Microsoft Security

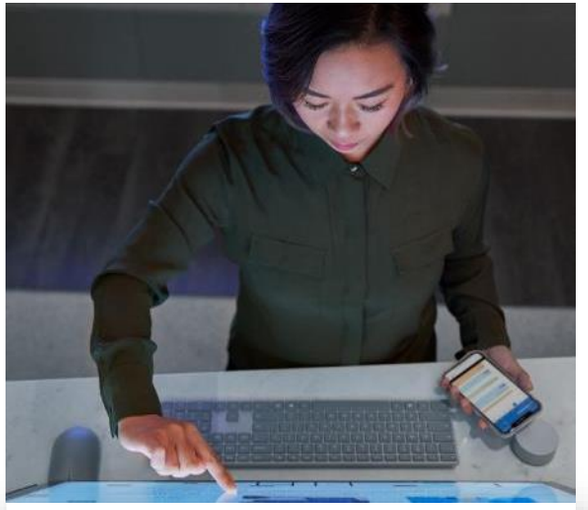
Microsoft Defender for Cloud Apps

Table of Contents

Microsoft security

Secure Access

Protect all points of access and real-time controls in a connected world

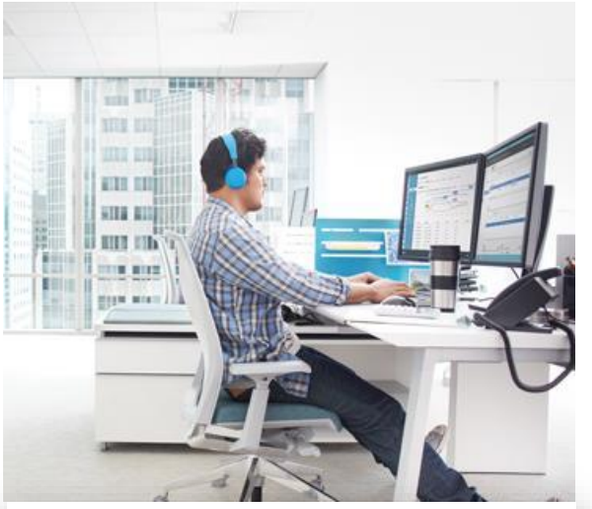


Threat Protection

Stop attacks with integrated, automated SIEM and XDR

Information Protection

Protect sensitive data and manage insider risks with intelligence



Cloud Security

Safeguard your multi-cloud resources

Microsoft Cloud App Security

Our approach

Safeguard your multi-cloud apps & resources

Strengthen multi-cloud security posture

Azure Security Center,
Microsoft Cloud App Security

Protect cloud workloads

Azure Security Center,
Azure Defender

Control activity across cloud apps

Microsoft Cloud App Security

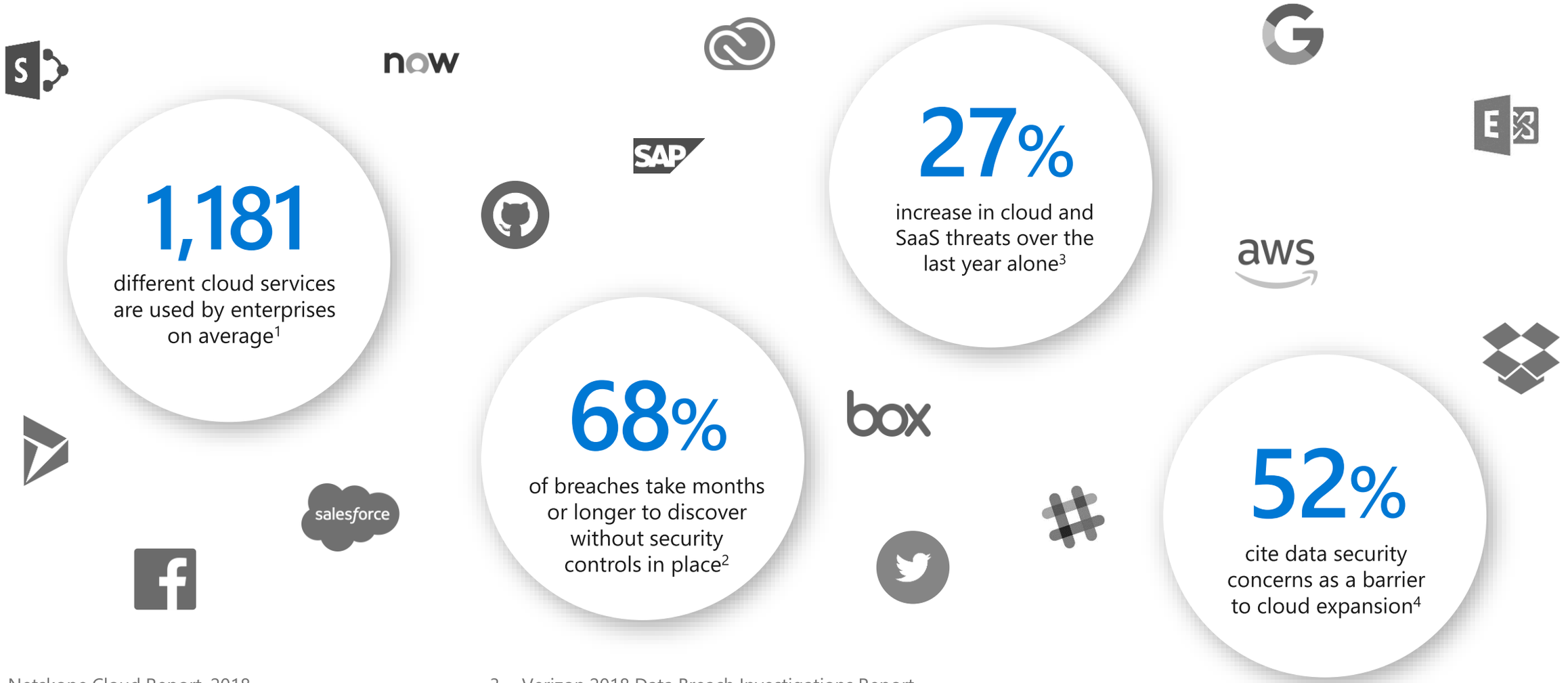
Develop secure applications

GitHub

01

Introduction to Cloud Access Security Brokers

Cloud services require a new approach to security



1. Netskope Cloud Report, 2018
2. Ponemon: 2017 Cost of Cybercrime Study
3. Verizon 2018 Data Breach Investigations Report
4. Securing Cloud Transformations, 451 Research, July 2020

Cloud Access Security Brokers

Gartner's definition for CASBs:

"Especially designed to protect and control access to data that's stored in someone else's systems, CASBs deliver differentiated, cloud-specific capabilities that generally aren't available as features in traditional security products. CASBs provide a central location for policy and governance concurrently across multiple cloud services and granular visibility into and control over user activities and sensitive data from both inside and outside the enterprise perimeter, including cloud-to-cloud access." [1]

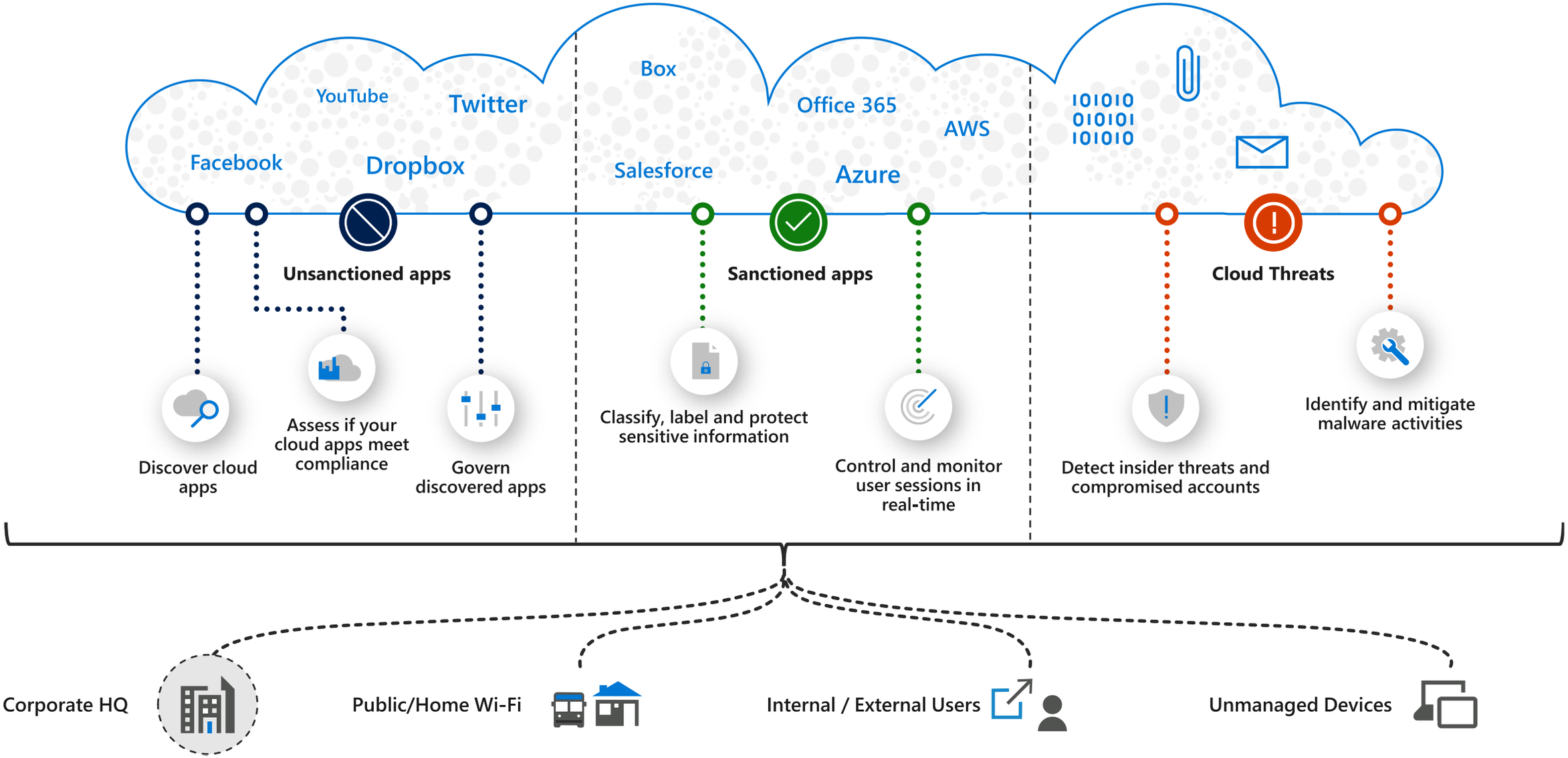
CASB spend investment is predicted to grow over

30% each year

between now and 2024[2]

1. Gartner, Magic Quadrant for Cloud Access Security Brokers 2020
2. Forecast: Information Security and Risk Management, Worldwide, 2018-2024

Top CASB use cases



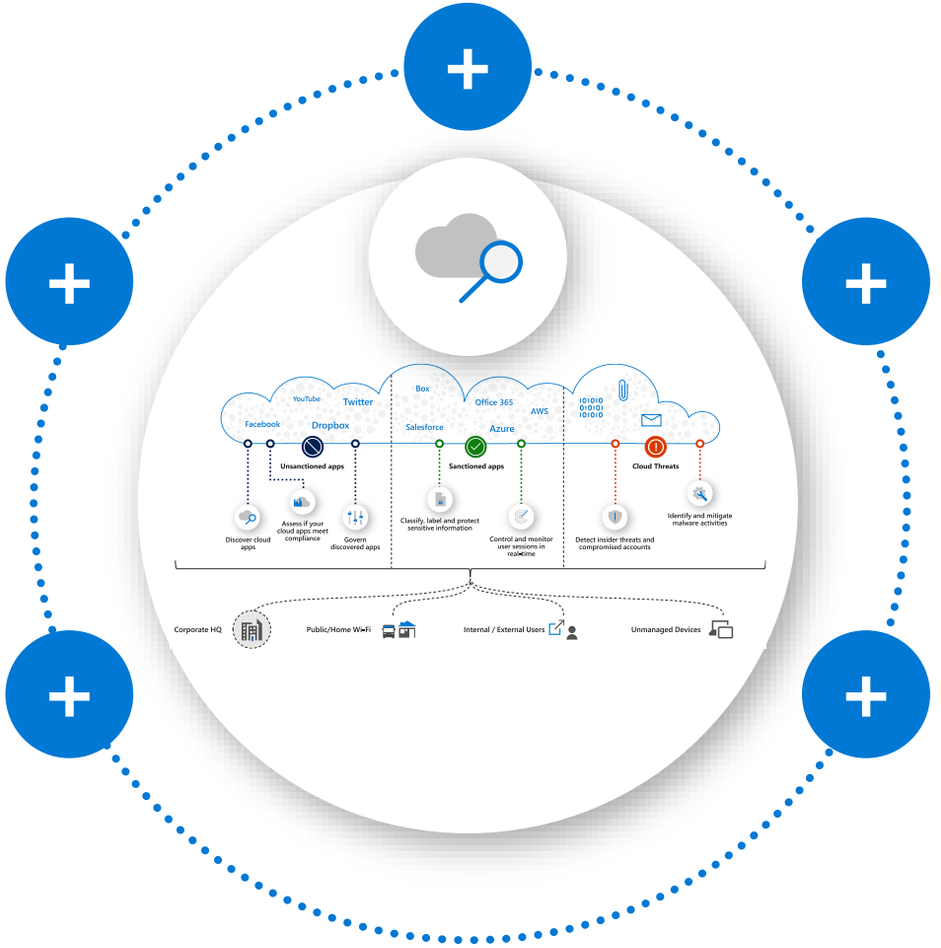
Microsoft does all of that and more

Discover and control the use of shadow IT

Identify, and assess risk of cloud apps and services used by your organization.

Protect your information anywhere in the cloud

Understand, classify, and protect the exposure of sensitive information—across all your cloud apps.



Protect against cyberthreats and anomalies

Detect unusual behavior, compromised users, or rogue applications and remediate automatically.

Secure Access

Secure access, without compromising performance, for any user on any device to any resource.

Security Posture Management

Investigate security configuration gaps by viewing all cloud platform security recommendations together.

02

Microsoft Cloud App Security

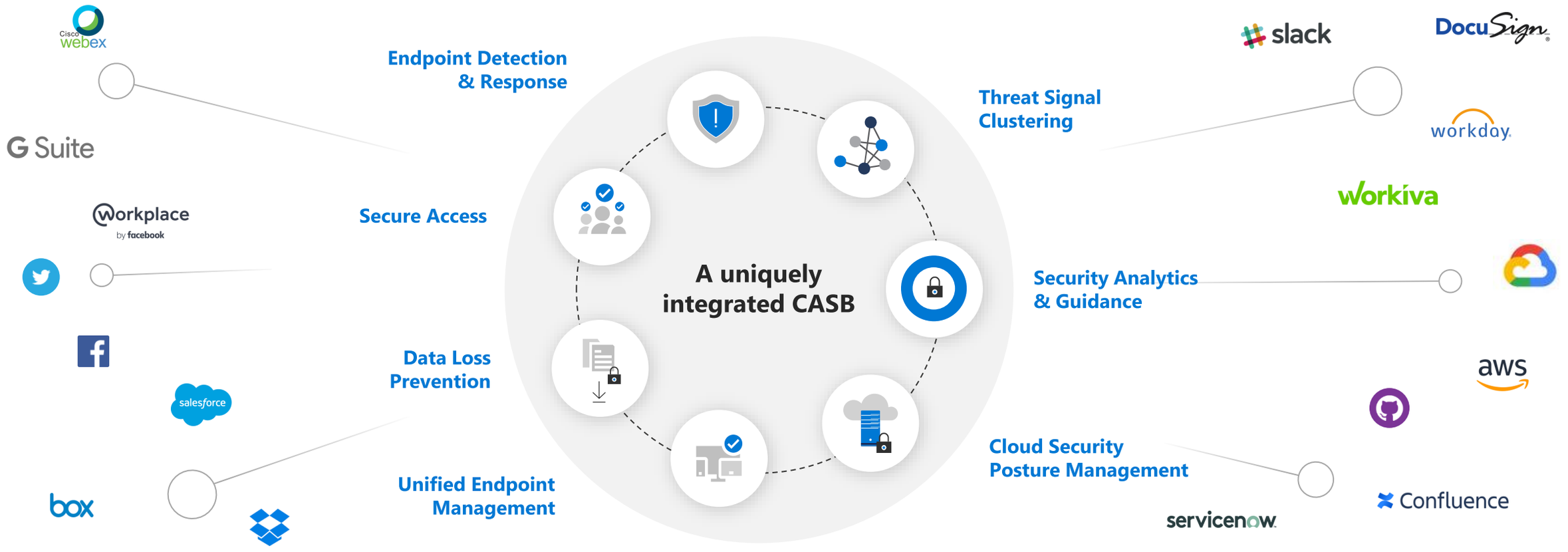
Microsoft Cloud App Security

The go-to CASB for all your cloud enablement, monitoring and governance

Simple deployment

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

Rooted in supporting any app



Microsoft Cloud App Security provides comprehensive session security and data use policies

Cloud platforms

- 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, LEARNING, Confluence, Cornerstone, DocuSign, Adobe, box, HighQ, Dropbox, G Suite, zendesk, workday, aws, Workiva, tableau, JIRA Software, Workplace by facebook, CONCUR, Cisco webex, okta, zoom, salesforce, slack, GitHub, servicenow

03

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.

Discovery with Cloud App Security is fast and easy to implement

Gain visibility across your entire cloud app portfolio through a single pane of glass

Cloud App Security initial implementation requires just 15 person-hours, and ongoing management of the solution itself requires an average of 12 person-hours per week. Prior to the investment in Cloud App Security, SecOps spent 90 person-hours per week monitoring the security and risk posture of cloud applications.

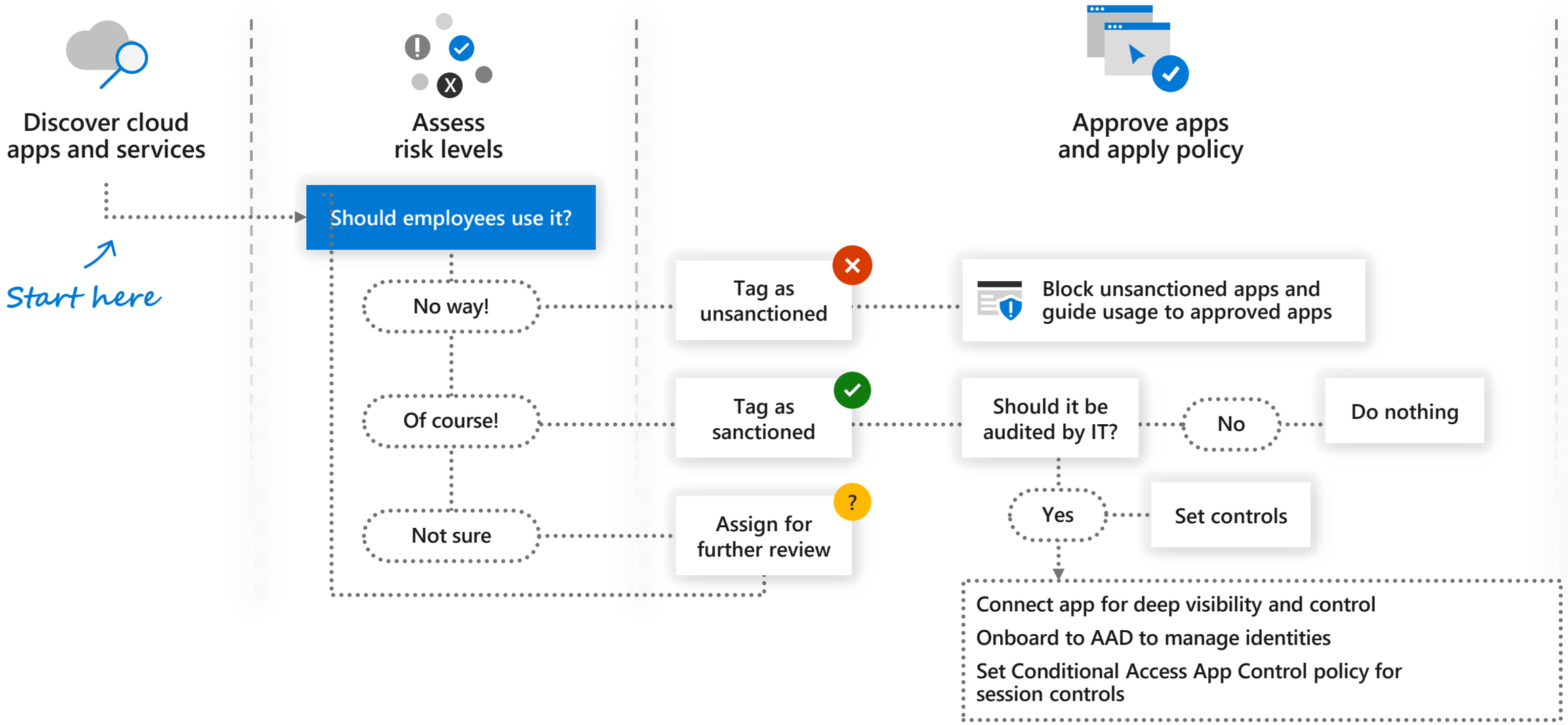
The visibility provided by Microsoft Cloud App Security enables customers to reduce time in monitoring, assessment, and governance of cloud risk by 80%

Cloud App Security also provides flexibility to integrate with existing architectures, including log ingestion from firewalls, secure web gateways and security information and event management solutions (SIEMs), API-based connectors, and reverse-proxy integration with their primary identity and access management (IAM) providers.

Source: Forrester, The Total Economic Impact™ Of Microsoft Cloud App Security, May 2020

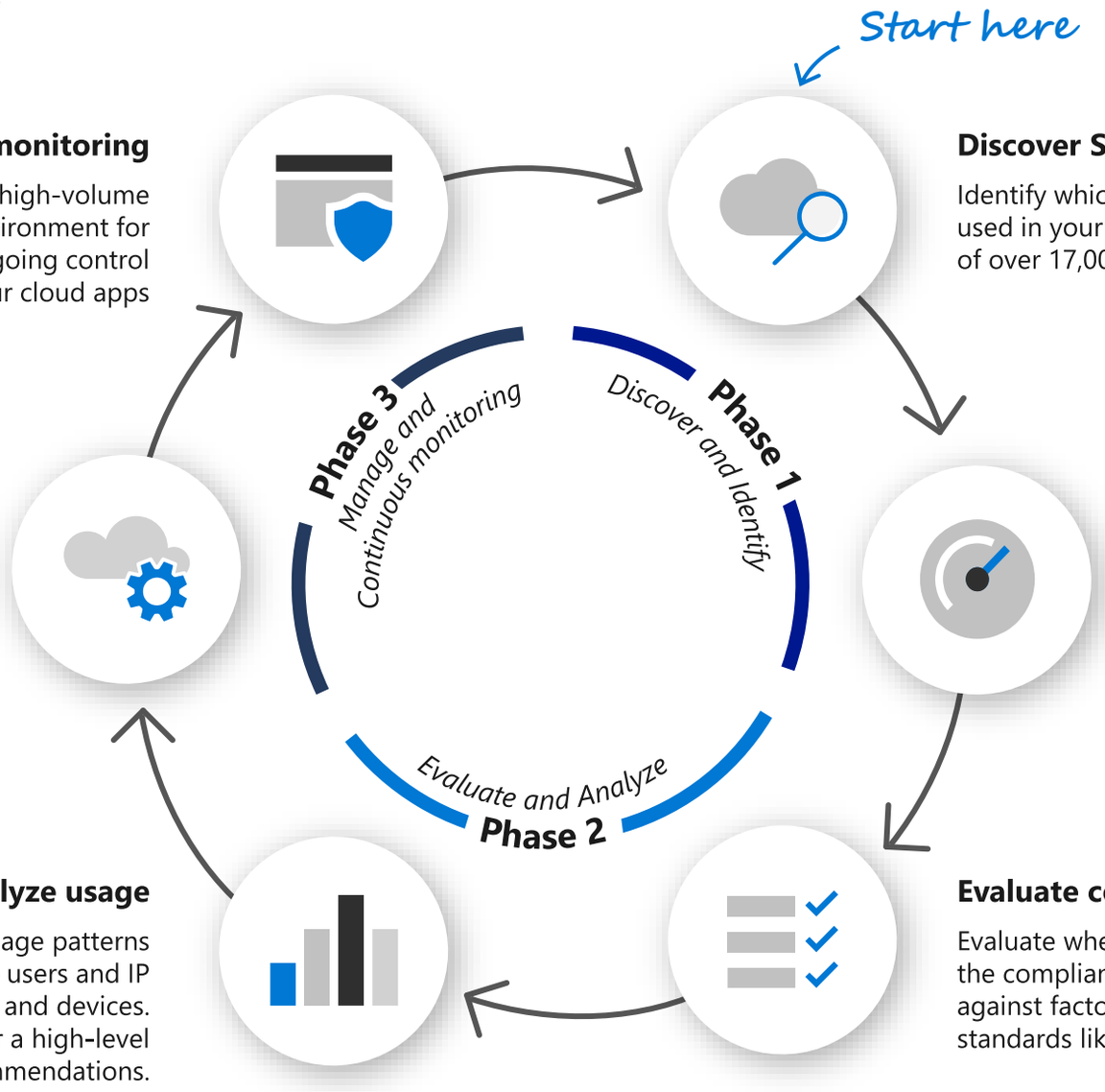
Discover and control apps in your environment

Take action: Manage newly discovered cloud app



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

Cloud App Discovery

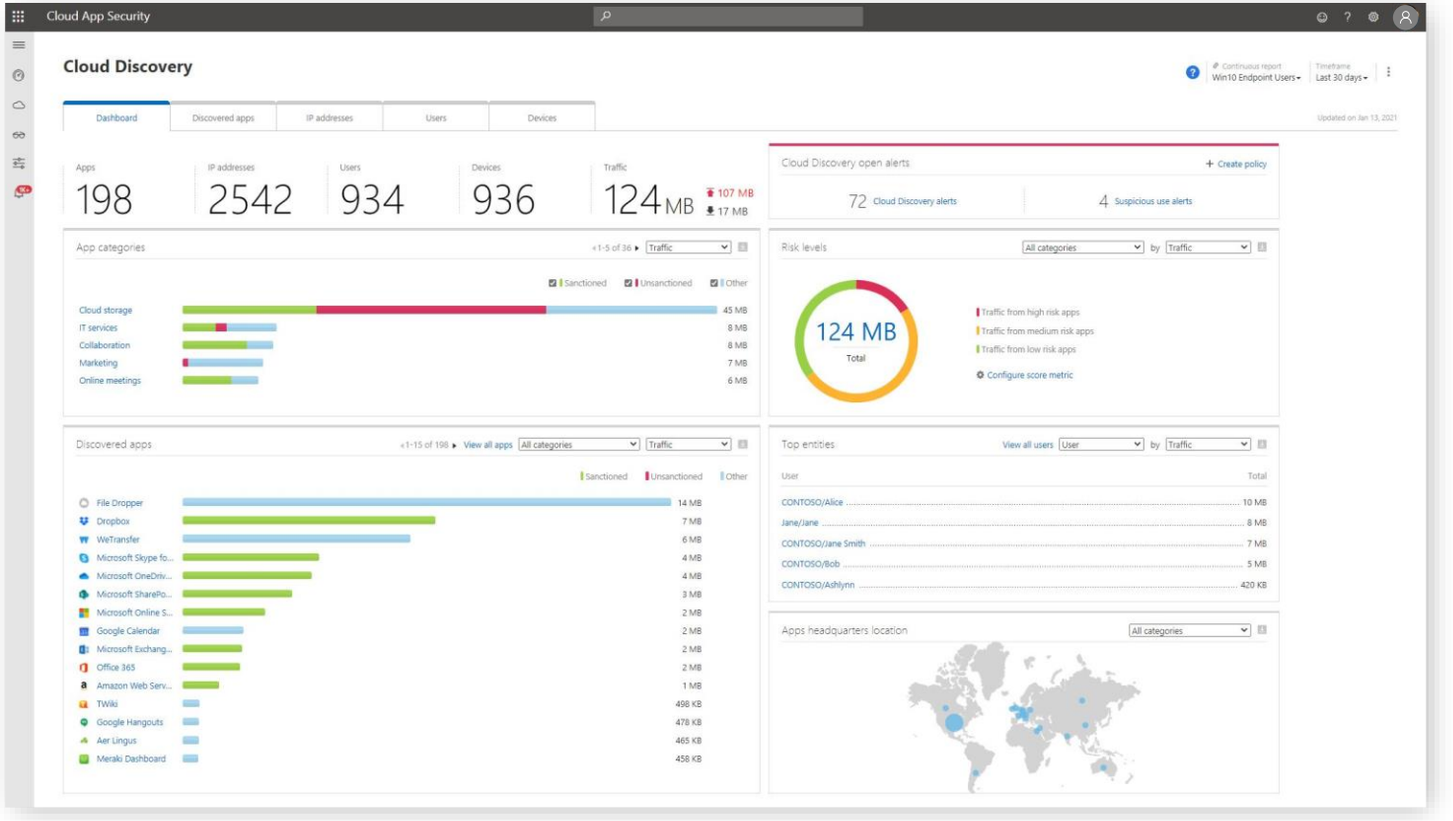
Discovery of Shadow IT across SaaS, IaaS and PaaS
Discover cloud usage across all locations (HQ, Branches, Remote) using native and programmatic integration with Microsoft Defender for Endpoint

Understand the risk of your SaaS apps
Risk assessment for 17,000+ cloud apps based on 90+ security and compliance risk factors

Analyze usage patterns
Understand the usage patterns and identify high risk volume users by understanding traffic data, top users and IP addresses, app categories

Block risky and unsanctioned apps
Using native integration with Microsoft Defender for Endpoint and leading SWGs and proxies

Continuous monitoring
Be alerted when new, risky or high-volume apps are discovered



Cloud Discovery with Microsoft Defender for Endpoint

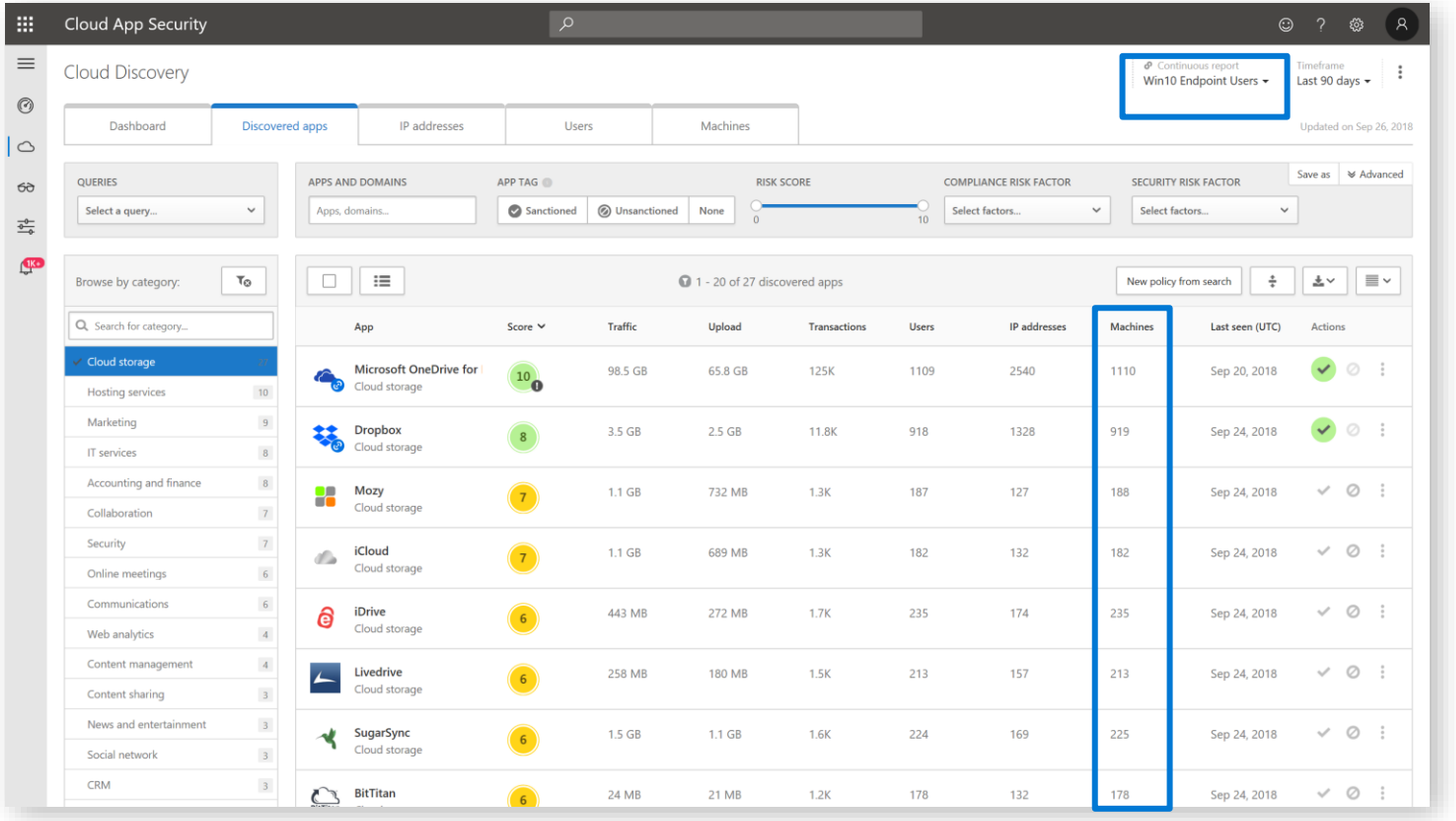
Native, endpoint-based discovery of Shadow IT
Connect your Defender for Endpoint system and gain visibility to your shadow IT from endpoints across your environment

Discovery of cloud apps beyond the corporate network from any managed Windows 10 device
Discover cloud app usage from any managed Windows 10 device anytime, anywhere, by anyone

Single-click enablement
With one click, stream traffic data from your managed Windows 10 devices into your Cloud App Security instance

Device-based Discovery
Go beyond user-based discovery and attribute cloud app usage to managed devices in the organization

Deep dive investigation in Microsoft Defender for Endpoint
In Microsoft Defender for Endpoint, drill down into each discovered device's behavior across your organization



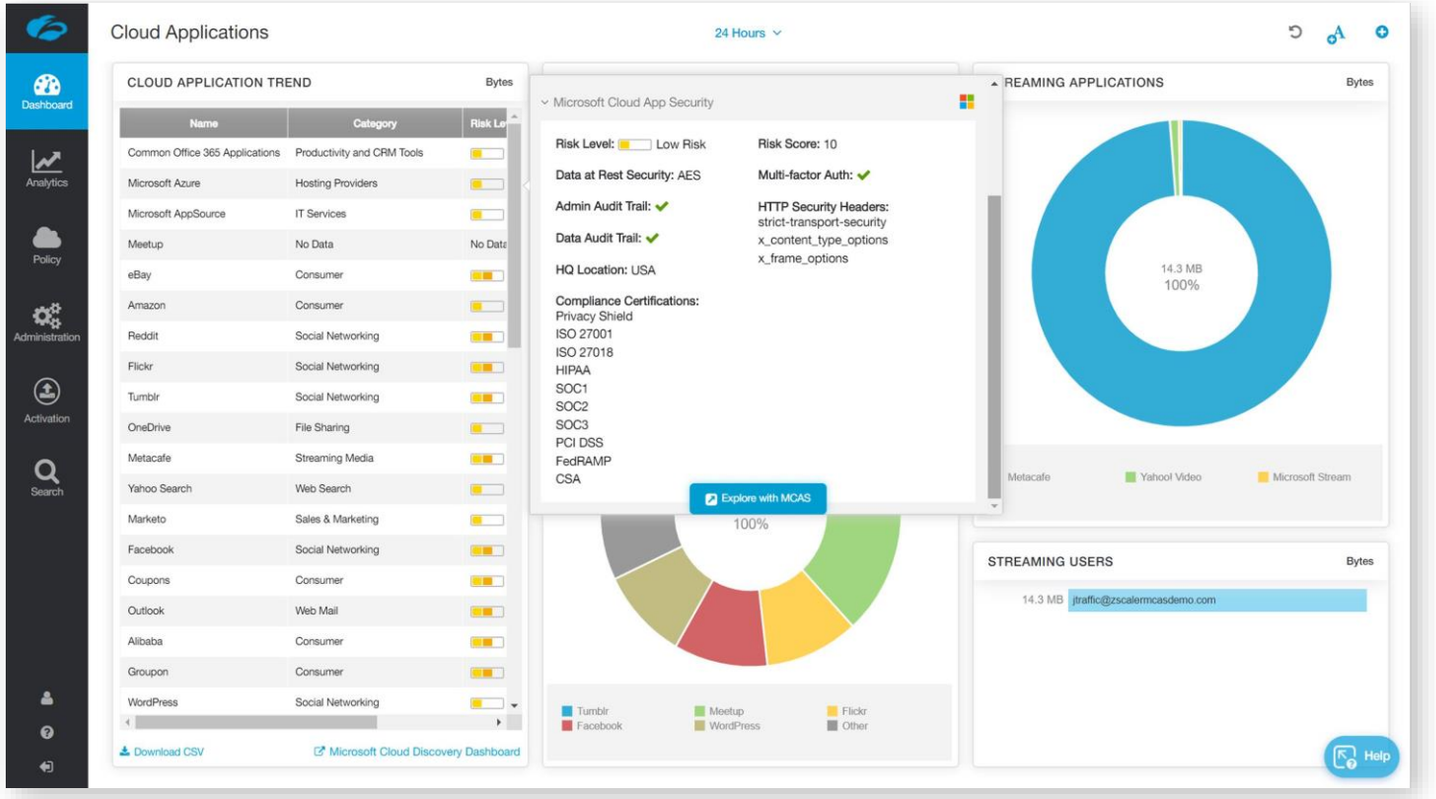
Integrate with your Secure Web Gateway

Enhanced visibility into Shadow IT and risk
Connect your existing Zscaler, iboss, or Menlo Security deployment to Cloud App Security for Discovery of Shadow IT, or to Corrata for mobile endpoint security

Zero-touch, 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, automatic log discovery
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



Discover and manage risky OAuth apps

Discover OAuth apps
That users have authorized to connect to your Microsoft 365 environment

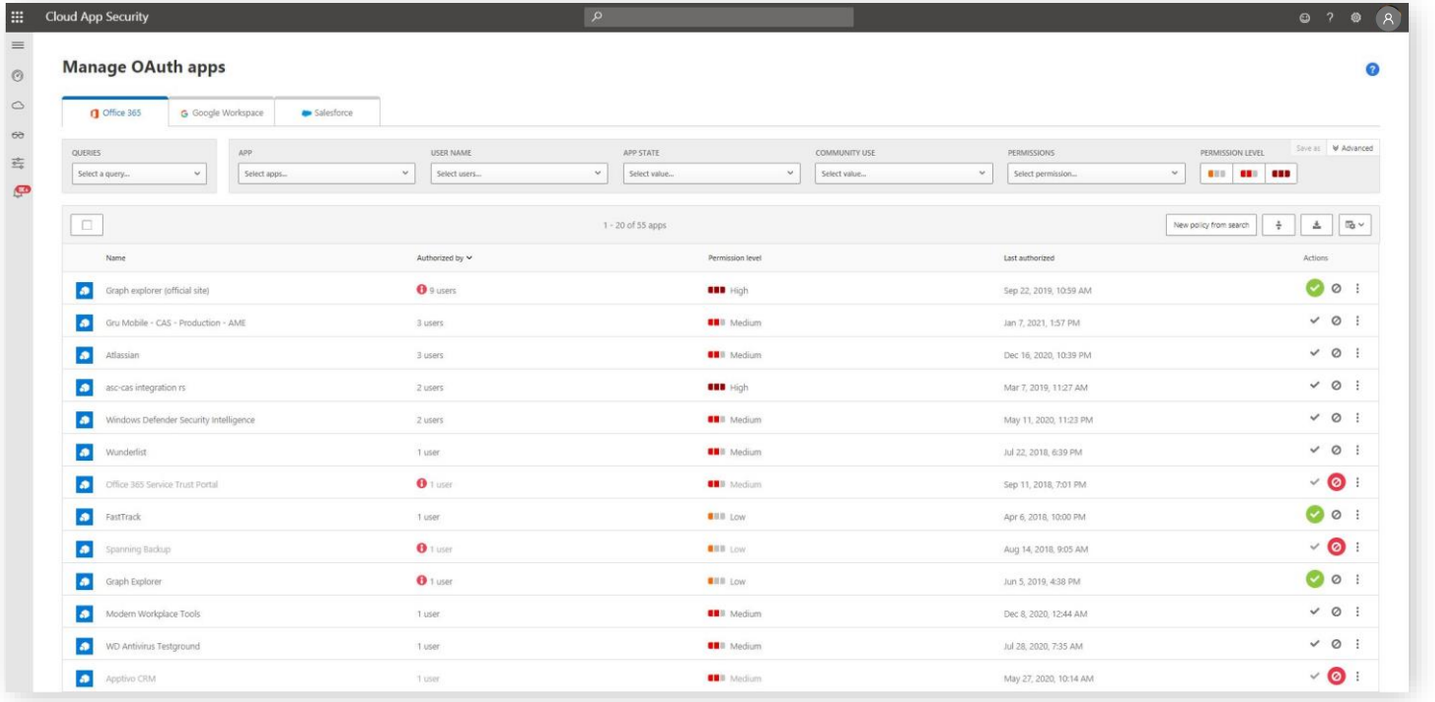
Identify and manage permission levels
Understand the implications to your business and take action

Define custom policies
Alert on trending, new and risky apps in use

Automatically revoke apps
Entire organizations or specific users and groups

Manage your SaaS and IaaS access
Such as G Suite and Salesforce (if these apps are connected to Cloud App Security)

Protect against attacks coming from OAuth vector
Modern phishing and the latest Solorigate attacks used OAuth apps as attack vectors. Protect your organization's cloud environments by gaining visibility and control over consented OAuth apps.



Discovered resources

Continuous report: Global
Timeframe: Last 30 days

APP: Select apps...
RESOURCE NAME: Select...
RESOURCE TYPE: Select value...
Advanced

1 - 20 of 27 resources

Resource	Resource type	App	Traffic	Upload	Transactions	Users	IP addresses	Last seen (UTC)
site-backup	Bucket	Amazon Web Services	70 KB	45 KB	95	11	7	May 14, 2019
general	Bucket	Google Cloud Platform	76 KB	49 KB	52	12	7	May 14, 2019
system2	Bucket	Google Cloud Platform	32 KB	21 KB	46	5	4	May 13, 2019
adatum	Bucket	Amazon Web Services	32 KB	20 KB	21	5	2	May 13, 2019
fabrikam company-files	Queue	Microsoft Azure	63 KB	41 KB	27	10	5	May 13, 2019
webapp	Bucket	Amazon Web Services	45 KB	29 KB	83	7	5	May 10, 2019
playground instance	File	Microsoft Azure	19 KB	12 KB	12	3	2	May 10, 2019
cohovineyard	Bucket	Google Cloud Platform	19 KB	12 KB	23	3	2	May 10, 2019
myteam	Bucket	Amazon Web Services	10 MB	4 MB	24	12	7	May 7, 2019
machines	Custom app	Google Cloud Platform	7 MB	3 MB	15	8	6	May 7, 2019
meetings	Bucket	Google Cloud Platform	7 MB	3 MB	9	9	6	May 6, 2019
storage	Bucket	Amazon Web Services	12 MB	5 MB	15	15	8	May 6, 2019

Shadow IT Discovery for IaaS and PaaS services

Discovered resources

Continuous report: Global
Timeframe: Last 30 days

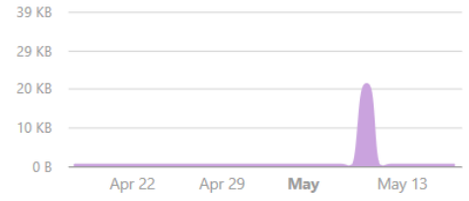
APP: Select apps...
RESOURCE NAME: Select...
RESOURCE TYPE: Select value...
Advanced

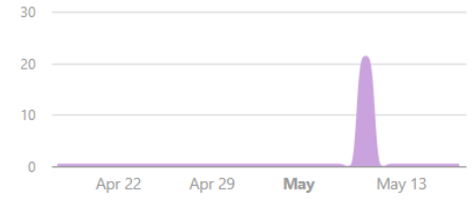
1 - 20 of 27 resources

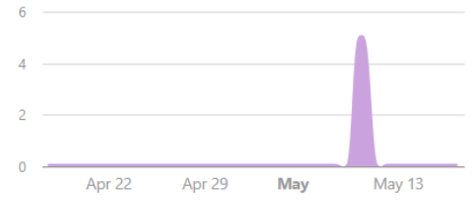
Resource	Resource type	App	Traffic	Upload	Transactions	Users	IP addresses	Last seen (UTC)
site-backup	Bucket	Amazon Web Services	70 KB	45 KB	95	11	7	May 14, 2019
general	Bucket	Google Cloud Platform	76 KB	49 KB	52	12	7	May 14, 2019
system2	Bucket	Google Cloud Platform	32 KB	21 KB	46	5	4	May 13, 2019
adatum	Bucket	Amazon Web Services	32 KB	20 KB	21	5	2	May 13, 2019
fabrikam company-files	Queue	Microsoft Azure	63 KB	41 KB	27	10	5	May 13, 2019
webapp	Bucket	Amazon Web Services	45 KB	29 KB	83	7	5	May 10, 2019
playground instance	File	Microsoft Azure	19 KB	12 KB	12	3	2	May 10, 2019
cohovineyard	Bucket	Google Cloud Platform	19 KB	12 KB	23	3	2	May 10, 2019

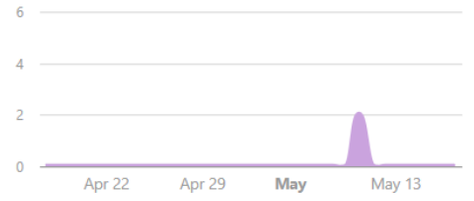
adatum
Amazon Web Services

User report
IP address report

TRAFFIC — Uploads


TRANSACTIONS


USERS


IP ADDRESSES


Shadow IT Discovery for IaaS and PaaS services: Drill down

Get started today: Shadow IT

1

Discover all cloud apps and services used in your organization

2

Govern discovered cloud apps and explore like solutions within your environment

3

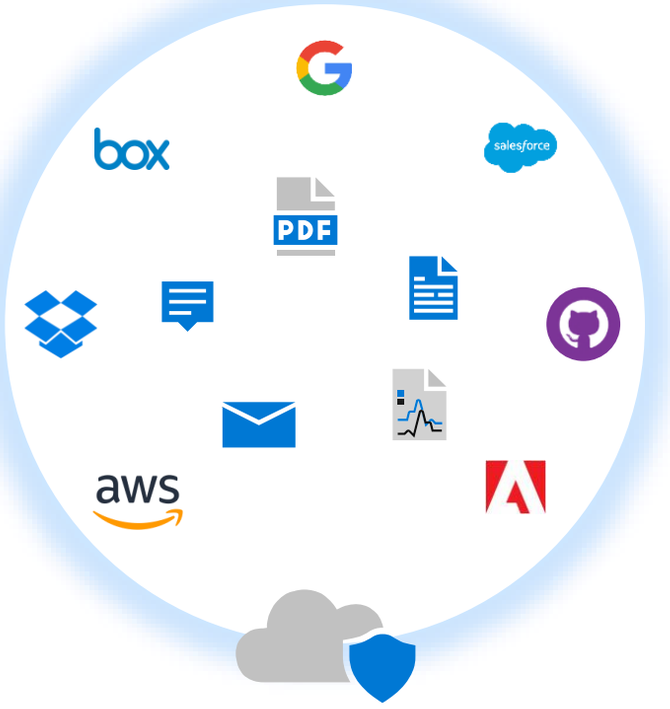
Assess the risk and compliance of all cloud apps

04

Information Protection

Information Protection

By leveraging information protection in Microsoft Cloud App Security, customers gain the power of Microsoft Information Protection applied to their environment holistically.



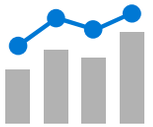
Microsoft Information Protection solutions

Protect your sensitive data—wherever it lives or travels

Discover

Classify

Protect



Monitor

Across

Devices

Apps

Cloud services

On-premises

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

Detect and remediate overexposed files and anomalies

Create policies to generate alerts and trigger automatic governance actions

Policy creation is simple via our templates, or you can create your own custom policies which generate alerts, trigger automatic governance over certain actions and notify via Power Automate integrated workflows

Be notified to identify and investigate policy violations and related activities

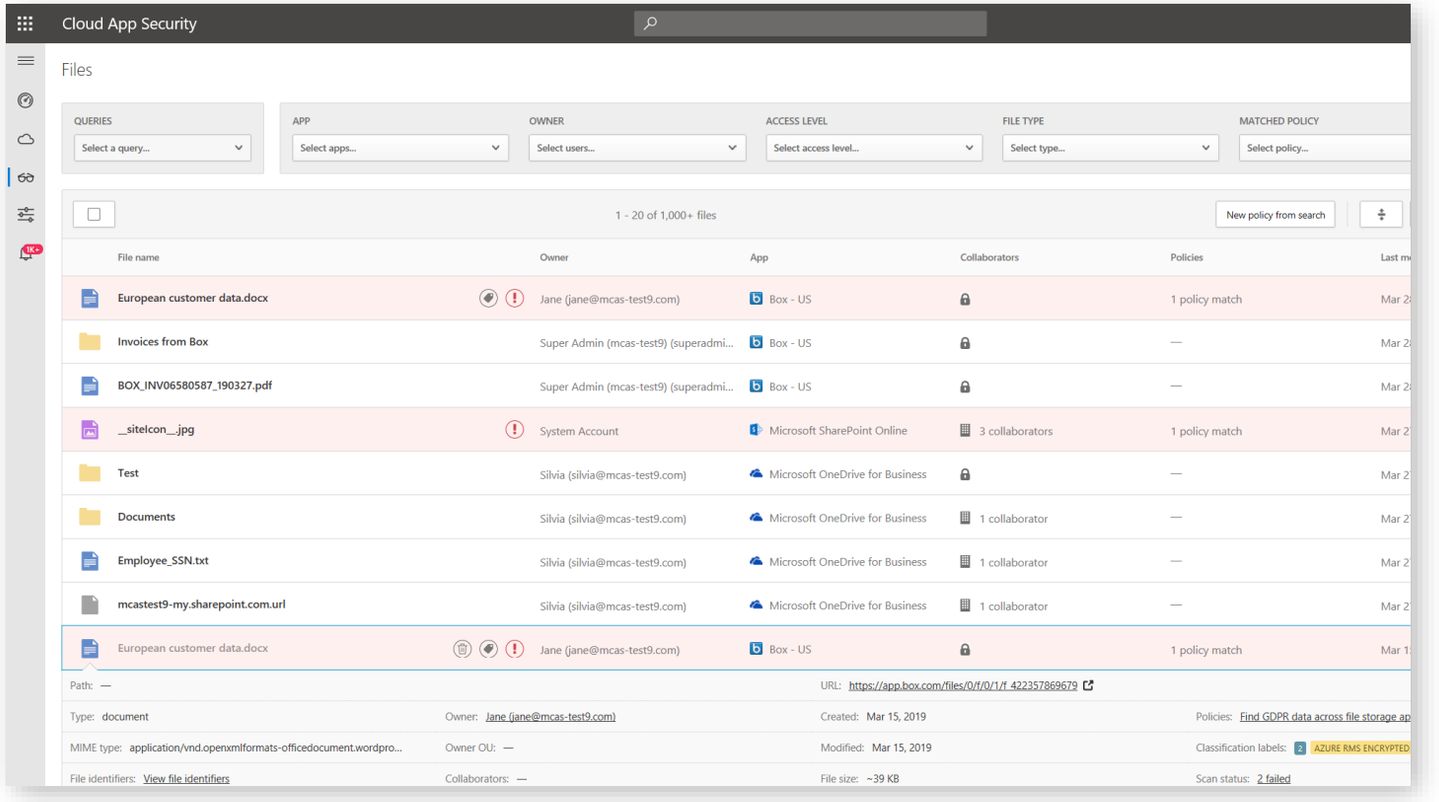
Notifications and investigations into violations of policy and any other activities are easy to sort, filter and compile to elevate your security teams' execution of security plans

Automatically remediate with built-in actions

Automatic remediation with Cloud App Security baseline actions or with additional granularity in Power Automate allow notify admin, quarantine, make private, authenticate and other key actions

Automatically label and protect existing sensitive information, and when new files are uploaded

Classify your sensitive data and then allow Cloud App Security to scale your protection through automatic labeling or other automatic remediation when new files when new files are uploaded to your environment



Key differentiators via Microsoft Information Protection approach

Unified labelling with Microsoft Information Protection
Leverage the powerful native integration of MIP with a streamlined experience across Office 365 Data Loss Prevention, Azure Information Protection and Cloud App Security

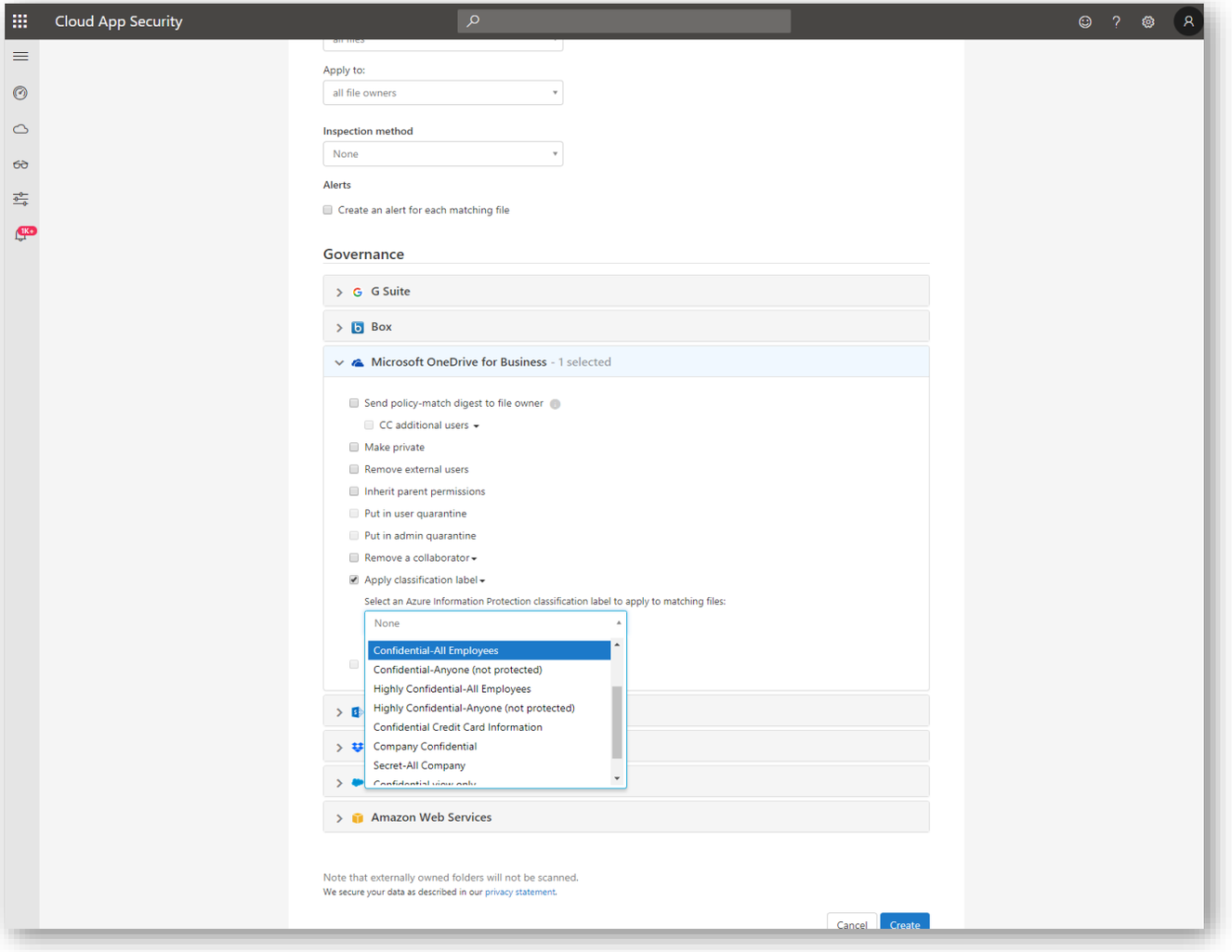
Over 150 built-in sensitive information types
Choose from 150+ built-in information types from credit card data, to data that triggers regulatory constraints such as GDPR or HIPAA

Custom sensitive information types using Regex, keywords and large dictionary
Ensure compliance and company policies are adhered to by further customizing your Cloud App Security information types

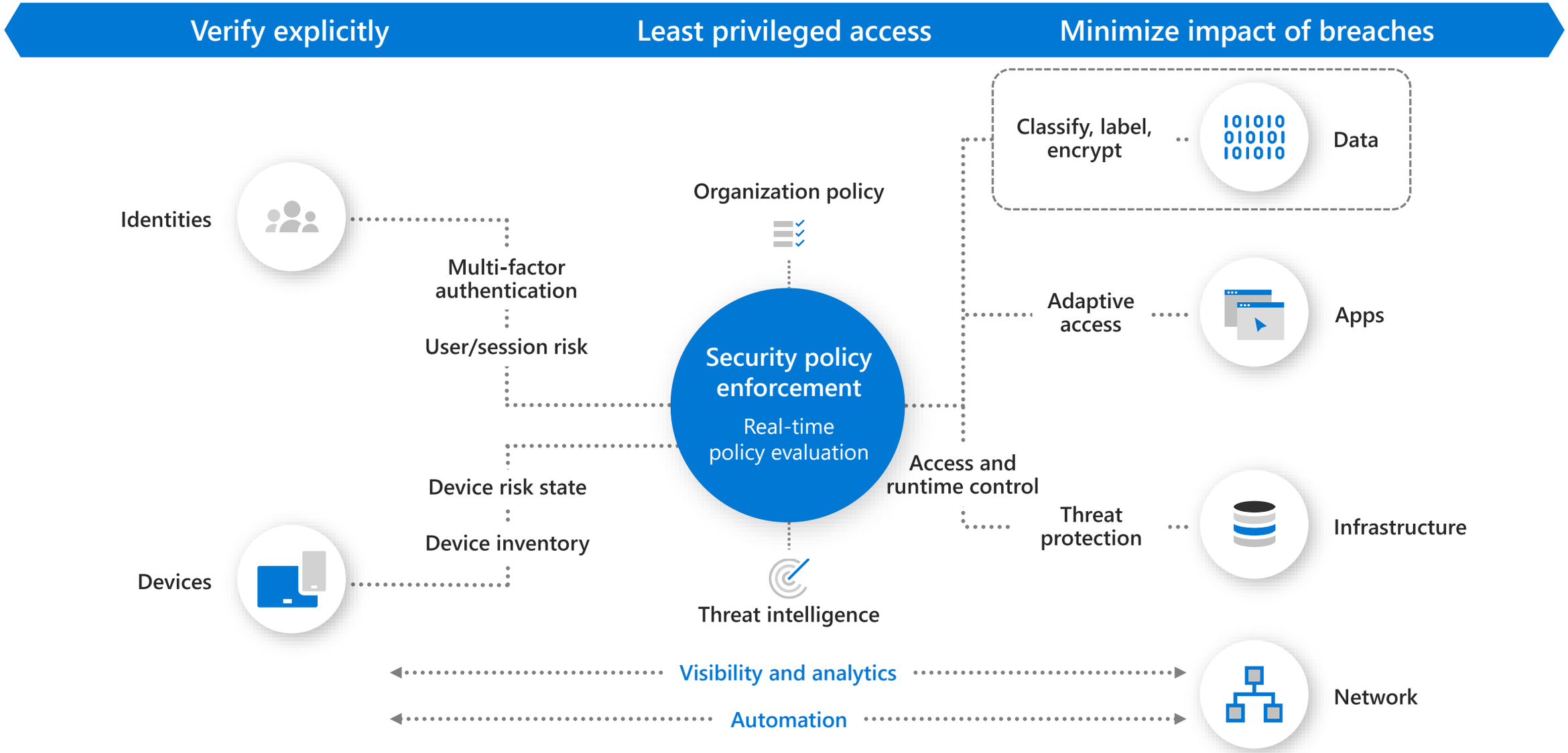
Custom and built-in classifiers as EDM, fingerprint, and trainable classifiers
Powerful machine learning classifiers are put to work to help your Cloud App Security instance classify sensitive data types outside of the typical file types and data sources

Leverage any DLP engine for classification
Use your choice of data loss prevention engine to train your Cloud App Security instance or amplify your connections to Office DLP engines in addition to your custom set of classifications

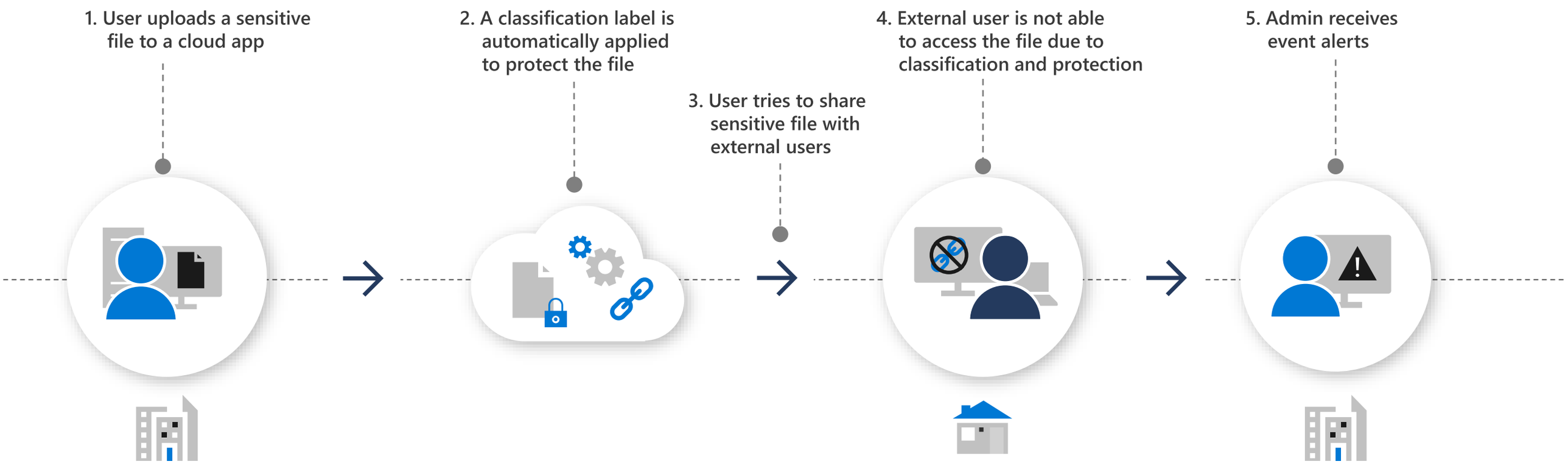
Leverage AIP labels
Azure Information Protection labels work hard to provide simple and straightforward labels for your data so all your employees and admins know how to appropriately leverage your sensitive data

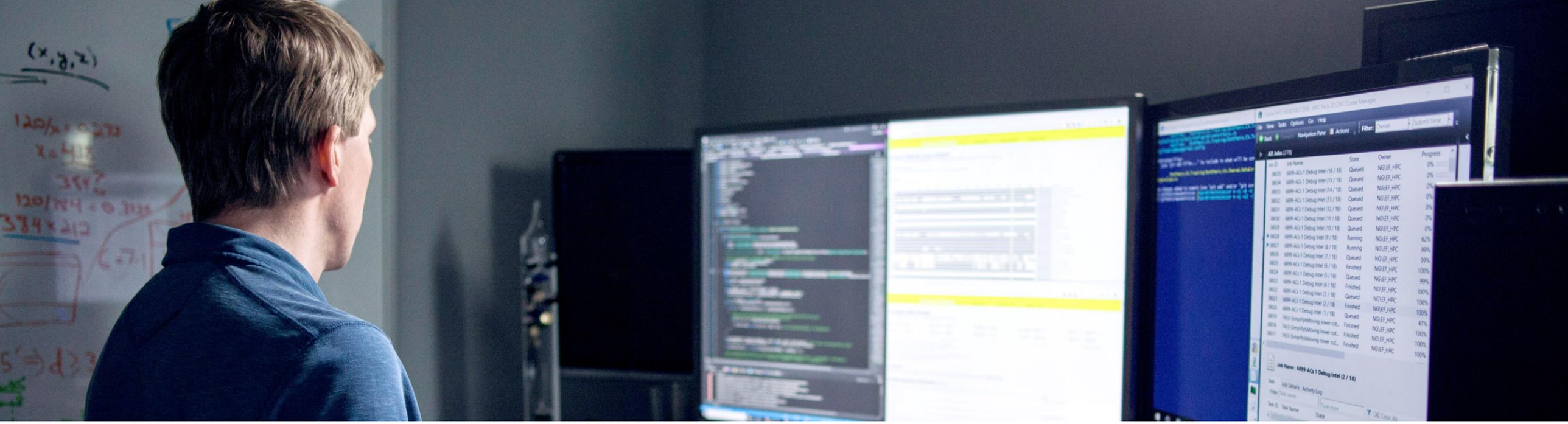


Information Protection incorporates Zero Trust principles



Lifecycle of protecting sensitive files in the cloud





Get started today: Information Protection

1

Enforce a corporate information classification strategy

2

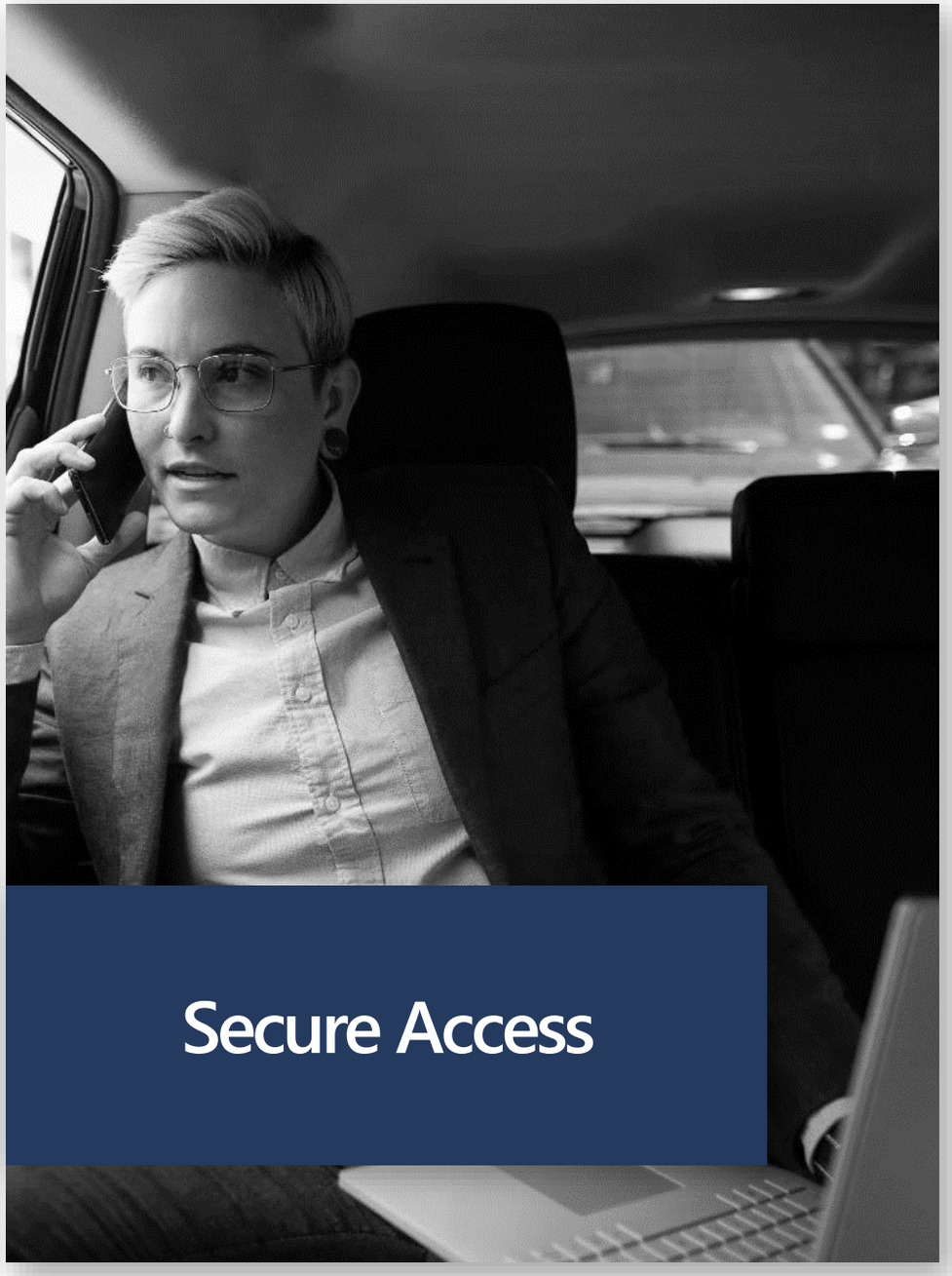
Create and enforce policies that require end-user classification

3

Deploy a “warn and educate” experience for your user population

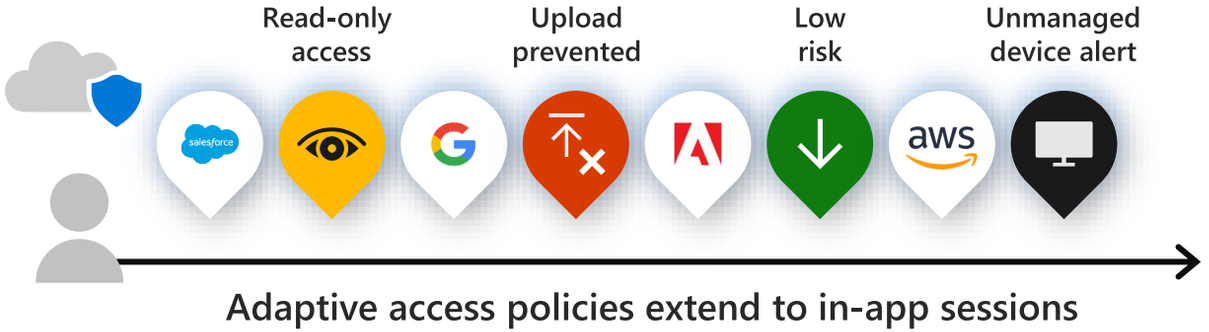
05

Secure Access

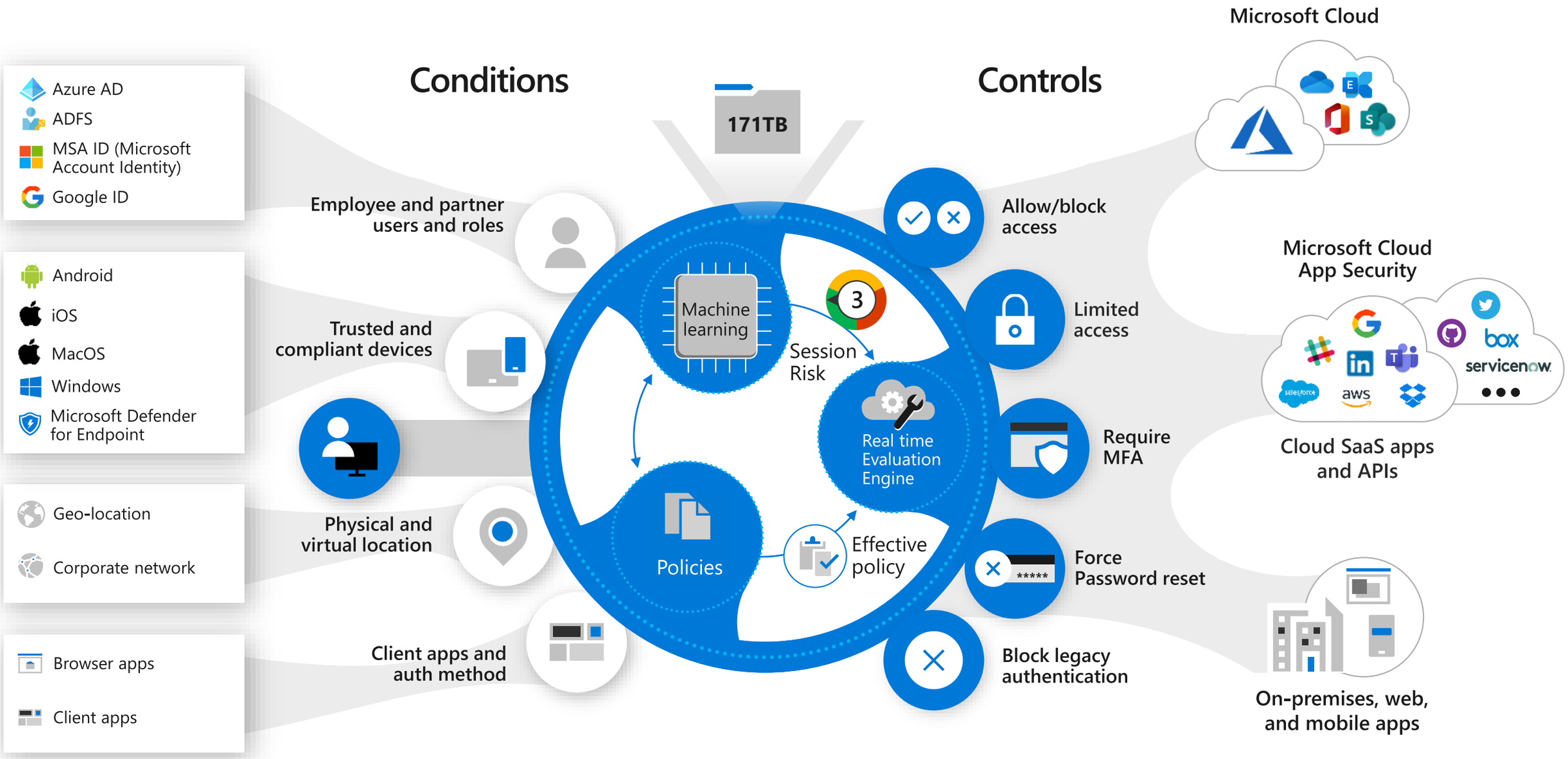


Secure Access

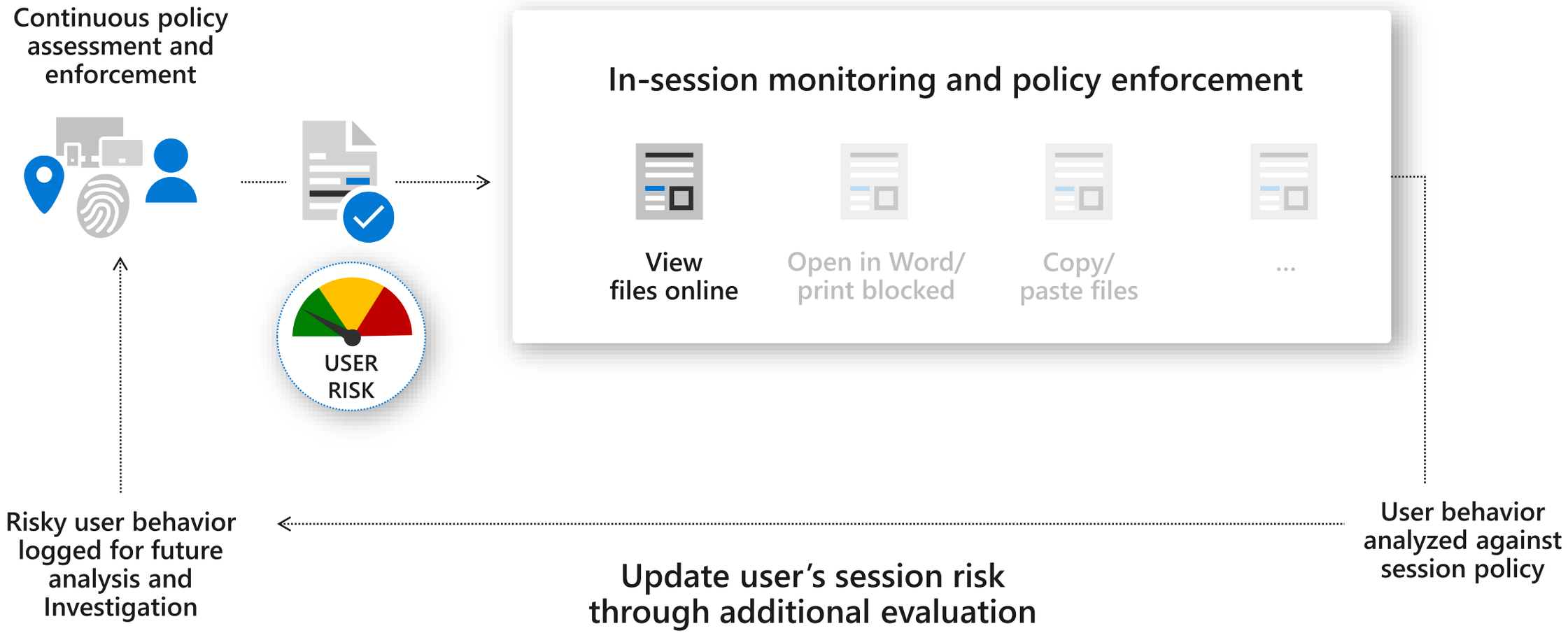
Integrating Microsoft Cloud App Security with your identity provider enables real-time enforcement of in-session actions.



Secure Access in real-time



Extend policy enforcement into the session



Real-time in-session App Control

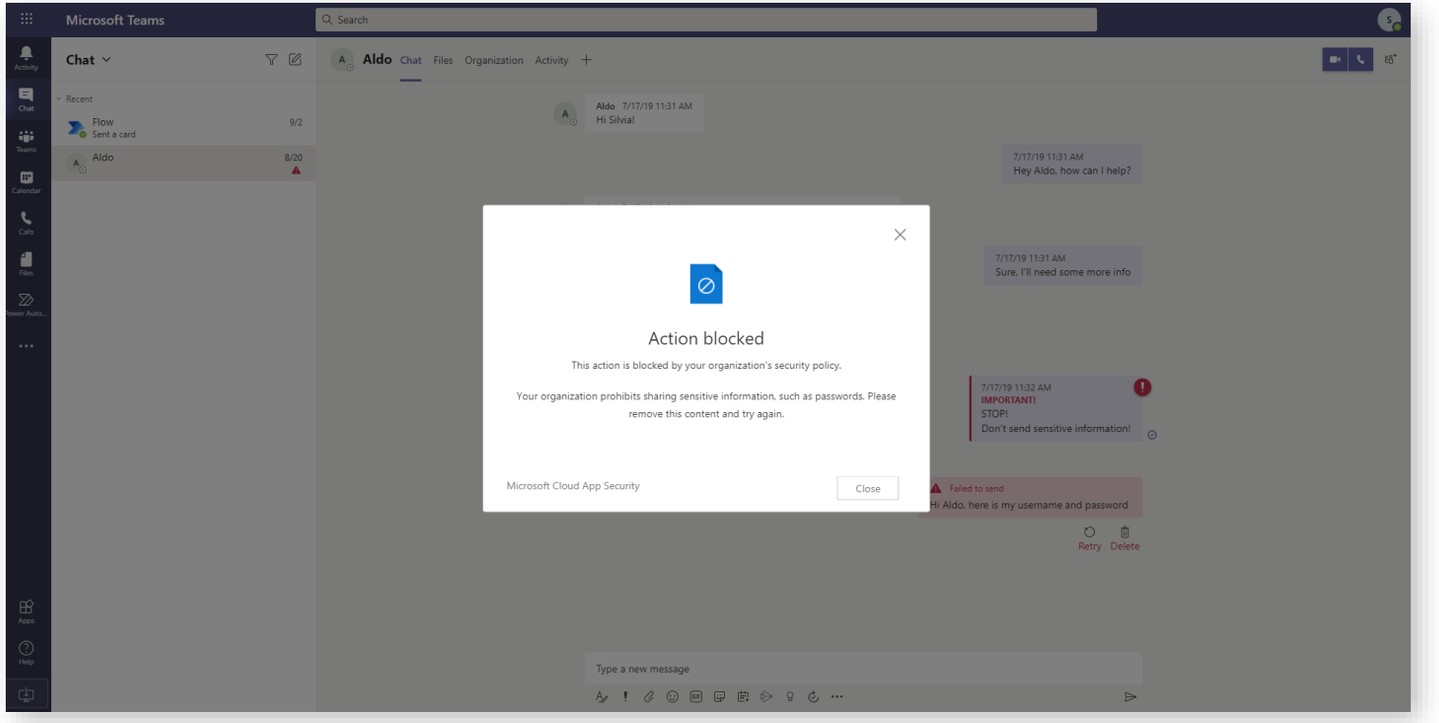
Context-aware session policies
Control access to cloud apps and sensitive data within those apps based on user, location, device, and the status of the application within the environment

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



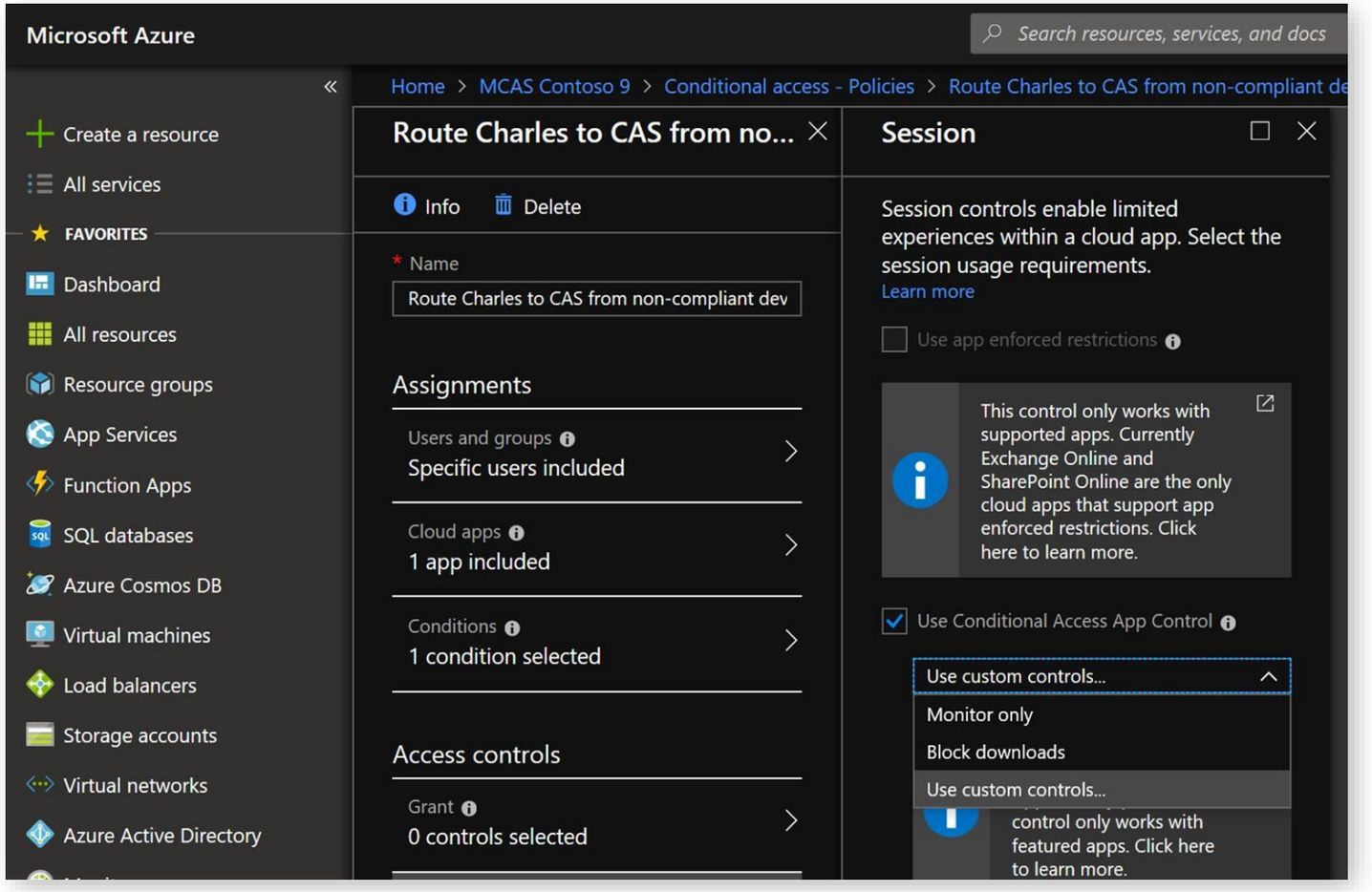
Key differentiators to optimize the admin and end user experience

Unique integration with Azure AD Conditional Access
Selective routing to Cloud App Security 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
Leverage the same powerful real-time controls for your on-prem apps by integrating them with Azure AD Application Proxy

Worldwide Azure datacenters infrastructure
Cloud App Security leverages Azure data centers across the world to optimize performance and user experience



Get started today: Secure Access

1

Gain visibility into corporate data stored in the cloud

2

Enforce DLP and compliance policies for sensitive data stored in your cloud apps

3

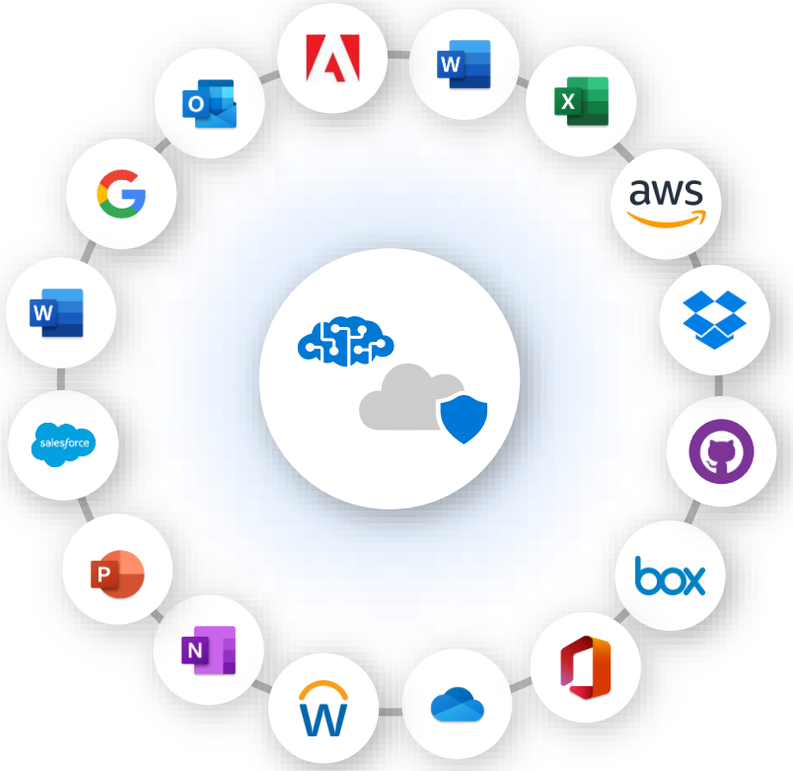
Ensure safe collaboration and data sharing practices in the cloud

06

Threat Protection for your cloud environment

Threat Protection

The integrated threat protection in Cloud App Security enables customers to detect advanced attackers and native cloud threats by detecting anomalous behavior and malicious activity in their cloud environment.



The challenge of securing your environment

Bad actors are using increasingly creative and sophisticated attacks

The digital estate offers a very broad surface area that is difficult to secure

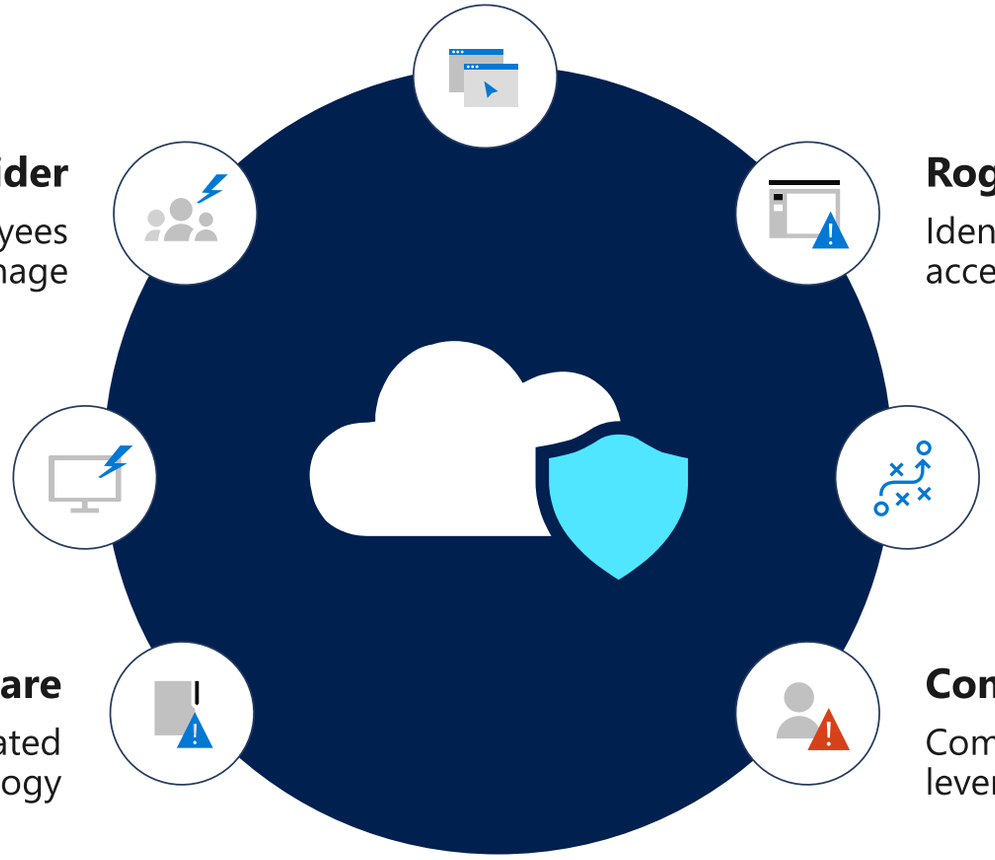
Identifying malicious behavior by intelligent correlation of signals is difficult, time-consuming, and expensive

Alongside our industry partners and the security community, Microsoft continues to investigate the extent of the recent nation-state attack on SolarWinds. As new information becomes available, we will make updates at https://aka.ms/solorigate

Protection against cloud threats

OAuth apps

OAuth Protection: Detect, Alert on and Revoke access to Malicious OAuth applications



Malicious Insider

Protect against disgruntled employees before they cause damage

Malware

Detect and detonate malware in cloud apps as soon as it's uploaded

Ransomware

Identify ransomware using sophisticated behavioral analytics technology

Rogue Application

Identify rogue applications that access your data

Data exfiltration

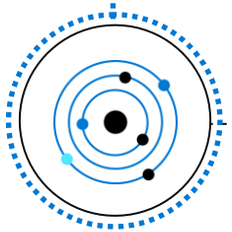
Detect unusual flow of data outside of your organization

Compromised Accounts

Combat advanced attackers that leverage compromised user credentials

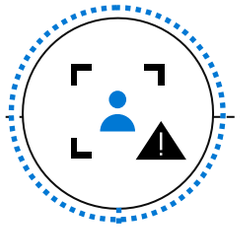
Detections across cloud apps

- Malware implanted in cloud apps
- Malicious OAuth application
- Multiple failed login attempts to app
- Suspicious inbox rules (delete, forward)
- Unusual addition of credentials to an OAuth app



Threat delivery and persistence

Indicators of a compromised session



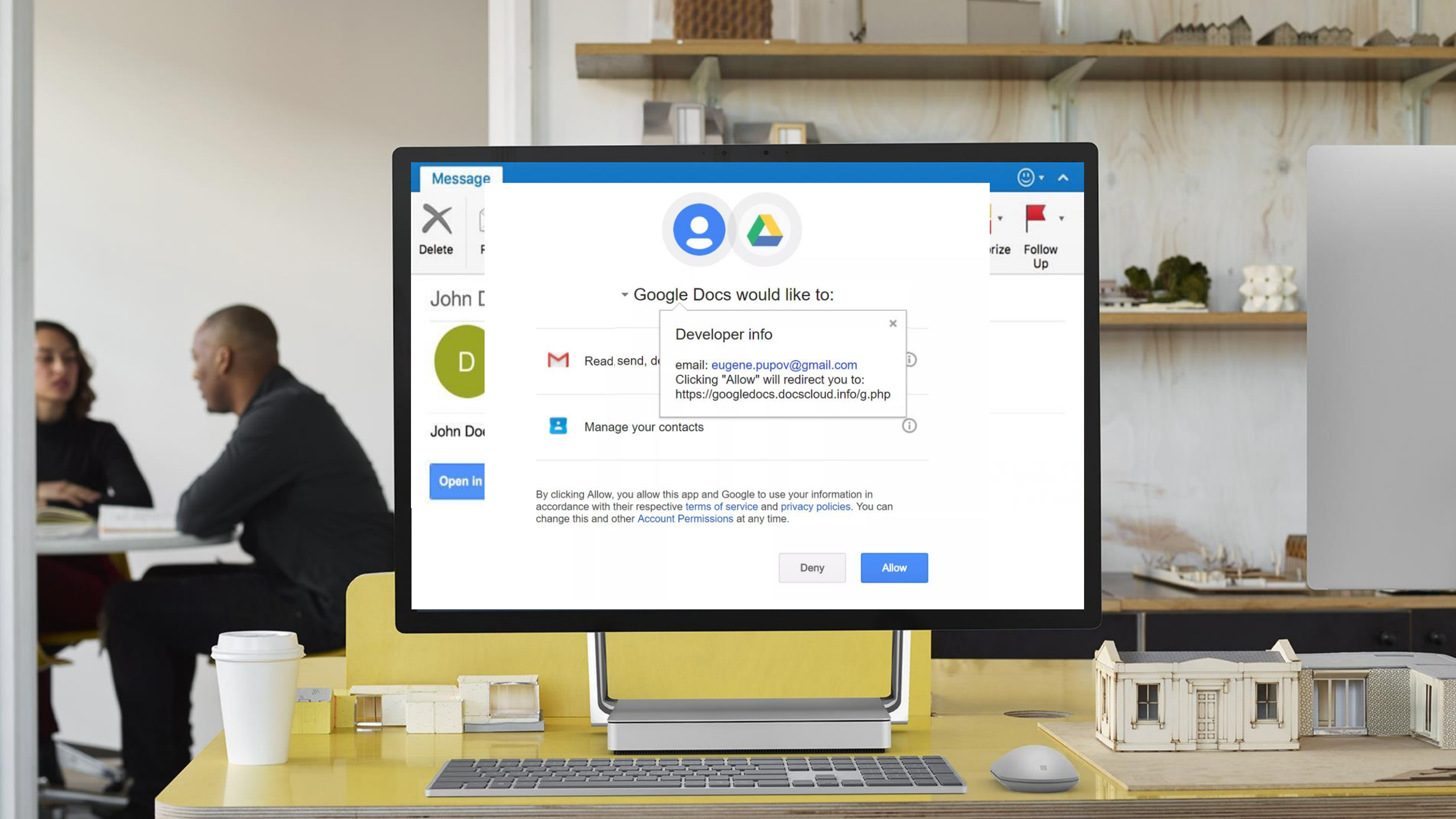
- Activity from suspicious IP addresses
- Activity from anonymous IP addresses
- Activity from an infrequent country
- Impossible travel between sessions
- Logon attempt from a suspicious user agent

- Unusual file share activity
- Unusual file download
- Unusual file deletion activity
- Ransomware activity
- Data exfiltration to unsanctioned apps
- Activity by a terminated employee
- Mail forwarding rules

Malicious use of an end-user account

Malicious use of a privileged user

- Unusual impersonated activity
- Unusual administrative activity
- Unusual multiple delete VM activity


Message
Delete
Follow Up
John D
D
John Doc
Open in
Google Docs would like to:
Developer info
email: eugene.pupov@gmail.com
Clicking "Allow" will redirect you to:
https://googledocs.docscloud.info/g.php
Read, send, de
Manage your contacts
By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.
Deny
Allow

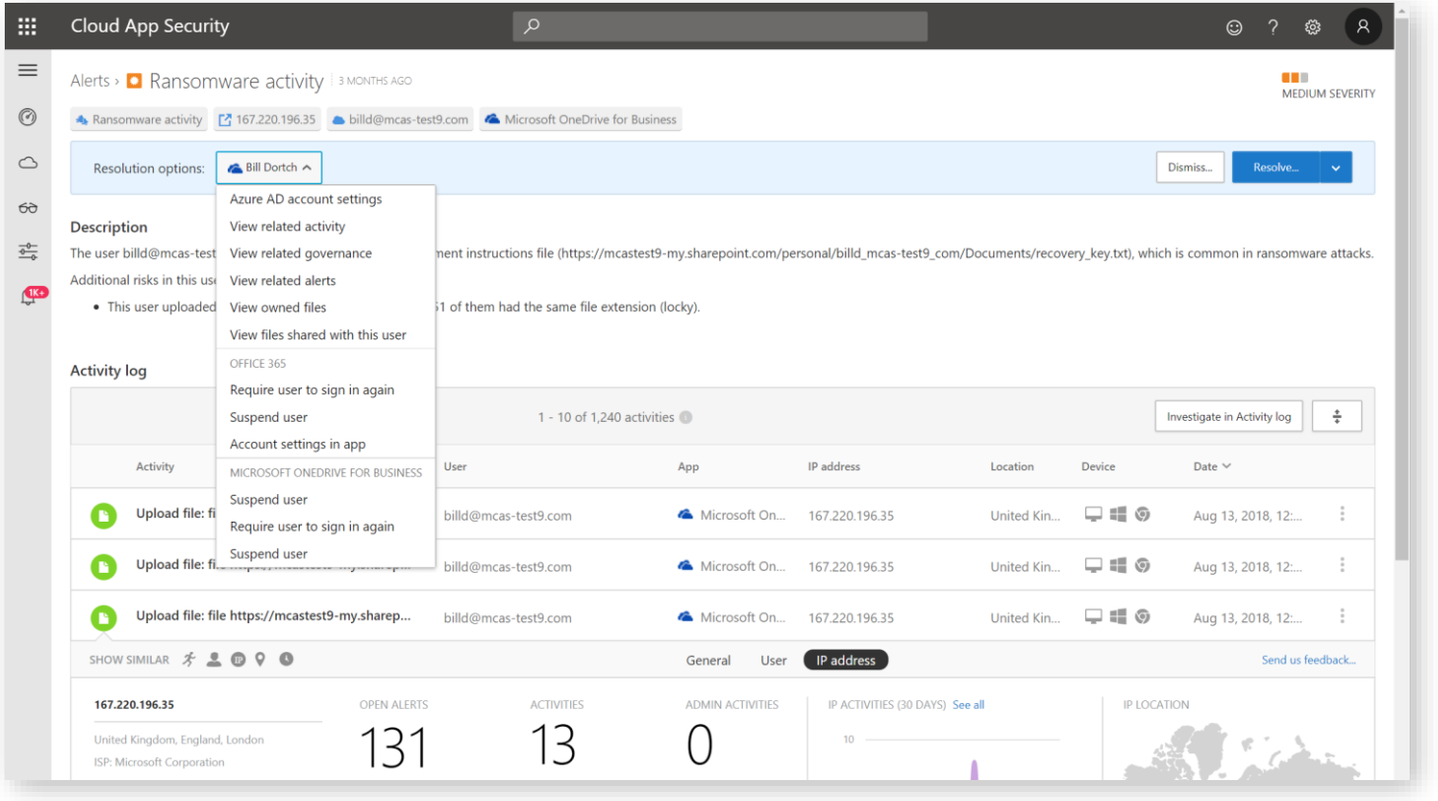
Key threat alerts and mitigation actions

Identify high-risk and anomalous usage
Ensure visibility to any anomalous activities where a high-risk app or session has been identified

Exfiltration of data to unsanctioned apps
Be alerted when your users attempt to exfiltrate data to applications that have been “unsanctioned” in your environment

Rogue 3rd party application alerts, mitigate ransomware attacks
Any application being accessed in your environment which falls into the parameters that Microsoft has determined as rogue or malicious will be alerted on

Suspend user sessions and revoke OAuth app access
Admin can auto-suspend, or be prompted to suspend user sessions or revoke OAuth token in order to mitigate risk



Comprehensive Threat Protection for your cloud apps

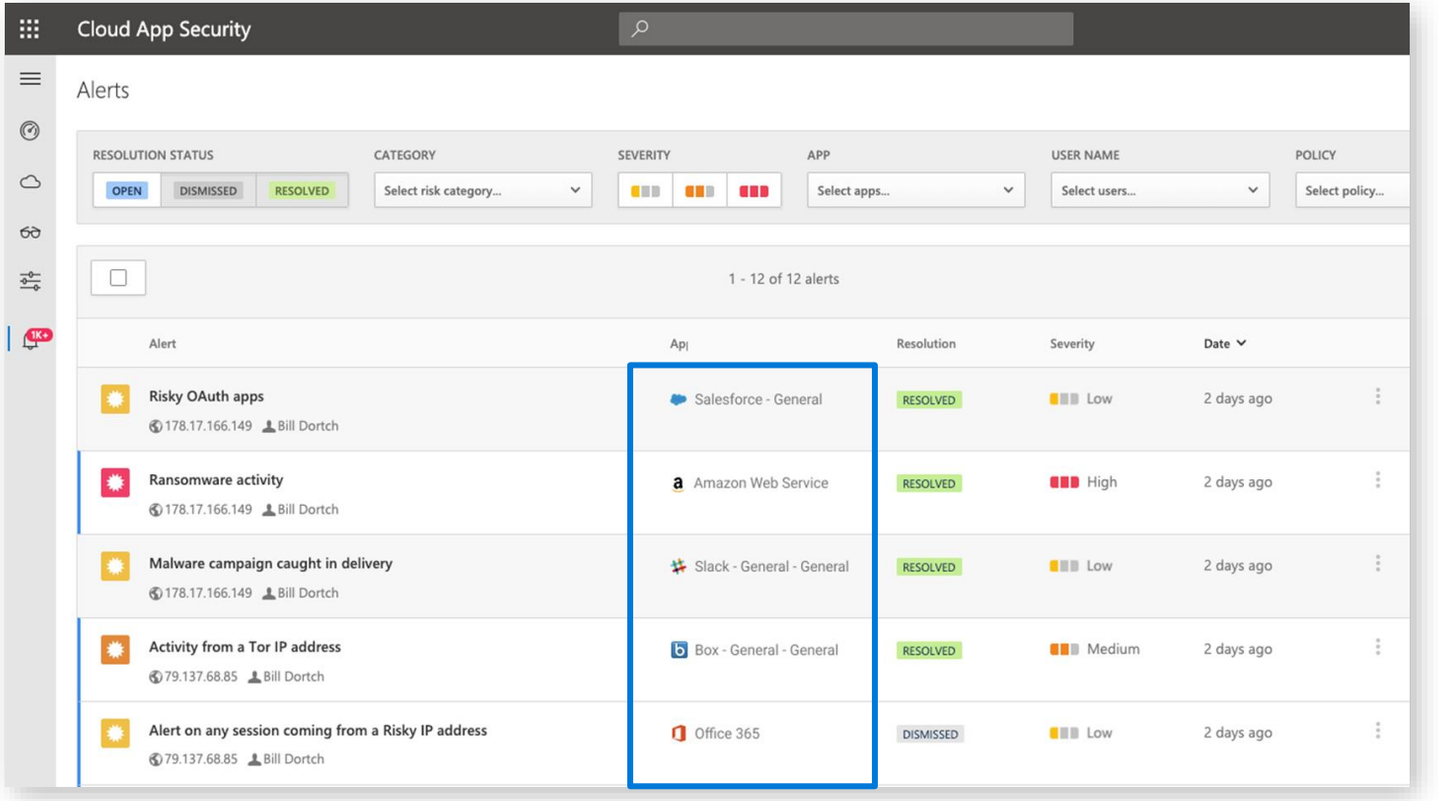
Built-in Threat Protection policies
More than 20 out-of-the-box policies and growing. Policies alert you on some of the most common cloud threats such as impossible travel, impersonation activities or ransomware detection

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]



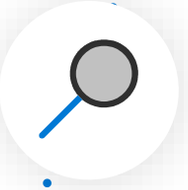
1. Gartner, Magic Quadrant for Cloud Access Security Brokers 2020

Protect organization identities and leverage unified investigation across on-premises and cloud activities

Microsoft Cloud App Security

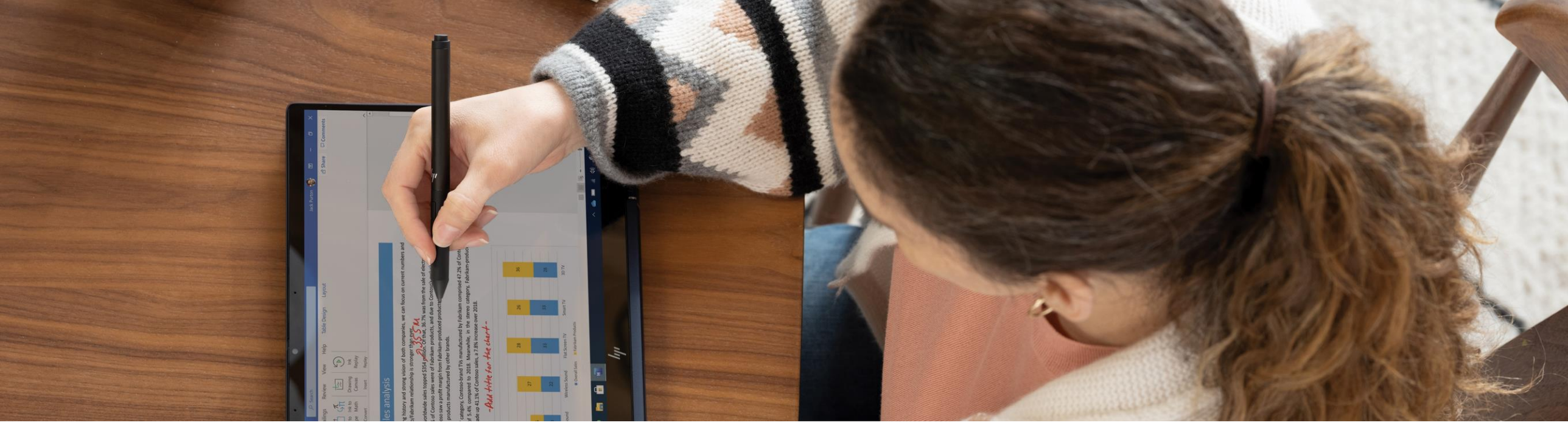
Microsoft Defender for Identity

Azure AD Identity Protection



Unified SecOps experience to investigate identity activities across on-prem and cloud

Investigation priority - based on User and Entity Behavior Analytics



Get started today: Threat Protection

1

Identify compromised user accounts

2

Record an audit trail for all user and privileged account activities across hybrid environments

3

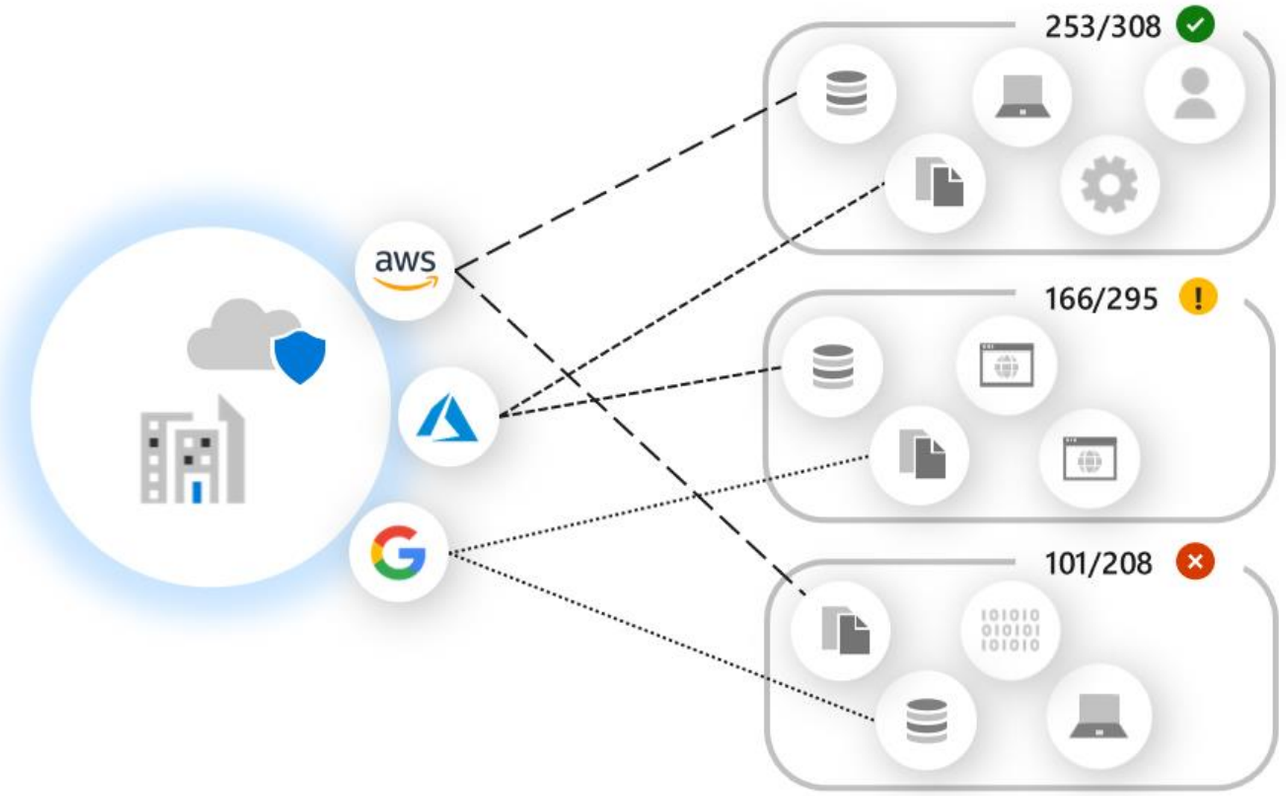
Detect and remediate malware in your cloud apps

07

Cloud Security Posture Management

Cloud Platform Security

Cloud platform security prioritizes the risks and makes recommendations for improvement against your pre-selected goals.



CASB for cloud platforms

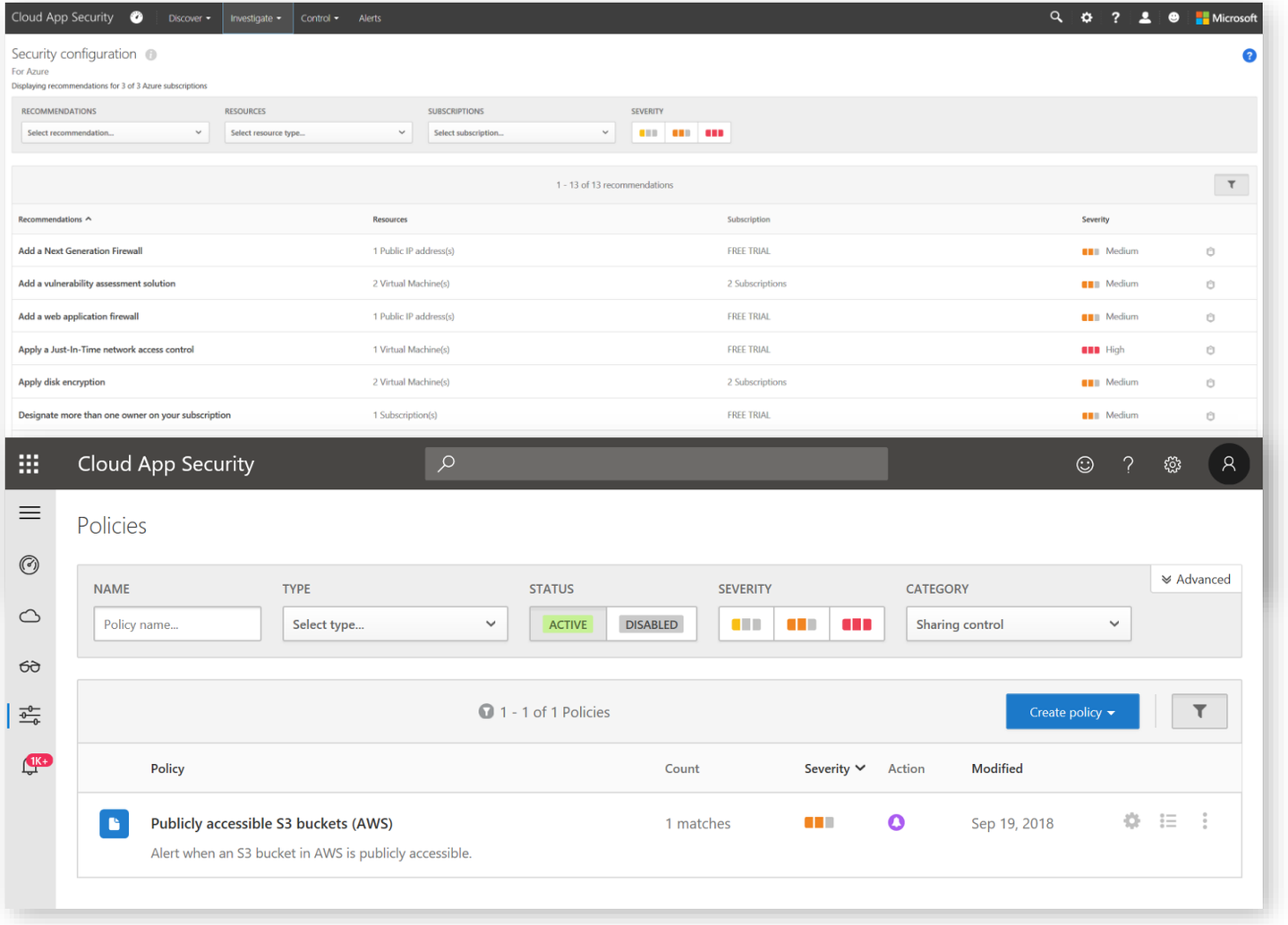
Detection and investigation of anomalous admin behavior
Identify anomalies in your cloud environment via advanced behavioral analytics

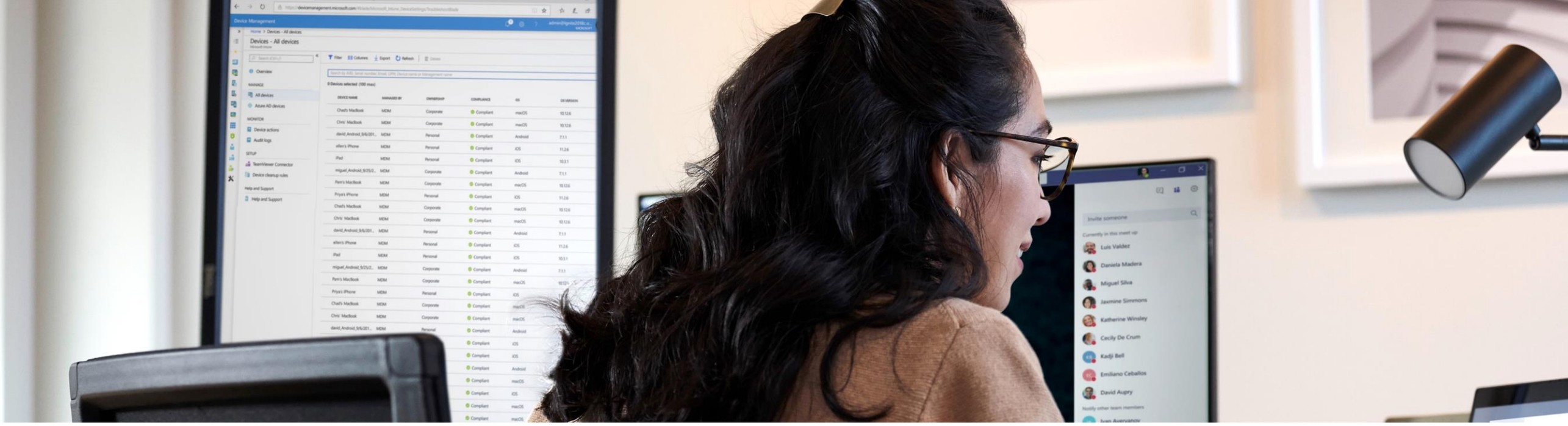
Pivot on users, IP addresses, resources, activities and locations

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

Unique integration with Azure Security Center
Pivot to Azure Security Center 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





Get started today: Cloud Security Posture Management

1

Decide which elements are key and unilateral according to your core priorities for security posture management

2

Leverage the recommendations from your multi-cloud platforms to create a unified and secure environment

3

Regularly check the platform alerts for maintenance of your intended security posture

08

Enterprise integrations

Benefits of enterprise integrations

Export alerts and activities to your SIEM
Better protect your cloud applications while maintaining your usual security workflow, automating security procedures and correlating between cloud-based and on-premises events

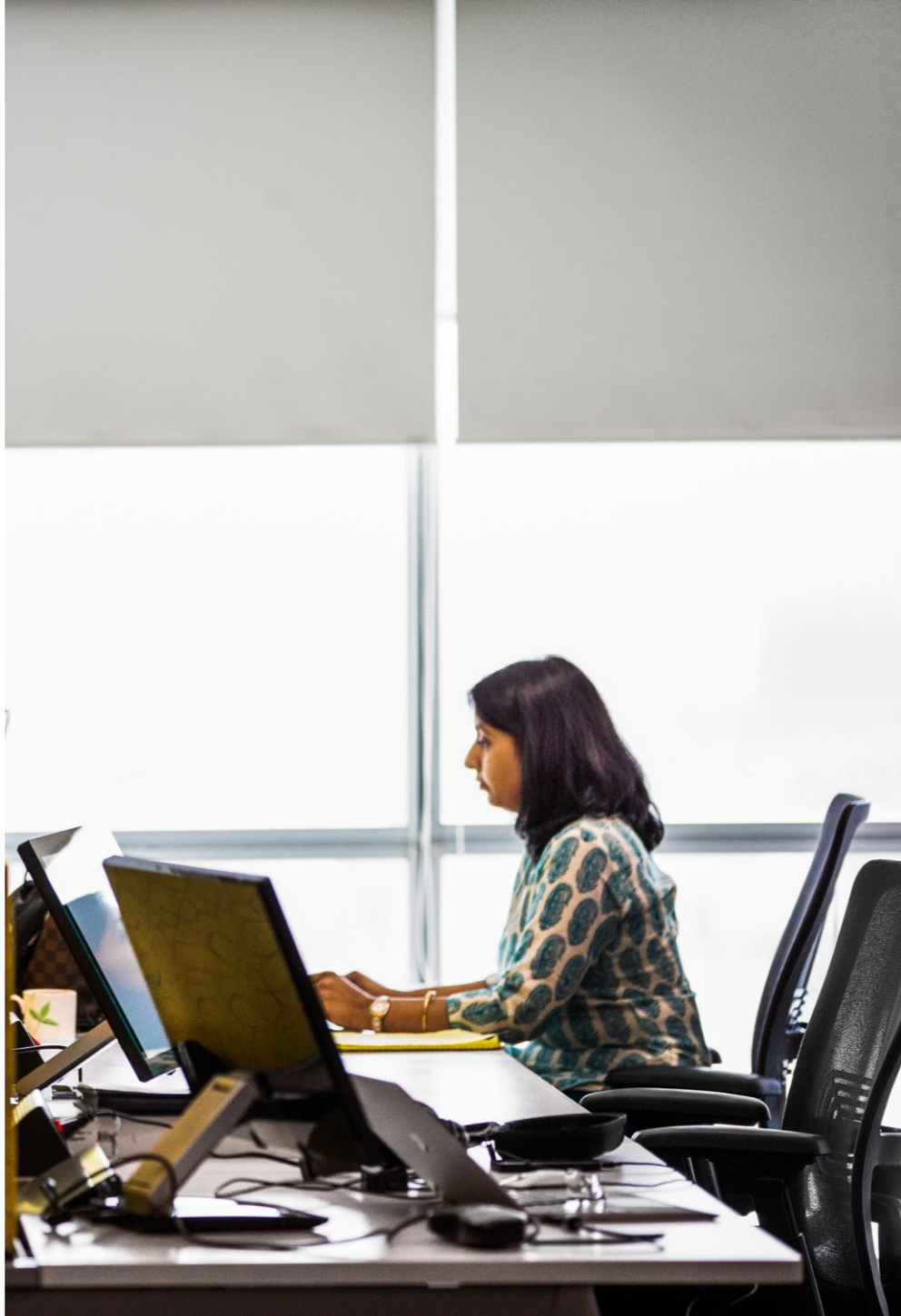
Automate processes via API or PowerShell
Create your own applications using programmatic access to Cloud App Security data and actions through REST API endpoints

Protect your sensitive data with Microsoft Information Protection
Bring awareness and visibility to your organization's sensitive data by leveraging Microsoft Information Protection integrated with Cloud App Security to provide labeling and safeguarding for your organization's information

Leverage your current DLP solution
Integrate with Security and Compliance Center to create and manage DLP policies across all cloud apps

Security Workflow automation with Power Automate
Centralized alert automation and orchestration of custom workflows using the ecosystem of connectors in Microsoft Power Automate. Enables routing alerts to ticketing systems (e.g. ServiceNow), gather end user input for alert investigation, get approval from SOC operator to execute action or apply additional security controls.

Secure your SecOps with Azure Sentinel and Microsoft Defender XDR
Elevate your security operations with Azure Sentinel and Microsoft Defender products (Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity)



09

Automating security workflows

Automating security workflows with Power Automate

Centralized alert automation and orchestration of custom workflows

Power Automate allows for deeply integrated orchestration of alerts from Cloud App Security

Automate the triage of alerts

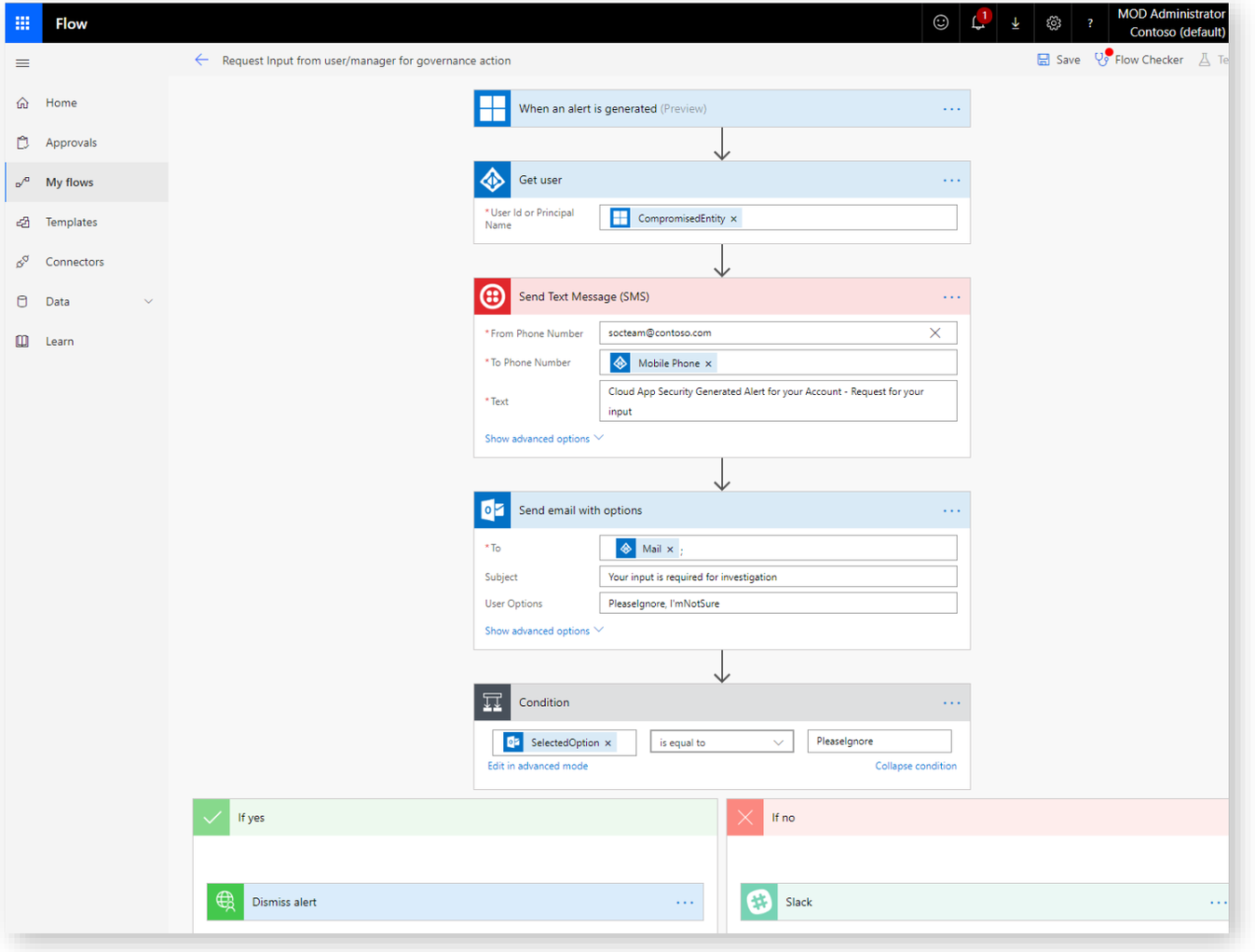
Triage your alerts into correct support queues, eliminating extra noise for your security and compliance teams

Enables an ecosystem of connectors in Power Automate including more than 100 connectors

Add more power to your triaging experience through connectors to apps such as Jira, ServiceNow, and DocuSign

Out-of-the-box and custom workflow playbooks that work with the systems of your choice

Playbooks enable your security and compliance teams to formulate repeatable actions to take when incidents occur, making your team more efficient



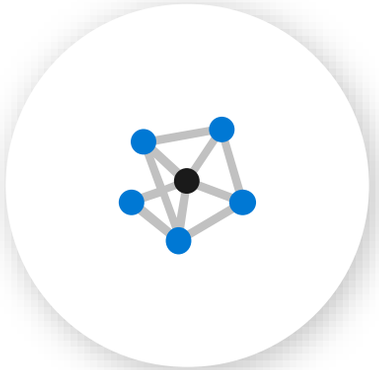
Sample automation scenarios

1. Route alerts to ticketing systems such as Jira or ServiceNow
2. Route alerts to different SOC teams based on geography of the user
3. Request input from a user's manager to triage alert
4. Request user input to decide how to triage an alert
5. Block unsanctioned apps on the firewall using CAS discovery alerts
6. Get admin approval to execute remediation action
7. Disable user in AAD and in on-prem Active Directory based on suspicious alerts
8. Remove malicious forwarding inbox rule in Exchange Online
9. Automatically dismiss “unusual location” alerts when a user has OOF message set to “On”
10. Cloud App Security alert triggers antivirus scan in Microsoft Defender for Endpoint

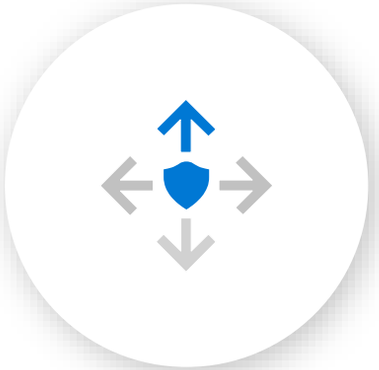
10

Summary and next steps

Investment areas

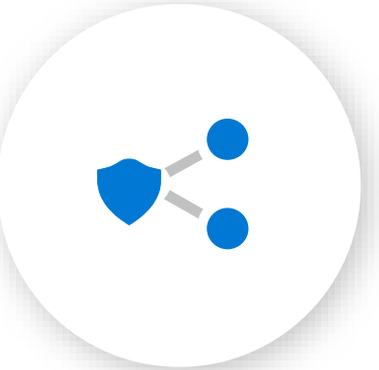


Build unique, native integrations with Microsoft's Security and Identity solutions



Protection for IaaS and PaaS, expanding our existing security posture management capabilities

Supporting any app anywhere with corporate identities



SecOps experience across Microsoft 365 Defender

Top 10 CASB use cases you should think about

1. Discover the cloud apps and services used in your organization
2. Assess the risk and compliance of all cloud apps
3. Govern access to discovered cloud apps and explore enterprise-ready alternatives
4. Discover OAuth apps with access to your environment
5. Gain visibility into all corporate data stored in the cloud apps and understand your exposure
6. Enforce DLP and compliance policies for sensitive data stored in your cloud apps
7. Protect data downloaded to unmanaged devices
8. Detect compromised user and admin accounts, and identify insider threats
9. Detect and remediate malware in your cloud apps
10. Audit the configuration of your IaaS environments

Next steps

1. Sign up for a Microsoft Cloud App Security Trial

2. Upload a log file from your network firewall or enable logging via Microsoft Defender for Endpoint to discover Shadow IT in your network and assess the risks of detected cloud apps

3. Connect your Cloud Apps to Microsoft Cloud App Security to detect suspicious user activity and exposed sensitive data

4. Enable out-of-the-box anomaly detection policies and start detecting cloud threats in your environment

5. Continue with more advanced use cases across Information Protection, Compliance and more

Resources

Visit our website:
aka.ms/MCAS

Join the conversation on Tech Community:
aka.ms/MCASCommunity

Stay up to date and subscribe to our blog:
aka.ms/MCASBlogPosts

Search documentation on Microsoft Cloud App Security:
aka.ms/MCASTech

Get started with a free trial:
aka.ms/MCASTrial

Understand your licensing options:
aka.ms/MCASLicensing

Q&A

Microsoft Security

Thank you.