Microsoft

Microsoft Cloud App Security Proof of Concept

Prepared by:

Banu Jafarli

Program Manager Cloud and AI Security Engineering

Contributors:

Sebastien Molendijk

Program Manager II Cloud and AI Security Engineering

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

Table of Contents

Microsoft Cloud App Security Proof of Concept

This document provides guidelines to explore different features of Microsoft Cloud App Security in a Proof of Concept (PoC). This guide contains steps to deploy the various features and is intended to provide a demonstration of the functionalities of the product. The planned audience of this document are Security Administrators, IT Professionals, and System Integrators.

Environment

Choosing the proper environment is essential to the success of a PoC deployment. The following can be used:

1. Production: using actual Firewall logs, containing user data, and connecting to production SaaS applications.
2. Lab / Trial: using a temporary environment to evaluate the product or one of its features using Firewall logs in a test environment or test tenants of SaaS applications in use within the organization.

Due to the non-invasive way MCAS operates we recommend deploying it directly within a production environment. This will provide relevant and accurate results.

How to use this playbook?

1. Use this information to guide you and start your Proof of Concept deployment.
2. Scope the PoC by choosing the scenarios which align best with your business goals. We recommend as short and concise as possible to convey the value to the stakeholder, while minimizing the complexity.
3. Use the PoC Implementation section to understand the scenarios and what they mean for your environment. In each scenario, we describe how to set it up (what we call building blocks), and how to navigate.
4. Each building block explains the pre-requisites needed, as well as an approximate time to complete. This can help you during the planning process.
5. Based on 1-3 above, define the environment in which to execute. We encourage to strive for a production environment to get a good feel of the experience for your users.

Role Based Access Control

It's recommended to use either the Global Admin or Security Admin credentials throughout this PoC due to the role's full access to the product.

For more information on RBAC read the linked documentation.

PoC Implementation Scenarios

Foundation: Setting up the Microsoft Cloud App Security Portal

To start your PoC, your first step it to sign up for a Microsoft Cloud App Security tenant and set up the portal.

You can sign up by one of the following options:

- Requesting a free trial which can later be converted into a paid subscription
- Using an EMS E5 licensing package
- Standalone MCAS license

PoC Introduction

Theme / Scenarios overview

This guide contains instructions for five recommended scenarios and the general steps to get started in each. We encourage going through each scenario to fully understand the functionality and different use cases available within the product.

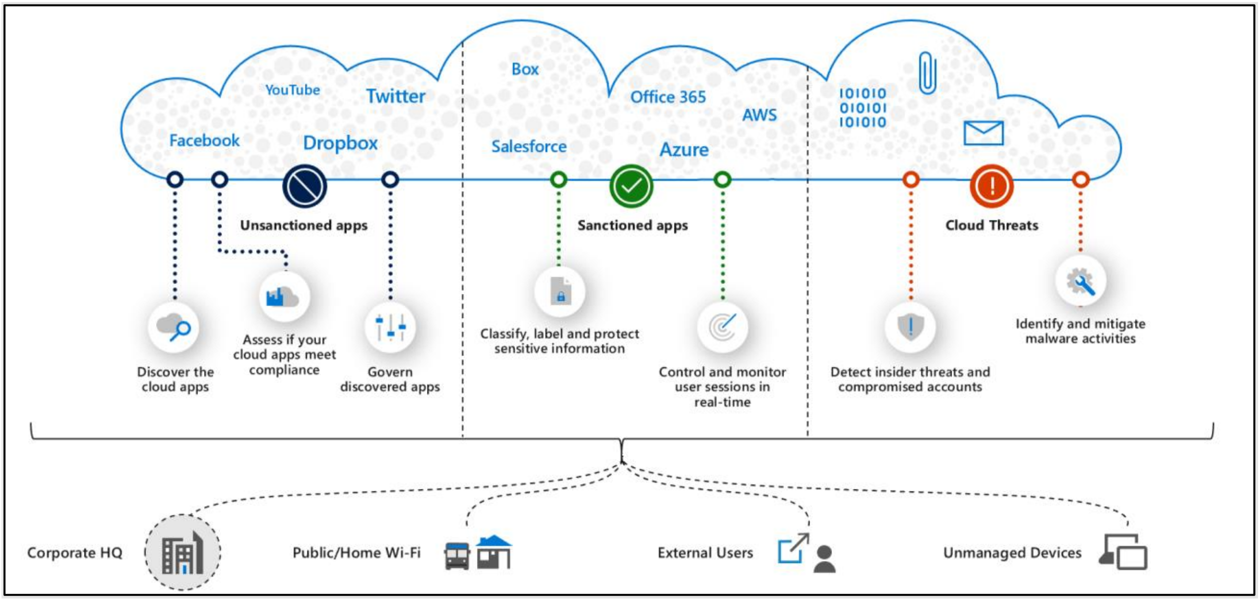
1. Discover Shadow IT
2. Protecting your files and data
3. Real-Time Monitoring and Control
4. Threat Protection
5. Cloud Access Security Broker (CASB) for Cloud Platforms

For Additional Microsoft Cloud App Security Resources review the following:

- Technical Documentation
- Tech Community
- MCAS Webinar
- Ignite Videos

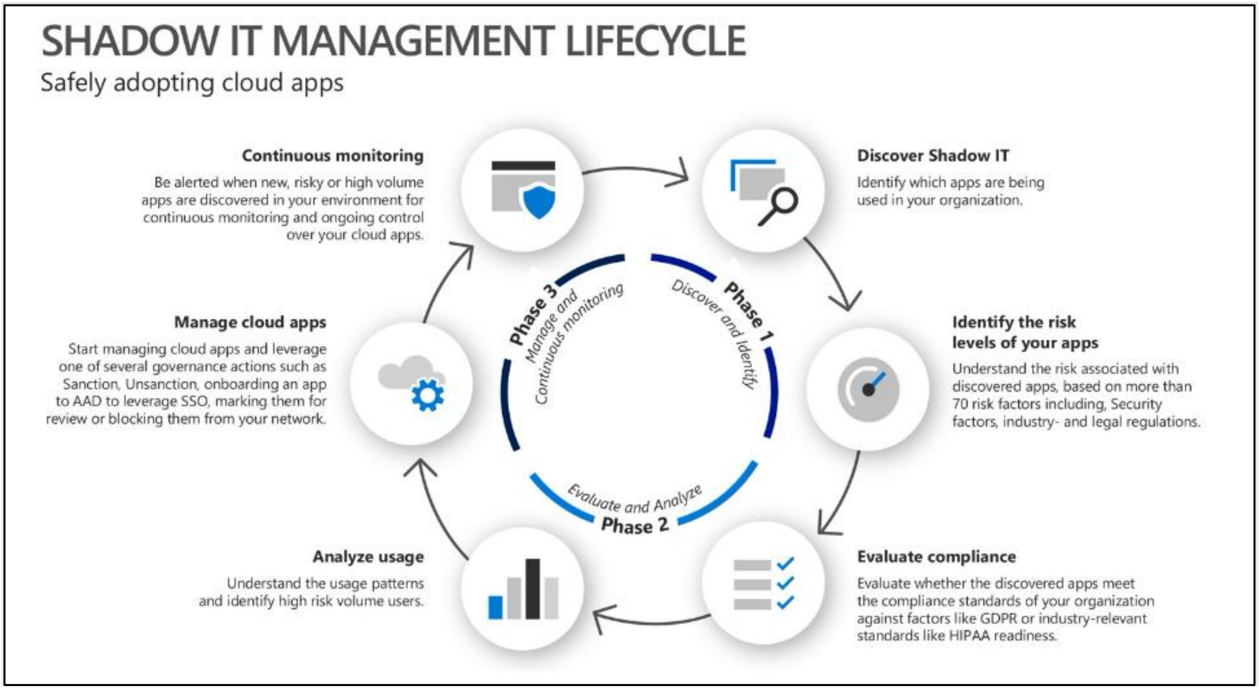
What is Microsoft Cloud App Security?

Microsoft Cloud App Security is Microsoft **CASB** (Cloud Access Security Broker) and is a critical component of the Microsoft Cloud Security stack. It's a comprehensive solution that can help your organization as you move to take full advantage of the promise of cloud applications but keeps you in control through improved visibility into activity. It also helps increase the protection of critical data across cloud applications (Microsoft **and** 3rd parties). With tools that help uncover shadow IT, assess risk, enforce policies, investigate activities, and stop threats, your organization can more safely move to the cloud while maintaining control of critical data.



Scenario 1: Discovery of Shadow IT

On average, more than 1,100 cloud applications are used by enterprises today, of which 61% are **not** sanctioned by IT. This results in duplicate capabilities, apps not meeting compliance standards or posing a security risk to the organization without any IT oversight. **Discovery** identifies cloud applications that you might not have visibility to, provides risk assessments and ongoing analytics and lifecycle management capabilities to control use. Cloud Discovery analyzes the traffic logs and runs it against the cloud app catalog; to provide information on the discovered applications and the users accessing them.


SHADOW IT MANAGEMENT LIFECYCLE
Safely adopting cloud apps
Phase 1
Discover and Identify
Phase 2
Evaluate and Analyze
Phase 3
Manage and Continuous monitoring

Continuous monitoring
Be alerted when new, risky or high volume apps are discovered in your environment for continuous monitoring and ongoing control over your cloud apps.

Discover Shadow IT
Identify which apps are being used in your organization.

Identify the risk levels of your apps
Understand the risk associated with discovered apps, based on more than 70 risk factors including, Security factors, industry- and legal regulations.

Evaluate compliance
Evaluate whether the discovered apps meet the compliance standards of your organization against factors like GDPR or industry-relevant standards like HIPAA readiness.

Analyze usage
Understand the usage patterns and identify high risk volume users.

Manage cloud apps
Start managing cloud apps and leverage one of several governance actions such as Sanction, Unsanction, onboarding an app to AAD to leverage SSO, marking them for review or blocking them from your network.

SnapShot Reports

Snapshot Reports are the manual method of uploading firewall traffic logs into Cloud App Security. This is a simple way to validate your log format and start viewing the Shadow IT capabilities of Discovery. You can upload batches of 20 logs of 1 GB max at a time and they will parse into their own separate report. Any discovery policies you create **will not** apply to a SnapShot report.

Follow the steps on this page to create your first snapshot report.

Once the SnapShot report is parsed you will be able to view the Cloud Discovery report. The report will give you visibility into the applications being used in your network and the users accessing them. The next step would be is to review the dashboard and understand the risk score behind each application.

Classifying Applications

Permissions: Compliance Admin should be reviewing this portion of the portal

Once you've reviewed which applications have been discovered - tag each app as sanctioned or unsanctioned.

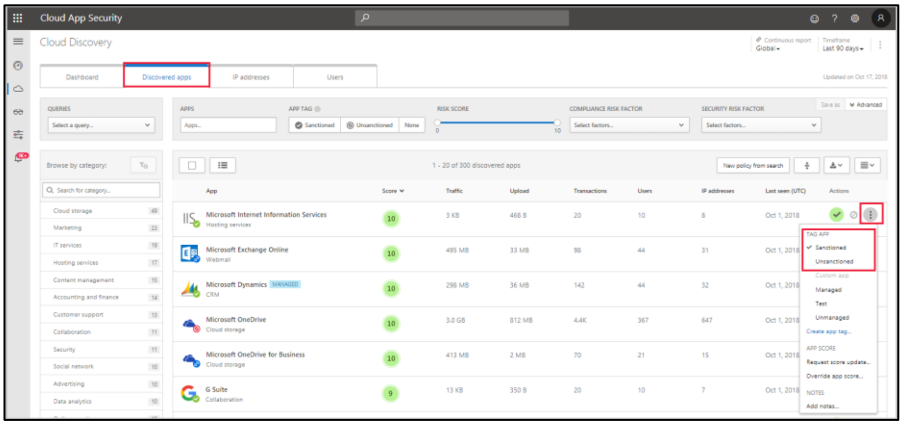
Sanctioned applications have been approved by your organization for use by users and unsanctioned apps have not. Once you find instance of applications that are unsanctioned - you can export a block script and block unsanctioned applications using your on-prem security appliances.

Example Scenario:

You identify that several users are watching Netflix when they're on your corporate network which is against corporate policy.

1. Un-Sanction the application in the MCAS portal

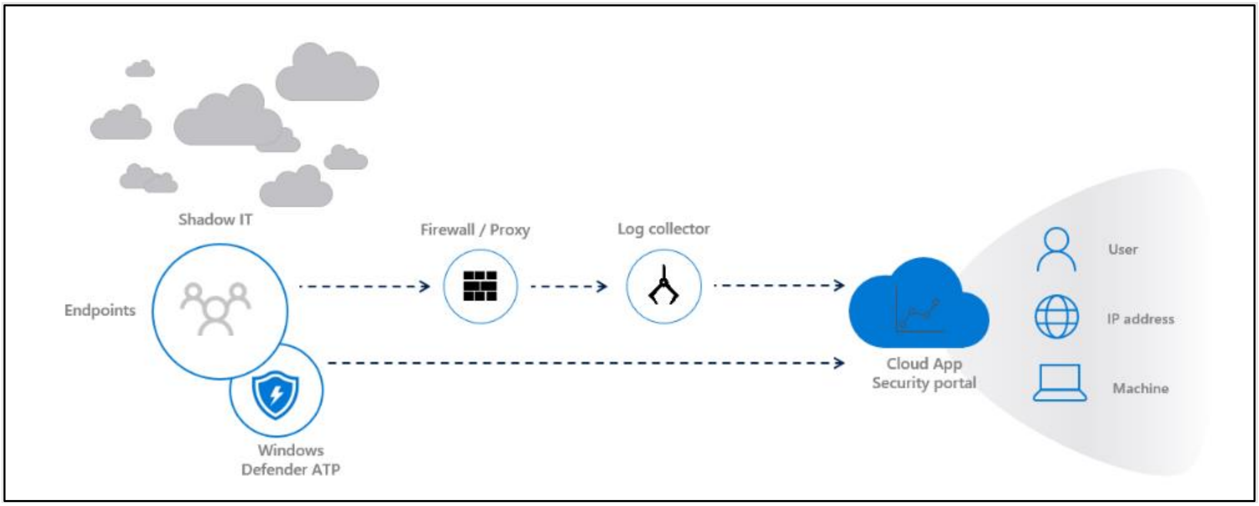
1.



App	Score	Traffic	Upload	Transactions	Users	IP addresses	Last seen (UTC)
Microsoft Internet Information Services Hosting services	10	3 KB	468 B	20	10	8	Oct 1, 2018
Microsoft Exchange Online Webmail	10	495 MB	33 MB	98	44	31	Oct 1, 2018
Microsoft Dynamics MANAGED CRM	10	298 MB	36 MB	142	44	32	Oct 1, 2018
Microsoft OneDrive Cloud storage	10	3.0 GB	812 MB	4.4K	367	647	Oct 1, 2018
Microsoft OneDrive for Business Cloud storage	10	413 MB	2 MB	70	21	15	Oct 1, 2018
G Suite Collaboration	9	13 KB	350 B	20	10	7	Oct 1, 2018

2. Generate a block script to your firewall appliance
3. Import the file your created appliance

Microsoft Defender ATP



Permissions: Global or Security Admin

To provide this visibility on Shadow IT and cloud apps usage, Cloud App Security can ingest and analyze network traffic from **Windows 10 1709 and above** clients within or **outside** the corporate network, using the Native integration with Windows Defender ATP. Identify a risky user or machine and able to see what applications are being used and do further investigation in the WDATP portal.

Turn on the integration with MDATP by following this link – the integration will give you additional information into Shadow IT taking place outside our corporate network. Once complete - create discovery policies for continuous monitoring and alerting.

Discovery Policies

Create cloud app discovery policies to give you the ability to get alerted when new apps are discovered that are either risky, non-compliant or trending.

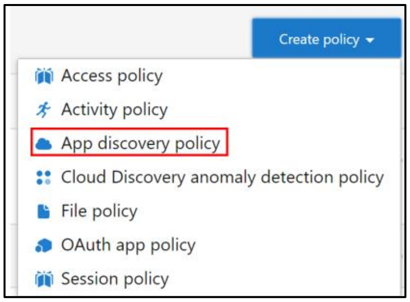
Start by using the built-in templates to create app discovery policies for risky and high volume apps. The configuration can be adjusted if needed.

- New high-volume app – alerts when new apps are discovered that have total daily traffic of more than 500 MB
- Risky app – alerts when new apps are discovered with risk score lower than 6 and that are used by more than 50 users with a total daily use of more than 50 MB

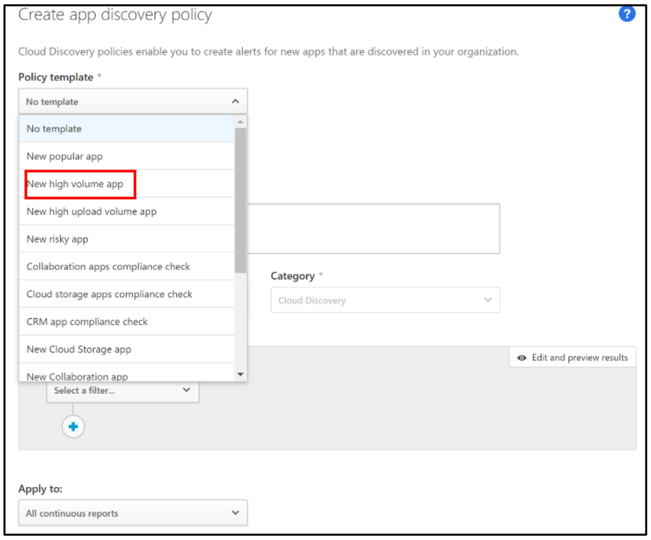
Once the policy is created, you will get notified when an application with high volume and high risk is discovered. This will allow to efficiently and continuously monitor applications in your network.

Creating an App Discovery Policy:

1. Go to the MCAS Portal
2. Click on Control and then Policies
3. Create Policy and pick App Discovery policy



4. Select the template for a New high-volume app



Create app discovery policy

Cloud Discovery policies enable you to create alerts for new apps that are discovered in your organization.

Policy template *

No template

Category *

Cloud Discovery

Apply to:

All continuous reports

5. Scroll down and Click Create

Note: Follow the same steps and choose 'Risky app' template in Step 4.

Scenario 2: Protecting your files and data

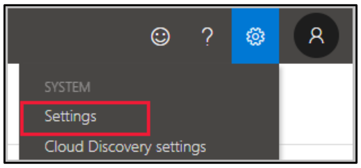
Integrate with Azure Information Protection

Permissions: Security Admin & have your information protection officer view this information and work together to come up with a governance plan

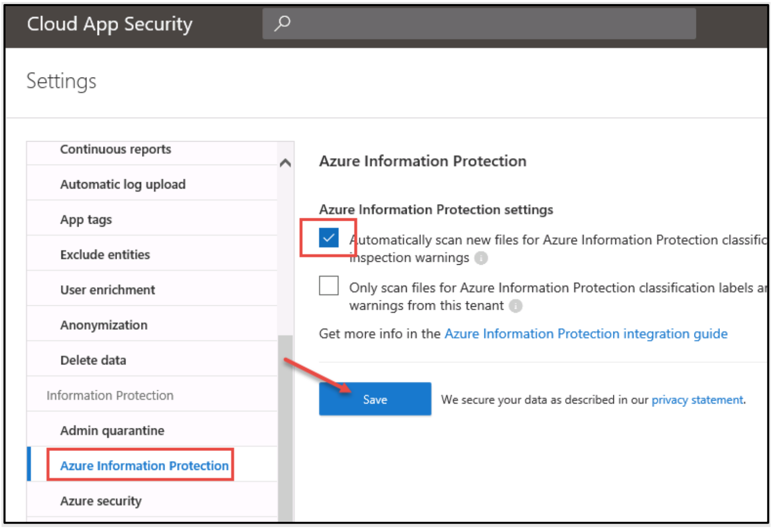
Note: To learn more about how to use AIP: https://aka.ms/aipdag. & Click here to learn how to create Azure Information Protection labels.

Once the integration is turned on you can apply labels as a governance action, view all files within the portal, create granular policies and investigate based on classification level.

1. Go to Settings in the MCAS Portal



2. Under Information Protection – Click on Azure Information Protection
    - Click on Automatically scan files for Azure Information Protection classification labels and content inspection warnings



Azure Information Protection

Azure Information Protection settings

☑ Automatically scan new files for Azure Information Protection classific inspection warnings

□ Only scan files for Azure Information Protection classification labels a warnings from this tenant

Get more info in the Azure Information Protection integration guide

We secure your data as described in our privacy statement.

Create File Policies

File policies are a great tool for finding threats to your information protection policies, for instance finding locations where users store sensitive information, credit card numbers and third-party ICAP files in your cloud. With Cloud App Security, not only can you detect these unwanted files stored in your cloud that leave you vulnerable, but you can take immediate action to stop them in their tracks and lock down the files that pose a threat. Using Admin quarantine, you can protect your files in the cloud and remediate problems, as well as prevent future leaks from occurring.

Use file policies to detect information sharing and scan for confidential information in your cloud applications.

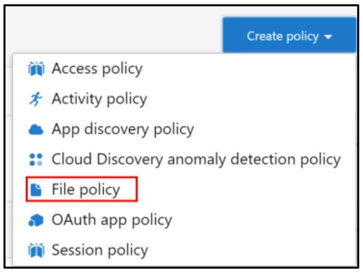
Create the following file policies to get visibility into how information is being used within your organization.

- File containing PII detected in the cloud (built-in DLP engine) - alert when a file containing personally identifiable information (PII) is detected by our built-in data loss prevention (DLP) engine in a sanctioned cloud app
- Files shared with unauthorized domains - alert when file is shared with an unauthorized domain (such as your competitor)
- File shared with personal email addresses - alert when a file is shared with a user's personal email address

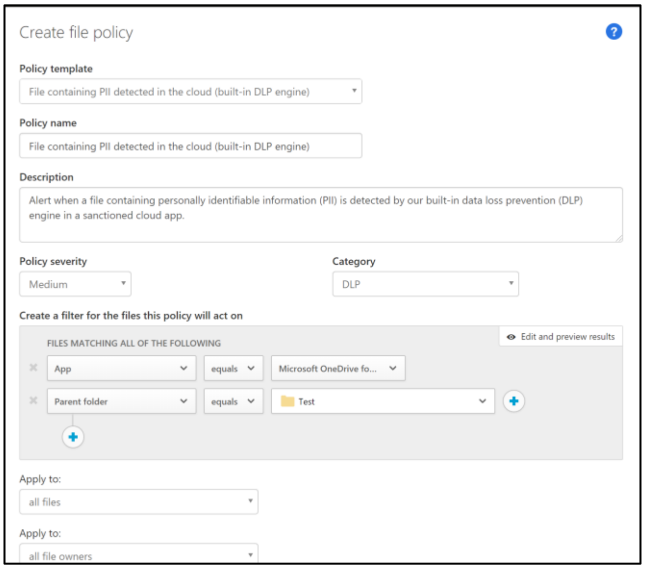
Use preset templates to start, review files in matched policies tab. Scope policies to a **single SharePoint/OneDrive site** to understand how the policies are working before adding additional applications or sites.

How to Create a File Policy:

1. Go to the MCAS Portal
2. Click on Control and then Policies
3. Create Policy and pick File Policy

2. 

4. Select the template for a File containing PII detected in the cloud (built-in DLP engine)
    - Scope it to down to SharePoint and OneDrive & Folder



Create file policy

Policy template

File containing PII detected in the cloud (built-in DLP engine)

Policy name

File containing PII detected in the cloud (built-in DLP engine)

Description

Alert when a file containing personally identifiable information (PII) is detected by our built-in data loss prevention (DLP) engine in a sanctioned cloud app.

Policy severity: Medium

Category: DLP

Create a filter for the files this policy will act on

FILES MATCHING ALL OF THE FOLLOWING

App equals Microsoft OneDrive fo...

Parent folder equals Test

Apply to: all files

Apply to: all file owners

5. Create

Follow the same steps and use the templates mentioned above in Step 4.

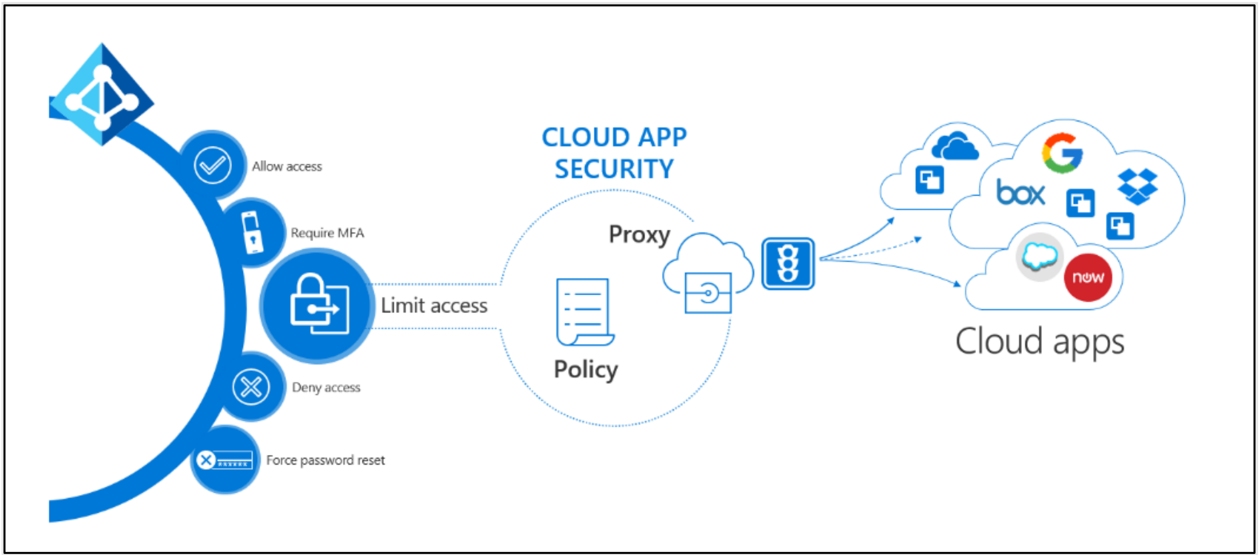
Note: Use the Data Classification Service for your inspection method.

Do not take any governance actions within the policy to avoid impact to the user.

For additional information about file policies follow this link.

Scenario 3: Real-Time Monitoring and Control

Permissions: Security Admin or Global Admin



Conditional access app control utilizes a reverse proxy architecture and is uniquely integrated with Azure AD's Conditional Access (CA). Azure AD Conditional Access allows you to enforce access controls on your organization's apps based on certain conditions. The conditions define the 'who' (for example a user, or group of users), the 'what' (which cloud apps) and the 'where' (which locations and networks) a conditional access policy is applied to. After you've determined the conditions, you can route users to the Microsoft Cloud App Security where you can protect data with Conditional Access App Control by applying access and session controls.

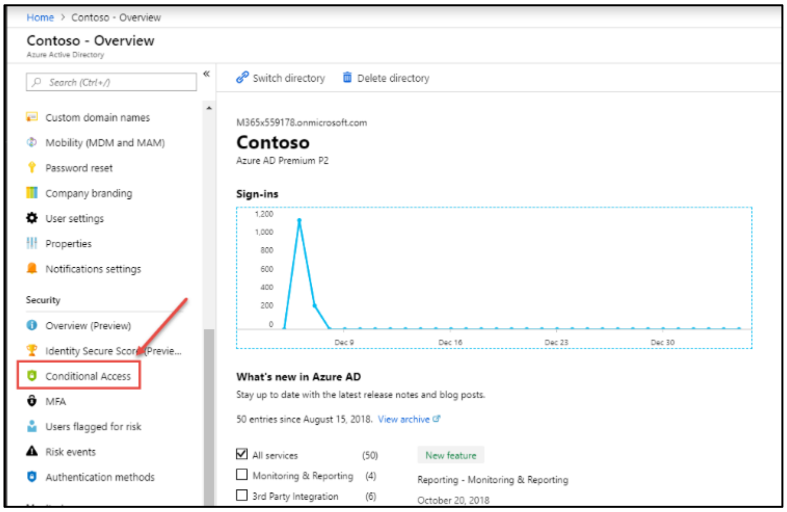
Conditional access app control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access policies are used for PC and mobile devices and session policies are used for browser sessions.

Access and Session policies give you the following capabilities:

- Block on download
- Protect on download
- Prevent documents copy/print
- Monitor low-trust sessions
- Block Access
- Create read-only mode
- Restrict user sessions from non-corporate network
- Block upload

Azure Portal - Azure Active Directory:

1. Go to Azure Active Directory (AAD) under Security, click on Conditional Access



M365x559178.onmicrosoft.com

Contoso

Azure AD Premium P2

What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

50 entries since August 15, 2018. View archive

☑ All services (50)

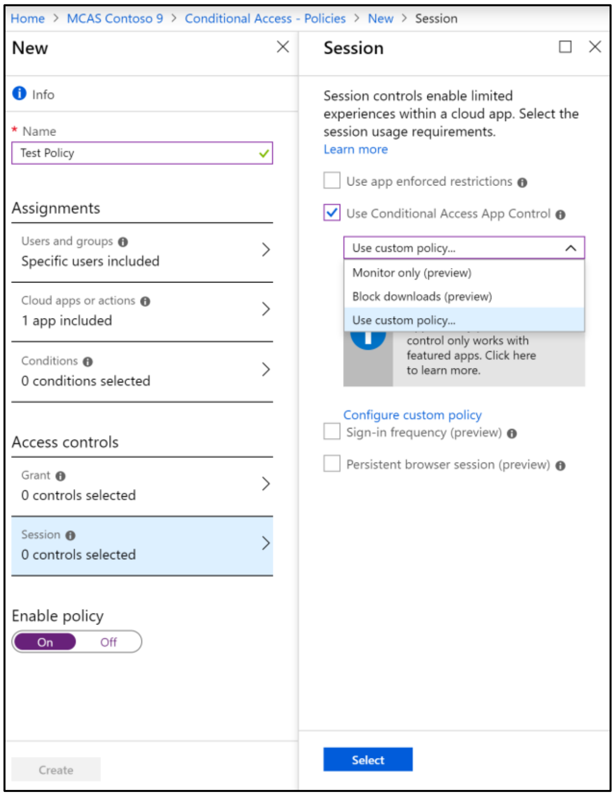
☐ Monitoring & Reporting (4)

☐ 3rd Party Integration (6)

Reporting - Monitoring & Reporting

October 20, 2018

2. Create a Policy within AAD to enable Conditional Apps
3. Assign a ***test*** user group and assign one Cloud App (SharePoint or 3rd party app that's SSO configured) to get started during testing
4. Click on Session and click on 'Use Conditional Access App Control"
5. Select "Use custom policy" which will route the session through MCAS


Home > MCAS Contoso 9 > Conditional Access - Policies > New > Session
New
Session
Info
Create
Select

* Name: Test Policy

Assignments

Users and groups: Specific users included

Cloud apps or actions: 1 app included

Conditions: 0 conditions selected

Access controls

Grant: 0 controls selected

Session: 0 controls selected

Enable policy: On Off

Session controls enable limited experiences within a cloud app. Select the session usage requirements. Learn more

☐ Use app enforced restrictions

☑ Use Conditional Access App Control

Use custom policy...

- Monitor only (preview)
- Block downloads (preview)
- Use custom policy...

control only works with featured apps. Click here to learn more.

Configure custom policy

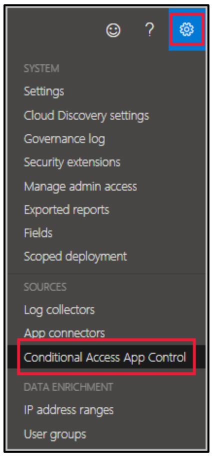
☐ Sign-in frequency (preview)

☐ Persistent browser session (preview)

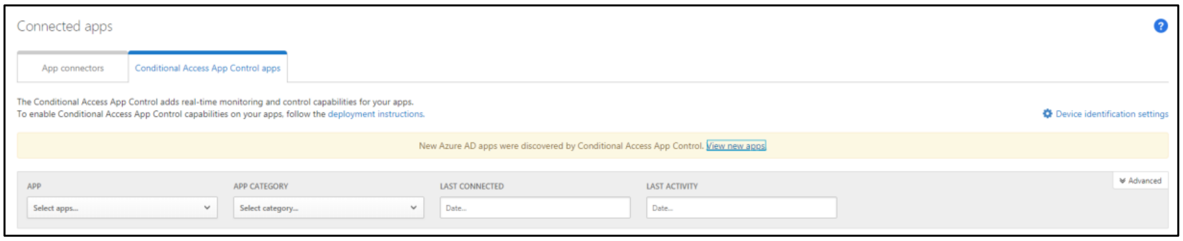
6. Once you created the policy, make sure to log out of each configured app and log back in

Microsoft Cloud App Security Portal:

7. Log back into the CAS portal, go into Settings and click on Conditional Access App Control



8. The configured applications should show up in the portal as Conditional Access App Control apps



The Conditional Access App Control adds real-time monitoring and control capabilities for your apps.
To enable Conditional Access App Control capabilities on your apps, follow the deployment instructions.

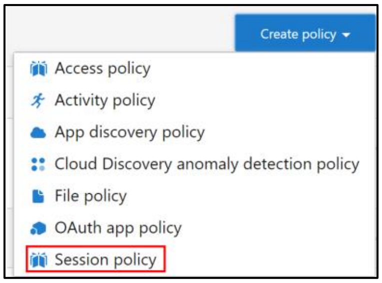
New Azure AD apps were discovered by Conditional Access App Control. View new apps

Creating a Session Policy:

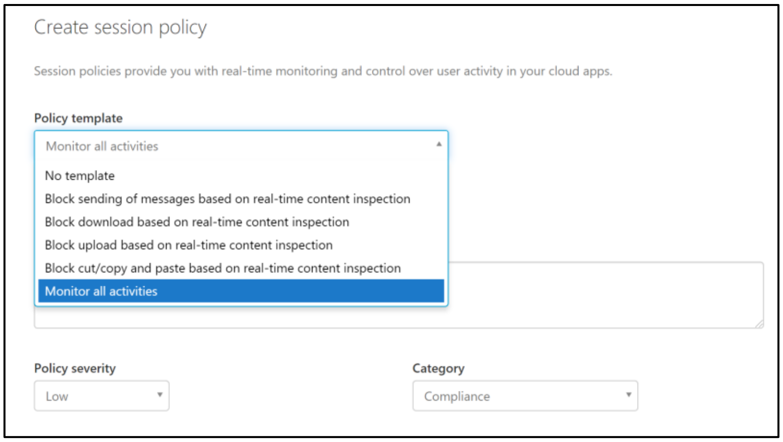
For this PoC, we'll be creating a session policy using a template to monitor all activities to get started.

Create additional policies using the preset templates to test the different controls available.

1. Go to the MCAS Portal
2. Click on Control and then Policies
3. Create Policy and pick Session Policy



4. Select the template to Monitor all activities



Create session policy

Session policies provide you with real-time monitoring and control over user activity in your cloud apps.

Policy template

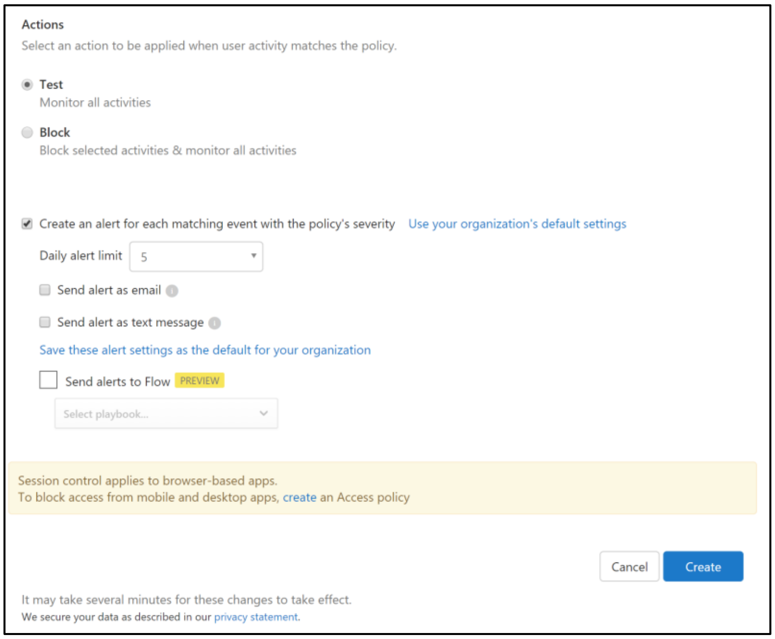
Monitor all activities

- No template
- Block sending of messages based on real-time content inspection
- Block download based on real-time content inspection
- Block upload based on real-time content inspection
- Block cut/copy and paste based on real-time content inspection
- Monitor all activities

Policy severity: Low

Category: Compliance

5. Click Create



Actions

Select an action to be applied when user activity matches the policy.

● Test
Monitor all activities

○ Block
Block selected activities & monitor all activities

☑ Create an alert for each matching event with the policy's severity 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

☐ Send alerts to Flow PREVIEW

Select playbook...

Session control applies to browser-based apps.
To block access from mobile and desktop apps, create an Access policy

It may take several minutes for these changes to take effect.
We secure your data as described in our privacy statement.

Scenario 4: Threat Protection

Permissions: Global Admin, Security Admin or User Group Admin

Creating an activity policy can help you detect malicious use of an end-user or privileged account or an indication of a possible compromised session.

Creating Activity Policies

Follow this link to learn more about activity policies.

- Mass download by a single user – this policy will give you visibility into possible data exfiltration
  - *By default, this policy will also alert on OneDrive client syncs*
- Multiple failed user logon attempts to an app – possible brute force attack or compromised account
- Login from a risky IP Address - possible compromised account
- Potential ransomware activity - alert when a user uploads files to the cloud that might be infected with ransomware

Malware Detection

This detection identifies malicious files in your cloud storage, whether they're from your Microsoft apps or third-party apps. Microsoft Cloud App Security uses Microsoft's threat intelligence to recognize whether certain files are associated with known malware attacks and are potentially malicious. This built-in policy is disabled by default. Not every file is scanned, but heuristics are used to look for files that are potentially risky. After files are detected, you can then see a list of **Infected files**. Click on the malware file name in the file drawer to open a malware report that provides you with information about that type of malware the file is infected with.

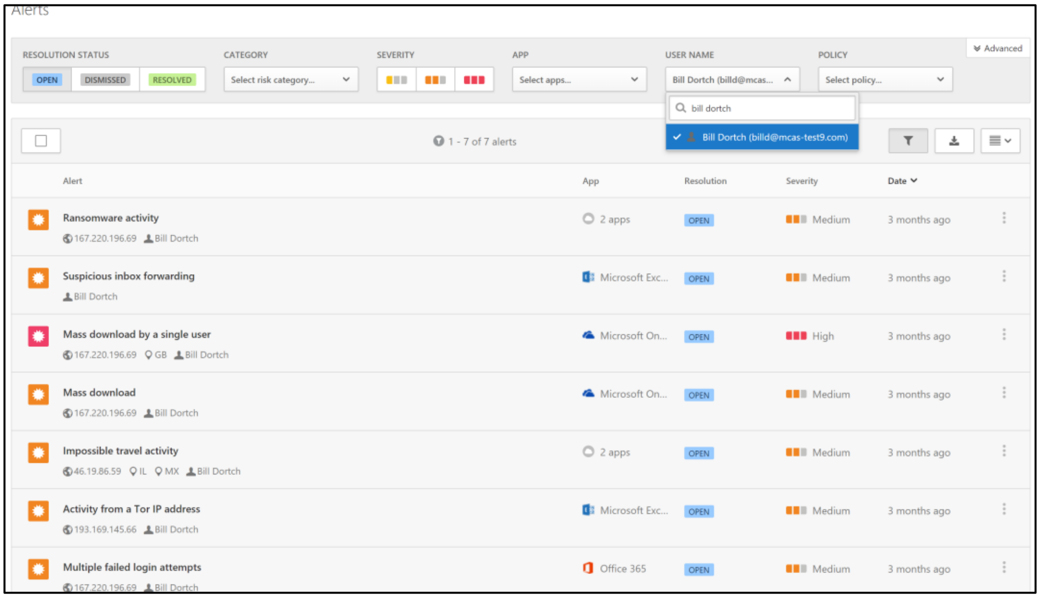
Malware detection is disabled by default. Make sure to enable it to get alerted on possible infected files.

Investigating and Remediating Alerts

Investigate and determine the nature of the violation associated with the alert. Try to understand if it's a serious, questionable violation or anomalous behavior for the user. Investigate further by looking at the description of the alert and what triggered as well as looking at similar activities.

If you dismiss alerts, it's important to understand why they are of no importance or if it's a false positive. If there is too much noise coming in, be sure to review and tune the policy triggering the alert.

1. In the MCAS Portal – Go to Alerts



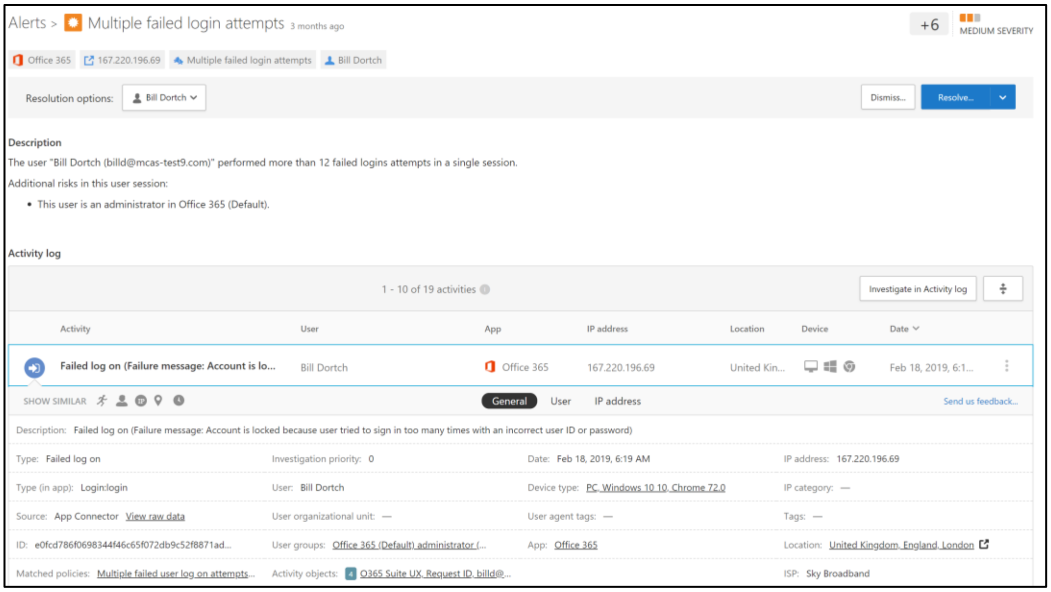
Alert	App	Resolution	Severity	Date
Ransomware activity 167.220.196.69 Bill Dortch	2 apps	OPEN	Medium	3 months ago
Suspicious inbox forwarding Bill Dortch	Microsoft Exc...	OPEN	Medium	3 months ago
Mass download by a single user 167.220.196.69 GB Bill Dortch	Microsoft On...	OPEN	High	3 months ago
Mass download 167.220.196.69 Bill Dortch	Microsoft On...	OPEN	Medium	3 months ago
Impossible travel activity 46.19.86.59 IL MX Bill Dortch	2 apps	OPEN	Medium	3 months ago
Activity from a Tor IP address 193.169.145.66 Bill Dortch	Microsoft Exc...	OPEN	Medium	3 months ago
Multiple failed login attempts 167.220.196.69 Bill Dortch	Office 365	OPEN	Medium	3 months ago

2. Click on an Alert you'd like to investigate

   In this example we're investigating a single user who had multiple failed login attempts which could be a sign of brute force and a compromised identity.

3. Read the description of the alert and look at the details provided to see if anything looks suspicious.

   We see that this user is an admin and has had over 12 failed logins. There is a chance that an attacker is trying to compromise this account.



Alerts > Multiple failed login attempts 3 months ago
+6
MEDIUM SEVERITY
Office 365
167.220.196.69
Multiple failed login attempts
Bill Dortch
Resolution options:
Bill Dortch
Dismiss...
Resolve...

Description

The user "Bill Dortch (billd@mcas-test9.com)" performed more than 12 failed logins attempts in a single session.

Additional risks in this user session:

- This user is an administrator in Office 365 (Default).

Activity log

1 - 10 of 19 activities

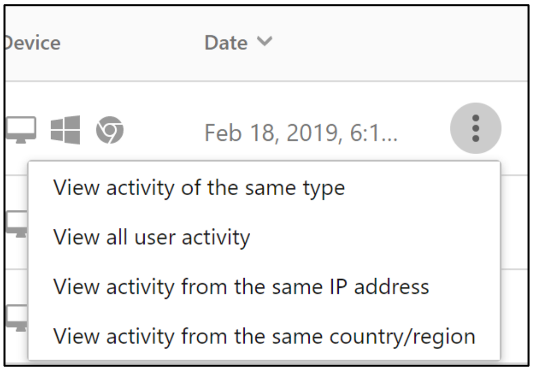
Investigate in Activity log

Activity	User	App	IP address	Location	Device	Date
Failed log on (Failure message: Account is lo...	Bill Dortch	Office 365	167.220.196.69	United Kin...		Feb 18, 2019, 6:1...

Description: Failed log on (Failure message: Account is locked because user tried to sign in too many times with an incorrect user ID or password)

Type: Failed log on	Investigation priority: 0	Date: Feb 18, 2019, 6:19 AM	IP address: 167.220.196.69
Type (in app): Login:login	User: Bill Dortch	Device type: PC, Windows 10 10, Chrome 72.0	IP category: —
Source: App Connector View raw data	User organizational unit: —	User agent tags: —	Tags: —
ID: e0fcd786f0698344f46c65f072db9c52f8871ad...	User groups: Office 365 (Default) administrator (...	App: Office 365	Location: United Kingdom, England, London
Matched policies: Multiple failed user log on attempts...	Activity objects: 4 O365 Suite UX, Request ID, billd@...		ISP: Sky Broadband

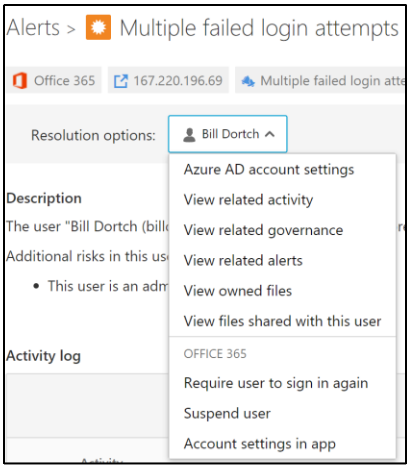
4. Click to on 'View all user activity' to view activities by this user for additional information for your investigation process.



Device
Date
Feb 18, 2019, 6:1...
View activity of the same type
View all user activity
View activity from the same IP address
View activity from the same country/region

5. If we look at the captured images in Step 1 and Step 3. We can see that he's an admin whose account has been compromised. We're able to make that conclusion by seeing that he had multiple failed logins from a TOR IP address and tried to exfiltrate data by his mass download alert.

6. Now that we have enough information to infer that the alert is true. We can resolve the alert by the options available to us. In this case, the best approach would be to **suspend the user** since his account is compromised.

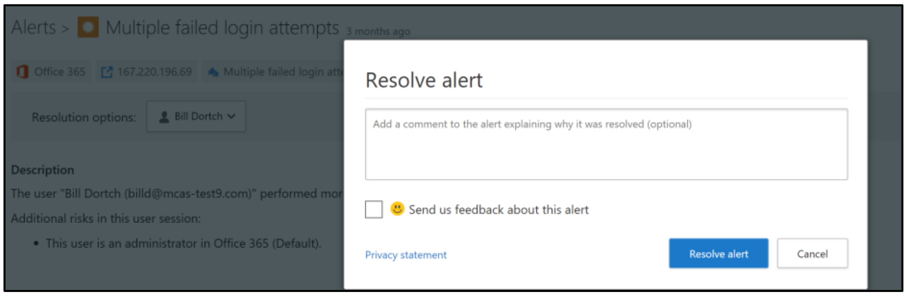


The user "Bill Dortch (bill

Additional risks in this us

- This user is an adm

7. Click on Resolve and write how you resolved the alert


Alerts > Multiple failed login attempts 3 months ago
Office 365
167.220.196.69
Multiple failed login att
Resolution options:
Bill Dortch
Description
Resolve alert
Add a comment to the alert explaining why it was resolved (optional)
□ Send us feedback about this alert
Privacy statement
Resolve alert
Cancel

The user "Bill Dortch (billd@mcas-test9.com)" performed mor

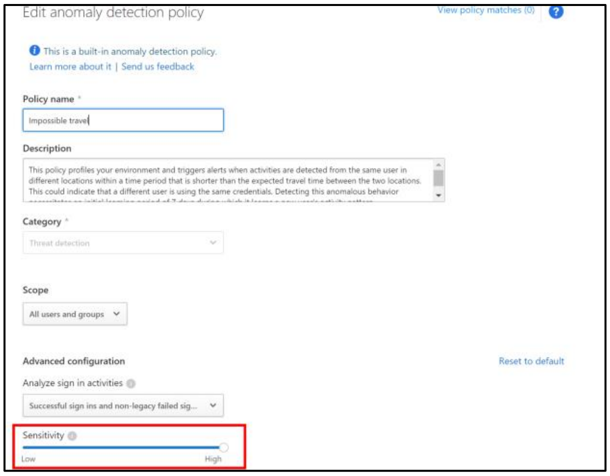
Additional risks in this user session:

- This user is an administrator in Office 365 (Default).

Reducing False Positives

Anomaly detection policies are triggered when they are unusual behaviors performed by the users in your environment. Microsoft Cloud App Security has a learning period where it uses entity behavioral analytics as well as machine learning to understand the "normal" behavior of your users.

Use the sensitivity slider to decide the sensitivity of that policy in addition to scoping specific policies for a given group only.



Edit anomaly detection policy

View policy matches (0)

This is a built-in anomaly detection policy.
Learn more about it | Send us feedback

Policy name *

Impossible travel

Description

This policy profiles your environment and triggers alerts when activities are detected from the same user in different locations within a time period that is shorter than the expected travel time between the two locations. This could indicate that a different user is using the same credentials. Detecting this anomalous behavior

Category *

Threat detection

Scope

All users and groups

Advanced configuration

Reset to default

Analyze sign in activities

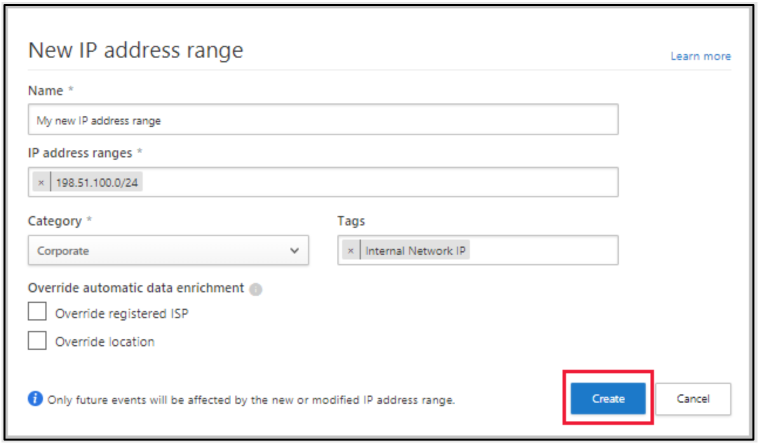
Successful sign ins and non-legacy failed sig...

Sensitivity

As an example, to reduce the number of false positives within the impossible travel alert you can set the sensitivity slider to low. If you have users in your organization that are frequent corporate travelers, you can add them to a user group and select that group in the scope of the policy.

Add your corporate IP Address and VPN ranges, you will see less alerts in relation to impossible travel and infrequent country.

1. Click on Settings followed by IP Address ranges
2. Name the range
3. Enter the IP address range
4. Select a Category
5. Add a tag to tag specific activities from this range



New IP address range

Learn more

Name *

My new IP address range

IP address ranges *

× 198.51.100.0/24

Category *

Corporate

Tags

× Internal Network IP

Override automatic data enrichment

□ Override registered ISP

□ Override location

Only future events will be affected by the new or modified IP address range.

Oauth Applications

These are the applications that installed by business users in your organization request permission to access user information and data and sign in on behalf of the user in other cloud apps, such as Office 365, G Suite and Salesforce. When users install these apps, they often click accept without closely reviewing the details in the prompt, including granting permissions to the app.

You'll have the capability to ban and revoke access to these apps.

Many users grant access to their Office 365, G-Suite and Salesforce corporate accounts when trying to access an Oauth applications. The issue that rises is that IT has usually has no visibility into these applications or what the risk level associated is.

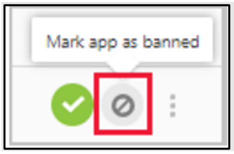
Cloud App Security gives you the capability to discover the Oauth applications your users have installed and which corporate account they're using to login. Once you discover which Oauth apps are being used by which account, you can allow or ban access right in the portal.

Manage Oauth Apps

The Oauth page contains information regarding which applications your users are granting access to using their corporate Office 365, Salesforce and G-Suite credentials.

Ban or approve and app:

1. Go to the Microsoft Cloud App Security Portal -> Click on Investigate -> Click on Oauth Apps
2. Click on the App Drawer to view additional information on each application and the permission that was granted
3. You can ban or approve the app by clicking either the approve or ban icon

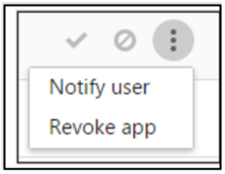


Note: If you decide to ban an app, you can notify the user that the app they installed and provided permissions to is banned and can add a custom notification message.

Revoke App

This functionality is only available for G-Suite and Salesforce connected applications.

1. On the Oauth apps page -> click on the three dots to the very right of the app row
2. Click on Revoke app



OAuth Polices

Oauth policies notify you when an Oauth app is discovered that meets a specific criteria.

Follow this link on directions to create OAuth app policies.

Scenario 5: CASB for Cloud Platforms

Permissions: Global Admin

Note: The Azure AD Global role doesn't automatically provide privileged users with access to Azure subscriptions.

Elevate permissions to privileged users to add your Azure subscriptions – after you add the subscriptions make sure to disable the elevation.

To improve your cloud security posture, add your azure subscriptions into Cloud App Security; the integration with Azure Security Center will notify you when there are missing configurations and security controls. You'll be able to identify anomalies in your environment and pivot to the Azure Security portal to apply these recommendations and solve for vulnerabilities.

To learn more about the integration with Azure Security Center click here.

Conclusion

At the end of this PoC you should have an understanding about the shadow IT, information protection, real-time monitoring and threat protection capabilities of Microsoft Cloud App Security.

The scenarios in this PoC showcase the following:

I. Shadow IT - Visibility into the use of SaaS applications across your organization and risk level associated with each application in use

II. Protecting your files and data – Identifying files that contain sensitive information and who has access to them and taking the right steps to stay protected

III. Real-Time Monitoring and Control – Understanding how to control and block access in real-time without losing productivity

IV. Threat Protection – Being able to detect threats and how to customize policies to get alerted on what's critical to your organization and investigate accordingly

V. CASB for Cloud Platforms – Improving your cloud security posture by leveraging Azure Security Center

Please head over to our TechCommunity for additional resources and questions about Microsoft Cloud App Security.