App Governance in Microsoft Defender for Cloud Apps

Beata Zalewa

zalnet

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

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

WWW: https://beatazalewa.com/

zalnet

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)

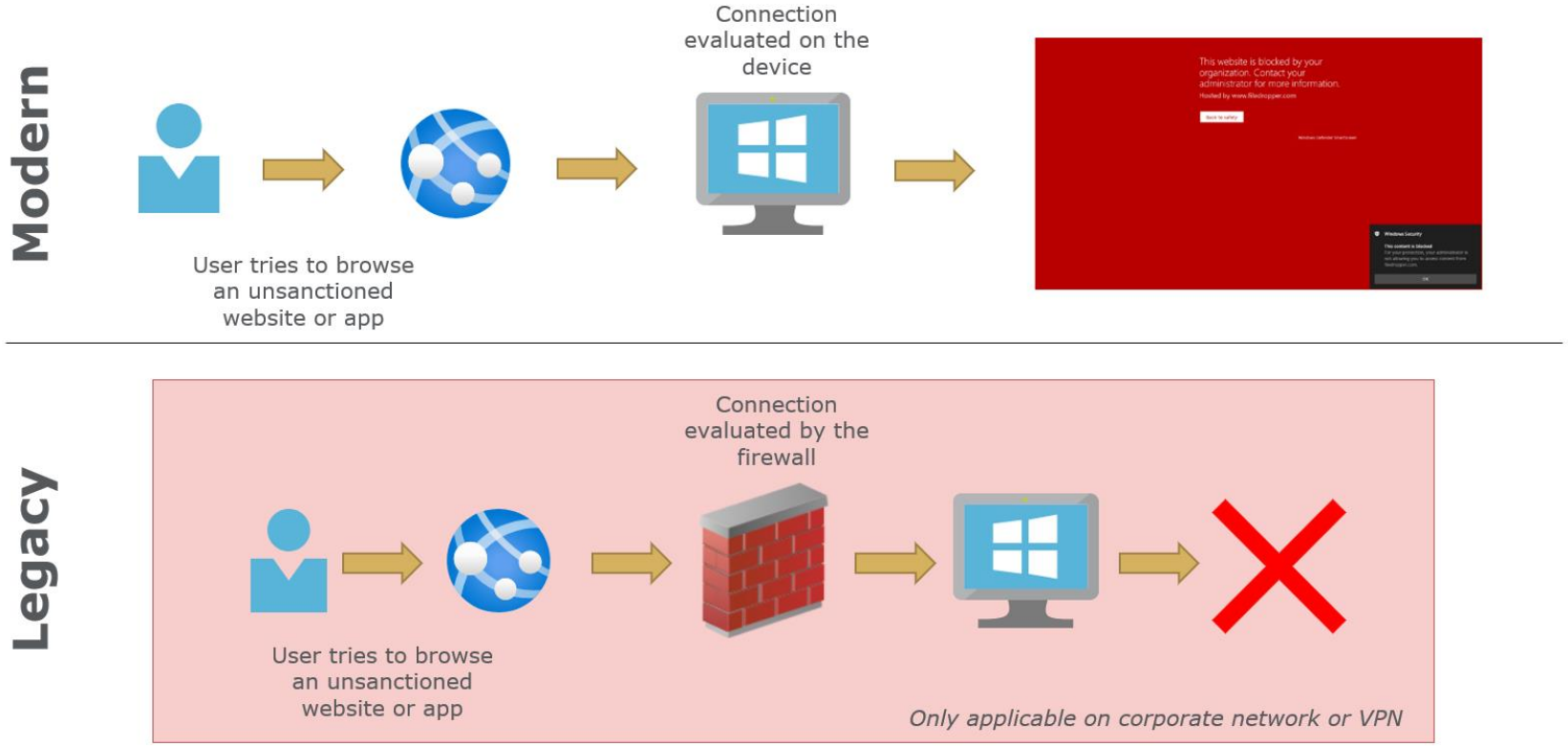
Decentralized / cloud-based solution where the security perimeter is built-in the Defender Suite

zalnet

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)

- 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.

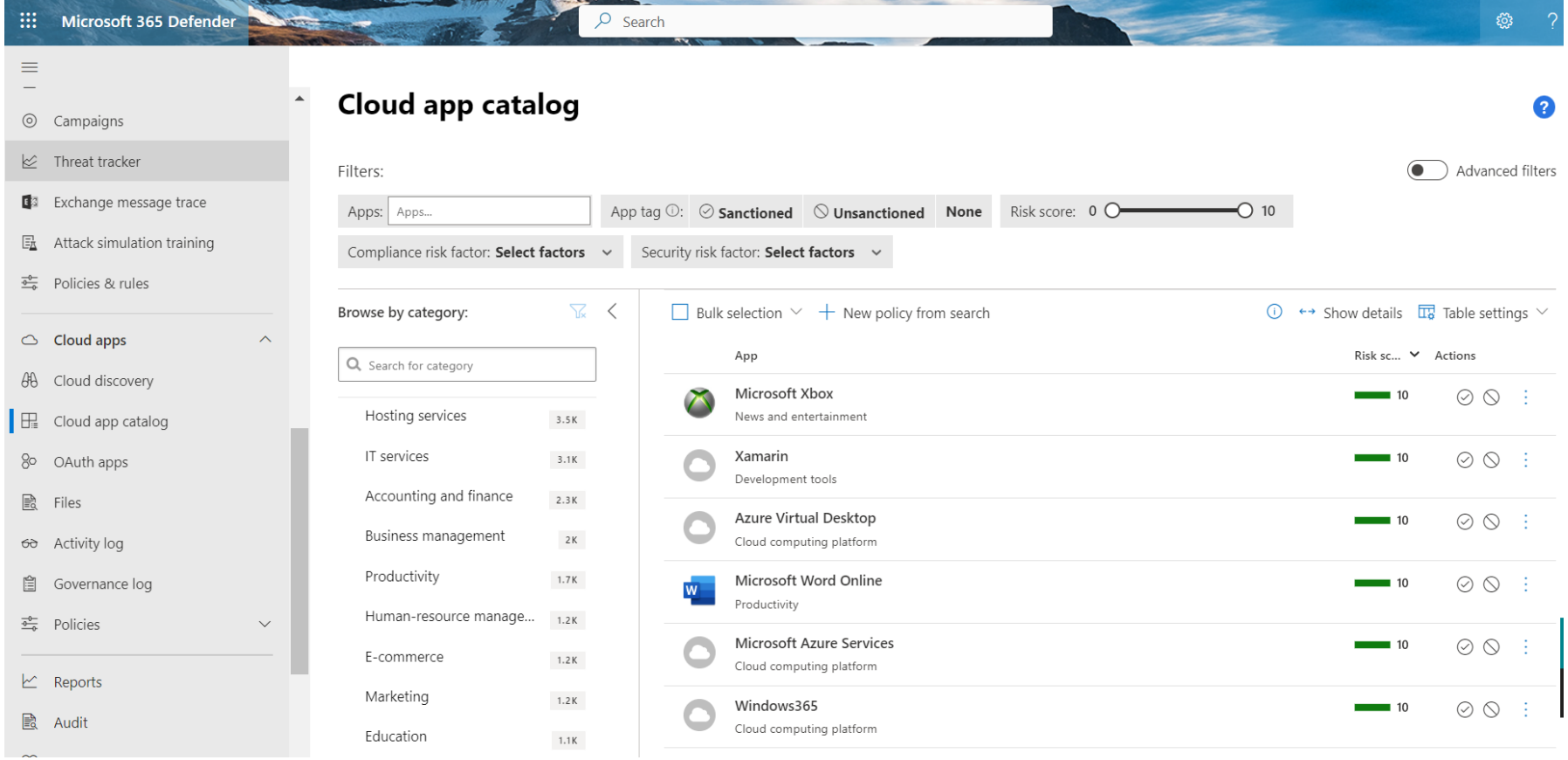
https://aka.ms/M365EnterprisePlans

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.

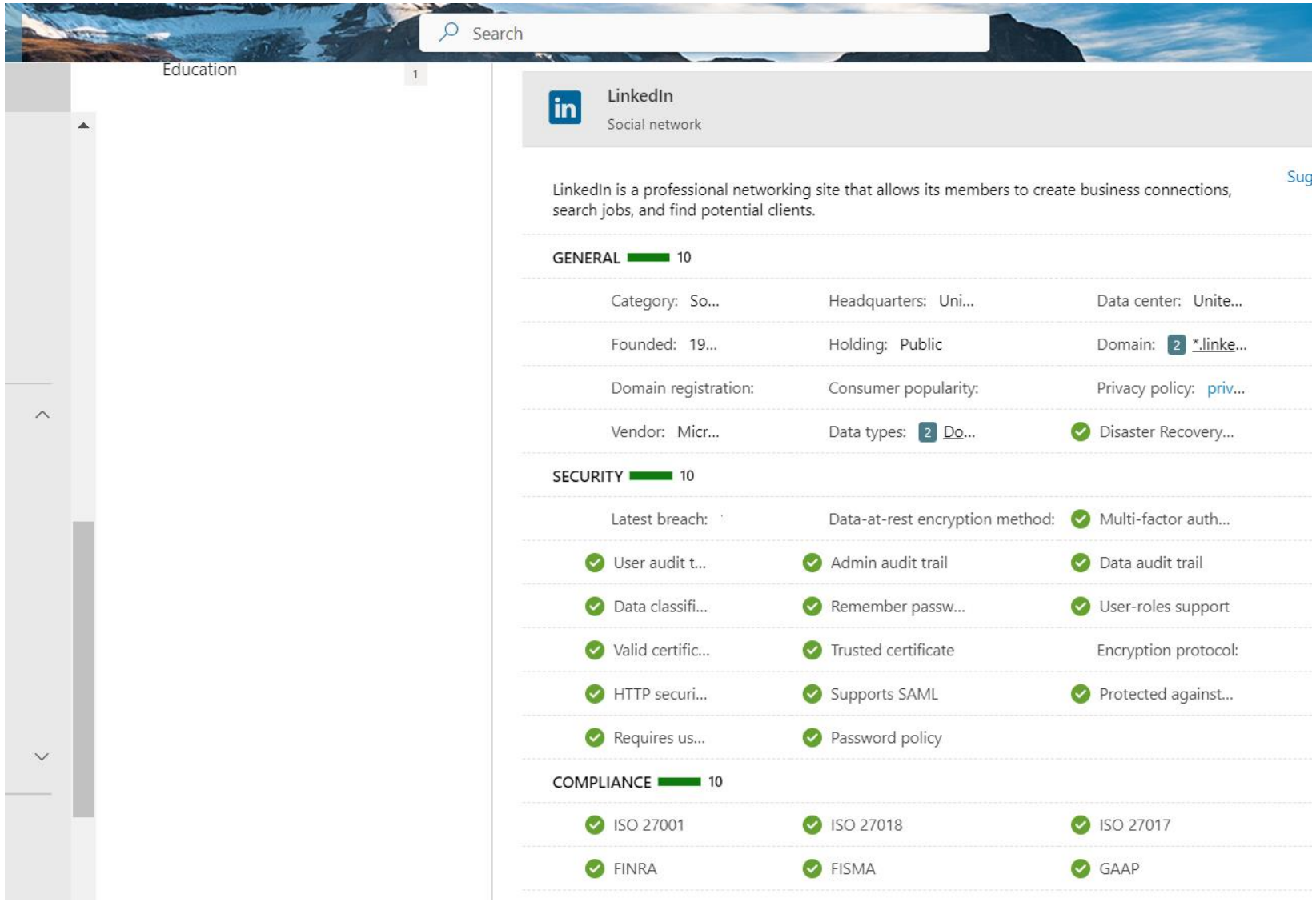


Cloud App catalog

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.



Demo 1

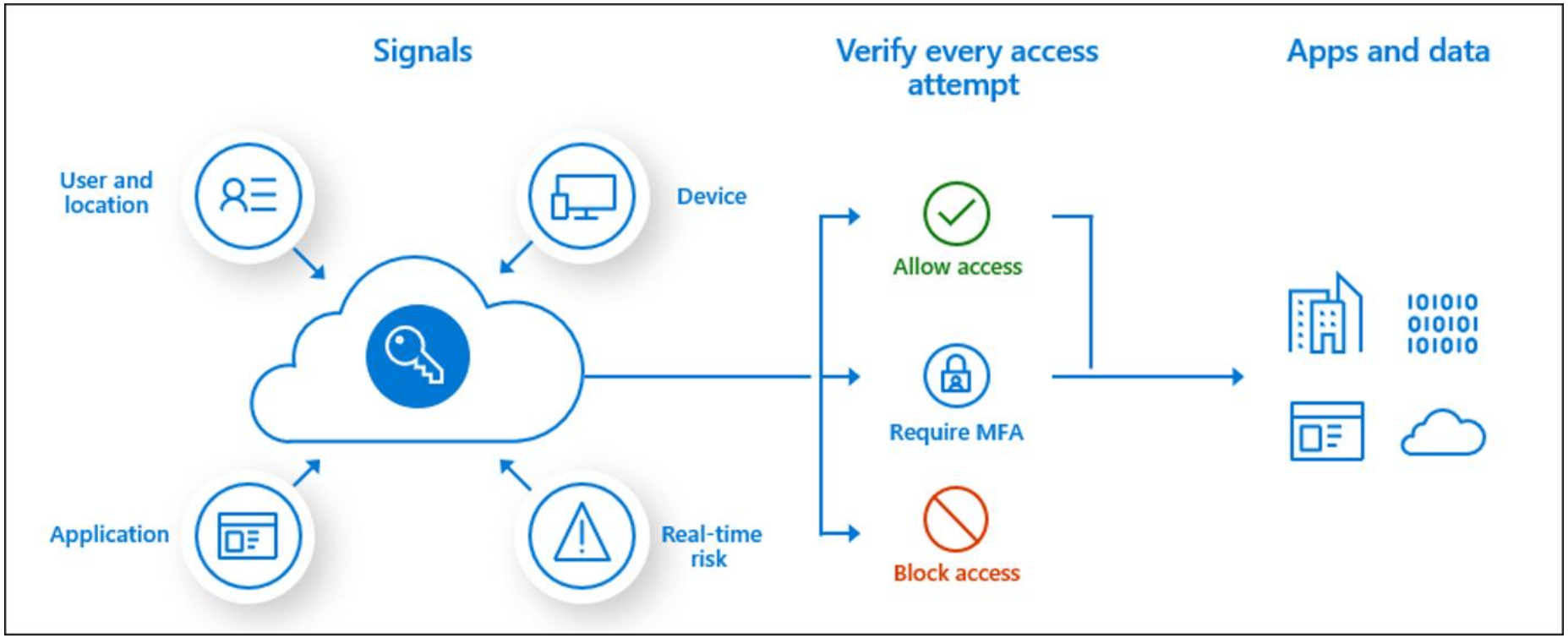
How to make it work

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

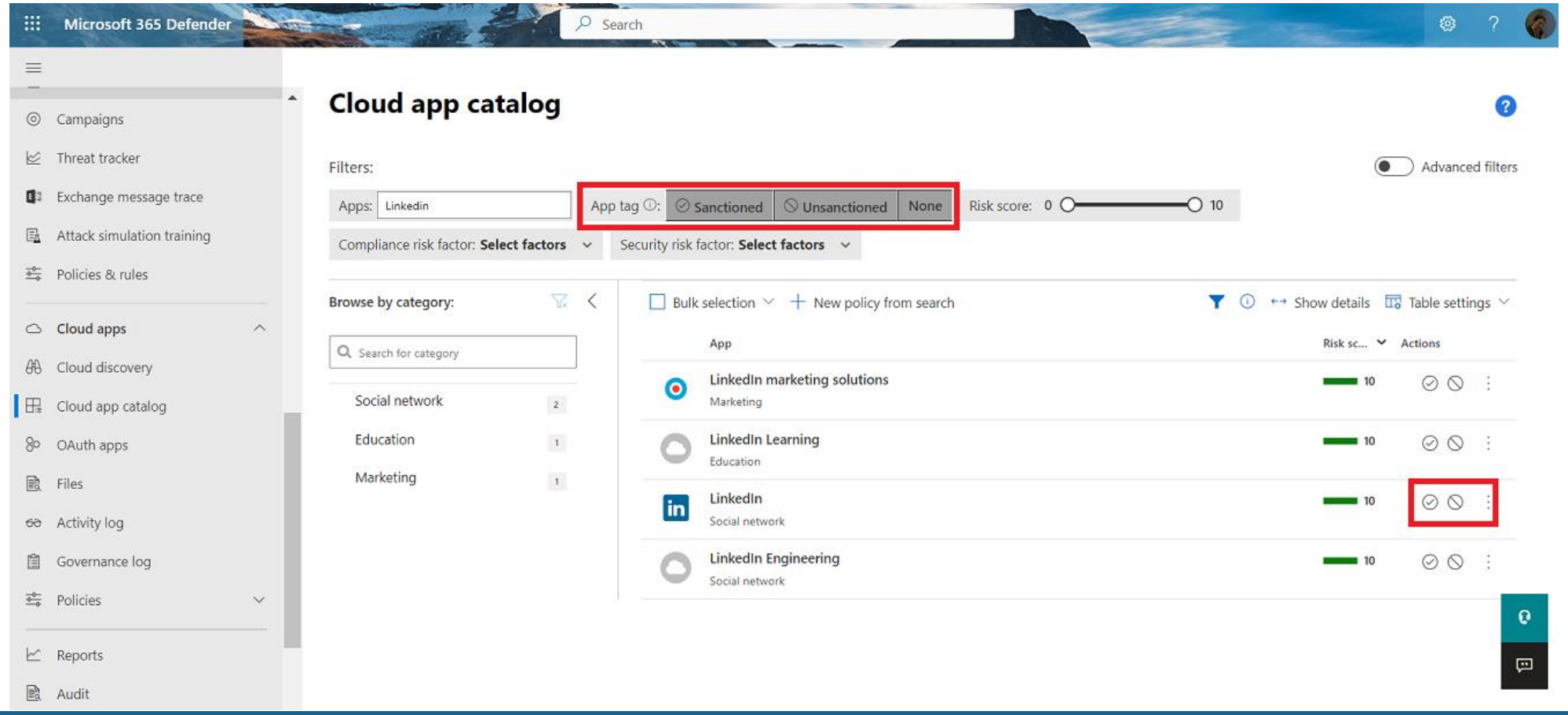
Apps can be tagged as:

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
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
Reports
Audit
Cloud app catalog
Filters:
Advanced filters
Apps: Linkedin
App tag: Sanctioned Unsanctioned None
Risk score: 0 10
Compliance risk factor: Select factors
Security risk factor: Select factors
Browse by category:
Search for category
Social network 2
Education 1
Marketing 1
Bulk selection
New policy from search
Show details
Table settings
App
Risk sc...
Actions
LinkedIn marketing solutions
Marketing
10
LinkedIn Learning
Education
10
LinkedIn
Social network
10
LinkedIn Engineering
Social network
10

App tags

DEMO 2

App tags

App risks score

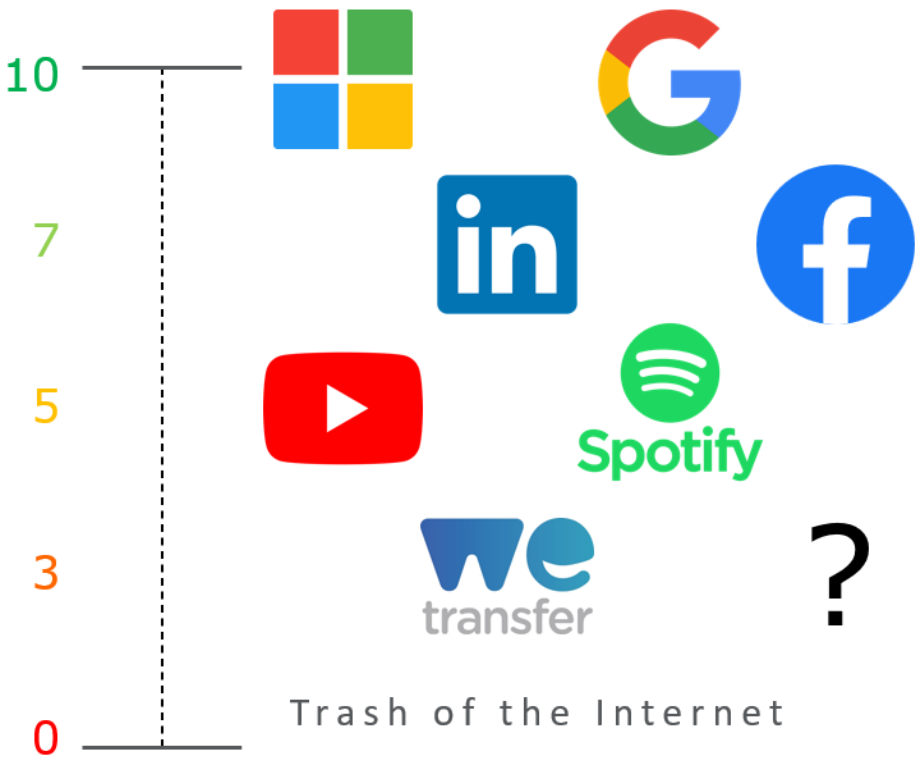
Each cloud app is rated by Microsoft by an individual risk score to:

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

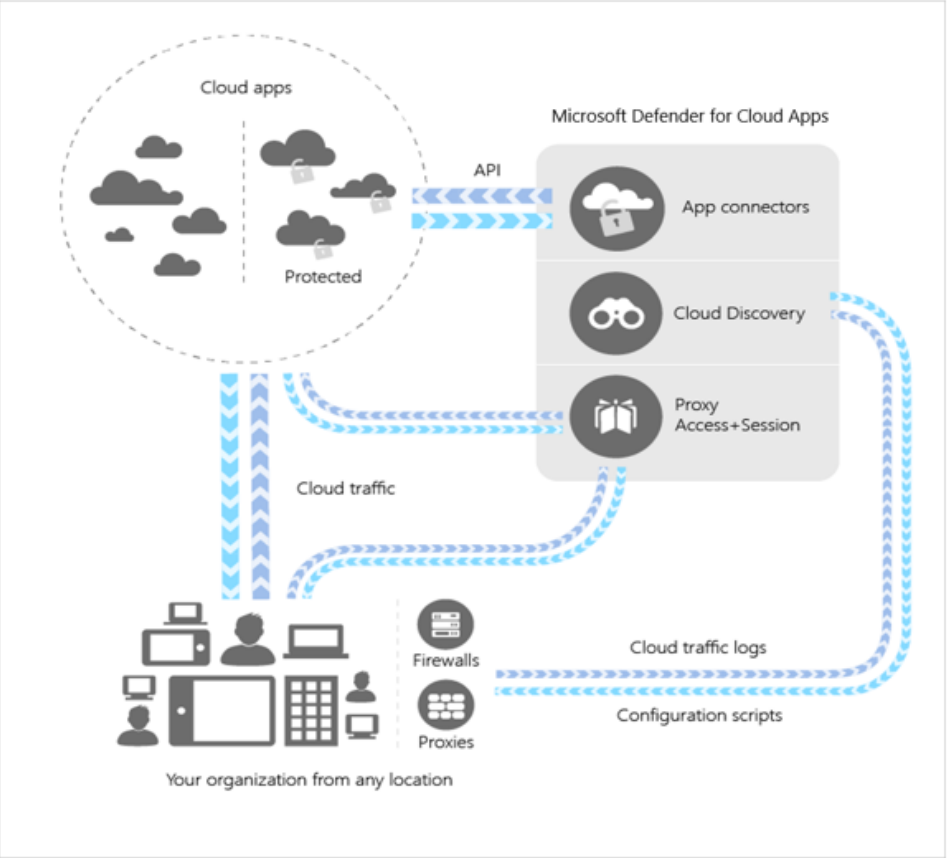
App risks score

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

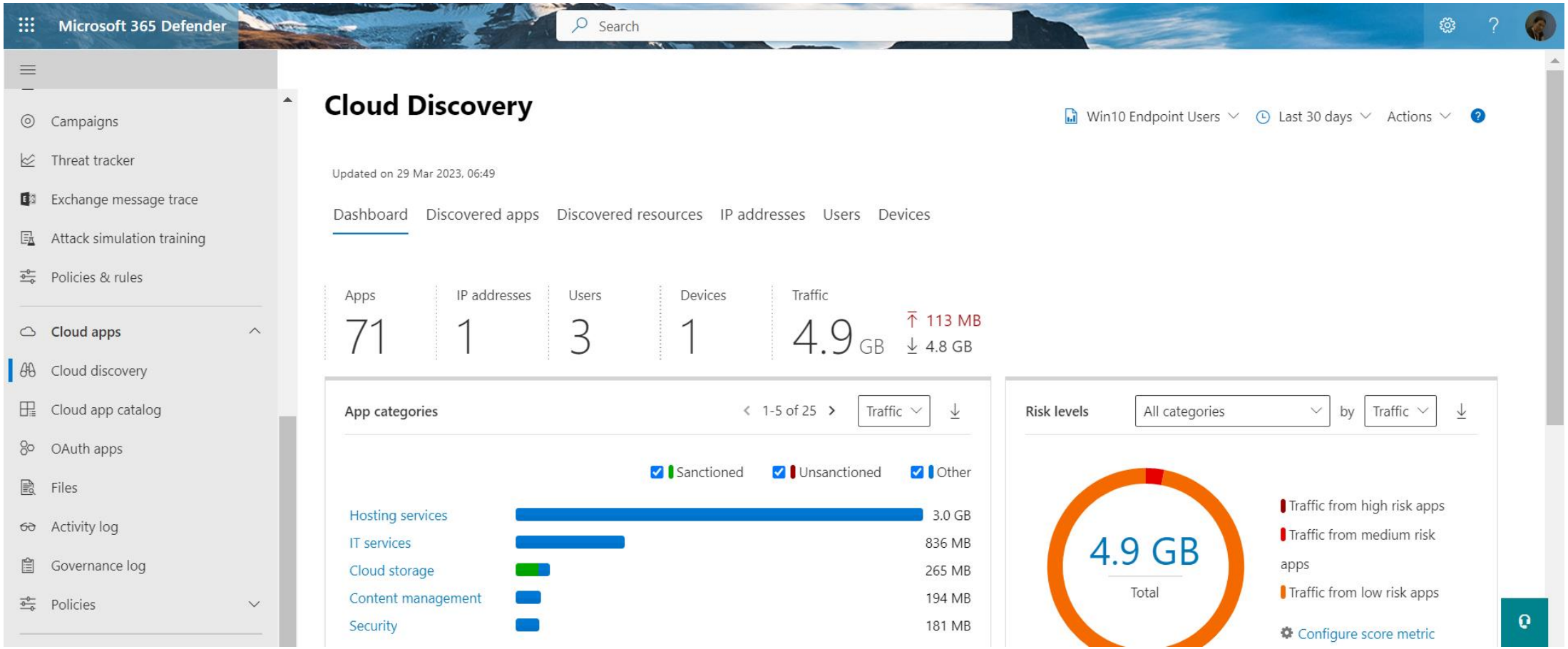
- Discover and control the use of Shadow IT
- Protect your sensitive information anywhere in the cloud
- Protect against cyberthreats and anomalies
- Assess the compliance of your cloud apps

Microsoft Defender for Cloud Apps architecture enables:

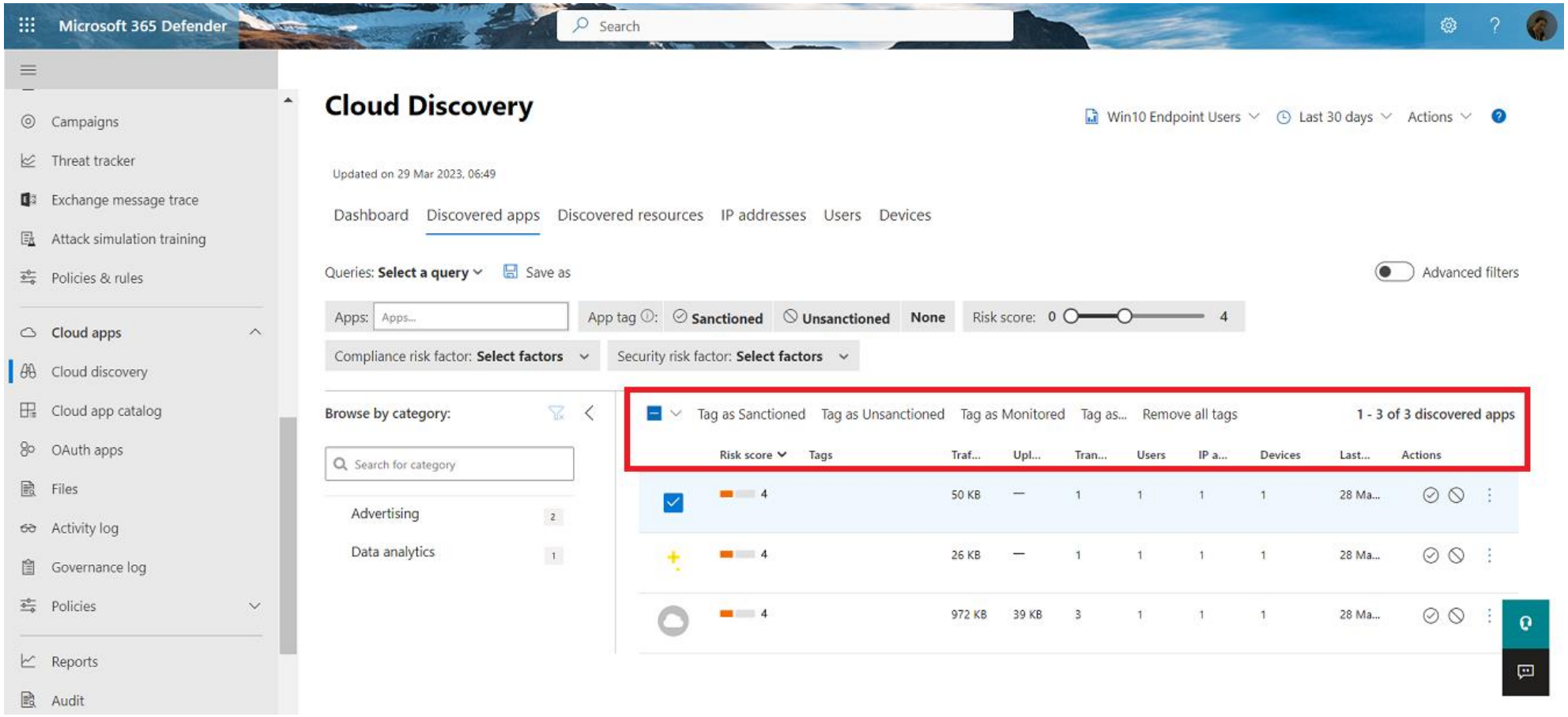
- Cloud Discovery
- Sanctioning and unsanctioning an app
- App connectors
- Conditional Access App Control protection
- Policy control



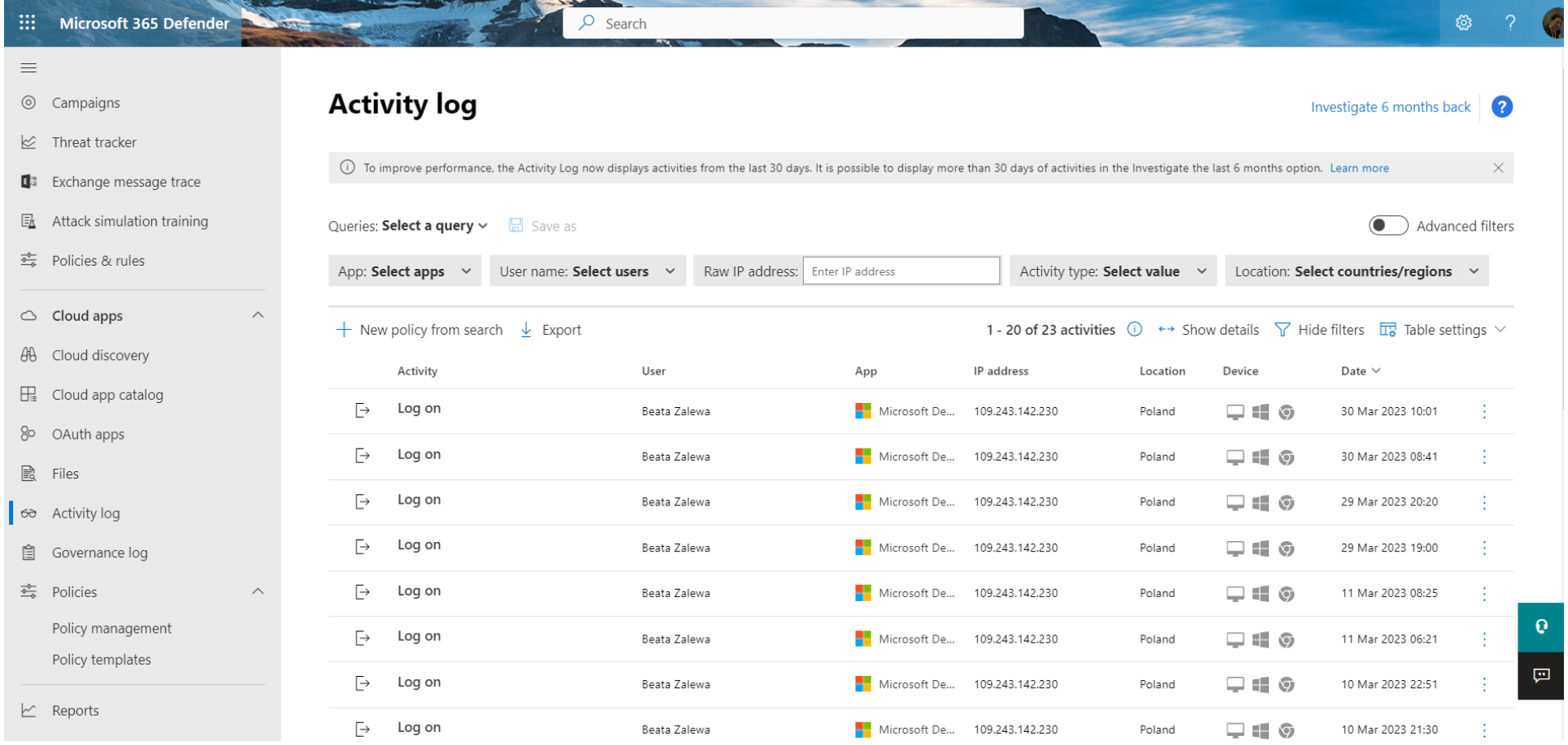
Explore Microsoft Defender for Cloud Apps



Cloud discovery



Cloud discovery



Discover and investigate

DEMO 4

Cloud discovery

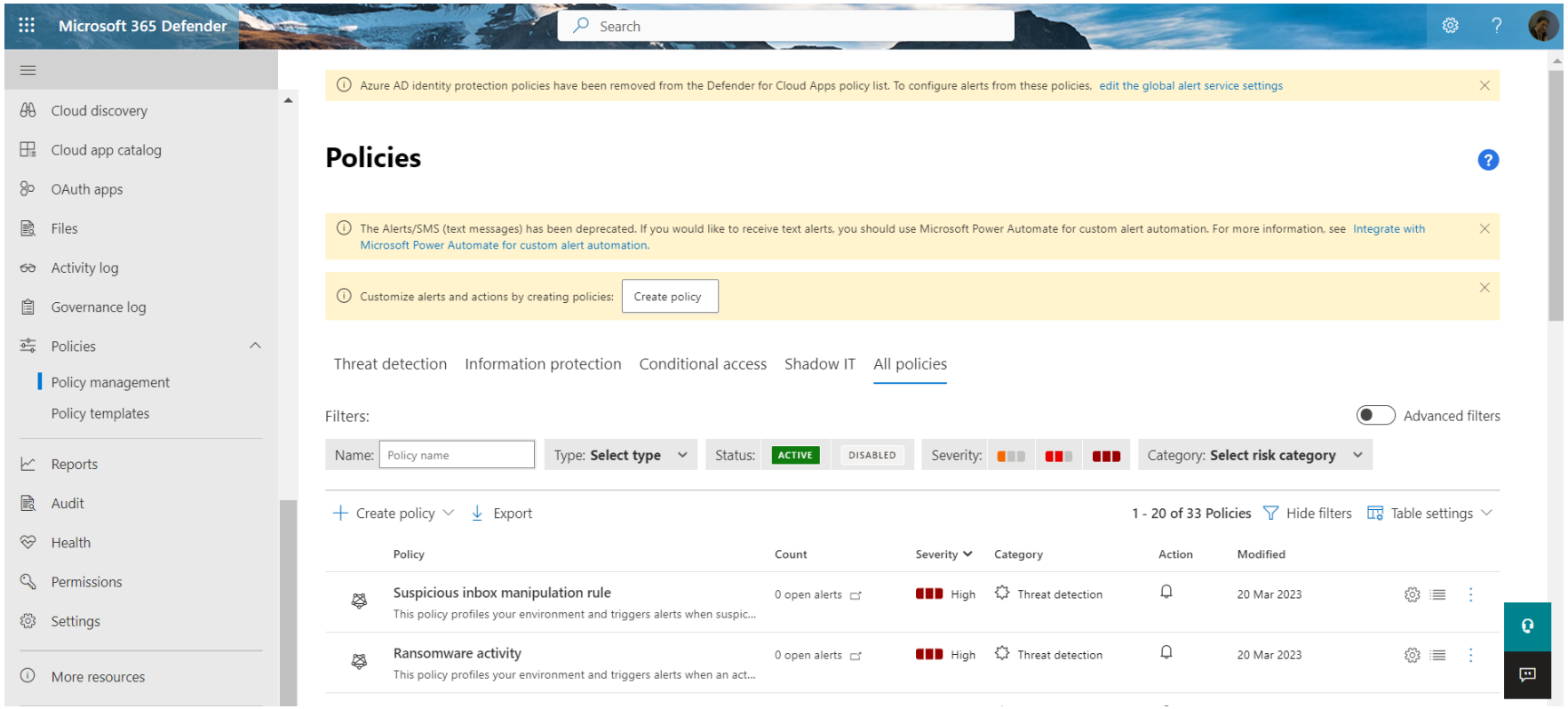
Policies and templates

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

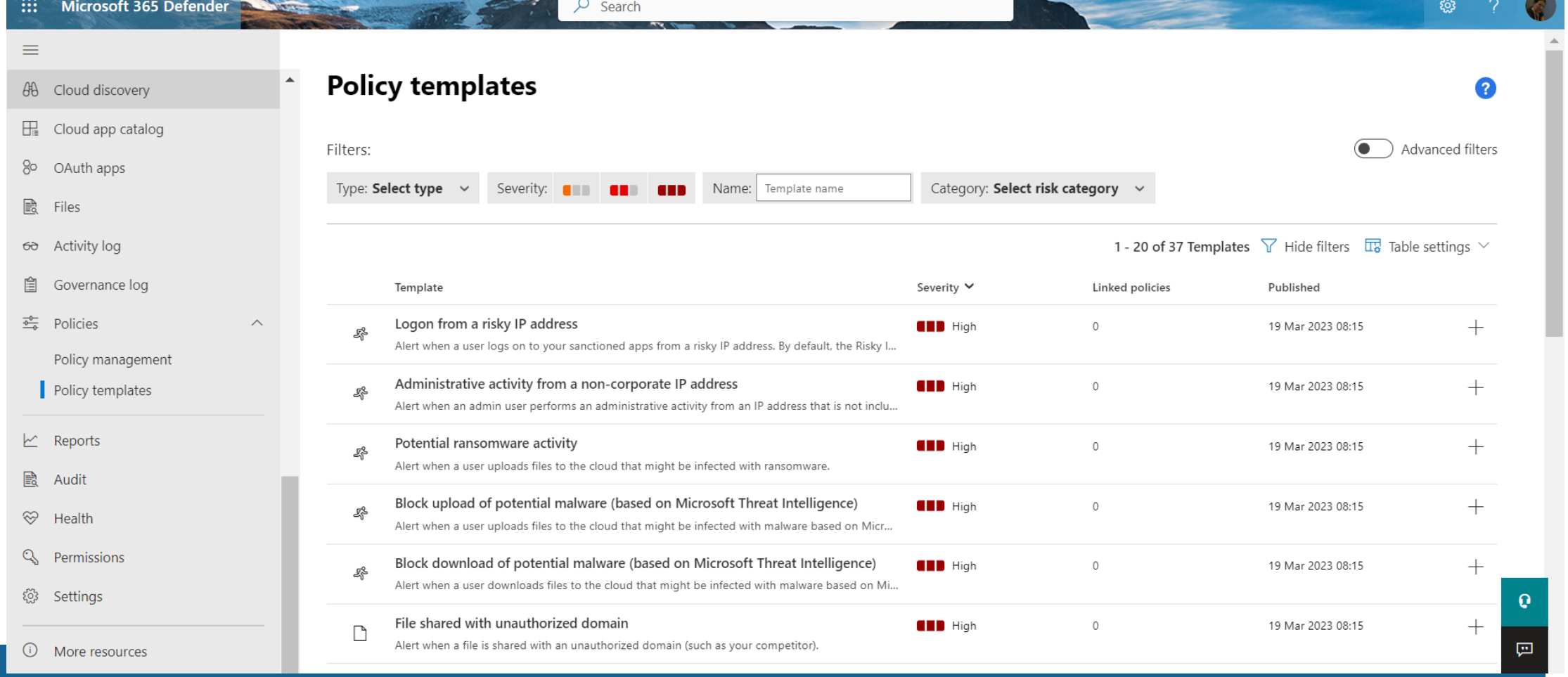
Difference between a policy and a template:

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
Policies
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:
Advanced filters
Name:
Policy name
Type: Select type
Status:
ACTIVE
DISABLED
Severity:
Category: Select risk category
Create policy
Export
1 - 20 of 33 Policies
Hide filters
Table settings
Policy
Count
Severity
Category
Action
Modified
Suspicious inbox manipulation rule
This policy profiles your environment and triggers alerts when suspic...
0 open alerts
High
Threat detection
20 Mar 2023
Ransomware activity
This policy profiles your environment and triggers alerts when an act...
0 open alerts
High
Threat detection
20 Mar 2023

Policies



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

Demo:

https://github.com/beatazalewa/ExpertSummit2023

Thank you for your precious time☺

zalnet