

# App Governance in Microsoft Defender for Cloud Apps

Beata Zalewa

# About



In professional life Lead Technical Architect, consultant, Microsoft Certified Trainer, developer, freelancer.



From the beginning of career associated with Microsoft technologies.



Private life in numbers: 1 husband, 1 daughter, 1 cat and 2 dogs. My hobbies are detective stories and photography.



Email: [info@zalnet.pl](mailto:info@zalnet.pl)



<https://www.linkedin.com/in/beatazalewa/>



WWW: <https://beatazalewa.com/>

# Solution overview

What is **Defender for Cloud Apps**?

A native *Cloud Access Security Broker (CASB)* that supports various deployment modes including log collection, API connectors, and reverse proxy.

Cloud app discovery platform that fetches data from Defender for Endpoint or Firewall logs

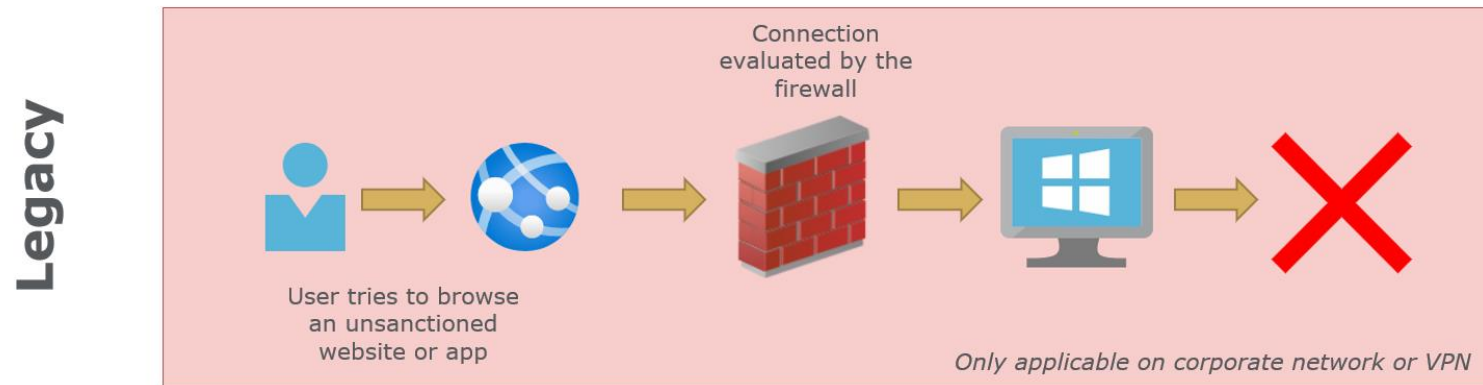
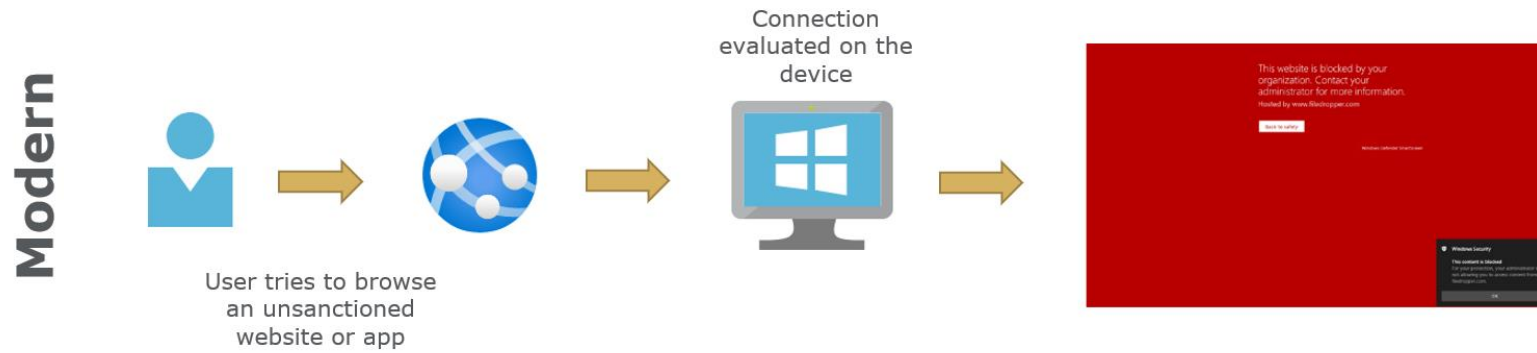
Granular control interface of collaboration and access to SaaS (Software as a service) apps in the web (security and compliance enablement)

Decentralized / cloud-based solution where the security perimeter is built-in the Defender Suite

## How the cloud changed the enterprise?

The modern vs. legacy approach on network controls differentiate through a central component, the firewall, which in the legacy flow was needed to control connections from a client.

The modern approach is that connections are evaluated on the device and thus independently of the network.



# How the cloud changed the enterprise?

# License requirements

- Microsoft Cloud App Security Licensing Datasheet

[RE2NXYO \(microsoft.com\)](https://aka.ms/RE2NXYO)

- When talking about pricing, Defender for Cloud Apps has some included features in Azure AD Premium P1, that is part of Enterprise Mobility + Security E3.

- The full capabilities get available with the Microsoft 365 E5 Security or the standalone CAS license, which costs ~ 3.5\$/user/month.

<https://aka.ms/M365EnterprisePlans>

# What are Cloud Apps?

The challenge consists of thousands of Cloud applications and websites that users need for collaboration.

Shadow IT describes non IT-personnel, that interacts with separate accounts (no SSO or central IdP) on cloud infrastructure/apps that the organization utilizes.

The problem is, that the IT department has no governance over these actions and lacks of security and compliance.

Microsoft 365 Defender

Search

Cloud app catalog

Filters:

Apps:  App tag: ☒ Sanctioned ☐ Unsanctioned ☐ None Risk score: 0  10

Compliance risk factor: **Select factors** Security risk factor: **Select factors**

Browse by category:

Hosting services	3.5K
IT services	3.1K
Accounting and finance	2.3K
Business management	2K
Productivity	1.7K
Human-resource manage...	1.2K
E-commerce	1.2K
Marketing	1.2K
Education	1.1K

☐ Bulk selection  New policy from search

App	Risk score	Actions
<b>Microsoft Xbox</b> News and entertainment	10	<input checked="" type="radio"/> <input type="radio"/> <input type="button" value="⋮"/>
<b>Xamarin</b> Development tools	10	<input checked="" type="radio"/> <input type="radio"/> <input type="button" value="⋮"/>
<b>Azure Virtual Desktop</b> Cloud computing platform	10	<input checked="" type="radio"/> <input type="radio"/> <input type="button" value="⋮"/>
<b>Microsoft Word Online</b> Productivity	10	<input checked="" type="radio"/> <input type="radio"/> <input type="button" value="⋮"/>
<b>Microsoft Azure Services</b> Cloud computing platform	10	<input checked="" type="radio"/> <input type="radio"/> <input type="button" value="⋮"/>
<b>Windows365</b> Cloud computing platform	10	<input checked="" type="radio"/> <input type="radio"/> <input type="button" value="⋮"/>

# Cloud App catalog

Microsoft's own database of discovered apps in the web has over 30'000 entries. They are added on the go.



# App details

Each app (example LinkedIn) has a lot of information assigned, such as general information, security related data and governance standards. As you can see, there is a lot of useful information that an ordinary consumer might never have known.

The screenshot displays the LinkedIn app details page. At the top, there is a search bar and a navigation bar with the LinkedIn logo and the text "Social network". Below this, a brief description of LinkedIn is provided. The page is organized into three main sections: GENERAL, SECURITY, and COMPLIANCE, each with a progress bar indicating a score of 10.

**GENERAL** 10

Category: So...	Headquarters: Uni...	Data center: Unite...
Founded: 19...	Holding: Public	Domain: 2 *.linke...
Domain registration:	Consumer popularity:	Privacy policy: priv...
Vendor: Micr...	Data types: 2 Do...	Disaster Recovery...

**SECURITY** 10

Latest breach:	Data-at-rest encryption method: Multi-factor auth...	
User audit t...	Admin audit trail	Data audit trail
Data classifi...	Remember passw...	User-roles support
Valid certific...	Trusted certificate	Encryption protocol:
HTTP securi...	Supports SAML	Protected against...
Requires us...	Password policy	

**COMPLIANCE** 10

ISO 27001	ISO 27018	ISO 27017
FINRA	FISMA	GAAP

## Demo 1



**KEEP  
CALM  
AND  
PRAY THE DEMO  
WORKS**

# How to make it work



You may ask yourself what to do with this data.



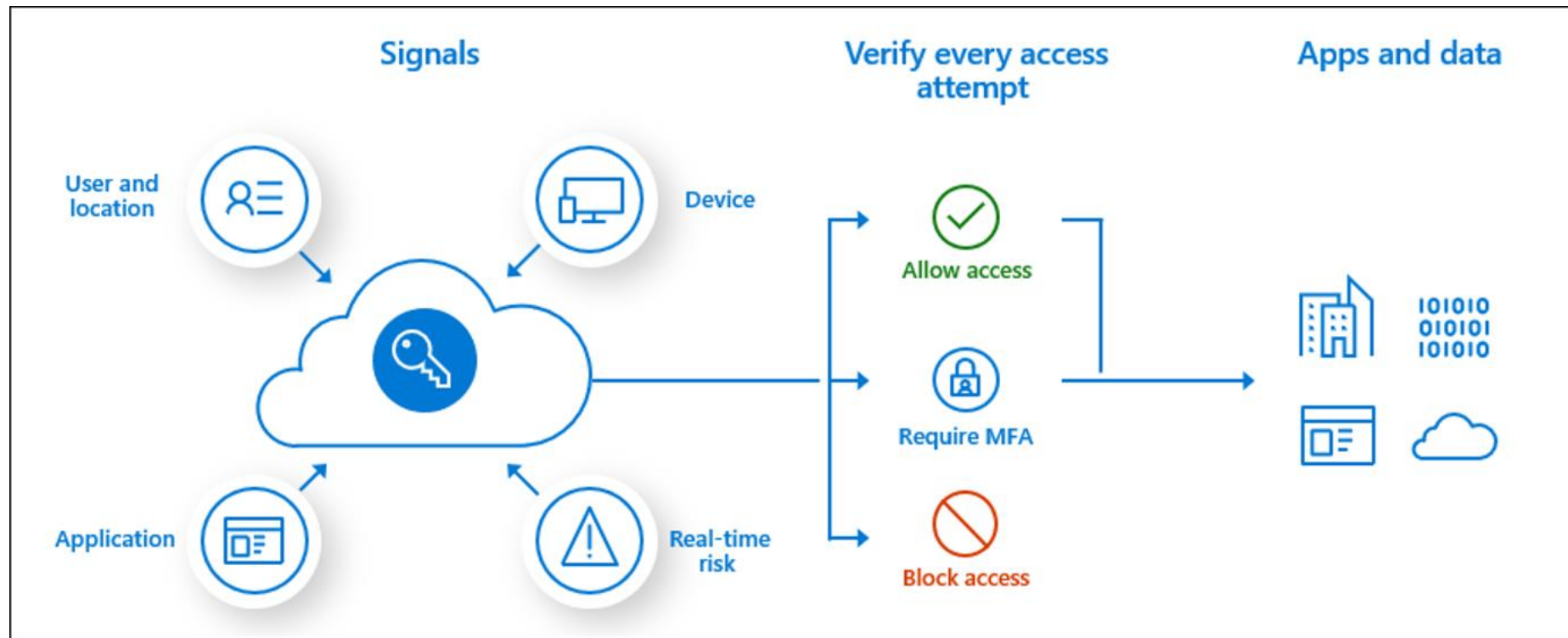
Usually in later step policies are enforced to strictly define which attributes of a cloud app are relevant or even required before accessing an app.



Score metrics can be configured to individual preferences and importance's.



Furthermore, session controls work with **Conditional Access**.



# Conditional access

# Session control

Through conditional access, we also have the great opportunity to take control even at the session level.

- **Use app enforced restrictions** this only works with Sharepoint Online and Exchange Online and can create a limited experience within the apps.
- **Use conditional access app control** uses Microsoft Cloud App security where you can protect data with Conditional Access App Control by applying access and session controls.
- **Sign-in frequency** defines the time period before a user is asked to sign in again when attempting to access a resource. You can set this from a few hours up to 365 days.
- A **persistent browser session** allows users to remain signed in after closing and reopening their browser window. The option "stay signed-in" will also be skipped.

# App tags

Apps can be tagged as:

**Sanctioned** - app is generally allowed and accessible

**Unsanctioned** - app is generally not allowed and might be not accessible

**Monitored** - app is under special observation, user receives a corresponding notification, that the access to this app is monitored

**Individual tag** - individual, for utilization in own policies

Microsoft 365 Defender

Search

# Cloud app catalog

Filters:

Apps:  App tag: ☒ Sanctioned ☐ Unsanctioned ☐ None Risk score: 0  10

Compliance risk factor: **Select factors** Security risk factor: **Select factors**





Advanced filters

Browse by category:

Search for category

- Social network 2
- Education 1
- Marketing 1

Bulk selection ☐ New policy from search

App	Risk score	Actions
 <b>LinkedIn marketing solutions</b> Marketing	10	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
 <b>LinkedIn Learning</b> Education	10	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
 <b>LinkedIn</b> Social network	10	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
 <b>LinkedIn Engineering</b> Social network	10	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

# App tags



**DEMO 2**



**App tags**



## App risks score

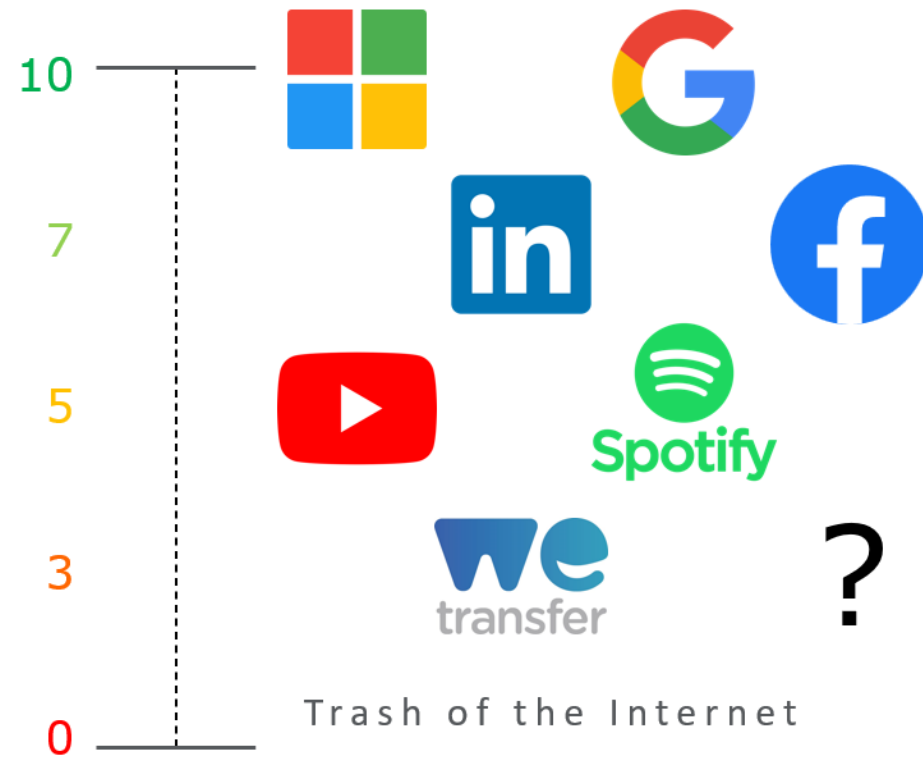
Each cloud app is rated by Microsoft by an individual risk score to:

Scores from **0** (worst, harmful) up to **10** (best, harmless)

App scores can be used to identify unwanted or malicious apps

Score metrics can be configured to own concerns, but Microsoft raises data and provides default score metrics

Block access to apps under a certain score (with Defender for Endpoint integration)



App risks score



**DEMO 3**



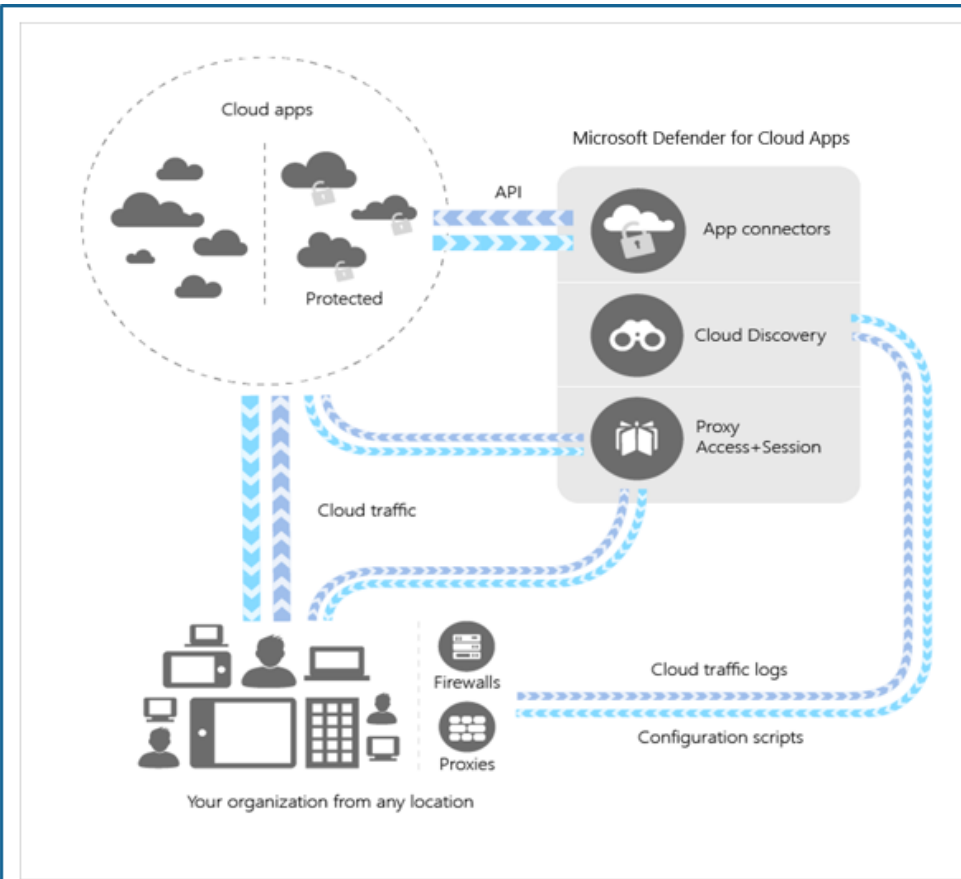
**App risks score**

The Defender for Cloud Apps framework provides the following threat intelligence protection:

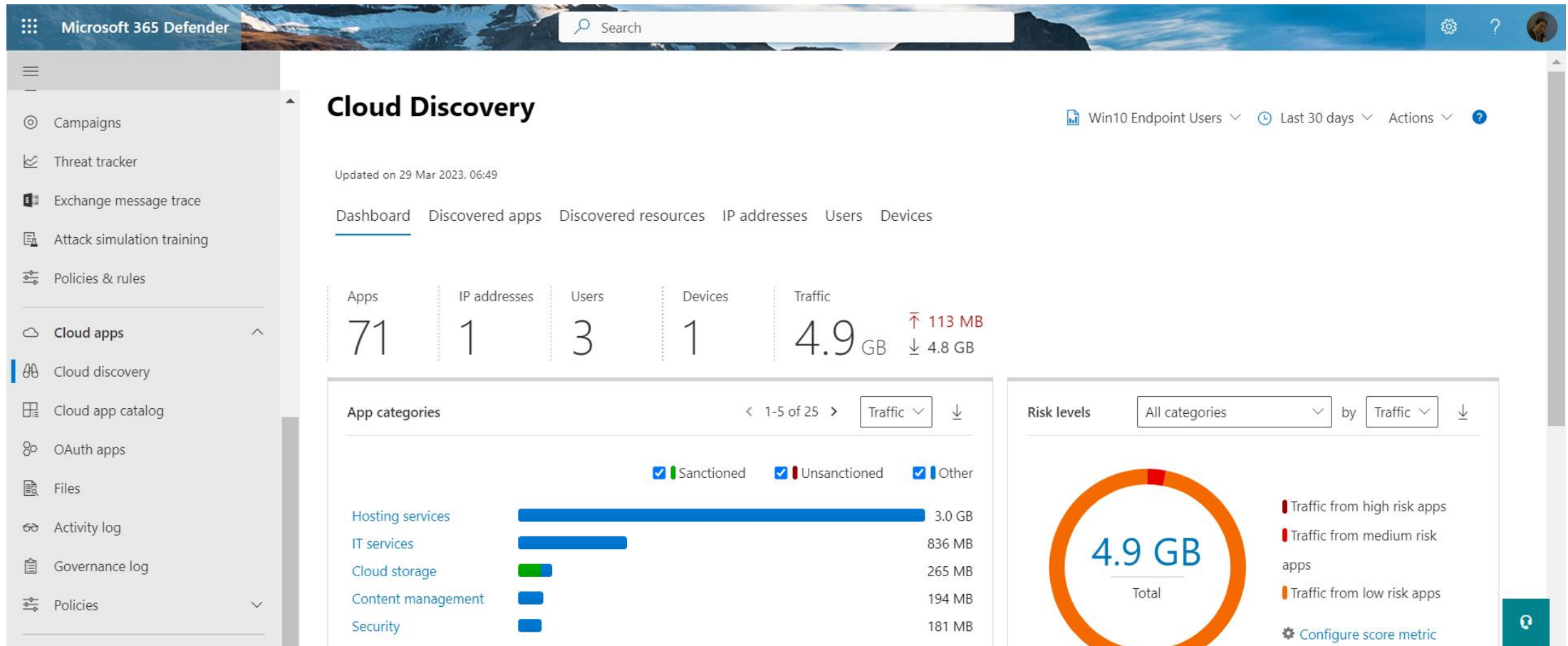
- Discover and control the use of Shadow IT
- Protect your sensitive information anywhere in the cloud
- Protect against cyberthreats and anomalies
- Assess the compliance of your cloud apps

Microsoft Defender for Cloud Apps architecture enables:

- Cloud Discovery
- Sanctioning and unsanctioning an app
- App connectors
- Conditional Access App Control protection
- Policy control



# Explore Microsoft Defender for Cloud Apps



# Cloud discovery

Microsoft 365 Defender

Search

Cloud Discovery

Win10 Endpoint Users Last 30 days Actions

Updated on 29 Mar 2023, 06:49

Dashboard Discovered apps Discovered resources IP addresses Users Devices

Queries: Select a query Save as Advanced filters

Apps: App tag: Sanctioned Unsanctioned None Risk score: 0 4

Compliance risk factor: Select factors Security risk factor: Select factors

Browse by category:

Advertising 2

Data analytics 1

1 - 3 of 3 discovered apps

	Risk score	Tags	Traf...	Upl...	Tran...	Users	IP a...	Devices	Last...	Actions
<input checked="" type="checkbox"/>	4		50 KB	—	1	1	1	1	28 Ma...	✓ ✕ ⋮
<input type="checkbox"/>	4		26 KB	—	1	1	1	1	28 Ma...	✓ ✕ ⋮
<input type="checkbox"/>	4		972 KB	39 KB	3	1	1	1	28 Ma...	✓ ✕ ⋮

# Cloud discovery

Microsoft 365 Defender

Search

Campaigns

Threat tracker

Exchange message trace

Attack simulation training

Policies & rules

Cloud apps

Cloud discovery

Cloud app catalog

OAuth apps

Files

Activity log

Governance log

Policies

Policy management

Policy templates

Reports

Activity log

Investigate 6 months back

To improve performance, the Activity Log now displays activities from the last 30 days. It is possible to display more than 30 days of activities in the Investigate the last 6 months option. [Learn more](#)

Queries: Select a query

Save as

Advanced filters

App: Select apps

User name: Select users

Raw IP address: Enter IP address

Activity type: Select value

Location: Select countries/regions

+ New policy from search

Export

1 - 20 of 23 activities

Show details

Hide filters

Table settings

Activity	User	App	IP address	Location	Device	Date
Log on	Beata Zalewa	Microsoft De...	109.243.142.230	Poland		30 Mar 2023 10:01
Log on	Beata Zalewa	Microsoft De...	109.243.142.230	Poland		30 Mar 2023 08:41
Log on	Beata Zalewa	Microsoft De...	109.243.142.230	Poland		29 Mar 2023 20:20
Log on	Beata Zalewa	Microsoft De...	109.243.142.230	Poland		29 Mar 2023 19:00
Log on	Beata Zalewa	Microsoft De...	109.243.142.230	Poland		11 Mar 2023 08:25
Log on	Beata Zalewa	Microsoft De...	109.243.142.230	Poland		11 Mar 2023 06:21
Log on	Beata Zalewa	Microsoft De...	109.243.142.230	Poland		10 Mar 2023 22:51
Log on	Beata Zalewa	Microsoft De...	109.243.142.230	Poland		10 Mar 2023 21:30

Discover and investigate



**DEMO 4**



**Cloud discovery**



# Policies and templates

Policy and templates are used to create alert definition and generation. And this is really the key point, why we are doing this.

Difference between a policy and a template:

**Policies** - are active templates that will produce alerts

**Templates** - are blueprints that can be used to create policies

Microsoft 365 Defender

Search

Cloud discovery

Cloud app catalog

OAuth apps

Files

Activity log

Governance log

Policies

Policy management

Policy templates

Reports

Audit

Health

Permissions

Settings

More resources

Azure AD identity protection policies have been removed from the Defender for Cloud Apps policy list. To configure alerts from these policies, [edit the global alert service settings](#)

The Alerts/SMS (text messages) has been deprecated. If you would like to receive text alerts, you should use Microsoft Power Automate for custom alert automation. For more information, see [Integrate with Microsoft Power Automate for custom alert automation](#).

Customize alerts and actions by creating policies: [Create policy](#)

Threat detection

Information protection

Conditional access

Shadow IT

All policies

Filters:

Name:

Type: 

Select type

Status: 

ACTIVE

DISABLED

Severity:

Category: 

Select risk category

Advanced filters

+ Create policy

↓ Export

1 - 20 of 33 Policies 

Hide filters

Table settings

Policy	Count	Severity	Category	Action	Modified
<div><div></div><div>Suspicious inbox manipulation rule</div><div>This policy profiles your environment and triggers alerts when suspic...</div></div>	0 open alerts	<div></div> <div>High</div>	<div></div> Threat detection	<div></div>	20 Mar 2023
<div><div></div><div>Ransomware activity</div><div>This policy profiles your environment and triggers alerts when an act...</div></div>	0 open alerts	<div></div> <div>High</div>	<div></div> Threat detection	<div></div>	20 Mar 2023

# Policies



Cloud discovery

Cloud app catalog

OAuth apps

Files

Activity log

Governance log

Policies

Policy management

Policy templates

Reports

Audit

Health

Permissions

Settings

More resources

## Policy templates















Filters:

☐ Advanced filtersType: **Select type** ▾

Severity:

Name: Category: **Select risk category** ▾1 - 20 of 37 Templates [Hide filters](#) [Table settings](#) ▾

Template	Severity ▾	Linked policies	Published	
 <b>Logon from a risky IP address</b> Alert when a user logs on to your sanctioned apps from a risky IP address. By default, the Risky L...	 High	0	19 Mar 2023 08:15	+
 <b>Administrative activity from a non-corporate IP address</b> Alert when an admin user performs an administrative activity from an IP address that is not inclu...	 High	0	19 Mar 2023 08:15	+
 <b>Potential ransomware activity</b> Alert when a user uploads files to the cloud that might be infected with ransomware.	 High	0	19 Mar 2023 08:15	+
 <b>Block upload of potential malware (based on Microsoft Threat Intelligence)</b> Alert when a user uploads files to the cloud that might be infected with malware based on Micr...	 High	0	19 Mar 2023 08:15	+
 <b>Block download of potential malware (based on Microsoft Threat Intelligence)</b> Alert when a user downloads files to the cloud that might be infected with malware based on Mi...	 High	0	19 Mar 2023 08:15	+
 <b>File shared with unauthorized domain</b> Alert when a file is shared with an unauthorized domain (such as your competitor).	 High	0	19 Mar 2023 08:15	+



# Policy templates



**DEMO 5**



**Policies**

Deploying Microsoft Defender for Cloud Apps requires the following tasks:

1. **Set instant visibility, protection, and governance actions for your apps (Required).** Connect apps to Microsoft Defender for Cloud Apps.
2. **Protect sensitive information with DLP policies (Recommended).** Enable file monitoring and create file policies.
3. **Control cloud apps with policies (Required).** Policies enable organizations to create governance actions and set data loss prevention and file-sharing controls.
4. **Set up Cloud Discovery (Required).** Enables Microsoft Defender for Cloud Apps to view your cloud app use.
5. **Deploy Conditional Access App Control for catalog apps (Recommended).** Access and session controls in Microsoft Defender for Cloud Apps work with both custom applications and apps from the Cloud app catalog.
6. **Personalize your experience (Recommended).** Customize email settings, set admin notifications, and customize the score metrics.
7. **Organize the data according to your needs (Recommended).** Create IP address tags and continuous reports and add domains for business units.

# Deploy Microsoft Defender for Cloud Apps



Policies allow you to define the way you want your users to behave in the cloud

---



There are multiple types of policies that correlate to the different types of information you want to gather about your cloud environment and the types of remediation actions you may want to take

---



**The Microsoft Defender for Cloud Apps engine combines three aspects under each policy:**

- Content scan based on preset templates or custom expressions
- Context filters
- Automated actions for governance and remediation

## Configure file policies in Microsoft Defender for Cloud Apps

**Cloud Discovery analyzes traffic logs against the Microsoft Defender for Cloud Apps catalog of over 25,000 cloud apps**

The apps are ranked and scored based on more than 90 risk factors

Provides ongoing visibility into cloud use, Shadow IT, and the risk Shadow IT poses into an organization

**Organizations can generate the following types of reports in Cloud Discovery:**

- Snapshot reports
- Continuous reports
- Reports created using the Cloud Discovery API

**The process of generating a risk assessment consists of the following steps:**

1. Upload web traffic logs from your network
2. Parse traffic data from the traffic logs
3. Analyze the traffic data
4. Generate a risk assessment report

# Configure Cloud Discovery in Microsoft Defender for Cloud Apps

# Troubleshoot Cloud Discovery in Microsoft Defender for Cloud Apps

Microsoft Defender for Endpoint integration

Log parsing errors

Log collector errors

Discovery dashboard errors



# Thank you 😊

## Used resources:

<https://learn.microsoft.com/en-us/defender-cloud-apps/>

<https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-cloud-apps/ba-p/2835842>

<https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad>

<https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>

<https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad>

<https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-aad>

<https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-any-app>

<https://www.aka.ms/mcaslicensing>

<https://learn.microsoft.com/en-us/defender-cloud-apps/editions-cloud-app-security-o365>

# Q & A

Email: [info@zalnet.pl](mailto:info@zalnet.pl)

Demo:

<https://github.com/beatazalewa/ExpertSummit2023>

Thank you for your precious time 😊