Summer 2021: Information Security Workshop

# Microsoft Cloud App Security

# Welcome

**Introductions**

In the chat, please say hello with your name, college, and position.

**Speaker**

Dan Rojas
Information Systems Security Officer, Santa Monica College

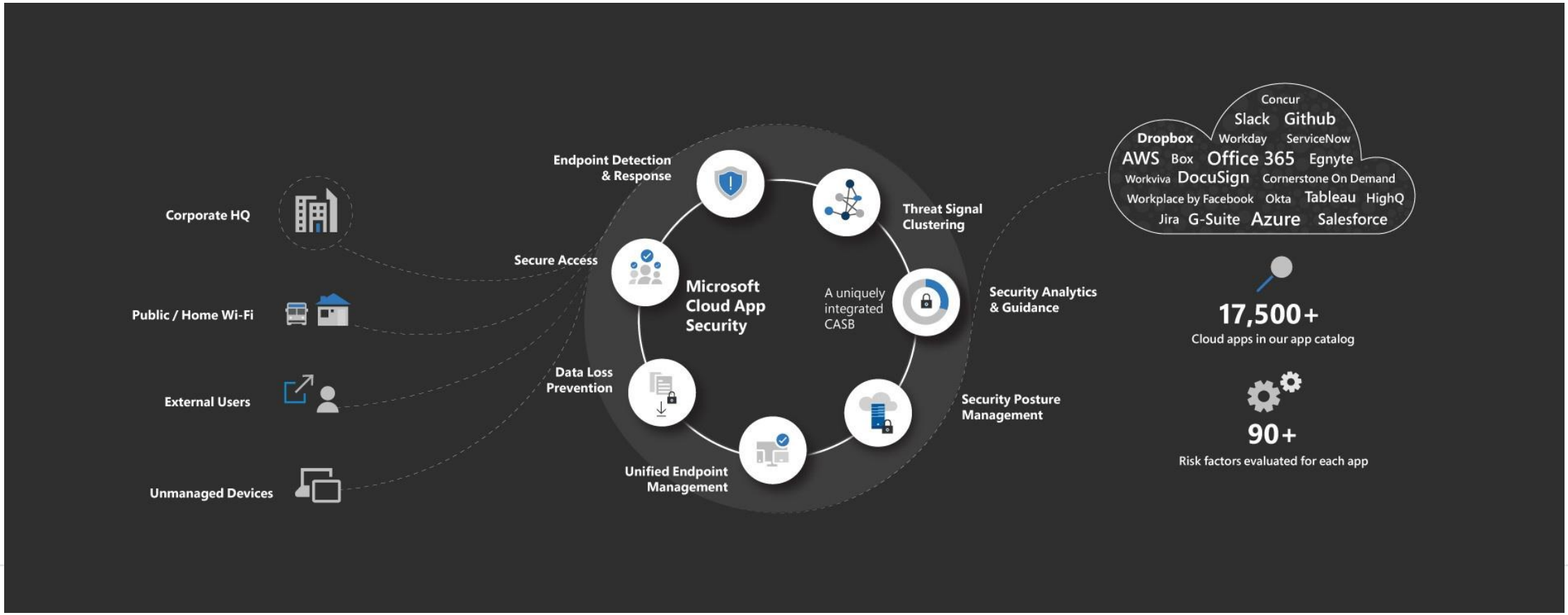
# Agenda

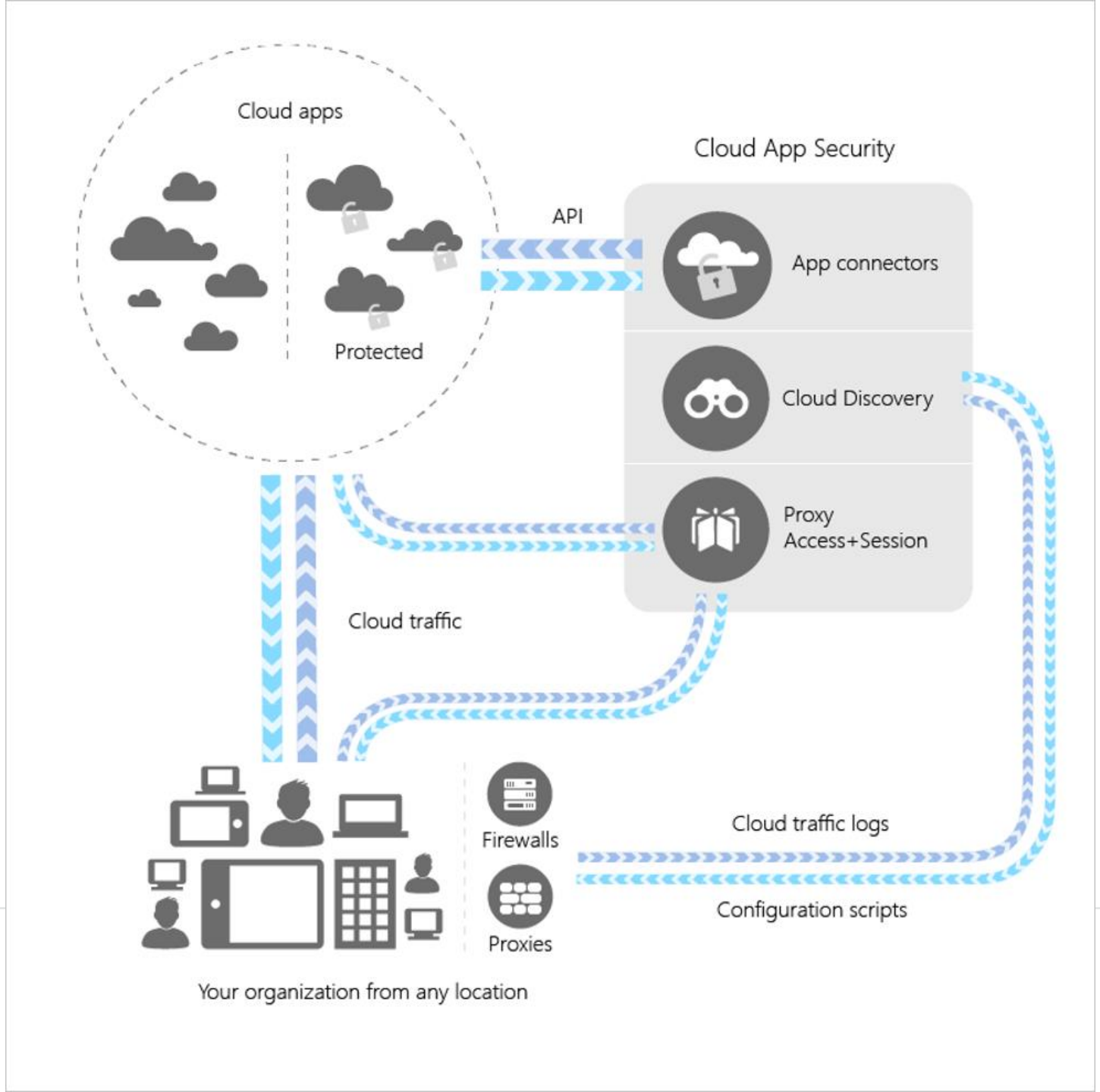
How to set up Microsoft Cloud App Security to monitor:

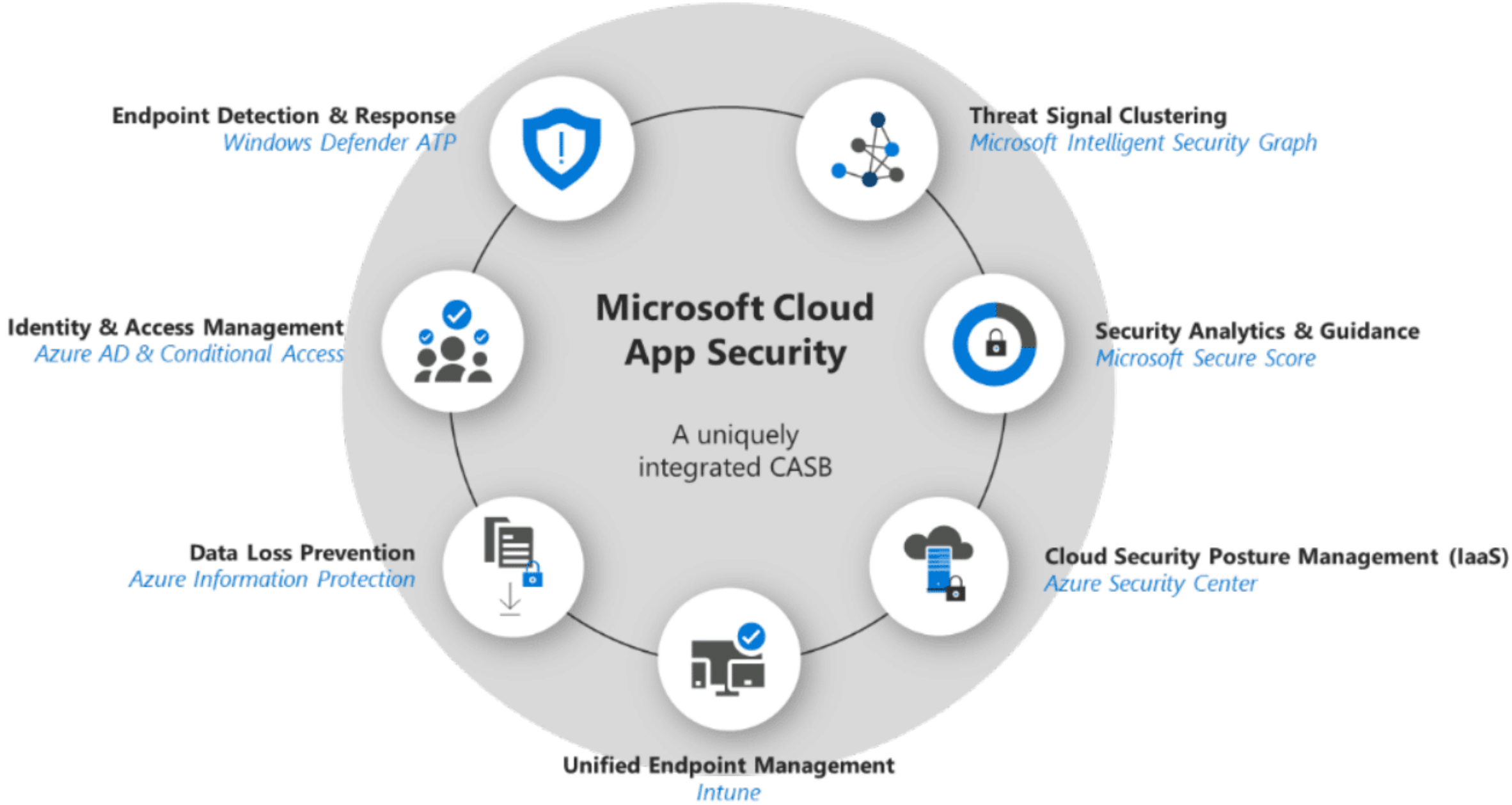
- Microsoft Defender
- Microsoft Azure
- Office 365 security assets and cyberthreats

# Microsoft Cloud App Security

- Cloud-delivered service for visibility and control of cloud apps
- Supports third-party cloud apps
- Alerts for atypical and suspicious activity
- Based on Adallom acquisition


Corporate HQ
Public / Home Wi-Fi
External Users
Unmanaged Devices
Endpoint Detection & Response
Secure Access
Data Loss Prevention
Unified Endpoint Management
Threat Signal Clustering
Security Analytics & Guidance
Security Posture Management
Microsoft Cloud App Security
A uniquely integrated CASB
Concur
Slack
Github
Dropbox
Workday
ServiceNow
AWS
Box
Office 365
Egnyte
Workviva
DocuSign
Cornerstone On Demand
Workplace by Facebook
Okta
Tableau
HighQ
Jira
G-Suite
Azure
Salesforce
17,500+
Cloud apps in our app catalog
90+
Risk factors evaluated for each app


Cloud apps
Protected
API
Cloud App Security
App connectors
Cloud Discovery
Proxy
Access+Session
Cloud traffic
Firewalls
Proxies
Cloud traffic logs
Configuration scripts
Your organization from any location


Endpoint Detection & Response
Windows Defender ATP
Threat Signal Clustering
Microsoft Intelligent Security Graph
Identity & Access Management
Azure AD & Conditional Access
Microsoft Cloud App Security
A uniquely integrated CASB
Security Analytics & Guidance
Microsoft Secure Score
Data Loss Prevention
Azure Information Protection
Cloud Security Posture Management (IaaS)
Azure Security Center
Unified Endpoint Management
Intune

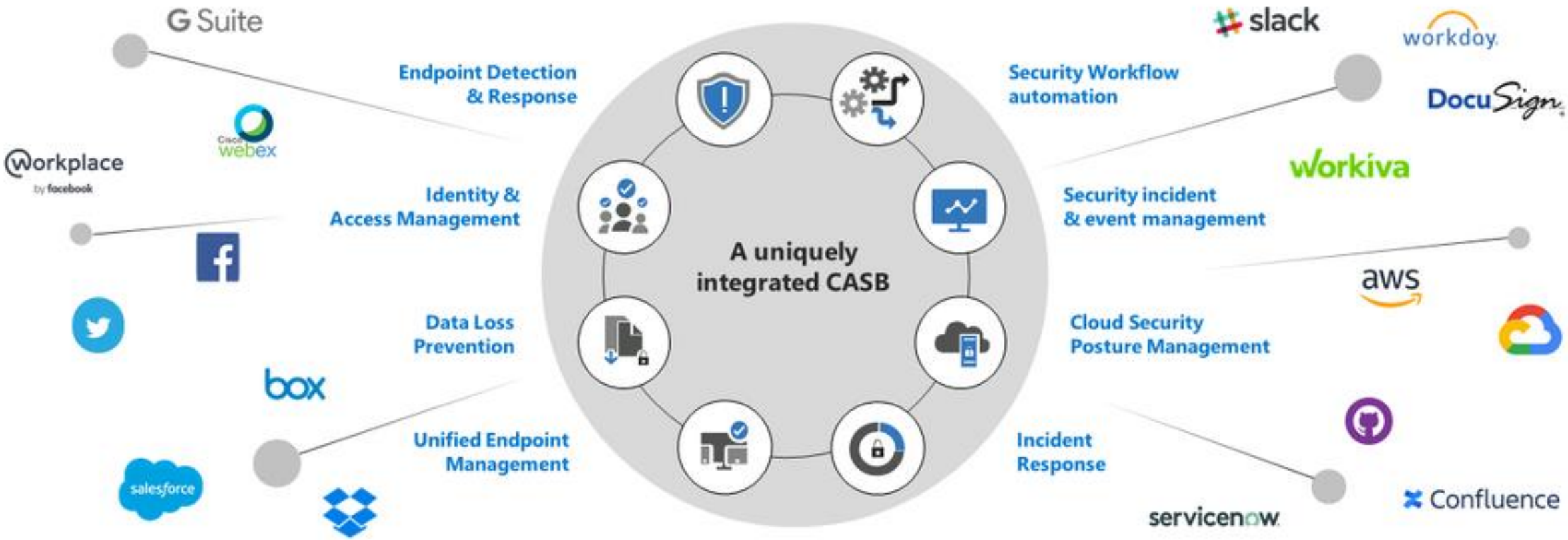
# Microsoft Cloud App Security

The go-to CASB for Office 365 and Azure that loves 3rd party

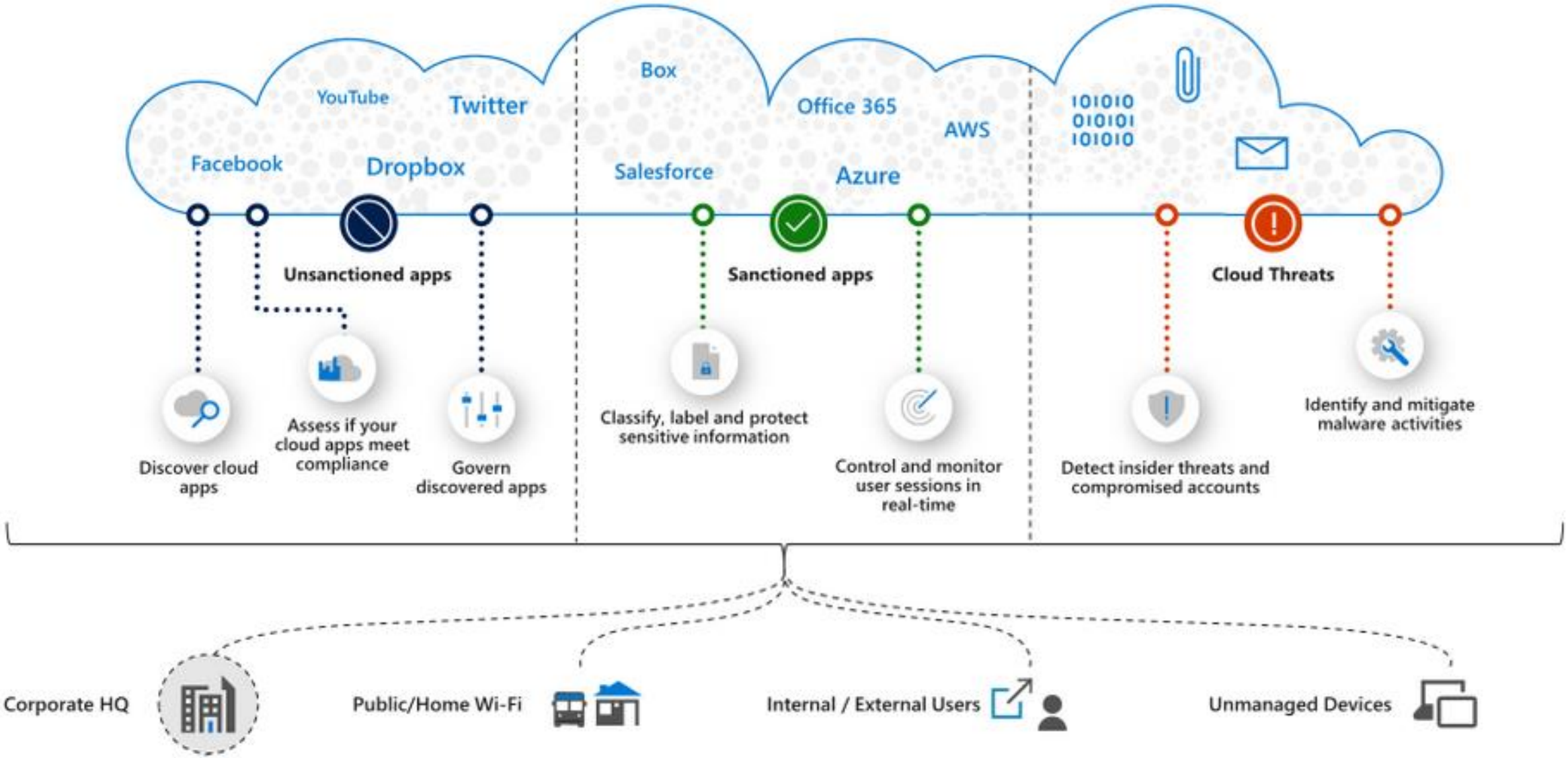
Simple deployment

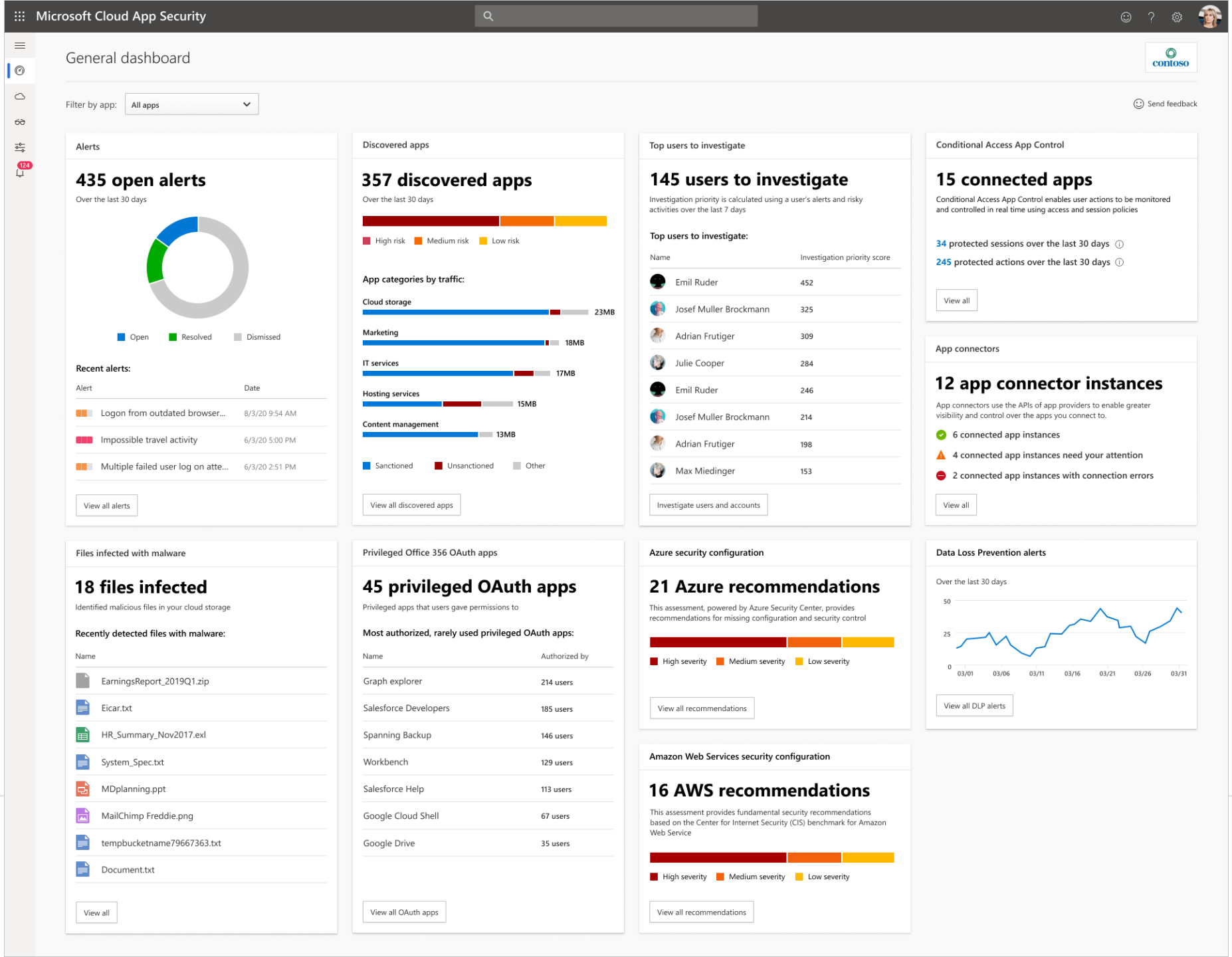
Natively integrated across the broader Microsoft product stack to deliver unique capabilities

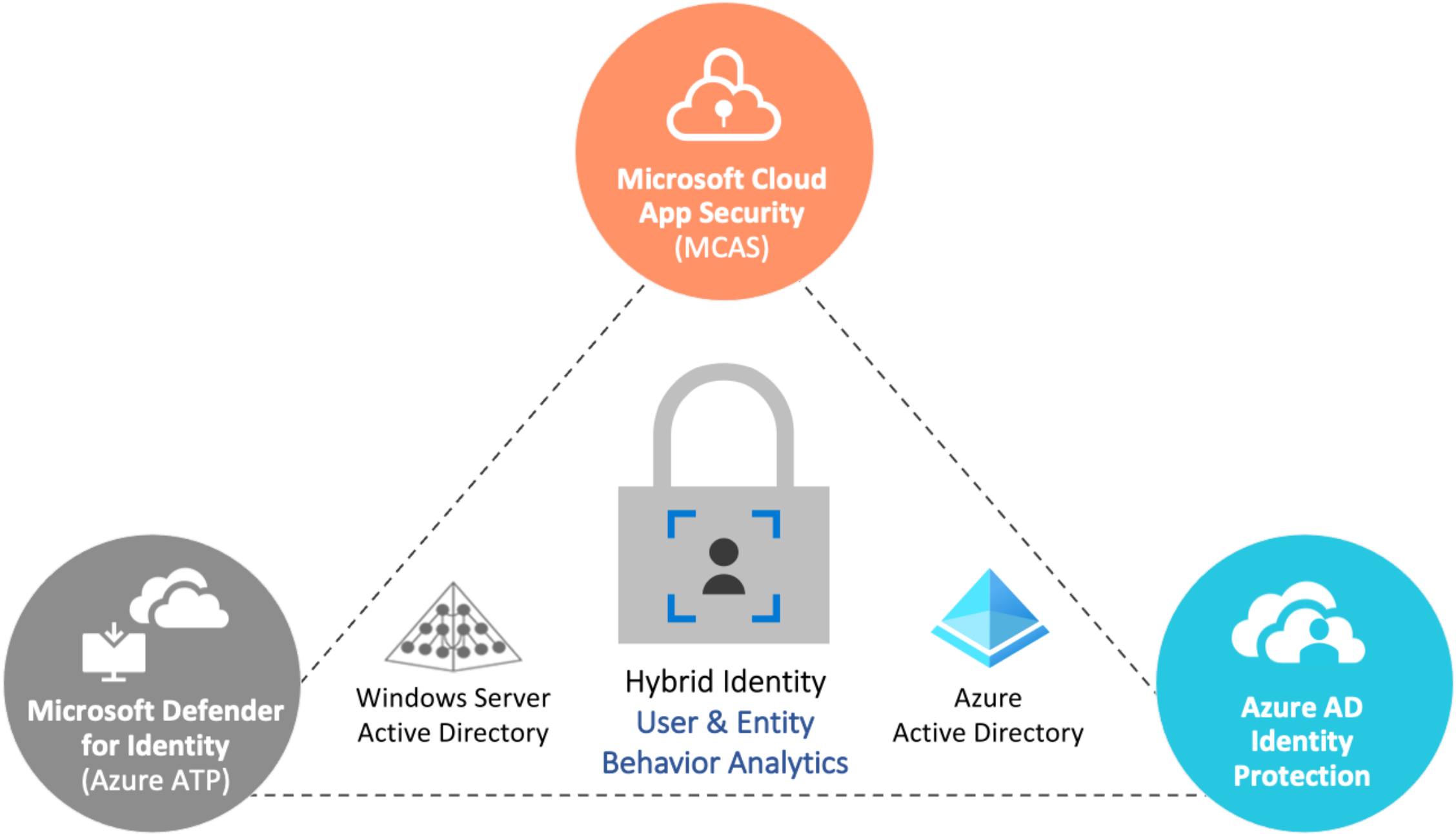
Rooted in supporting any app



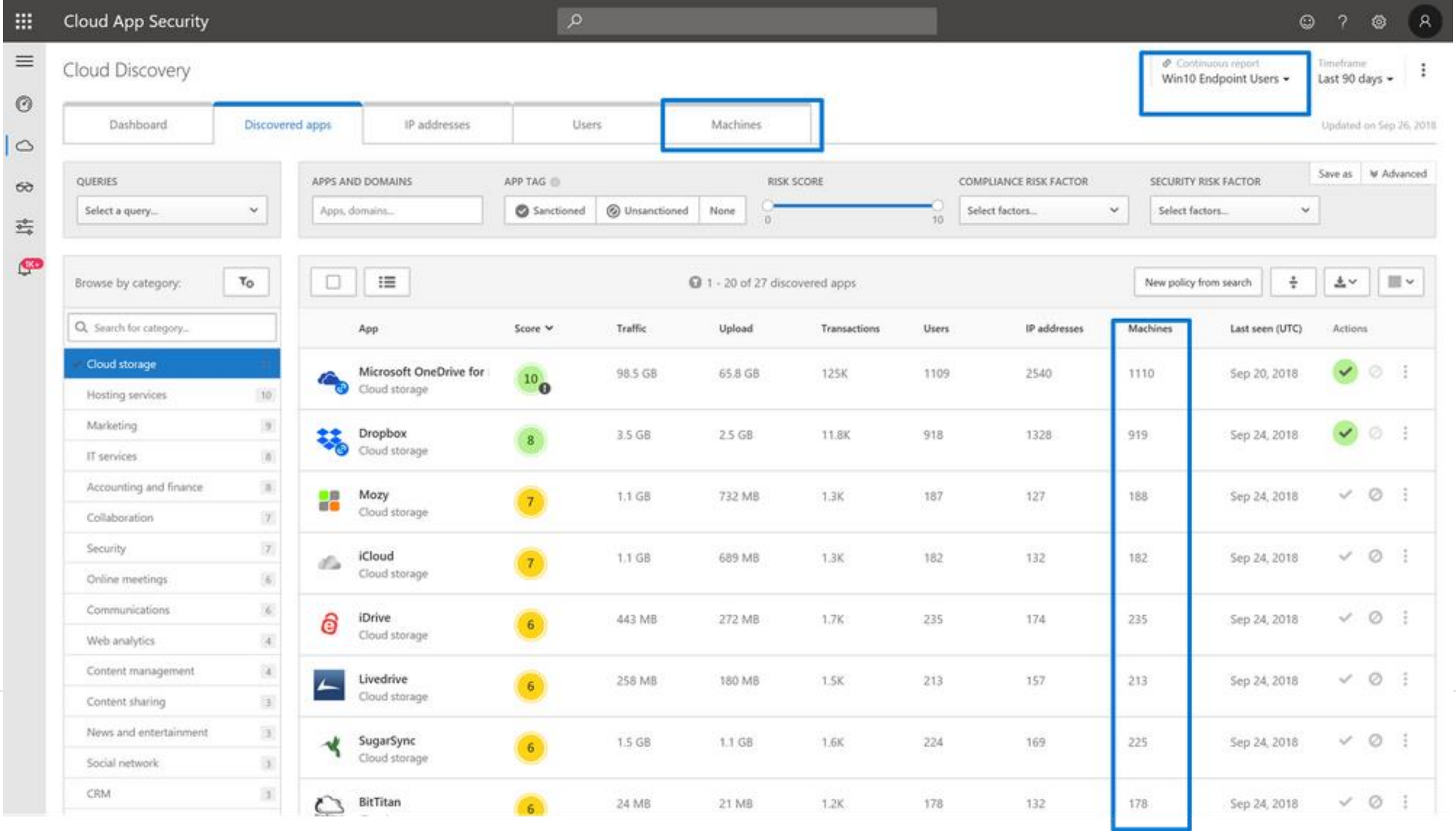
# Top CASB use cases




Microsoft Cloud App Security
General dashboard
contoso
Filter by app:
All apps
Send feedback
Alerts
435 open alerts
Over the last 30 days
Open
Resolved
Dismissed
Recent alerts:
Alert
Date
Logon from outdated browser...
8/3/20 9:54 AM
Impossible travel activity
6/3/20 5:00 PM
Multiple failed user log on atte...
6/3/20 2:51 PM
View all alerts
Discovered apps
357 discovered apps
Over the last 30 days
High risk
Medium risk
Low risk
App categories by traffic:
Cloud storage
23MB
Marketing
18MB
IT services
17MB
Hosting services
15MB
Content management
13MB
Sanctioned
Unsanctioned
Other
View all discovered apps
Top users to investigate
145 users to investigate
Investigation priority is calculated using a user's alerts and risky activities over the last 7 days
Top users to investigate:
Name
Investigation priority score
Emil Ruder
452
Josef Muller Brockmann
325
Adrian Frutiger
309
Julie Cooper
284
Emil Ruder
246
Josef Muller Brockmann
214
Adrian Frutiger
198
Max Miedinger
153
Investigate users and accounts
Conditional Access App Control
15 connected apps
Conditional Access App Control enables user actions to be monitored and controlled in real time using access and session policies
34 protected sessions over the last 30 days
245 protected actions over the last 30 days
View all
App connectors
12 app connector instances
App connectors use the APIs of app providers to enable greater visibility and control over the apps you connect to.
6 connected app instances
4 connected app instances need your attention
2 connected app instances with connection errors
View all
Files infected with malware
18 files infected
Identified malicious files in your cloud storage
Recently detected files with malware:
Name
EarningsReport_2019Q1.zip
Eicar.txt
HR_Summary_Nov2017.exl
System_Spec.txt
MDplanning.ppt
MailChimp Freddie.png
tempbucketname79667363.txt
Document.txt
View all
Privileged Office 356 OAuth apps
45 privileged OAuth apps
Privileged apps that users gave permissions to
Most authorized, rarely used privileged OAuth apps:
Name
Authorized by
Graph explorer
214 users
Salesforce Developers
185 users
Spanning Backup
146 users
Workbench
129 users
Salesforce Help
113 users
Google Cloud Shell
67 users
Google Drive
35 users
View all OAuth apps
Azure security configuration
21 Azure recommendations
This assessment, powered by Azure Security Center, provides recommendations for missing configuration and security control
High severity
Medium severity
Low severity
View all recommendations
Amazon Web Services security configuration
16 AWS recommendations
This assessment provides fundamental security recommendations based on the Center for Internet Security (CIS) benchmark for Amazon Web Service
High severity
Medium severity
Low severity
View all recommendations
Data Loss Prevention alerts
Over the last 30 days
50
25
0
03/01
03/06
03/11
03/16
03/21
03/26
03/31
View all DLP alerts

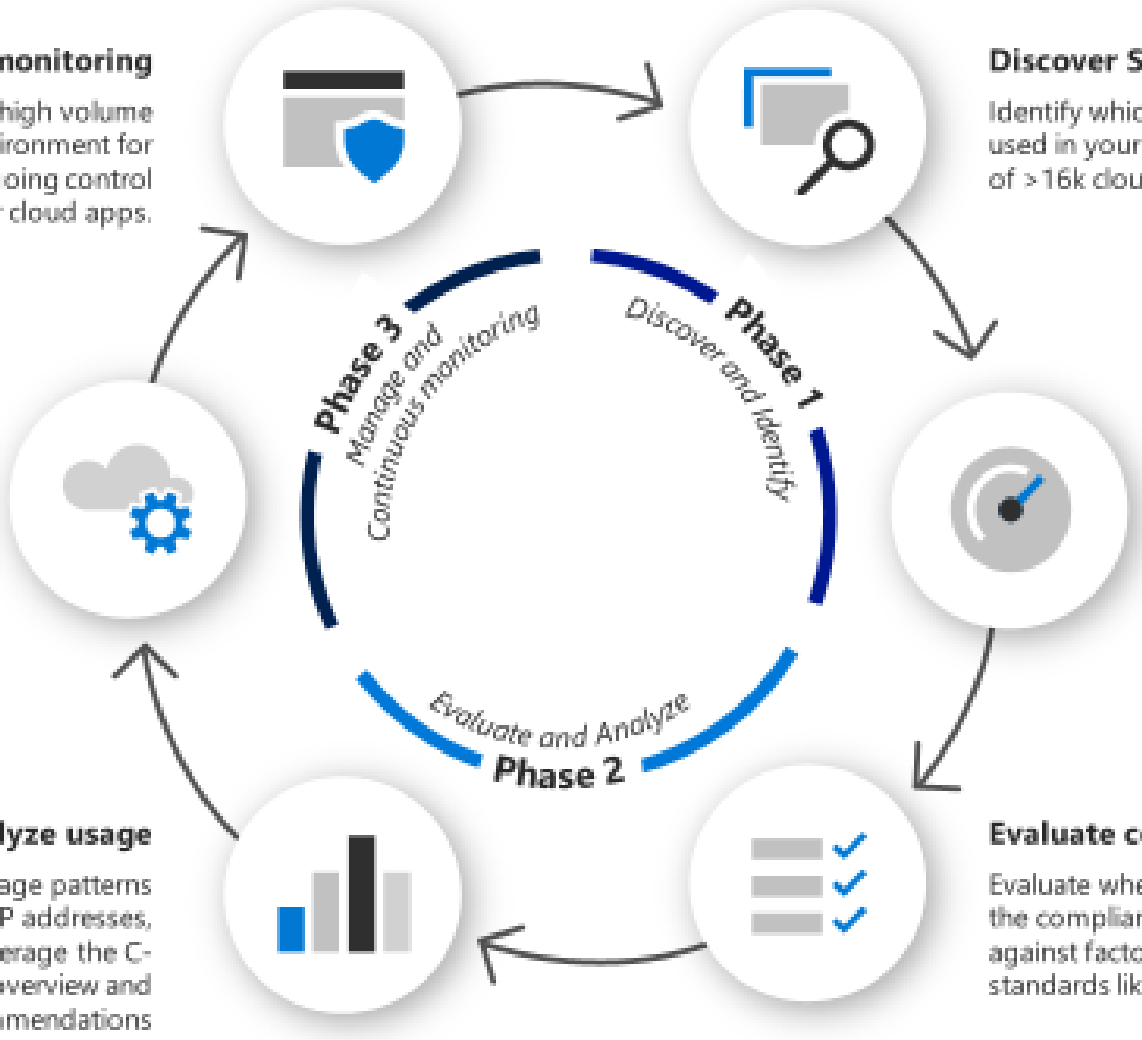

Microsoft Cloud App Security (MCAS)
Microsoft Defender for Identity (Azure ATP)
Windows Server Active Directory
Hybrid Identity User & Entity Behavior Analytics
Azure Active Directory
Azure AD Identity Protection

# Microsoft Defender ATP &
# Microsoft Cloud App Security Integration


Cloud App Security
Cloud Discovery
Continuous report
Win10 Endpoint Users
Timeframe
Last 90 days
Dashboard
Discovered apps
IP addresses
Users
Machines
Updated on Sep 26, 2018
QUERIES
Select a query...
APPS AND DOMAINS
Apps, domains...
APP TAG
Sanctioned
Unsanctioned
None
RISK SCORE
0
10
COMPLIANCE RISK FACTOR
Select factors...
SECURITY RISK FACTOR
Select factors...
Save as
Advanced
Browse by category:
Search for category...
Cloud storage
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
1 - 20 of 27 discovered apps
New policy from search
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

# SHADOW IT MANAGEMENT LIFECYCLE

## Safely adopting cloud apps




**Discover Shadow IT**

Identify which apps are being used in your organization from an app catalog of >16k cloud apps and custom apps.

**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 – with the ability to customize risk scoring

**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**

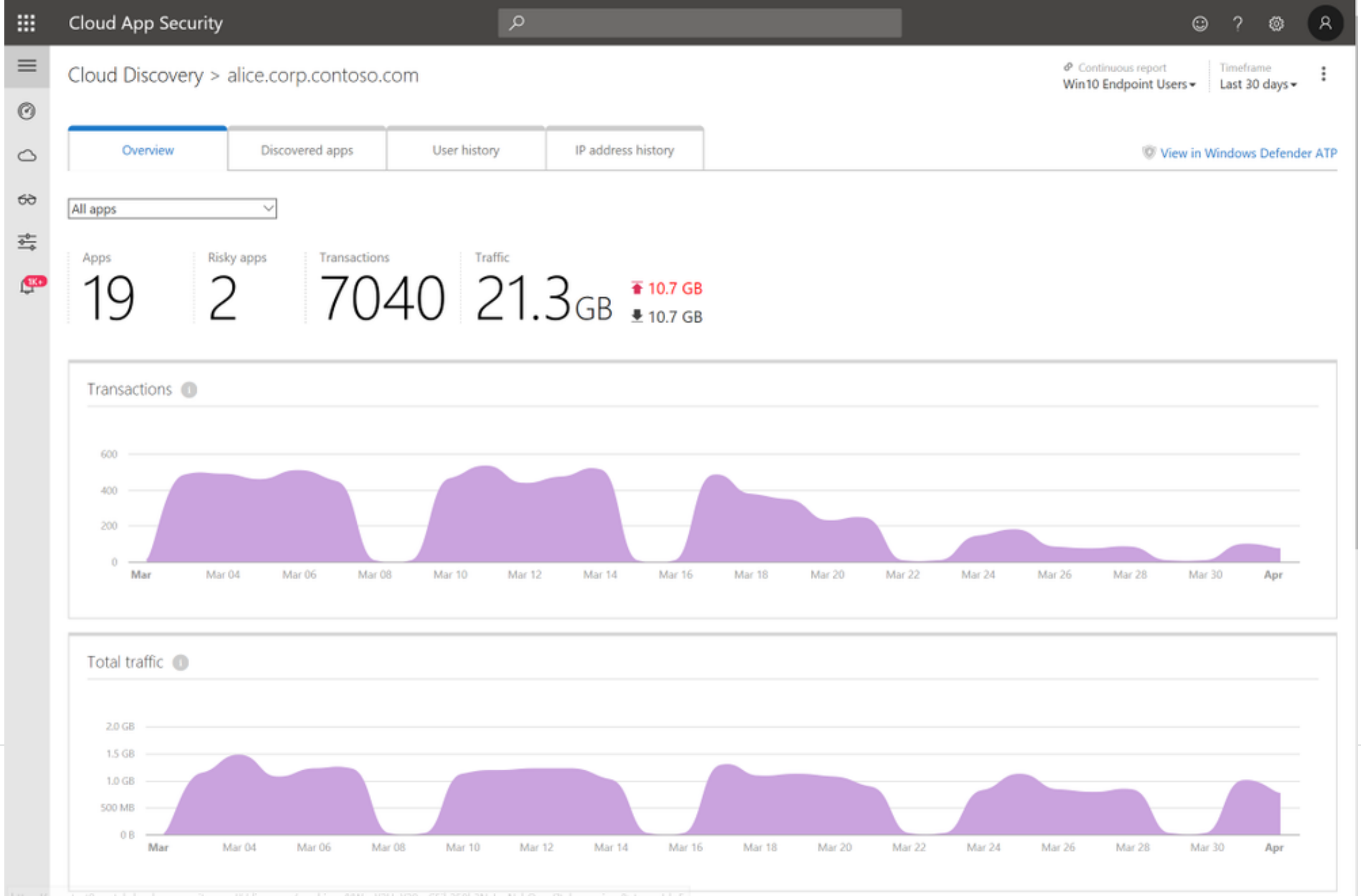
Understand the usage patterns based on traffic data, top users and IP addresses, app categories and machines. Leverage the C-level report for a high level overview and recommendations

**Govern your 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.


Cloud App Security
Cloud Discovery > alice.corp.contoso.com
Continuous report
Win10 Endpoint Users
Timeframe
Last 30 days
Overview
Discovered apps
User history
IP address history
View in Windows Defender ATP
All apps
Apps
19
Risky apps
2
Transactions
7040
Traffic
21.3 GB
10.7 GB
10.7 GB
Transactions
600
400
200
0
Mar
Mar 04
Mar 06
Mar 08
Mar 10
Mar 12
Mar 14
Mar 16
Mar 18
Mar 20
Mar 22
Mar 24
Mar 26
Mar 28
Mar 30
Apr
Total traffic
2.0 GB
1.5 GB
1.0 GB
500 MB
0 B
Mar
Mar 04
Mar 06
Mar 08
Mar 10
Mar 12
Mar 14
Mar 16
Mar 18
Mar 20
Mar 22
Mar 24
Mar 26
Mar 28
Mar 30
Apr

# Microsoft Azure

- What are the differences in discovery capabilities for Azure Active Directory and Microsoft Cloud App Security?
- Azure security baseline for Microsoft Cloud App Security
- Overview of the Azure Security Benchmark

# Azure Defender

Advanced workload protection for selected resource types


# Azure Sentinel

Security information event management, orchestration & automation across your environment, including 3rd party devices

# Azure Security Center

Your base level of security posture management including on-prem via Azure Arc

# Security Center | Overview

Showing 40 subscriptions

Search (Ctrl+/)

Subscriptions | What's new

**General**

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Community

**Cloud Security**

- Secure Score
- Regulatory compliance
- Azure Defender

**Management**

- Pricing & settings
- Security policy
- Security solutions
- Workflow automation
- Coverage
- Cloud connectors (Preview)

**40** Azure subscriptions

**1** AWS accounts

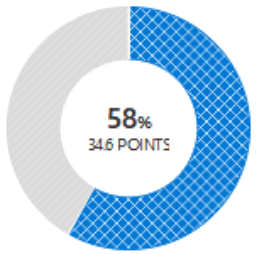
**4** GCP projects

**151** Active recommendations

**100** Security alerts

## Secure score

Current secure score




COMPLETE Controls 1/16

COMPLETE Recomm... 43/194

Improve your secure score >

## Regulatory compliance

Current compliance by passed controls

| | |
|---|---|
| HIPAA H... | 1/22 |
| SOC TSP | 1/13 |
| NIST SP ... | 3/29 |
| PCI DSS ... | 5/45 |
| Azure CI... | 3/24 |

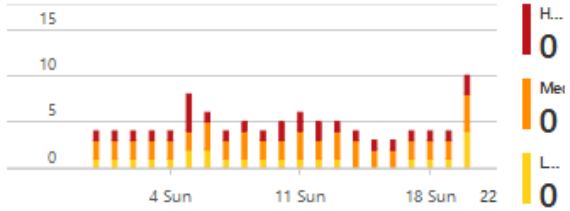
Improve your compliance >

## Azure Defender

Resource coverage

**88%** For full protection, enable 8 resource plans

Alerts by severity




Enhance your threat protection capabilities >

## Inventory

Unmonitored VMs

**54** To better protect your organization, we recommend installing agents

Total Resources

**2967**

| Unhealthy (1648) | Healthy (1064) | Not applicable (255) |
|---|---|---|

Explore your resources >

## Insights

Most prevalent recommendations (by resources)

| | |
|---|---|
| Audit diagnostic setting | 684 |
| Storage account public access sh... | 290 |
| A vulnerability assessment soluti... | 123 |
| Disk encryption should be applie... | 115 |

Controls with the highest potential increase

| | |
|---|---|
| Remediate vulnerabilities | +11% (6pt) |
| Enable encryption at rest | +6% (4pt) |
| Remediate security configura... | +5% (4pt) |

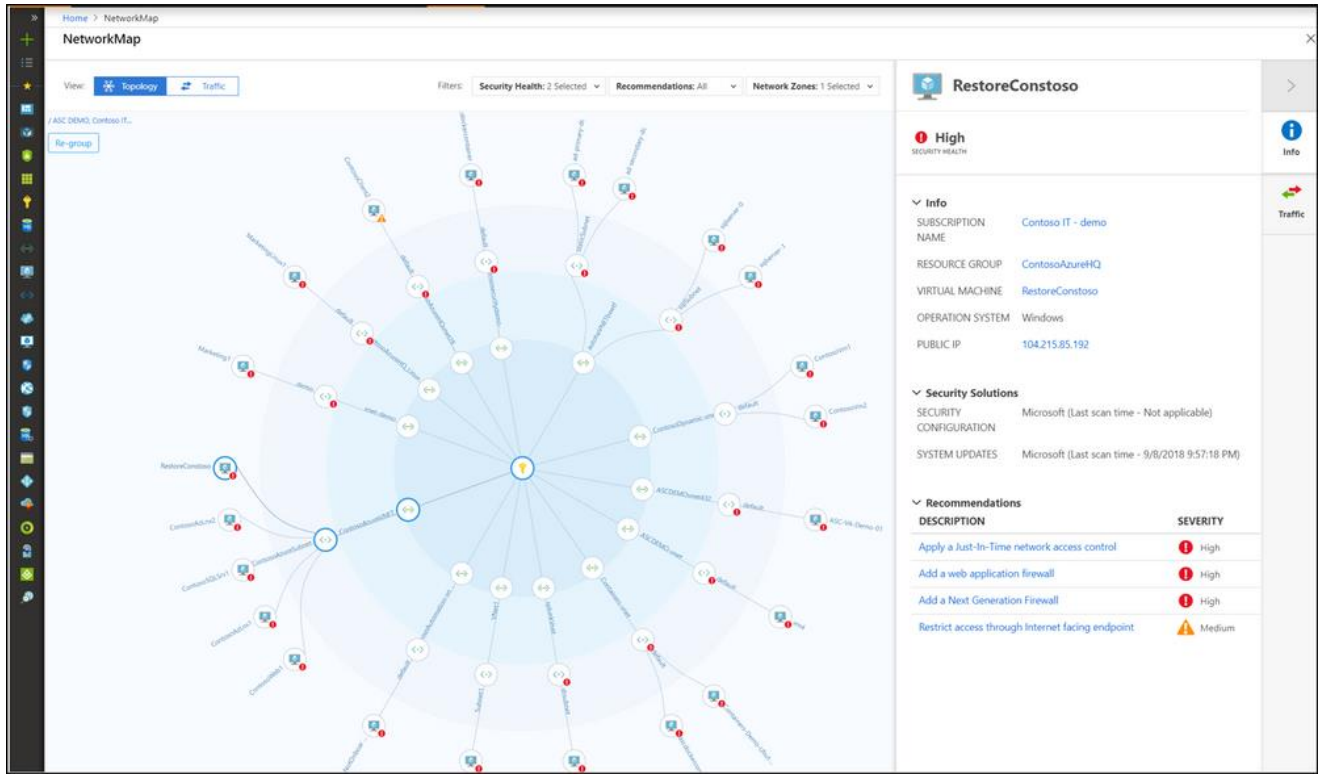
View controls >

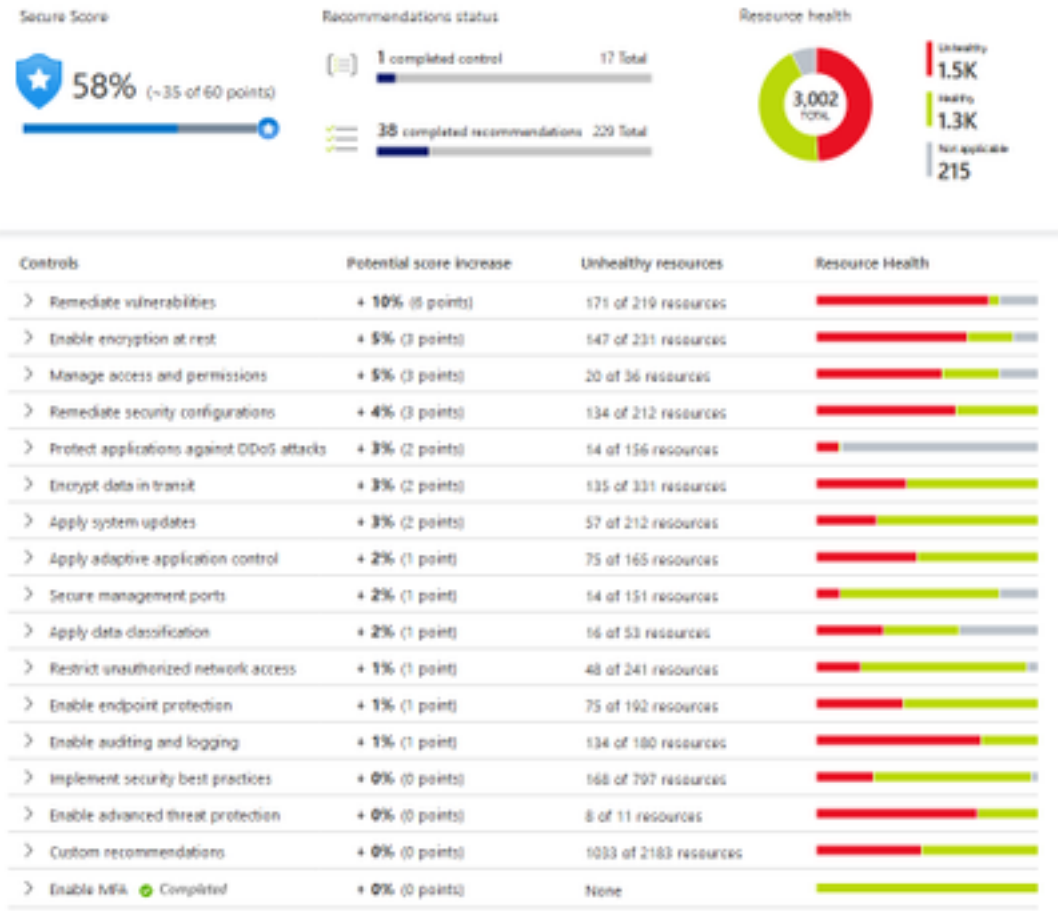
Azure Security Center community

Join the Azure Security Center community on GitHub to interact with other customers and experts and learn, provide feedback, and share knowledge about Security Center.

View Azure Community >

# Azure Security Center - Security Posture Management



# Useful Links

- Onboard Windows Defender Endpoints
  - https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-configure?view=o365-worldwide
- Onboard Microsoft Defender for Identity
  - https://docs.microsoft.com/en-us/cloud-app-security/mdi-integration
- Connect Office 365
  - https://docs.microsoft.com/en-us/cloud-app-security/connect-office-365-to-microsoft-cloud-app-security
- Connect Microsoft Azure
  - https://docs.microsoft.com/en-us/cloud-app-security/connect-azure-to-microsoft-cloud-app-security