

БИТВА ЗА ДОМЕН

PROTECT

DETECT

RESPOND

Microsoft Cloud App Security

Дмитрий Узлов

Компания «ТЕХНОПОЛИС»

Cloud services require a new approach to security



now



>1,000

different cloud services
are used by the
average enterprise



28%

increase in cloud and
SaaS threats over the last
year alone*



73

Data records are stolen
every second

box



12%

of IT teams understand
how GDPR will affect
their cloud services**



Cloud Access Security Brokers

CASBs are defined by Gartner as:

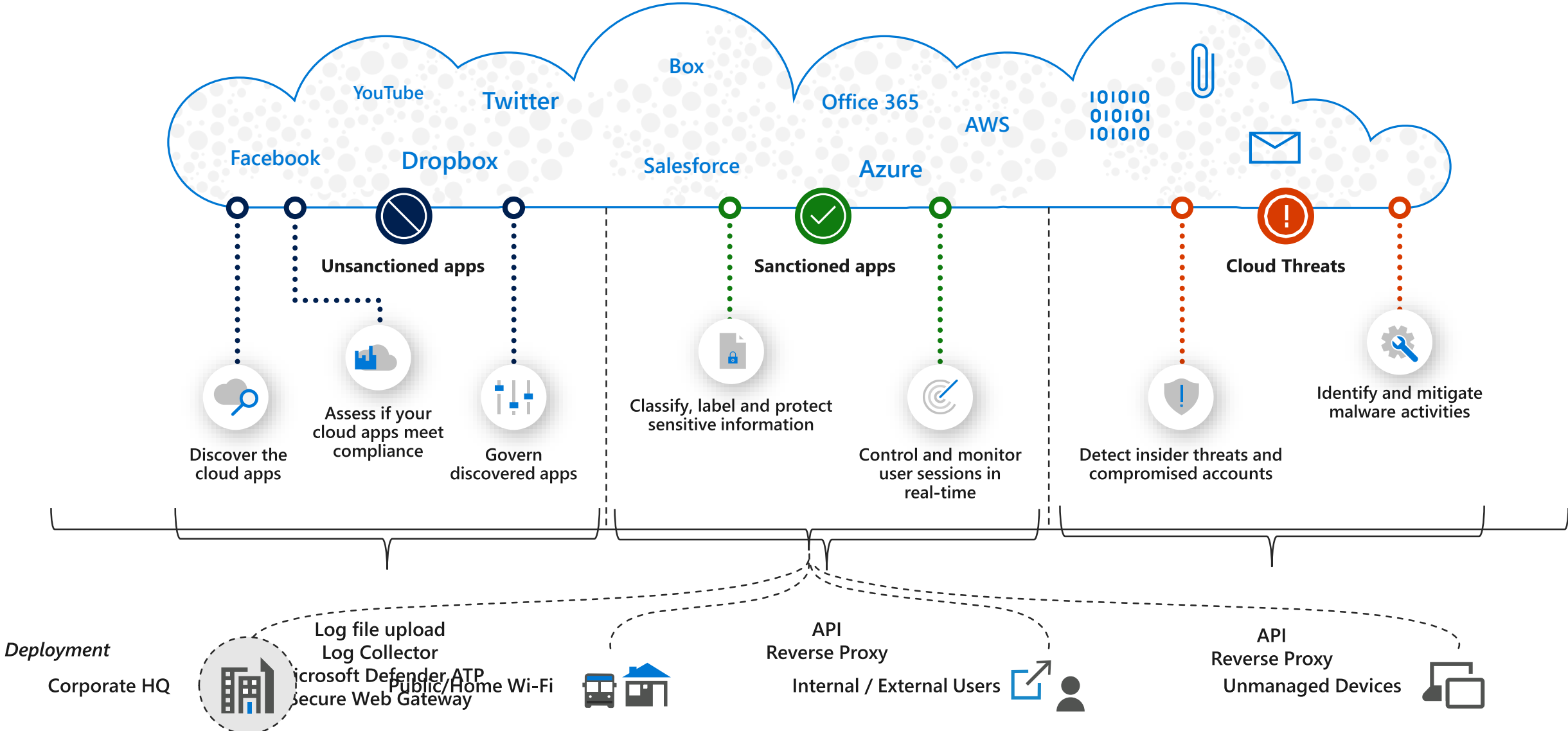
On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement.

- Top 10 Security projects for companies in 2019
- Microsoft has the largest market share with >30%**

By
2020
85%

of large enterprises
will use CASBs*

Top CASB use cases



Microsoft Cloud App Security in the marketplace

Featured Apps



Office 365



Microsoft Teams



Featured Customers

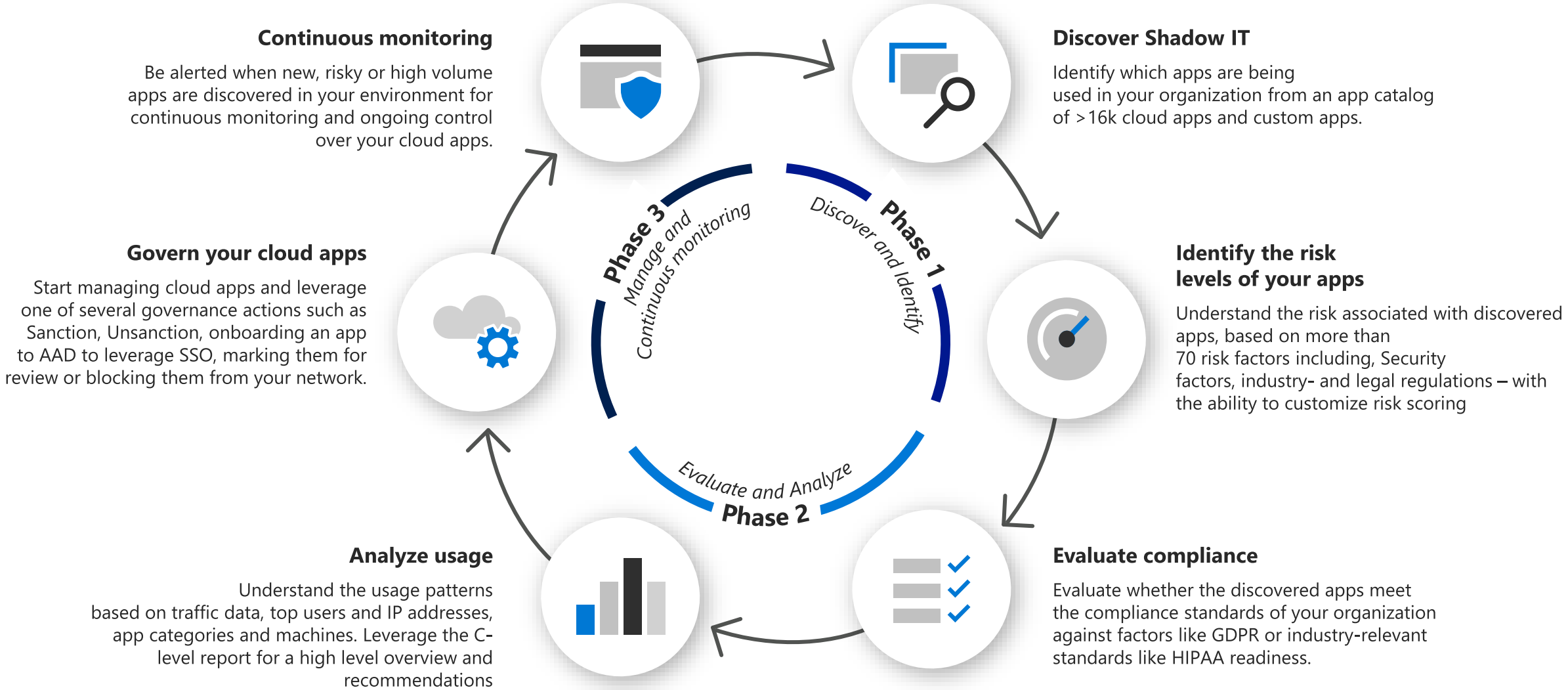


MEDITERRANEAN SHIPPING COMPANY



Shadow IT management lifecycle

Safely adopting cloud apps



Cloud App Discovery

Discovery of Shadow IT across SaaS, IaaS and PaaS

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

Understand the risk of your SaaS apps

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

Analyze usage patterns

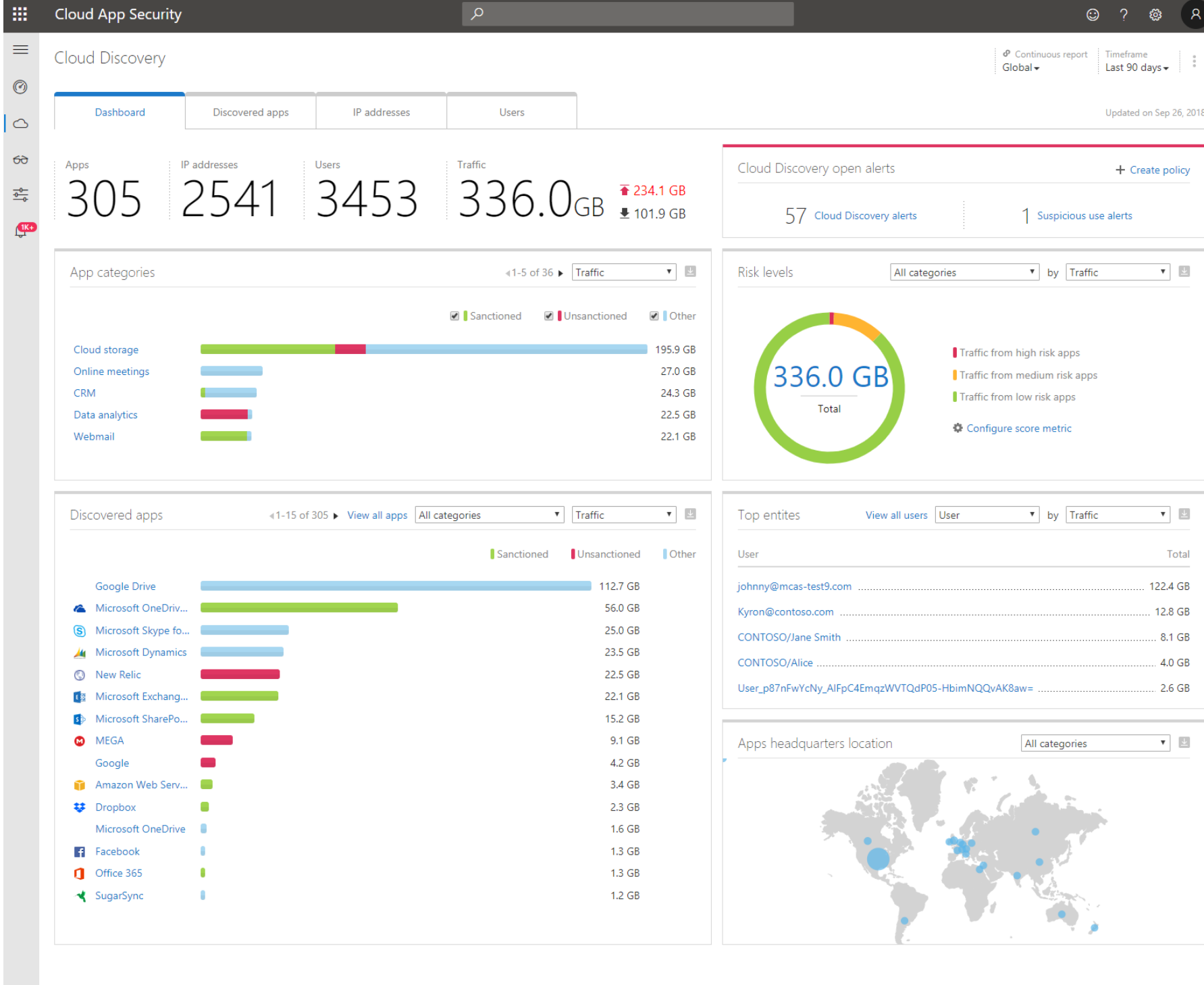
Understand the usage patterns and identify high risk volume users by understanding traffic data, top users and IP addresses, app categories

Block risky and unsanctioned apps

Using native and programmatic integration with leading SWG and Proxies

Continuous monitoring

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



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

The screenshot displays the 'Cloud App Security' dashboard. The 'Discovered apps' tab is active, showing a list of cloud storage applications. A blue box highlights the 'Machines' column in the table, and another blue box highlights the 'Continuous report Win10 Endpoint Users' dropdown menu in the top right corner.

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Machines	Last seen (UTC)
Microsoft OneDrive for Business 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 Cloud storage	6	24 MB	21 MB	1.2K	178	132	178	Sep 24, 2018

Discover and manage risky OAuth apps

Discover OAuth apps

That users have authorized to connect to your Office 365 environment

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

The screenshot displays the 'Manage app permissions' interface in the Microsoft Cloud App Security console. At the top, there are filters for 'APP' (Office 365, G Suite, Salesforce), 'USER NAME', 'APP STATE', 'COMMUNITY USE', 'PERMISSIONS', and 'PERMISSION LEVEL'. Below these filters is a table listing 31 apps. The table columns are Name, Authorized by, Permission level, Last authorized, and Actions. A detailed view for the 'Wunderlist' app is shown below the table, including its description, publisher, app website, app ID, permissions, community use, and related activities.

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	✓ ⚙ ⋮
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	✓ ⚙ ⋮

Wunderlist App Details:

- Description: Wunderlist
- Publisher: Wunderlist
- App website: <https://www.wunderlist.com/>
- App ID: 4b4b1d56-1f03-47d9-a0a3-87d4afc913c9
- Permissions: Sign-in and read user profile, Sign you in and read your profile
- Community use: Common
- Related activities: [View in activity log](#)

Settings

- General
 - Data retention
 - Alert notifications
 - Power BI reports
 - Secure score
 - Advanced features**
- Permissions
 - Roles
 - Machine groups
- APIs
 - Threat intel
 - SIEM
- Rules
 - Alert suppression
 - Automation allowed/blocked lists
 - Automation uploads
 - Automation folder exclusions
- Machine management
 - Onboarding
 - Offboarding
- Development
 - Flags

This section provides a set of advanced features you can enable. These features require integration with other products. You need to verify that these settings are enabled to use the features.

- On **Automated Investigation**
Enables the automation capabilities for investigation and response.
- On **Block file**
Make sure that Windows Defender is turned on and cloud-based protection feature is enabled in your organization to use the block file feature.
- On **Show user details**
Enables displaying user details: picture, name, title, department, stored in Azure Active Directory.
- On **Skype for business integration**
Enables 1-click communication with users.
- On **Azure ATP integration**
Connects to [Azure ATP](#) to enrich user and machine data and enable analysts to perform investigations across both services.
- On **Office 365 Threat Intelligence connection**
Connects to Office 365 Threat Intelligence to enable security investigations across Office 365 mailboxes and Windows machines. For more information, see the [Office 365 Threat Intelligence overview](#).
- On **Microsoft Cloud App Security**
Forwards Windows Defender ATP signals, giving [Cloud App Security](#) administrators deeper visibility of cloud usage, including the use of unsupported cloud services (shadow IT). Forwarded data will be stored and processed in the same location as your Cloud App Security data.
- On **Microsoft Intune connection**
Connects to [Microsoft Intune](#) to enable sharing of device information and enhanced policy enforcement. Intune provides additional information about managed devices for secure score. It can use risk information to enforce [conditional access](#) and other security policies.
- On **Preview features**
Allow access to preview features. Turn on to be among the first to try upcoming features. See the [Windows Defender ATP preview features](#) section in the [Windows Defender ATP guide](#).

Cloud Discovery

Continuous report
 Win10 Endpoint Users

Timeframe
 Last 30 days

- Dashboard
- Discovered apps
- IP addresses
- Users
- Machines**

Updated on May 7, 2019

Apps: **190**

IP addresses: **2542**

Users: **968**

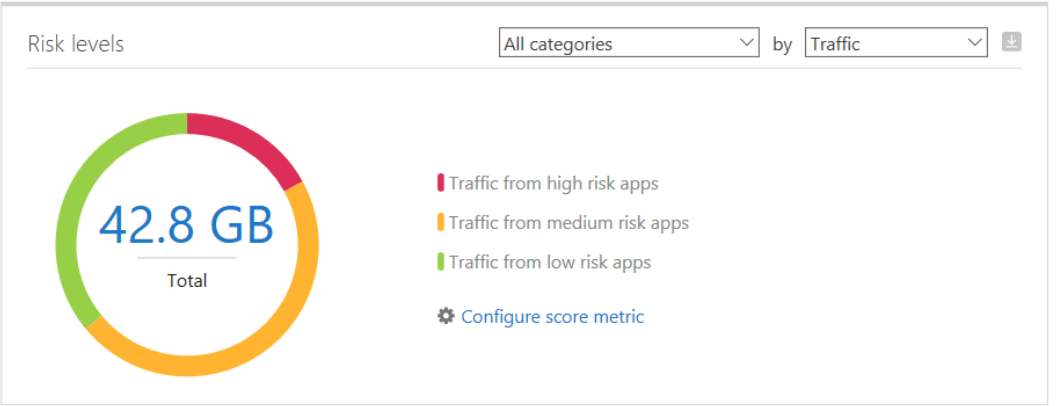
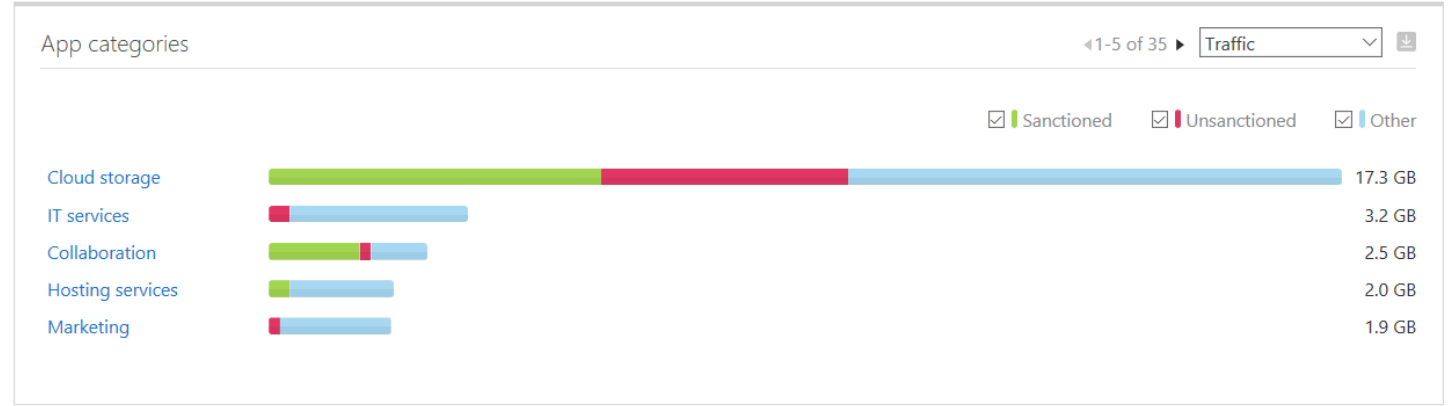
Machines: **970**

Traffic: **42.9GB** ↑ 38.6 GB ↓ 4.3 GB

Cloud Discovery open alerts + Create policy

109 Cloud Discovery alerts

9 Suspicious use alerts



Discovered apps

Sanctioned Unsanctioned Other

App	Sanctioned	Unsanctioned	Other	Total
MEGA	0	0	5.0 GB	5.0 GB
Dropbox	2.5 GB	0	0	2.5 GB
WeTransfer	0	2.3 GB	0	2.3 GB
Microsoft OneDriv...	2.0 GB	0	0	2.0 GB
Microsoft Live	0	0	1.6 GB	1.6 GB
Microsoft Skype fo...	0	0	602 MB	602 MB
Microsoft Exchang...	0	0	594 MB	594 MB
Box	0	0	547 MB	547 MB
Microsoft SharePo...	0	0	513 MB	513 MB

Top entites

View all users User by Traffic

User	Total
CONTOSO/Alice	3.6 GB
CONTOSO/Jane Smith	2.7 GB
CONTOSO/Bob	2.0 GB
CONTOSO/Derrick	129 MB
CONTOSO/Tripp	124 MB

Apps headquarters location

All categories

Cloud Discovery

Continuous report Win10 Endpoint Users Timeframe Last 30 days

- Dashboard
- Discovered apps**
- IP addresses
- Users
- Machines

Updated on Mar 4, 2019

QUERIES
Select a query...

APPS APP TAG RISK SCORE COMPLIANCE RISK FACTOR SECURITY RISK FACTOR
Apps... [Icons] None 0 4 10 Select factors... Select factors...

- Browse by category: 1K+
- Search for category...
- ✓ Cloud storage 7
 - Content management 3
 - Hosting services 3
 - IT services 2
 - Operations management 1
 - Online meetings 1
 - News and entertainment 1
 - Code hosting 1
 - Advertising 1
 - Accounting and finance 1

1 - 7 of 7 discovered apps

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Machines	Last seen (...)	Actions
Asigra Cloud storage	4	642 B	642 B	642	195	134	195	Mar 3, 2019	✓ ⏸ ⋮
Oxygen Cloud Cloud storage	4	37 KB	37 KB	718	217	153	217	Mar 3, 2019	✓ ⛔ ⋮
DollyDrive Cloud storage	4	11 KB	11 KB	720	218	156	218	Mar 3, 2019	✓ ⛔ ⋮
Arab Loads Cloud storage	4	606 B	606 B	606	185	140	185	Mar 3, 2019	✓ ⏸ ⋮
MEGA Cloud storage	3	1 MB	956 KB	51.5K	970	1472	971	Mar 3, 2019	✓ ⏸ ⋮

Security	3
News and entertainment	2
Productivity	2
Collaboration	2
CRM	2
Accounting and finance	2
Supply chain and logistics	1
Code hosting	1
Product design	1
Development tools	1
Content sharing	1
Business intelligence	1
Online meetings	1
Human-resource management	1
Transportation and travel	1
Operations management	1

MEGA
Cloud storage

4

11.8 GB
10.8 GB
85K
1904
1294

Sep 25, 2018
✓
⊘
⋮

⊘

Unsanctioned app
MEGA provides free cloud storage with convenient and powerful always-on privacy.

Suggest an improvement
Disclaimer

6

GENERAL

Category: Cloud storage

Headquarters: New Zealand

Data center: Luxembourg

Hosting company: Datacenter Luxembo...

Founded: 2013

Holding: Private

Domain: 2 *.mega.co.nz, *.mega.nz

main registration: Jul 26, 2012

Consumer popularity: 10

on URL: mega.nz

Vendor: Mega

5

SECURITY

Latest breach: Jan 1, 2018

⊘
IP address restriction

⊘

⊘
Data audit trail

✓

✓
Remember password

⊘

✓
Valid certificate name

✓

✓
Heartbleed patched

✓

✓
Protected against DROWN

✓

0

COMPLIANCE

⊘
FINRA

⊘

⊘

⊘
HIPAA

⊘

⊘

HTTP security headers

Which HTTP headers are implemented by the app on its website?

Source: Advanced data extraction

6/10

- ✓ x-frame-options
- ⊘ x-xss-protection
- ✓ strict-transport-security
- ⊘ x-content-type-options
- ✓ content-security-policy

6%
Weight in category

HTTP security headers: Partial ⓘ ⊘

⊘
Supports SAML

✓
Requires user authentication

⊘
Password policy

⊘
FINRA

⊘
FISMA

⊘
GAAP

⊘
HIPAA

⊘
ISAE 3402

⊘
ISO 27001

- System
- Organization details
- Mail settings
- Export settings
- Cloud Discovery
- Score metrics**
- Snapshot reports
- Continuous reports
- Automatic log upload
- App tags
- Exclude entities
- User enrichment
- Anonymization
- Delete data
- Information Protection
- Admin quarantine
- Azure Information Protection
- Files
- Conditional Access App Control
- Default behavior
- User monitoring
- Device identification
- App onboarding/maintenance

Score metrics

Configure your own preferences and priorities for each app property to customize the calculation of discovered app scores.

General

Field

- Founded**
The year in which the provider was founded.
- Holding**
Displays whether the provider is a publicly or privately held company.
- Domain registration**
The date on which the domain was registered.
- Consumer popularity**
Popularity of this app among SaaS users world-wide. A high score indicates a popular app with high-use rates.

Importance

Medium (x2)

Medium (x2)

Medium (x2)

Medium (x2)

N/A values ⓘ

- Exclude N/As
- Exclude N/As
- Exclude N/As
- Exclude N/As

Category importance: Low (x1)

Security

Field

- Data-at-rest encryption method**
The type of encryption of data-at-rest performed on the app.
- Multi-factor authentication**
Does this app support multi-factor authentication solutions?

Importance

Medium (x2)

Medium (x2)

N/A values ⓘ

- Exclude N/As
- Exclude N/As

Category importance: Medium (x2)

Cloud Discovery

Continuous report: Global | Timeframe: Last 30 days

- Dashboard
- Discovered apps**
- IP addresses
- Users

Updated on Mar 26, 2019

QUERIES
Select a query...

APPS: Apps... | APP TAG: [✓] [🚫] None | RISK SCORE: 0-10 slider (set to 3) | COMPLIANCE RISK FACTOR: Select factors... | SECURITY RISK FACTOR: Select factors... | Save as | Advanced

- Browse by category: 🔍
- Search for category...
- ✓ Cloud storage 5
 - Marketing 3
 - IT services 3
 - Hosting services 3
 - Customer support 3
 - Website monitoring 2
 - Productivity 2
 - Collaboration 2
 - Advertising 2
 - Content management 2

1 - 5 of 5 discovered apps

New policy from search | [🔍] | [📄] | [📄]

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Last seen (...)	Actions
MEGA Cloud storage	3	90 MB	46 MB	86	62	56	Mar 25, 2019	✓ [🚫] [⋮]
SendMyWay Cloud storage	3	90 MB	47 MB	83	70	45	M	✓ [🚫] [⋮]
PowerFolder Cloud storage	3	94 MB	49 MB	88	73	52	M	✓ [🚫] [⋮]
NetFortris Cloud storage	3	83 MB	42 MB	80	65	42	M	✓ [🚫] [⋮]
OwnCube Cloud storage	3	93 MB	48 MB	85	72	45	M	✓ [🚫] [⋮]

- TAG APP
- Sanctioned
 - ✓ Unsanctioned**
 - Custom app
 - Accounting Dept
 - Deprecated
 - In legal review
 - In review
 - In technical POC
 - Managed

Tag an app as unsanctioned to block it from being accessed by users in the future

This website is blocked by your organization. Contact your administrator for more information.

mega.nz

[Back to safety](#)

Windows Defender SmartScreen

Discovered resources

Continuous report: Global | Timeframe: Last 30 days

APP: | RESOURCE NAME: | RESOURCE TYPE: Advanced

1 - 20 of 27 resources

Sort, Download, Filter

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

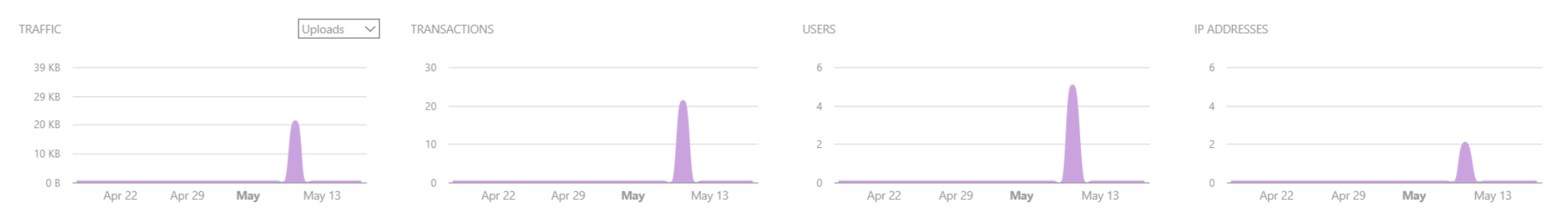
Discovered resources

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

adatum
 Amazon Web Services
 User report
 IP address report



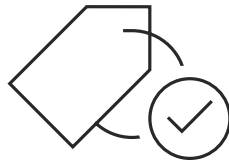
fabrikam company-files	Queue	Microsoft Azure	63 KB	41 KB	27	10	5	May 13, 2019
webapp	Bucket	Amazon Web Services	45 KB	29 KB	83	7	5	May 10, 2019
playground instance	File	Microsoft Azure	19 KB	12 KB	12	3	2	May 10, 2019
cohovineyard	Bucket	Google Cloud Platform	19 KB	12 KB	23	3	2	May 10, 2019

Microsoft Information Protection solutions

Protect your sensitive data – wherever it lives or travels



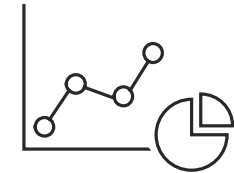
Discover



Classify

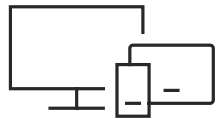


Protect



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-prem 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

Be notified to identify and investigate policy violations and related activities

Automatically remediate with built-in actions incl. notify owner, notify admin, make private, quarantine, etc.

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

The screenshot displays the Microsoft Cloud App Security interface. At the top, there are search and filter options for queries, apps, owners, access levels, file types, and matched policies. Below this is a table of files, with columns for File name, Owner, App, Collaborators, Policies, and Last modified. Several files are highlighted in red, indicating policy matches or violations. A detailed view of a selected file, 'European customer data.docx', is shown below the table, including its path, type, MIME type, file identifiers, collaborators, and scan status. The scan status indicates '2 failed'.

File name	Owner	App	Collaborators	Policies	Last modified
European customer data.docx	Jane (jane@mcas-test9.com)	Box - US	1	1 policy match	Mar 21
Invoices from Box	Super Admin (mcas-test9) (superadmi...)	Box - US	1	—	Mar 21
BOX_INV06580587_190327.pdf	Super Admin (mcas-test9) (superadmi...)	Box - US	1	—	Mar 21
__sitelcon_.jpg	System Account	Microsoft SharePoint Online	3 collaborators	1 policy match	Mar 21
Test	Silvia (silvia@mcas-test9.com)	Microsoft OneDrive for Business	1	—	Mar 21
Documents	Silvia (silvia@mcas-test9.com)	Microsoft OneDrive for Business	1 collaborator	—	Mar 21
Employee_SSN.txt	Silvia (silvia@mcas-test9.com)	Microsoft OneDrive for Business	1 collaborator	—	Mar 21
mcastest9-my.sharepoint.com.url	Silvia (silvia@mcas-test9.com)	Microsoft OneDrive for Business	1 collaborator	—	Mar 21
European customer data.docx	Jane (jane@mcas-test9.com)	Box - US	1	1 policy match	Mar 15
European customer data.docx	Jane (jane@mcas-test9.com)	Box - US	1	1 policy match	Mar 15
European customer data.docx	Jane (jane@mcas-test9.com)	Box - US	1	1 policy match	Mar 15
European customer data.docx	Jane (jane@mcas-test9.com)	Box - US	1	1 policy match	Mar 15
Trade Secrets	Super Admin (mcas-test9) (superadmi...)	Box - US	3 collaborators	—	Mar 15
Secrets Ingredients 2.docx	Super Admin (mcas-test9) (superadmi...)	Box - US	3 collaborators	—	Mar 15

File Details: European customer data.docx

- Path: —
- URL: <https://app.box.com/files/0/f/0/1/f/422357869679>
- Type: document
- Owner: Jane (jane@mcas-test9.com)
- Created: Mar 15, 2019
- Policies: Find GDPR data across file storage ap...
- MIME type: application/vnd.openxmlformats-officedocument.wordpro...
- Owner OU: —
- Modified: Mar 15, 2019
- Classification labels: 2 AZURE RMS ENCRYPTED
- File identifiers: [View file identifiers](#)
- Collaborators: —
- File size: ~39 KB
- Scan status: 2 failed

Key Differentiators via Microsoft Information Protection approach

Unified labelling with Microsoft Information Protection - streamlined experience across O365 DLP, AIP and MCAS

90 built-in, sensitive information types you can choose from

Custom sensitive information types using Regex, keywords and large dictionary

Leverage Microsoft or 3rd party DLP engines for classification

Leverage AIP labels

Cloud App Security

Apply to: all file owners

Inspection method: None

Alerts: Create an alert for each matching file

Governance

- > G Suite
- > Box
- ▼ Microsoft OneDrive for Business - 1 selected
 - Send policy-match digest to file owner
 - CC additional users
 - Make private
 - Remove external users
 - Inherit parent permissions
 - Put in user quarantine
 - Put in admin quarantine
 - Remove a collaborator
 - Apply classification label
 - Select an Azure Information Protection classification label to apply to matching files:
 - None
 - Confidential-All Employees**
 - Confidential-Anyone (not protected)
 - Highly Confidential-All Employees
 - Highly Confidential-Anyone (not protected)
 - Confidential Credit Card Information
 - Company Confidential
 - Secret-All Company
 - Confidential-view only

- > Amazon Web Services

Note that externally owned folders will not be scanned.
We secure your data as described in our [privacy statement](#).

Cancel Create

Protect sensitive files in the cloud

1. User uploads a sensitive file to a cloud app



2. A classification label is automatically applied to protect the file



3. User tries to share sensitive file with external users



4. External user is not able to access the file due to classification and protection



5. Admin receives event alerts



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

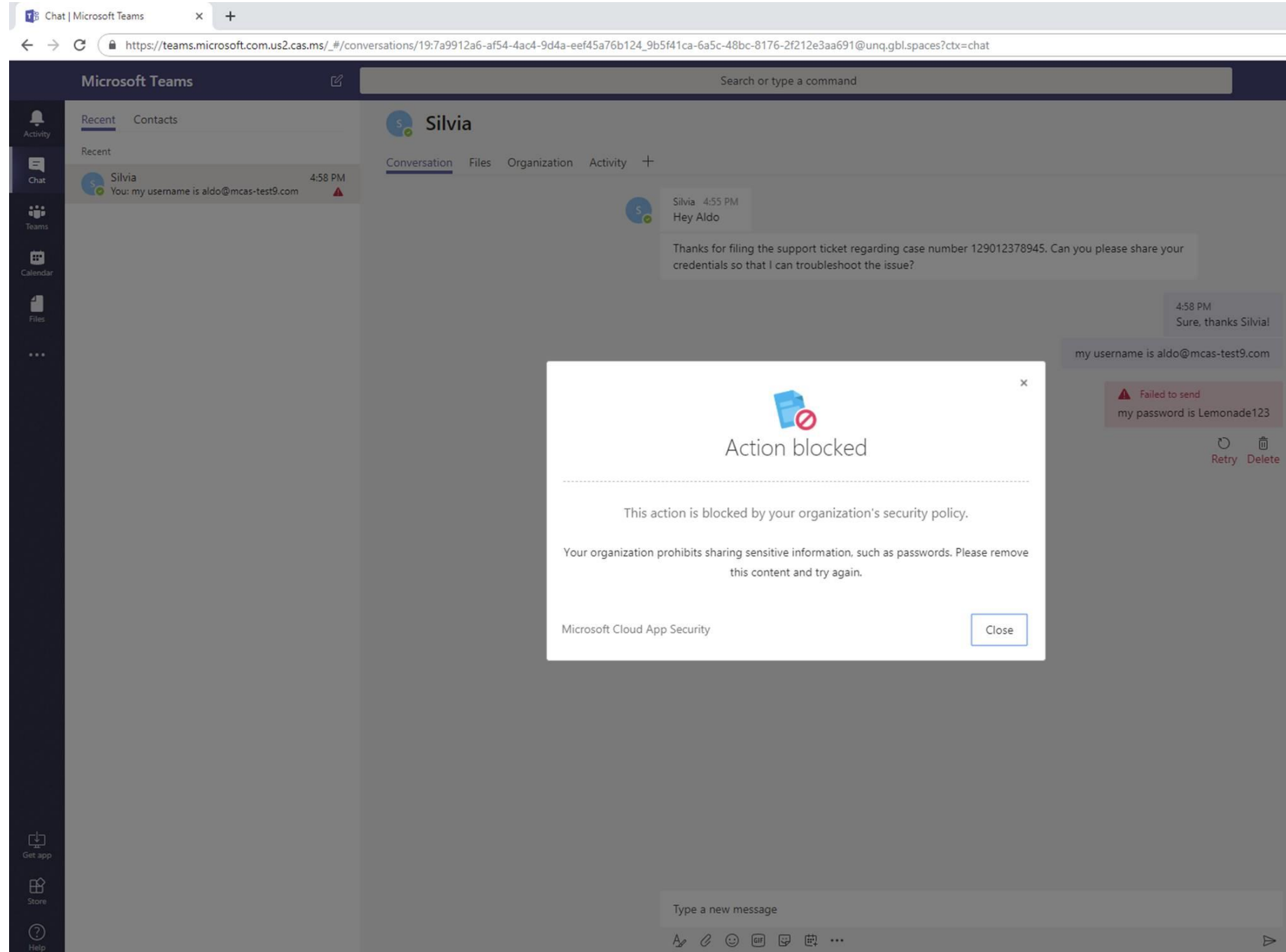
Enforce granular monitoring & control for risky user sessions

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



Key differentiators to optimize the admin and end user experience

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

Home > MCAS Contoso 9 > Conditional access - Policies > Route Charles to CAS from non-compliant dev

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](#)

Conditions

Controls

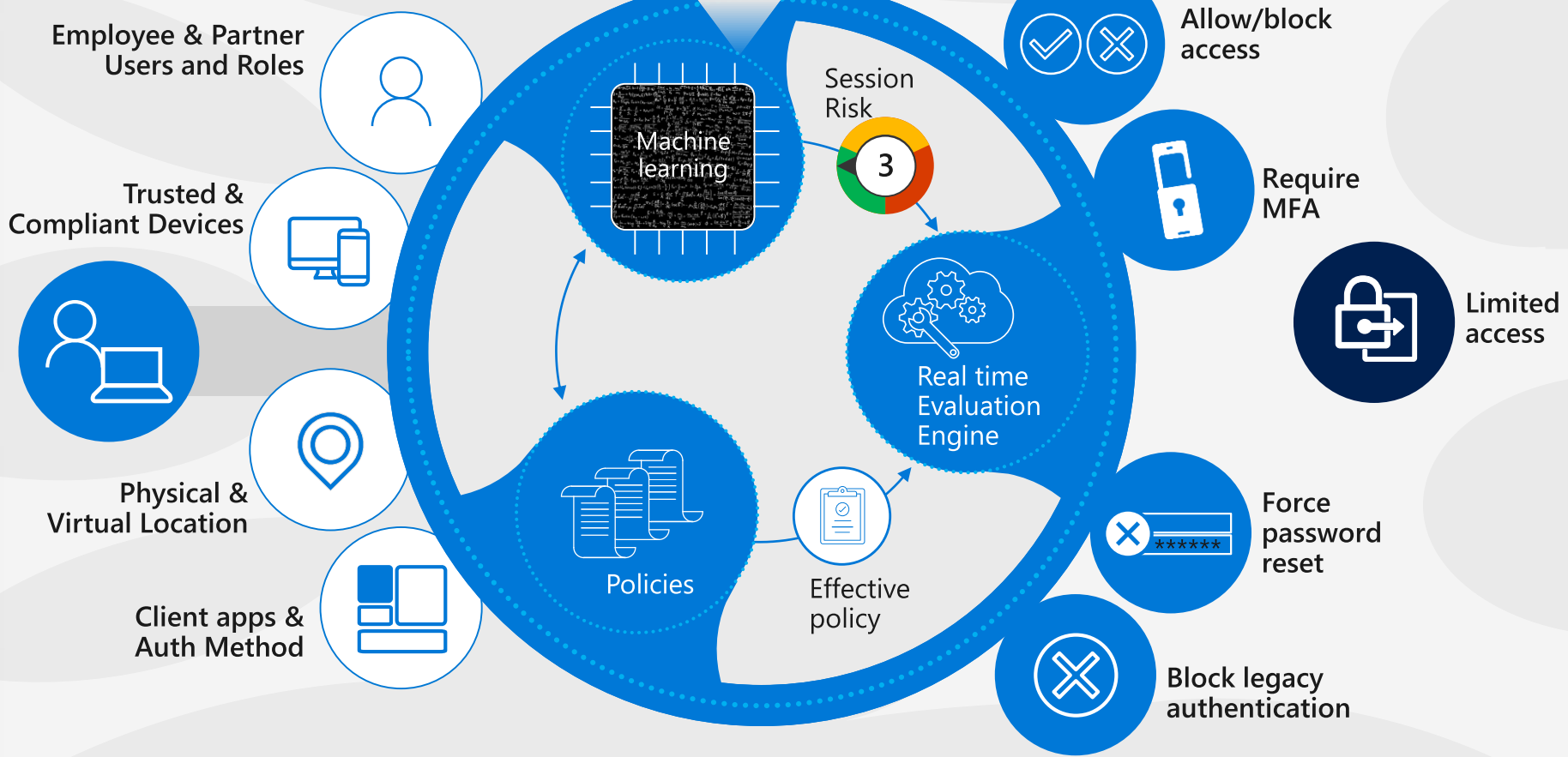
0 1 0 0
1 0 0 1
40TB

- Azure AD
- ADFS
- MSA
- Google ID

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

- Geo-location
- Corporate Network

- Browser apps
- Client apps



Microsoft Cloud



Microsoft Cloud App Security



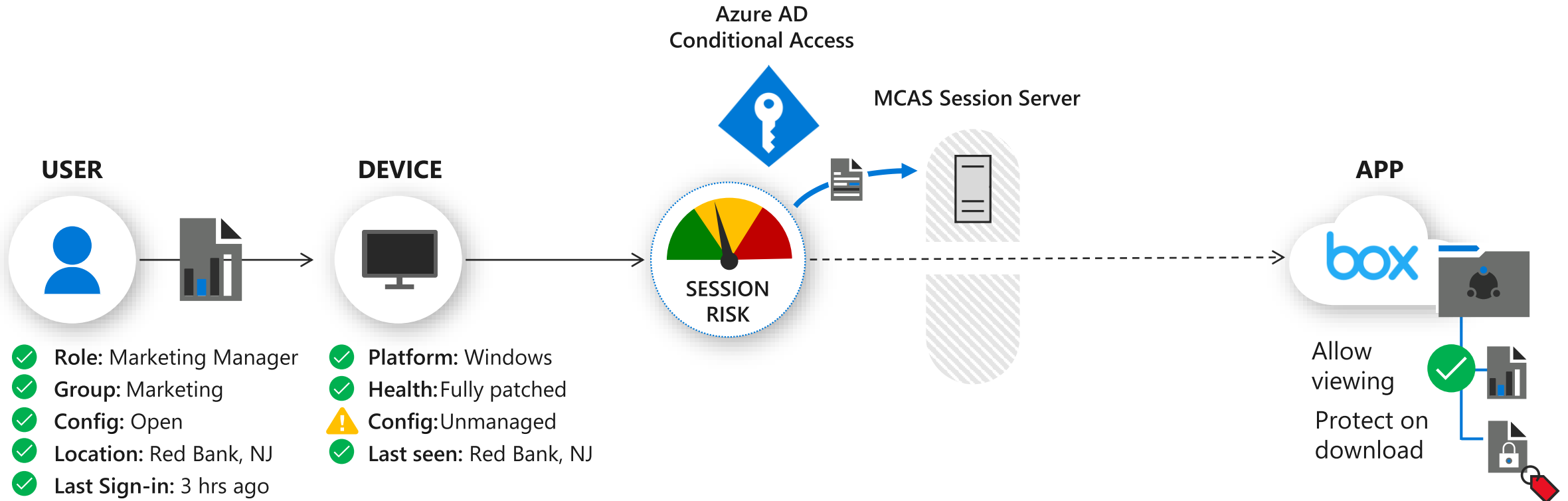
Cloud apps & services



On-premises apps

USE CASE: PREVENT DOWNLOAD OF RISKY FILES

Risk based in-session controls



⚠ Device is unmanaged

- ☰
- Dashboard
- Discover
- Investigate
- Control
 - Policies
 - Templates
- Alerts 1K+

Create session policy

Session policies provide you with real-time monitoring and control over user activity in your cloud apps.

Policy template

Block download based on real-time content inspection

No template

Block sending of messages based on real-time content inspection

Block download based on real-time content inspection

Block upload based on real-time content inspection

Block cut/copy and paste based on real-time content inspection

Monitor all activities

and will block any violations in real-time.

Policy severity

Medium

Category

DLP

Session control type

Select the type of control you want to enable:

Control file download (with DLP)

Activity source

Add activity filters to the policy

[Edit and preview results](#)

ACTIVITIES MATCHING ALL OF THE FOLLOWING

Device
Tag
does not equal
Compliant, Domain joi...

+

Add file filters to the policy

FILES MATCHING ALL OF THE FOLLOWING

Create session policy

Session policies provide you with real-time monitoring and control over user activity in your cloud apps.

Policy template

Block sending of messages based on real-time content inspection

Policy name

Block sending of messages based on real-time content inspection

Description

Cloud App Security will evaluate the content of messages that are sent or posted and will block any violations in real-time.

Policy severity

Medium

Category

DLP

Session control type

Select the type of control you want to enable:

Block activities

Activity source

Add activity filters to the policy

ACTIVITIES MATCHING ALL OF THE FOLLOWING Edit and preview results

Activity type	equals	Send Teams message, ...
App	equals	Microsoft Teams

Send Teams message, ...

Search: |

- Send item
 - Send Teams message
 - Send Salesforce message
 - Send Slack message
 - Publish Workplace by Facebook pos
 - Send Workplace by Facebook messag
 - Publish Salesforce post
- Add item to list

Create a session policy to block IM messages in Microsoft Teams that contain sensitive content

Content inspection Enabled Currently supports Activity type(s): Cut/Copy, Paste, and Send item

Include text that matches a preset expression

All countries: Finance: Credit card number ▾

Don't require relevant context ●

Include text that matches a custom expression

Use case-sensitive search

Custom expression...

Match substring Exact match Match a regular expression ●

Exclude text that matches:

Regular expression

Unmask the last 4 characters of a match ●

Actions

Select an action to be applied when user activity matches the policy.

- Test**
Monitor all activities
- Block**
Block selected activities & monitor all activities
 - Also notify user by email
 - Customize block message ●

Create an alert for each matching event with the policy's severity [Use your organization's default settings](#)

Daily alert limit

- Send alert as email ●
- Send alert as text message ●

[Save these alert settings as the default for your organization](#)

Send alerts to Flow PREVIEW

Select playbook... ▾

Session control applies to browser-based apps.
To block access from mobile and desktop apps, [create](#) an Access policy

Recent Contacts

Recent

S Silvia 4:58 PM
You: my username is aldo@mcas-test9.com

S Silvia

Conversation Files Organization Activity +

S 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?

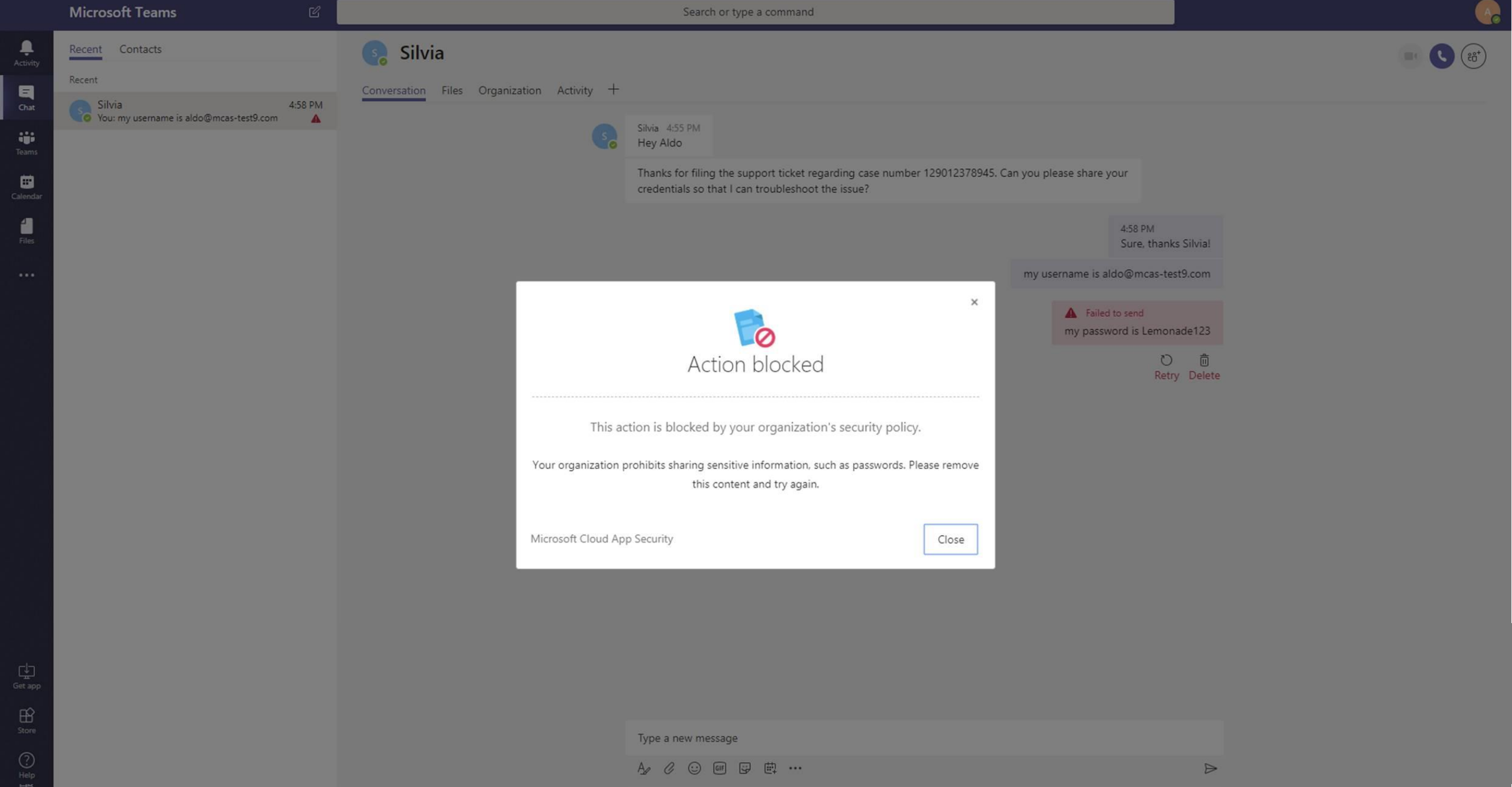
4:58 PM
Sure, thanks Silvia!

my username is aldo@mcas-test9.com

my password is Lemonade123



End user attempts to send sensitive information (password) via IM message



The IM message is blocked in real-time and not delivered



Access to Microsoft Exchange Online is monitored

For improved security, your organization allows access to **Microsoft Exchange Online** in monitor mode.

Access is only available from a web browser.

[Continue to Microsoft Exchange Online](#)

InPrivate Mail - Silvia@mcas-test x + v
https://outlook.office365.com.us2.cas.ms/owa/?path=/attachmentlightbox

Office 365 Outlook

Download Hide email Edit and reply

PowerPoint Online Product strategy [Internal] Start Slide Show Print to PDF Comments Help

Product strategy
Internal

The documents you requested

Aldo
Wed 1/24/2018, 3:20 PM
Silvia

- Product strategy [Intern... 36 KB
- Roadmap.pptx 39 KB
- Usage report [Internal].x... 8 KB

3 attachments (83 KB) Download all Save all to OneDrive - MCAS Contoso 9

SLIDE 1 OF 1 HELP IMPROVE OFFICE NOTES

End user attempts to download an email attachment containing sensitive, internal information

The screenshot shows a web browser window displaying an Outlook interface. The main content area is a PowerPoint slide titled "Product strategy [Internal]". A modal dialog box is overlaid on the slide, titled "Download blocked". The dialog contains the following text:

Download blocked

Downloading **Product strategy [Internal].pptx** is blocked by your organization's security policy.

The file you attempted to download is marked as confidential. For more information contact admin@contoso.com

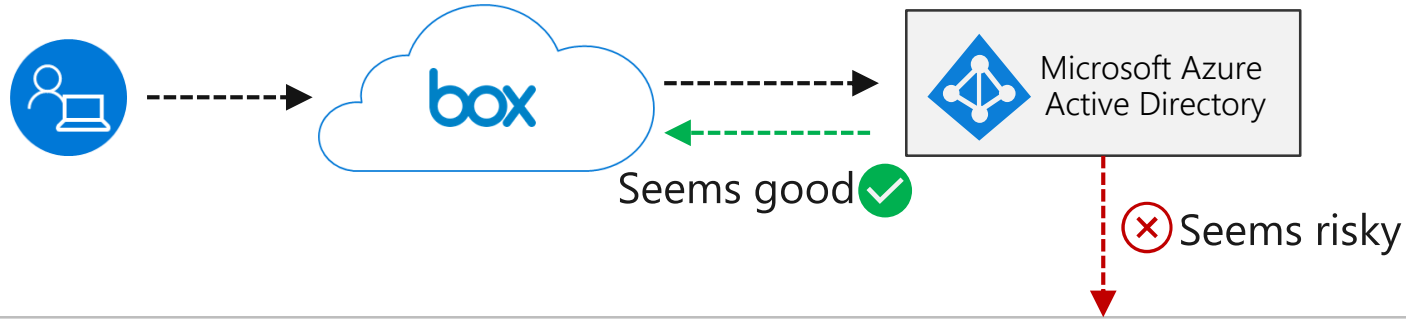
Microsoft Cloud App Security Close

In the background, the Outlook interface shows an email from Aldo dated Wed 1/24/2018, 3:20 PM. The email has three attachments: "Product strategy [Intern...]" (36 KB), "Roadmap.pptx" (39 KB), and "Usage report [Internal].x..." (8 KB). A "Download all" button is visible below the attachments.

At the bottom of the screen, a file download dialog is open, asking "What do you want to do with Blocked_2019-04-09_01-20-08_tzwXDysSPCIY.txt?". The dialog includes buttons for "Open", "Save", "Cancel", and a close button (X).

End user is notified that the download to his personal device was blocked

CONDITIONAL ACCESS APP CONTROL

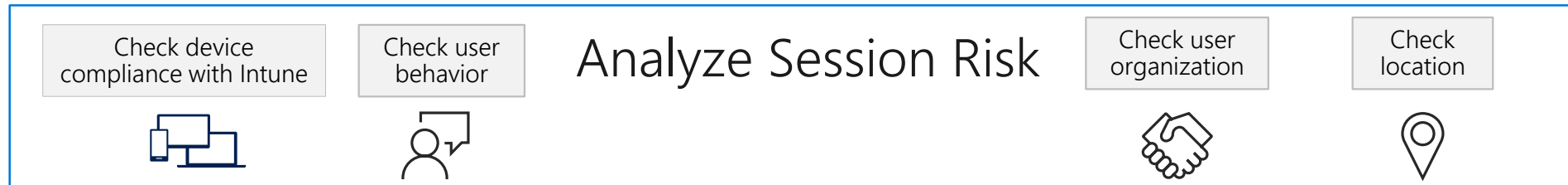


Cloud App Security integrates with:

- Azure Active Directory
- Azure Information Protection
- Microsoft Intune

to help protect any app in your organization.

MICROSOFT CLOUD APP SECURITY



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



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

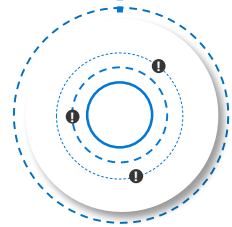
Require MFA and define session timeouts for unfamiliar locations

Detections across cloud apps

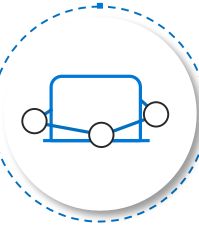
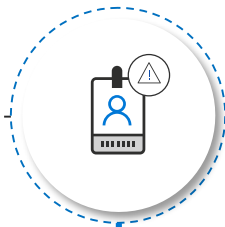
- Malware implanted in cloud apps
- Malicious OAuth application
- Multiple failed login attempts to app
- Suspicious inbox rules (delete, forward)

- 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

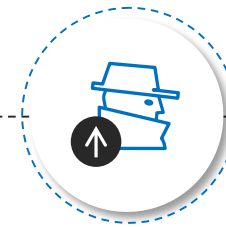
Indicators of a compromised session



Threat delivery and persistence



Malicious use of an end-user account



Malicious use of a privileged user

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

Key threat alerts and mitigation actions

Identify high-risk and anomalous usage

Exfiltration of data to unsanctioned apps

Rogue 3rd party applications

Ransomware attacks

Mitigate ransomware attacks

Suspend user sessions

Revoke OAuth app access

Cloud App Security

Alerts > Ransomware activity | 3 MONTHS AGO

Ransomware activity | 167.220.196.35 | billd@mcas-test9.com | Microsoft OneDrive for Business

Resolution options: Bill Dortch

- Azure AD account settings
- View related activity
- View related governance
- View related alerts
- View owned files
- View files shared with this user
- OFFICE 365
- Require user to sign in again
- Suspend user
- Account settings in app
- MICROSOFT ONEDRIVE FOR BUSINESS
- Suspend user
- Require user to sign in again
- Suspend user

Description

The user billd@mcas-test9.com uploaded a ransomware recovery instructions file (https://mcastest9-my.sharepoint.com/personal/billd_mcas-test9_com/Documents/recovery_key.txt), which is a critical file. Additional risks in this usage:

- This user uploaded 1 of them had the same file extension (locky).

Activity log

Activity	User	App	IP address	Location	Device
Upload file: file https://mcastest9-my.sharepoint.com/personal/billd_mcas-test9_com/Documents/recovery_key.txt	billd@mcas-test9.com	Microsoft On...	167.220.196.35	United Kin...	Windows
Upload file: file https://mcastest9-my.sharepoint.com/personal/billd_mcas-test9_com/Documents/recovery_key.txt	billd@mcas-test9.com	Microsoft On...	167.220.196.35	United Kin...	Windows
Upload file: file https://mcastest9-my.sharepoint.com/personal/billd_mcas-test9_com/Documents/recovery_key.txt	billd@mcas-test9.com	Microsoft On...	167.220.196.35	United Kin...	Windows

SHOW SIMILAR | General | User | IP address

167.220.196.35 | OPEN ALERTS: 131 | ACTIVITIES: 13 | ADMIN ACTIVITIES: 0

United Kingdom, England, London | ISP: Microsoft Corporation

Filter by this IP address | IP address actions

IP ACTIVITIES (30 DAYS) | Oct

Comprehensive Threat Protection for your cloud apps

Built-in Threat Protection policies

More than 15 out-of-the-box policies that 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 the 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-prem and cloud

Cloud App Security

Alerts

RESOLUTION STATUS: OPEN, DISMISSED, RESOLVED

CATEGORY: Select risk category...

SEVERITY: Low, Medium, High

APP: Select apps...

USER NAME: Select users...

1 - 12 of 12 alerts

Alert	App	Resolution	Severity	Date
Risky OAuth apps 178.17.166.149 Bill Dortch	Salesforce - General	RESOLVED	Low	2 d
Ransomware activity 178.17.166.149 Bill Dortch	Amazon Web Service	RESOLVED	High	2 d
Malware campaign caught in delivery 178.17.166.149 Bill Dortch	Slack - General - General	RESOLVED	Low	2 d
Activity from a Tor IP address 79.137.68.85 Bill Dortch	Box - General - General	RESOLVED	Medium	2 d
Alert on any session coming from a Risky IP address 79.137.68.85 Bill Dortch	Office 365	DISMISSED	Low	2 d
Logon from a risky IP address 79.137.68.85 Bill Dortch	Workplace by Facebook...	DISMISSED	High	2 d
Logon from a risky IP address 79.137.68.85 Bill Dortch	Microsoft SharePoint O...	DISMISSED	High	2 d

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

External DLP solution

Integrate with existing DLP solutions to extend these controls to the cloud while preserving a consistent and unified policy across on-premises and cloud activities

Security Workflow automation with Microsoft Flow

Centralized alert automation and orchestration of custom workflows using the ecosystem of connectors in Microsoft Flow. 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

Automating Security Workflows with MS Flow

Centralized alert automation and orchestration of custom workflows

Automate the triage of alerts

Enables an ecosystem of connectors in Microsoft Flow incl. >100 3rd party connectors such as Jira, ServiceNow, and DocuSign

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

Predefined governance options when creating policies

The screenshot displays the Microsoft Power Automate (MS Flow) interface. The top navigation bar includes a 'Flow' title, a search icon, and user information for 'MOD Administrator Contoso (default)'. The left sidebar contains navigation options: Home, Approvals, My flows (selected), Templates, Connectors, Data, and Learn. The main workspace shows a workflow titled 'Request Input from user/manager for governance action'. The workflow steps are: 1. 'When an alert is generated (Preview)' connector. 2. 'Get user' connector with 'User Id or Principal Name' set to 'CompromisedEntity'. 3. 'Send Text Message (SMS)' connector with 'From Phone Number' as 'socteam@contoso.com', 'To Phone Number' as 'Mobile Phone', and 'Text' as 'Cloud App Security Generated Alert for your Account - Request for your input'. 4. 'Send email with options' connector with 'To' as 'Mail', 'Subject' as 'Your input is required for investigation', and 'User Options' as 'PleaseIgnore, I'mNotSure'. 5. 'Condition' connector with 'SelectedOption' 'is equal to' 'PleaseIgnore'. Below the condition, there are two paths: 'If yes' (green background) leading to a 'Dismiss alert' connector, and 'If no' (red background) leading to a 'Slack' connector.

Microsoft Cloud App Security Alerts

 Cloud Threats

 File policy violations

 App Discovery

 User activity

Microsoft Flow Connectors

 twilio

 JIRA

 now  zendesk



Open incident in ticketing system & populate with alert attributes



Routing CAS alerts to different SOC units



Get admin approval to execute remediation action




Request user input to provide context during alert investigation



Block risky apps based on discovery alerts

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. MCAS alert triggers antivirus scan in Microsoft Defender ATP
- 

Edit app discovery policy

Policy template *

No template

Policy name *

Non-compliant app usage detected - ISO27018 & rec

Description

Policy severity *

Low

Category *

Cloud Discovery

APPS MATCHING ALL OF THE FOLLOWING

Select a filter...

Edit and preview results

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
- 