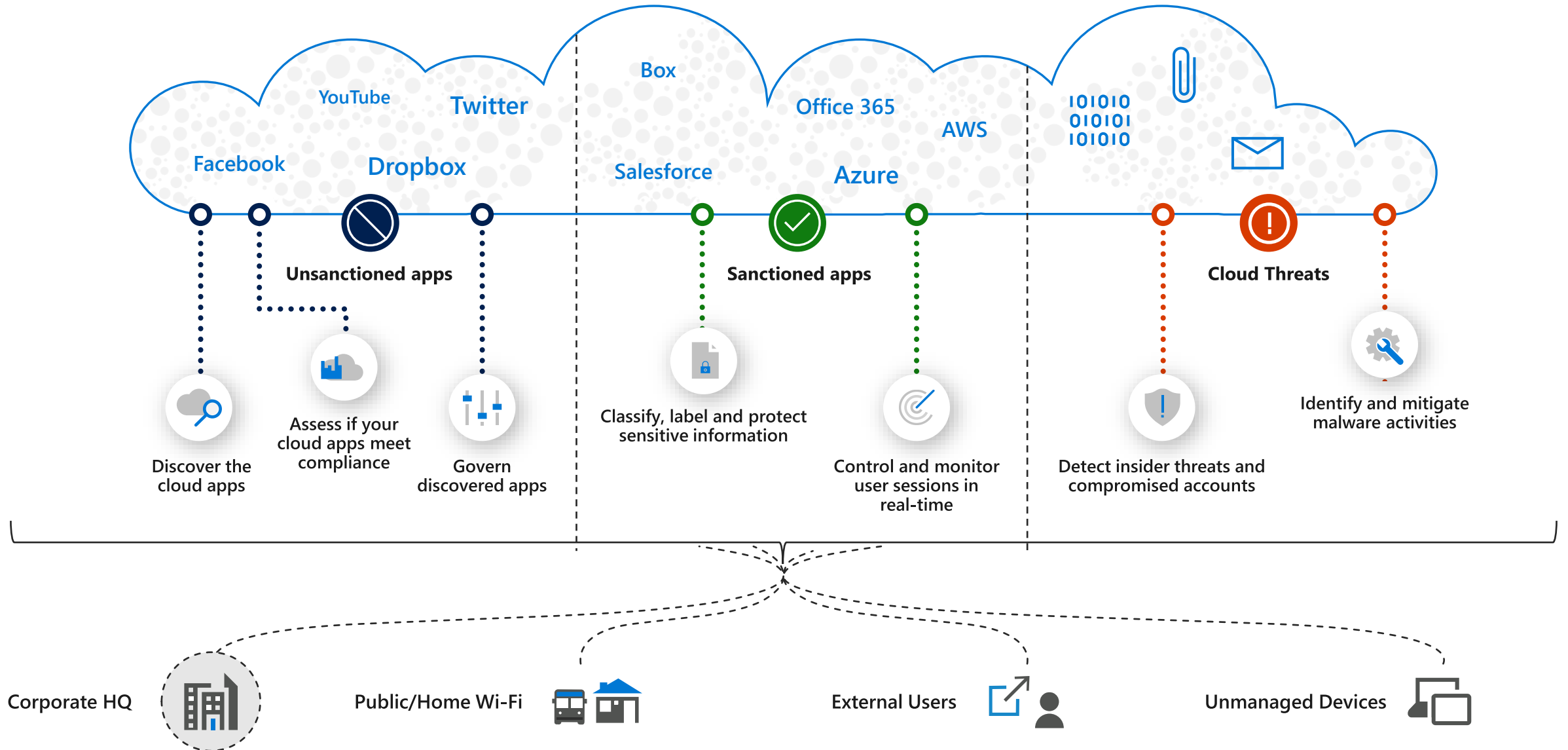
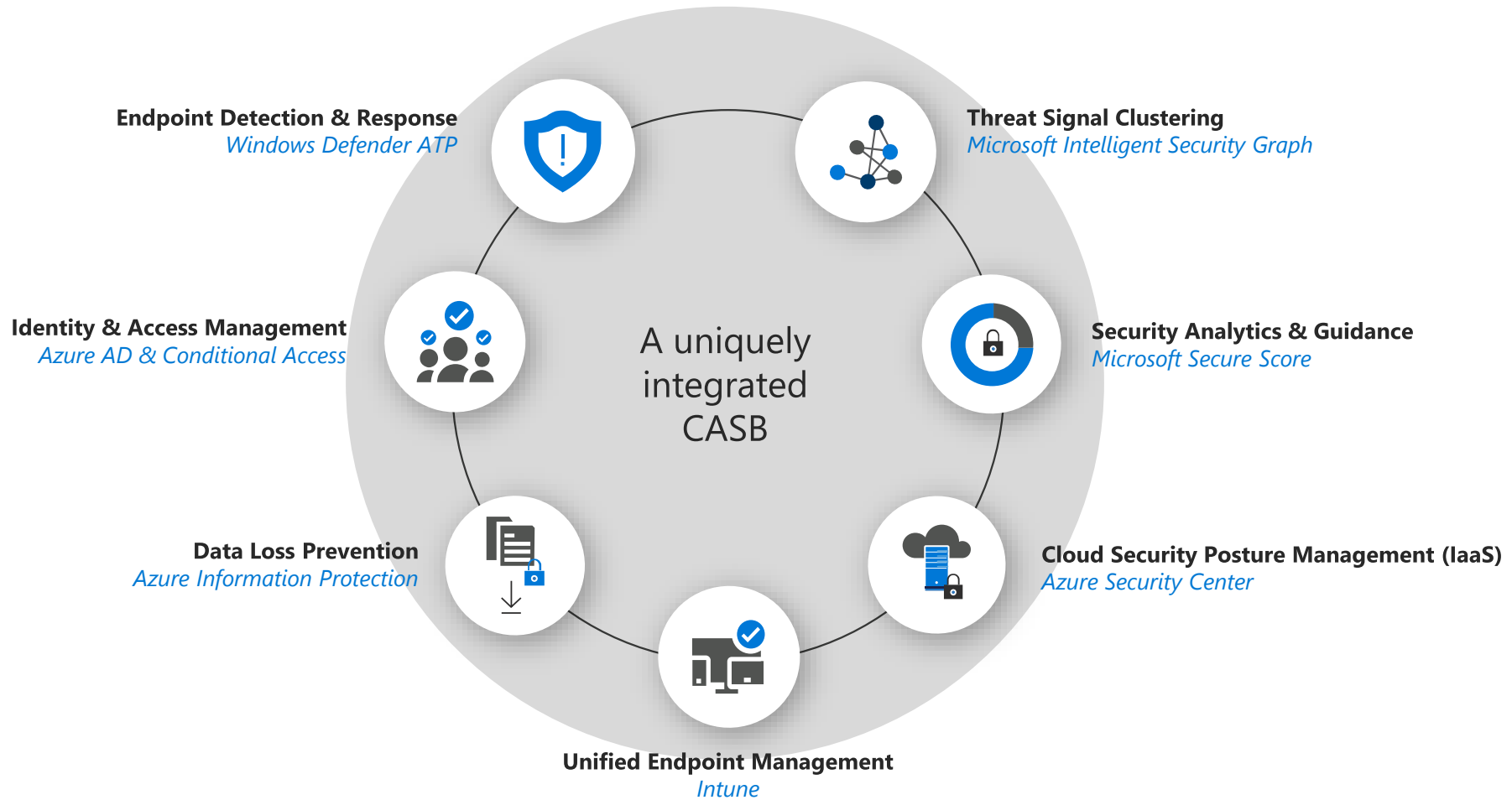


CASB

Microsoft

TOP Security USE CASES





MICROSOFT CLOUD APP SECURITY

Elevate the security for all your cloud apps and services

Discovery

Use traffic log data to discover the cloud apps in your organization and get detailed insights about traffic- and user data

Managing discovered cloud apps

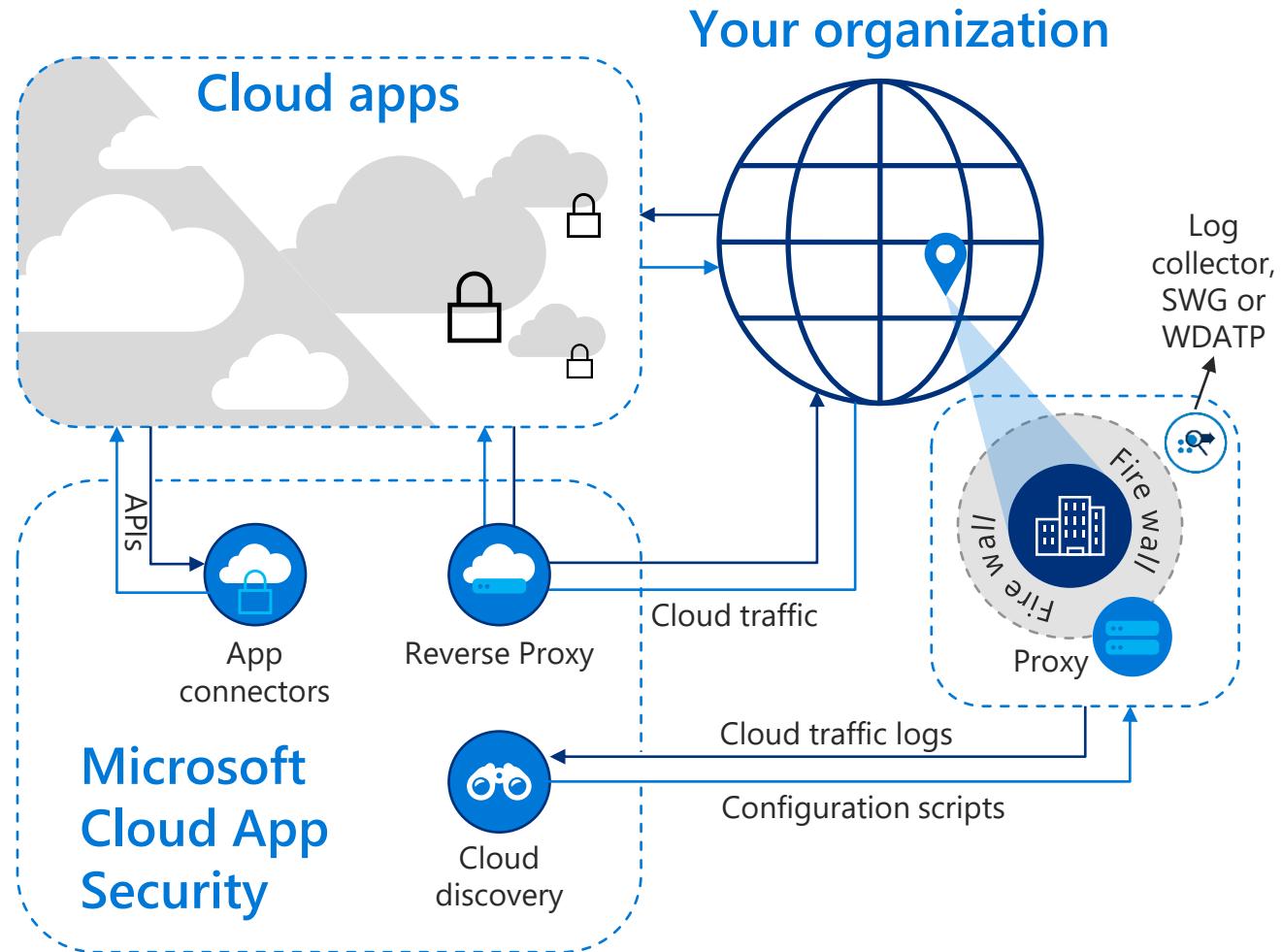
Evaluate the risk of discovered cloud apps and take action by sanctioning, tagging or blocking them

App connectors

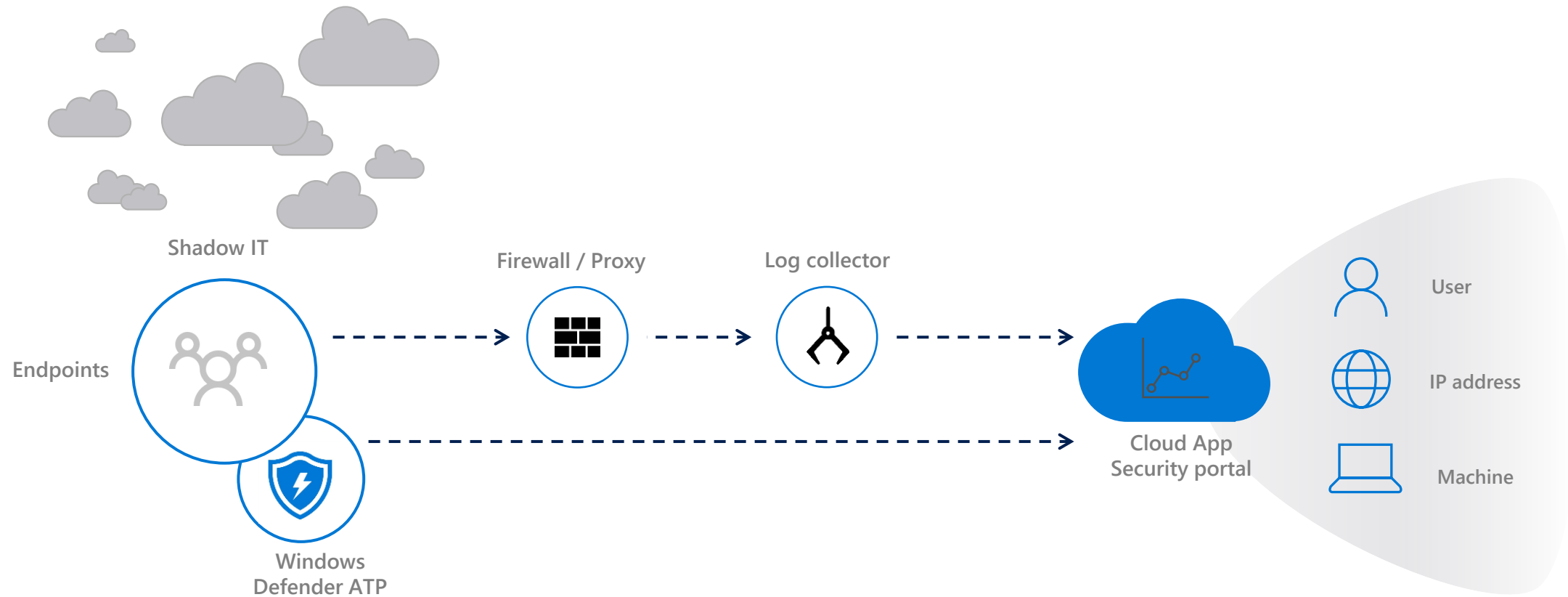
Be alerted on user or file behavior anomalies and control the data stored in your cloud apps leveraging our API connectors

Conditional Access App Control

Leverage our reverse proxy infrastructure and integration with Azure AD Conditional Access to configure real-time monitoring and control



DISCOVERY ARCHITECTURE WITH WINDOWS DEFENDER ATP

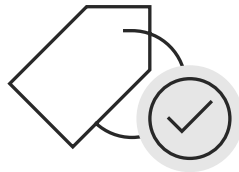


MICROSOFT INFORMATION PROTECTION SOLUTIONS

Comprehensive protection of sensitive data throughout its lifecycle—across devices, apps, cloud services, and on-premises



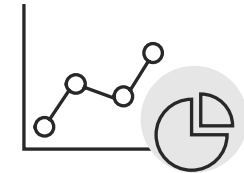
Discover



Classify

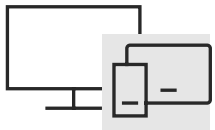


Protect



Monitor

Across



Devices



Apps



Cloud services



On-premises

PROTECT YOUR FILES AND DATA IN THE CLOUD

Data is ubiquitous and you need to make it accessible and collaborative, while safeguarding it



Understand your data and exposure in the cloud

- Connect your apps via our API-based App Connectors
- Visibility into sharing level, collaborators and classification labels
- Quantify over-sharing exposure, external- and compliance risks



Classify and protect your data no matter where it's stored

- Govern data in the cloud with granular DLP policies
- Leverage Microsoft's IP capabilities for classification
- Extend on-prem DLP solutions
- Automatically protect and encrypt your data using Azure Information Protection



Monitor, investigate and remediate violations

- Create policies to generate alerts and trigger automatic governance actions
- Identify policy violations
- Investigate incidents and related activities
- Quarantine files, remove permissions and notify users

CONDITIONAL ACCESS APP CONTROL

Context-aware session policies

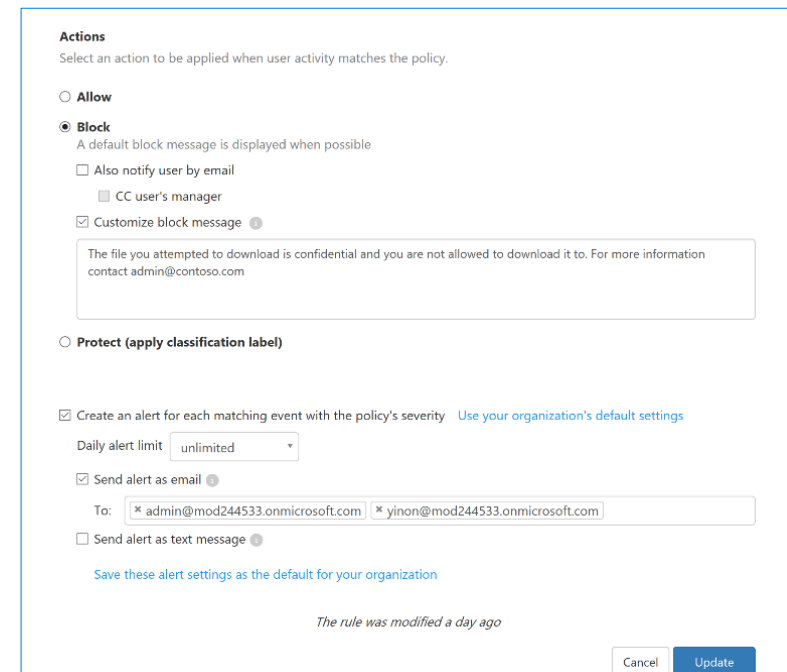
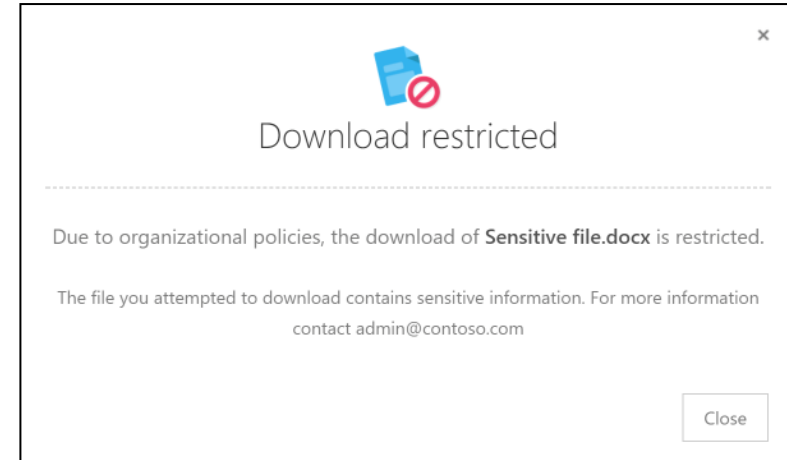
Control access to cloud apps and sensitive data within apps based on user, location, device, and app

Investigate & enforce app and data restrictions

Enforce browser-based “view only” mode for low-trust sessions. Classify, label, and protect on download. Gain visibility into unmanaged device activity.

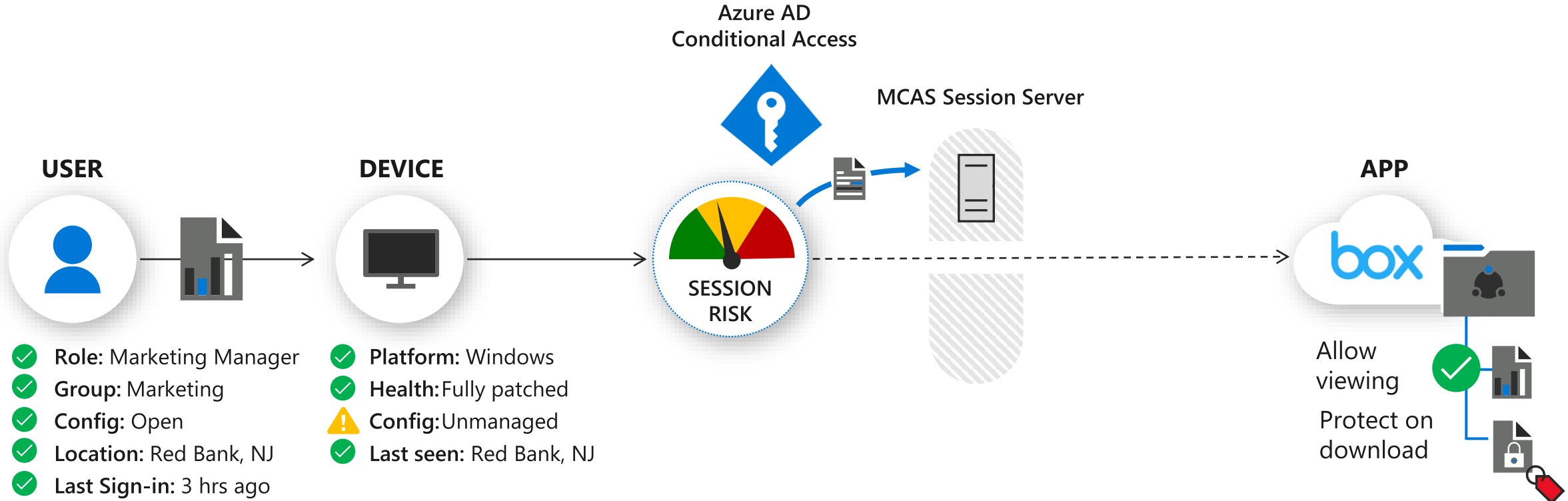
Unique integration with Azure Active Directory

Limit activities performed within user sessions in SaaS apps based on user identity, location, device state, and detected sign-in risk level.



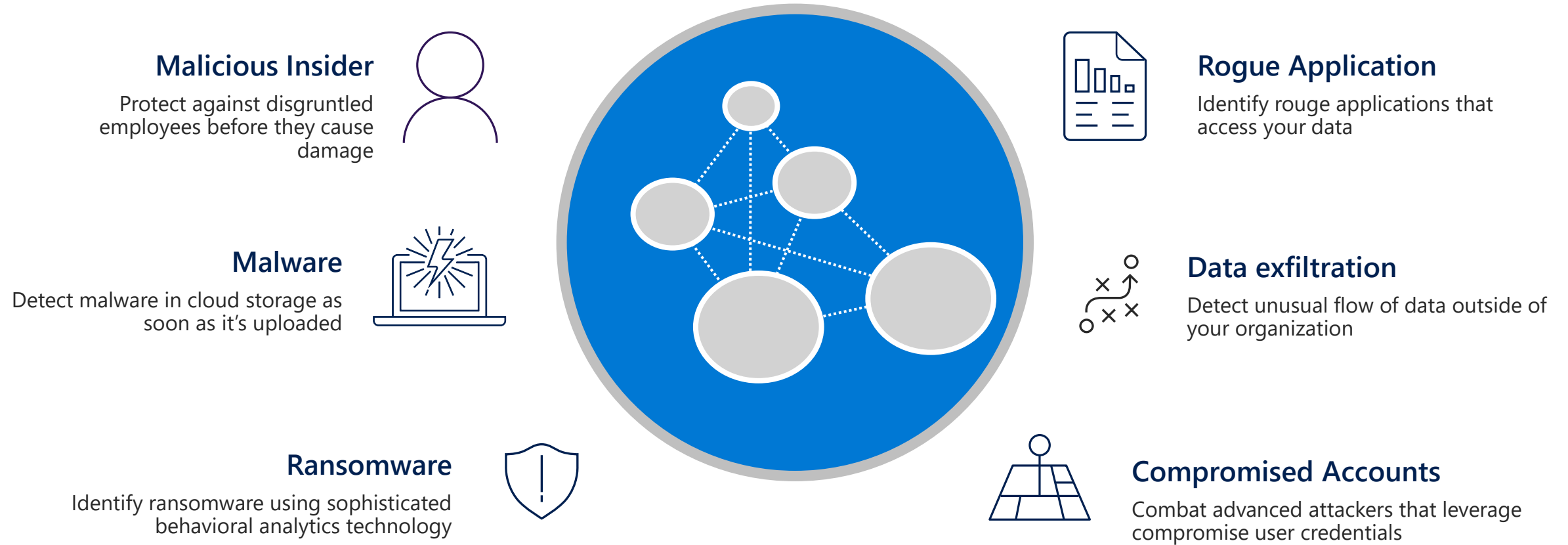
USE CASE: PREVENT DOWNLOAD OF FILES

Risk based in-session controls



⚠ Device is unmanaged

PROTECTION AGAINST CLOUD THREATS



Threat detection in Microsoft Cloud App Security



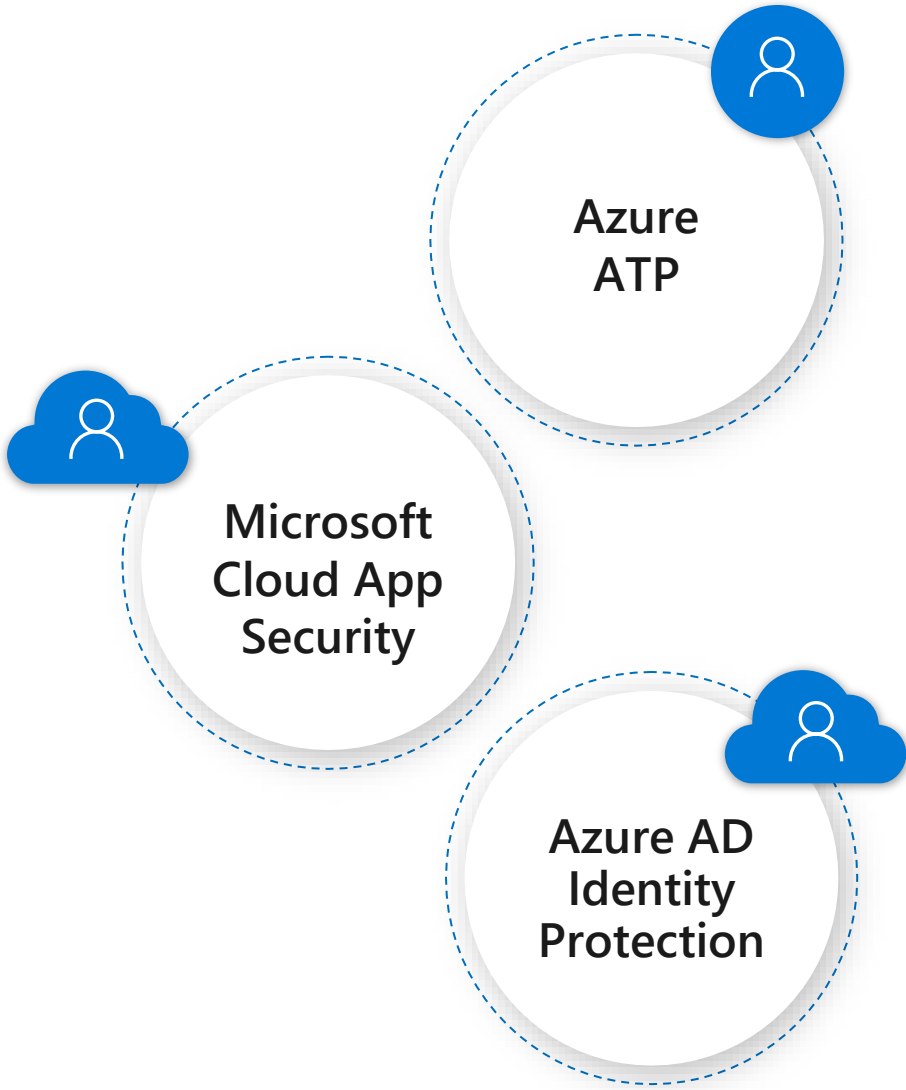
Get alerts

- Identify high-risk and anomalous usage
- Exfiltration of data to unsanctioned apps
- Rogue 3rd party applications
- Ransomware attacks



Investigate and remediate

- Mitigate ransomware attacks
- Suspend user sessions
- Revoke app (coming)



One SecOps experience to investigate identity activities across on-premises & the cloud

Consolidated view of user information and insights

Triage users to investigate based on User and Entity Behavior Analytics

Unified Hunting experience through Identity Activities

Activity log

[Investigate in Web traffic log](#)

Activity log filters:

- QUERIES: Select a query...
- APP: Select apps...
- USER NAME: Jeff Leatherman (jeffl@mcast...)
- RAW IP ADDRESS: Enter IP address...
- ACTIVITY TYPE: Select activity...
- LOCATION: Select countries/regions...
- Buttons: Save as, Advanced

1 - 20 of 76 activities

New policy from search

Sort, Filter, Download, View icons

Activity	User	App	IP address	Location	Device	Date
Run command: SAMR query QueryUser user Jeff Leather...	Jeff Leatherman	Active Directory	10.0.8.7	—	Jeff-DSK	Mar 6, 2019, 6:02 AM
Access file: file https://mcastest9.sharepoint.com/sites/Dr...	Jeff Leatherman (jeffl@mcastest9.onmicr...	Microsoft ShareP...	5.29.115.84	—	—	—
WACTokenShared	Jeff Leatherman (jeffl@mcastest9.onmicr...	Microsoft ShareP...	5.29.115.84	—	—	—
Log on	Jeff Leatherman	Active Directory	10.0.8.8	—	Financeserv53	Mar 5, 2019, 11:59 PM
Credentials validation	Jeff Leatherman	Active Directory	N/A	—	YOBASHA-LAP	Mar 5, 2019, 11:59 PM
Add member to group: user jeffl@mcastest9.onmicrosoft....	Jeff Leatherman	Office 365	N/A	—	—	—
Add member to group: user jeffl@mcastest9.onmicrosoft....	Jeff Leatherman	Office 365	N/A	—	—	Mar 5, 2019, 11:59 PM
MemberAdded: user jeffl@mcastest9.onmicrosoft.com	Jeff Leatherman	Microsoft Teams	N/A	—	—	Mar 5, 2019, 11:59 PM
Log on	Jeff Leatherman	Microsoft Teams	5.29.115.84	Israel	—	Mar 5, 2019, 11:53 PM

Cloud Activities – via Azure AD IP, Office 365 and MCAS

On Premises Activities – via Azure ATP

Unified Alerts investigation & management

Alerts

RESOLUTION STATUS: OPEN DISMISSED RESOLVED

CATEGORY: Select risk category...

SEVERITY: [Yellow] [Orange] [Red]

APP: Select apps...

USER NAME: Jeff Leatherman (jeffv@igniteaat...)

POLICY: Select policy...

Advanced

1 - 10 of 10 alerts


Alert	App	Resolution	Severity	Date
Risky sign-in: Anonymous IP address 197.231.221.211 LR Jeff Leatherman	Microsoft Azure			
Suspicious VPN connection Jeff Leatherman	—	OPEN	Medium	2 months ago
Abnormal access to protected data 84.59.125.30 Jeff Leatherman	—			
Suspicious inbox forwarding 185.220.101.45 Jeff Leatherman	Microsoft Excha...	OPEN	Medium	2 months ago
Risky sign-in: Unfamiliar sign-in properties DE 185.220.102.6 Jeff Leatherman	—			
Leaked credentials Jeff Leatherman	—	OPEN	High	2 months ago

On Premises alert – via Azure ATP

Cloud alert – via MCAS

Cloud alert – via Azure AD Identity Protection

User investigation & User behavior analytics: Vanadium



Jeff Leatherman

Financial Accounting Manager
Finance

User threat ^

Investigation priority **▲ 124** Alerts **2 open alerts**

Identity risk level
No user sign-in risk

User exposure ^

Devices 2	Accounts 4
Resources 0	Locations 1
Matched files 0	

Basic information ^

Email
Jeff@mcastest9.onmicrosoft.com

Phone
1-425-93-MSPHONE

Manager
Roderick Brooks

Last seen ●
Mar 5, 2019

Extended information ∨

Overview

Investigation priority score

Score is based on the last 7 days [How do we score?](#)

124

Alerts Score: 92
Risky activities Score: 32

User score in the last two weeks

User's score compared to the organisation **100%**

■ Top 90% in your organization

Alerts and risky activities that contributed to the score (last 7 days) [View all alerts \(2\)](#)

- 3/6/19 ●
- +23 ● File access from unauthorized locations
Mar 6, 2019, 12:07 AM | ■ | ● Dismissed alert
- +23 ● File access from unauthorized locations
Mar 6, 2019, 12:05 AM | ■ | ● Resolved alert
- 3/5/19 ●
- +3 ● Access file: file <https://mcastest9.sharepoint.com/sites/DreamTeam/Shared Documents/Forms/AllItems.aspx>
Mar 5, 2019, 11:59 PM
- +23 ● File access from unauthorized locations
Mar 5, 2019, 11:58 PM | ■
- +3 ● Add user to group in site: group Jeff's teams Members to group Site Members
Mar 5, 2019, 11:53 PM
- +23 ● File access from unauthorized locations
Mar 5, 2019, 11:15 PM | ■
- +2 ● Log on
Mar 5, 2019, 11:13 PM
- +10 ● Create folder: folder [https://mcastest9-my.sharepoint.com/TeamsNotebook\(Shared\)](https://mcastest9-my.sharepoint.com/TeamsNotebook(Shared))
Mar 5, 2019, 11:04 PM

Investigation priority score

Score compared to other users

Abnormal activity

Alert priority

Malware Detection

- Scan cloud storage apps
- Identify potentially risky files
- Powered by Microsoft Threat Intelligence

Cloud App Security

Policies > Malware detection

Infected files | History


AUTHORIZATION APP OWNER ACCESS LEVEL Advanced

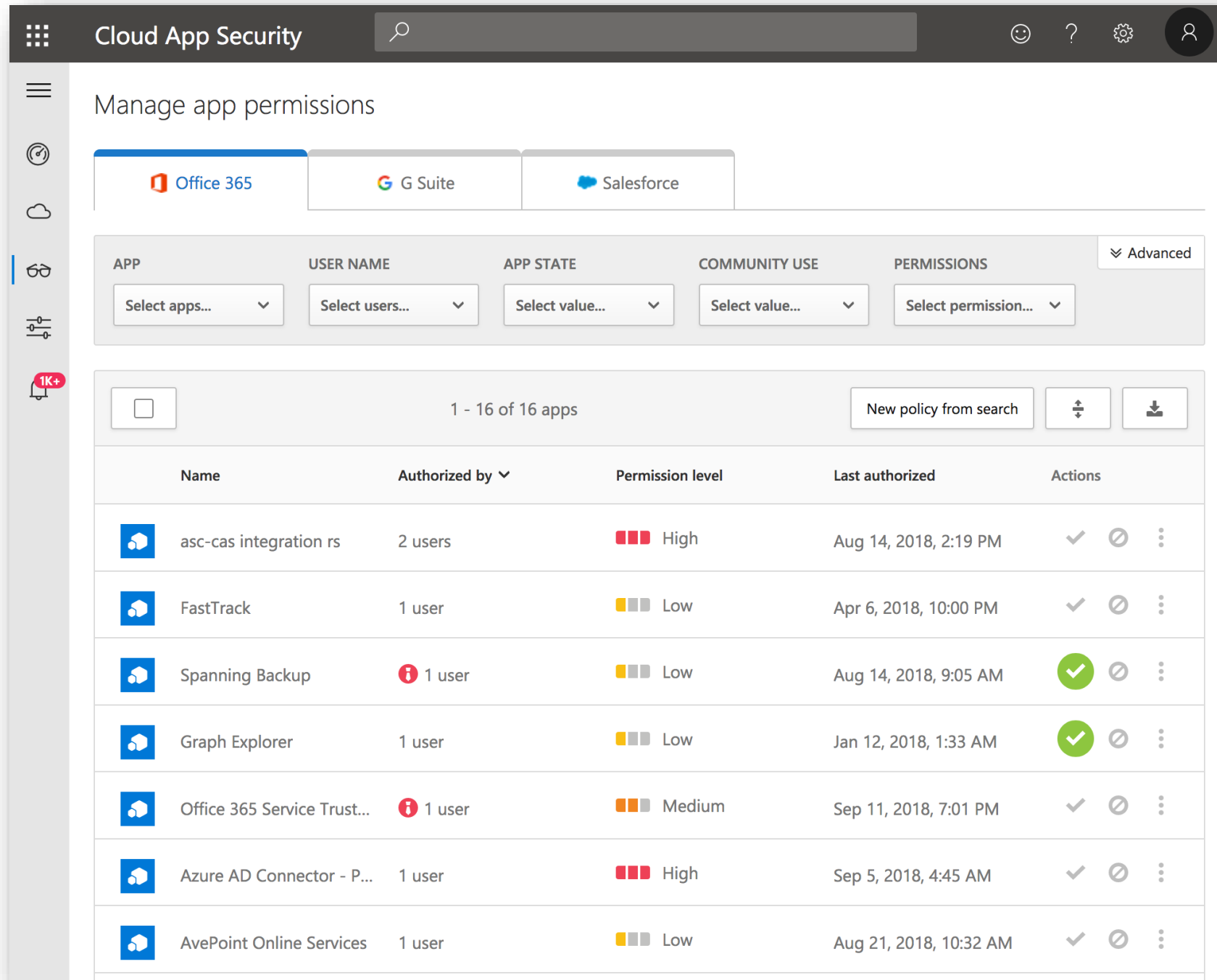
1K+

1 - 6 of 6 files

File name	Malware	Confidence	Owner	App	Collaborators	Status	Detection date
eic...	EIC...	High	Super Ad...	Box -...	1 coll...	I...	Jul 19, 2018
Path: All Files - View hierarchy		URL: https://app.box.com/files/0/f/0/1/f_300544144254					
Type: text		Owner: Super Admin (mcas-tes...		Created: Jun 25, 2018		Policies: 2 G56: Publicly Shared...	
MIME type: text/plain		Owner OU: —		Modified: Jun 25, 2018		Classification labels: —	
File identifiers: View file identifiers		Collaborators: 1 collaborator		File size: ~68 B		Scan status: 2 completed	
Malware: EICAR-Test-File, EIC...							
eic...	EIC...	High	Super Ad...	Box -...		I...	Jun 25, 2018
HR...	DOS...	High	MCAS Te...	Micro...	3 coll...	I...	Apr 11, 2018

OAuth App Permissions

- Monitor cloud permissions authorized by your users.
- Act on suspicious apps
- Define automated app permission policies 



The screenshot displays the Microsoft Cloud App Security interface for managing app permissions. At the top, there are tabs for Office 365, G Suite, and Salesforce. Below these are filter dropdowns for APP, USER NAME, APP STATE, COMMUNITY USE, and PERMISSIONS. A table lists 16 apps with columns for Name, Authorized by, Permission level, Last authorized, and Actions. The table includes entries like 'asc-cas integration rs', 'FastTrack', 'Spanning Backup', 'Graph Explorer', 'Office 365 Service Trust...', 'Azure AD Connector - P...', and 'AvePoint Online Services'.

Name	Authorized by	Permission level	Last authorized	Actions
asc-cas integration rs	2 users	High	Aug 14, 2018, 2:19 PM	✓ ⓧ ⋮
FastTrack	1 user	Low	Apr 6, 2018, 10:00 PM	✓ ⓧ ⋮
Spanning Backup	1 user	Low	Aug 14, 2018, 9:05 AM	✓ ⓧ ⋮
Graph Explorer	1 user	Low	Jan 12, 2018, 1:33 AM	✓ ⓧ ⋮
Office 365 Service Trust...	1 user	Medium	Sep 11, 2018, 7:01 PM	✓ ⓧ ⋮
Azure AD Connector - P...	1 user	High	Sep 5, 2018, 4:45 AM	✓ ⓧ ⋮
AvePoint Online Services	1 user	Low	Aug 21, 2018, 10:32 AM	✓ ⓧ ⋮