TOPIC

Secure how your users interact with cloud apps

Mario Cuomo & Edoardo Garofano

Security Cloud Solution Architects @ Microsoft

Thanks for collaboration

Microsoft

Packt›

JET BRAINS

KIRATECH®
PLATFORM HEROES

elettrone
intelligenza energetica

addvalue
A DIFFERENT COMPANY

NET COM
Networking Communication

DOCUTECH
Technical Documentation Software

GPA
Gestione Processi Aziendali

AZUREBOX

Who I am

MARIO CUOMO

https://github.com/mariocuomo

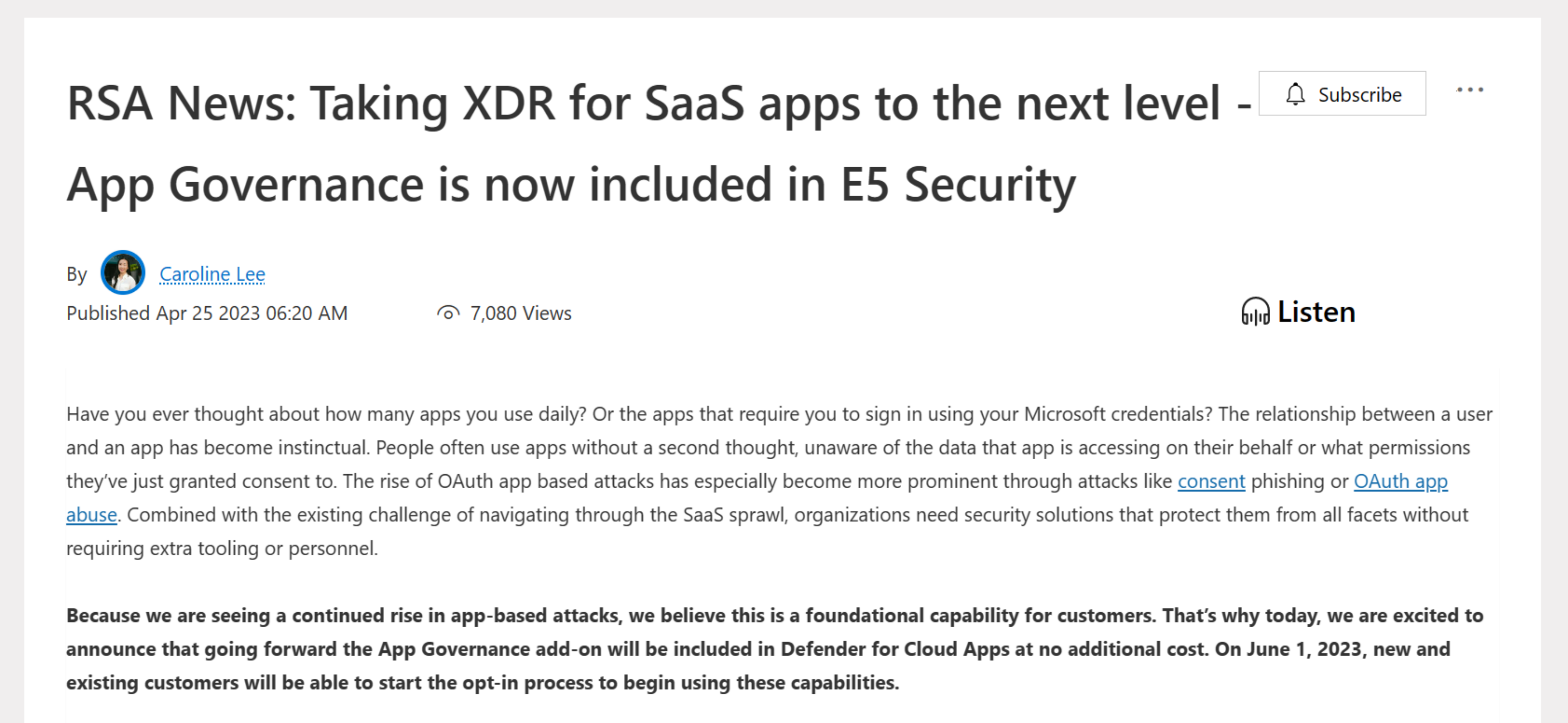
https://www.linkedin.com/in/mariocuomo

Who I am

EDOARDO GAROFANO

https://www.linkedin.com/in/edoardo-g-44b314b2

RSA News



RSA News: Taking XDR for SaaS apps to the next level - App Governance is now included in E5 Security

By Caroline Lee

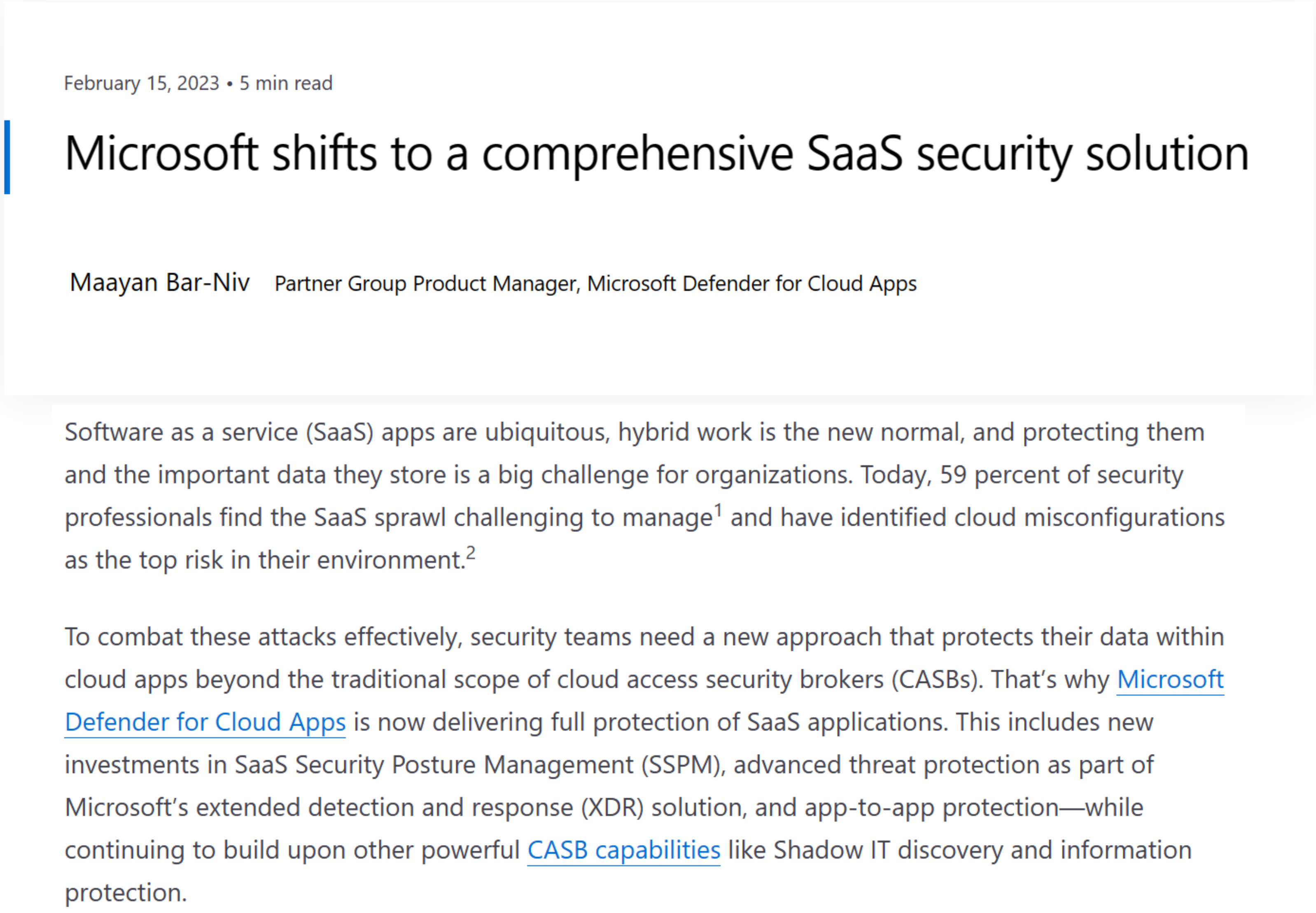
Published Apr 25 2023 06:20 AM

7,080 Views

Have you ever thought about how many apps you use daily? Or the apps that require you to sign in using your Microsoft credentials? The relationship between a user and an app has become instinctual. People often use apps without a second thought, unaware of the data that app is accessing on their behalf or what permissions they've just granted consent to. The rise of OAuth app based attacks has especially become more prominent through attacks like consent phishing or OAuth app abuse. Combined with the existing challenge of navigating through the SaaS sprawl, organizations need security solutions that protect them from all facets without requiring extra tooling or personnel.

Because we are seeing a continued rise in app-based attacks, we believe this is a foundational capability for customers. That's why today, we are excited to announce that going forward the App Governance add-on will be included in Defender for Cloud Apps at no additional cost. On June 1, 2023, new and existing customers will be able to start the opt-in process to begin using these capabilities.

Microsoft shifts to a comprehensive SaaS security solution



February 15, 2023 • 5 min read

Microsoft shifts to a comprehensive SaaS security solution

Maayan Bar-Niv Partner Group Product Manager, Microsoft Defender for Cloud Apps

Software as a service (SaaS) apps are ubiquitous, hybrid work is the new normal, and protecting them and the important data they store is a big challenge for organizations. Today, 59 percent of security professionals find the SaaS sprawl challenging to manage[1] and have identified cloud misconfigurations as the top risk in their environment.[2]

To combat these attacks effectively, security teams need a new approach that protects their data within cloud apps beyond the traditional scope of cloud access security brokers (CASBs). That's why Microsoft Defender for Cloud Apps is now delivering full protection of SaaS applications. This includes new investments in SaaS Security Posture Management (SSPM), advanced threat protection as part of Microsoft's extended detection and response (XDR) solution, and app-to-app protection—while continuing to build upon other powerful CASB capabilities like Shadow IT discovery and information protection.

Azure

So not only cloud apps…also **DevOps cloud security solutions for any asset!**

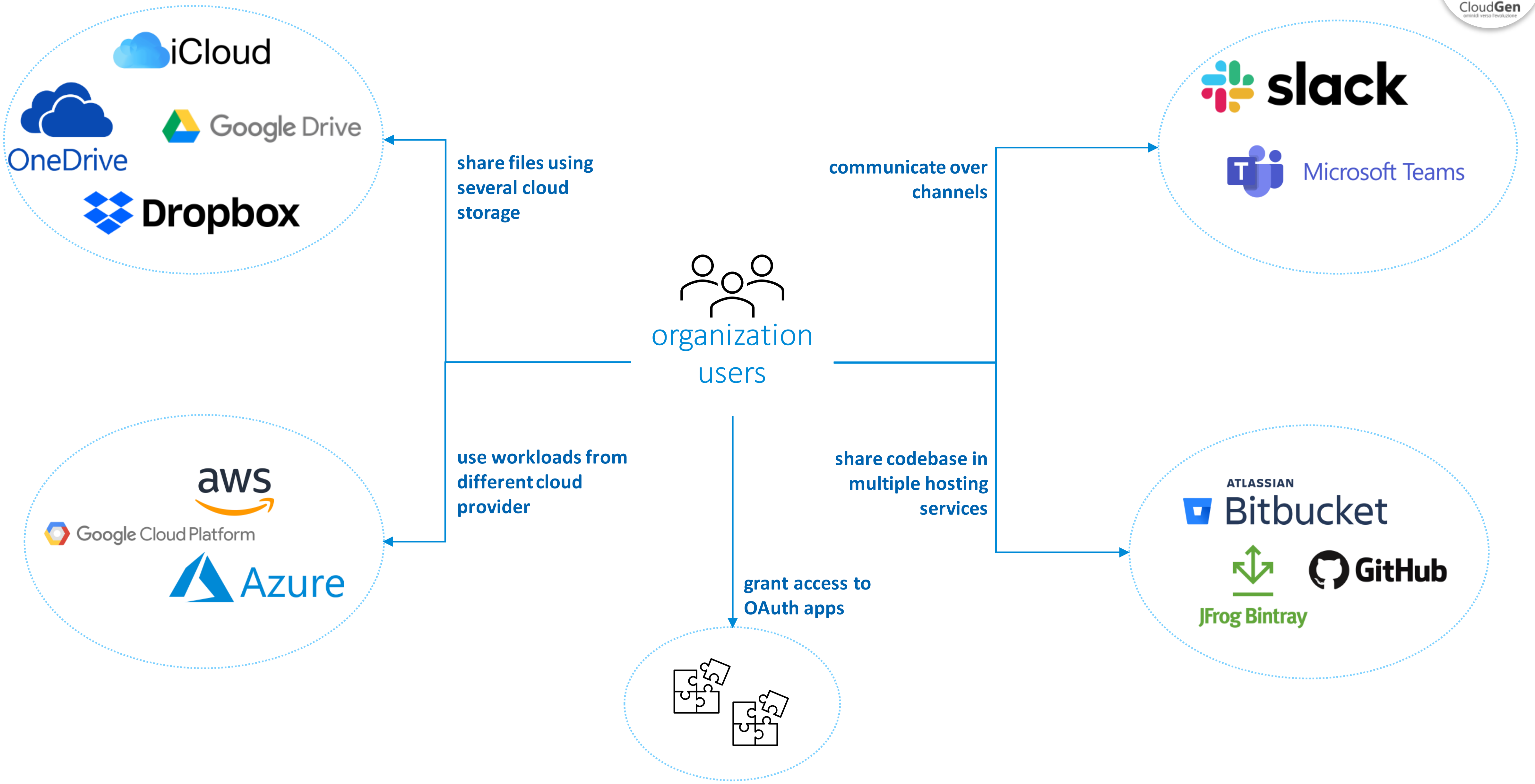
☺

GitHub

Agenda

- What is a Cloud Access Security Broker (CASB) and why I need it
- Defender for Cloud Apps as CASB
  - Shadow IT Discovery
  - Information Protection
  - Threat Protection
- Not just a simple CASB for apps, more a Software as a Service (SaaS) security solution
  - Multi-Cloud Protection
  - OAuth applications
  - Security Posture Management
  - App Governance

A realistic multi-cloud situation



organization users

share files using several cloud storage

use workloads from different cloud provider

communicate over channels

share codebase in multiple hosting services

grant access to OAuth apps

Cloud services require a new approach to security

1,558

different cloud services are used by enterprises on average[1]

95%

of organizations are moderately to extremely concerned about cloud security[3]

68%

of breaches take months or longer to discover without security controls in place[2]

79%

of users regularly upload, create, share, or store data in cloud apps[1]

[1] Netskope Cloud and Threat Report, 2022

[2] Cost of a data breach 2022 | IBM

[3] 2022 Cloud Security Report | Fortinet Blog

Cloud Access Security Brokers

Gartner’s definition for CASBs:

“Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on.”[1]

CASB spend investment is predicted to grow over

30% during 2024

37.2% in 2021, 33.2% in 2022, 32.0% in 2023[2]

1. Definition of Cloud Access Security Brokers (CASBs) - IT Glossary | Gartner
2. Forecast: Information Security and Risk Management, Worldwide, 2018-2024

Microsoft CASB?
Microsoft Defender for Cloud Apps

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

Cloud platforms

aws
Amazon Web Services

Microsoft Azure

Google Cloud

Native integrations

Microsoft Defender

Azure Sentinel

Microsoft Information Protection

Azure Active Directory

17,000+ supported apps

Microsoft Azure

Power BI

Office 365

Microsoft Teams

Microsoft Dynamics 365

in LEARNING

Confluence

cornerstone

DocuSign

Adobe

box

HighQ

Dropbox

G Suite

zendesk

workday.

aws

Workiva

+ a b l e a u

JIRA Software

Workplace
by facebook

CONCUR.

Cisco webex

okta

zoom

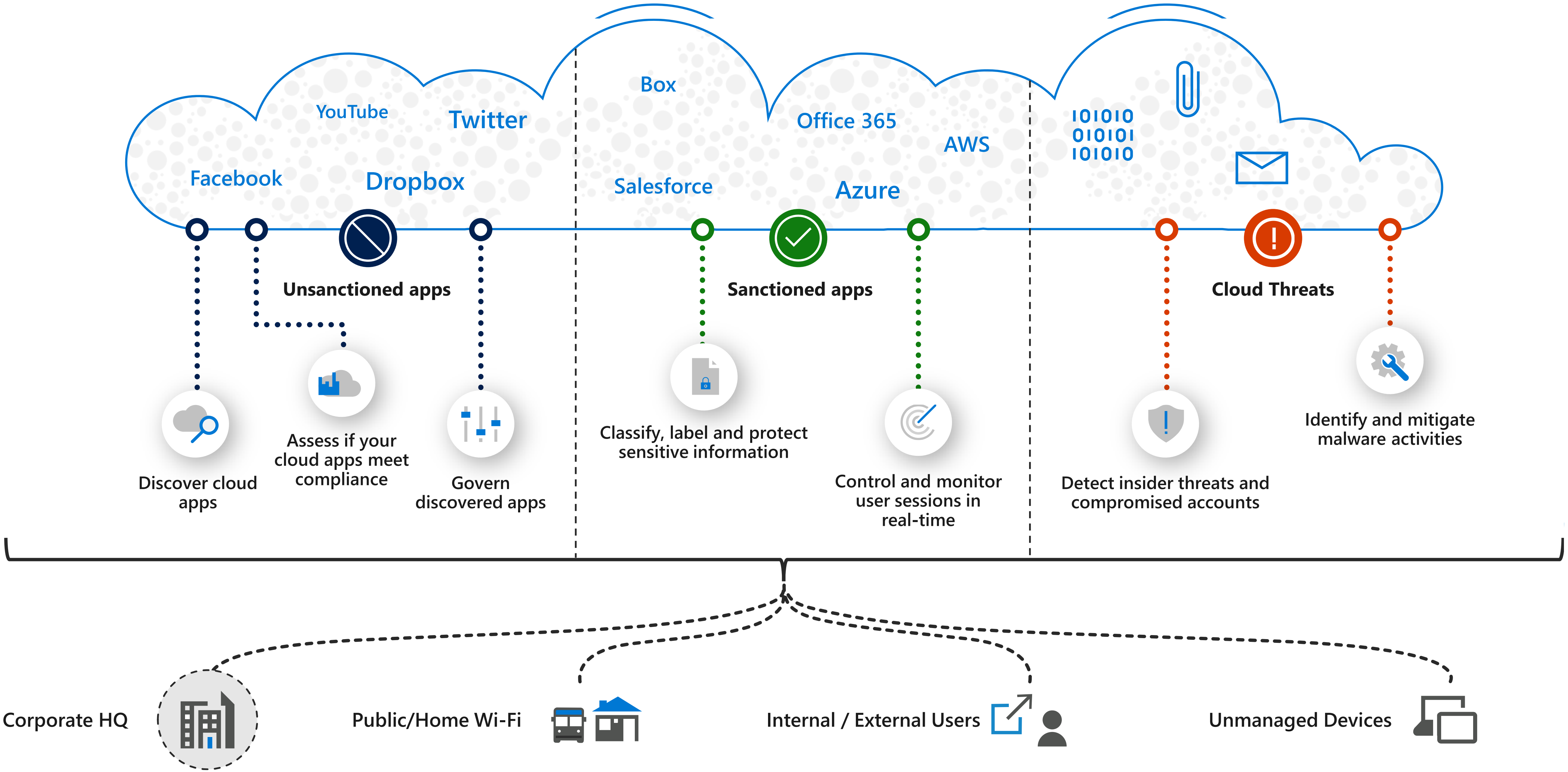
salesforce

slack

GitHub

servicenow.

Top Defender for Cloud Apps use cases



Unsanctioned apps

Discover cloud apps

Assess if your cloud apps meet compliance

Govern discovered apps

Sanctioned apps

Classify, label and protect sensitive information

Control and monitor user sessions in real-time

Cloud Threats

Detect insider threats and compromised accounts

Identify and mitigate malware activities

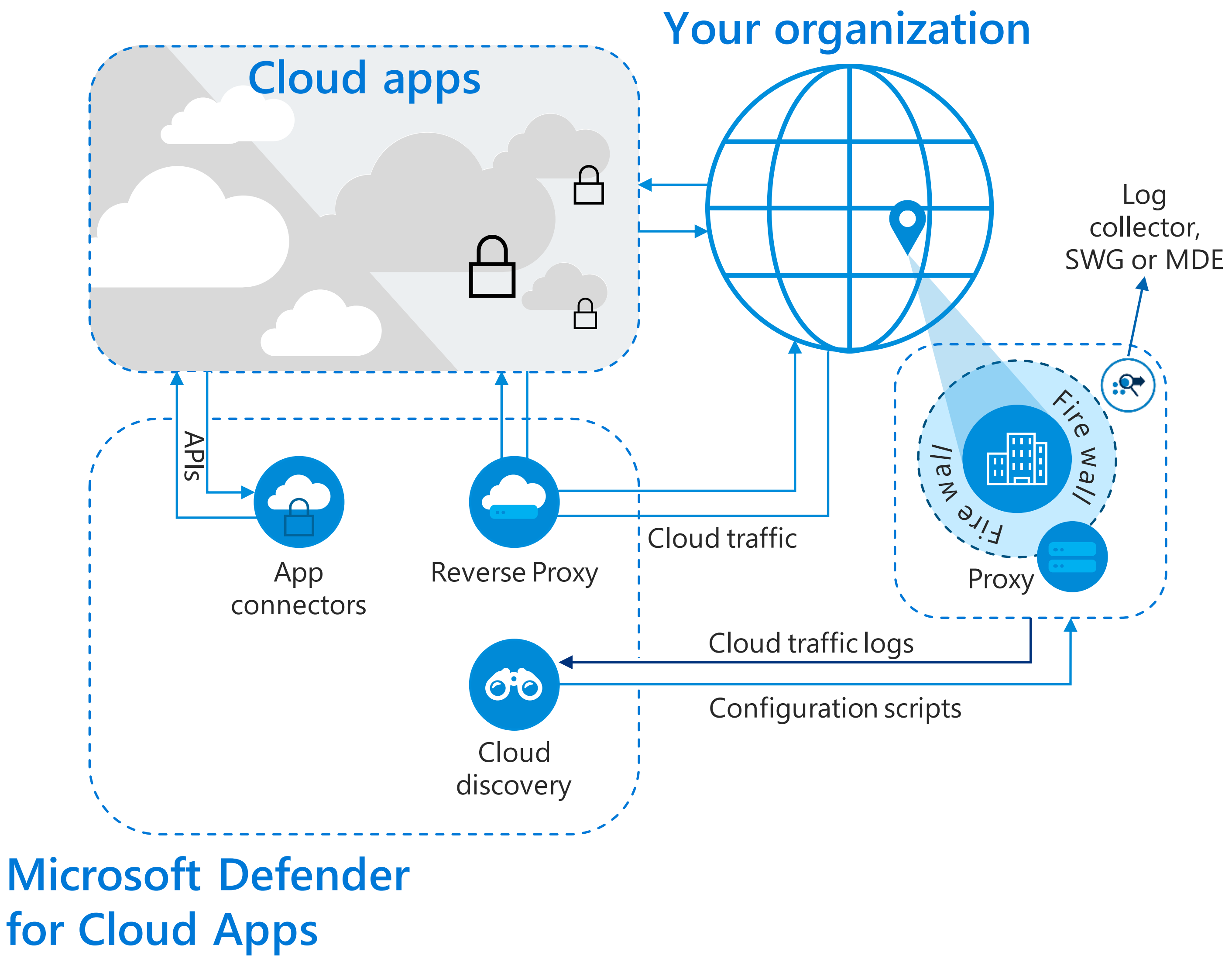
Corporate HQ

Public/Home Wi-Fi

Internal / External Users

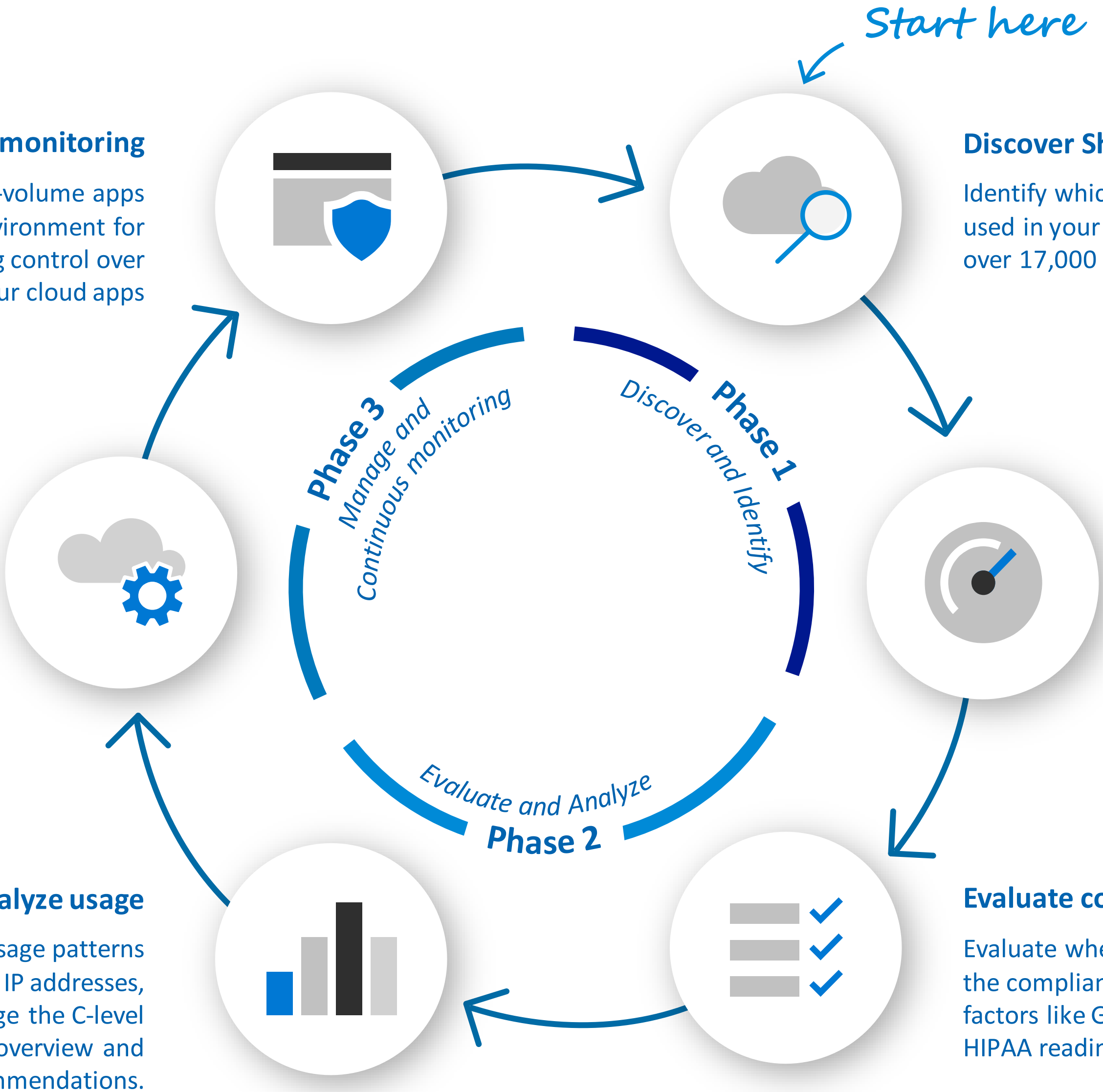
Unmanaged Devices

How Microsoft Defender for Cloud Apps works



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 over 17,000 cloud apps and custom apps

Identify the risk levels of your apps

Understand the risk associated with discovered apps, based on more than 90 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 devices. Leverage the C-level report for a high-level overview and recommendations.

Govern your cloud apps

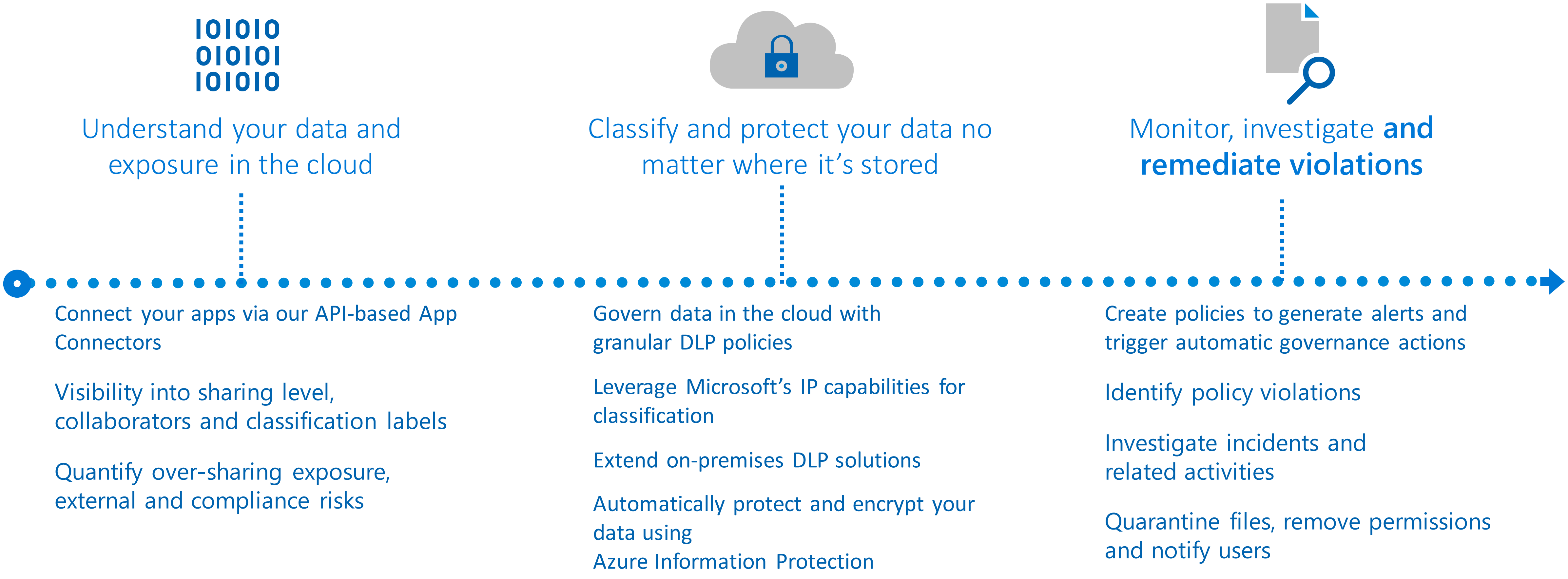
Start managing cloud apps and leverage one of several governance actions such as Sanction, Unsanction, onboarding an app to AAD to leverage SSO, marking them for review or blocking them from your network

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

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-premises DLP solutions

Automatically protect and encrypt your data using Azure Information Protection

Monitor, investigate **and remediate violations**

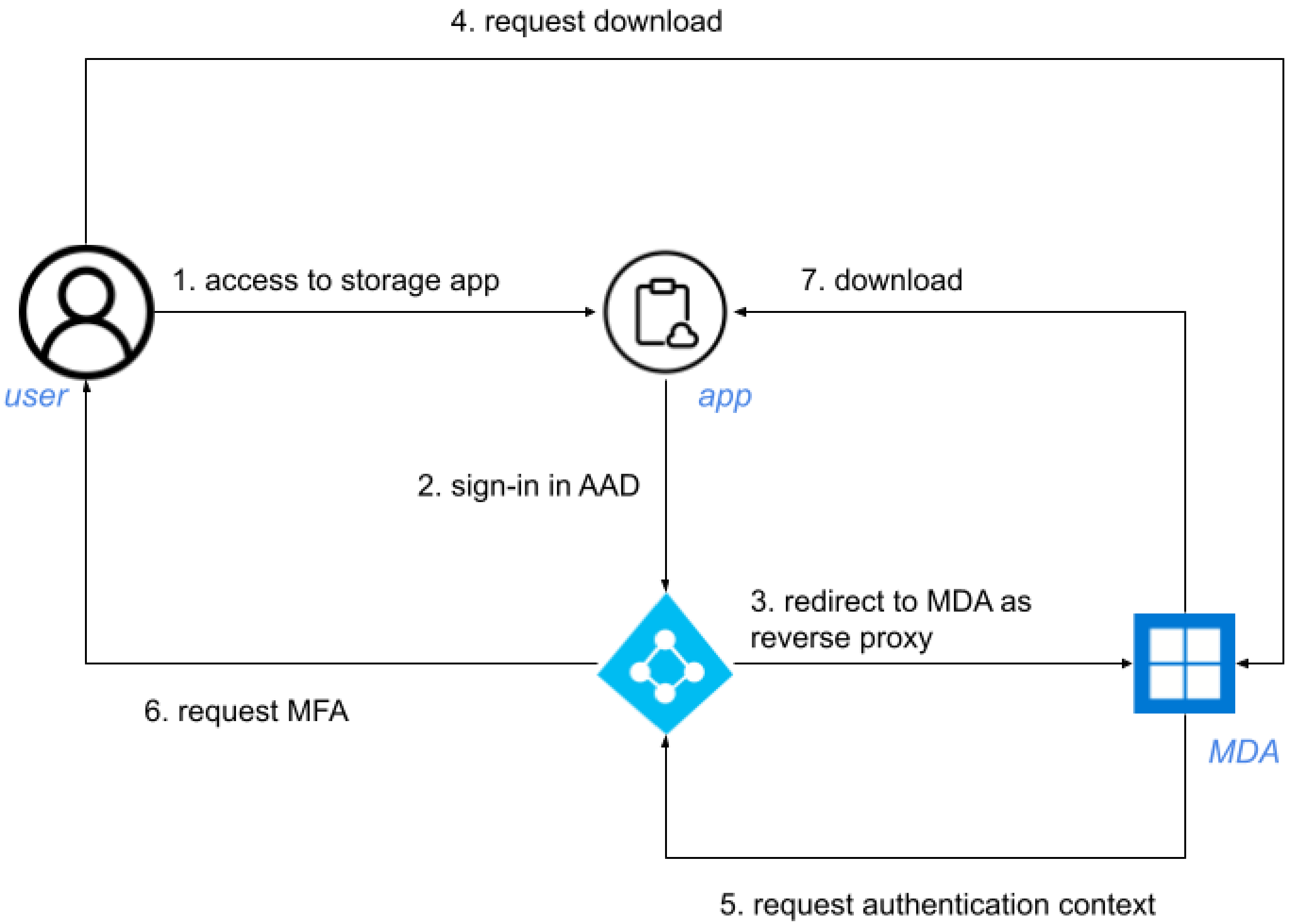
Create policies to generate alerts and trigger automatic governance actions

Identify policy violations

Investigate incidents and related activities

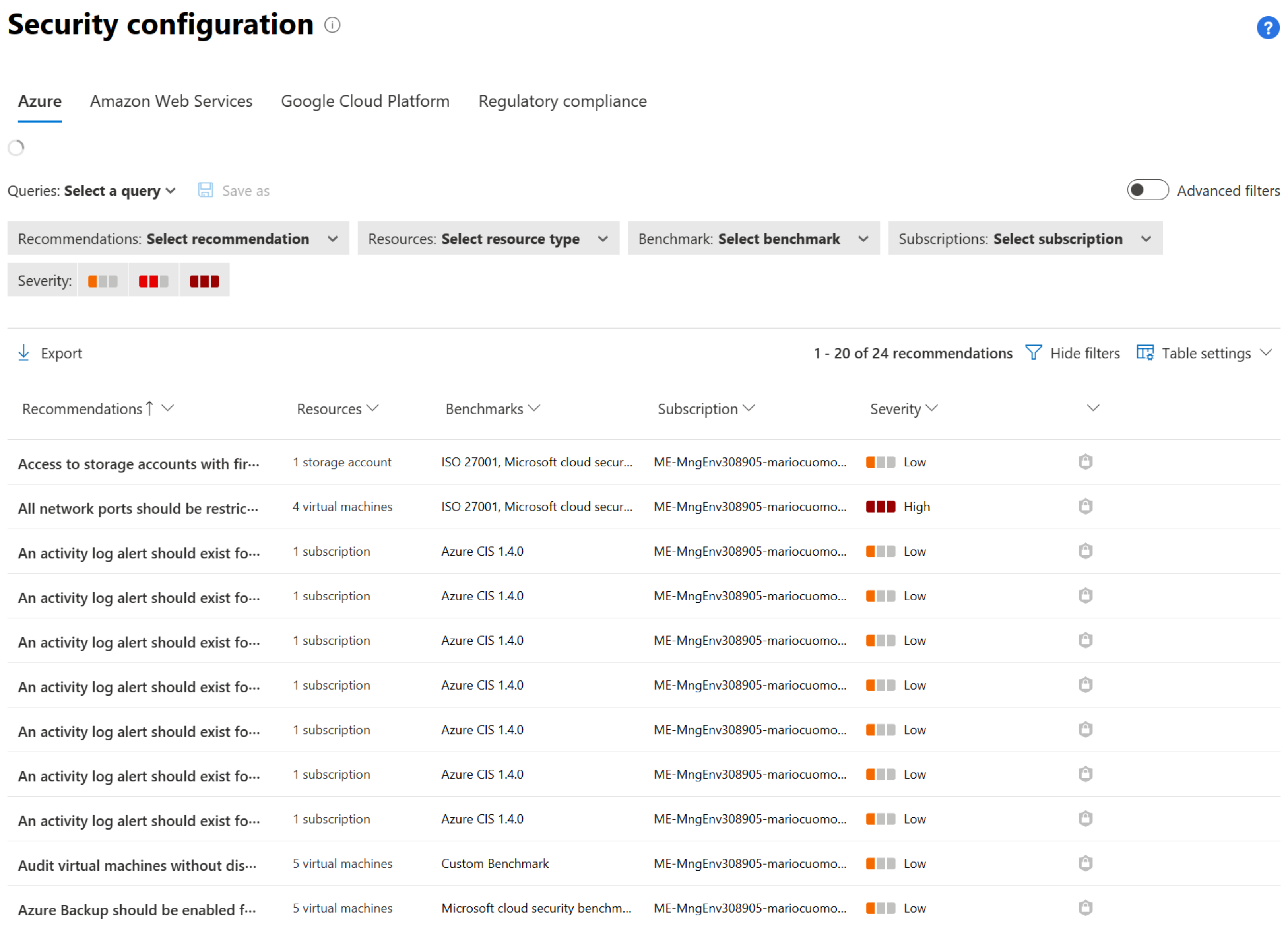
Quarantine files, remove permissions and notify users

Real Time Protection – scenario example



DEMO

Security Posture Management



Security configuration

Azure | Amazon Web Services | Google Cloud Platform | Regulatory compliance

Queries: **Select a query** | Save as | Advanced filters

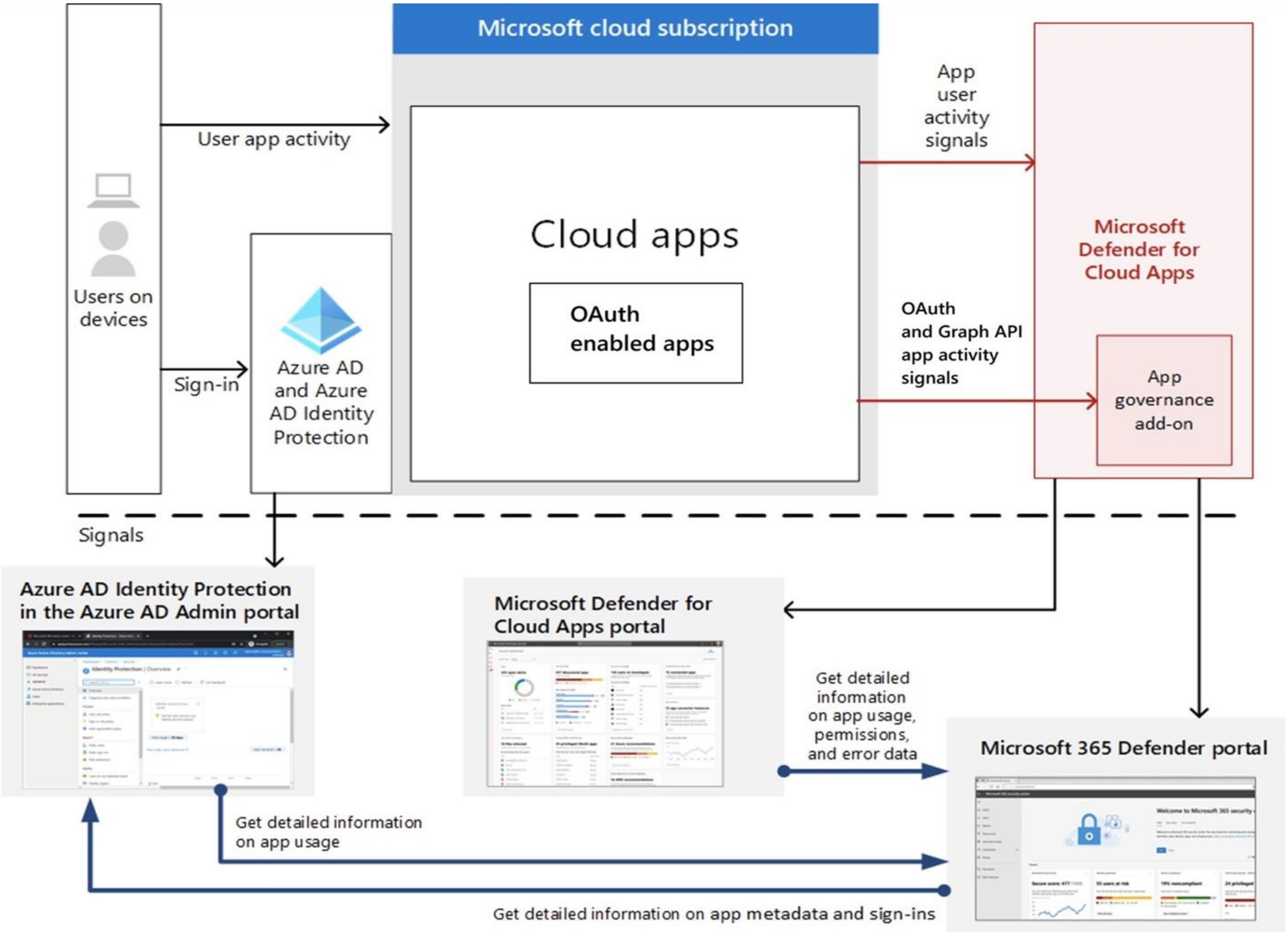
Recommendations: **Select recommendation** | Resources: **Select resource type** | Benchmark: **Select benchmark** | Subscriptions: **Select subscription**

Severity:

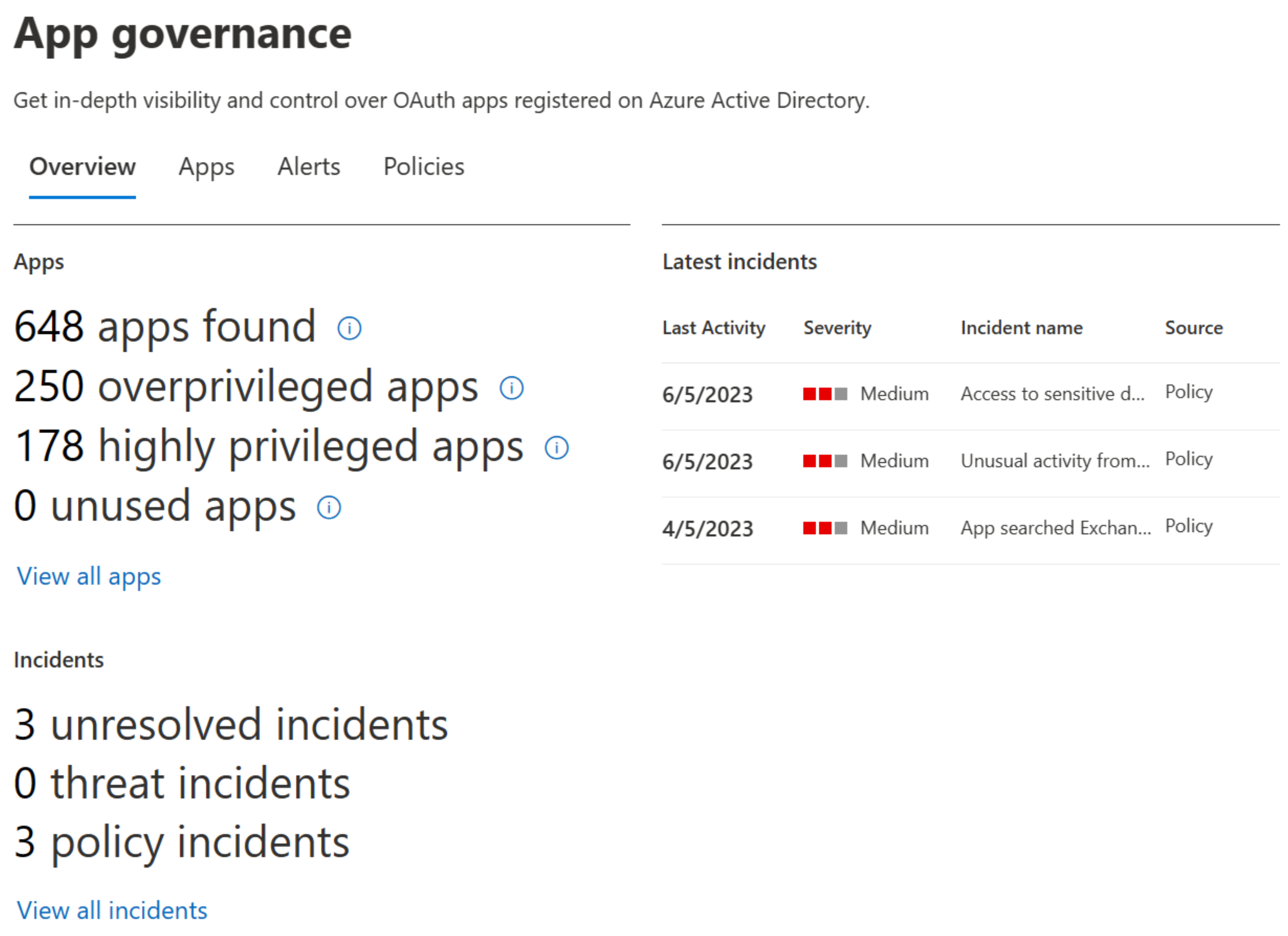
Export | 1 - 20 of 24 recommendations | Hide filters | Table settings

Recommendations ↑	Resources	Benchmarks	Subscription	Severity
Access to storage accounts with fir···	1 storage account	ISO 27001, Microsoft cloud secur...	ME-MngEnv308905-mariocuomo...	Low
All network ports should be restric···	4 virtual machines	ISO 27001, Microsoft cloud secur...	ME-MngEnv308905-mariocuomo...	High
An activity log alert should exist fo···	1 subscription	Azure CIS 1.4.0	ME-MngEnv308905-mariocuomo...	Low
An activity log alert should exist fo···	1 subscription	Azure CIS 1.4.0	ME-MngEnv308905-mariocuomo...	Low
An activity log alert should exist fo···	1 subscription	Azure CIS 1.4.0	ME-MngEnv308905-mariocuomo...	Low
An activity log alert should exist fo···	1 subscription	Azure CIS 1.4.0	ME-MngEnv308905-mariocuomo...	Low
An activity log alert should exist fo···	1 subscription	Azure CIS 1.4.0	ME-MngEnv308905-mariocuomo...	Low
An activity log alert should exist fo···	1 subscription	Azure CIS 1.4.0	ME-MngEnv308905-mariocuomo...	Low
An activity log alert should exist fo···	1 subscription	Azure CIS 1.4.0	ME-MngEnv308905-mariocuomo...	Low
Audit virtual machines without dis···	5 virtual machines	Custom Benchmark	ME-MngEnv308905-mariocuomo...	Low
Azure Backup should be enabled f···	5 virtual machines	Microsoft cloud security benchm...	ME-MngEnv308905-mariocuomo...	Low

OAuth applications


Microsoft cloud subscription
User app activity
Users on devices
Sign-in
Azure AD and Azure AD Identity Protection
Cloud apps
OAuth enabled apps
App user activity signals
OAuth and Graph API app activity signals
Microsoft Defender for Cloud Apps
App governance add-on
Signals
Azure AD Identity Protection in the Azure AD Admin portal
Microsoft Defender for Cloud Apps portal
Get detailed information on app usage, permissions, and error data
Microsoft 365 Defender portal
Get detailed information on app usage
Get detailed information on app metadata and sign-ins

App Governance



App governance

Get in-depth visibility and control over OAuth apps registered on Azure Active Directory.

Apps

648 apps found ⓘ
250 overprivileged apps ⓘ
178 highly privileged apps ⓘ
0 unused apps ⓘ

View all apps

Incidents

3 unresolved incidents
0 threat incidents
3 policy incidents

View all incidents

Latest incidents

Last Activity	Severity	Incident name	Source
6/5/2023	🟥🟥⬜ Medium	Access to sensitive d...	Policy
6/5/2023	🟥🟥⬜ Medium	Unusual activity from...	Policy
4/5/2023	🟥🟥⬜ Medium	App searched Exchan...	Policy

Thanks

Question?