Microsoft Cloud App Security

One portal for insights and management of Cloud Applications

Who am I

- Frans Oudendorp
- Consultant

- Modern Workplace
- Security
- Microsoft P-TSP

Twitter - @Oudendorp

Blog – TalkingWorkplace.com

MICROSOFT’S SECURITY APPROACH

Identity and Access Management

Protect users’ identities and control access to valuable resources.

Information Protection

Ensure documents and emails are seen only by authorized people.

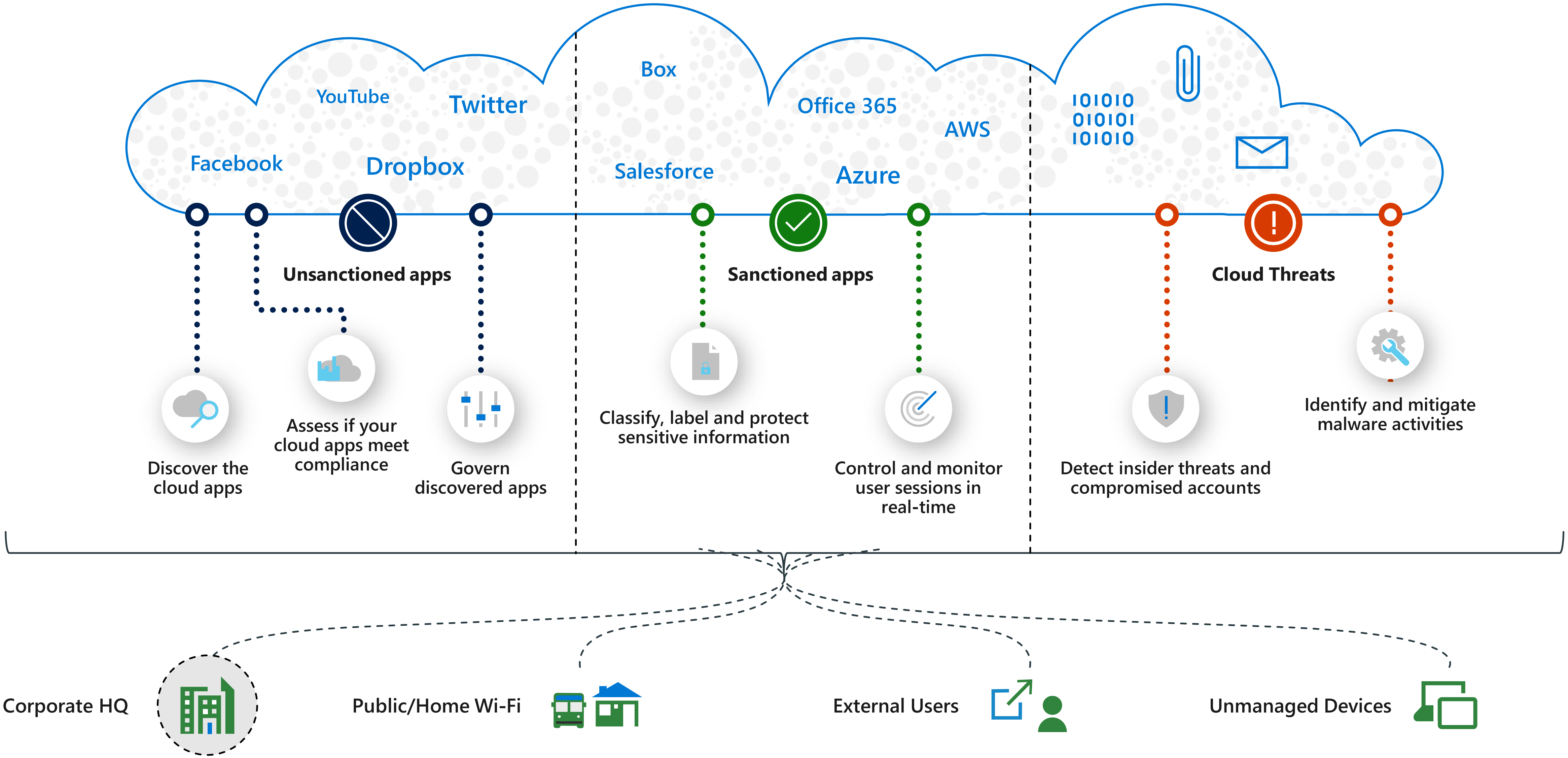
Threat Protection

Protect against advanced threats and recover quickly when attacked.

Security Management

Gain visibility and control over security tool.

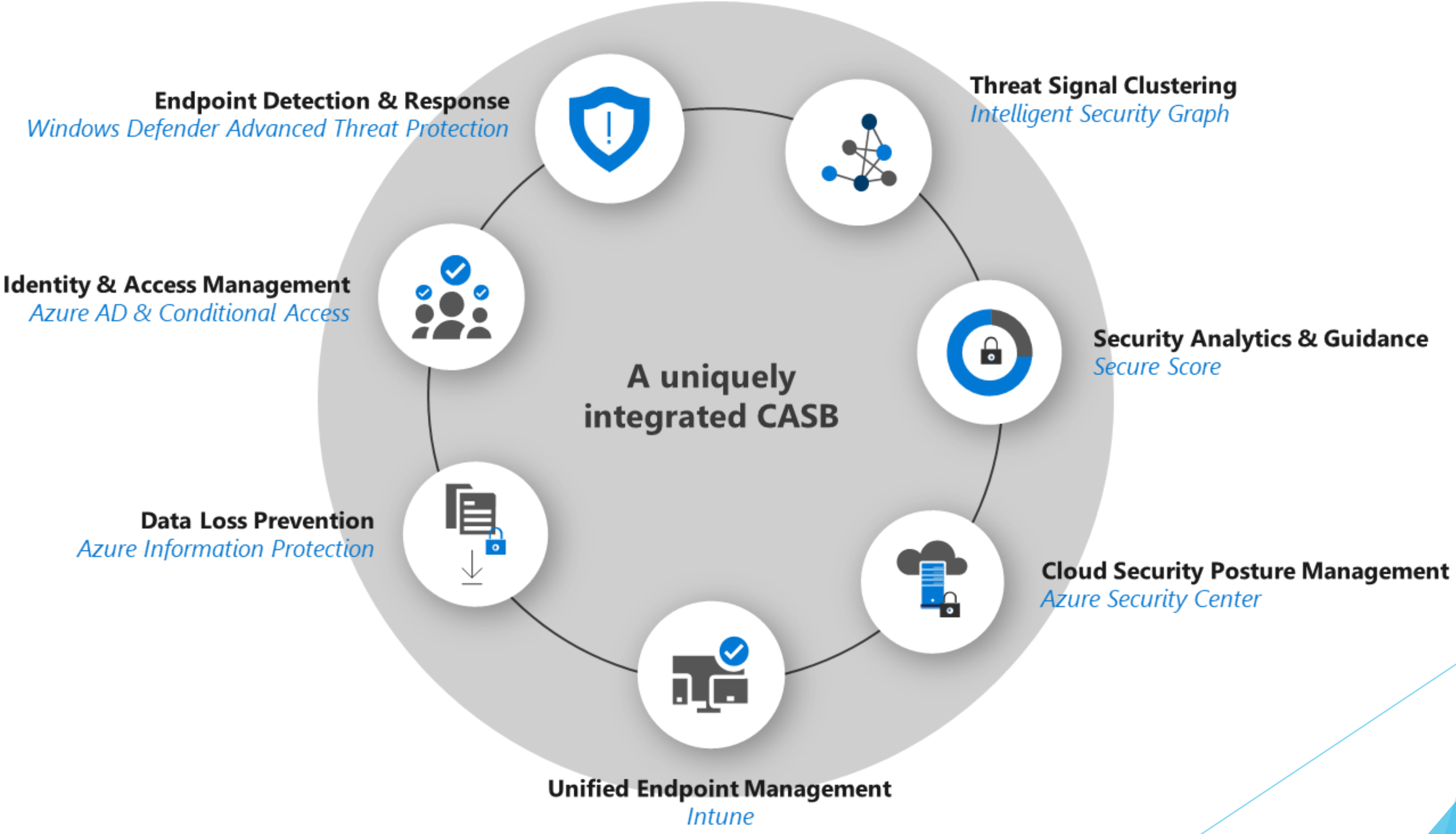
CASB USE CASES



Sensitivity: Regular

MICROSOFT CLOUD APP SECURITY

Natively integrated with Microsoft 365 and beyond



Endpoint Detection & Response
Windows Defender Advanced Threat Protection

Threat Signal Clustering
Intelligent Security Graph

Identity & Access Management
Azure AD & Conditional Access

A uniquely integrated CASB

Security Analytics & Guidance
Secure Score

Data Loss Prevention
Azure Information Protection

Cloud Security Posture Management
Azure Security Center

Unified Endpoint Management
Intune

Sensitivity: Regular

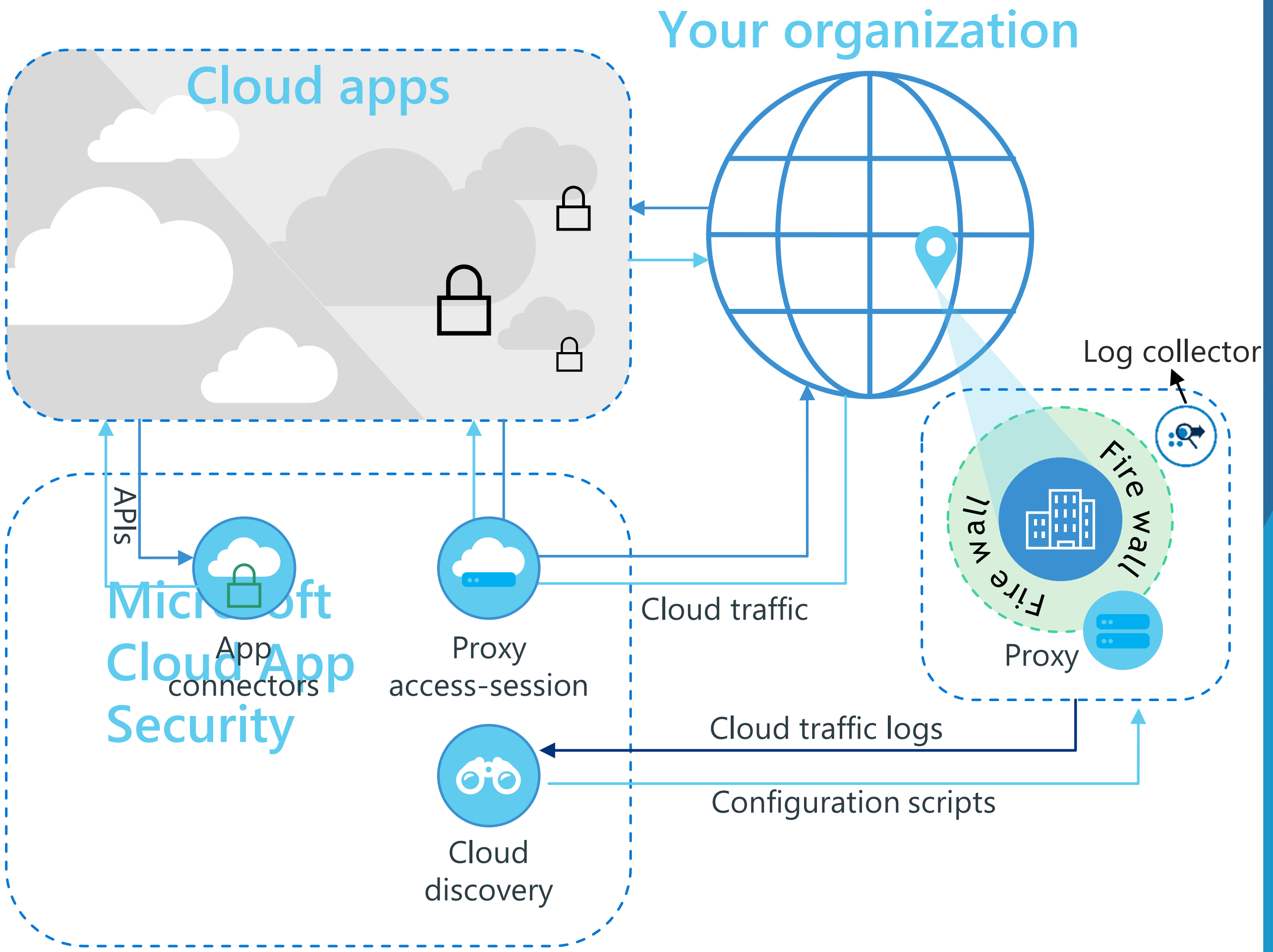
How Microsoft Cloud App Security works

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



Sensitivity: Regular

Detect

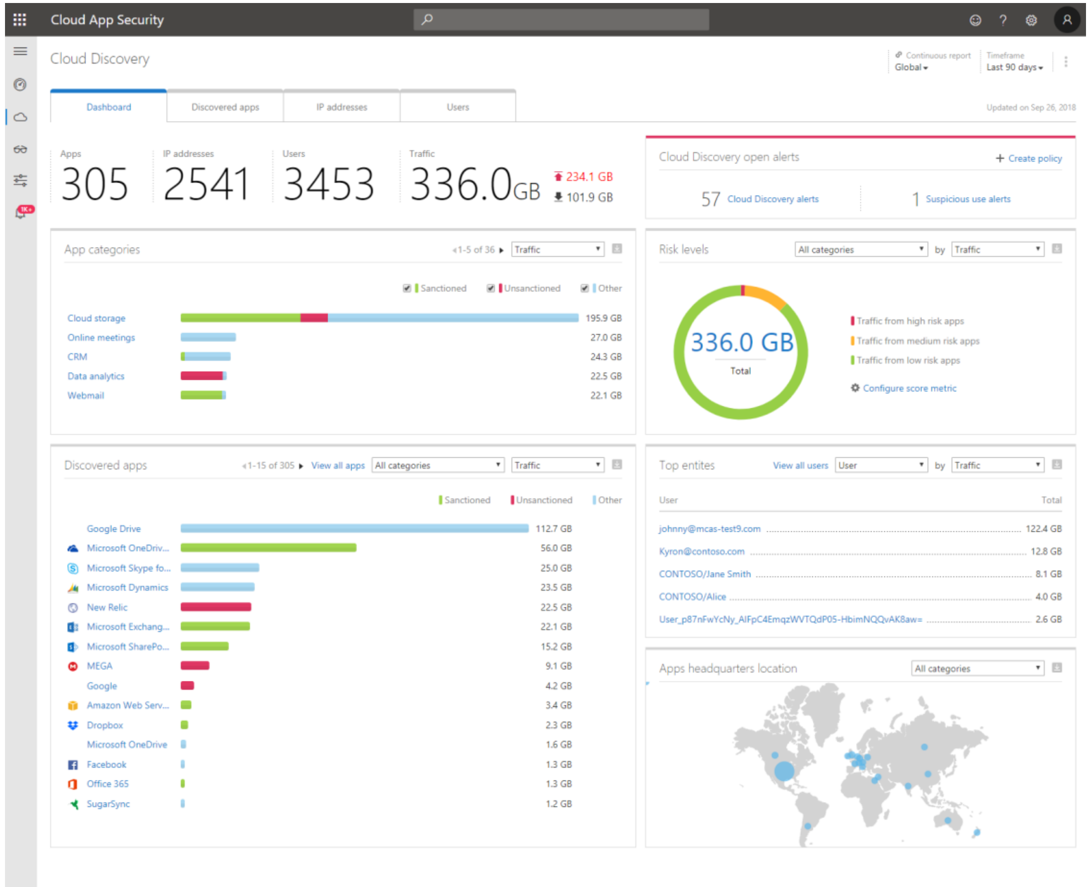
Cloud App Discovery

Discovery of Shadow IT

Discover cloud usage across all locations (HQ, Branches, Remote..)

Understand the risk of your apps

Risk assessment for 16,000+ cloud apps based on 70+ security and compliance risk factors



Apps	IP addresses	Users	Traffic
305	2541	3453	336.0GB 234.1 GB 101.9 GB

Cloud Discovery open alerts

+ Create policy

57 Cloud Discovery alerts

1 Suspicious use alerts

App categories

◂1-5 of 36 ▸ Traffic ▾

☑ Sanctioned ☑ Unsanctioned ☑ Other

Cloud storage	195.9 GB
Online meetings	27.0 GB
CRM	24.3 GB
Data analytics	22.5 GB
Webmail	22.1 GB

Risk levels

All categories ▾ by Traffic ▾

336.0 GB
Total

🟥 Traffic from high risk apps

🟧 Traffic from medium risk apps

🟩 Traffic from low risk apps

Configure score metric

Discovered apps

◂1-15 of 305 ▸ View all apps All categories ▾ Traffic ▾

Sanctioned Unsanctioned Other

Google Drive	112.7 GB
Microsoft OneDriv...	56.0 GB
Microsoft Skype fo...	25.0 GB
Microsoft Dynamics	23.5 GB
New Relic	22.5 GB
Microsoft Exchang...	22.1 GB
Microsoft SharePo...	15.2 GB
MEGA	9.1 GB
Google	4.2 GB
Amazon Web Serv...	3.4 GB
Dropbox	2.3 GB
Microsoft OneDrive	1.6 GB
Facebook	1.3 GB
Office 365	1.3 GB
SugarSync	1.2 GB

Top entites

View all users User ▾ by Traffic ▾

User	Total
johnny@mcas-test9.com	122.4 GB
Kyron@contoso.com	12.8 GB
CONTOSO/Jane Smith	8.1 GB
CONTOSO/Alice	4.0 GB
User_p87nFwYcNy_AlFpC4EmqzWVTQdP05-HbimNQQvAK8aw=	2.6 GB

Apps headquarters location

All categories ▾

Integrate with your Secure Web Gateway

Enhanced visibility into Shadow IT and risk

Connect your existing Zscaler or iboss deployment to Cloud App Security for Discovery of Shadow IT

Seamless integration

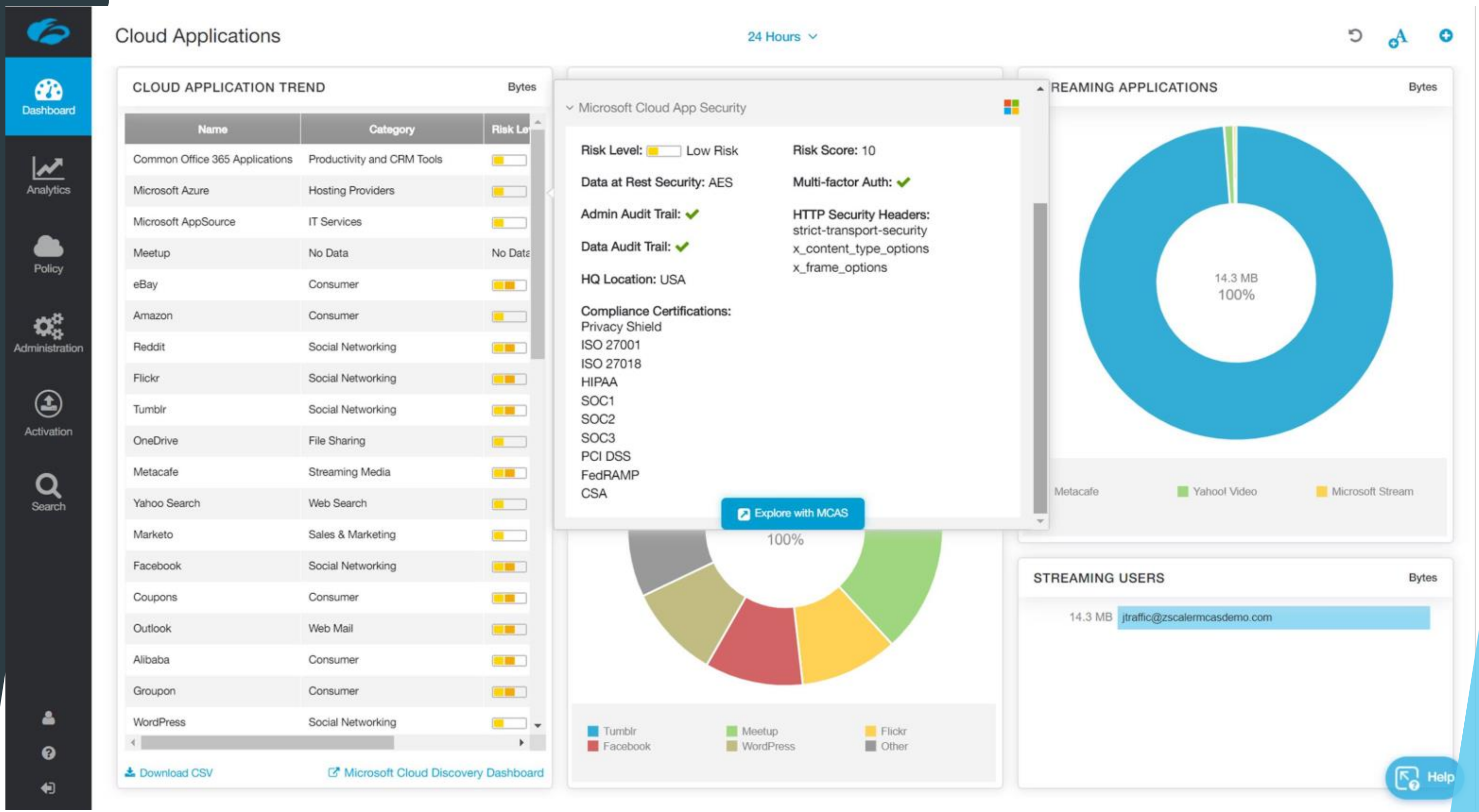
Pivot from SWG portal to Cloud App Security for comprehensive risk assessment and investigation of user traffic

Control access to discovered cloud apps

Automatically sync apps that you tag as unsanctioned within Cloud App Security to your SWG and control user access

Removes the need to deploy a separate log collector

Stream data directly from SWG to Cloud App security with no additional deployments



Cloud Applications

CLOUD APPLICATION TREND — Bytes

Name	Category	Risk Le
Common Office 365 Applications	Productivity and CRM Tools	▮
Microsoft Azure	Hosting Providers	▮
Microsoft AppSource	IT Services	▮
Meetup	No Data	No Data
eBay	Consumer	▮▮
Amazon	Consumer	▮
Reddit	Social Networking	▮▮
Flickr	Social Networking	▮▮
Tumblr	Social Networking	▮▮
OneDrive	File Sharing	▮
Metacafe	Streaming Media	▮▮
Yahoo Search	Web Search	▮
Marketo	Sales & Marketing	▮
Facebook	Social Networking	▮▮
Coupons	Consumer	▮▮
Outlook	Web Mail	▮▮
Alibaba	Consumer	▮▮
Groupon	Consumer	▮▮
WordPress	Social Networking	▮

Download CSV

Microsoft Cloud Discovery Dashboard

Microsoft Cloud App Security

Risk Level: ▮ Low Risk

Data at Rest Security: AES

Admin Audit Trail: ✓

Data Audit Trail: ✓

HQ Location: USA

Compliance Certifications:
Privacy Shield
ISO 27001
ISO 27018
HIPAA
SOC1
SOC2
SOC3
PCI DSS
FedRAMP
CSA

Risk Score: 10

Multi-factor Auth: ✓

HTTP Security Headers:
strict-transport-security
x_content_type_options
x_frame_options

Explore with MCAS

STREAMING USERS — Bytes

14.3 MB jtraffic@zscalermcasdemo.com

Discover and manage risky OAuth apps

Discover OAuth apps

That users have authorized to connect to your Office 365 envrionment

Identify and manage permission levels

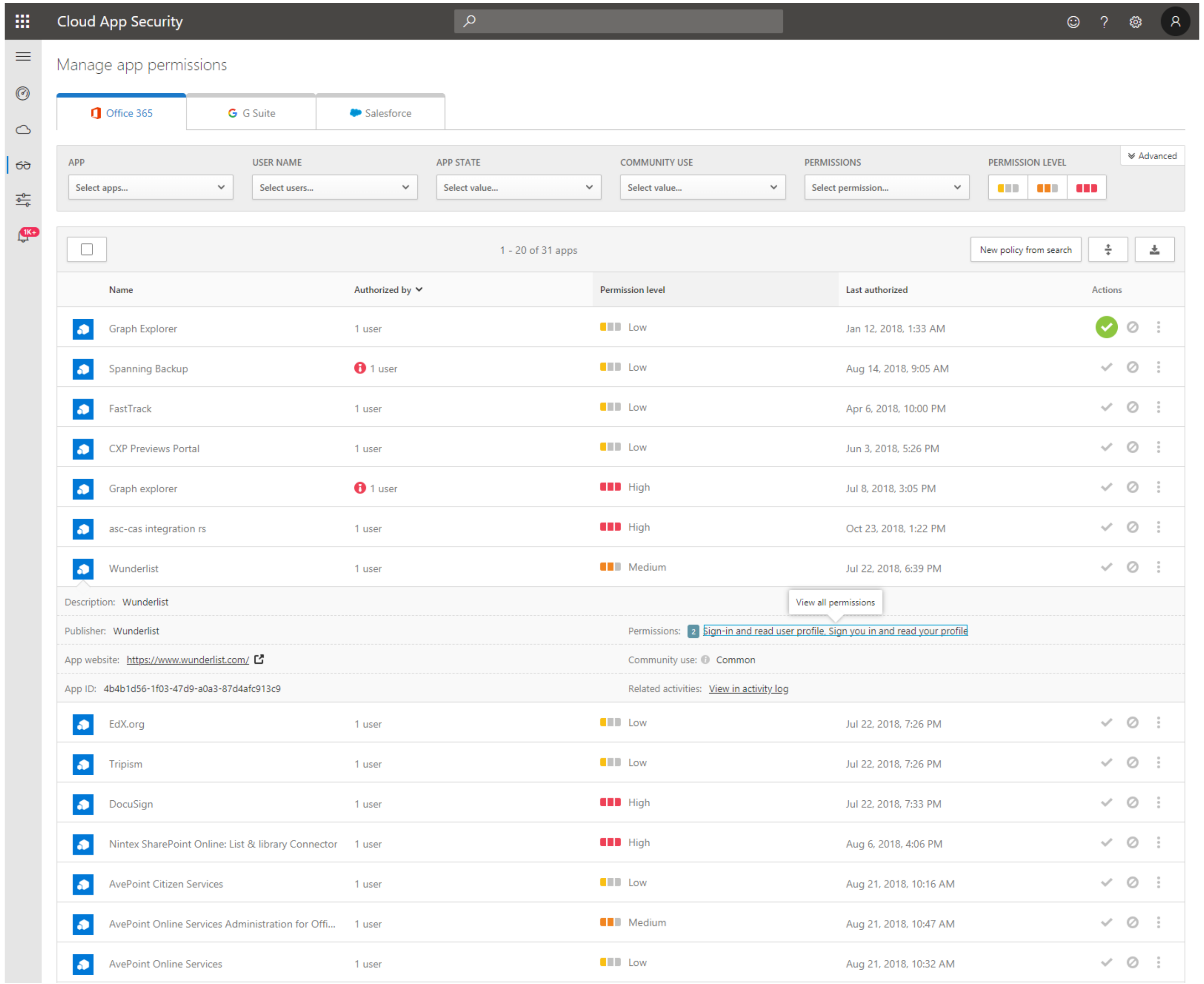
Understand the implications to your business and take action

Define custom policies

to alert on trending, new and risky apps in use

Automatically revoke apps

for the entire organization or specific users and groups



Manage app permissions

1 - 20 of 31 apps

Name	Authorized by	Permission level	Last authorized	Actions
Graph Explorer	1 user	Low	Jan 12, 2018, 1:33 AM	✓ ⊘ ⋮
Spanning Backup	❗ 1 user	Low	Aug 14, 2018, 9:05 AM	✓ ⊘ ⋮
FastTrack	1 user	Low	Apr 6, 2018, 10:00 PM	✓ ⊘ ⋮
CXP Previews Portal	1 user	Low	Jun 3, 2018, 5:26 PM	✓ ⊘ ⋮
Graph explorer	❗ 1 user	High	Jul 8, 2018, 3:05 PM	✓ ⊘ ⋮
asc-cas integration rs	1 user	High	Oct 23, 2018, 1:22 PM	✓ ⊘ ⋮
Wunderlist	1 user	Medium	Jul 22, 2018, 6:39 PM	✓ ⊘ ⋮

Description: Wunderlist

View all permissions

Publisher: Wunderlist

Permissions: 2 Sign-in and read user profile, Sign you in and read your profile

App website: https://www.wunderlist.com/

Community use: Common

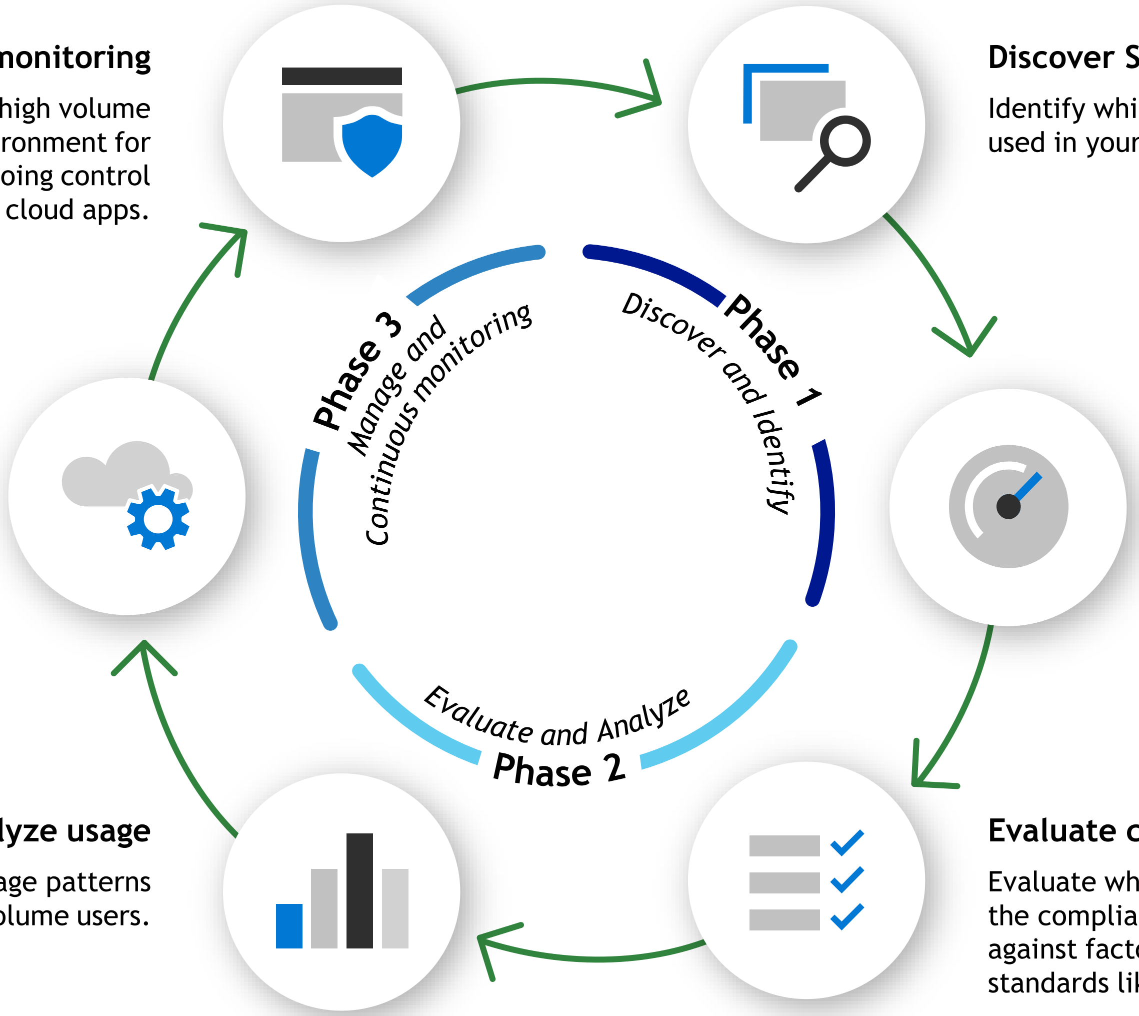
App ID: 4b4b1d56-1f03-47d9-a0a3-87d4afc913c9

Related activities: View in activity log

Name	Authorized by	Permission level	Last authorized	Actions
EdX.org	1 user	Low	Jul 22, 2018, 7:26 PM	✓ ⊘ ⋮
Tripism	1 user	Low	Jul 22, 2018, 7:26 PM	✓ ⊘ ⋮
DocuSign	1 user	High	Jul 22, 2018, 7:33 PM	✓ ⊘ ⋮
Nintex SharePoint Online: List & library Connector	1 user	High	Aug 6, 2018, 4:06 PM	✓ ⊘ ⋮
AvePoint Citizen Services	1 user	Low	Aug 21, 2018, 10:16 AM	✓ ⊘ ⋮
AvePoint Online Services Administration for Offi...	1 user	Medium	Aug 21, 2018, 10:47 AM	✓ ⊘ ⋮
AvePoint Online Services	1 user	Low	Aug 21, 2018, 10:32 AM	✓ ⊘ ⋮

Shadow IT Discovery Lifecycle

Safely adopting cloud apps



Phase 1
Discover and Identify

Phase 2
Evaluate and Analyze

Phase 3
Manage and Continuous monitoring

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.

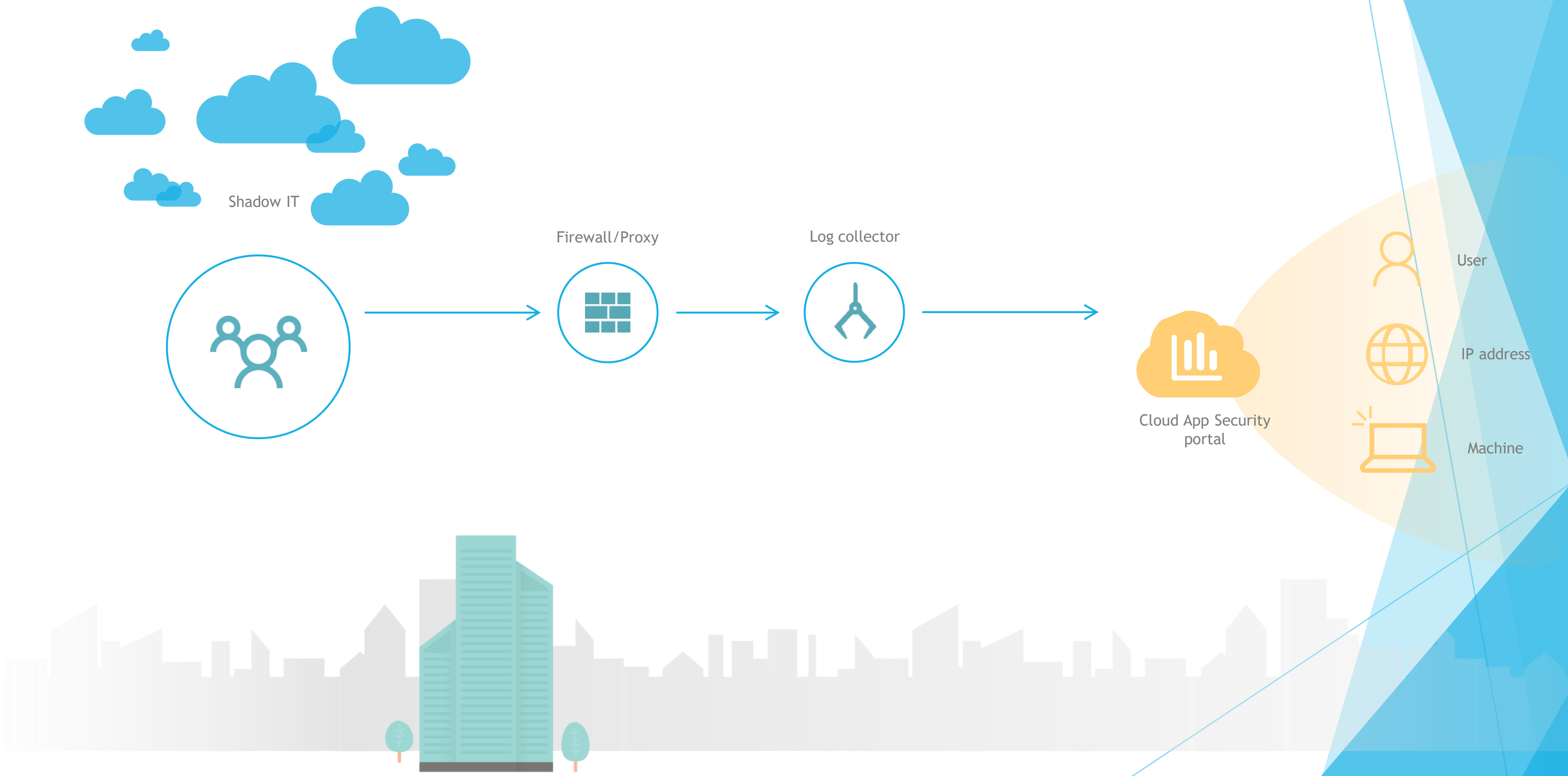
Manage cloud apps

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.

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.

MCAS Cloud Discovery architecture



Cloud Discovery with Microsoft Defender ATP

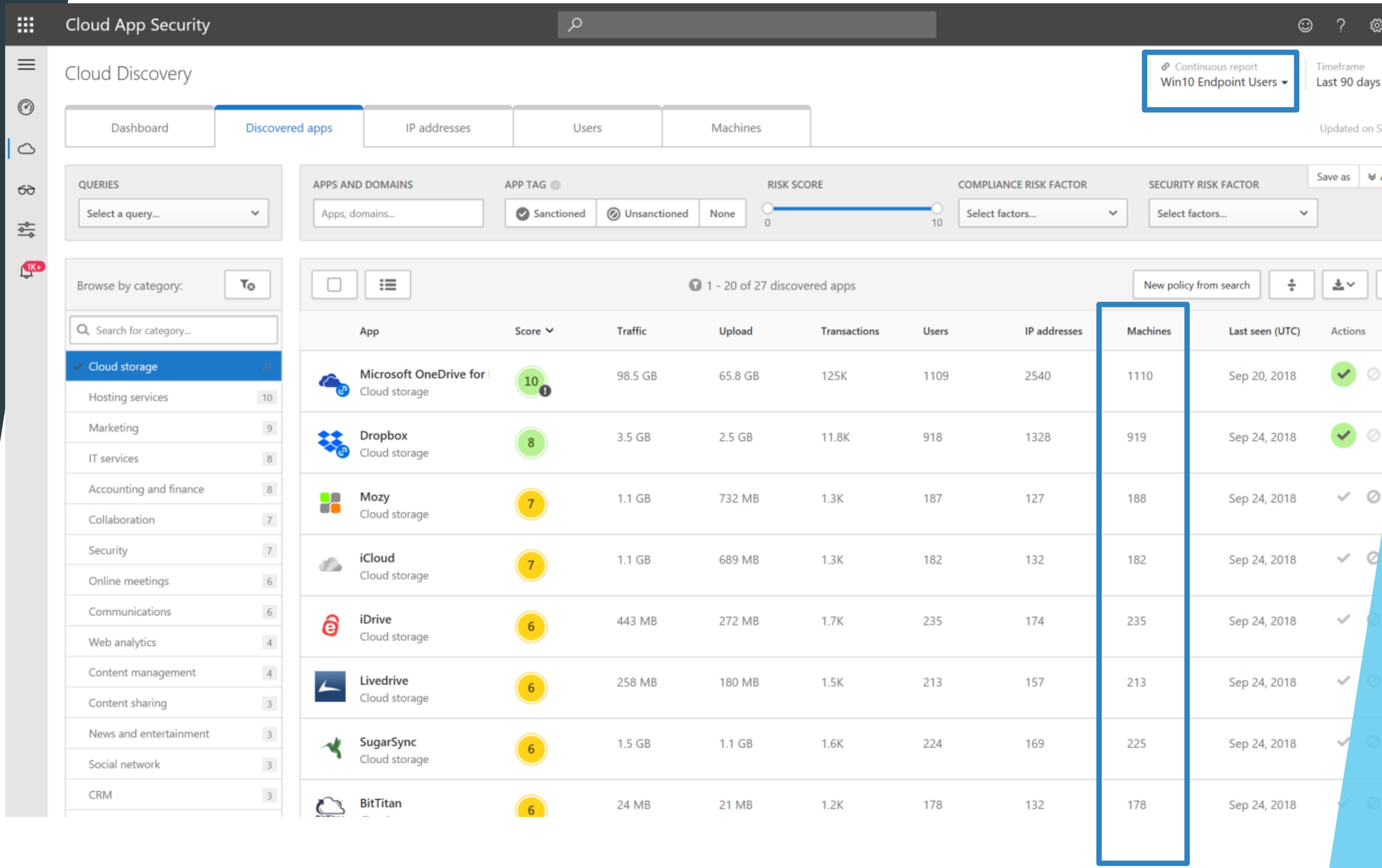
Native, endpoint-based Discovery of Shadow IT

Discovery of cloud apps beyond the corporate network from any Windows 10 machine

Single-click enablement

Machine-based Discovery

Deep dive investigation in Windows Defender ATP

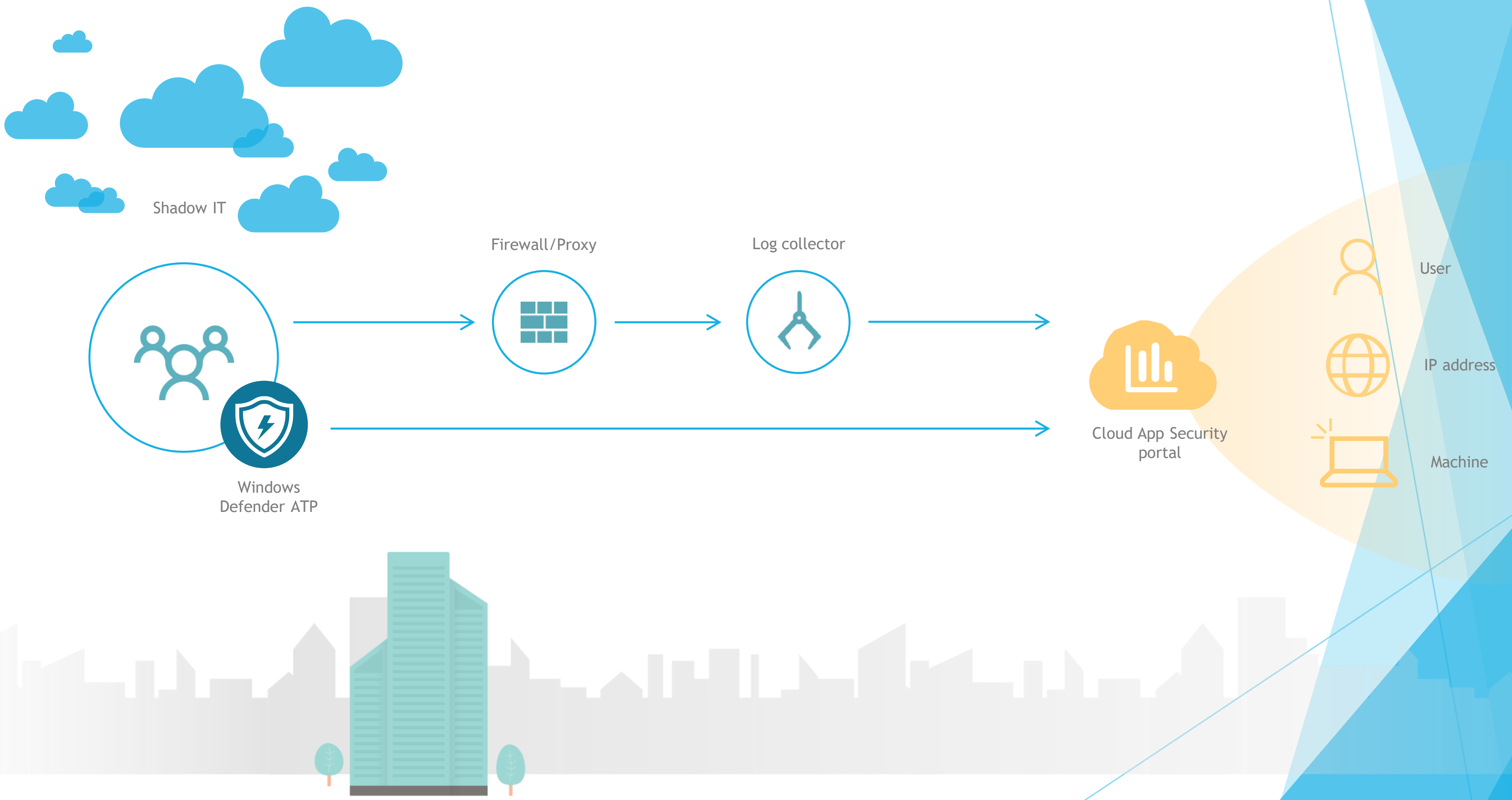


1 - 20 of 27 discovered apps

Browse by category	
Cloud storage	27
Hosting services	10
Marketing	9
IT services	8
Accounting and finance	8
Collaboration	7
Security	7
Online meetings	6
Communications	6
Web analytics	4
Content management	4
Content sharing	3
News and entertainment	3
Social network	3
CRM	3

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Machines	Last seen (UTC)	Actions
Microsoft OneDrive for Cloud storage	10	98.5 GB	65.8 GB	125K	1109	2540	1110	Sep 20, 2018	✓
Dropbox Cloud storage	8	3.5 GB	2.5 GB	11.8K	918	1328	919	Sep 24, 2018	✓
Mozy Cloud storage	7	1.1 GB	732 MB	1.3K	187	127	188	Sep 24, 2018	
iCloud Cloud storage	7	1.1 GB	689 MB	1.3K	182	132	182	Sep 24, 2018	
iDrive Cloud storage	6	443 MB	272 MB	1.7K	235	174	235	Sep 24, 2018	
Livedrive Cloud storage	6	258 MB	180 MB	1.5K	213	157	213	Sep 24, 2018	
SugarSync Cloud storage	6	1.5 GB	1.1 GB	1.6K	224	169	225	Sep 24, 2018	
BitTitan	6	24 MB	21 MB	1.2K	178	132	178	Sep 24, 2018	

MCAS Cloud Discovery architecture



Sensitivity: Regular

Demo

Shadow IT Discovery en MDATP integratie

Protect

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

SAML, Open ID Connect, & on-prem apps

Support for Microsoft and non-Microsoft web apps, including on-prem apps onboarded via Azure AD App proxy

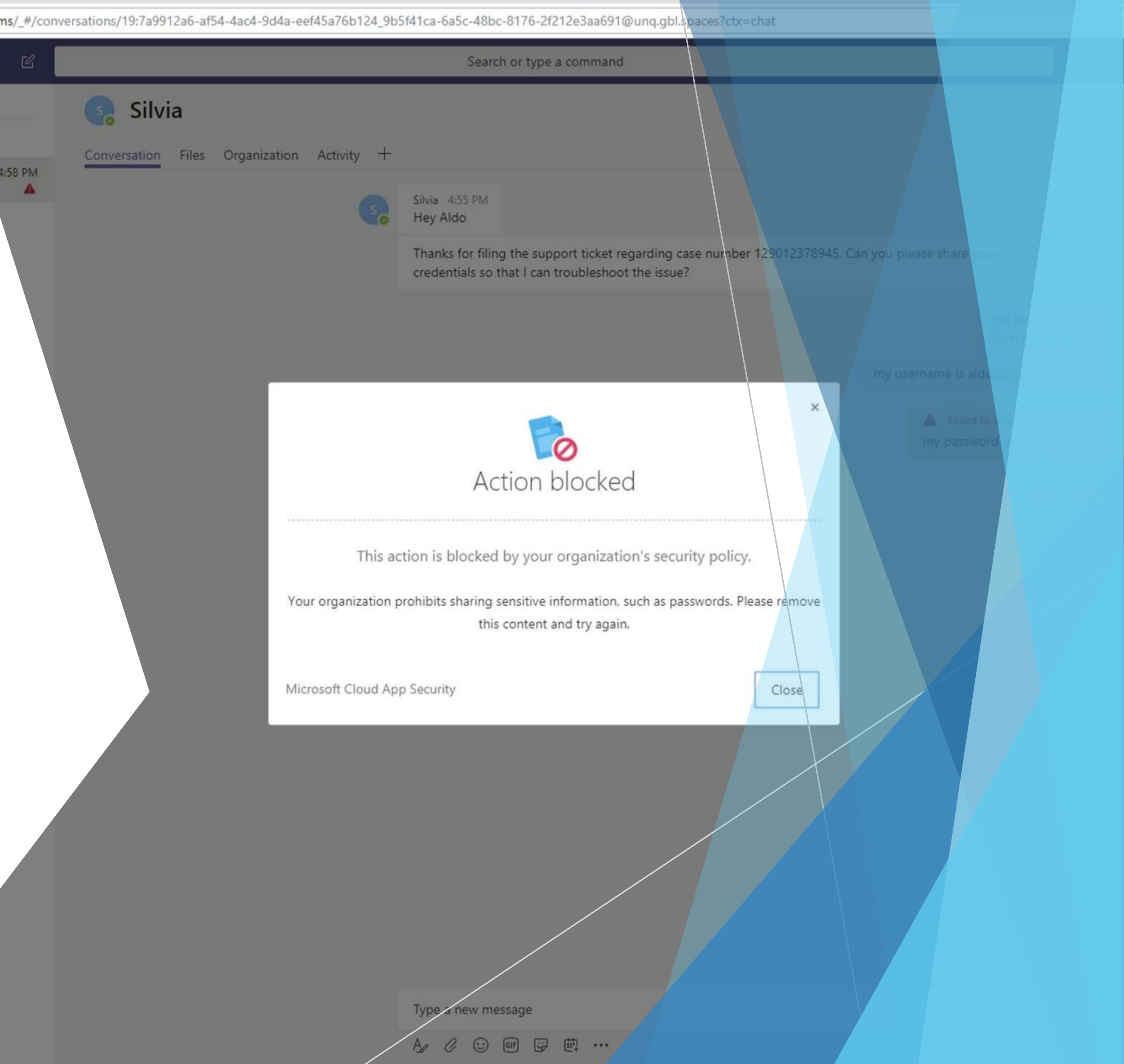
Enforce granular monitoring & control for risky user sessions

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



m.us2.cas.ms/_#/conversations/19:7a9912a6-af54-4ac4-9d4a-eef45a76b124_9b5f41ca-6a5c-48bc-8176-2f212e3aa691@unq.gbl.spaces?ctx=chat

Silvia 4:55 PM
Hey Aldo

Thanks for filing the support ticket regarding case number 129012378945. Can you please share your credentials so that I can troubleshoot the issue?

my username is aldo@m

Failed to s
my password

Action blocked

This action is blocked by your organization's security policy.

Your organization prohibits sharing sensitive information, such as passwords. Please remove this content and try again.

Microsoft Cloud App Security

Sensitivity: Regular

Conditional Access App Control

Unique integration with Azure AD Conditional Access

Selective routing to MCAS based on the session risk determined by Conditional Access to optimize end user productivity

Simple deployment

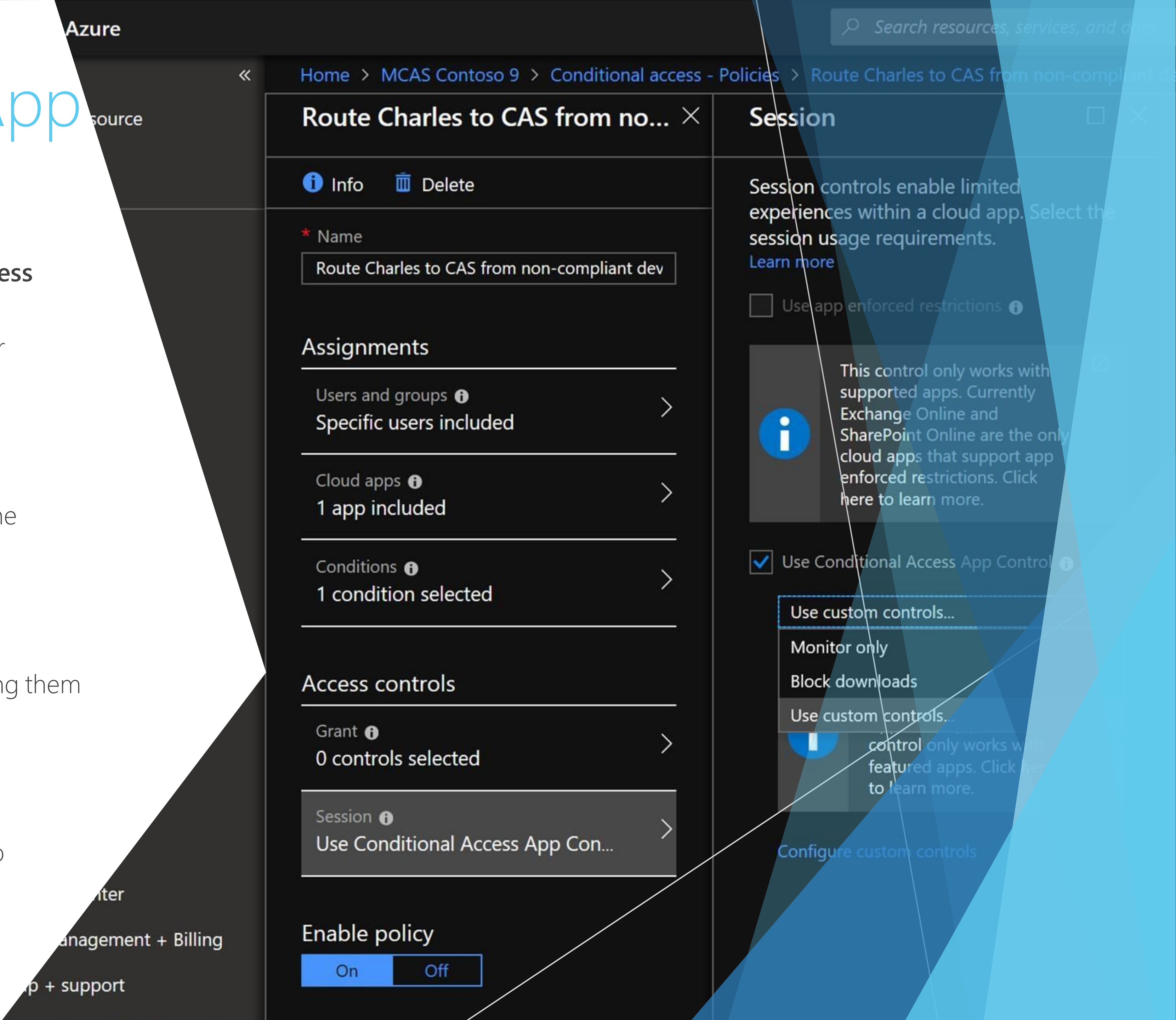
Built-in policies that can be configured directly within the Azure AD portal for an easy deployment.

Control your on-prem apps

With the same powerful real-time controls by integrating them with Azure AD Application Proxy

Worldwide Azure datacenters infrastructure

MCAS leverages Azure data centers across the world to optimize performance and user experience



Azure
Search resources, services, and d...
Home > MCAS Contoso 9 > Conditional access - Policies > Route Charles to CAS from non-compliant
source
iter
anagement + Billing
p + support

Route Charles to CAS from no...

Info | Delete

* Name: Route Charles to CAS from non-compliant dev

Assignments

Users and groups: Specific users included

Cloud apps: 1 app included

Conditions: 1 condition selected

Access controls

Grant: 0 controls selected

Session: Use Conditional Access App Con...

Enable policy: ● On ○ Off

Session

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

□ Use app enforced restrictions

This control only works with supported apps. Currently Exchange Online and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

☑ Use Conditional Access App Control

Use custom controls...

- Monitor only
- Block downloads
- Use custom controls...

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

Configure custom controls

Sensitivity: Regular

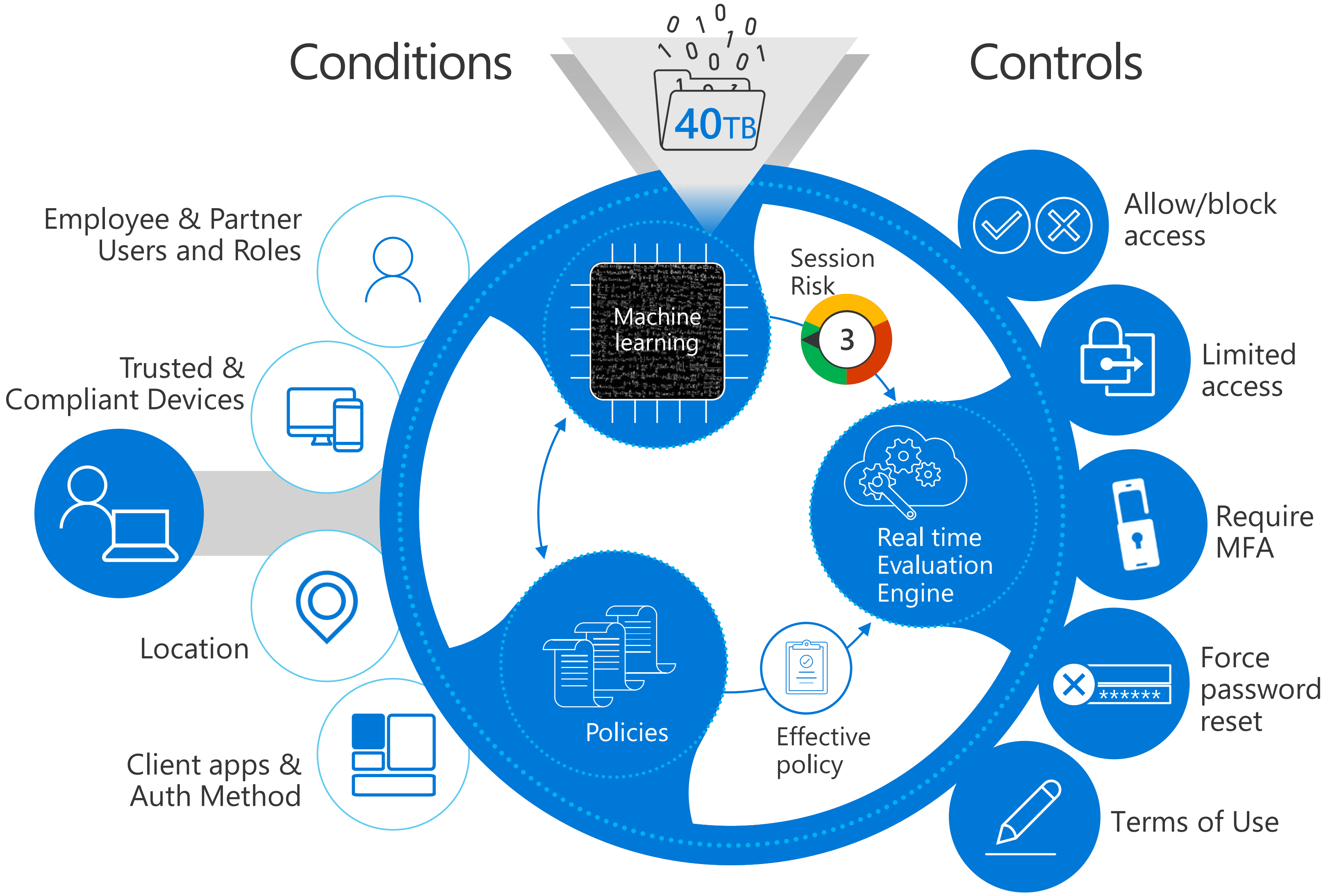
AZURE AD CONDITIONAL ACCESS

- Azure AD
- ADFS
- MSA
- Google ID

- Android
- iOS
- MacOS
- Windows
- Windows Defender ATP

- Geo-location
- Corporate Network

- Browser apps
- Client apps



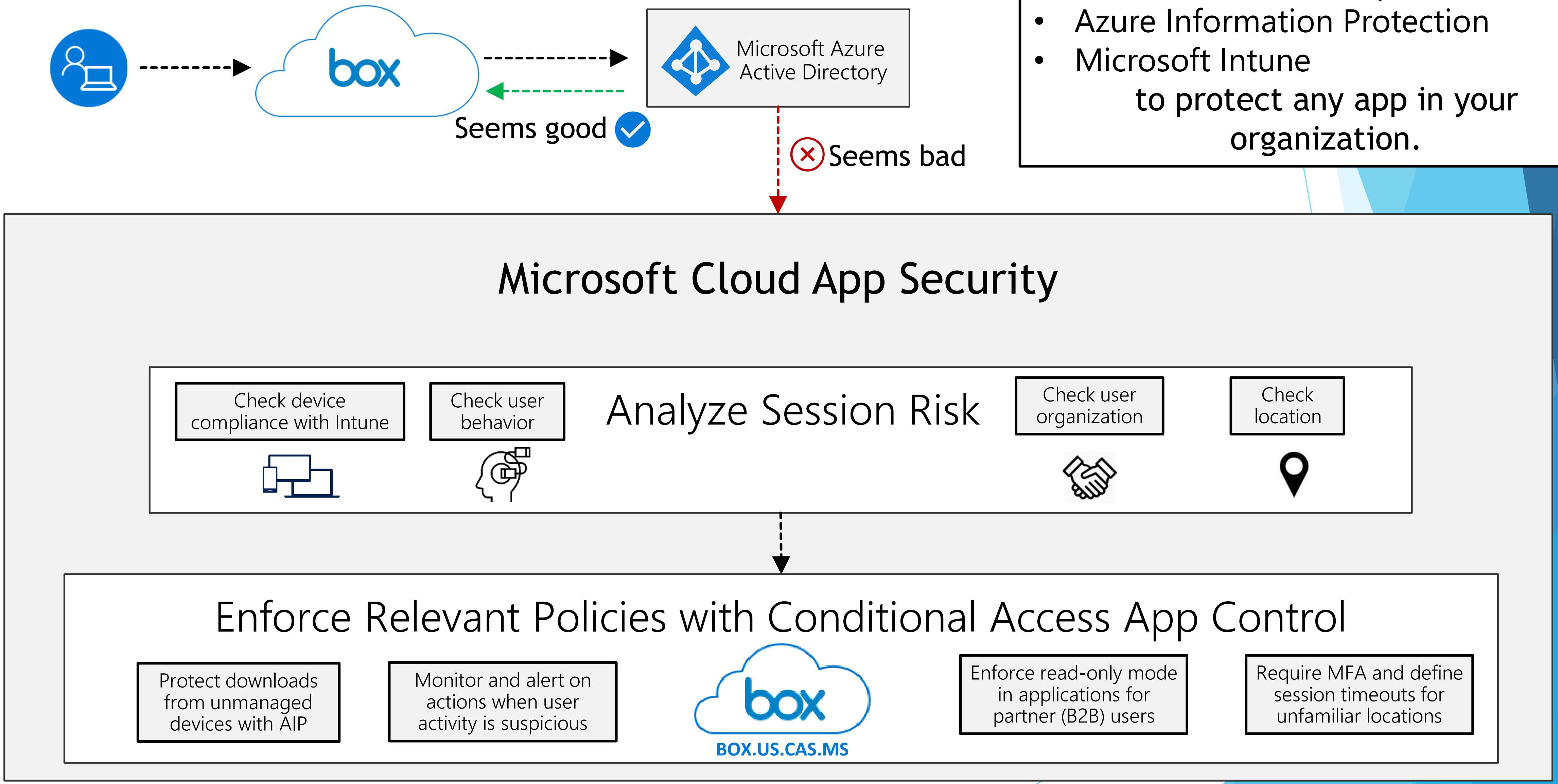
CONDITIONAL ACCESS APP CONTROL

Microsoft is better together!

Cloud App Security integrates with:

- Azure Active Directory
- Azure Information Protection
- Microsoft Intune

to protect any app in your organization.



Microsoft Azure Active Directory

Seems good

Seems bad

Microsoft Cloud App Security

Analyze Session Risk

Check device compliance with Intune

Check user behavior

Check user organization

Check location

Enforce Relevant Policies with Conditional Access App Control

Protect downloads from unmanaged devices with AIP

Monitor and alert on actions when user activity is suspicious

BOX.US.CAS.MS

Enforce read-only mode in applications for partner (B2B) users

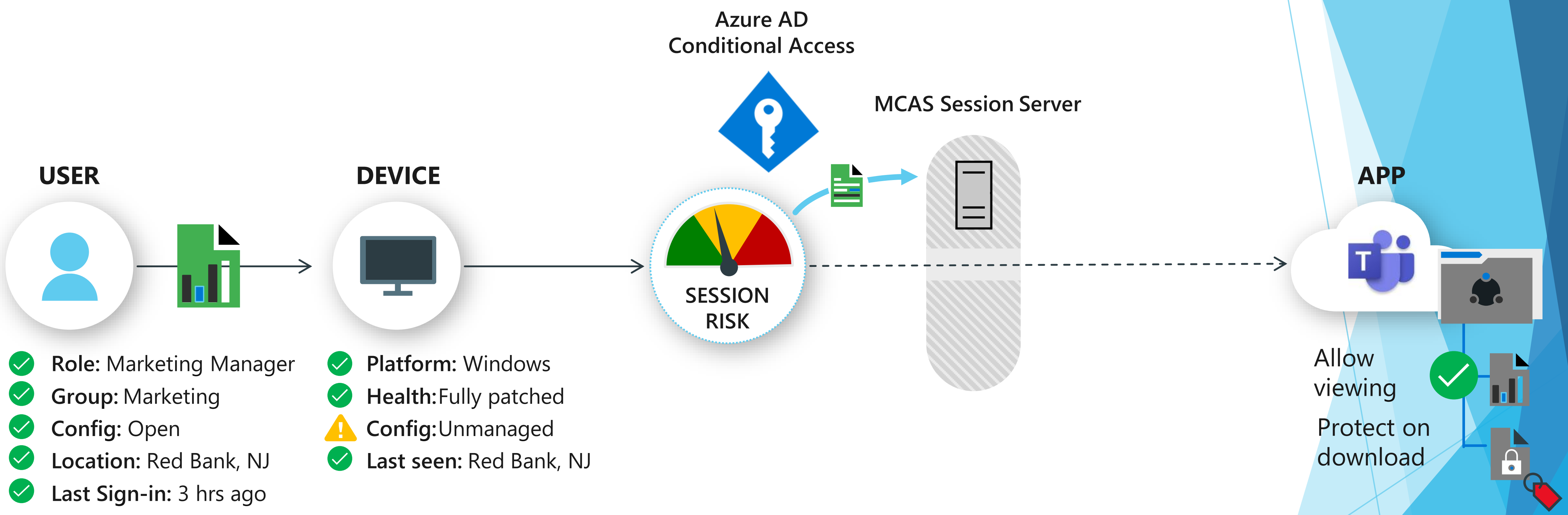
Require MFA and define session timeouts for unfamiliar locations

Demo

Conditional Access integratie

USE CASE: PREVENT DOWNLOAD OF FILES

Risk based in-session controls



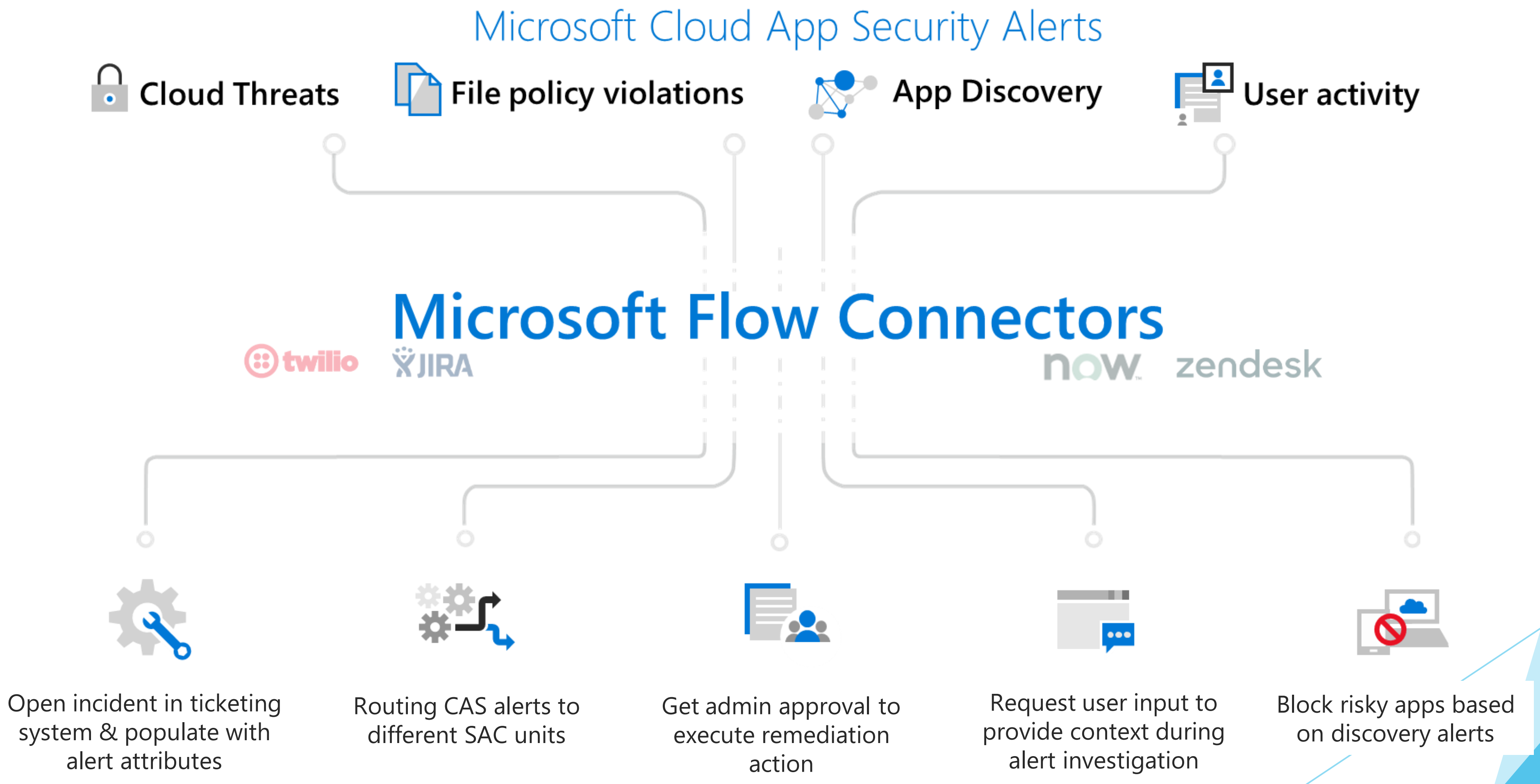
- ✓ **Role:** Marketing Manager
- ✓ **Group:** Marketing
- ✓ **Config:** Open
- ✓ **Location:** Red Bank, NJ
- ✓ **Last Sign-in:** 3 hrs ago

- ✓ **Platform:** Windows
- ✓ **Health:**Fully patched
- ⚠ **Config:**Unmanaged
- ✓ **Last seen:** Red Bank, NJ

⚠ Device is unmanaged

Respond

Automated security workflow



Microsoft Cloud App Security Alerts

Cloud Threats

File policy violations

App Discovery

User activity

Microsoft Flow Connectors

Open incident in ticketing system & populate with alert attributes

Routing CAS alerts to different SAC units

Get admin approval to execute remediation action

Request user input to provide context during alert investigation

Block risky apps based on discovery alerts

Demo

Microsoft Flow integratie

Recap

- Discover the use of Cloud Applications
- Integration of other Microsoft Products in MCAS
- Protect and Monitor the use of Cloud applications
- Use Microsoft Flow to automate your security workflows

Thank You