

# Protect all your cloud apps with Azure AD and Cloud App Security

10.2.2021

# Markus Lintuala

*Public Cloud and Microsoft 365  
Hero @ Elisa Oyj*

- 11+ yrs in 
- 7+ yrs in 
- Currently working much with modern public cloud security solutions 



Lintuala



MarkusLintuala



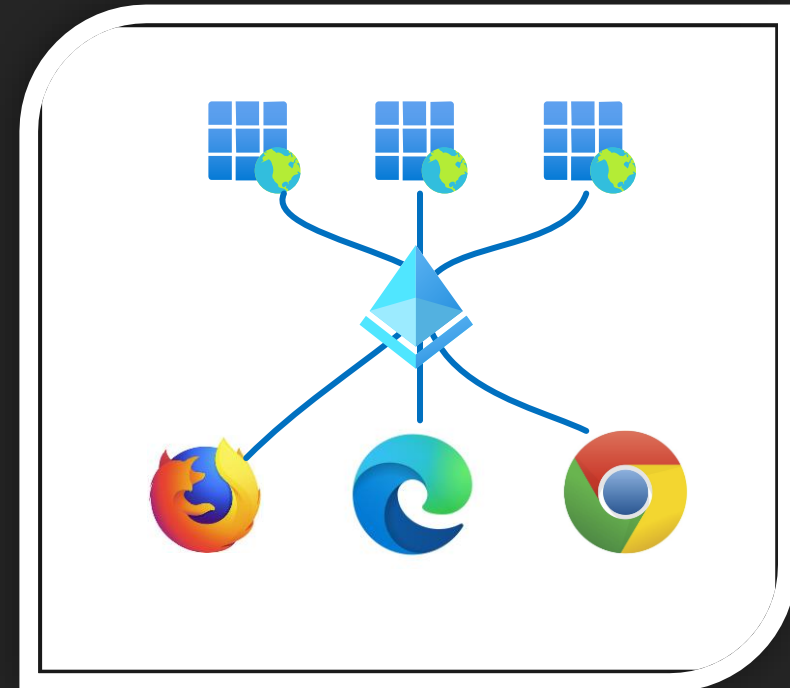
bloggerz.cloud

# Agenda

- What kind of applications we are interested in?
- Centralized Identity
- Types of application publishing
- What is Cloud App Security
- What is access and session controls
- Application management in Cloud App Security
- Where to start?
- What I suggest not to do 😊

# What kind of cloud application we are interested in?

- Uses your company identities
- Used with a browser
- Can be accessed from the internet



# Benefit of centralized identity



- Only one identity for all cloud applications
- Much easier and safer for end user
- End-user authenticates once to Azure AD
- Centralized security

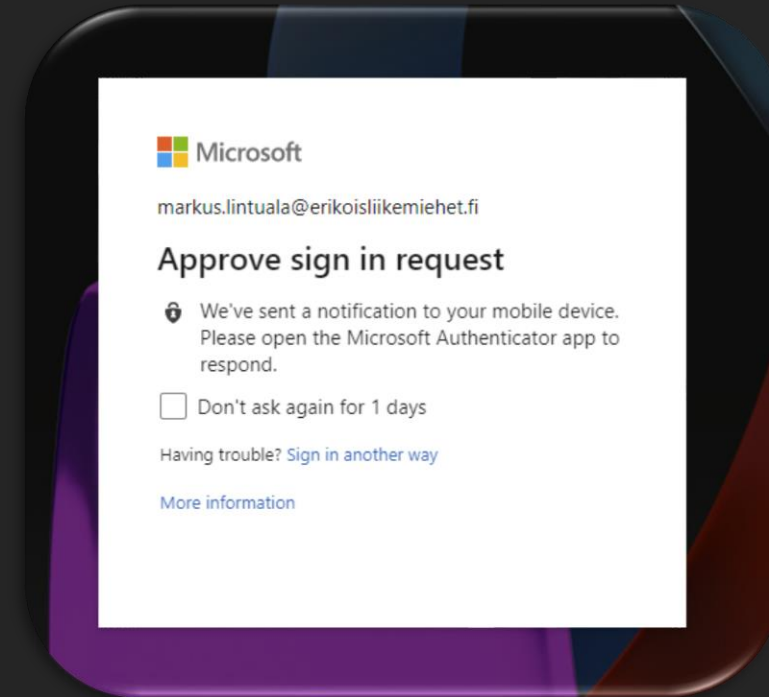
# Security perspective of centralized identity

- Centralized identity protection (Conditional Access, MFA, Identity Protection etc.)
- Centralized logging
- Single-sign-on capabilities
- No need to trust for external authentication providers
- Make any app authentication *passwordless*



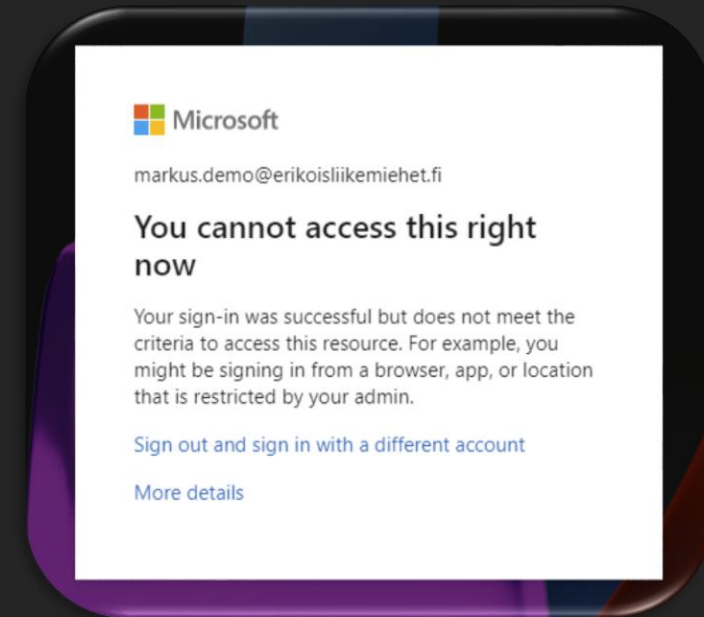
# Traditional application publishing

- With or without MFA
- Access allowed from unmanaged device
- Risk for data leakage
- No control or monitor for anything that is happening in session



# Secure application publishing

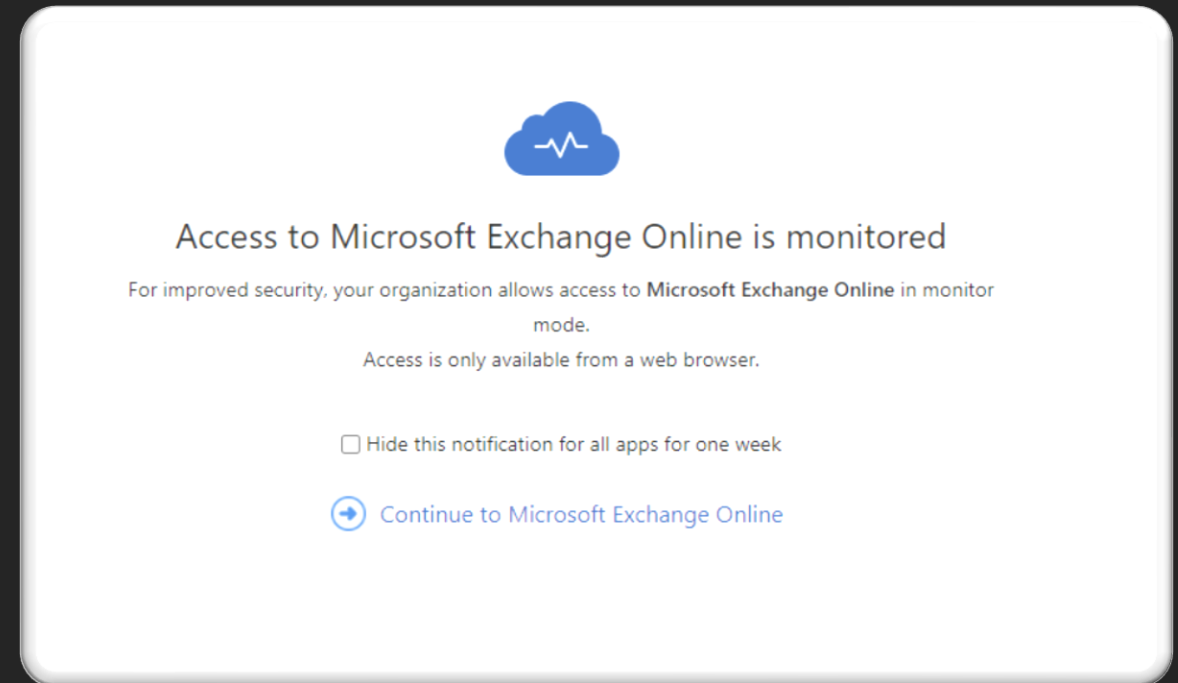
- Conditional access blocks sessions from unmanaged devices
- Secure, but not as productive
- No support for BYOD or Zero Trust scenarios



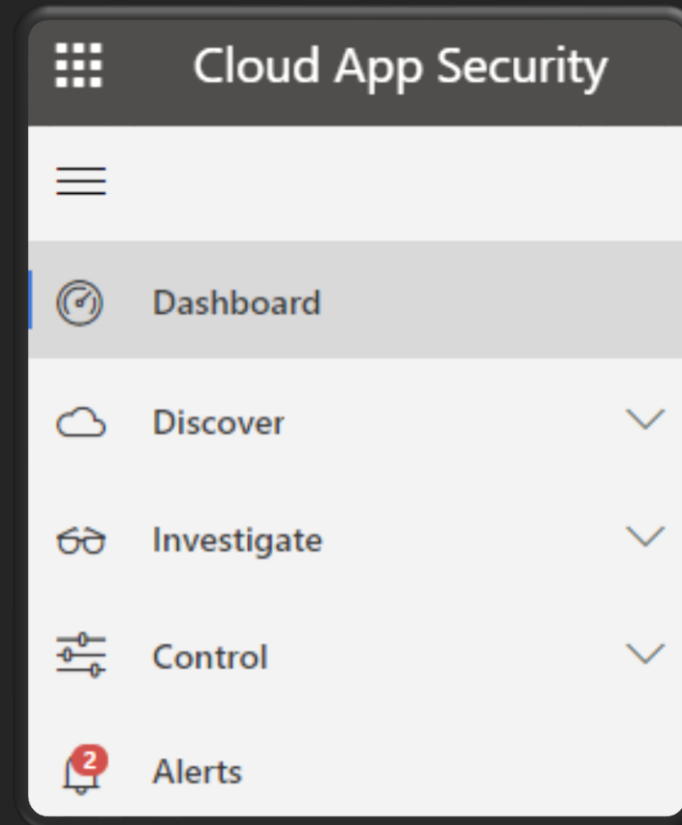


# Modern application publishing

- Enable productive and secure access for cloud applications
- Monitor and control sessions on unmanaged devices
- Reduce data leakage risk with download encryption or download block

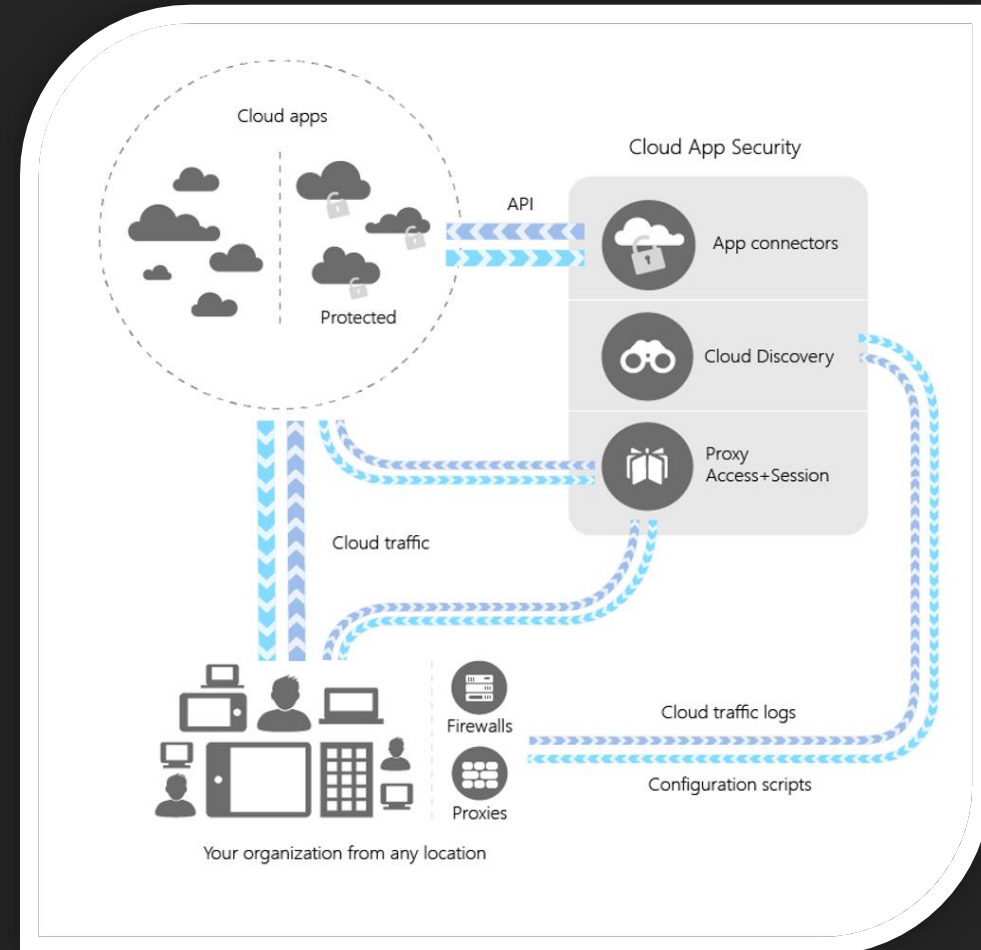


# Cloud App Security



# What is Cloud App Security

- Cloud Access Security Broker (CASB)
- Can be integrated with several identity providers
- Centralizes user activity for UEBA and threat protection



# Access control redirection to Cloud App Security

### MCAS Demo

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

MCAS Demo

#### Assignments

Users and groups ⓘ >

Specific users included

Cloud apps or actions ⓘ >

1 app included

Conditions ⓘ >

1 condition selected

#### Access controls

Grant ⓘ >

1 control selected

Session ⓘ >

Use Conditional Access App Cont...

### Session

Control user access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

☐ Use app enforced restrictions ⓘ

☒ Use Conditional Access App Control ⓘ

Use custom policy... ^

Monitor only (Preview)

Block downloads (Preview)

Use custom policy...

app. Click here to learn more about both scenarios.

[Configure custom policy](#)

☐ Sign-in frequency ⓘ

☐ Persistent browser session ⓘ

- Use conditional access to forward control to Cloud App Security
- Custom policy for more detailed control
- Session control available also built in in Exchange Online and SharePoint Online

# What is access control

- Is the device or user allowed to use application or not
- Custom policies allow to choose several conditions for access policy
- Supports browser and native applications

### Create access policy

Access policies provide you with real-time monitoring and control over user logins to your cloud apps.

Policy name \*

Policy severity \*      Category \*

☐ ☐ ☐ ☐ ☐

Access control

Description

activities matching all of the following [Edit and preview results](#)

Filters:

☐ Device

☐ Tag

☐ does not equal

☐ Intune compliant, Hybrid Azure AD joined

☐ App

☐ equals

☐ Office 365

[+ Add a filter](#)

### Actions

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

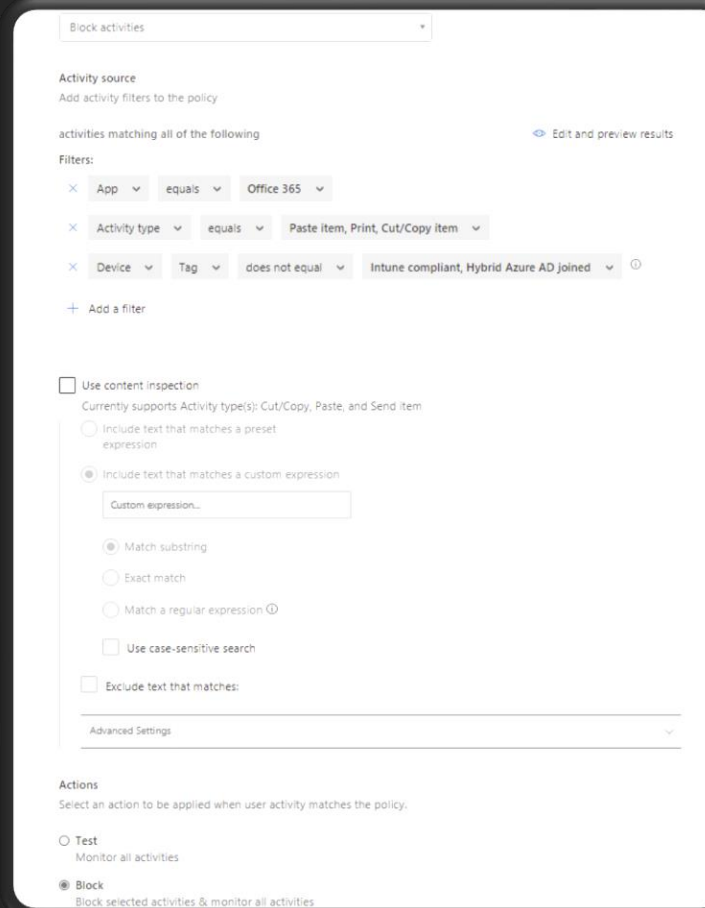
☐ Test  
Monitor login activities

☒ Block  
A default block message is displayed when possible

☐ Customize block message

# What is session control

- Controls in-session actions
- Block actions to reduce data leakage risk
- Supports **only** browser sessions



The screenshot shows the configuration for a 'Block activities' policy in Microsoft Intune. The 'Activity source' section indicates that the policy applies to activities matching all of the following filters. The filters are: App equals Office 365, Activity type equals Paste item, Print, Cut/Copy item, and Device Tag does not equal Intune compliant, Hybrid Azure AD joined. There is an option to 'Add a filter'. The 'Use content inspection' section is expanded, showing options to include text that matches a preset or custom expression. The 'Custom expression' field is empty, and the 'Match substring' option is selected. There are also options for 'Exact match', 'Match a regular expression', 'Use case-sensitive search', and 'Exclude text that matches'. The 'Advanced Settings' section is collapsed. The 'Actions' section shows two options: 'Test' (Monitor all activities) and 'Block' (Block selected activities & monitor all activities), with 'Block' being the selected action.

Block activities

Activity source  
Add activity filters to the policy

activities matching all of the following [Edit and preview results](#)

Filters:

- App equals Office 365
- Activity type equals Paste item, Print, Cut/Copy item
- Device Tag does not equal Intune compliant, Hybrid Azure AD joined

+ Add a filter

☐ Use content inspection  
Currently supports Activity type(s): Cut/Copy, Paste, and Send item

☐ Include text that matches a preset expression

☒ Include text that matches a custom expression

Custom expression...

☒ Match substring

☐ Exact match

☐ Match a regular expression ⓘ

☐ Use case-sensitive search

☐ Exclude text that matches:

Advanced Settings

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

☐ Test  
Monitor all activities

☒ Block  
Block selected activities & monitor all activities

# Actions in session control

**Activity source**  
Add activity filters to the policy

activities matching all of the following [Edit and preview results](#)

**Filters:**

- App equals Office 365
- Activity type equals Paste item, Print, Cut/Copy item
- Device Tag does not contain Microsoft Azure AD joined

+ Add a filter

☐ Use content inspection  
Currently supports Activity type(s): Cut, Copy, Paste, Print, Send

☐ Include text that matches a preset expression

**Actions:**

- ☒ Paste item
- ☒ Print
- ☒ Cut/Copy item
- ☐ Send item
- ☐ Send Teams message

# Actions in session control

**Session control type**  
Select the type of control you want to enable:

Control file download (with inspection) ▼

**Activity source**  
Add activity filters to the policy

activities matching all of the following [Edit and preview results](#)

Filters:

✕ App ▼ equals ▼ Office 365 ▼

✕ Device ▼ Tag ▼ does not equal ▼ Intune compliant, Hybrid Azure AD joined ▼ ⓘ

+ Add a filter

Add file filters to the policy

files matching all of the following

Filters:

✕ Classification label ▼ equals ▼ Highly Confidential-All Employees ▼

+ Add a filter



# Actions in session control

**Session control type**  
Select the type of control you want to enable:

Control file upload (with inspection) ▼

**Activity source**  
Add activity filters to the policy

activities matching all of the following [Edit and preview results](#)

Filters:

× App ▼ equals ▼ Office 365 ▼

× Device ▼ Tag ▼ does not equal ▼ Intune compliant, Hybrid Azure AD joined ▼ ⓘ

+ Add a filter

Add file filters to the policy

files matching all of the following

Filters:

Select a filter... ▼

+ Add a filter

**Inspection method**

Malware detection ▼

Detect threats using the following methods:

☒ Microsoft Threat Intelligence ⓘ

#NVSummit2021

# DEMO - Access Control and Session Control

**NORDIC**

— VIRTUAL SUMMIT —

# Recognizing device in Cloud App Security

**Activity source**  
Add activity filters to the policy

activities matching all of the following [Edit and preview results](#)

**Filters:**

✕ App equals Office 365

✕ Device Tag does not equal

Intune compliant, Hybrid Azure AD joined ⓘ

- ✓ Intune compliant
- ✓ Hybrid Azure AD joined
- Valid client certificate

**Device identification**

Create [access and session policies](#) based on device state, by identifying your managed devices.

**Intune compliant device identification**  
Identify devices that are considered Intune compliant by [Microsoft Intune](#). ⓘ  
Automatically synced with Microsoft Intune | [View configuration](#)

**Hybrid Azure AD joined identification**  
Identify devices that are hybrid Azure AD joined in your on-premises Active Directory and are registered with [Azure AD](#). ⓘ  
Automatically synced with Azure AD | [View configuration](#)

**Client certificate based identification**  
Identify managed devices by authenticating devices against client certificates.  
Upload your trusted root or intermediate certificate as a PEM file.

+ Add a root certificate

Name	Description	Issuer
Erikoisliikemiehet CA	—	—

☐ Require certificate revocation check: certificates that have been revoked by the CA will no longer be trusted. Note: A client certificate check requires the CRL protocol and applies to all certificates. If your client certificate does not contain a CRL endpoint, you will not be able to connect from managed devices.

[Save](#) We secure your data as described in our [privacy statement](#) and [online service terms](#).

# Using access and session control together



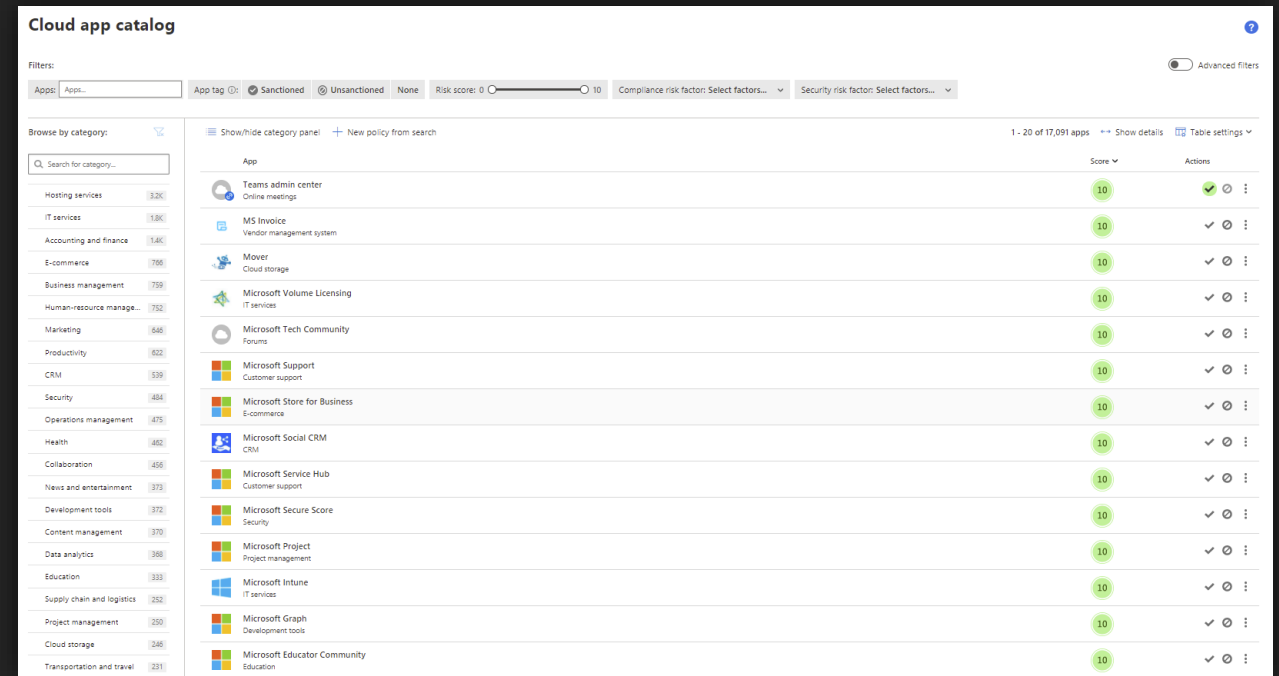
Access Control

The diagram features a large, light blue arrow pointing from left to right. Inside this arrow are two rounded rectangular boxes. The first box on the left is blue and contains the text 'Access Control'. The second box on the right is green and contains the text 'Session Control'.

Session Control

# Application managing in Cloud App Security

- Featured apps (currently 17 091 apps)
- Any other app
- If Azure AD used as IdP
  - SAML 2.0
  - OpenID Connect
- If another IdP used
  - SAML 2.0 supported

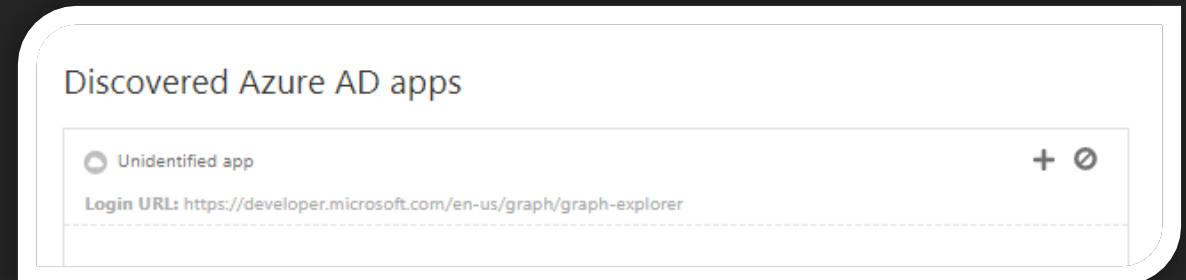


The screenshot shows the 'Cloud app catalog' interface. It features a search bar at the top with filters for 'App tag' (Sanctioned, Unsanctioned, None), 'Risk score' (0 to 10), and 'Compliance risk factor' and 'Security risk factor' dropdowns. Below the search bar, there's a 'Browse by category' section with a list of categories and their counts. The main table displays a list of apps with columns for 'App', 'Score', and 'Actions'. The 'App' column lists various Microsoft services like 'Teams admin center', 'MS Invoice', 'Mover', 'Microsoft Volume Licensing', 'Microsoft Tech Community', 'Microsoft Support', 'Microsoft Store for Business', 'Microsoft Social CRM', 'Microsoft Service Hub', 'Microsoft Secure Score', 'Microsoft Project', 'Microsoft Intune', 'Microsoft Graph', and 'Microsoft Educator Community'. The 'Score' column shows a score of 10 for all listed apps. The 'Actions' column contains icons for checking, deleting, and adding policies.

App	Score	Actions
Teams admin center Online meetings	10	✓ ⓧ ⋮
MS Invoice Vendor management system	10	✓ ⓧ ⋮
Mover Cloud storage	10	✓ ⓧ ⋮
Microsoft Volume Licensing IT services	10	✓ ⓧ ⋮
Microsoft Tech Community Forums	10	✓ ⓧ ⋮
Microsoft Support Customer support	10	✓ ⓧ ⋮
Microsoft Store for Business E-commerce	10	✓ ⓧ ⋮
Microsoft Social CRM CRM	10	✓ ⓧ ⋮
Microsoft Service Hub Customer support	10	✓ ⓧ ⋮
Microsoft Secure Score Security	10	✓ ⓧ ⋮
Microsoft Project Project management	10	✓ ⓧ ⋮
Microsoft Intune IT services	10	✓ ⓧ ⋮
Microsoft Graph Development tools	10	✓ ⓧ ⋮
Microsoft Educator Community Education	10	✓ ⓧ ⋮

# Application onboarding

1. Log in to app using IdP Credentials that forwards the session control to Cloud App Security
2. Add application URL's if not already added
3. If you added some URL's, test the application
4. Turn on the Cloud App Security conditional access policy for the application
5. Deploy session policy



#NVSummit2021

# DEMO - Adding a featured application

**NORDIC**

— VIRTUAL SUMMIT —

#NVSummit2021

# DEMO - Adding an unlisted featured application

**NORDIC**

— VIRTUAL SUMMIT —



# Where to start and how to implement it?

1. Forward applications to Cloud App Security and add session control support for all applications that you want
2. Make policy for small group and test, test and test
3. Bring more people for session control and at the end all internal users
4. Extend policies also to guest user accounts

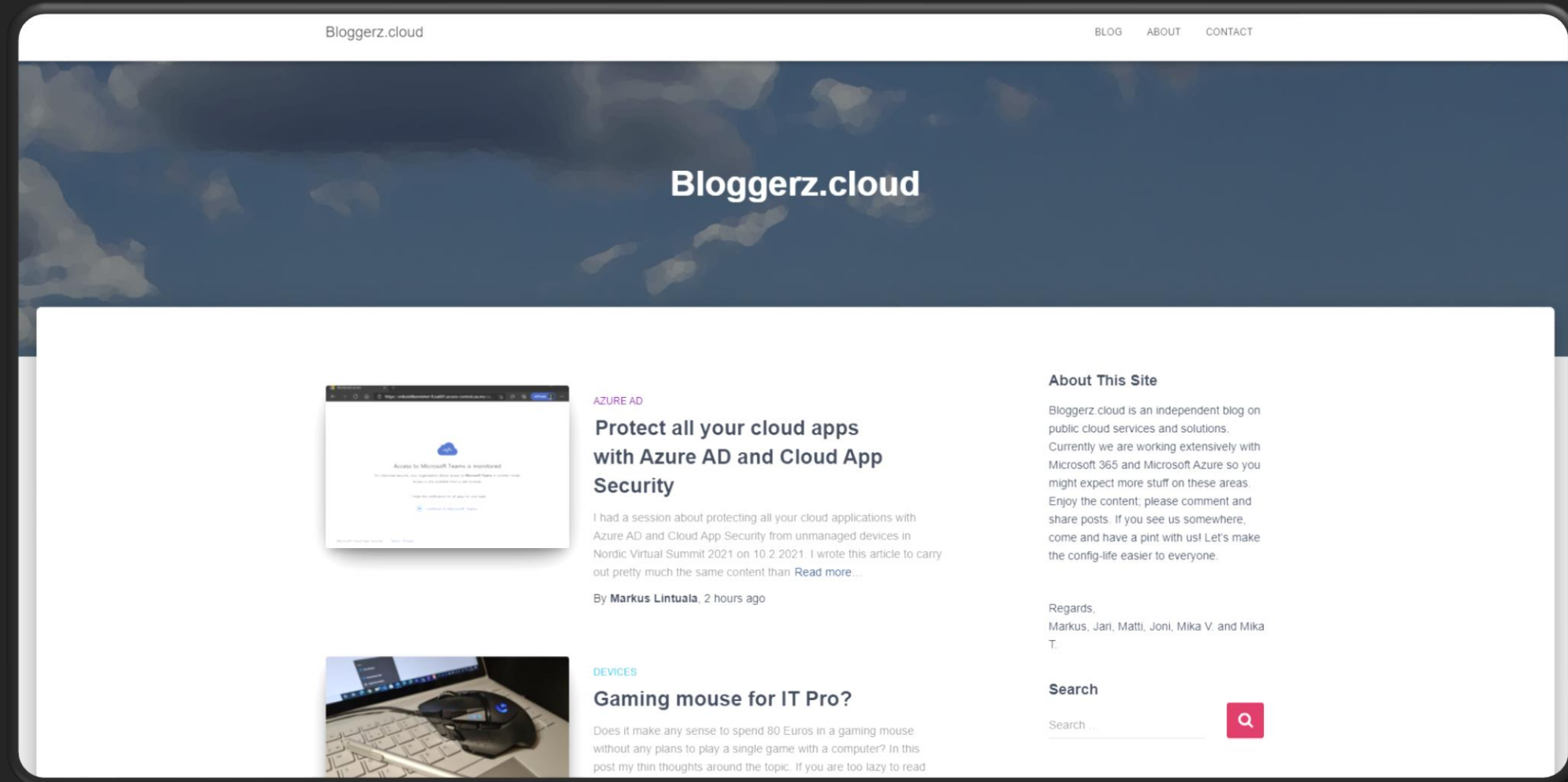


# What I should have done better 😊

- Test applications before onboarding to session control
- Monitor used applications and prepare before pilot
- Take enough large pilot group
- Do not use Cut, Copy and Paste actions in every app
- Inform your users

# Same content available now at

<https://bloggerz.cloud/2021/02/10/protect-all-your-cloud-apps-with-azure-ad-and-cloud-app-security/>



# Thank you!



MSEndPointMgr.com  
#MSEndPointMgr

System Center User Group  
Finland  
#SCUGFI

System Center User Group  
Denmark  
#SCUGDK

System Center User Group  
Sweden  
#SCUGSE



lintuala



MarkusLintuala



bloggerz.cloud

Modern Management User Group  
Norway  
#MMUGNO