

# Detect & Respond: Cloud App Security

## Defender for Cloud Apps

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

The screenshot displays the Microsoft Cloud App Security portal interface. The top navigation bar includes tabs for 'Discover', 'Investigate', 'Control', and 'Alerts'. The main content area is titled 'Policy templates' and features a filter bar with options for 'TYPE', 'SEVERITY', 'NAME', and 'CATEGORY'. Below the filter bar, a table lists 17 templates, with the first seven visible. Each template entry includes an icon, a title, a description, a severity level (indicated by three red squares), the number of linked policies (0), and the publication date (Sep 17, 2017, 2:05 AM). A plus sign icon is present at the end of each row.

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



# User and entity behavioral analytics

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

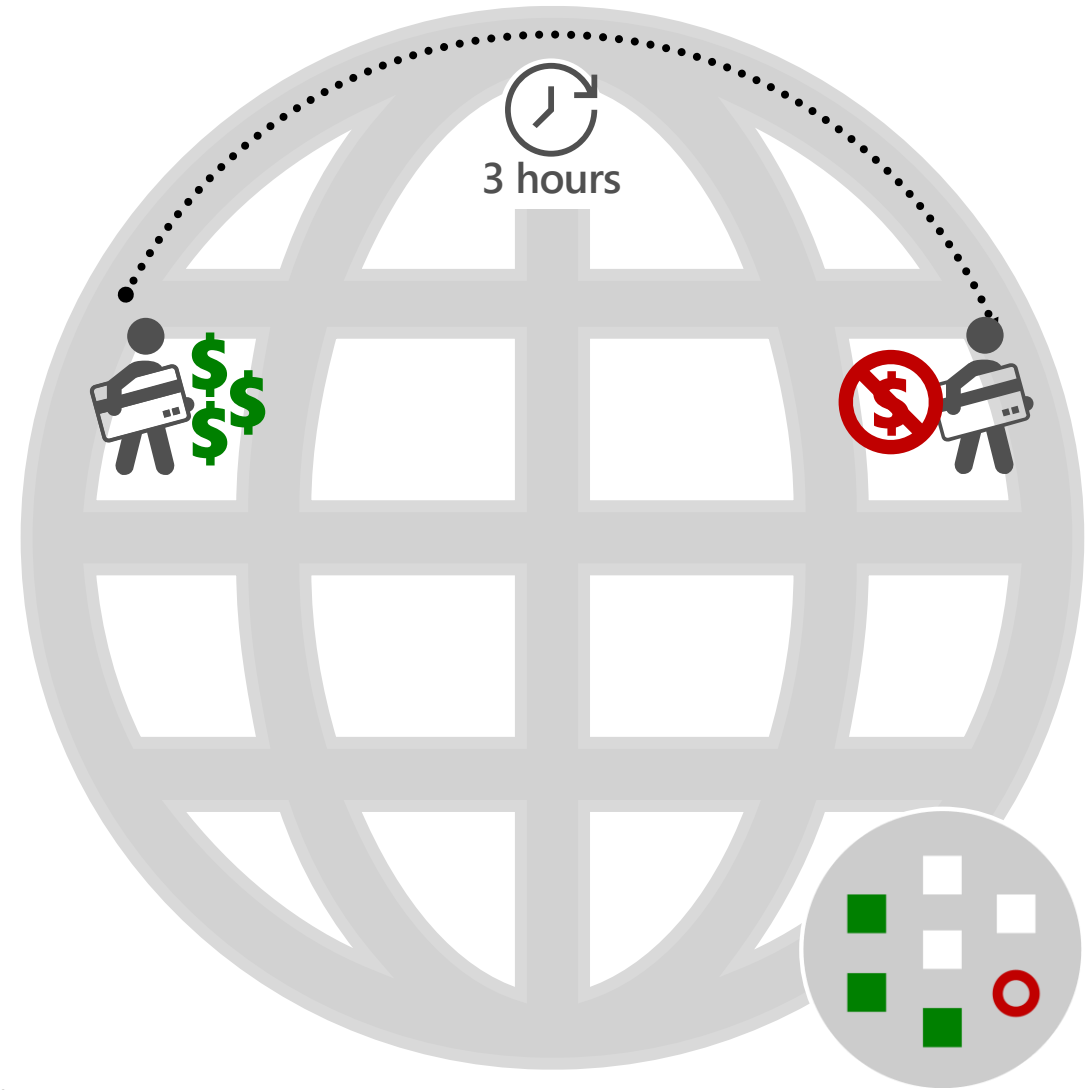
Profiles behavior and detects anomalies by using **machine learning** algorithms

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

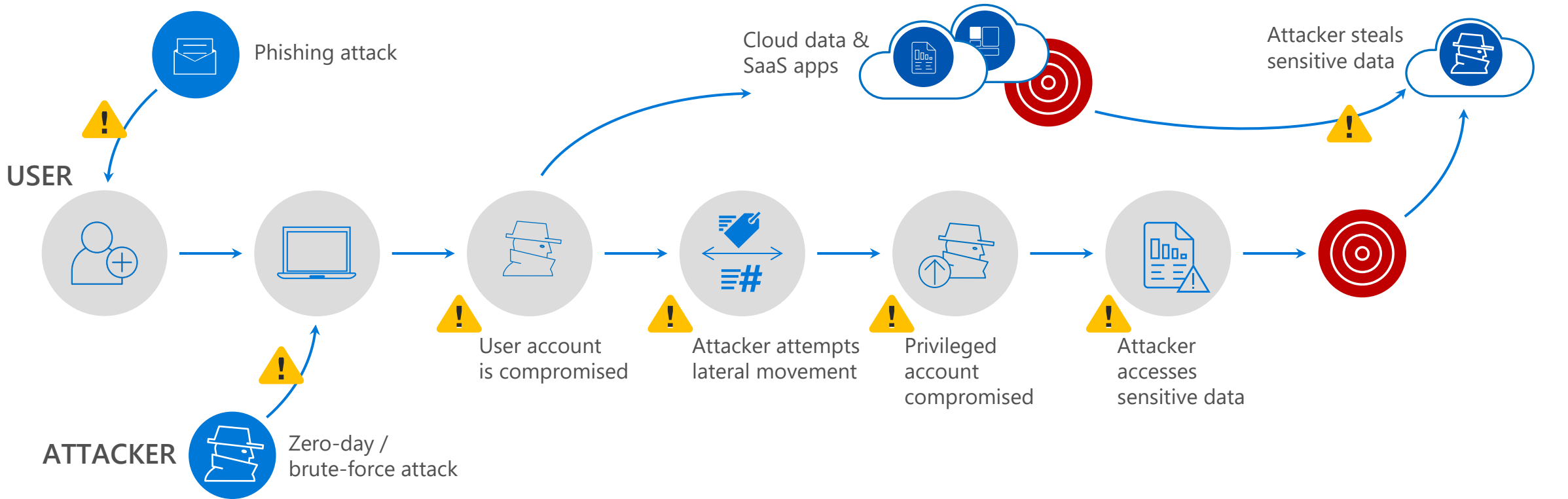
Credit card companies monitor cardholders' behavior.

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

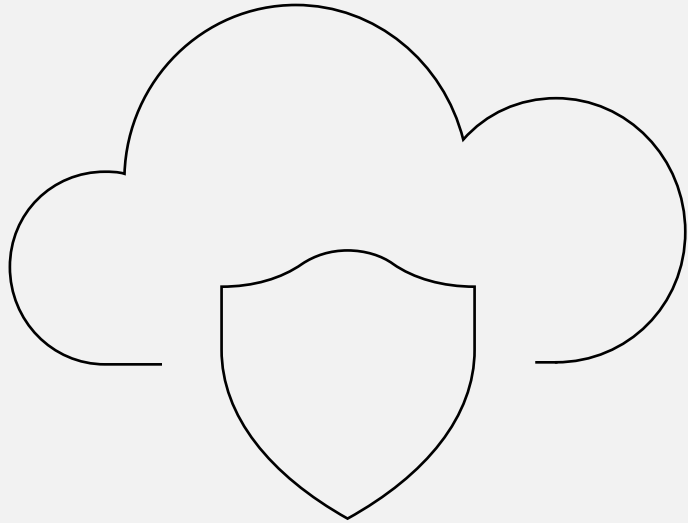


Anonymous user behavior



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

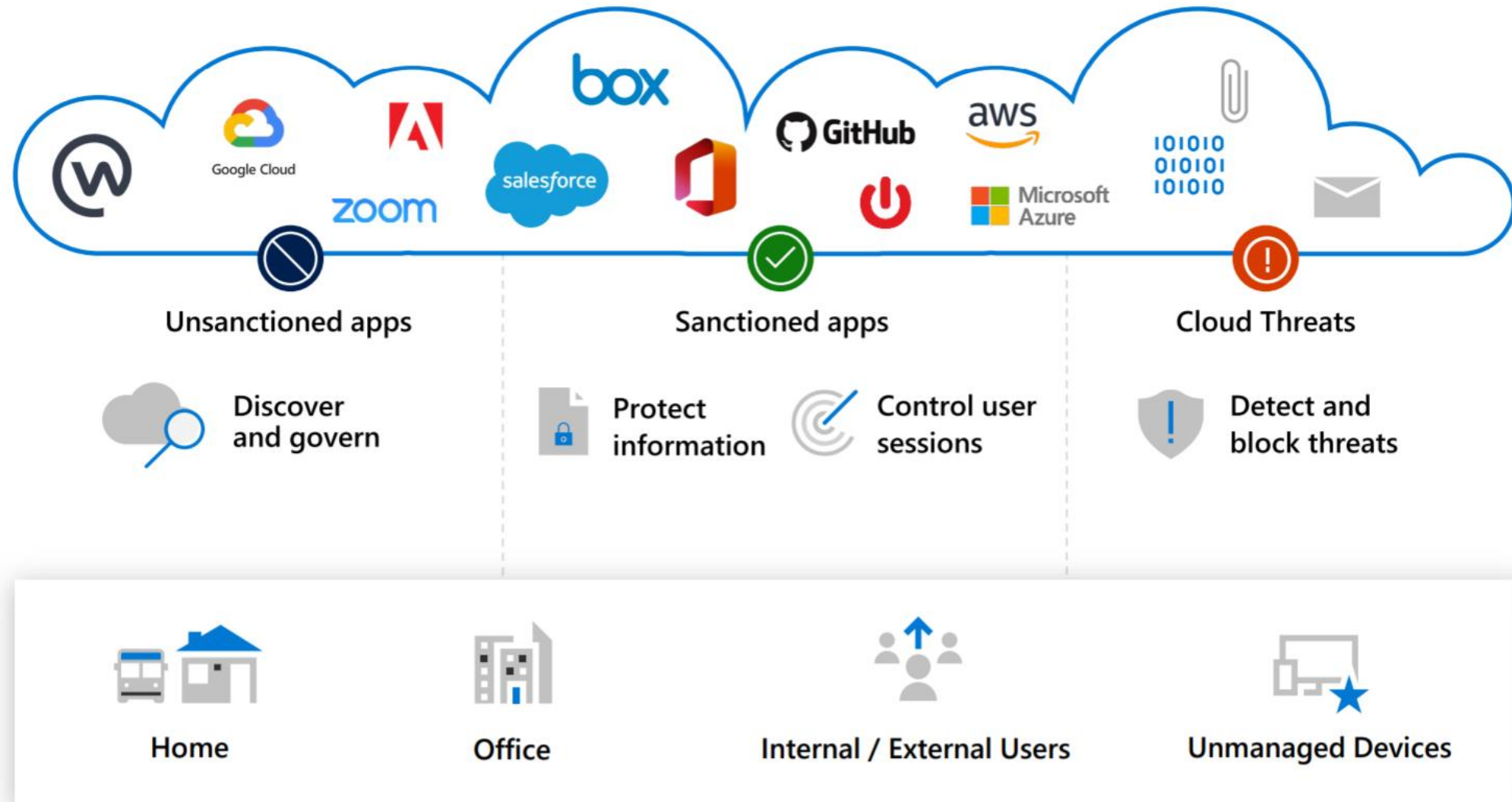
Raise alerts on user or file behavior anomalies in cloud apps leveraging their API connectors

## 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

box

slack



Workplace  
by facebook



G Suite

okta



workday

zoom



tableau

workiva

GitHub



zendesk

Confluence

JIRA Software

servicenow

CONCUR

Microsoft  
Dynamics 365

DocuSign

aws  
Amazon  
Web Services

Microsoft  
Azure

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

Exploitation & Installation



Command & Control



## Entra ID Identity Protection

Identity protection & conditional access



Brute force account or use stolen account credentials

Attacker collects recon and config data



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



Attacker accesses sensitive data



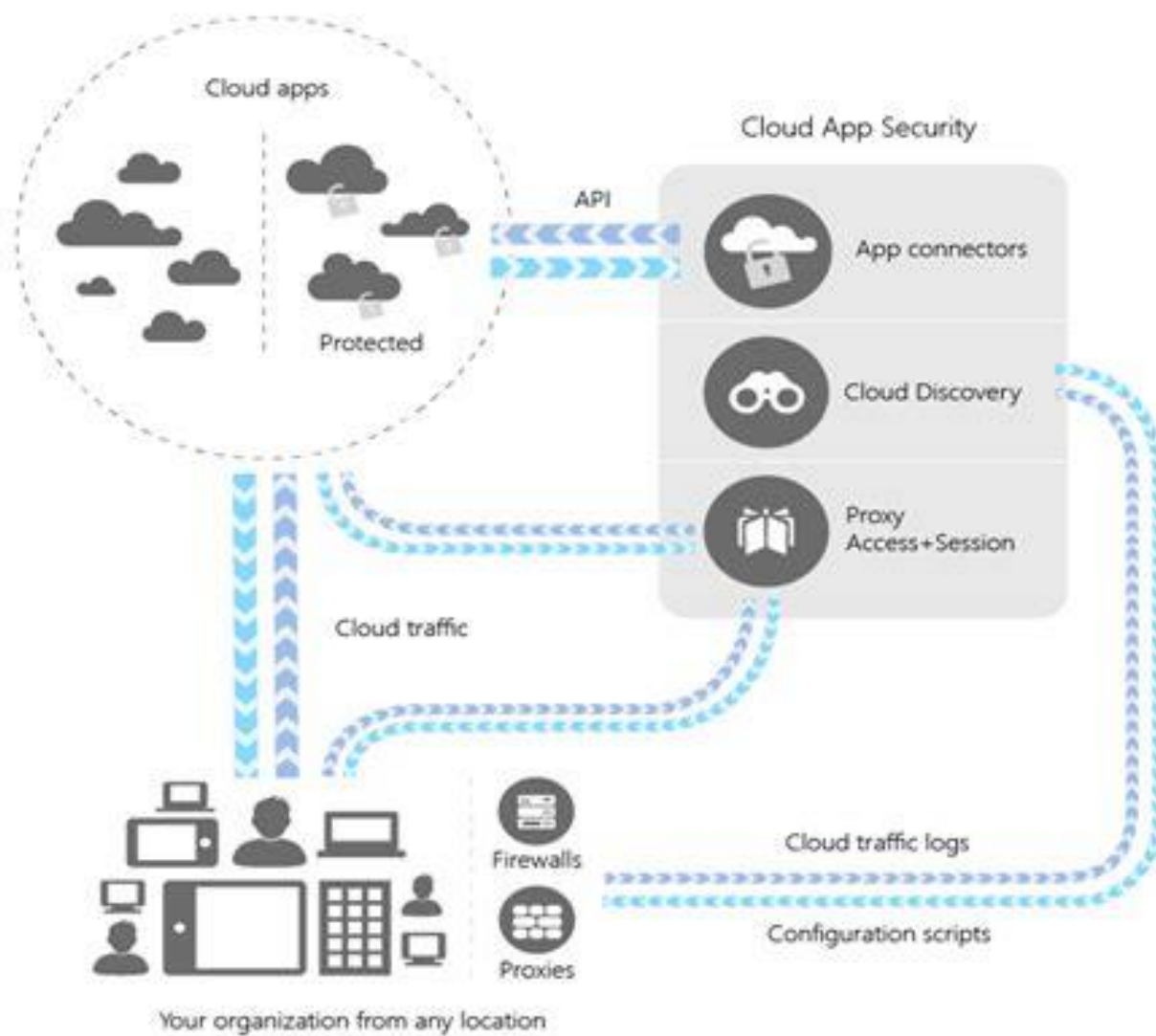
## Defender for Endpoint

Endpoint protection

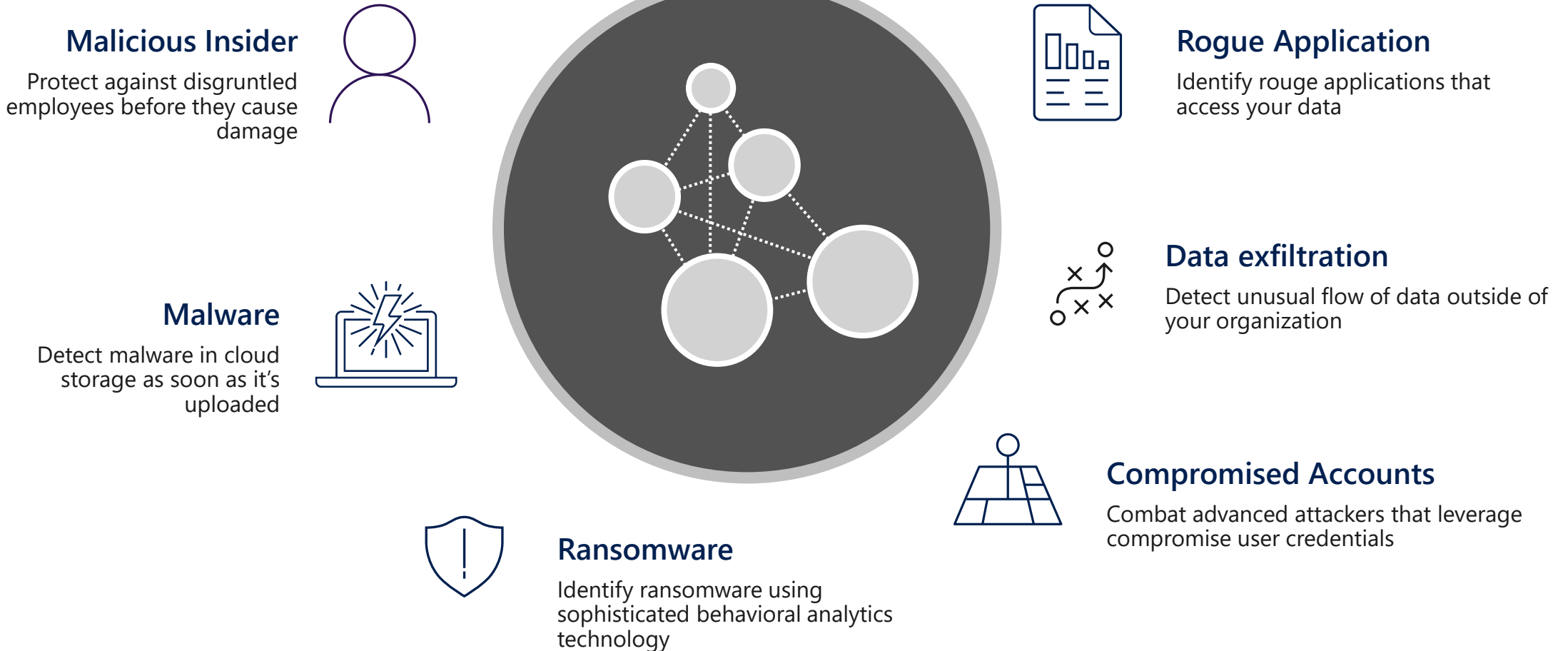
## Defender for Cloud

Identity protection

# Architecture



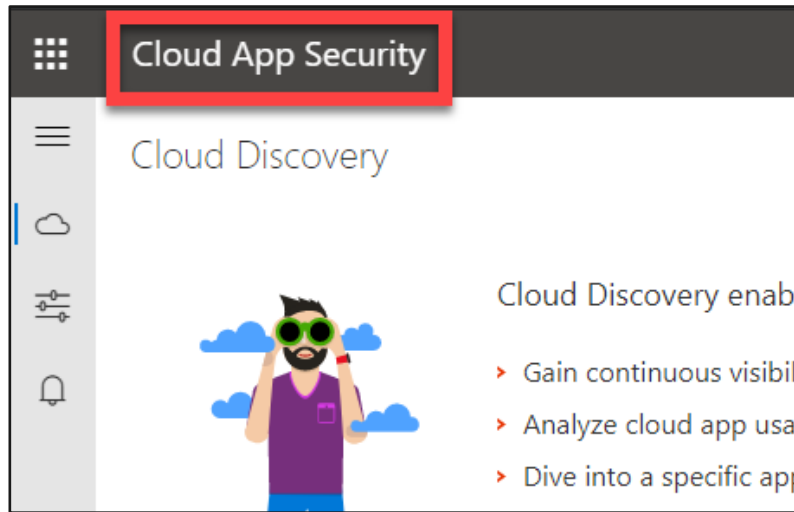
# Defender for Cloud Apps protects the application session



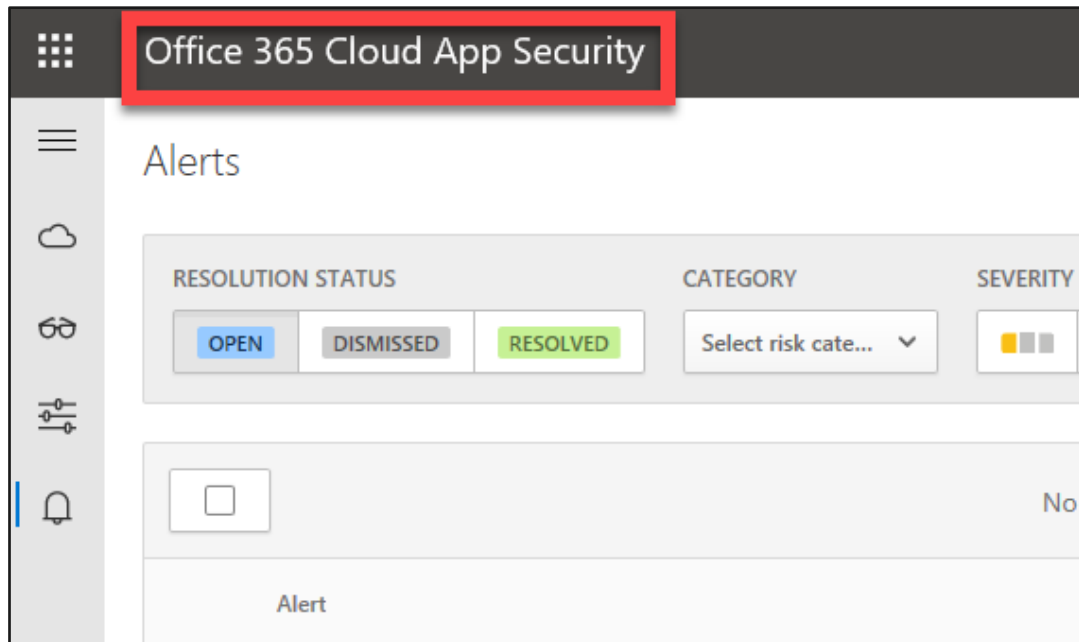
Microsoft Cloud App Security  
licensing datasheet -  
<https://aka.ms/mcaslicensing>

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 Discovery - included with Azure AD P1

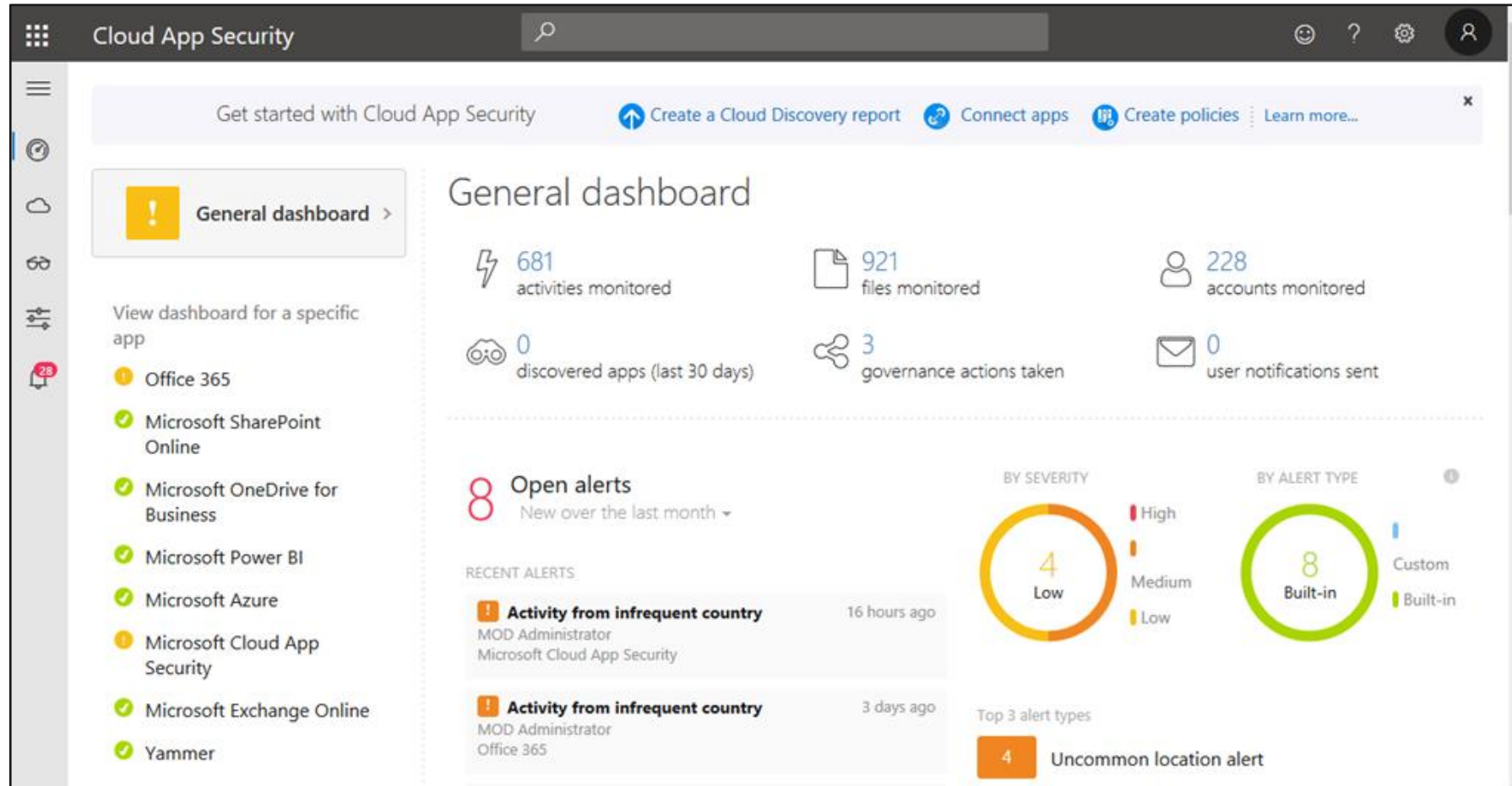


Office 365 Cloud App Security

\$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

 Office 365 Cloud App Security

Protect more cloud apps    




## Alerts




RESOLUTION STATUS

OPEN DISMISSED RESOLVED


CATEGORY

Select risk cat... 


SEVERITY


APP


Select apps... 

USER NAME

Select users... 

POLICY

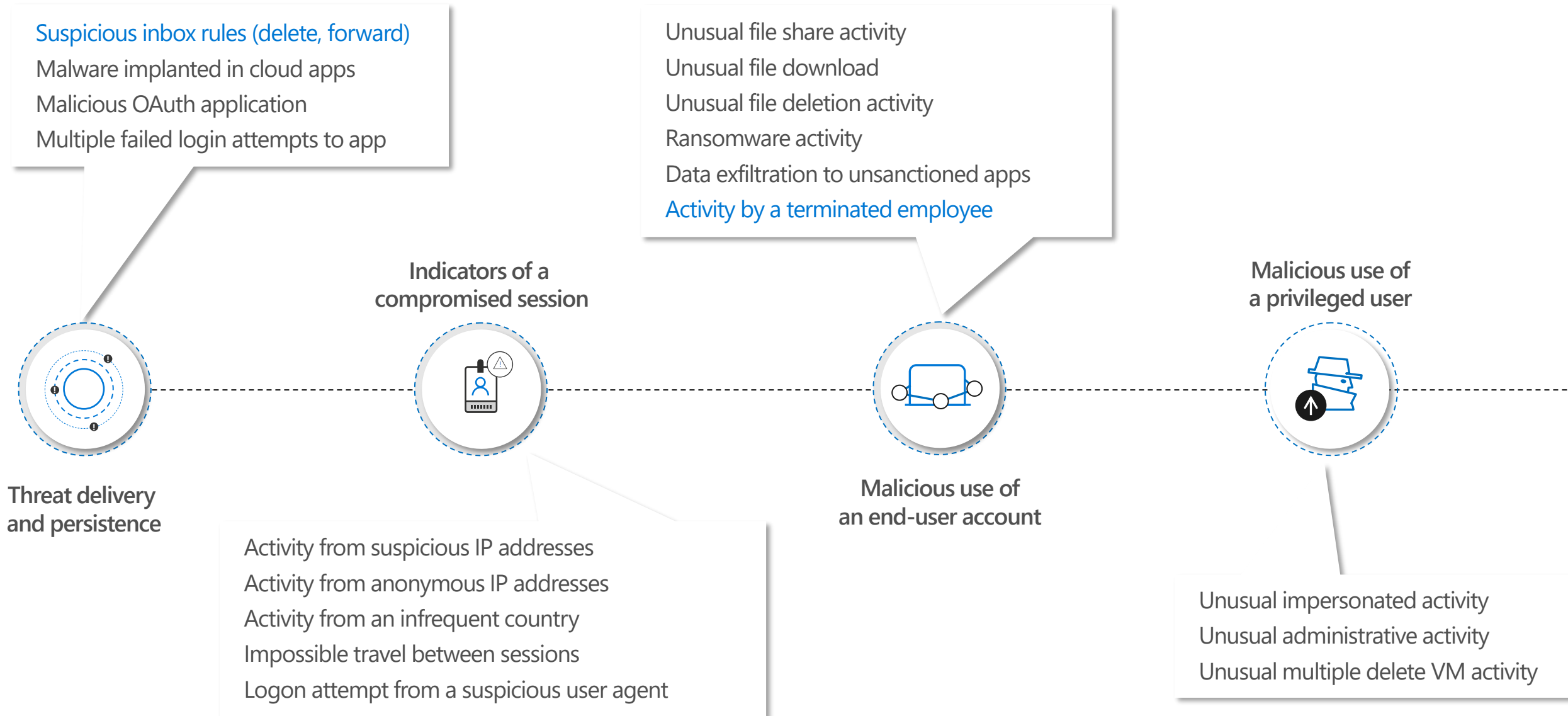
Select policy... 

Advanced 

Alerts  1 - 20 of 83 alerts   

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

# Microsoft Cloud App Security – Cross apps detections





# Policy Templates



340

## Policy templates



TYPE

SEVERITY

NAME

CATEGORY

Advanced

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

## Policies



NAME

TYPE

STATUS

SEVERITY

CATEGORY

Advanced


















Policy name...

Select type...

ACTIVE

DISABLED

Select risk category...

1 - 20 of 45 Policies					Create policy			
Policy	Count	Severity	Action	Modified				
<div></div> <div>Mass download by a single user</div> <div>Alert when a single user performs more than 50 downloads within 1 minute.</div>	0 open alerts	<div></div>	<div></div>	Nov 5, 2020				
<div></div> <div>Multiple failed user log on attempts to an app</div> <div>Alert when a single user attempts to log on to a single app, and fails more than 1...</div>	0 open alerts	<div></div>	<div></div>	Nov 5, 2020				
<div></div> <div>Logon from a risky IP address</div> <div>Alert when a user logs on to your sanctioned apps from a risky IP address. By def...</div>	0 open alerts	<div></div>	<div></div>	Nov 5, 2020				

# Alerts

## 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 ▼	
<div><div></div><div>Administrative activity from a non-corporate IP address</div><div>Administrative activity fro... Office 365 Robert Crane 20.190.142.179 Aust...</div></div>	OPEN	—	<div><div></div><div></div><div></div></div> High	11/25/20, 9:3...	
<div><div></div><div>Administrative activity from a non-corporate IP address</div><div>Administrative activity fro... Office 365 Robert Crane 20.190.142.178 Aust...</div></div>	OPEN	—	<div><div></div><div></div><div></div></div> High	11/25/20, 8:4...	
<div><div></div><div>Administrative activity from a non-corporate IP address</div><div>Administrative activity fro... Office 365 Robert Crane 20.190.142.179 Aust...</div></div>	OPEN	—	<div><div></div><div></div><div></div></div> High	11/25/20, 8:4...	

# Alerts - Detail

Office 365 Cloud App Security

Protect more cloud apps

P

340

Alerts >

Administrative activity from a non-corp...

11/25/20 9:37 PM

+50HIGH SEVERITY

Administrative activity from a non-corporate IP address

Office 365

Robert Crane

20.190.142.179

Australia

Resolution options:

Robert Crane

Close alert

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 ⓘInvestigate in Activity log

Activity	User	App	IP address	Location	Device	Date ▾
<div></div> Delete user: user 9f1f662c24...	Robert Crane	Office 365	20.190.142.179	Aus...	—	Nov 25, 2020... <div></div>

Users

1 - 1 of 1 users and accounts

User name	Investigation prior...	Type	Email	Apps	Groups	Last seen
<div></div> Robert Crane	360	User	admin@ciaops36...	<div></div>	Office 365 admini...	Nov 26, 2020, 4:25 ... <div></div>



## General Anomaly Detection 2 days ago

86%



Risk score

High severity



Microsoft Exchange Online



General Anomaly Detection



claudio@acme.com

Resolution options:



claudio@acme.com ▾

Dismiss...

Resolve alert... ▾

## Description

The user claudio@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 claudio@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

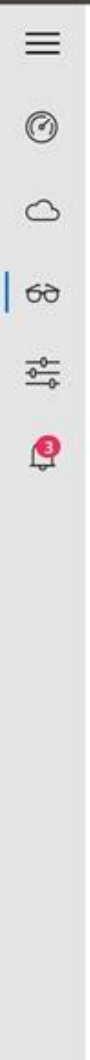
It is recommended to confirm the user is familiar with these actions.

## 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

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:...	



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: <a href="#">Jane Doe</a>	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="#">Exfil, Mailbox: ceo@securescorete...</a>	App: <a href="#">Microsoft Exchange Online</a>	Location: <a href="#">Russia, Moscow</a>
Matched policies: —	ISP: <a href="#">OOO Fishnet Communications</a>		

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

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](#)  
  
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:...





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 Fintnet 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

☰

☑

☁

🔍

⚙️

🔔 1K+

Cloud App Security

🔍

😊 ? ⚙️ 👤

Alerts > 🚨 Suspicious inbox forwarding 5 DAYS AGO

MEDIUM SEVERITY

📧 Microsoft Exchange Online

🔗 Suspicious inbox forwarding

📄 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@bablingdan.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


1K+

Cloud App Security

Alerts >  Activity by terminated user 2 MONTHS AGO

 Richard Munger

 Amazon Web Services - US

 Activity performed by terminated user

Resolution options: 

Richard Munger

Dismiss...

Resolve...









Description

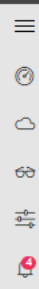
The user Richard Munger (richard@mcas-test9.com) performed an activity in Amazon Web Services (Amazon Web Services - US), after their Azure AD account was deleted.

Activity log

1 - 10 of 10 activities

Investigate in 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

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@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

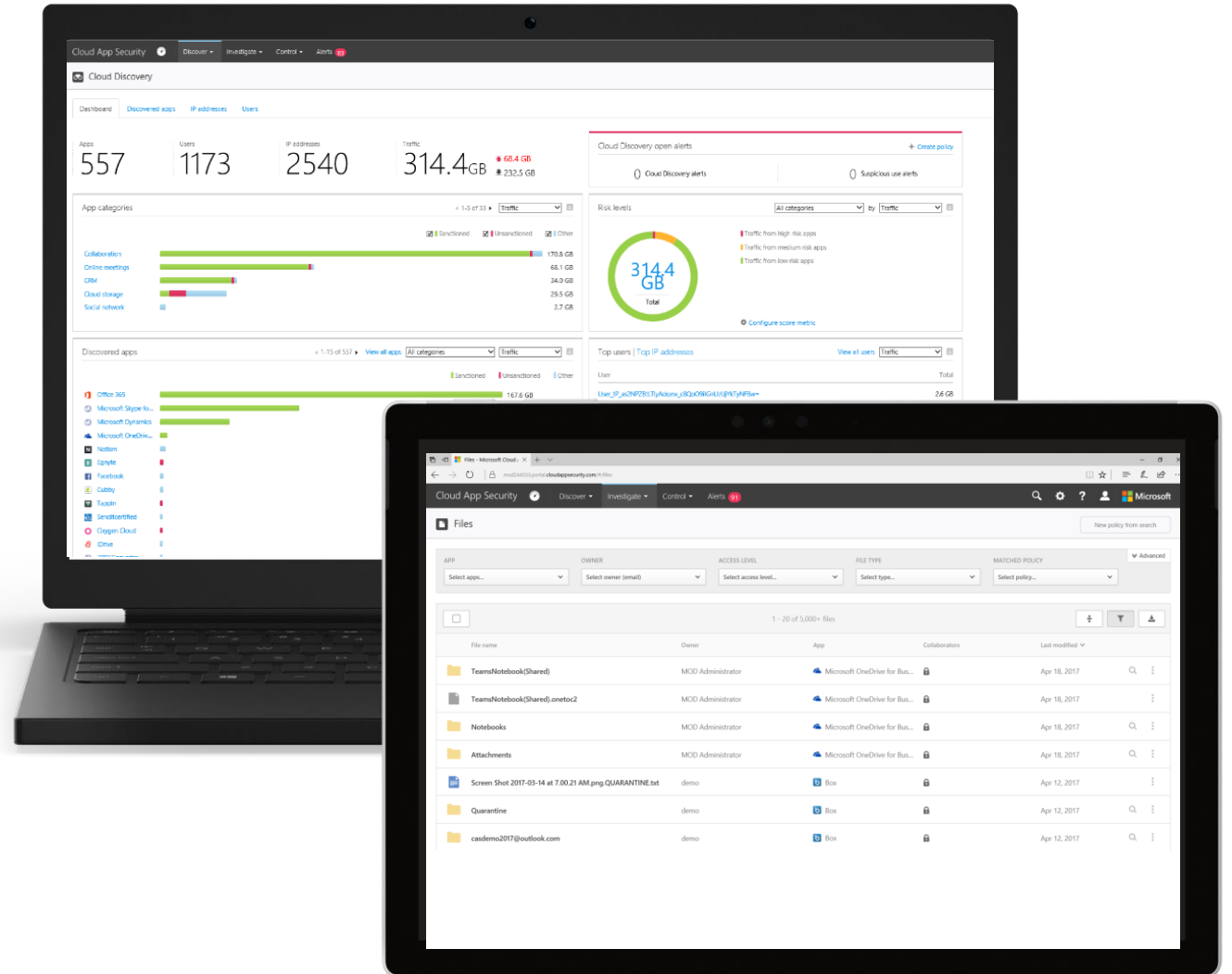
Identify how data – both classified and not classified – is shared across cloud apps and identify risk

## 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

