



Emiliano Iacomino

Security, Compliance and Identity

Digital Technical Specialist

[Emiliano.Iacomino@microsoft.com](mailto:Emiliano.Iacomino@microsoft.com)

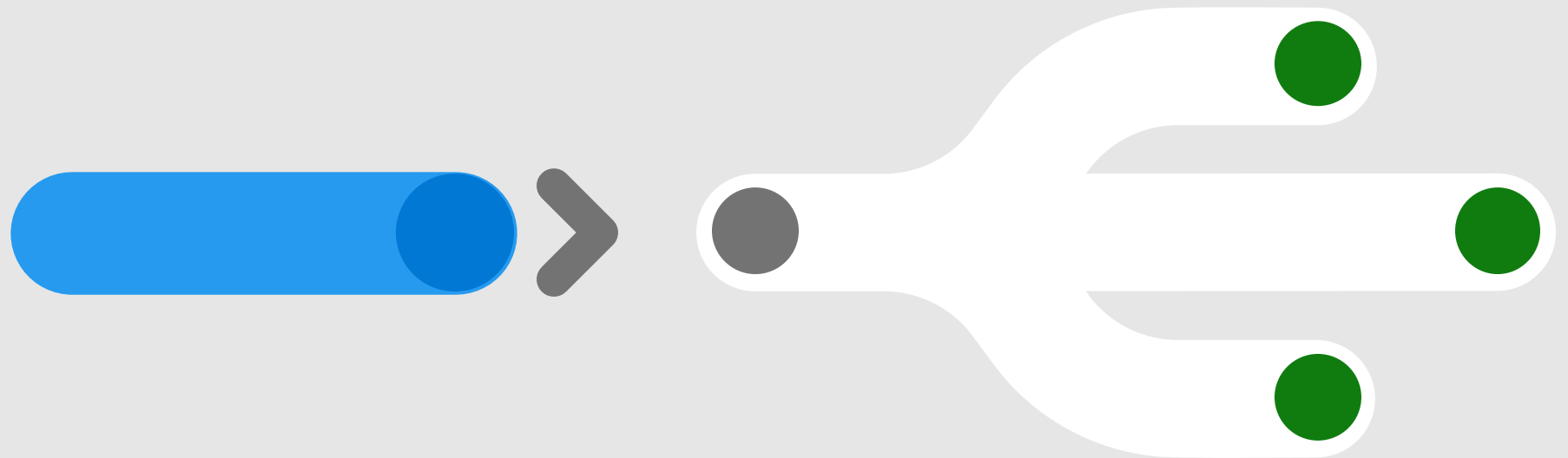


Pacho Baratta

Marketing Manager e Solutions Architect

[p.baratta@yooda.tech](mailto:p.baratta@yooda.tech)

# Defender for Cloud Apps: casi d'uso e funzionalita'

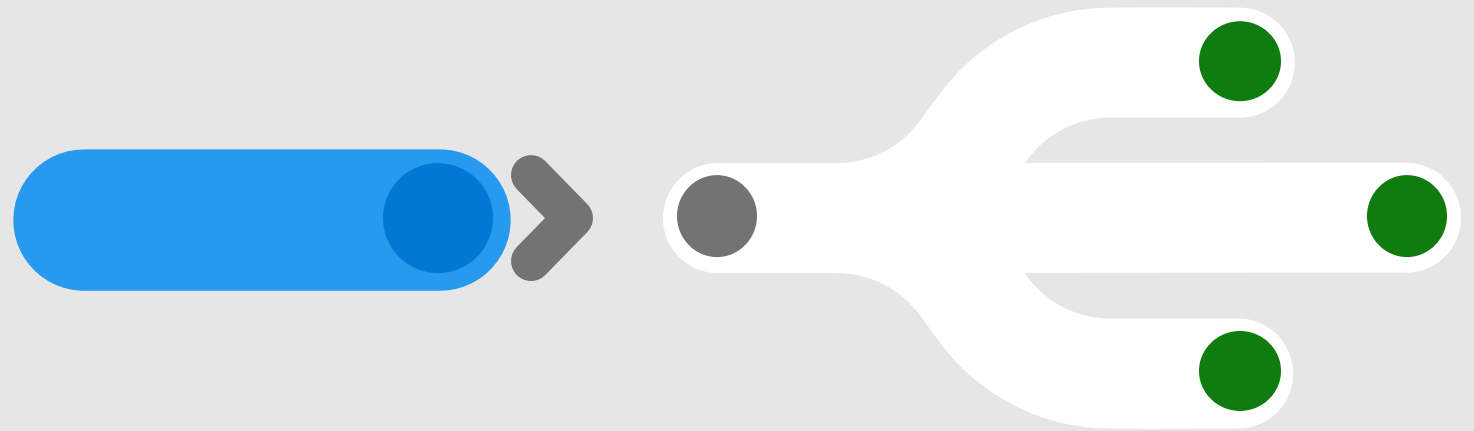


# Table of contents

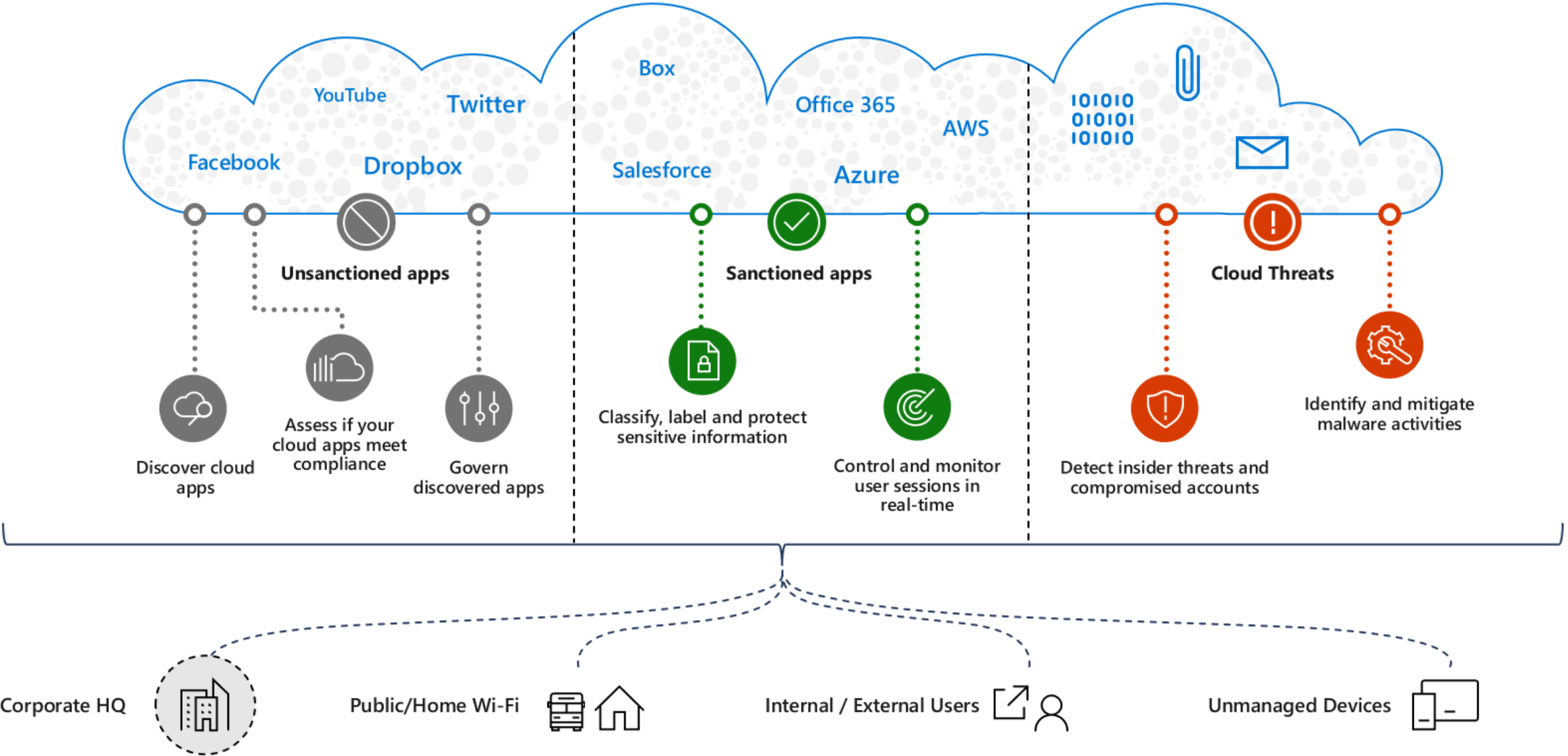
- 01 Introduction to Cloud Access Security Brokers
- 02 Shadow IT Discovery and Control
- 03 Secure Access to your apps
- 04 Information Protection
- 05 Threat Protection for your cloud environment
- 06 Security Posture Management
- 07 Summary and next steps

01

# Introduction to Cloud Access Security Brokers



# Top CASB use cases



# Defender for Cloud Apps provides comprehensive session security and data use policies

## Cloud platforms



## Native integrations

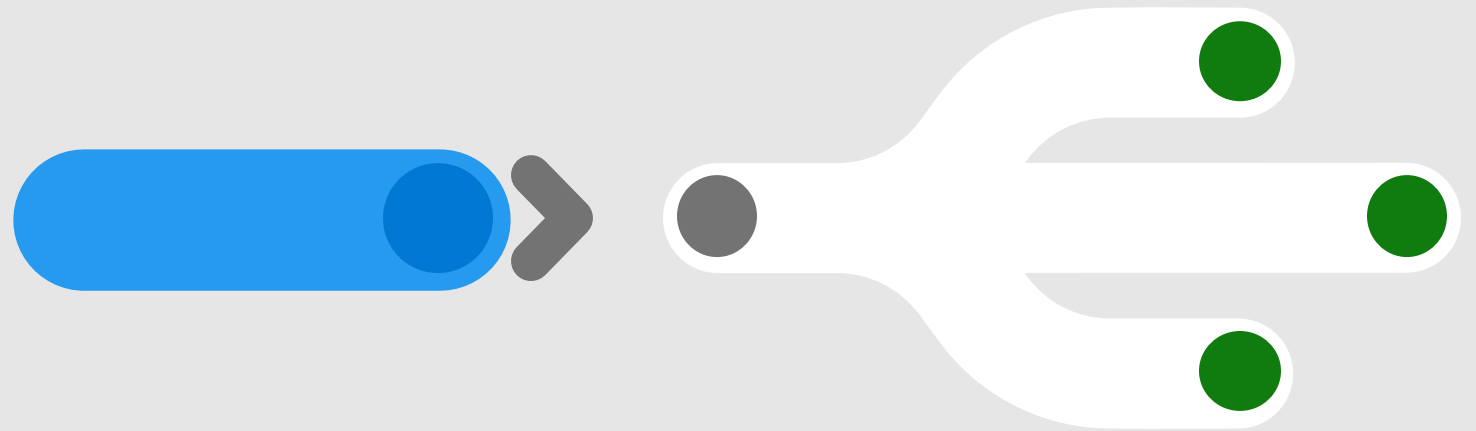


## 17,000+ supported apps



02

## Shadow IT Discovery and Control



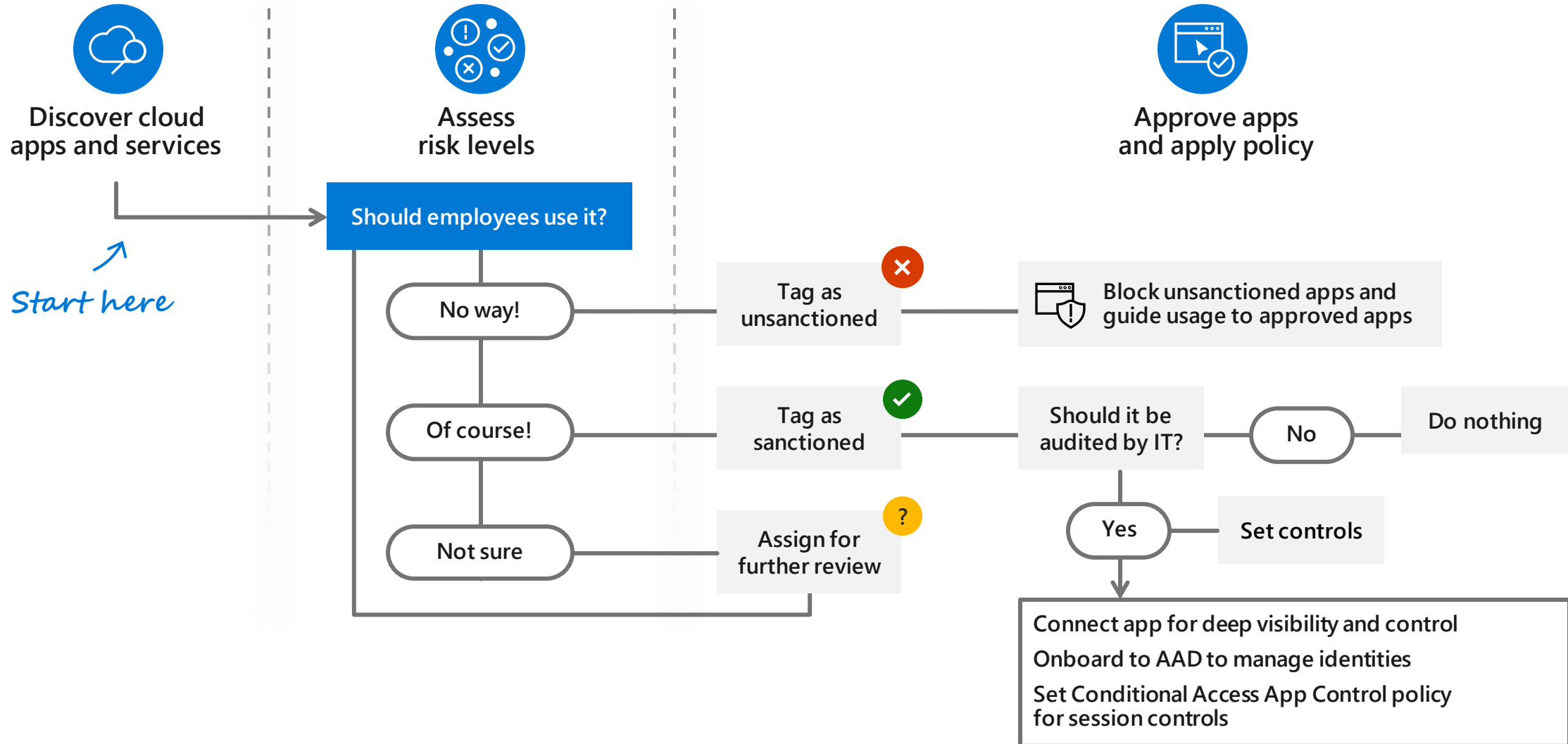


Shadow IT discovery identifies cloud apps, provides risk assessments, usage analytics and app lifecycle management and control capabilities.



# Discover and control apps in your environment

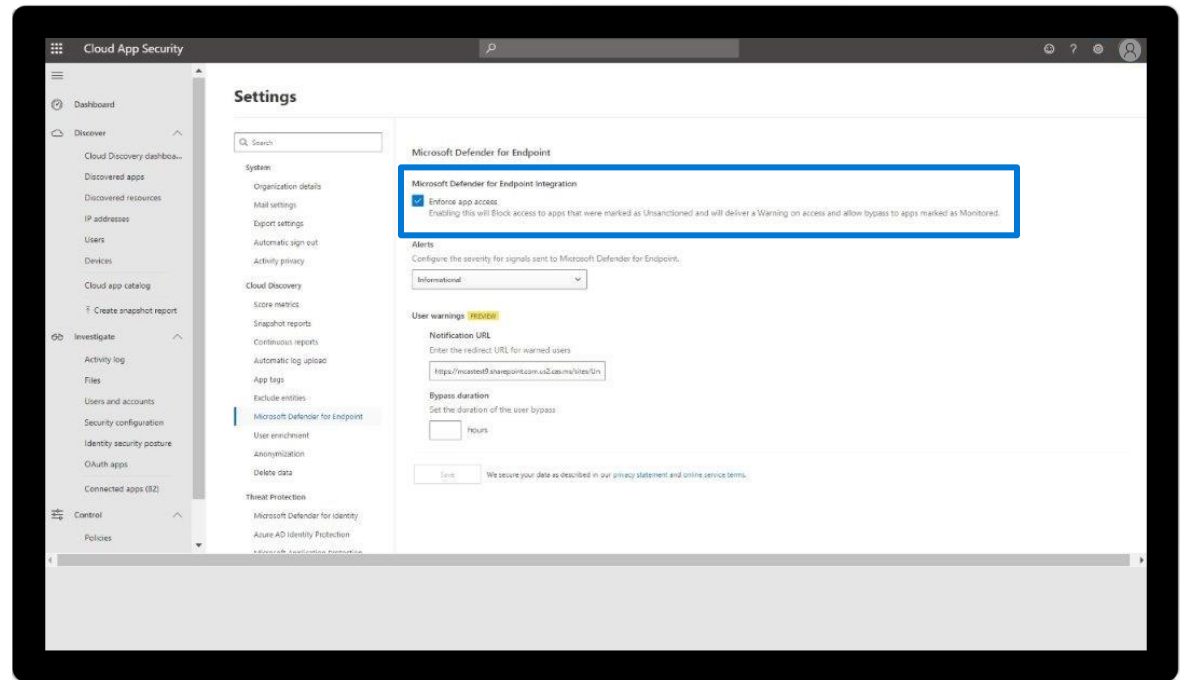
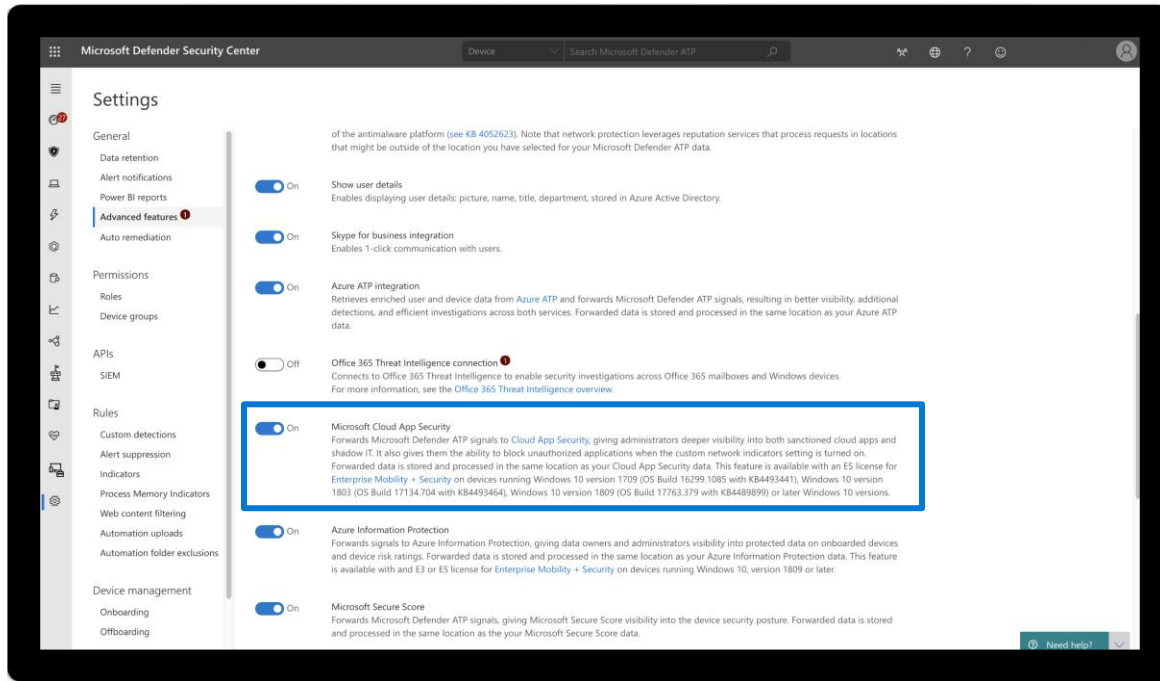
Take action: Manage newly discovered cloud app





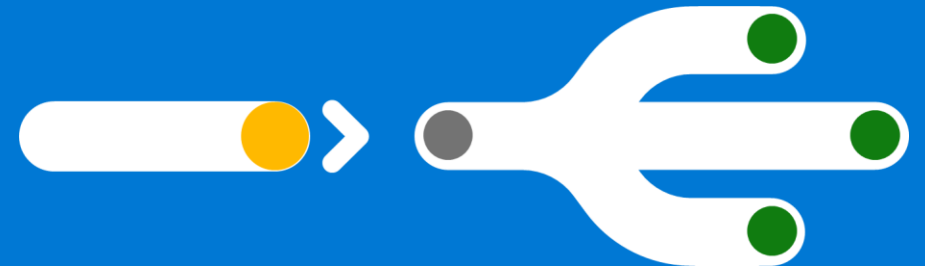
# Endpoint CASB - Shadow IT management with 2 clicks

Shadow IT Discovery, monitoring and governance on the endpoint



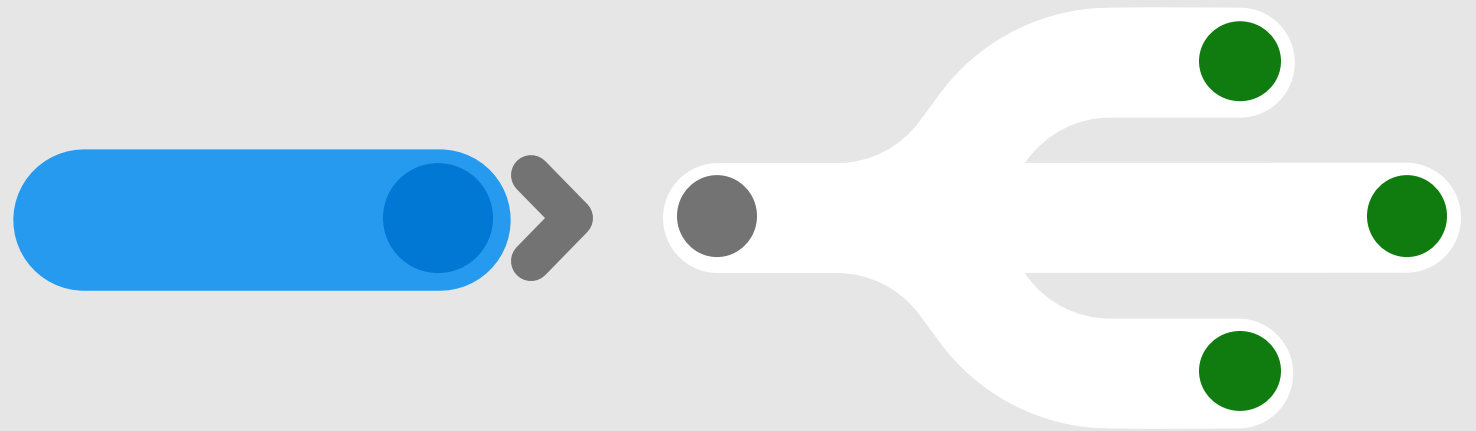
# Demo

Discovering and assessing the risk of Shadow IT



03

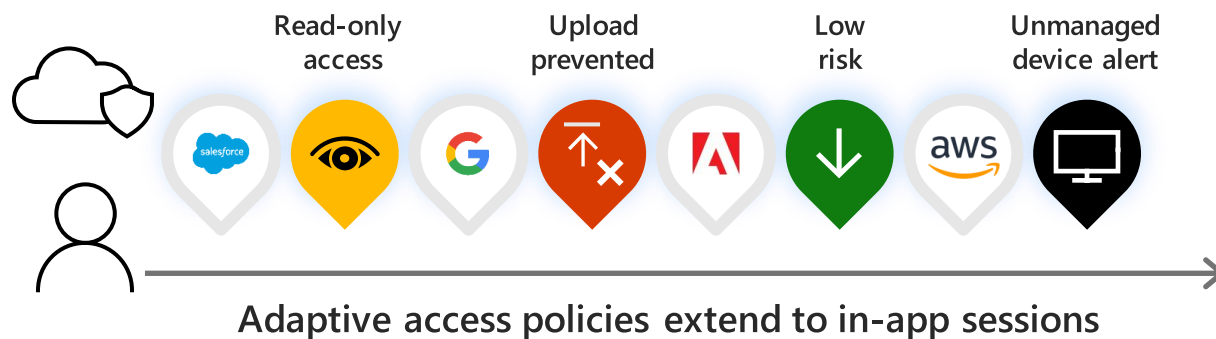
## Secure Access to your apps



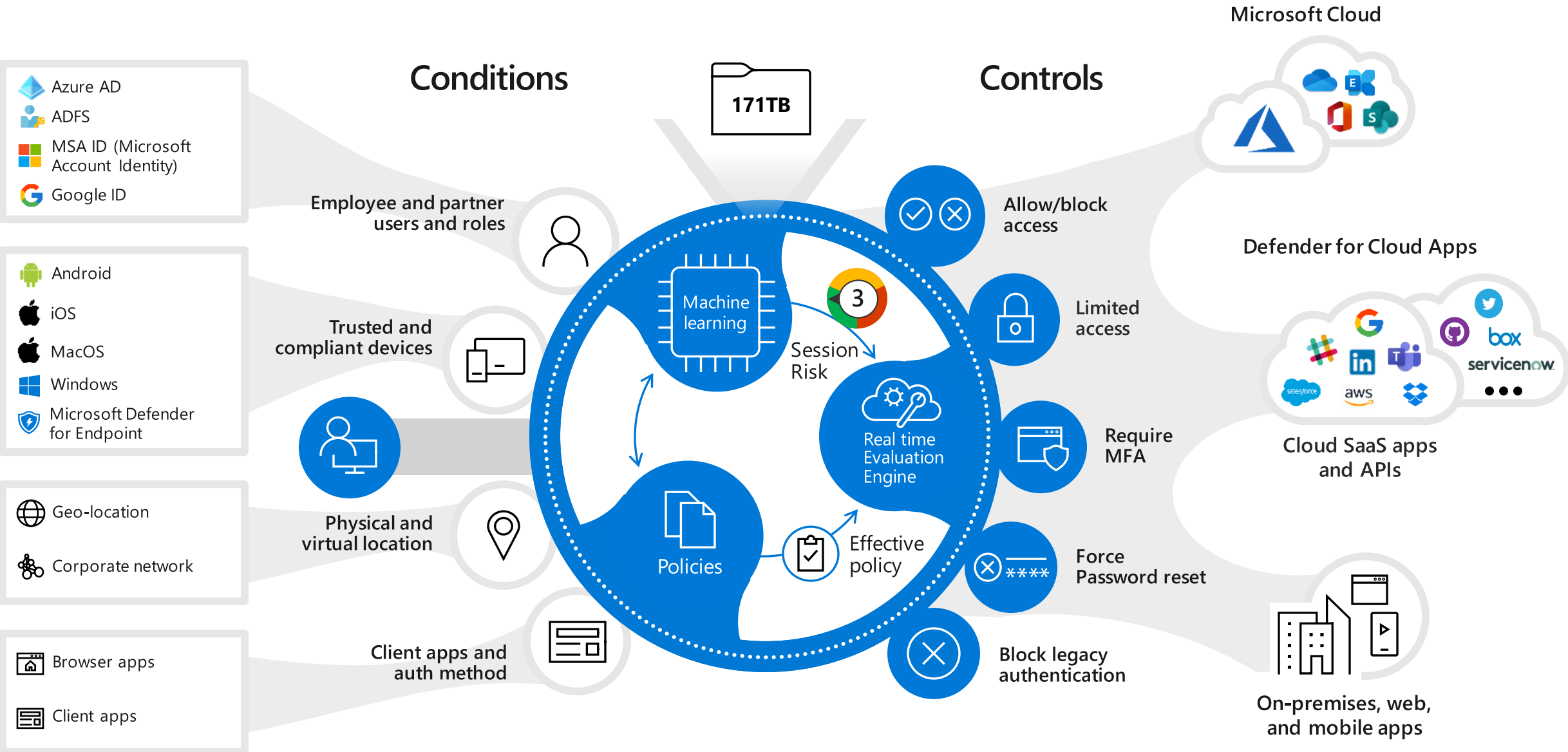


## Secure Access

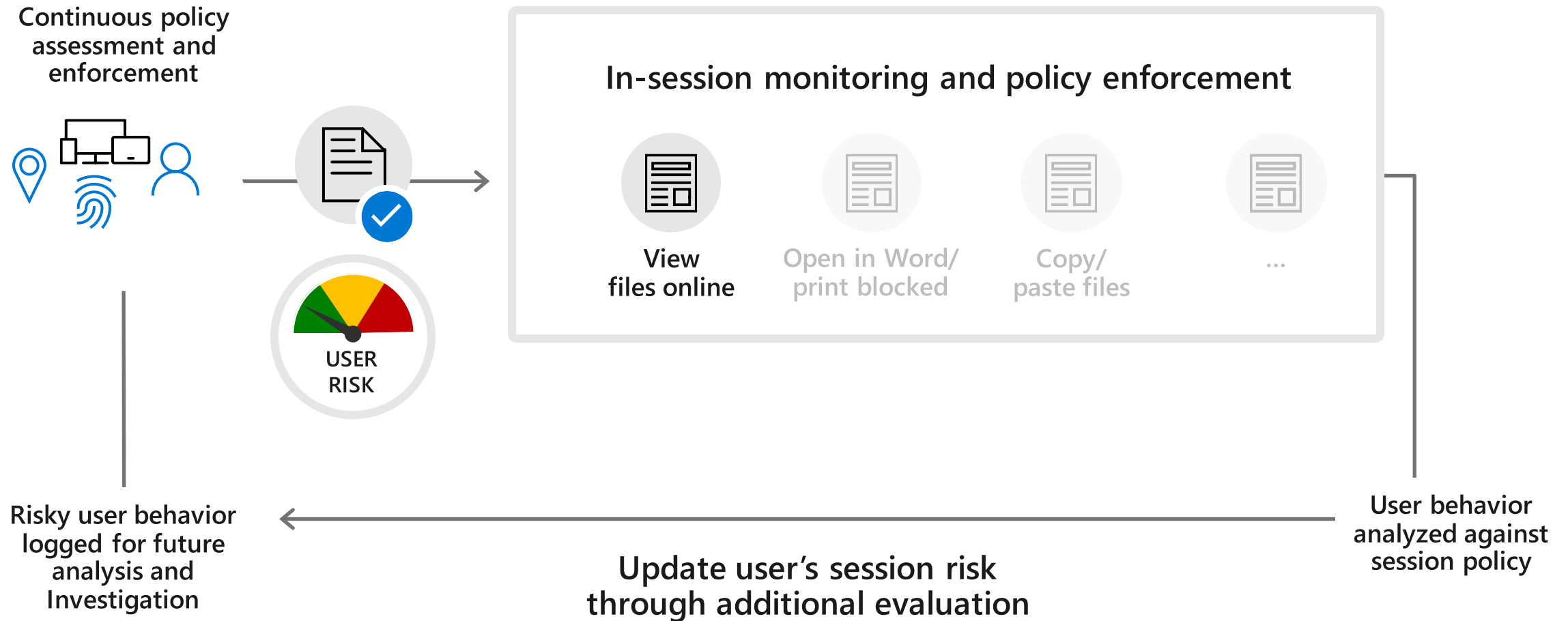
Integrating Defender for Cloud Apps with your identity provider enables real-time enforcement of in-session actions.



# Secure Access in real-time



# Extend policy enforcement into the session



# Real-time in-session App Control

## Context-aware session policies

Control access to cloud apps and sensitive data within those apps based on user, location, device, and the status of the application within the environment

## SAML, Open ID Connect, & on-prem apps

Support for any web app onboarded via an enterprise-level identity provider

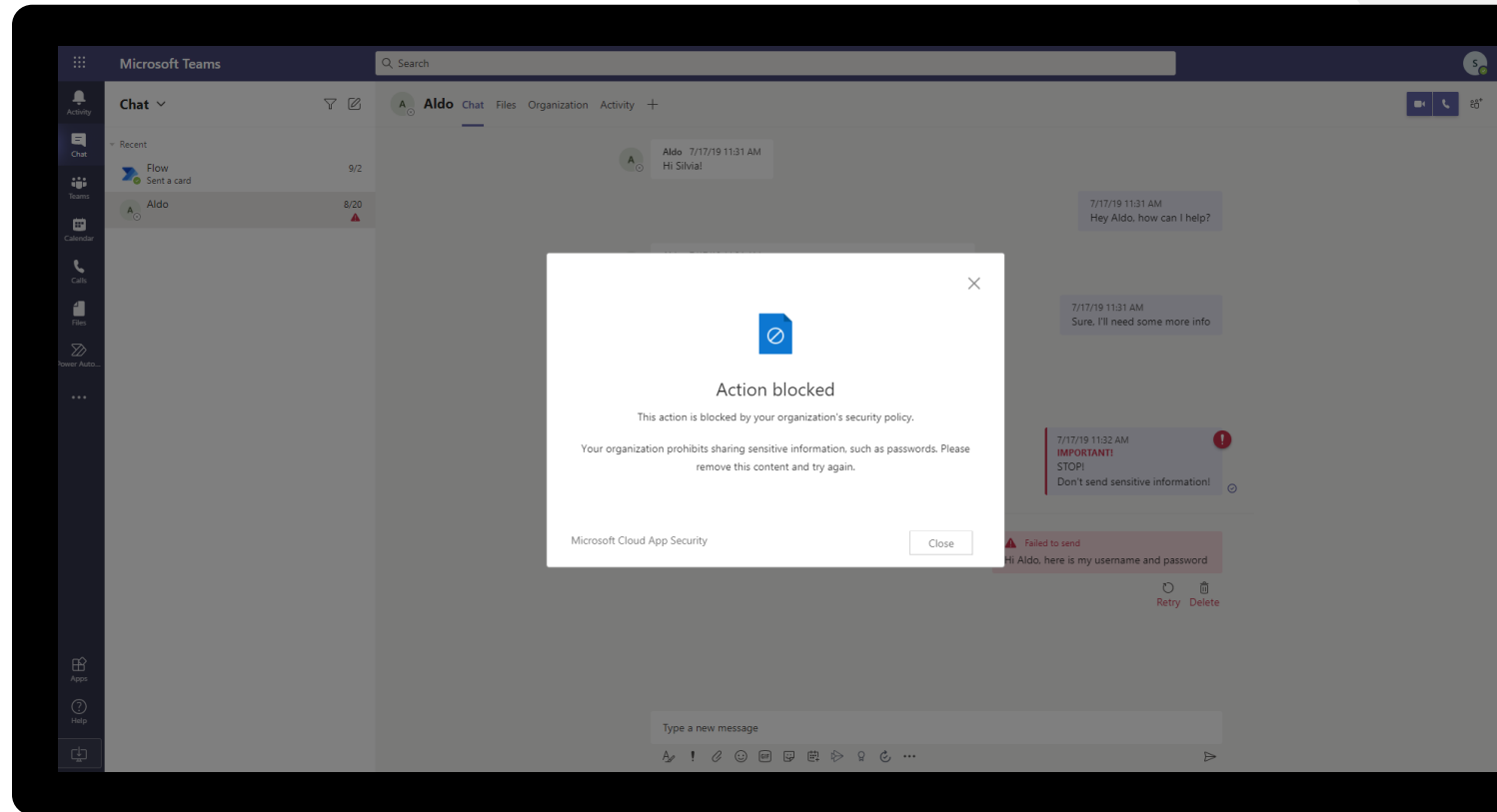
## Enforce granular monitoring & control for risky user sessions

### Data Exfiltration:

- Block download, Apply AIP label on download
- Block print
- Block copy/cut
- Block custom activities: (e.g., IMs with sensitive content)

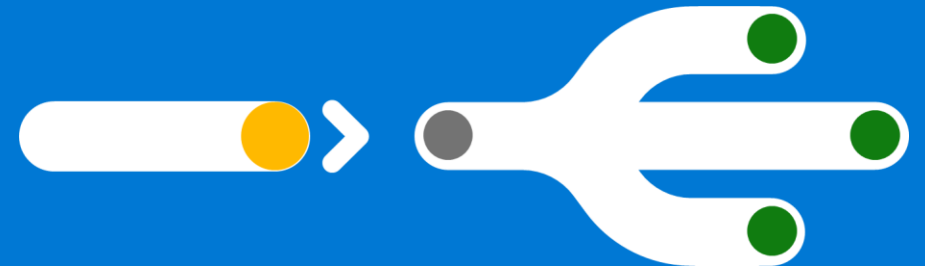
### Data Infiltration:

- Block upload
- Block paste



# Demo

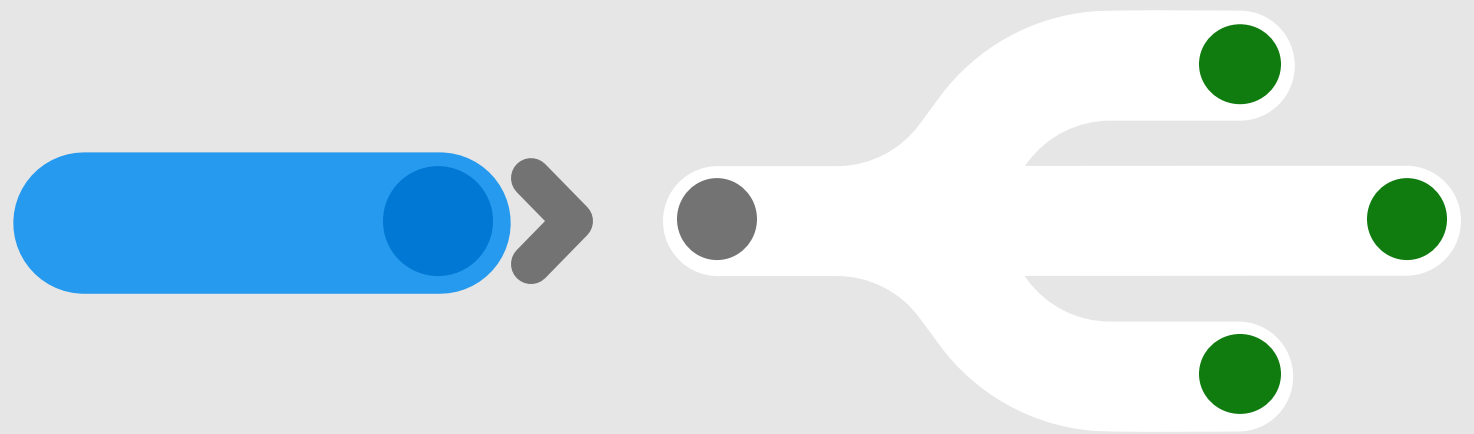
Enabling real-time access controls





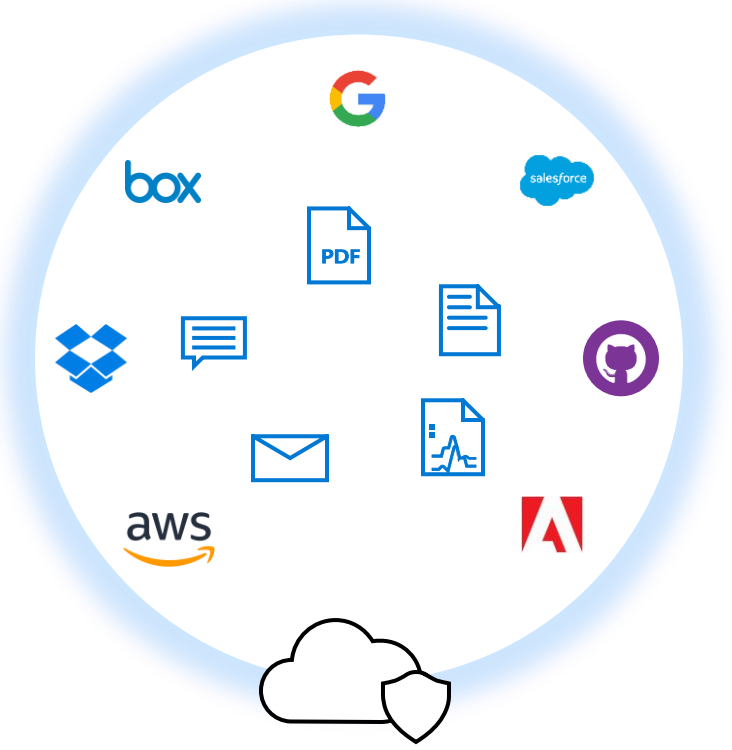
04

# Information Protection





By leveraging information protection in Defender for Cloud Apps, customers gain the power of Microsoft Information Protection applied to their environment holistically.



# Microsoft Information Protection solutions

Protect your sensitive data—wherever it lives or travels



Discover



Classify



Protect

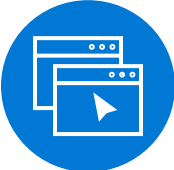


Monitor

**Across**



Devices



Apps



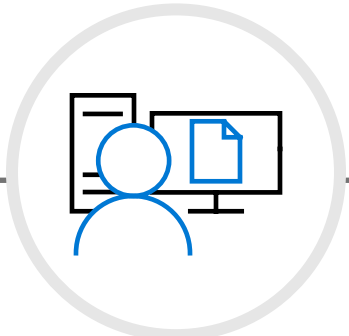
Cloud services



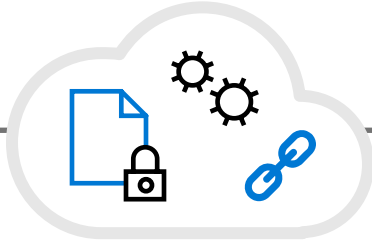
On-premises

# Lifecycle of protecting sensitive files in the cloud

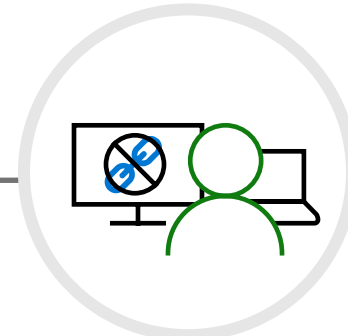
1. User uploads a sensitive file to a cloud app



2. A classification label is automatically applied to protect the file



3. User tries to share sensitive file with external users



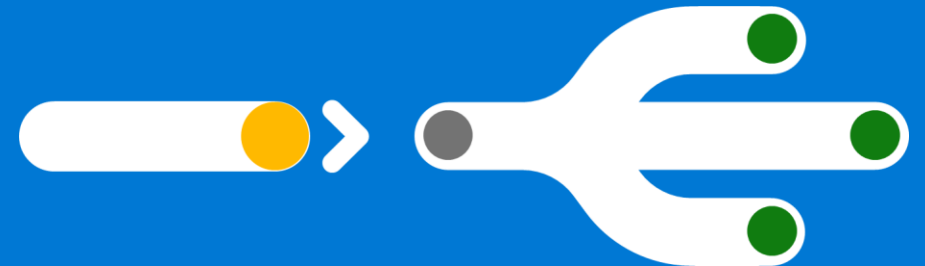
4. External user is not able to access the file due to classification and protection



5. Admin receives event alerts

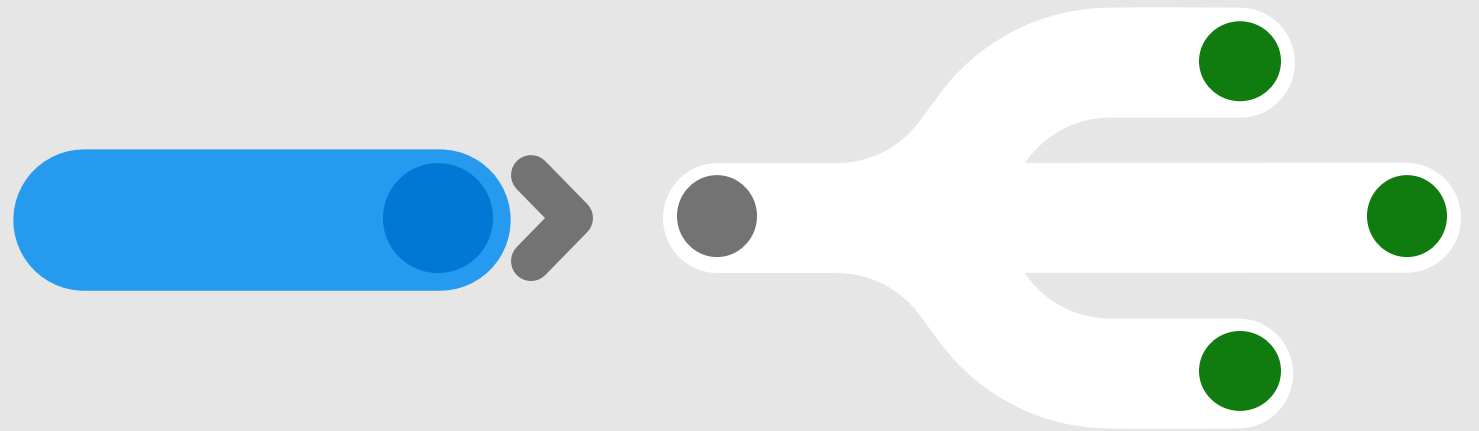
# Demo

## Information Protection



05

## Threat Protection for your cloud environment



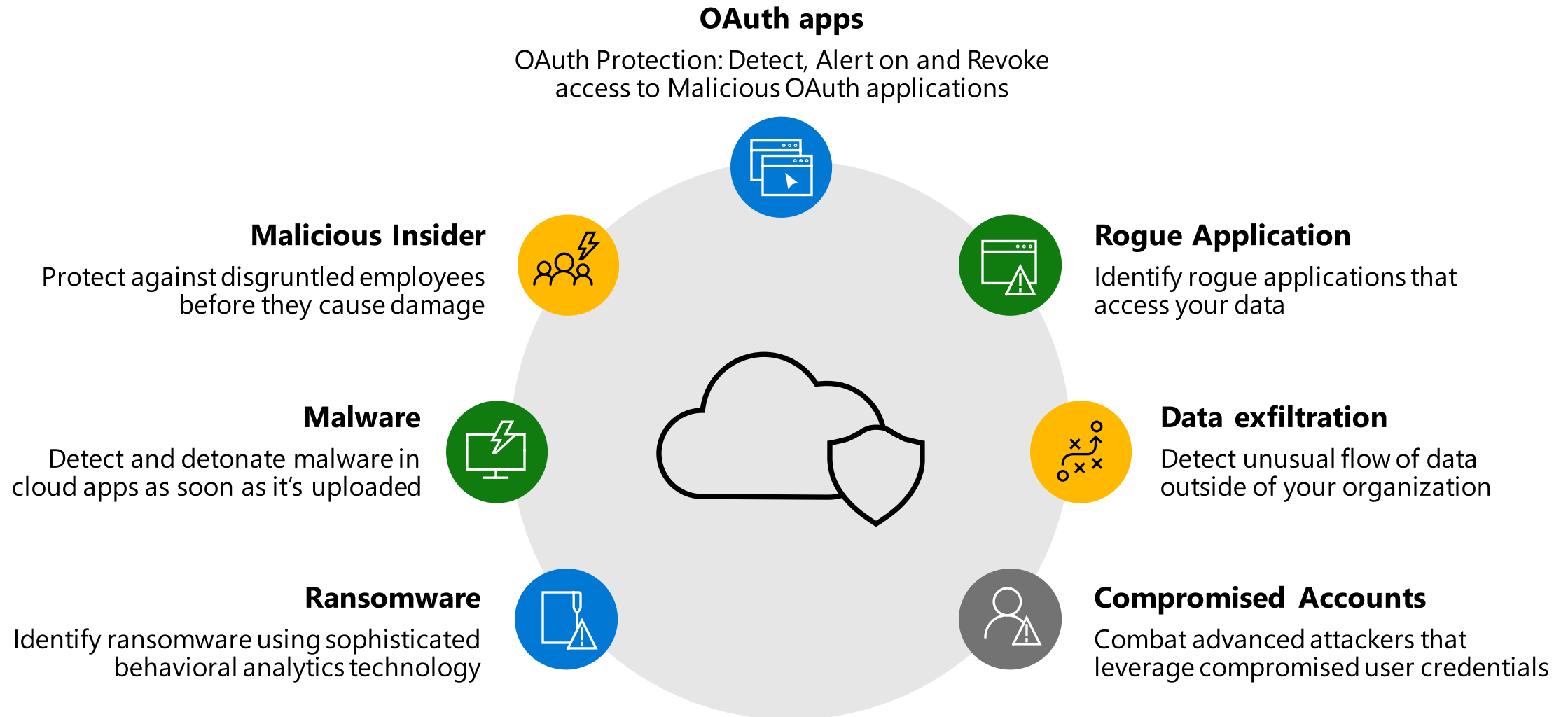


## Threat Protection

The integrated threat protection in Defender for Cloud Apps enables customers to detect advanced attackers and native cloud threats by detecting anomalous behavior and malicious activity in their cloud environment.



# Protection against cloud threats





# Comprehensive Threat Protection for your cloud apps

## Built-in Threat Protection policies

More than 20 out-of-the-box policies and growing. Policies alert you on some of the most common cloud threats such as impossible travel, impersonation activities or ransomware detection

## Malware detonation

Intelligent heuristics identify potentially malicious files and detonate them in a sandbox environment—for existing and newly uploaded files

## Customize policies to alert and remediate

Customize what you want to be alerted on to minimize noise and configure automatic remediation

## Prioritized investigation of alerts

Overview of users who likely pose the greatest risk to the organization and are recommended for immediate review with a unified view of identity threat across on-premises and cloud

Achieved 100% product features in the threat protection pillar Gartner Magic Quadrant 20201

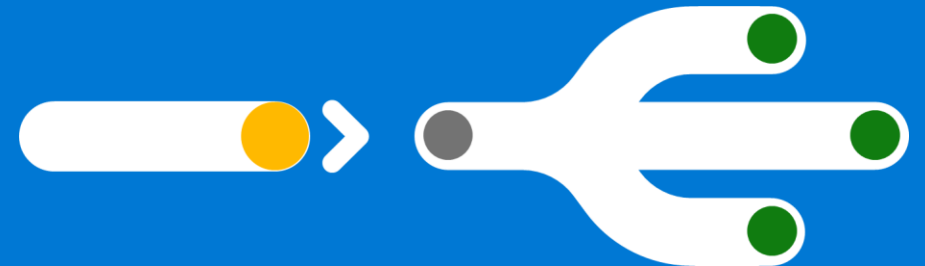
The screenshot displays the 'Cloud App Security' Alerts dashboard. At the top, there's a search bar and a navigation menu. Below that, a filter bar allows users to filter alerts by Resolution Status (OPEN, DISMISSED, RESOLVED), Category (Select risk category...), Severity (Low, Medium, High), App (Select apps...), User Name (Select users...), and Policy (Select policy...). The main area shows a list of 12 alerts, with the first five visible. A blue box highlights the 'Api' column, which lists the following applications: Salesforce - General, Amazon Web Service, Slack - General - General, Box - General - General, and Office 365. The alerts are filtered by 'RESOLVED' status and 'Low' severity. The 'Date' column shows that all alerts occurred '2 days ago'.

Alert	Api	Resolution	Severity	Date
Risky OAuth apps 178.17.166.149 Bill Dortch	Salesforce - General	RESOLVED	Low	2 days ago
Ransomware activity 178.17.166.149 Bill Dortch	Amazon Web Service	RESOLVED	High	2 days ago
Malware campaign caught in delivery 178.17.166.149 Bill Dortch	Slack - General - General	RESOLVED	Low	2 days ago
Activity from a Tor IP address 79.137.68.85 Bill Dortch	Box - General - General	RESOLVED	Medium	2 days ago
Alert on any session coming from a Risky IP address 79.137.68.85 Bill Dortch	Office 365	DISMISSED	Low	2 days ago

1. Gartner, Magic Quadrant for Cloud Access Security Brokers 2020

# Demo

## Threat Protection





Policies > Malware detection

Infected files

History

AUTHORIZATION

APP

OWNER

ACCESS LEVEL

FILE TYPE

OWNER OU

Advanced



Select apps...

Select users...

Select access level...

Select type...

Select organizational units...



1 - 6 of 6 files

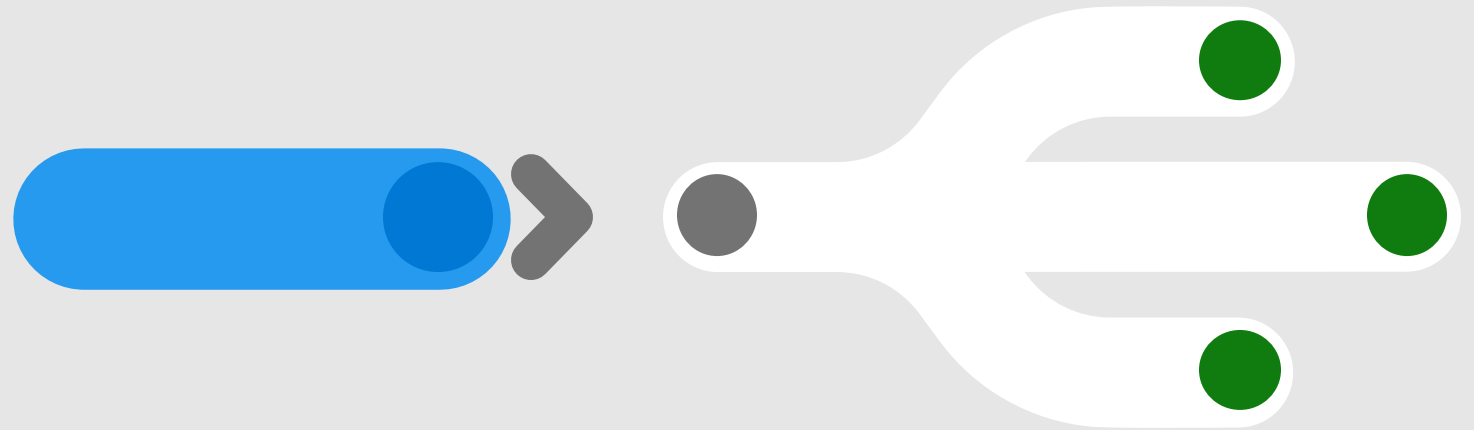


File name	Malware	Confidence	Owner	App	Collaborators	Status	Detection date
eicar.exe.txt	EICAR-Test-File,...	<span style="color: red;">■■■</span> High	Super Admin (mcas-test...	Box - US	1 collaborator	Infected	Jul 19, 2018
Path: All Files - <a href="#">View hierarchy</a>		Owner: <a href="#">Super Admin (mcas-test9) (superadmin@mca...</a>		Created: Jun 25, 2018		Policies: <span style="border: 1px solid black; padding: 2px;">2</span> <a href="#">G56: Publicly Shared Files, Malware detecti...</a>	
Type: text		Owner OU: —		Collaborators: <a href="#">1 collaborator</a>		Detection labels: —	
MIME type: text/plain		Collaborators: <a href="#">1 collaborator</a>		Malware: <a href="#">EICAR-Test-File, EICAR test file NOT a viru...</a>		Status: <a href="#">2 completed</a>	
File identifiers: <a href="#">View file identifiers</a>							
eicar.exe	EICAR-Test-File,...	<span style="color: red;">■■■</span> High	Super Admin (mcas-test...	Box - US		Infected	Jun 25, 2018
HR_Summary_Nov...	DOS/EICAR_Tes...	<span style="color: red;">■■■</span> High	MCAS Test 9 (admin@m...	Microsoft SharePoin...	3 collaborators	Infected	Apr 11, 2018

EICAR-Test-File, EICAR test file NOT a virus., EICAR test file, Eicar-Test-Signature, Virus.44D88612FEA8A8F3.Eicar, EICAR\_TEST\_FILE, EICAR-Test-File (not a virus), qex.eicar.gen.gen, Eicar test fil...

06

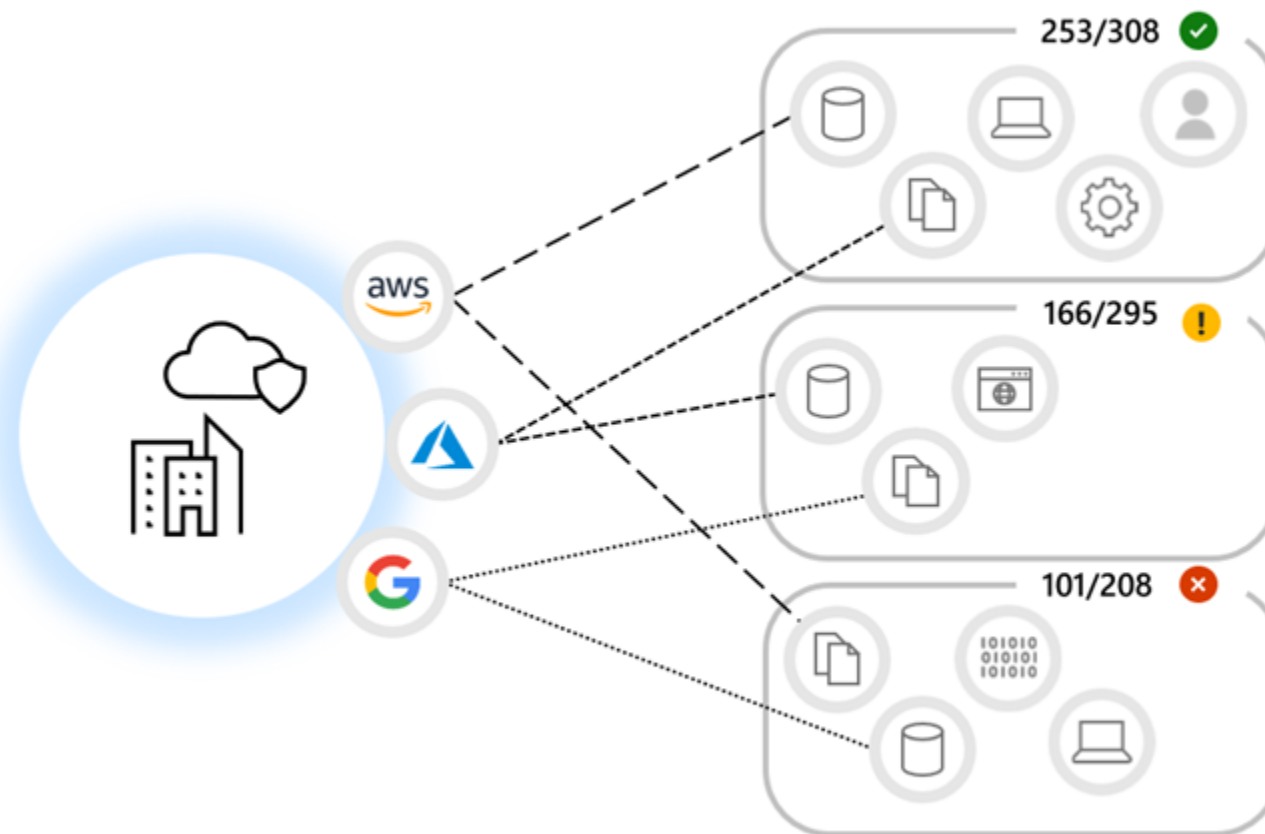
# Security Posture Management





## Cloud Platform Security

SaaS application security prioritizes the risks and makes recommendations for improvement against your pre-selected goals.



# CASB for cloud platforms

## Detection and investigation of anomalous admin behavior

Identify anomalies in your cloud environment via advanced behavioral analytics

Pivot on users, IP addresses, resources, activities and locations

## Security posture assessment

Analyze the security posture of your cloud platform and identify missing security configurations and controls

## Unique integration with Microsoft Defender for Cloud

Pivot to Microsoft Defender for Cloud to apply recommendation and remediate vulnerabilities

## Multi-cloud capabilities and integration

Connect your AWS Security Hub and GCP Security Configurations for visibility into third-party cloud security recommendations

The screenshot displays the Microsoft Cloud App Security interface. The top section, titled "Security configuration", shows a table of recommendations for 3 Azure subscriptions. The table includes columns for Recommendations, Resources, Subscriptions, and Severity. Below this, the "Policies" section is visible, showing a table with columns for Name, Type, Status, Severity, and Category. A specific policy, "Publicly accessible S3 buckets (AWS)", is highlighted, showing 1 match and a severity of Medium.

Recommendations	Resources	Subscriptions	Severity
Add a Next Generation Firewall	1 Public IP address(s)	FREE TRIAL	Medium
Add a vulnerability assessment solution	2 Virtual Machine(s)	2 Subscriptions	Medium
Add a web application firewall	1 Public IP address(s)	FREE TRIAL	Medium
Apply a Just-In-Time network access control	1 Virtual Machine(s)	FREE TRIAL	High
Apply disk encryption	2 Virtual Machine(s)	2 Subscriptions	Medium
Designate more than one owner on your subscription	1 Subscription(s)	FREE TRIAL	Medium

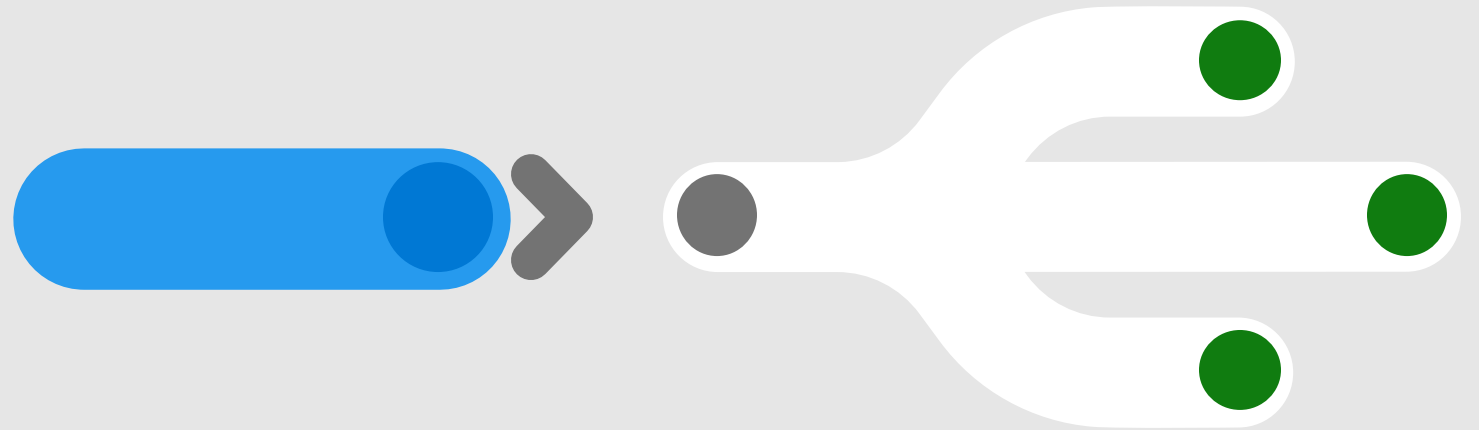
NAME	TYPE	STATUS	SEVERITY	CATEGORY
Policy name...	Select type...	ACTIVE   DISABLED	Medium	Sharing control

Policy	Count	Severity	Action	Modified
Publicly accessible S3 buckets (AWS) Alert when an S3 bucket in AWS is publicly accessible.	1 matches	Medium		Sep 19, 2018

# 8

## Summary and next steps



# Top 10 CASB use cases you should think about

1. Discover all cloud apps and services used in your environment
2. Assess the risk and compliance of your cloud apps
3. Govern discovered cloud apps
4. Discover OAuth apps that have access to your environment
5. Record an audit trail for all user activities across hybrid environments
6. Identify compromised user accounts
7. Identify and revoke access to risky OAuth apps
8. Ensure safe collaboration and data sharing practices in the cloud
9. Enforce adaptive session controls to manager user actions in real-time
10. Detect when data is being exfiltrated from your corporate apps





# Licensing

- Defender for Cloud Apps – Standalone SKU
- EMS E5
- M365 E5 Security
- M365 E5 Information Protection & Governance
- M365 E5 Compliance
- M365 E5

Some Features might require additional add-ons



# Questions?

Thank you



<https://forms.office.com/r/tbWfiwpD8A>