago

**Activity from infrequent country**  
MOD Administrator  
Office 365    3 days ago

BY SEVERITY    BY ALERT TYPE

High (Red)    Medium (Orange)    Low (Yellow)

Custom (Blue)    Built-in (Green)

Top 3 alert types: Uncommon location alert (4)

View dashboard for a specific app

- Office 365
- Microsoft SharePoint Online
- Microsoft OneDrive for Business
- Microsoft Power BI
- Microsoft Azure
- Microsoft Cloud App Security
- Microsoft Exchange Online
- Yammer

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

Office 365 Cloud App Security

Protect more cloud apps    

Alerts

RESOLUTION STATUS: OPEN, DISMISSED, RESOLVED | CATEGORY: Select risk cat... | SEVERITY: Low, Medium, High | APP: Select apps... | USER NAME: Select users... | POLICY: Select policy... | Advanced

83 Alerts 1 - 20 of 83 alerts

Alert	Resolution	Severity	Date
Logon from an outdated browser Logon from an outdated browser  36.255.1 Australia	OPEN	Low	1/28/20, 9:19 ...
Failed logins from external Failed logins from external  203.27.190.10 Australia	OPEN	Medium	1/28/20, 9:16 ...
Logon from an outdated browser Logon from an outdated browser  115.70 Australia	OPEN	Low	1/28/20, 8:27 ...
Logon from an outdated browser Logon from an outdated browser  61.69.1 Australia	OPEN	Low	1/28/20, 6:51 ...

<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

Unusual file share activity

Unusual file download

Unusual file deletion activity

Ransomware activity

Data exfiltration to unsanctioned apps

Activity by a terminated employee

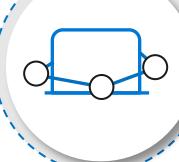
Indicators of a compromised session



Threat delivery and persistence

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

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

Office 365 Cloud App Security

Protect more cloud apps    

## Policy templates

340

Type	Severity	Name	Category	Advanced
Select type...	  	Template name...	Select risk category...	

1 - 18 of 18 Templates

Template	Severity	Linked policies	Published	
 Multiple failed user log on attempts to an app Alert when a single user attempts to log on to a single app, and fails more than ...		1	Nov 15, 2020, 6:02 PM	
 Anomalous behavior in discovered users Alert when anomalous behavior is detected in discovered users and apps, such a...		0	Nov 15, 2020, 6:02 PM	
 Mass download by a single user Alert when a single user performs more than 50 downloads within 1 minute.		1	Nov 15, 2020, 6:02 PM	

# Policies

Office 365 Cloud App Security

Protect more cloud apps



## Policies



Name	Type	Status	Severity	Category	Advanced
Policy name...	Select type...	ACTIVE DISABLED	Yellow Orange Red	Select risk category...	?

1 - 20 of 45 Policies

Create policy

Policy	Count	Severity	Action	Modified	More
Mass download by a single user <small>Alert when a single user performs more than 50 downloads within 1 minute.</small>	0 open alerts	Red		Nov 5, 2020	
Multiple failed user log on attempts to an app <small>Alert when a single user attempts to log on to a single app, and fails more than 1...</small>	0 open alerts	Red		Nov 5, 2020	
Logon from a risky IP address <small>Alert when a user logs on to your sanctioned apps from a risky IP address. By def...</small>	0 open alerts	Red		Nov 5, 2020	

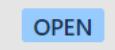
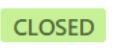
# Alerts

Office 365 Cloud App Security

Protect more cloud apps    

## Alerts

Status	Category	Severity	App	User Name	Policy	Advanced
 	Select risk categ...	  	Select apps...	Select users...	Select policy...	

1 - 20 of 340 alerts

Alert	Status	Resolution type	Severity	Date	More
 Administrative activity from a non-corporate IP address Administrative activity fro... Office 365 Robert Crane 20.190.142.179 Aust...		—	 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...		—	 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...		—	 High	11/25/20, 8:4...	

# Alerts - Detail

Office 365 Cloud App Security

Protect more cloud apps

Alerts > **Administrative activity from a non-corp...** 11/25/20 9:37 PM +50 HIGH SEVERITY

Robert Crane 20.190.142.179 Australia

Resolution options: Robert Crane

340

Description

Activity policy "Administrative activity from a non-corporate IP address" was triggered by "Robert Crane (admin@ciaops365.com)"

Activity log

1 - 1 of 1 activities ⓘ									
Activity	User	App	IP address	Location	Device	Date			
Delete user: user 9f1f662c24...	Robert Crane		20.190.142.179	Aus...	—	Nov 25, 2020...			

Users

1 - 1 of 1 users and accounts							
User name	Investigation prior...	Type	Email	Apps	Groups	Last seen	
Robert Crane	360	User	admin@ciaops365...		Office 365 admini...	Nov 26, 2020, 4:25 ...	



## General Anomaly Detection

2 days ago

86%



Risk score

High severity



Microsoft Exchange Online



claudie@acme.com

Resolution options:

claudie@acme.com ▾

Dismiss...

Resolve alert... ▾

### Description

The user claudie@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 claudie@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 ...



## Activity log

QUERIES	APP	USER NAME	RAW IP ADDRESS	ACTIVITY TYPE	Save as	Advanced
Select a query...	Select apps...	Jane Doe (janedoe@securescoreteam.com)	Enter IP address...	Select activity...		
<p>1 - 11 of 11 activities</p>						
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; Par...	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:...

## Activity log

QUERIES	APP	USER NAME	RAW IP ADDRESS	ACTIVITY TYPE	Save as	Advanced
Select a query...	Select apps...	Jane Doe (janedoe@securescoreteam.com)	Enter IP address...	Select activity...		

1 - 11 of 11 activities

Activity	User	App	IP address	Location	Device	Date	More
Add mailbox folder permission: privilege Ow...	Jane Doe	Microsoft Exc...	94.242.62.254	Russia	—	Sep 13, 2018, 10:32 PM	
Create forwarding Inbox rule: Outlook Inbox...	Jane Doe	Microsoft Exc...	94.242.62.254	Russia	—	Sep 13, 2018, 10:32 PM	

**SHOW SIMILAR** Send us feedback...

Description: Create forwarding Inbox rule: Outlook Inbox Rule **Exfil**

Type: Create > Create forwarding Inbox rule	User: <u>Jane Doe</u>	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 <a href="#">View raw data</a>	User groups: <a href="#">Office 365 administrator (81 users)</a>	User agent tags: —	Tags: —				
ID: 17035763_20893_577a08a6-821c-4f6a-15...	Activity objects: <a href="#">6 Exfil, Mailbox: ceo@securescorete...</a>	App: <a href="#">Microsoft Exchange Online</a>	Location: <a href="#">Russia, Moscow</a>				
Matched policies: —			ISP: OOO Fishnet Communications				
Run command: task New-JournalRule; Para...	Jane Doe	Microsoft Exc...	94.242.62.254	Russia	—	Sep 13, 2018, 10:32 PM	
Run command: task Remove-JournalRule; Pa...	Jane Doe	Microsoft Exc...	94.242.62.254	Russia	—	Sep 13, 2018, 10:32 PM	

## 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

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:...



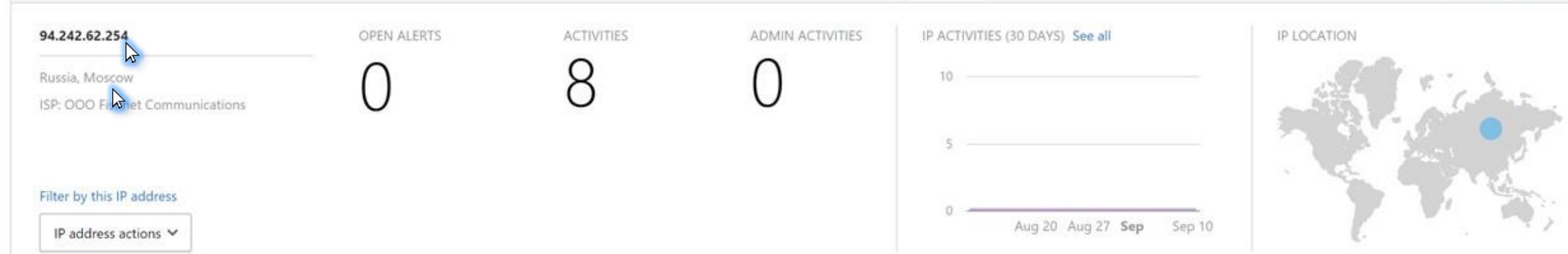
Run command: task New-JournalRule; Para...	Jane Doe	Microsoft Exc...	94.242.62.254	Russia	—	Sep 13, 2018, 10:...
Run command: task Remove-JournalRule; Pa...	Jane Doe	Microsoft Exc...	94.242.62.254	Russia	—	Sep 13, 2018, 10:...

## Activity log

QUERIES	APP	USER NAME	RAW IP ADDRESS	ACTIVITY TYPE	Save as	Advanced
Select a query...	Select apps...	Jane Doe (janedoe@securescoreteam.com)	Enter IP address...	Select activity...		

1 - 11 of 11 activities

Activity	User	App	IP address	Location	Device	Date	More
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:...	



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

Cloud App Security

Alerts > Suspicious inbox forwarding | 5 DAYS AGO

Suspicious inbox forwarding Microsoft Exchange Online 2a01:110:8012:1010:c0fa:cce5:afb4:dd60 Johnny Olivo

Resolution options: Johnny Olivo Dismiss... Resolve... ▾

**Description**

A suspicious inbox forwarding rule was set on a user's inbox. This may indicate that the user account is compromised, and that the mailbox is being used to exfiltrate information from your organization. The user Johnny Olivo (johnny@mcas-test9.com) created or updated an inbox forwarding rule that forwards all incoming email to the external address dan@babblingdan.space.

Additional risks in this user session:

- This user is an administrator in Office 365 (Default).
- United Kingdom was visited for the first time in 72 days by this user.
- 2a01:110:8012:1010:c0fa:cce5:afb4:dd60 was used for the first time in 72 days in your organization.
- ISP Microsoft Corporation was used for the first time in 72 days by this user.

**Activity log**

1 - 1 of 1 activities

Investigate in Activity log ▾

Activity	User	App	IP address	Location	Device	Date
Create forwarding Inbox rule: Outlook Inbox ...	Johnny Olivo	Microsoft Exc...	2a01:110:8012:1010:c0fa:c...	United Kin...	—	Sep 20, 2018, 2:4...

# Activity by a terminated employee

Cloud App Security

Alerts > **Activity by terminated user** 2 MONTHS AGO

MEDIUM SEVERITY

Richard Munger Amazon Web Services - US Activity performed by terminated user

Resolution options: Richard Munger Dismiss... Resolve... ▾

Description

The user Richard Munger (richard@mcas-test9.com) performed an activity in Amazon Web Services (Amazon Web Services - US), after their Azure AD account was deleted.

1K+ Activity log

Activity	User	App	IP address	Location	Device	Date
AWS identity and access management: task Lis...	Richard Munger (richard@mcas-test9)	Amazon Web S...	167.220.196.35	United Kingc...	—	Aug 8, 2018, 05:03
AWS identity and access management: task Ge...	Richard Munger (richard@mcas-test9)	Amazon Web S...	167.220.196.35	United Kingc...	—	Aug 8, 2018, 05:03
AWS identity and access management: task Lis...	Richard Munger (richard@mcas-test9)	Amazon Web S...	167.220.196.35	United Kingc...	—	Aug 8, 2018, 05:03
AWS identity and access management: task Lis...	Richard Munger (richard@mcas-test9)	Amazon Web S...	167.220.196.35	United Kingc...	—	Aug 8, 2018, 05:03



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

ACTIVITIES MATCHING ALL OF THE FOLLOWING

Activity type equals Set-JournalRule

[Edit and preview results](#)

### 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@securecoreteam.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

The screenshot displays the Microsoft Cloud App Security platform's user interface across two devices. The desktop monitor shows the 'Cloud Discovery' dashboard, which provides a high-level overview of cloud usage. Key statistics include 557 discovered apps, 1173 users, 2540 IP addresses, and a total traffic volume of 314.4 GB. A large circular gauge indicates the total traffic volume. Below the dashboard, there are sections for 'App categories' (with a chart showing sanctioned, unsanctioned, and other categories) and 'Risk levels' (with a chart showing traffic from high-risk, medium-risk, and low-risk apps). The tablet below shows the 'Files' management interface, where users can search for specific files, view file details, and manage access levels. The interface includes columns for APP, OWNER, ACCESS LEVEL, FILE TYPE, and MATCHED POLICY.

# 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

Unusual file share activity

Unusual file download

Unusual file deletion activity

Ransomware activity

Data exfiltration to unsanctioned apps

Activity by a terminated employee

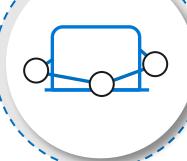
Indicators of a compromised session



Threat delivery and persistence

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

Malicious use of an end-user account



Malicious use of a privileged user



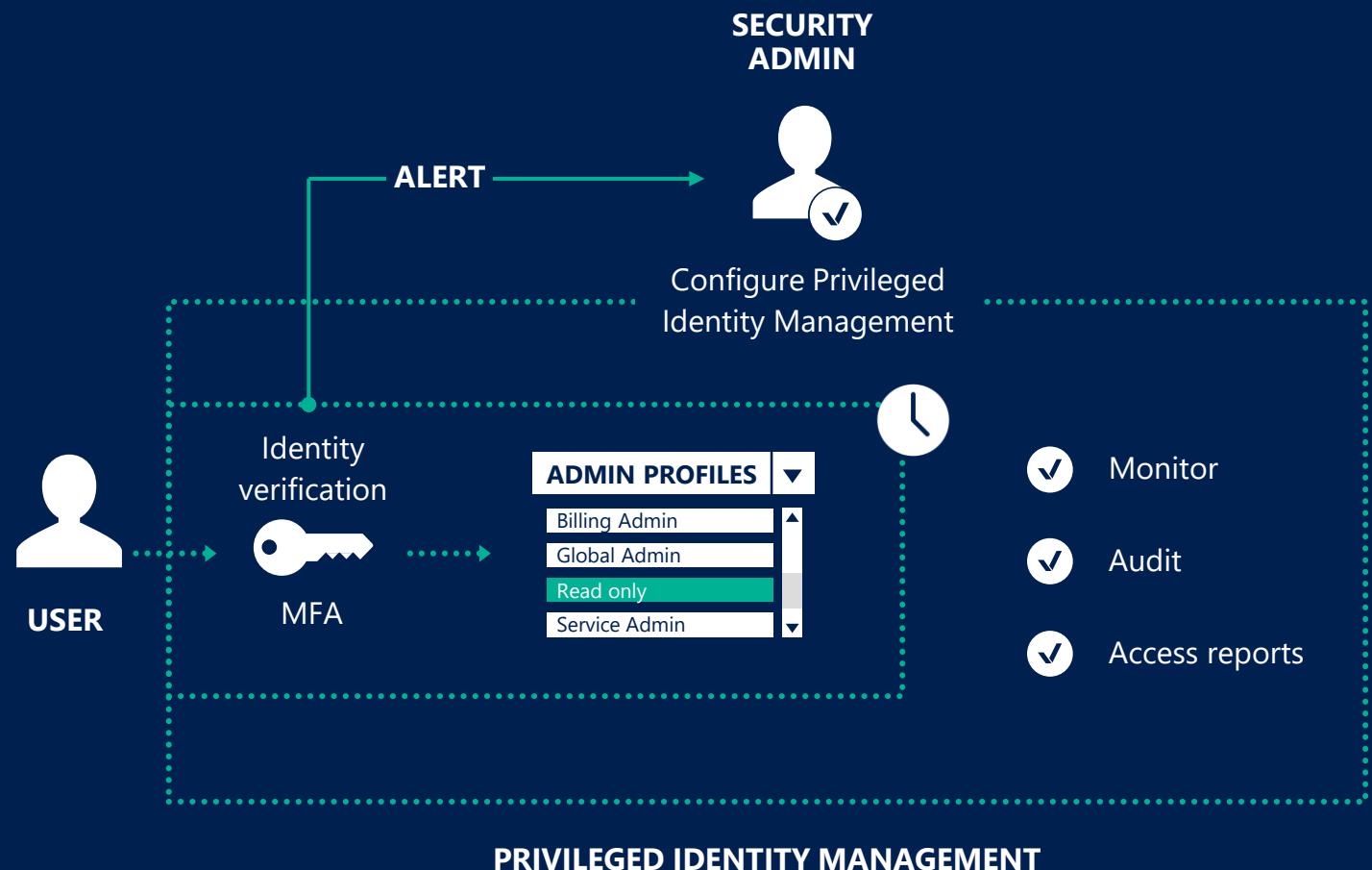
Unusual impersonated activity  
Unusual administrative activity  
Unusual multiple delete VM activity

# DEMO

# Privileged Identity Management

How time-limited activation of privileged roles works

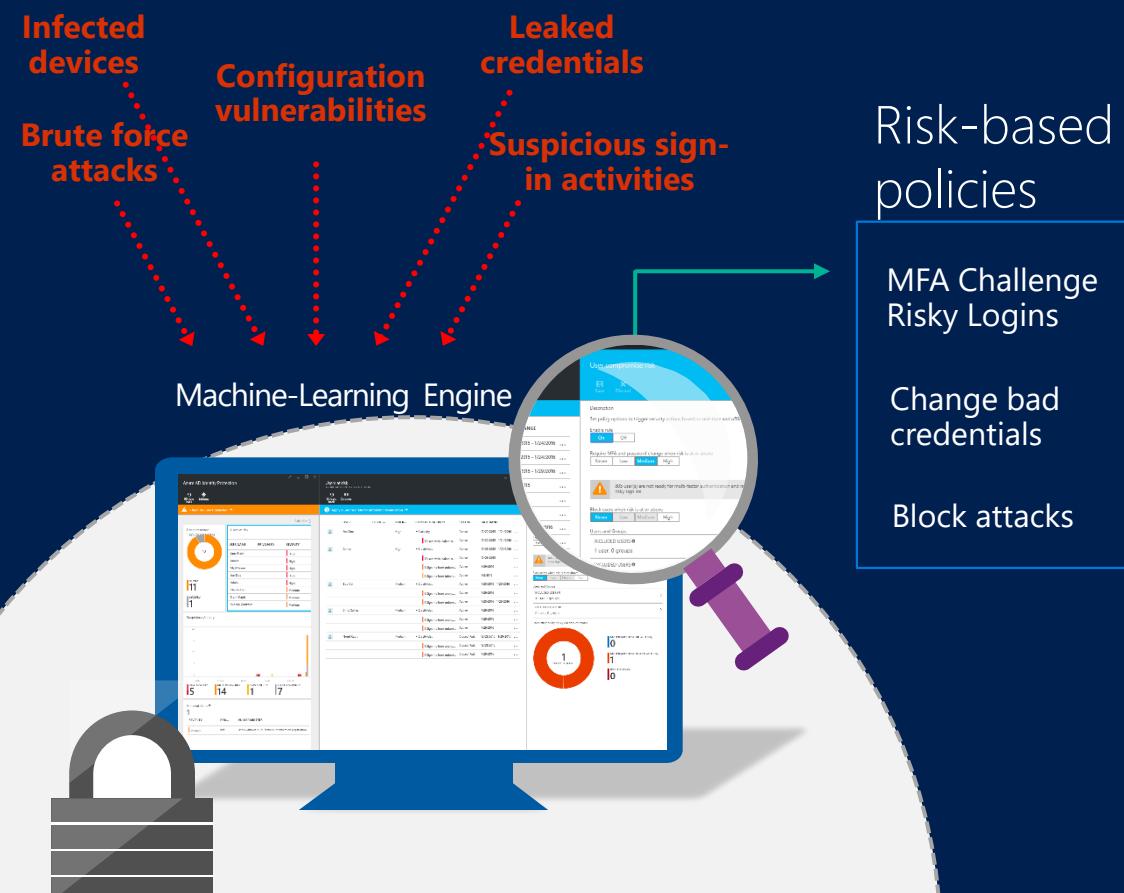
- ▶ Users need to activate their privileges to perform a task
- ▶ MFA is enforced during the activation process
- ▶ Alerts inform administrators about out-of-band changes
- ▶ Users will retain their privileges for a pre-configured amount of time
- ▶ Security admins can discover all privileged identities,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



# 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



## Identity Protection - Overview

 Search (Ctrl+/)[Learn more](#)

Refresh

Got feedback?

[Overview](#)

Date range = 30 days

### Protect

User risk policy

Sign-in risk policy

MFA registration policy

### Report

Risky users

Risky sign-ins

Risk detections

### Notify

Users at risk detected alerts

Weekly digest

### Troubleshooting + Support

New risky users detected

User risk level = All

01/04 01/11 01/18 01/25

[Configure user risk policy >](#)

New risky sign-ins detected

Sign-in risk type = Real-time

Sign-in risk level = All

2  
1.5  
1  
0.5

High risk users

1

High risk users detected. Investigate users and reset passwords.

# Microsoft Azure

 Microsoft

## Sign in

to continue to Microsoft Azure

clara@fourthcoffee.club| X

No account? [Create one!](#)

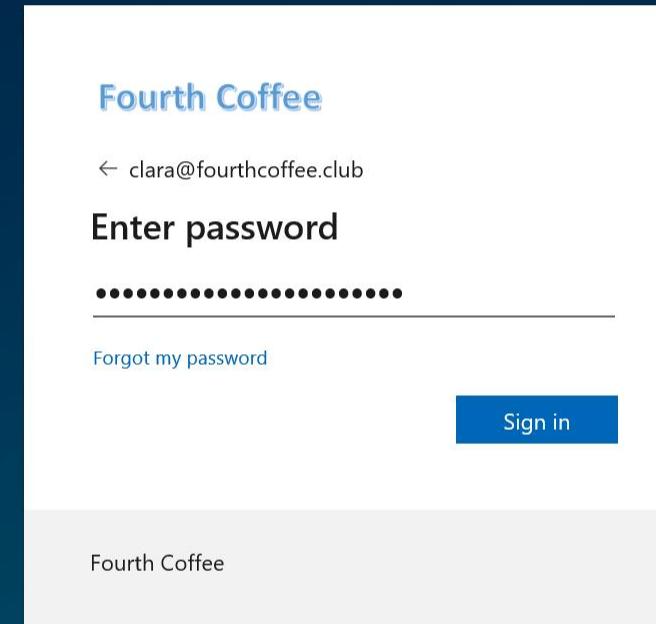
[Can't access your account?](#)

[Sign in with Windows Hello or a security key](#) ⓘ

Back Next



[Sign in with GitHub](#)



**Fourth Coffee**

← clara@fourthcoffee.club

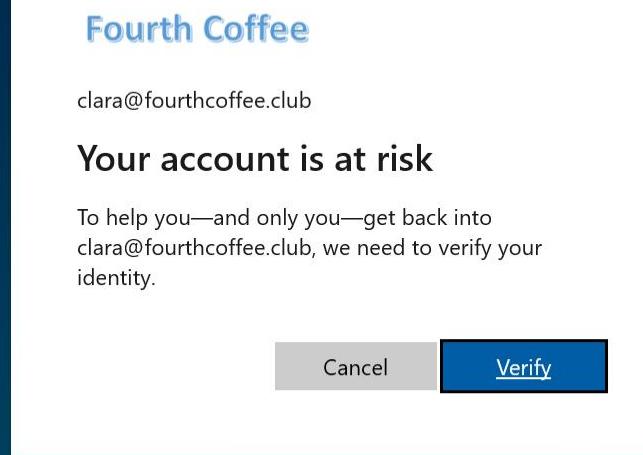
**Enter password**

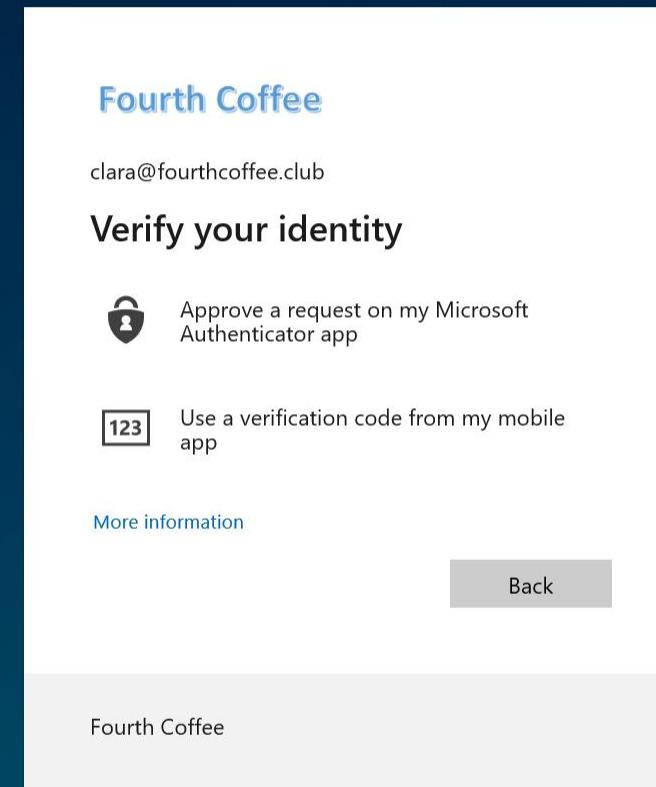
••••••••••••••••

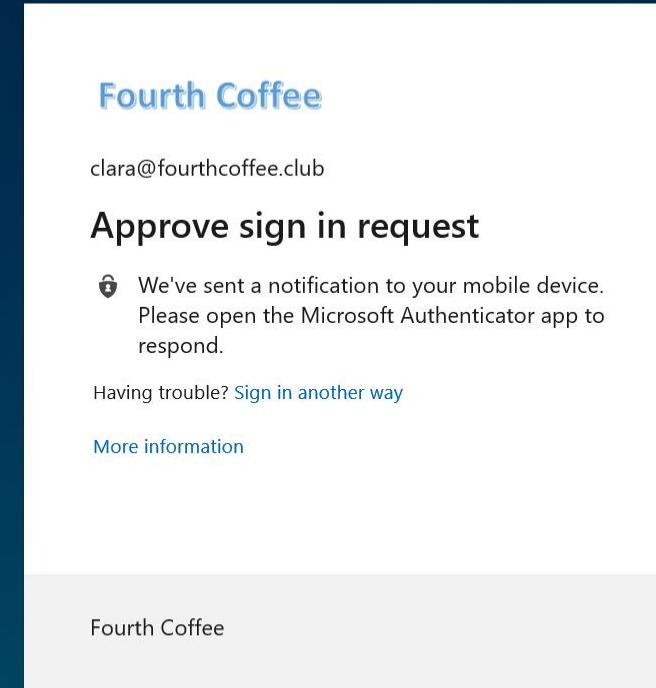
[Forgot my password](#)

**Sign in**

Fourth Coffee







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

Microsoft Azure

Search resources, services, and docs (G+)

Home > Fourth Coffee > Security > Identity Protection - Risky users

## Identity Protection - Risky users

Search (Ctrl+ /) | 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
<input type="checkbox"/> Dominic Jones	At risk	High	11/1/2019, 3:14:05 PM
<input checked="" type="checkbox"/> 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

User	Clara Pinto	Risk state	At risk	Office location
Roles	Limited admin	Risk level	High	Department Services
Username	clara@M365x066108.onmicrosoft.com	Details	-	Mobile phone
User ID	cc314e6c-5d13-42c3-8db5-efc89aca657a	Risk last updated	11/1/2019, 3:14:05 PM	

## Identity Protection – Risky users

## Identity Protection - Risky users

 Search (Ctrl+ /)[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
<input type="checkbox"/> Dominic Jones	At risk	High	11/1/2019, 3:14:05 PM
<input checked="" type="checkbox"/> 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

Microsoft Azure

Search resources, services, and docs (G+)

Home > Fourth Coffee > Security > Identity Protection - Risky users

Identity Protection - Risky users

Search (Ctrl+/)

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
<input type="checkbox"/> Dominic Jones	At risk	High	11/1/2019, 3:14:05 PM
<input checked="" type="checkbox"/> Clara Pinto	At risk	High	11/1/2019, 3:14:05 PM

Risky users

Risky sign-ins

Risk detections

Vulnerabilities

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Troubleshoot

New support request

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

Detection type	Time Detected	Detection risk state	Detection risk level	Detection risk details
Azure AD threat intelligence ⓘ	10/30/2019, 9:36:38 AM	At risk	-	-
Leaked credentials ⓘ	10/30/2019, 7:36:38 AM	At risk	-	-

Identity Protection – Risky users

Microsoft Azure

Search resources, services, and docs (G+)

Home > Fourth Coffee > Security > Identity Protection - Risky users > Clara Pinto - Risky sign-ins

## Clara Pinto - Risky sign-ins

[Download](#) [Learn more](#) [Export Data Settings](#) [Troubleshoot](#) [Select all](#) [Confirm sign-in\(s\) compromised](#) [Confirm sign-in\(s\) safe](#) [Refresh](#) [Columns](#) [Got feedback?](#)

Welcome to Azure AD Identity Protection's advanced 'Risky sign-ins' view. Manage all your risky sign-ins here.

Date : Last 1 month	Show dates as: Local	User : Clara Pinto	Risk state : 5 selected	Risk level (real-time) : None Selected	Risk level (aggregate) : None Selected	Detection type(s) : None Selected	+ Add filters		
Date	User	Status	IP address	Location	Operating system	Device browser	Risk state	Risk level (aggregate)	Risk level (real-time)
<input type="checkbox"/> 11/1/2019, 11:04:51 AM	Clara Pinto	Success	85.10.51.86	Zagreb, Grad Zagreb, HR	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
<input checked="" type="checkbox"/> 11/1/2019, 11:04:46 AM	Clara Pinto	Interrupted	85.10.51.86	Zagreb, Grad Zagreb, HR	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
<input type="checkbox"/> 10/30/2019, 5:55:53 PM	Clara Pinto	Success	85.10.51.12	Zagreb, Grad Zagreb, HR	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
<input type="checkbox"/> 10/30/2019, 5:55:48 PM	Clara Pinto	Interrupted	85.10.51.12	Zagreb, Grad Zagreb, HR	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
<input type="checkbox"/> 10/30/2019, 4:58:13 PM	Clara Pinto	Success	192.154.196.13	Guadalajara, Jalisco, MX	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
<input type="checkbox"/> 10/30/2019, 4:58:12 PM	Clara Pinto	Success	192.154.196.13	Guadalajara, Jalisco, MX	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
<input type="checkbox"/> 10/30/2019, 4:58:09 PM	Clara Pinto	Interrupted	192.154.196.13	Guadalajara, Jalisco, MX	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
<input type="checkbox"/> 10/30/2019, 1:36:38 PM	Clara Pinto	Success	37.120.143.222	Brussels, Brussels, BE	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
<input type="checkbox"/> 10/30/2019, 1:20:57 PM	Clara Pinto	Success	71.107.102.210	Kirkland, Washington, US	Windows 10	Chrome 77.0.3865	Remediated	-	Medium

Details

User's risk report User's sign-ins User's risky sign-ins User's risk detections Sign-in's risk detections Confirm sign-in compromised Confirm sign-in safe

Basic info Device info Risk info MFA info Conditional Access Report-only (Preview)

DETECTION TYPE	DETECTION RISK STATE	TIME DETECTED	DETECTION TIMING
Anonymous IP address ⓘ	Remediated	11/1/2019, 11:04 AM	Real-time
Risk level	Medium	Sign-in time 11/1/2019, 11:04 AM	Token issuer type Azure AD
Risk detail	User performed secured password change	IP address 85.10.51.86	
Source	Identity Protection	Sign-in location Zagreb, Grad Zagreb, HR	
Detection last updated	11/1/2019, 5:04 PM	Sign-in client Mozilla/5.0 (iPhone; CPU iPhone OS 13_1 like Mac OS X)	

## Identity Protection – Risky sign-ins

Microsoft Azure

Search resources, services, and docs (G+)

Home > Fourth Coffee > Security > Identity Protection - Risky users > Clara Pinto - Risky sign-ins > Clara Pinto - Risk detections

## Clara Pinto - Risk detections

[Learn more](#) [Download](#) [Refresh](#) | [Columns](#) | [Got feedback?](#)

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

Detection time : Last 1 month		Show dates as: Local		User : Clara Pinto		Detection type : None Selected		Risk state : 5 selected		Risk level : None Selected		<a href="#">Add filters</a>	
Detection time	User	IP address	Location	Detection type	Risk state	Risk level	Request ID						
<input checked="" type="checkbox"/> 11/1/2019, 11:04:51 AM	Clara Pinto	85.10.51.86	Zagreb, Grad Zagreb, HR	Anonymous IP address	Remediated	Medium	b7d0827f-6ee7-40ae-bc54-40a...						
<input type="checkbox"/> 11/1/2019, 11:04:46 AM	Clara Pinto	85.10.51.86	Zagreb, Grad Zagreb, HR	Anonymous IP address	Remediated	Medium	550a044d-d36f-4c8d-9766-da...						
<input type="checkbox"/> 10/30/2019, 5:55:53 PM	Clara Pinto	85.10.51.12	Zagreb, Grad Zagreb, HR	Anonymous IP address	Remediated	Medium	bbbb6941-f29c-43d9-b793-5a...						
<input type="checkbox"/> 10/30/2019, 5:55:48 PM	Clara Pinto	85.10.51.12	Zagreb, Grad Zagreb, HR	Anonymous IP address	Remediated	Medium	60336bfa-702f-49ff-bf20-9896...						
<input type="checkbox"/> 10/30/2019, 4:58:13 PM	Clara Pinto	192.154.196.13	Guadalajara, Jalisco, MX	Anonymous IP address	Remediated	Medium	92657fc4-d1a6-4a2e-a194-578...						
<input type="checkbox"/> 10/30/2019, 4:58:12 PM	Clara Pinto	192.154.196.13	Guadalajara, Jalisco, MX	Anonymous IP address	Remediated	Medium	3e91319f-5e97-4039-bd65-cb...						
<input type="checkbox"/> 10/30/2019, 4:58:09 PM	Clara Pinto	192.154.196.13	Guadalajara, Jalisco, MX	Anonymous IP address	Remediated	Medium	5bafa9a1-2e1c-40e9-abd4-b3f...						
<input type="checkbox"/> 10/30/2019, 1:36:38 PM	Clara Pinto	37.120.143.222	Brussels, Brussels, BE	Anonymous IP address	Remediated	Medium	a5c23c62-07de-4054-8f9d-788...						
<input type="checkbox"/> 10/30/2019, 11:57:58 AM	Clara Pinto	37.120.143.222	Brussels, Brussels, BE	Anonymous IP address	Remediated	Medium	a48a5d56-8ac5-4338-89d2-c5f...						
<input type="checkbox"/> 10/30/2019, 11:57:51 AM	Clara Pinto	37.120.143.222	Brussels, Brussels, BE	Anonymous IP address	Remediated	Medium	4f3ha711-80ed-48c7-aa36-c54...						

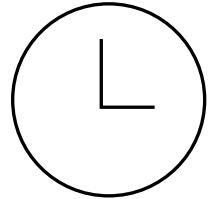
Details

User's risk report User's sign-ins User's risky sign-ins Linked risky sign-in User's risk detections

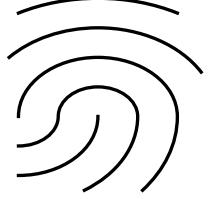
Detection type	Anonymous IP address	Activity	Sign-in	Sign-in time	11/1/2019, 11:04 AM
Risk state	Remediated	Detection time	11/1/2019, 11:04 AM	IP address	85.10.51.86
Risk level	Medium	Detection last updated	11/1/2019, 5:04 PM	Sign-in location	Zagreb, Grad Zagreb, HR
Risk detail	User performed secured password change	Token issuer type	Azure AD	Sign-in client	Mozilla/5.0 (iPhone; CPU iPhone OS 13_1 like Mac OS X)
Source	Identity Protection			Sign-in request id	b7d0827f-6ee7-40ae-bc54-40a7771e0200
Detection timing	Real-time			Sign-in correlation id	82b62279-0fae-4b48-95a0-f0cc9c6c8da3

## Identity Protection – Risk detections

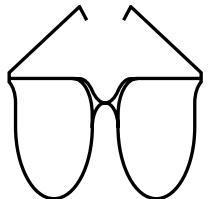
# Privileged Identity Management



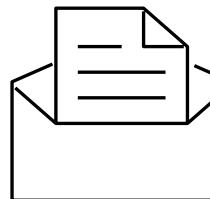
Privileged role membership only granted for a limited amount of time



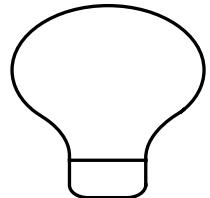
Roles can be configured to require staff to perform MFA prior to elevation of privilege



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

 Privileged Identity Management - Quick start  
Privileged Identity Management

[What's new](#) [Get started](#)

- ## 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

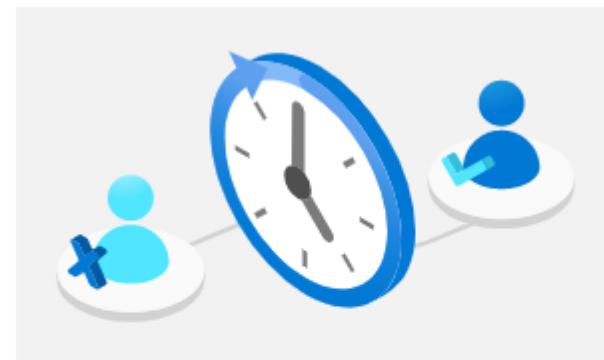
## Manage your privileged access

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](#)



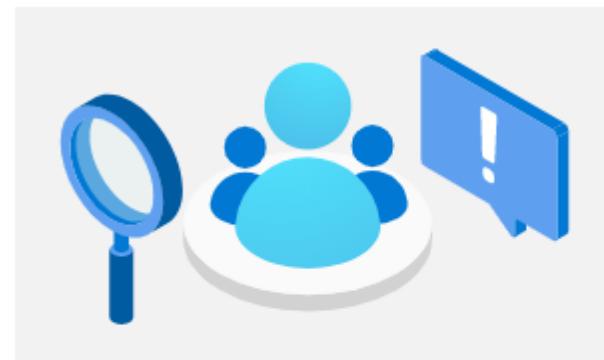
## Manage access

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

Microsoft Azure

Search resources, services, and docs (G+)

vance@fourthcoffee.club FOURTH COFFEE

Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Verify my identity

**Global Administrator** X

Role activation details

Activate  Deactivate

! Verify your identity before proceeding →

NAME  
Vance Brown

EMAIL  
vance@fourthcoffee.club

ACTIVATION  
Eligible

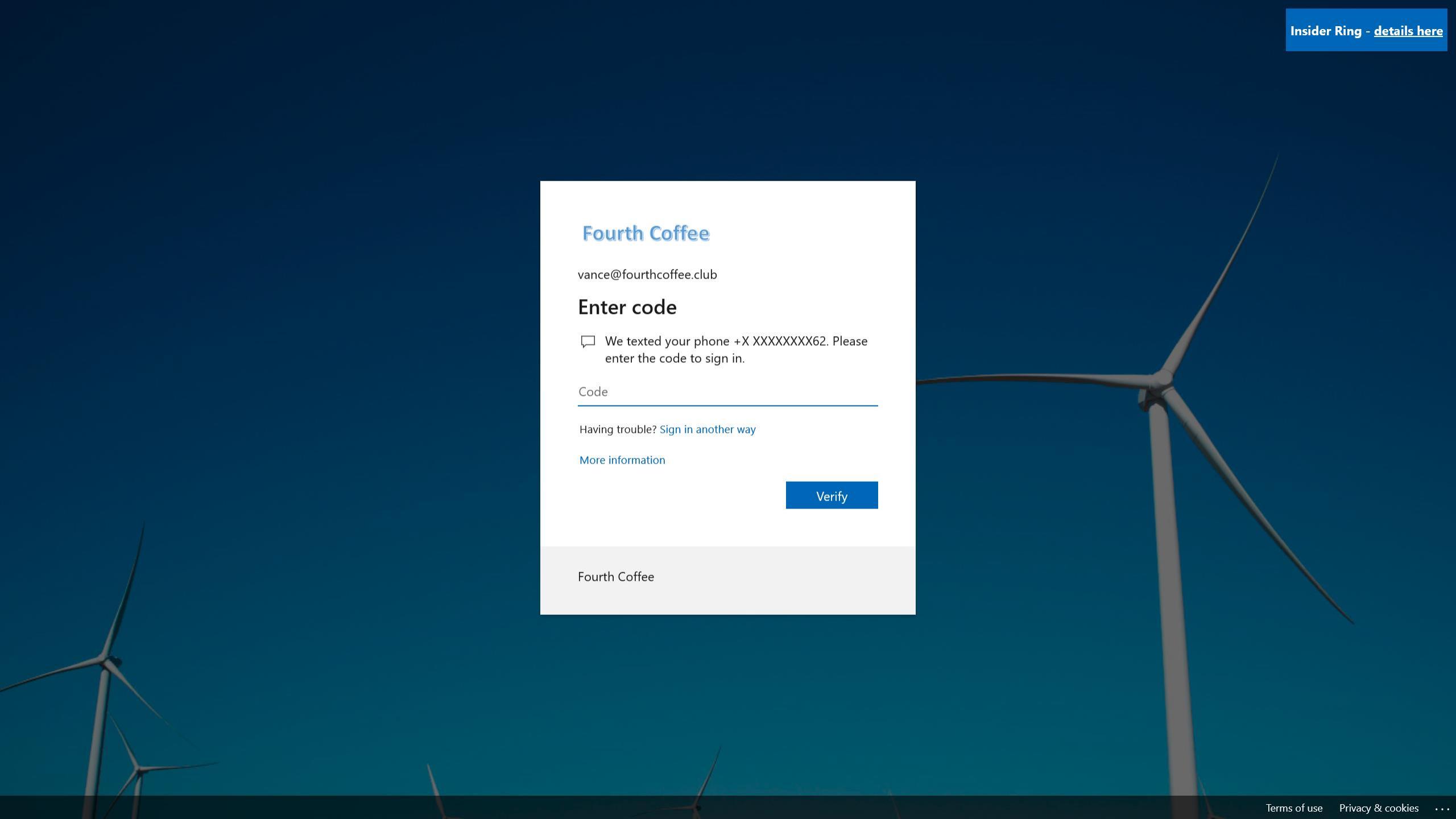
EXPIRATION  
-

**Verify my identity** X

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 X



**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

Microsoft Azure

Search resources, services, and docs (G+)

vance@fourthcoffee.club  
FOURTH COFFEE

Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator

**Global Administrator** X □ ×

Role activation details

Activate  Deactivate

---

NAME  
Vance Brown

EMAIL  
vance@fourthcoffee.club

ACTIVATION  
Eligible

EXPIRATION  
-

Microsoft Azure

Search resources, services, and docs (G+)

vance@fourthcoffee.club  
FOURTH COFFEE

Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Activation

## Activation

Role activation details

Custom activation start time

Activation duration (hours)

Ticket number \* ⓘ  ✓

Ticket system  ✓

Activation reason (max 500 characters) \*

I need to access a privileged app for CAPN project.

**Activate**

Microsoft Azure

Search resources, services, and docs (G+)

vance@fourthcoffee.club FOURTH COFFEE

Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Activation > Activation status

**Activation**

Role activation details

Custom activation start time

Activation duration (hours)

Ticket number \*  

Ticket system  

Activation reason (max 500 characters) \*

I need to access a privileged app for CAPN project.

**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](#)

Microsoft Azure

Search resources, services, and docs (G+)

vance@fourthcoffee.club FOURTH COFFEE

Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Activation > Activation status

**Activation**

Role activation details

Custom activation start time

Activation duration (hours)

Ticket number \*  

Ticket system  

Activation reason (max 500 characters) \*

I need to access a privileged app for CAPN project.

**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](#)

Microsoft Azure

Search resources, services, and docs (G+)

vance@fourthcoffee.club FOURTH COFFEE

Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Activation > Activation status

**Activation** X

Role activation details

Custom activation start time

Activation duration (hours) 1

Ticket number \* ① ✓  
85739

Ticket system ✓  
ServiceNow

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

Activate

**Activation status** X

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](#)

# Microsoft Azure

 Microsoft

**Sign in**  
to continue to Microsoft Azure

vance@fourthcoffee.club

No account? [Create one!](#)

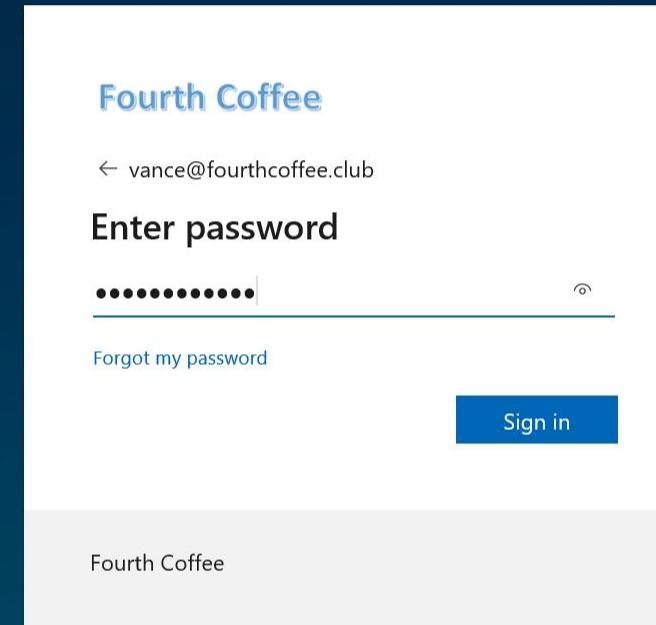
[Can't access your account?](#)

[Sign in with Windows Hello or a security key](#) ⓘ

[Back](#) [Next](#)



[Sign in with GitHub](#)



**Fourth Coffee**

← vance@fourthcoffee.club

**Enter password**

••••••••••| ↶

[Forgot my password](#)

**Sign in**

Fourth Coffee

# Demo