Microsoft Security
Emiliano Iacomino
Security, Compliance and Identity
Digital Technical Specialist
Emiliano.Iacomino@microsoft.com

Yooda
Pacho Baratta
Marketing Manager e Solutions Architect
p.baratta@yooda.tech

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

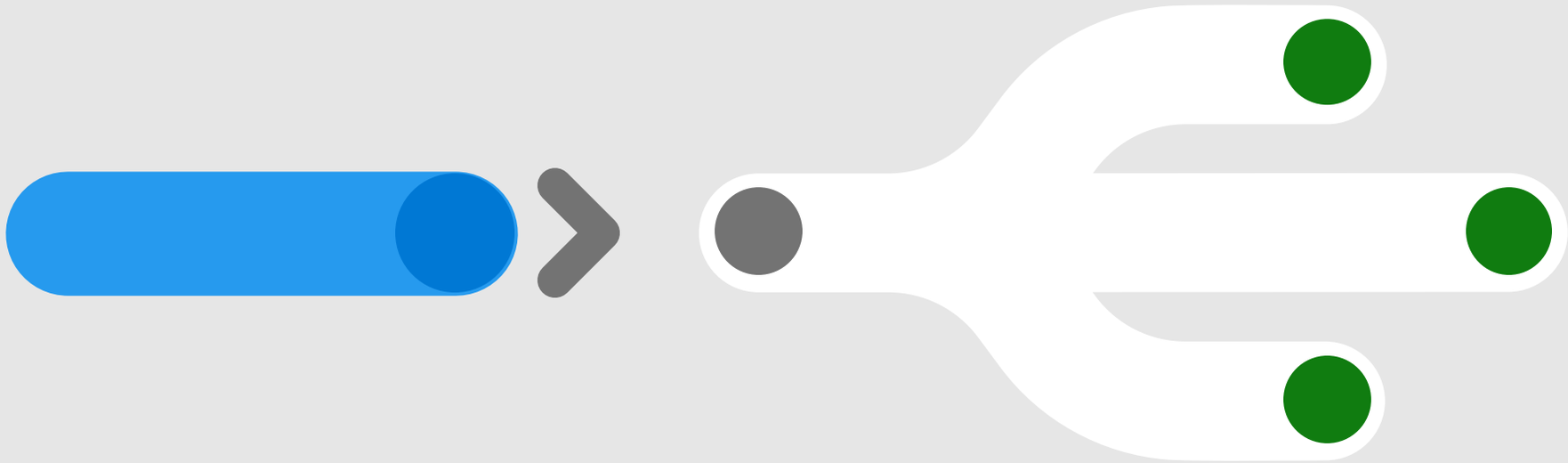
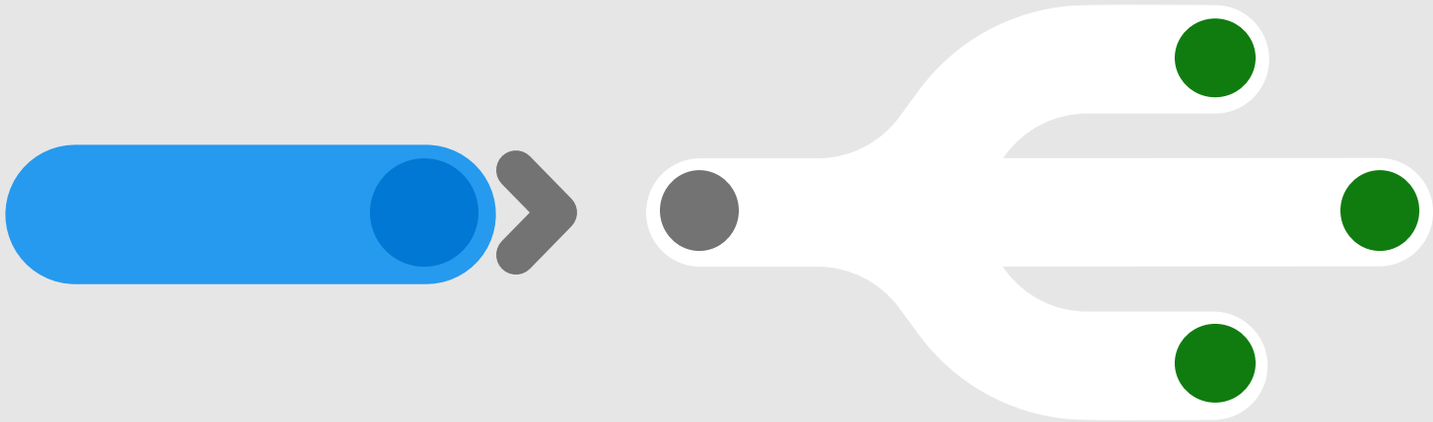
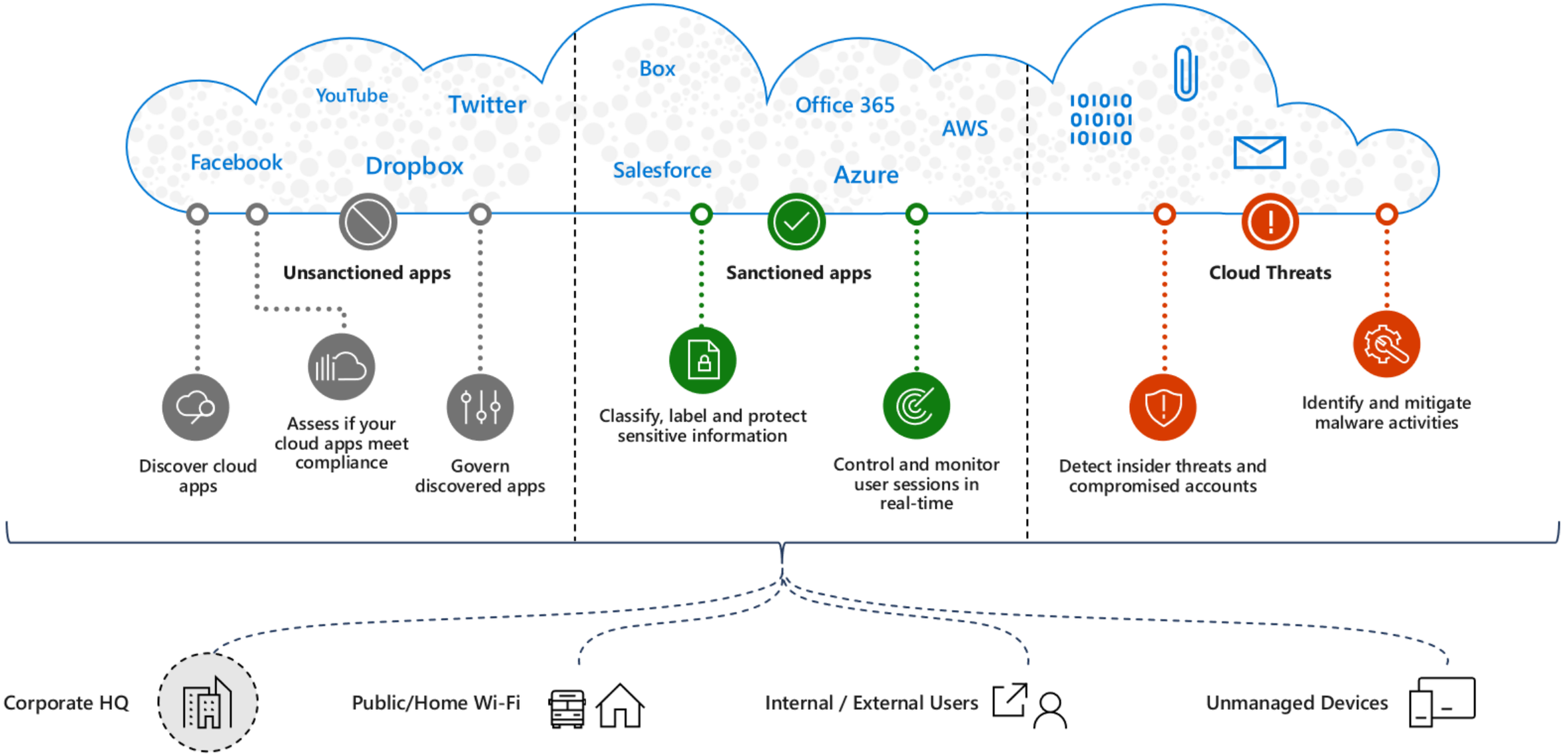


Table of contents

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

- Amazon Web Services
- Microsoft Azure
- Google Cloud

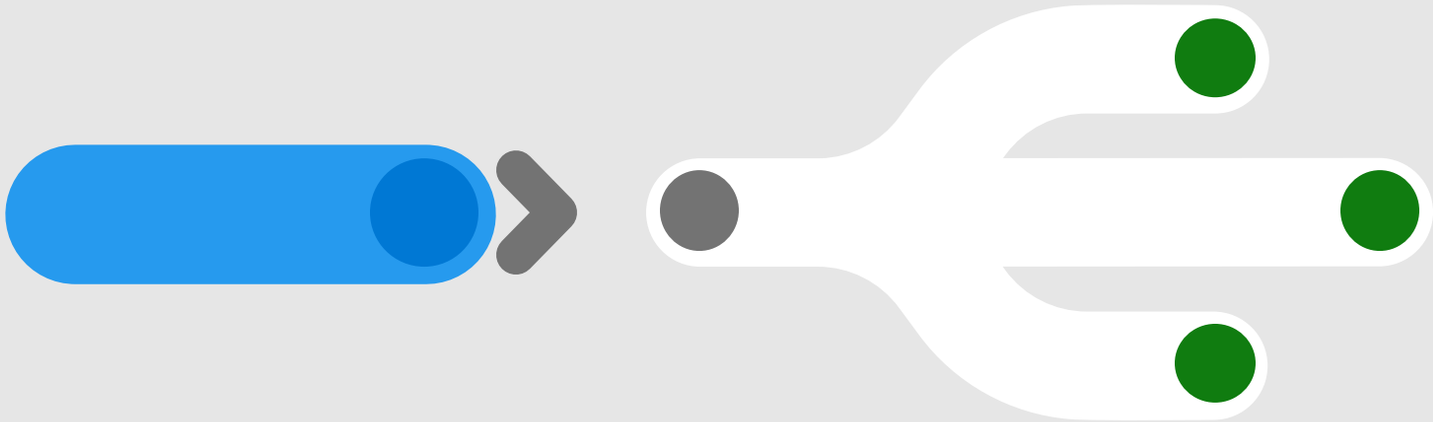
Native integrations

- Microsoft Defender
- Microsoft Sentinel
- Microsoft Information Protection
- Azure Active Directory

17,000+ supported apps

Office 365, box, slack, Dropbox, Microsoft Teams, G Suite, okta, salesforce, zoom, webex by cisco, Adobe, tableau, GitHub, Power BI, zendesk, Confluence, servicenow, SAP Concur, Microsoft Dynamics 365, DocuSign, Jira Software, Workiva, workday, Workplace by facebook

02
Shadow IT Discovery and Control

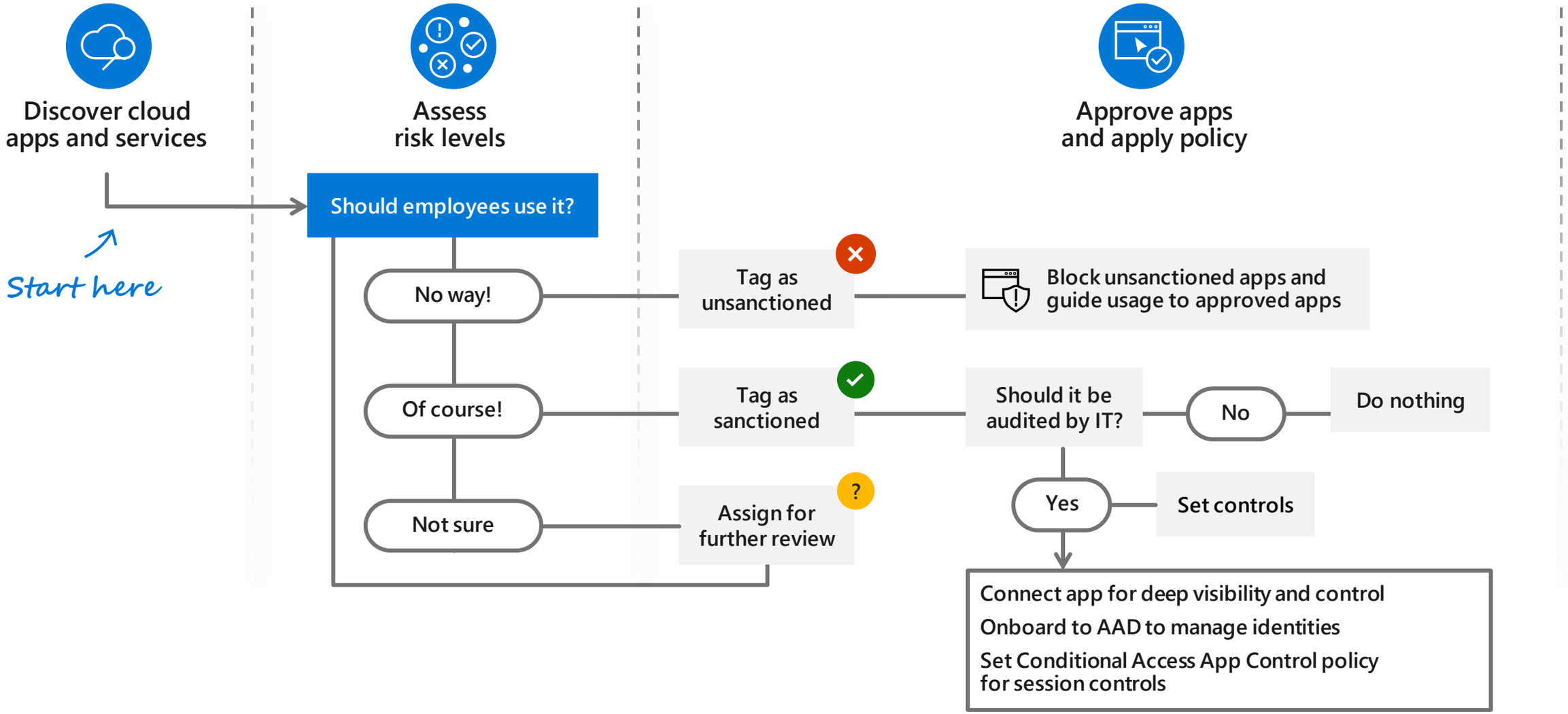


Discover Shadow IT

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

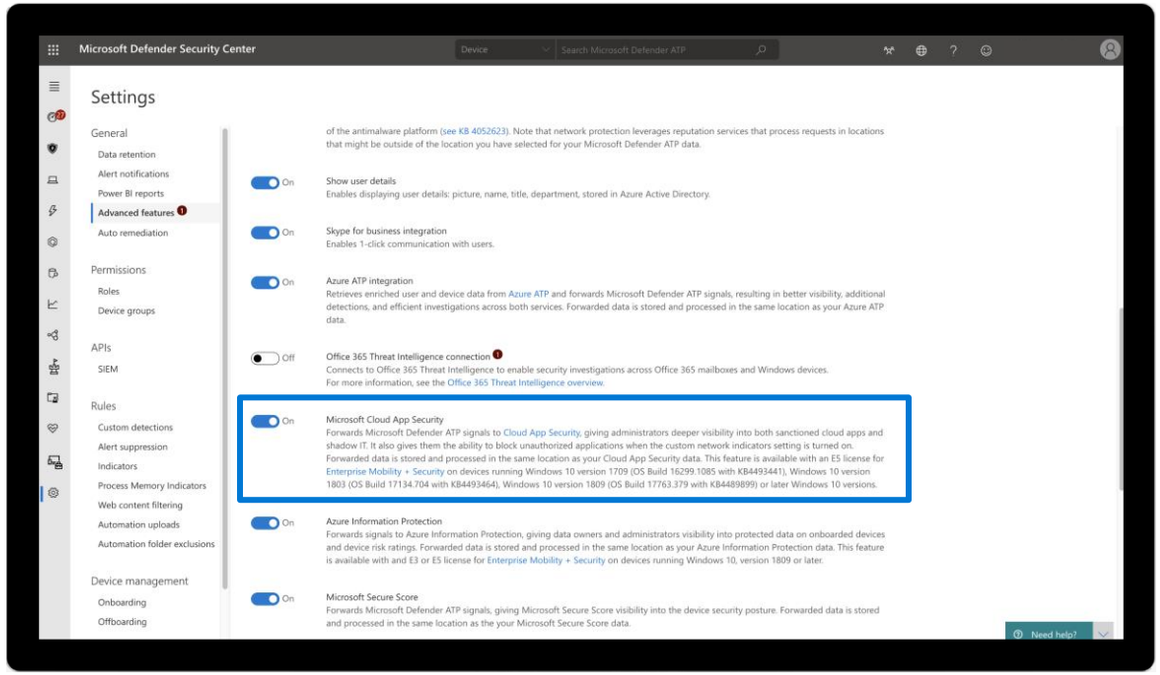
Discover and control apps in your environment

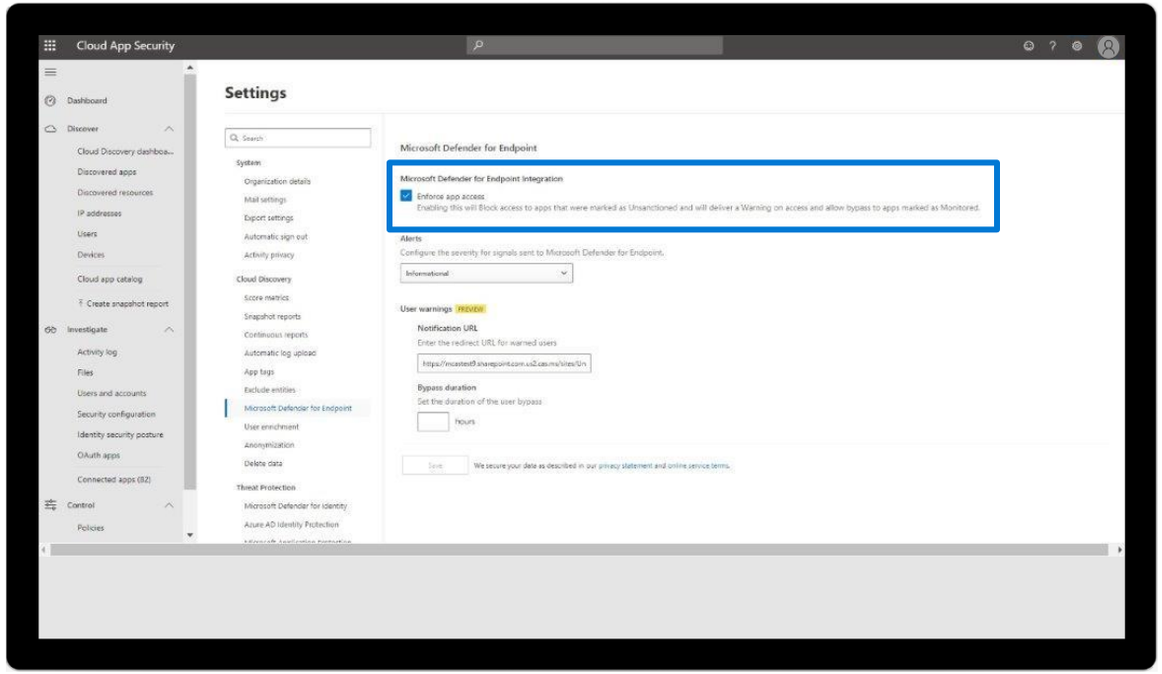
Take action: Manage newly discovered cloud app



Endpoint CASB - Shadow IT management with 2 clicks

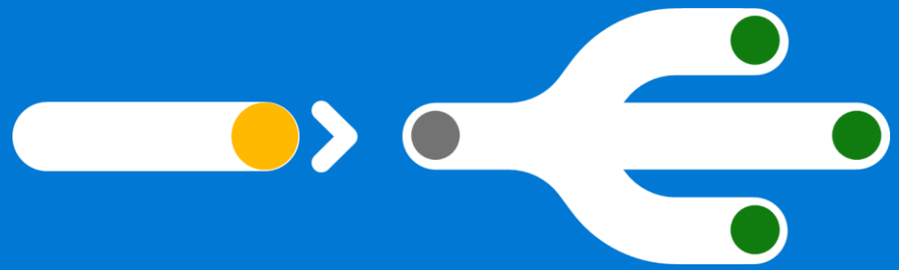
Shadow IT Discovery, monitoring and governance on the endpoint





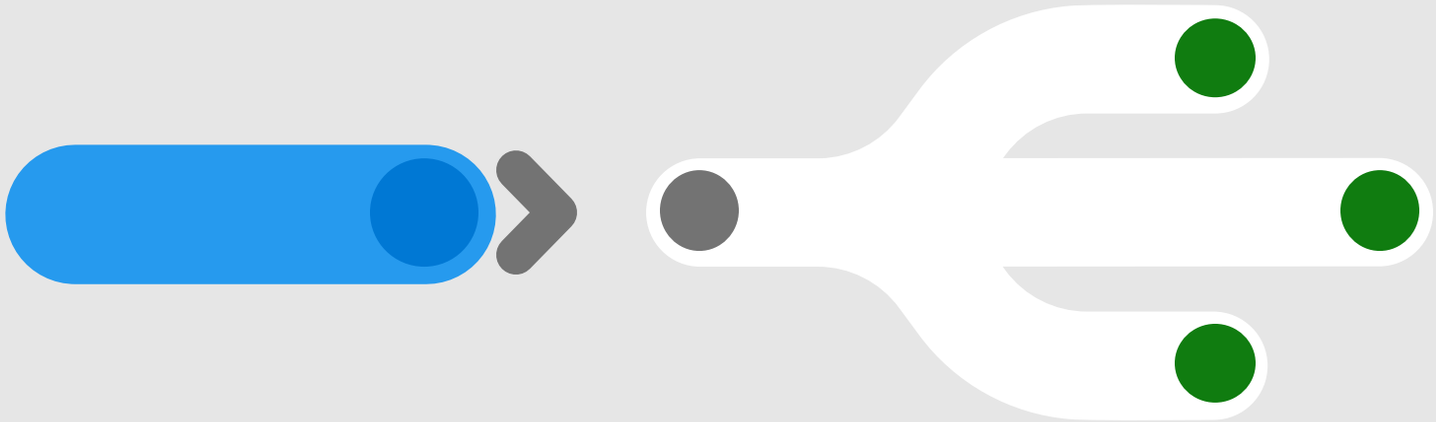
Demo

Discovering and assessing the risk of Shadow IT



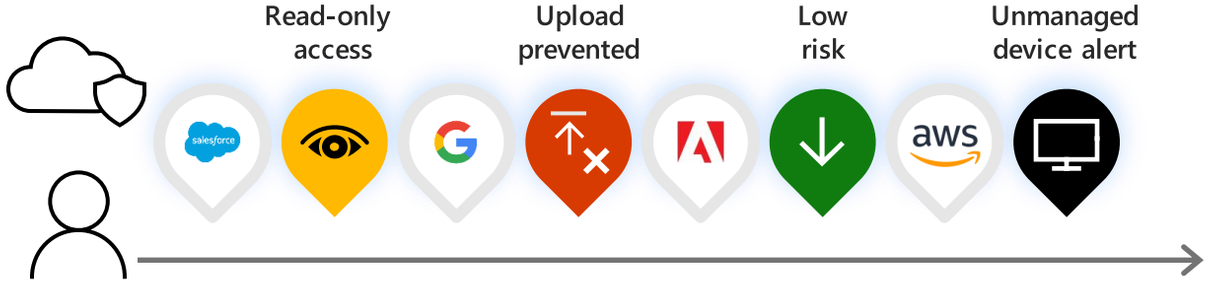
03

Secure Access to your apps

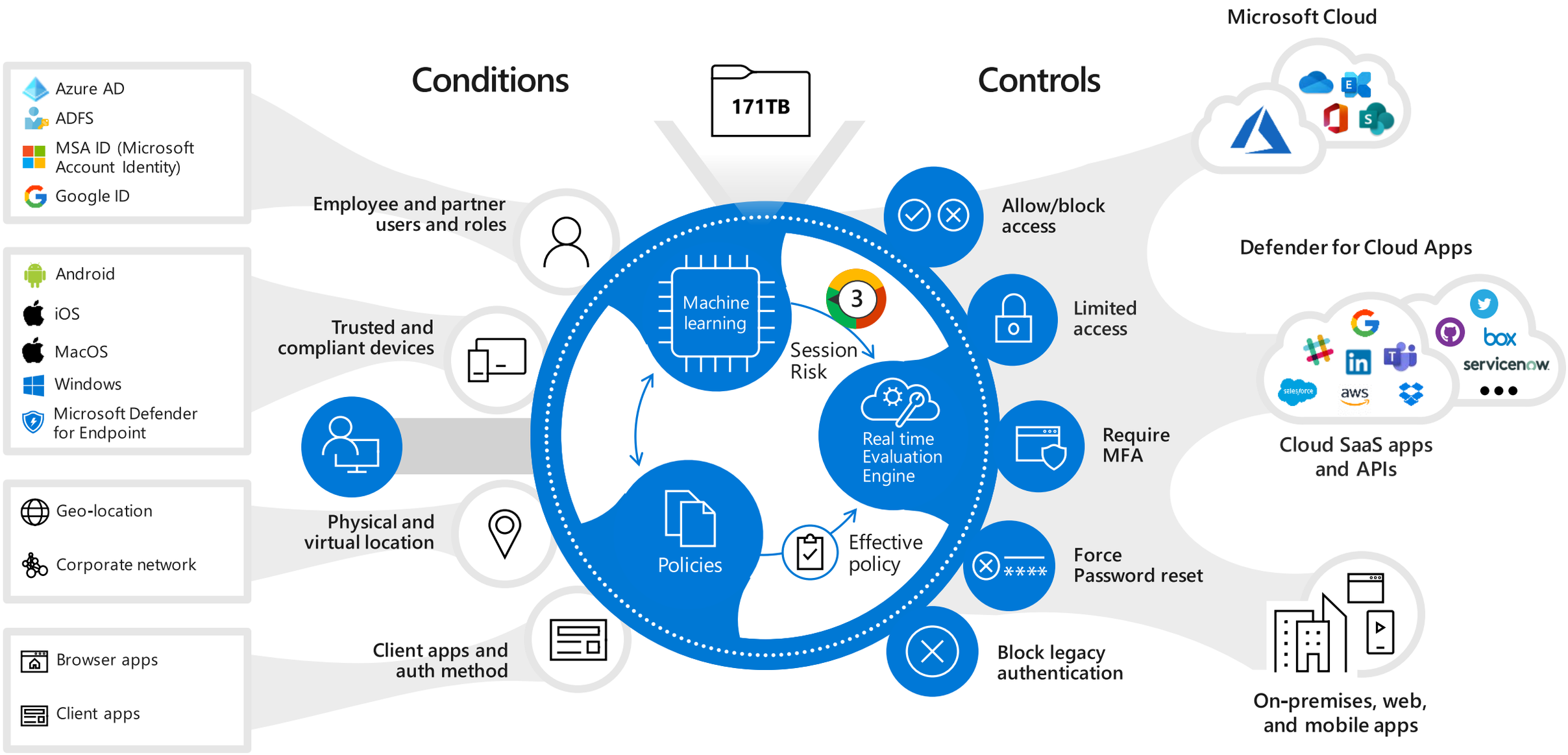


Secure Access

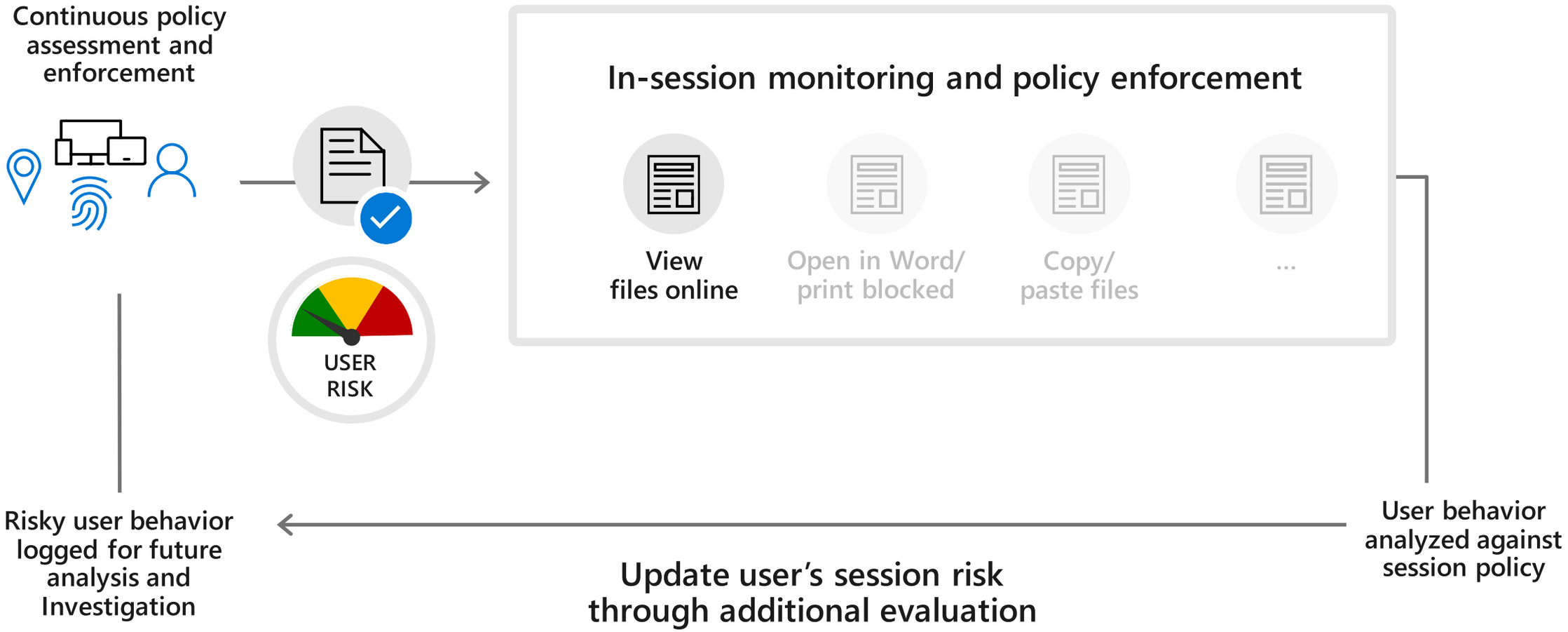
Integrating Defender for Cloud Apps with your identity provider enables real-time enforcement of in-session actions.



Secure Access in real-time



Extend policy enforcement into the session



Real-time in-session App Control

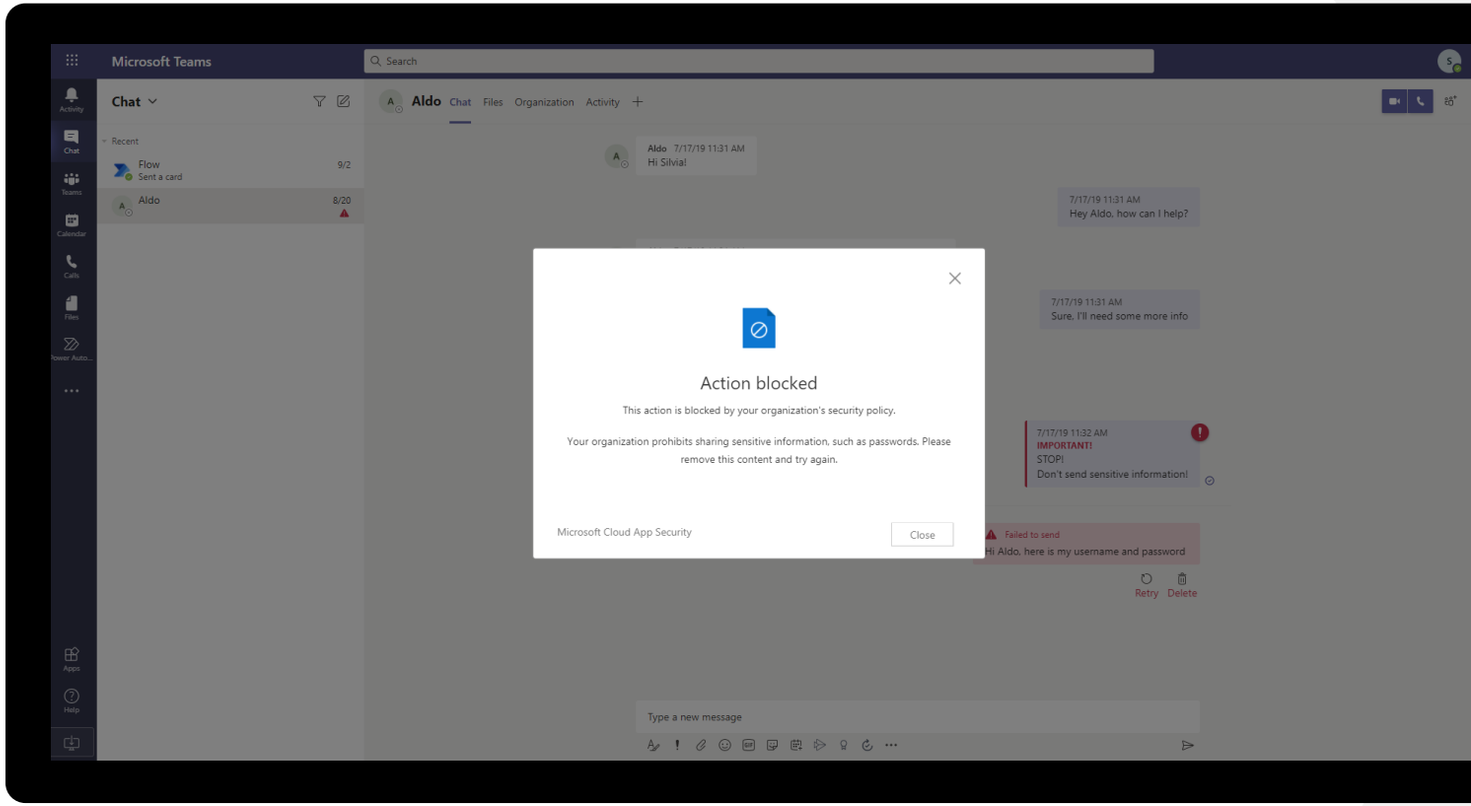
Context-aware session policies
Control access to cloud apps and sensitive data within those apps based on user, location, device, and the status of the application within the environment

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

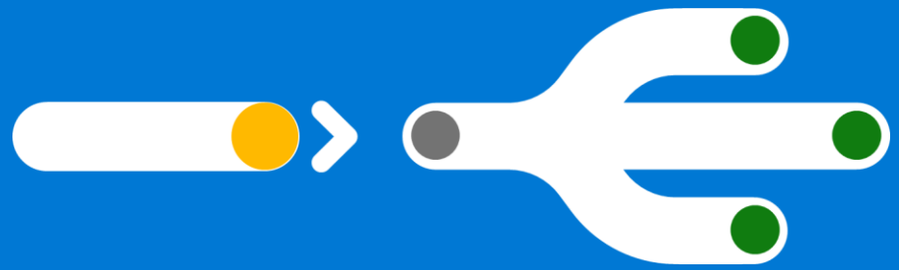
Data Exfiltration:
- Block download, Apply AIP label on download
- Block print
- Block copy/cut
- Block custom activities: (e.g., IMs with sensitive content)

Data Infiltration:
- Block upload
- Block paste

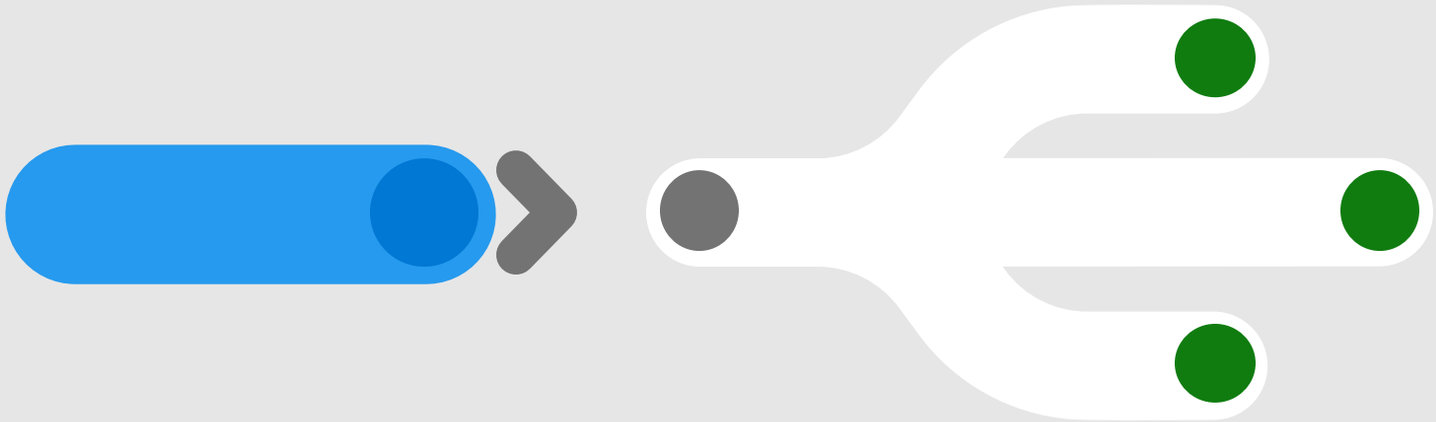


Demo

Enabling real-time access controls

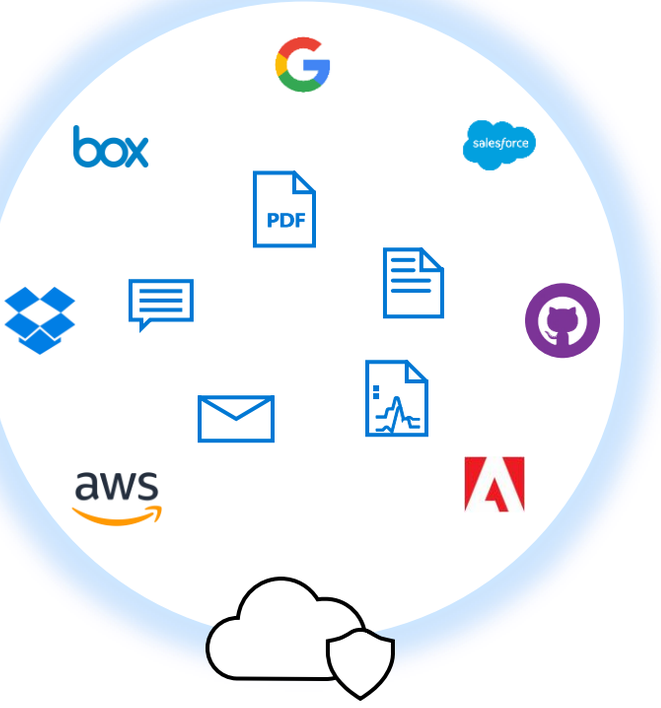


04
Information Protection



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

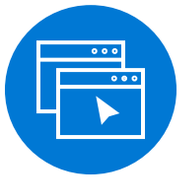
Classify

Protect

Monitor

Across

Devices

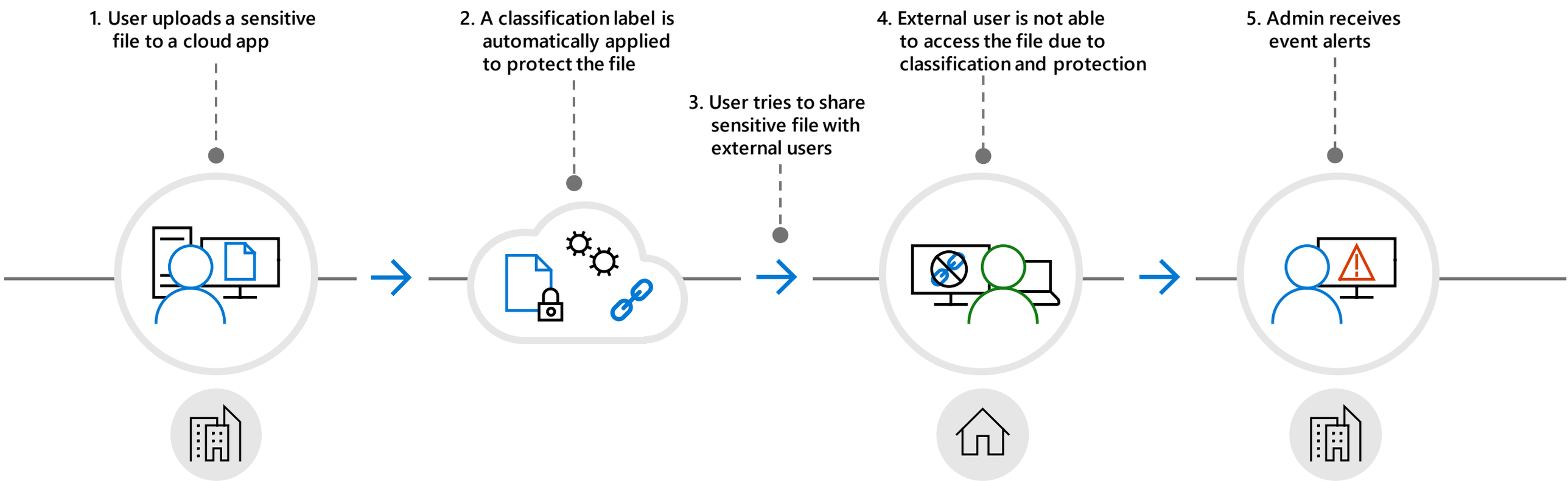


Apps

Cloud services

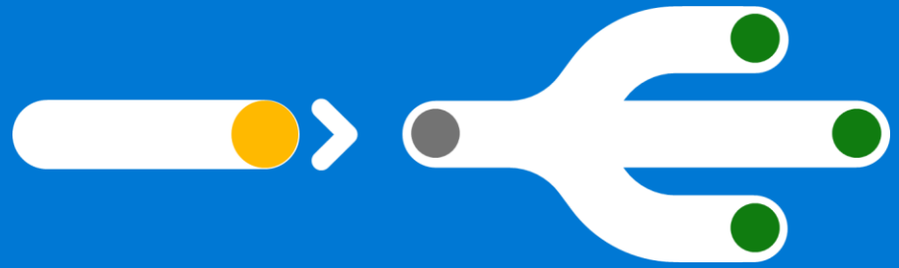
On-premises

Lifecycle of protecting sensitive files in the cloud



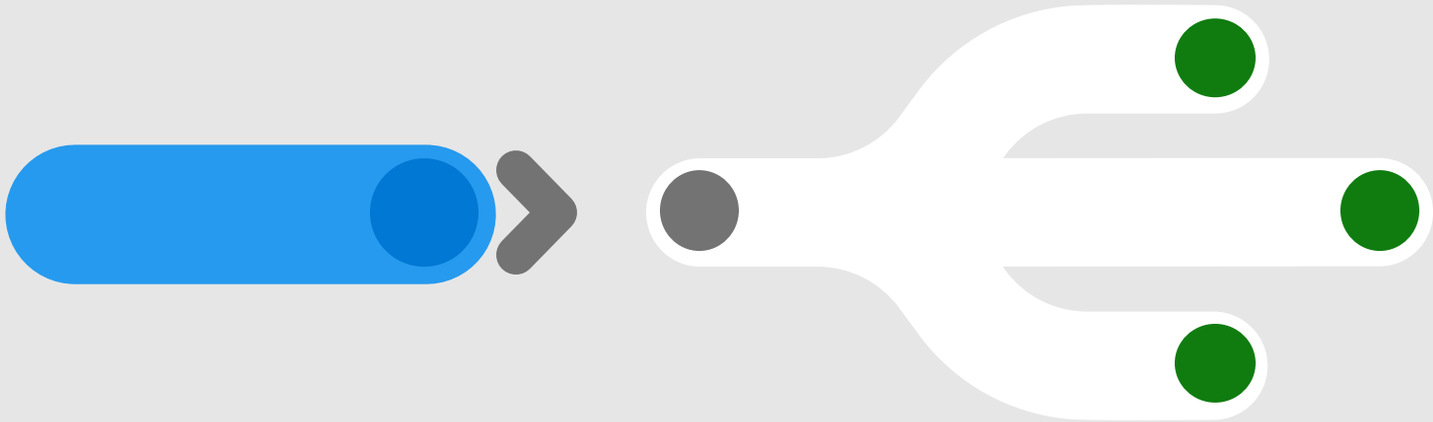
Demo

Information Protection



05

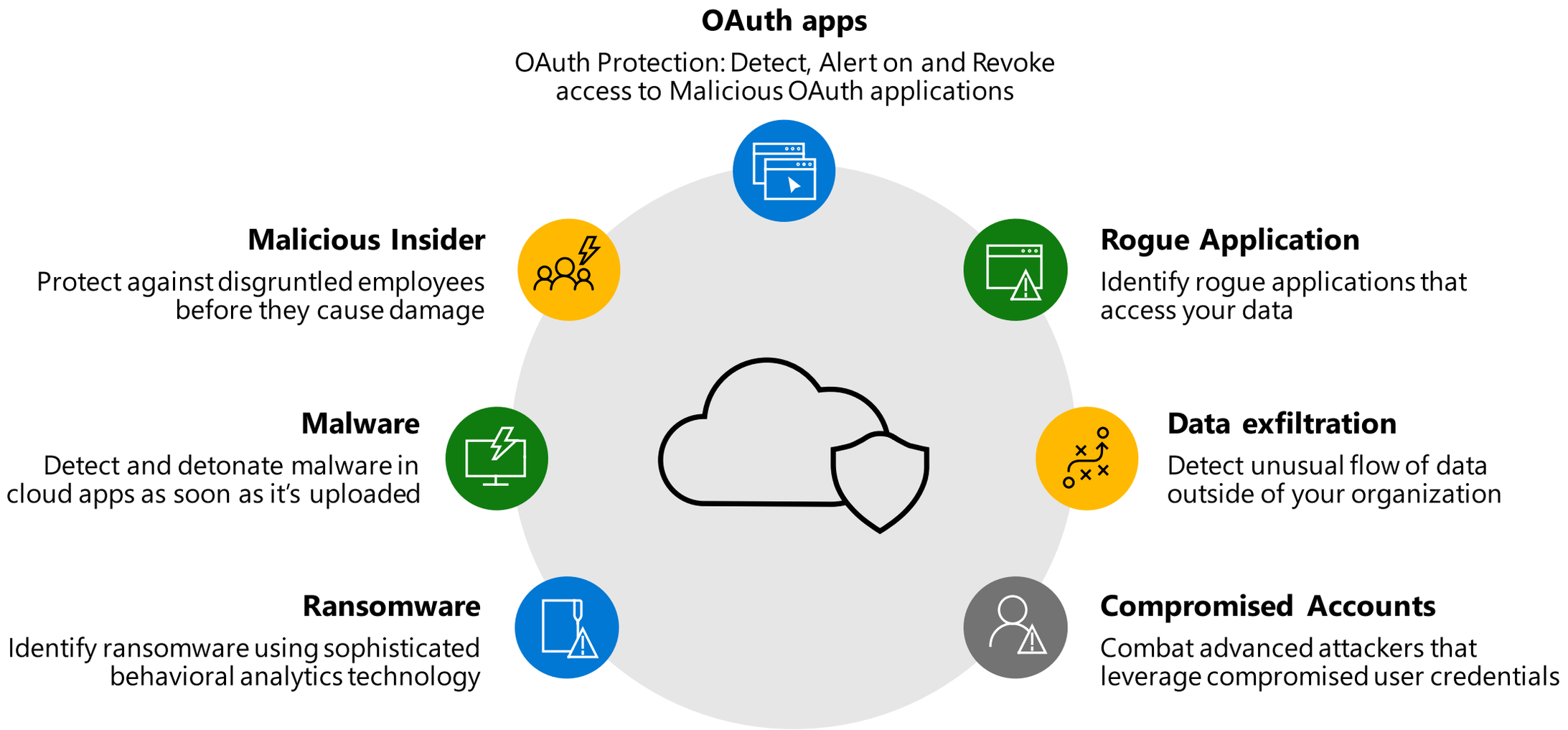
Threat Protection for your cloud environment



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

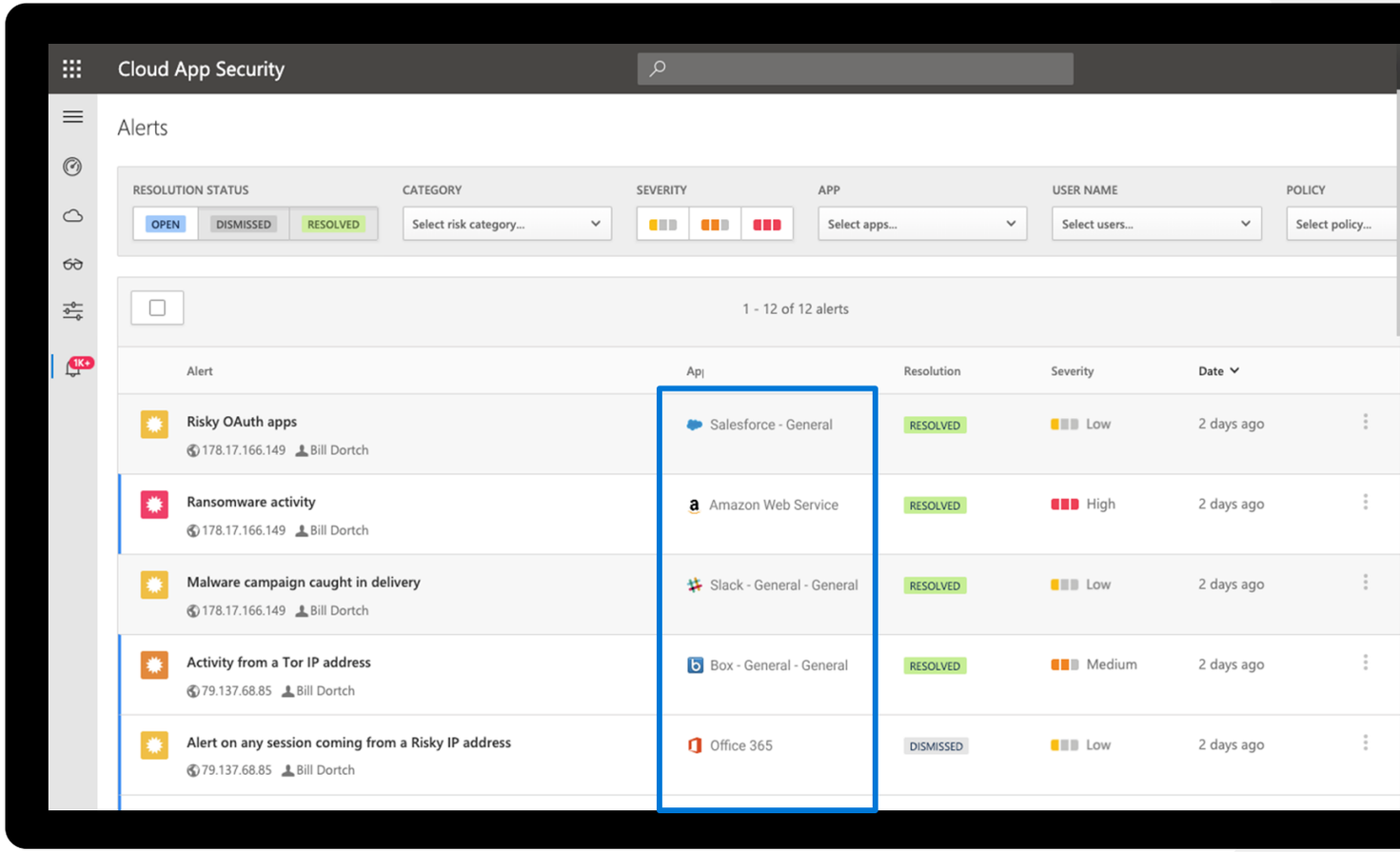
Built-in Threat Protection policies
More than 20 out-of-the-box policies and growing. Policies alert you on some of the most common cloud threats such as impossible travel, impersonation activities or ransomware detection

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

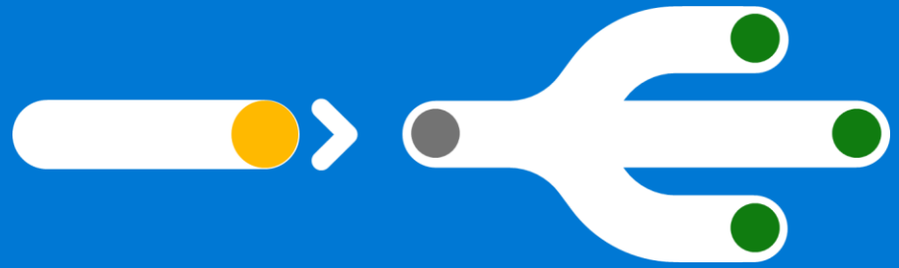
Prioritized investigation of alerts
Overview of users who likely pose the greatest risk to the organization and are recommended for immediate review with a unified view of identity threat across on-premises and cloud

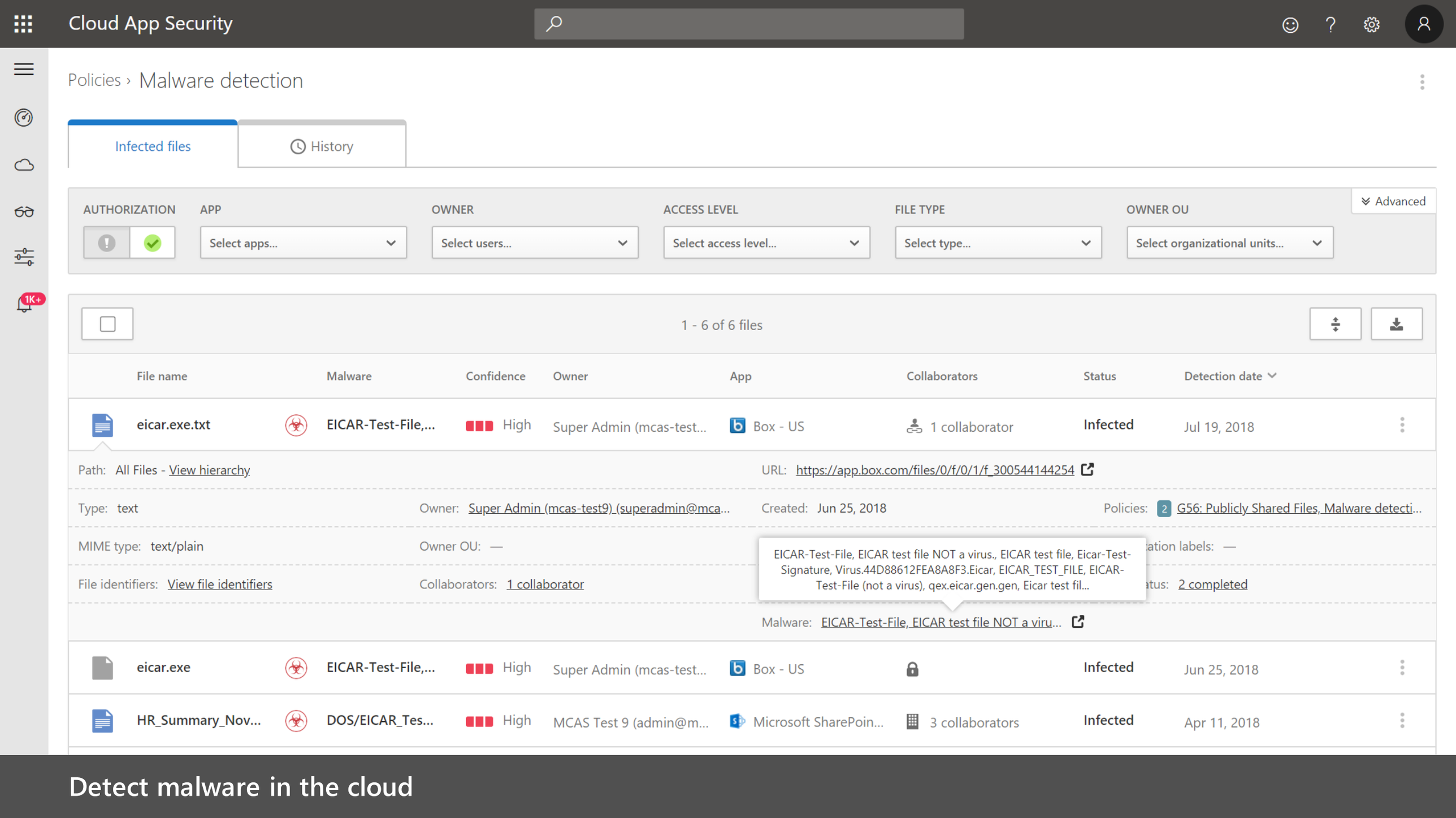
Achieved 100% product features in the threat protection pillar Gartner Magic Quadrant 20201



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

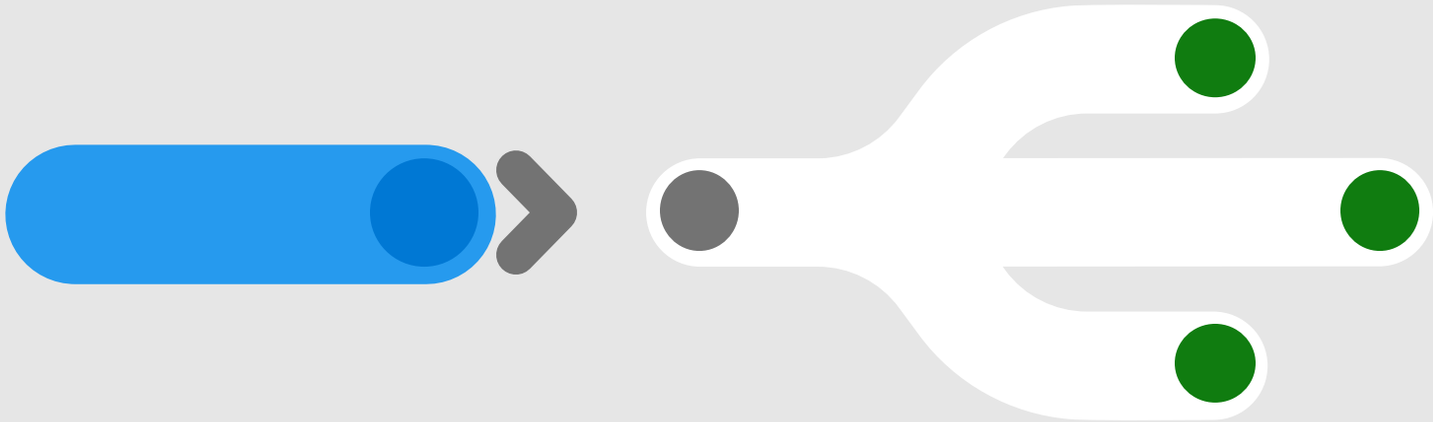
Demo
Threat Protection





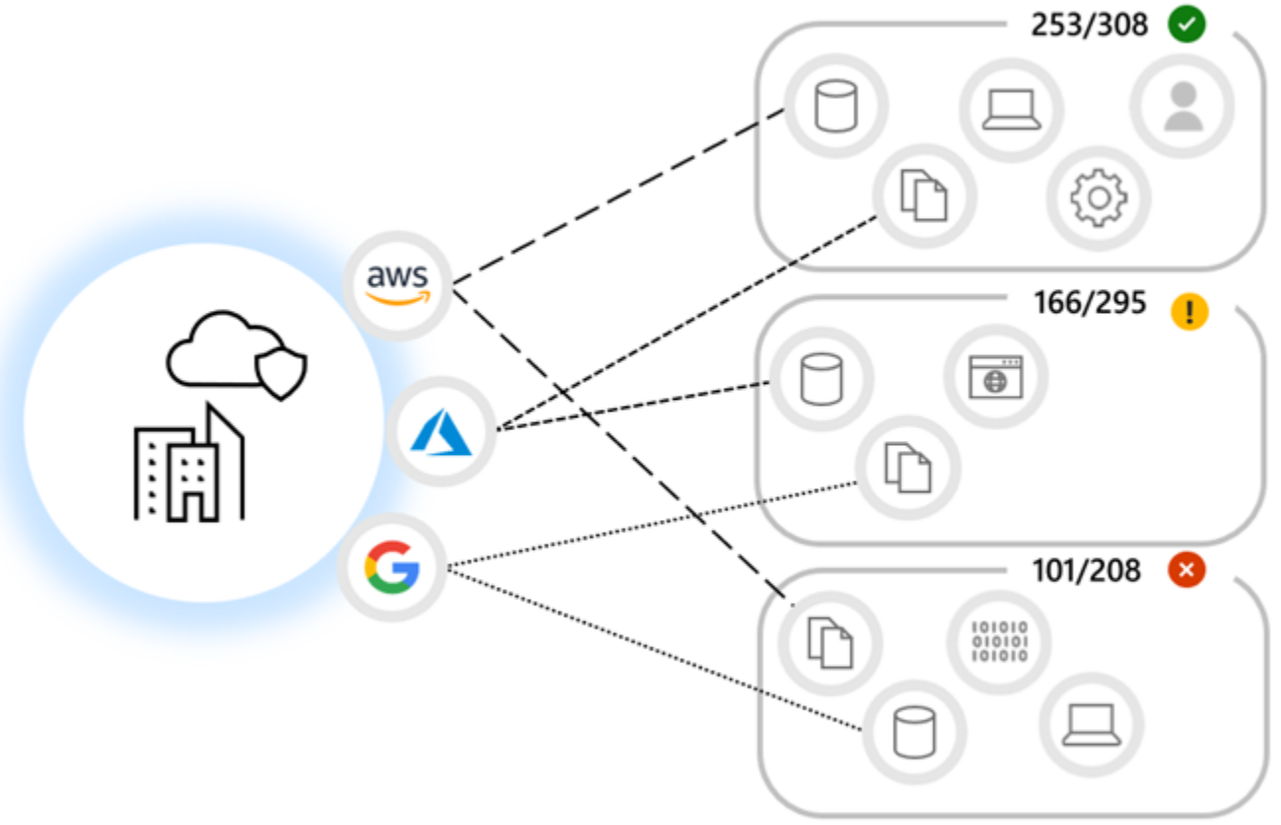
Detect malware in the cloud

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

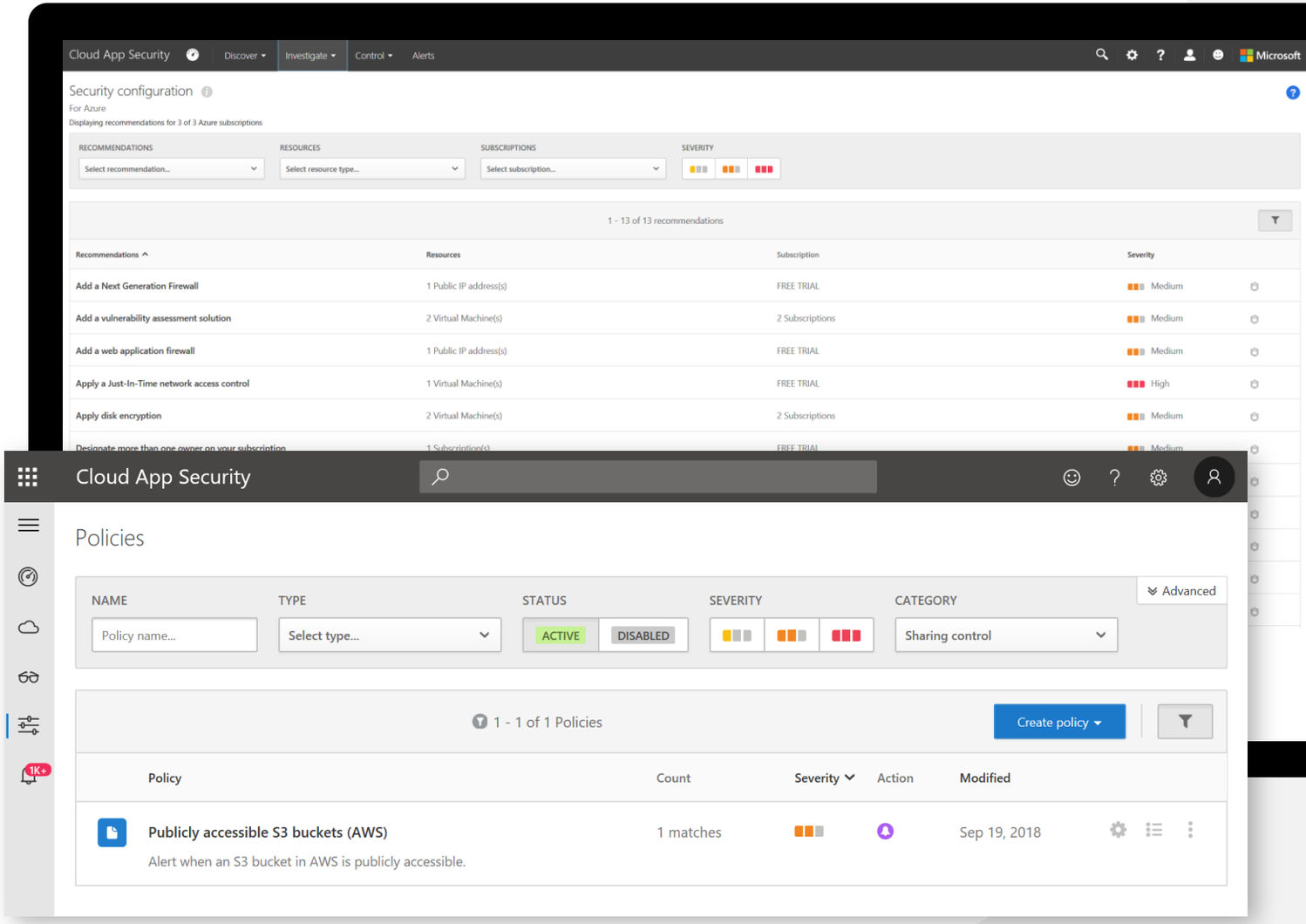
Analyze the security posture of your cloud platform and identify missing security configurations and controls

Unique integration with Microsoft Defender for Cloud

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

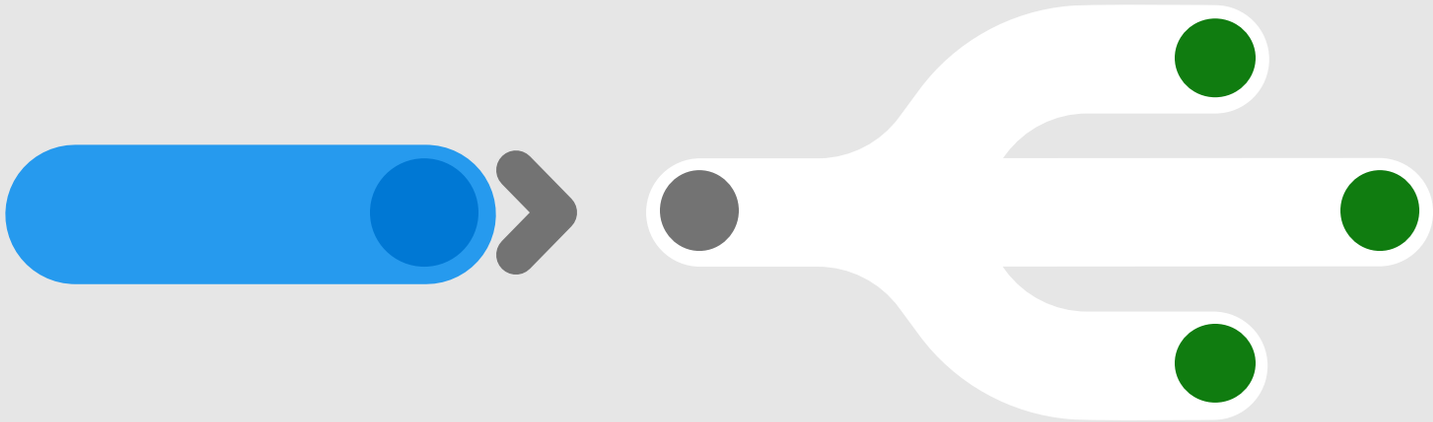
Multi-cloud capabilities and integration

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



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

Microsoft Security

Questions?

Thank you

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