Working with MCAS in the real life

- Anders Olsson
- IT/Information Security Advisor
- Twitter @AndersPsYnet
- MVP

NORDIC — VIRTUAL SUMMIT —

Working with MDCA in the real life

- Anders Olsson
- IT/Information Security Advisor
- Twitter @AndersPsYnet
- MVP

NORDIC — VIRTUAL SUMMIT —

Working with MDfCA in the real life

- Anders Olsson
- IT/Information Security Advisor
- Twitter @AndersPsYnet
- MVP

NORDIC — VIRTUAL SUMMIT —

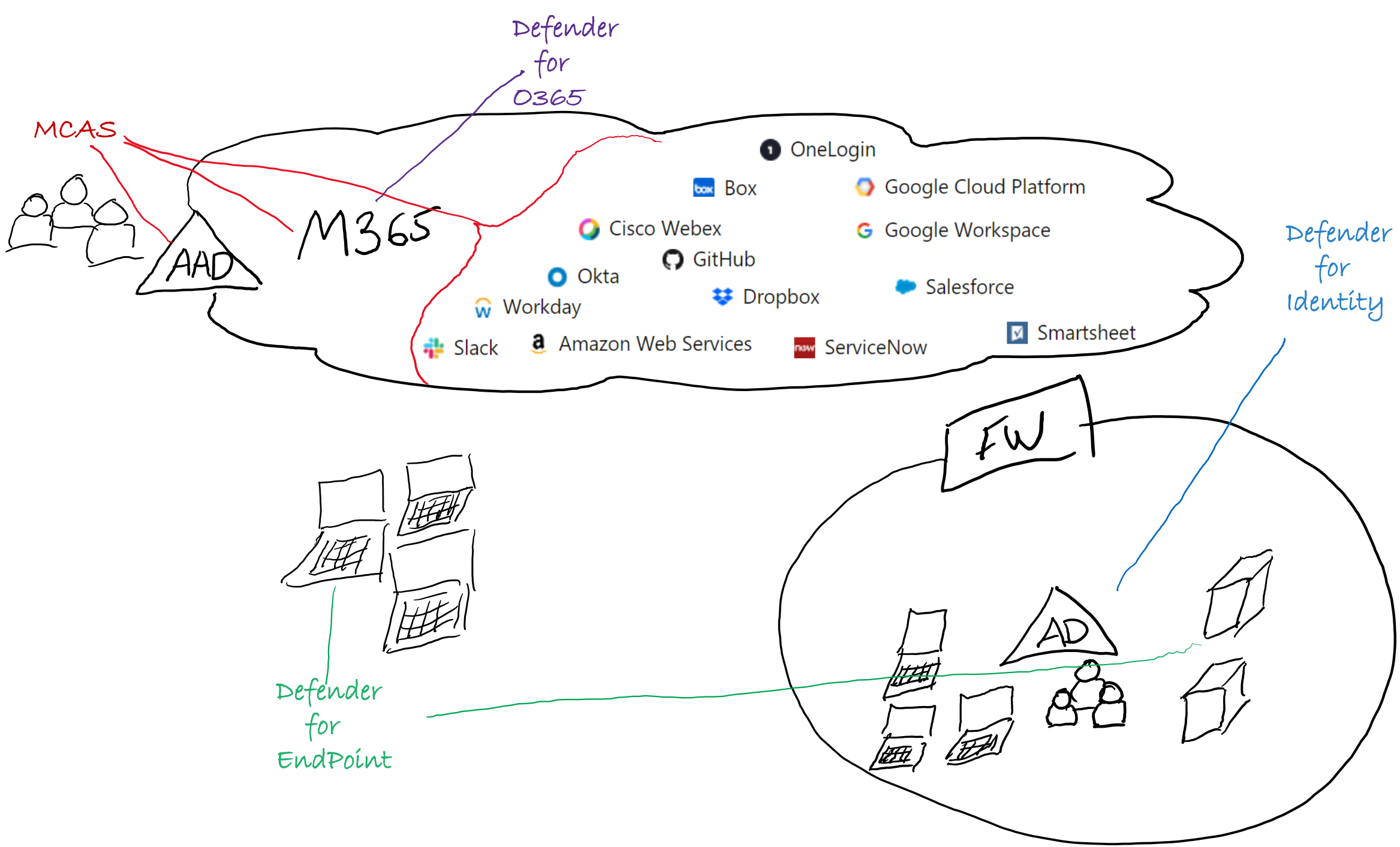
Working with

Microsoft Defender for Cloud Apps

in the real life

- Anders Olsson
- IT/Information Security Advisor
- Twitter @AndersPsYnet
- MVP

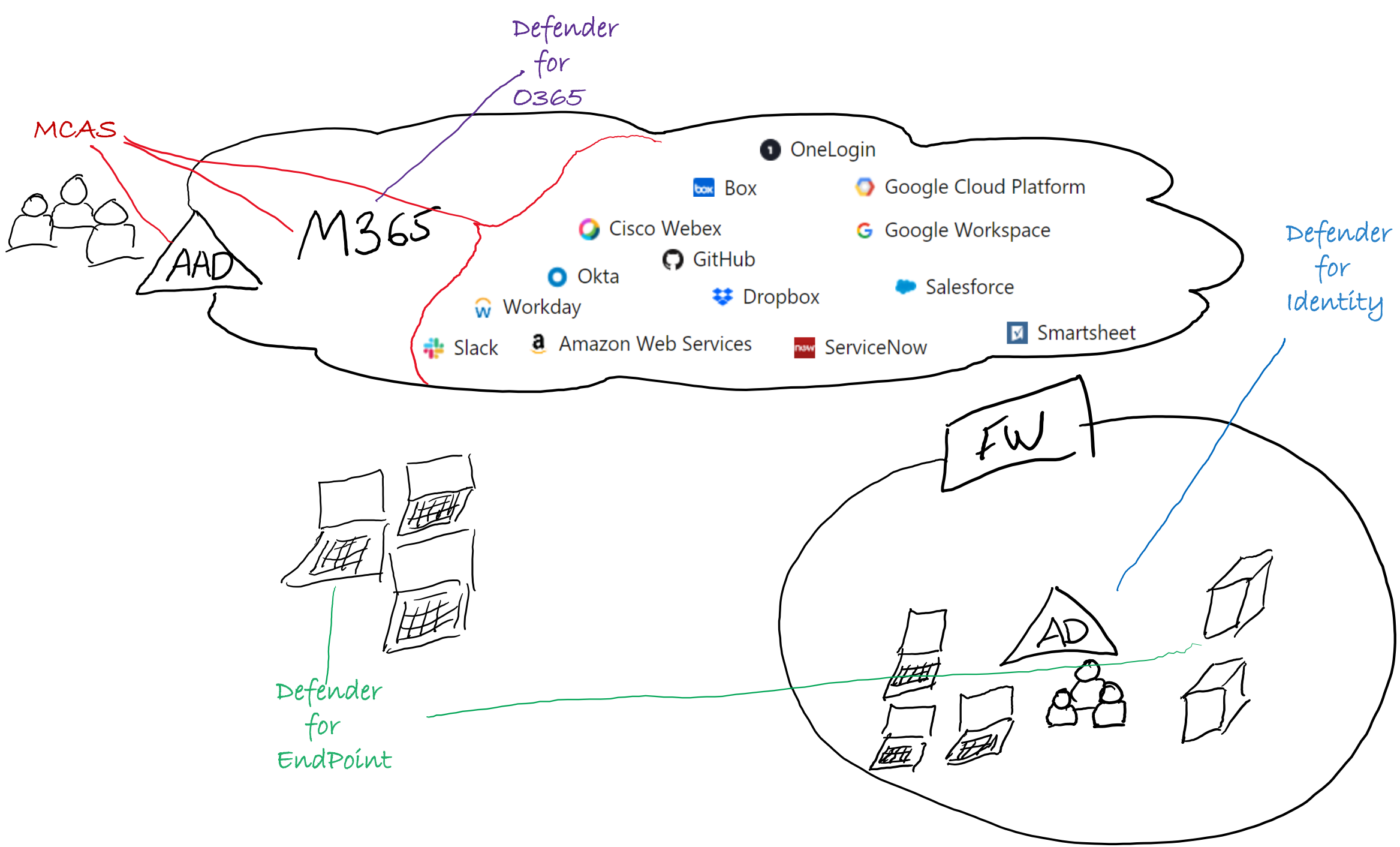
NORDIC — VIRTUAL SUMMIT —

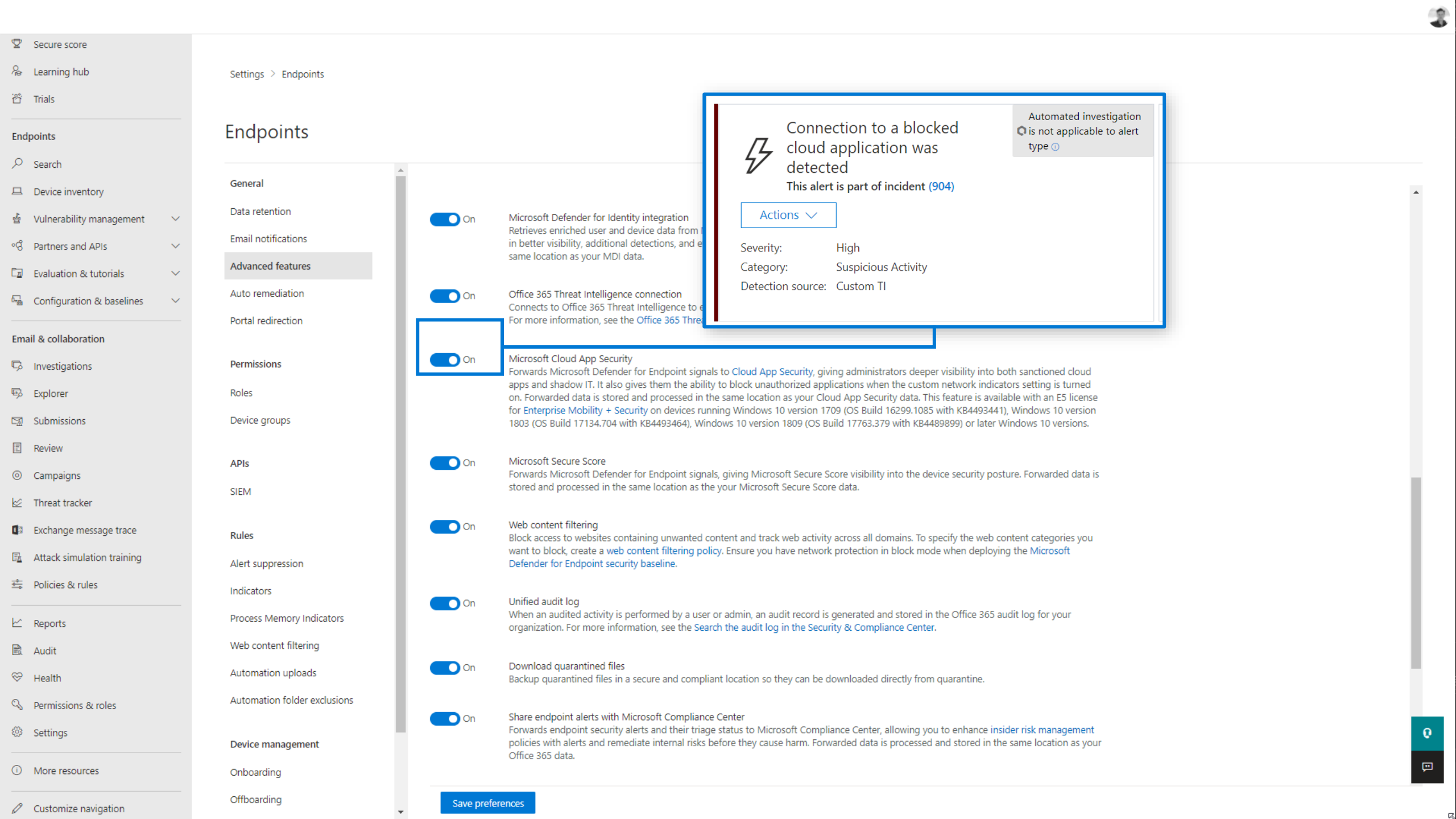

Defender for O365
MCAS
AAD
M365
OneLogin
Box
Google Cloud Platform
Cisco Webex
Google Workspace
GitHub
Okta
Dropbox
Salesforce
Workday
Slack
Amazon Web Services
ServiceNow
Smartsheet
Defender for Identity
FW
AD
Defender for EndPoint

Cloud discovery

26 000 Scored cloud apps

90 risk factors


Defender for O365
MCAS
AAD
M365
OneLogin
Box
Google Cloud Platform
Cisco Webex
Google Workspace
GitHub
Okta
Dropbox
Salesforce
Workday
Slack
Amazon Web Services
ServiceNow
Smartsheet
Defender for Identity
FW
AD
Defender for EndPoint


Secure score
Learning hub
Trials
Endpoints
Search
Device inventory
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration & baselines
Email & collaboration
Investigations
Explorer
Submissions
Review
Campaigns
Threat tracker
Exchange message trace
Attack simulation training
Policies & rules
Reports
Audit
Health
Permissions & roles
Settings
More resources
Customize navigation
Settings > Endpoints
Endpoints
General
Data retention
Email notifications
Advanced features
Auto remediation
Portal redirection
Permissions
Roles
Device groups
APIs
SIEM
Rules
Alert suppression
Indicators
Process Memory Indicators
Web content filtering
Automation uploads
Automation folder exclusions
Device management
Onboarding
Offboarding
Connection to a blocked cloud application was detected
This alert is part of incident (904)
Actions
Severity: High
Category: Suspicious Activity
Detection source: Custom TI
Automated investigation is not applicable to alert type
On
Microsoft Defender for Identity integration
Retrieves enriched user and device data from
in better visibility, additional detections, and e
same location as your MDI data.
On
Office 365 Threat Intelligence connection
Connects to Office 365 Threat Intelligence to e
For more information, see the Office 365 Thre
On
Microsoft Cloud App Security
Forwards Microsoft Defender for Endpoint signals to Cloud App Security, giving administrators deeper visibility into both sanctioned cloud apps and shadow IT. It also gives them the ability to block unauthorized applications when the custom network indicators setting is turned on. Forwarded data is stored and processed in the same location as your Cloud App Security data. This feature is available with an E5 license for Enterprise Mobility + Security on devices running Windows 10 version 1709 (OS Build 16299.1085 with KB4493441), Windows 10 version 1803 (OS Build 17134.704 with KB4493464), Windows 10 version 1809 (OS Build 17763.379 with KB4489899) or later Windows 10 versions.
On
Microsoft Secure Score
Forwards Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture. Forwarded data is stored and processed in the same location as the your Microsoft Secure Score data.
On
Web content filtering
Block access to websites containing unwanted content and track web activity across all domains. To specify the web content categories you want to block, create a web content filtering policy. Ensure you have network protection in block mode when deploying the Microsoft Defender for Endpoint security baseline.
On
Unified audit log
When an audited activity is performed by a user or admin, an audit record is generated and stored in the Office 365 audit log for your organization. For more information, see the Search the audit log in the Security & Compliance Center.
On
Download quarantined files
Backup quarantined files in a secure and compliant location so they can be downloaded directly from quarantine.
On
Share endpoint alerts with Microsoft Compliance Center
Forwards endpoint security alerts and their triage status to Microsoft Compliance Center, allowing you to enhance insider risk management policies with alerts and remediate internal risks before they cause harm. Forwarded data is processed and stored in the same location as your Office 365 data.
Save preferences

Twitch | New tab

For quick access, place your favorites here on the favorites bar. Manage favorites now

48 °F

Search DemoOnevinn and the web

Quick links

Like this background?

Office 365 | My Feed | Coronavirus | News | Sports | Weather | Traffic | Money | Travel

Personalize | Content visible

WEATHER

Karlstad, Varmland County, Sweden

48 °F °C

Mostly cloudy

11%

Today	Tue	Wed	Thu	Fri
51° 48°	53° 44°	56° 51°	56° 50°	52° 46°

See full forecast

RECOMMENDED

You frequently open this

Finance planned changes
Yesterday at 11:37 AM

You recently opened this

Conf info
Oct 18

View more

MLB

Red Sox	0	Final Oct 23
Astros	5	
Dodgers	2	Final Oct 24
Braves	4	
Braves		Oct 27 2:09 AM
Astros		

See more MLB

INDUSTRY NEWS

CBS News · 42 mins ago
James Michael Tyler, who played Gunther on "Friends," dies at age 59

Newsweek · 2 hours ago
When Is Kieran Culkin Hosting 'SNL'? Everything You Need to Know

Fortune · 5 hours ago
Shiba Inu coin surges on rumors that it would be listed on Robinhood

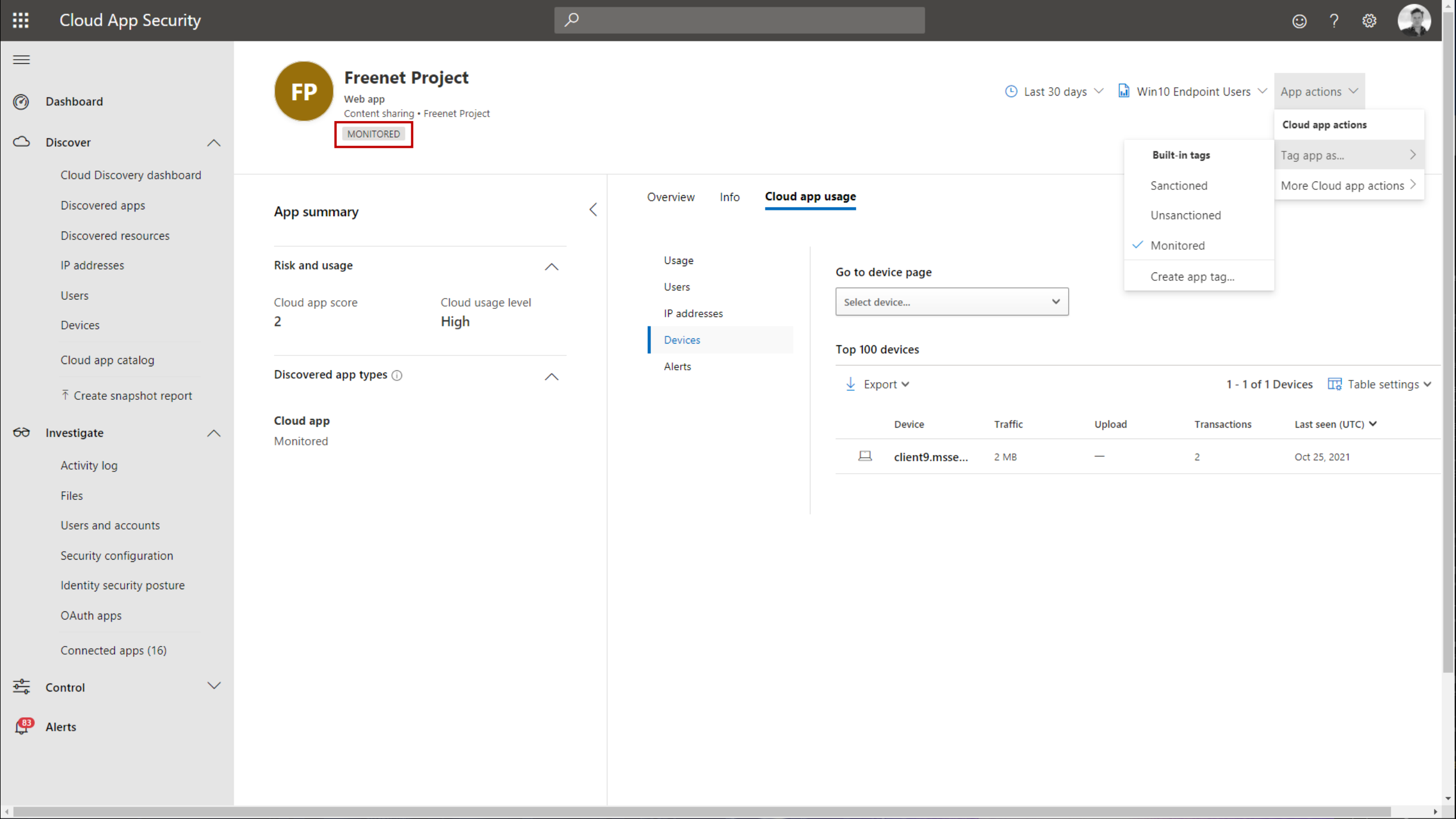
Esquire · 15 hours ago
Jason Sudeikis Was Hilarious

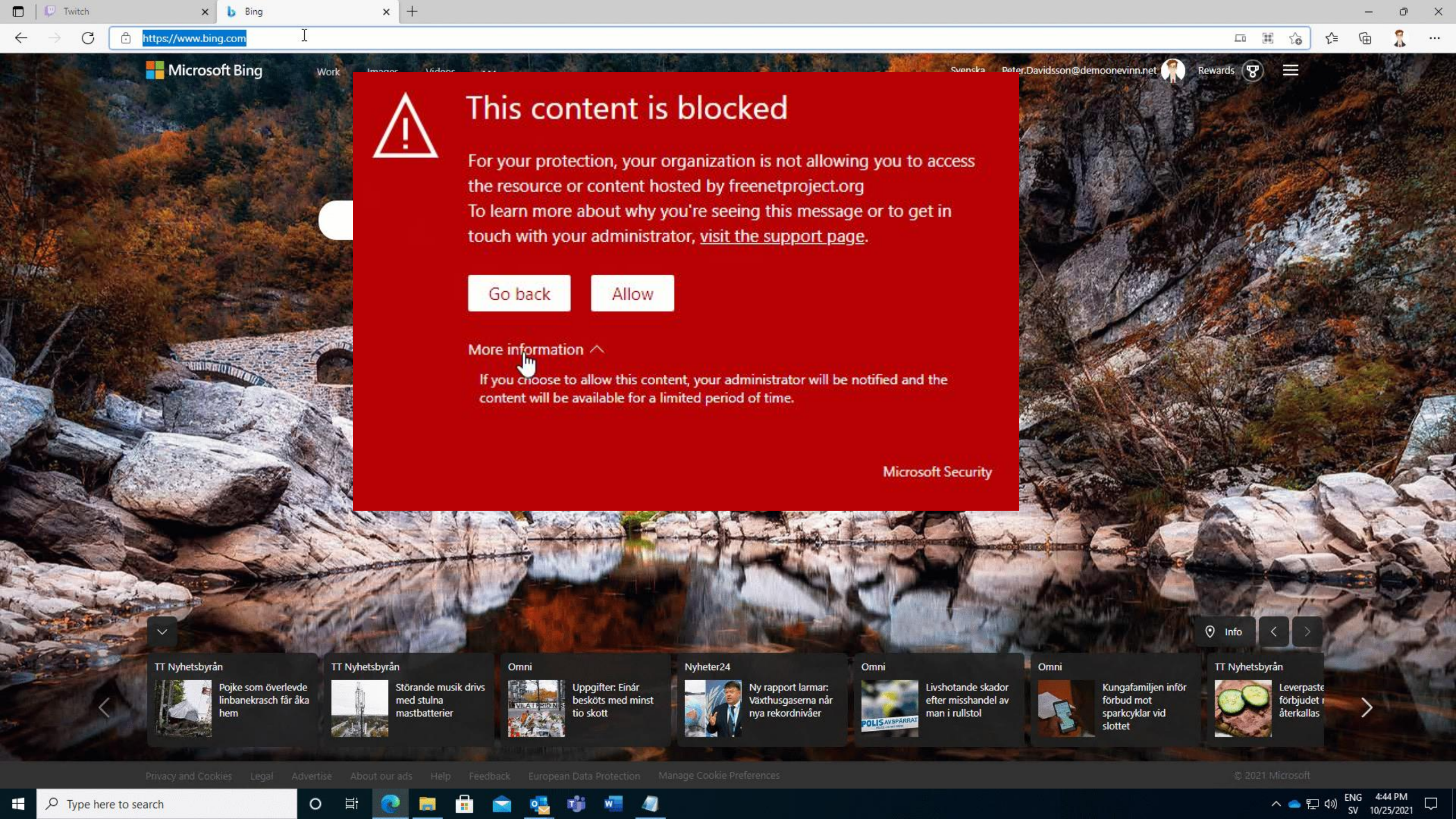
TODAY'S MARKET

DJI DOW 0.21% 35,677.02

Type here to search

ENG SV 2:34 PM 10/25/2021


Cloud App Security
Dashboard
Discover
Cloud Discovery dashboard
Discovered apps
Discovered resources
IP addresses
Users
Devices
Cloud app catalog
Create snapshot report
Investigate
Activity log
Files
Users and accounts
Security configuration
Identity security posture
OAuth apps
Connected apps (16)
Control
Alerts
83
FP
Freenet Project
Web app
Content sharing • Freenet Project
MONITORED
Last 30 days
Win10 Endpoint Users
App actions
Cloud app actions
Built-in tags
Tag app as...
Sanctioned
Unsanctioned
Monitored
Create app tag...
More Cloud app actions
App summary
Risk and usage
Cloud app score
2
Cloud usage level
High
Discovered app types
Cloud app
Monitored
Overview
Info
Cloud app usage
Usage
Users
IP addresses
Devices
Alerts
Go to device page
Select device...
Top 100 devices
Export
1 - 1 of 1 Devices
Table settings
Device
Traffic
Upload
Transactions
Last seen (UTC)
client9.msse...
2 MB
—
2
Oct 25, 2021


Twitch
Bing
https://www.bing.com
Microsoft Bing
Work
Images
Videos
Svenska
Peter.Davidsson@demoonevinn.net
Rewards
This content is blocked
For your protection, your organization is not allowing you to access the resource or content hosted by freenetproject.org
To learn more about why you're seeing this message or to get in touch with your administrator, visit the support page.
Go back
Allow
More information
If you choose to allow this content, your administrator will be notified and the content will be available for a limited period of time.
Microsoft Security
Info
TT Nyhetsbyrån
Pojke som överlevde linbanekrasch får åka hem
TT Nyhetsbyrån
Störande musik drivs med stulna mastbatterier
Omni
Uppgifter: Einár besköts med minst tio skott
Nyheter24
Ny rapport larmar: Växthusgaserna når nya rekordnivåer
Omni
Livshotande skador efter misshandel av man i rullstol
Omni
Kungafamiljen inför förbud mot sparkcyklar vid slottet
TT Nyhetsbyrån
Leverpaste förbjudet återkallas
Privacy and Cookies
Legal
Advertise
About our ads
Help
Feedback
European Data Protection
Manage Cookie Preferences
© 2021 Microsoft
Type here to search
ENG
SV
4:44 PM
10/25/2021

Communications 1
Operations management 1
E-commerce 1

T-Mobile
Communications
6

Carnival
Transportation and travel
6
278 MB | 44 MB | 290 | 12 | 15 | 13 | Oct 28, 2021

Carnival Corporation is a cruise company.

Suggest an improvement
Disclaimer
6

8 GENERAL

Category: Transportation and travel
Headquarters: United States
Data center: Germany
Hosting company: Akamai Technologies
Founded: 1972
Holding: Public
Domain: *.carnival.com
Terms
carnival.com/profilemanagement/accounts/login
Domain registration: Jun 24, 1994
Consumer popularity: 9
Privacy policy: carnival.com/about-carnival/l...
Logon URL: carnival.com/profilemanagemen...
Vendor: Carnival Corporation
Data types: 2 Documents, Media files
Disaster Recovery Plan

5 SECURITY

Latest breach: Mar 19, 2021
Data-at-rest encryption method: Not suppor...
Multi-factor authentication
IP address restriction
User audit trail
Admin audit trail
Data audit trail
User can upload data
Data classification
Remember password
User-roles support
File sharing
Valid certificate name
Trusted certificate
Encryption protocol: TLS 1.2
Heartbleed patched
HTTP security headers
Supports SAML
Protected against DROWN
Penetration Testing
Requires user authentication
Password policy: Partial

1 COMPLIANCE

ISO 27001
ISO 27018
ISO 27017
ISO 27002
FINRA
FISMA
GAAP
HIPAA
ISAE 3402
ITAR
SOC 1
SOC 2
SOC 3
SOX
SP 800-53
SSAE 16
Safe Harbor
PCI DSS version
GLBA
FedRAMP level: Not supported
CSA STAR level: Not supported
Privacy Shield
FFIEC
GAPP
COBIT
COPPA
FERPA
HITRUST CSF
Jericho Forum Commandments

9 LEGAL

Data ownership
DMCA
Data retention policy: Deleted within more t...
GDPR readiness statement
GDPR - Right to erasure
GDPR - Report data breaches
GDPR - Data protection
GDPR - User ownership: Partial

Alerts > Discovered app security breach

8/19/21 10:47 AM

LOW SEVERITY

Win10 Endpoint Users

Close alert

Description

According to public information, the app "T-Mobile" was breached on Aug 18, 2021. For more information, see here.
See the list of users who used this app in the last 90 days according to "Win10 Endpoint Users" data view.

Discovered apps

Bulk selection

1 - 1 of 1 discovered apps | Show details | Table settings

App	Score	Traffic	Upload	Trans...	Users	IP ad...	Last s...	Actions
T-Mobile Communications	6	1.1 GB	181 MB	1.7K	135	150	Nov 1, 2...	

Cloud Discovery

Continuous report: Global
Timeframe: Last 30 days

Dashboard | Discovered apps | Discovered resources | IP addresses | Users

Updated on Nov 2, 2021, 11:02 AM

Apps	IP addresses	Users	Traffic
211	17.7 K	0	258.2 GB (4.5 GB ↑, 253.7 GB ↓)

Cloud Discovery open alerts

+ Create policy

9 Cloud Discovery alerts

326 Suspicious use alerts

App categories

1-5 of 37 ▸ Traffic

Sanctioned | Unsanctioned | Other

Social network	94.1 GB
Collaboration	74.7 GB
Security	25.5 GB
Code hosting	19.8 GB
Hosting services	15.6 GB

Risk levels

All categories by Traffic

258.2 GB
Total

- Traffic from high risk apps
- Traffic from medium risk apps
- Traffic from low risk apps

Configure score metric

Discovered apps

1-15 of 211 ▸ View all apps | All categories | Traffic

Sanctioned | Unsanctioned | Other

LinkedIn	89.6 GB
Notion	73.2 GB
CloudFlare	25.4 GB
GitHub	19.8 GB
Amazon CloudFront	14.3 GB
tawk.to	5.1 GB
Discord	4.5 GB
Yahoo!	4.2 GB
	2.9 GB

Top entities

View all users | User by Traffic

There's no relevant data to display

Apps headquarters location

All categories

Dashboard
Discover
Cloud Discovery dashboard
Discovered apps
Discovered resources
IP addresses
Users
Devices
Cloud app catalog
Create snapshot report
Investigate
Control
Alerts

Alerts > Cloud Discovery anomaly detection

10/30/21 8:17 PM

+40

HIGH SEVERITY

Cloud Discovery anomaly detection | 10.[redacted]7 | 4 Discovered users | Win10 Endpoint Users

Close alert

Description

Anomalous activity was detected in Microsoft Live on Oct 29, 2021:

- The user user 1 uploaded 848 MB.
- The IP address [redacted] uploaded 848 MB.
- The user user 2 downloaded 609 MB.
- The user user 3 uploaded 139 MB.
- The user user 4 downloaded 310 MB.

Average use of Microsoft Live on Oct 29, 2021 in your organization:

- 58 KB were uploaded per user.
- 65 KB were uploaded per IP address.
- 84 KB were downloaded per user.

Average use of Microsoft Live in your organization:

- 59 KB were uploaded daily per user.
- 64 KB were uploaded daily per IP address.
- 76 KB were downloaded daily per user.

Discovered apps

Bulk selection

1 - 1 of 1 discovered apps | Show details | Table settings

App	Score	Traffic	Upload	Transactions	Users	IP addresses	Last seen (UTC)	Actions
Microsoft Live IT services	10	319.1 GB	153.6 GB	499.4K	25975	34315	Nov 2, 2021	

NORDIC
— VIRTUAL SUMMIT —

Security Posture

Dashboard
Discover
Investigate
Activity log
Files
Users and accounts
Security configuration
Identity security posture
OAuth apps
Connected apps (16)
Control
Policies
Templates
Alerts 83

Identity Security Posture > Weak cipher usage

Improvement actions

Stop weak cipher usage | Most critical: 2 entities | High

Send us feedback...

Report description

Top entities using weak ciphers (RC4, DES) in your on-premises environment (last 30 days). Learn why this is important to remediate and create an action plan

Export

1 - 3 of 3 top entities using weak ciphers | Table settings

Entity	Type	Tags	Protocol	Cipher	Activities	Recommended actions	Last seen
Administrator	Account	SENSITIVE	Kerberos	Rc4	10	Stop **Administrator** from using **Rc4** cipher	Oct 28, 2021, 10:00 ...
WAP2	Device		Kerberos	Rc4	6	Stop **WAP2** from using **Rc4** cipher	Oct 28, 2021, 10:00 ...
FILE	Device		Kerberos	Rc4	4	Stop **FILE** from using **Rc4** cipher	Oct 13, 2021, 10:00 ...

Dashboard
Discover
Investigate
Activity log
Files
Users and accounts
Security configuration
Identity security posture
OAuth apps
Connected apps (16)
Control
Alerts 80

Manage OAuth apps

Queries: Select a query | Save as | Advanced filters

App: Select apps... | User name: Select users... | App state: Select value... | Community use: Select value... | Permissions: Select permission...

Permission level:

Bulk selection | New policy from search | Export | 1 - 20 of 39 apps | Show details | Table settings

Name	Authorized by	Permission level	Last authorized	Actions
Graph Explorer	4 users	High	Apr 24, 2018, 11:21 AM	
IntuneAutomation		High	Apr 20, 2018, 6:20 PM	
Microsoft Intune PowerShell	1 user	High	Sep 27, 2018, 10:28 AM	
MSFT Power Platform - Azure AD	1 user	High	Jun 7, 2019, 8:17 AM	
MSFT Power Platform	1 user	High	Jun 7, 2019, 10:43 AM	
O365 Management API		High	Aug 17, 2021, 3:43 PM	
Microsoft Graph PowerShell	1 user	High	Oct 13, 2021, 9:18 AM	
TomTestarDeklegateDConsent		High	Oct 18, 2021, 4:14 PM	
Lookout MTP	5 users	Medium	May 20, 2019, 3:26 PM	
Azure AD Power BI Content Pack App	1 user	Medium	Mar 5, 2018, 11:23 PM	
Vafe AIP & MIP test	1 user	Medium	Mar 13, 2018, 10:38 AM	
WD Antivirus Testground	2 users	Medium	Mar 24, 2021, 1:30 PM	
Apple Internet Accounts	1 user	Medium	Jan 20, 2020, 10:52 AM	
Vafe-MIPsdk-Sample-Apps		Medium	Mar 25, 2019, 9:45 AM	

Mark app as banned

NORDIC
– VIRTUAL SUMMIT –

Threat detection and automatic response

Dashboard
Discover
Investigate
Control
Policies
Templates
Alerts 83

Create an alert for each matching event with the policy's severity

Save as default settings | Restore default settings

Send alert as email

tomadm@demoonevinn.net × anders@demoonevinn.net ×

Send alert as text message

Daily alert limit per policy 5

Send alerts to Power Automate

Select playbook...

Governance actions

All apps — Notify user, Confirm user compromised

Notify user

Notify additional users

Suspend user

For Azure Active Directory users

Confirm the user as compromised in Azure Active Directory (regardless of which app was used by the user to trigger the alert)

Confirm user compromised

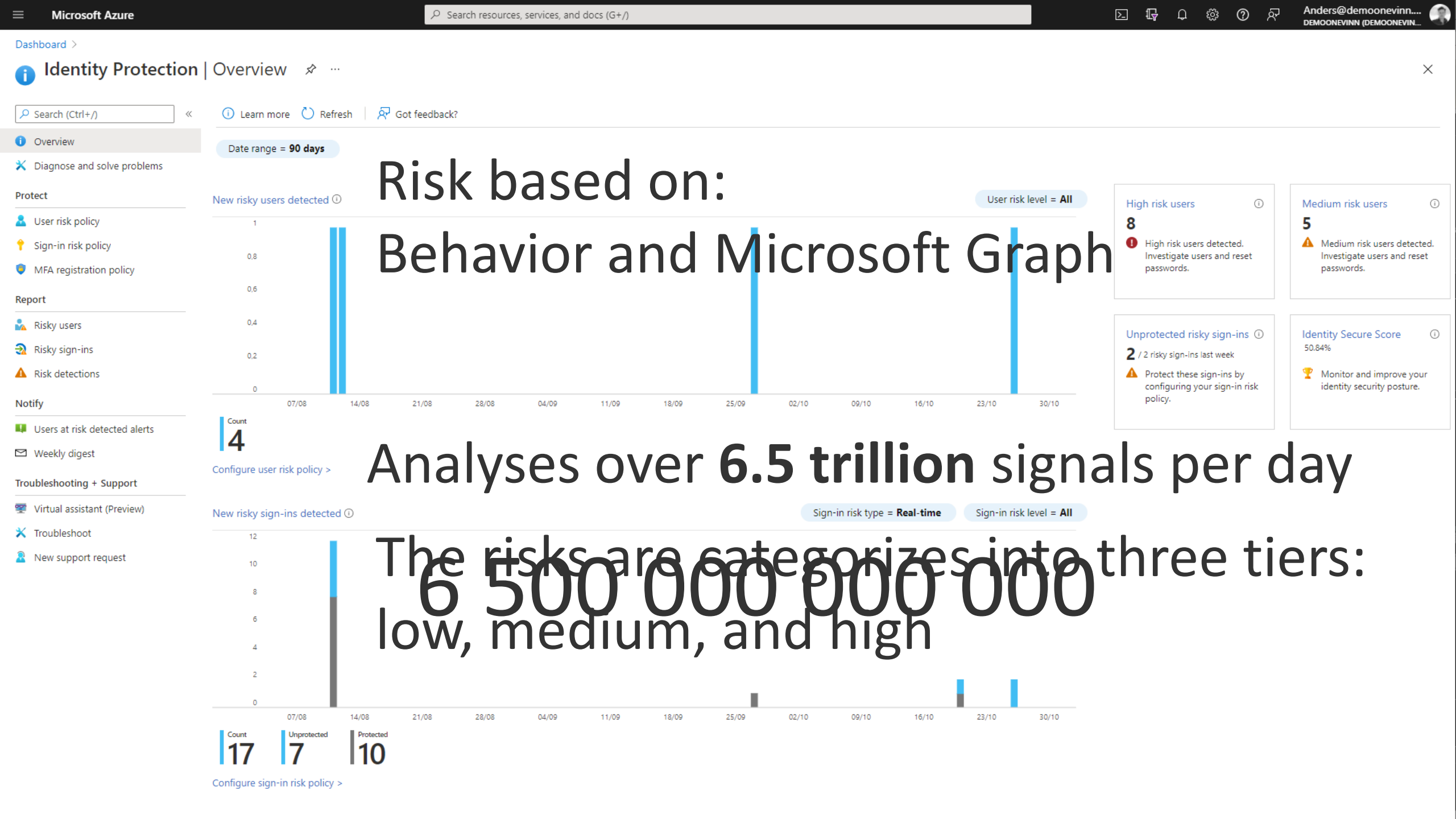
For Azure Active Directory users

Office 365

Enter a custom notification message:

B I U

Potential ransomware activity have been detected from your account. By security reason you need to change password.


Microsoft Azure
Search resources, services, and docs (G+/)
Anders@demoonevinn....
DEMOONEVINN (DEMOONEVIN...
Dashboard
Identity Protection | Overview
Search (Ctrl+/)
Learn more
Refresh
Got feedback?
Overview
Diagnose and solve problems
Protect
User risk policy
Sign-in risk policy
MFA registration policy
Report
Risky users
Risky sign-ins
Risk detections
Notify
Users at risk detected alerts
Weekly digest
Troubleshooting + Support
Virtual assistant (Preview)
Troubleshoot
New support request
Date range = 90 days
New risky users detected
User risk level = All
Count
4
Configure user risk policy >
New risky sign-ins detected
Sign-in risk type = Real-time
Sign-in risk level = All
Count
17
Unprotected
7
Protected
10
Configure sign-in risk policy >
High risk users
8
High risk users detected. Investigate users and reset passwords.
Medium risk users
5
Medium risk users detected. Investigate users and reset passwords.
Unprotected risky sign-ins
2 / 2 risky sign-ins last week
Protect these sign-ins by configuring your sign-in risk policy.
Identity Secure Score
50.84%
Monitor and improve your identity security posture.
Risk based on:
Behavior and Microsoft Graph
Analyses over 6.5 trillion signals per day
6 500 000 000 000
The risks are categorizes into three tiers:
low, medium, and high

Identity Protection | Overview

Search (Ctrl+/)

Overview
Diagnose and solve problems

Protect
User risk policy
Sign-in risk policy
MFA registration policy

Report
Risky users
Risky sign-ins
Risk detections

Notify
Users at risk detected alerts
Weekly digest

Troubleshooting + Support
Virtual assistant (Preview)
Troubleshoot
New support request

Learn more | Refresh | Got feedback?

Date range = **90 days**

New risky users detected

User risk level = **All**

Count
4

Configure user risk policy >

New risky sign-ins detected

Sign-in risk type = **Real-time**

Sign-in risk level = **All**

Count **17** | Unprotected **7** | Protected **10**

Configure sign-in risk policy >

High risk users
8
High risk users detected. Investigate users and reset passwords.

Medium risk users
5
Medium risk users detected. Investigate users and reset passwords.

Unprotected risky sign-ins
2 / 2 risky sign-ins last week
Protect these sign-ins by configuring your sign-in risk policy.

Identity Secure Score
50.84%
Monitor and improve your identity security posture.

Identity Protection | Sign-in risk policy

Search (Ctrl+/)

Overview
Diagnose and solve problems

Protect
User risk policy
Sign-in risk policy
MFA registration policy

Report
Risky users
Risky sign-ins
Risk detections

Notify
Users at risk detected alerts
Weekly digest

Troubleshooting + Support
Virtual assistant (Preview)
Troubleshoot
New support request

Policy Name
Sign-in risk remediation policy

Assignments

Users
All users included and 11 users excluded

Sign-in risk
Medium and above

Controls

Access
Require multi-factor authentication

Enforce policy
On Off

Save

Identity Protection | Sign-in risk policy

Search (Ctrl+/)

Overview

Diagnose and solve problems

Protect

User risk policy

Sign-in risk policy

MFA registration policy

Report

Risky users

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Policy Name

Sign-in risk remediation policy

Assignments

Users

All users included and 11 users excluded

Sign-in risk

Medium and above

Controls

Access

Require multi-factor authentication

Identity Protection | Sign-in risk policy

Search (Ctrl+/)

Overview
Diagnose and solve problems

Protect
User risk policy
Sign-in risk policy
MFA registration policy

Report
Risky users
Risky sign-ins
Risk detections

Notify
Users at risk detected alerts
Weekly digest

Troubleshooting + Support
Virtual assistant (Preview)
Troubleshoot
New support request

Policy Name
Sign-in risk remediation policy

Assignments

Users
All users included and 11 users excluded

Sign-in risk
Medium and above

Controls

Access
Require multi-factor authentication

Enforce policy
On Off

Save

Identity Protection | User risk policy

Search (Ctrl+/)

Overview
Diagnose and solve problems

Protect
User risk policy
Sign-in risk policy
MFA registration policy

Report
Risky users
Risky sign-ins
Risk detections

Notify
Users at risk detected alerts
Weekly digest

Troubleshooting + Support
Virtual assistant (Preview)
Troubleshoot
New support request

Policy Name
User risk remediation policy

Assignments

Users
3 users included and 8 users excluded

User risk
High

Controls

Access
Require password change

Enforce policy
On Off

Save

Identity Protection | User risk policy

Search (Ctrl+/)

Overview

Diagnose and solve problems

Protect

User risk policy

Sign-in risk policy

MFA registration policy

Report

Risky users

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Policy Name

User risk remediation policy

Assignments

Users

3 users included and 8 users excluded

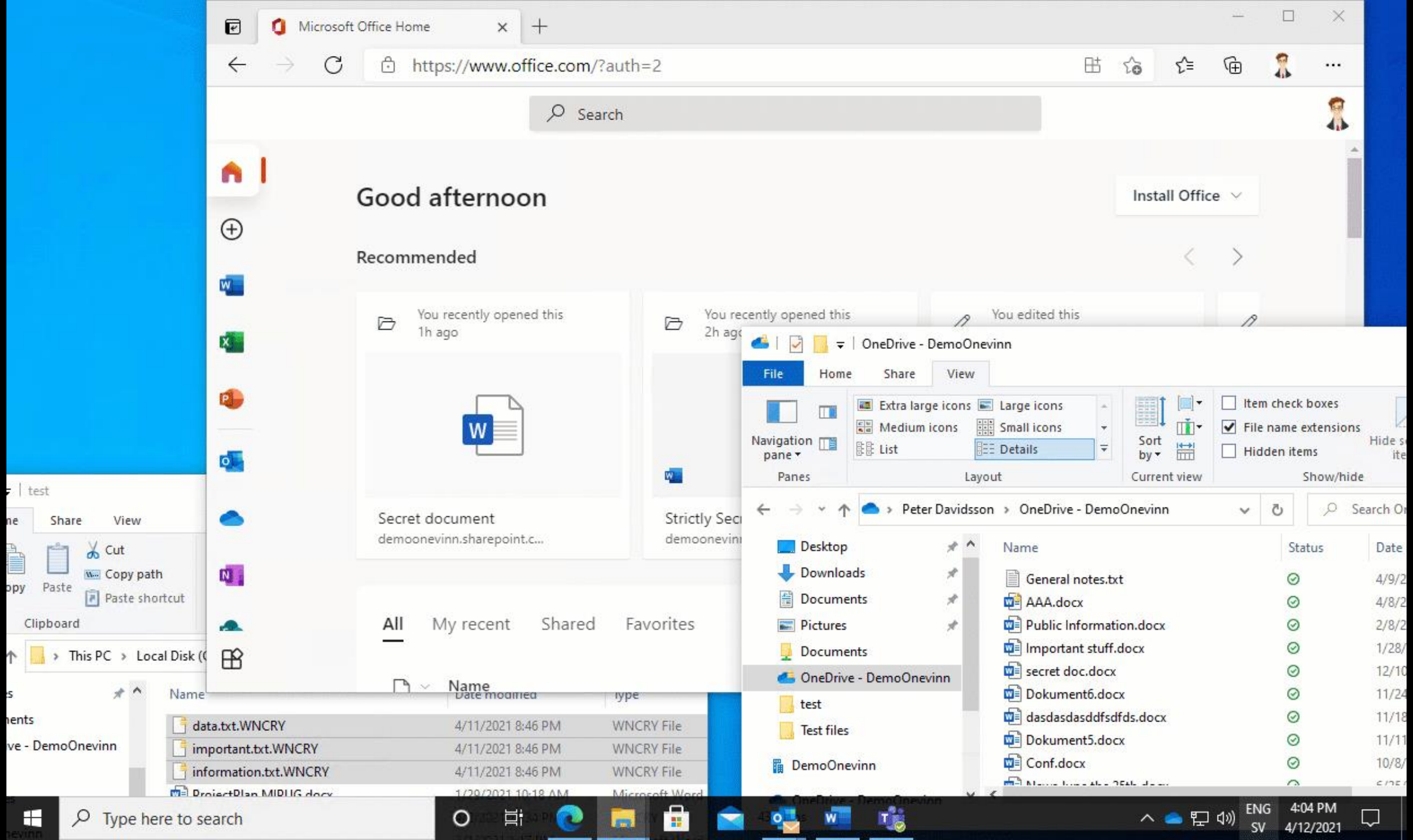
User risk

High

Controls

Access

Require password change


Microsoft Office Home
https://www.office.com/?auth=2
Search
Good afternoon
Install Office
Recommended
You recently opened this 1h ago
You recently opened this 2h ago
You edited this
Secret document
demoonevinn.sharepoint.c...
Strictly Sec
demoonevinn
All
My recent
Shared
Favorites
Name
Date modified
Type
data.txt.WNCRY 4/11/2021 8:46 PM WNCRY File
important.txt.WNCRY 4/11/2021 8:46 PM WNCRY File
information.txt.WNCRY 4/11/2021 8:46 PM WNCRY File
ProjectPlan.MIPUG.docx 1/29/2021 10:18 AM Microsoft Word
test
File Share View
Cut
Copy path
Paste shortcut
Paste
Clipboard
This PC › Local Disk (
OneDrive - DemoOnevinn
File Home Share View
Extra large icons
Large icons
Medium icons
Small icons
List
Details
Navigation pane
Panes
Layout
Sort by
Current view
Item check boxes
File name extensions
Hidden items
Show/hide
Peter Davidsson › OneDrive - DemoOnevinn
Search On
Desktop
Downloads
Documents
Pictures
Documents
OneDrive - DemoOnevinn
test
Test files
DemoOnevinn
Name
Status
Date
General notes.txt
AAA.docx
Public Information.docx
Important stuff.docx
secret doc.docx
Dokument6.docx
dasdasdasddfsdfds.docx
Dokument5.docx
Conf.docx
Type here to search
ENG SV
4:04 PM 4/12/2021

Peter Davidsson
Manager
Management

SENSITIVE

User threat

Investigation priority
480

Open alerts
36

Identity risk level
No user risk

User exposure

First seen
Oct 20, 2020

Last seen
Apr 14, 2021

Accounts
3

Devices
8

Logon Types
3

Locations
5

Matched files
5

Investigation priority score

Score is based on the last 7 days How do we score?

480

Alerts Score: 480
Risky activities Score: 0

User's score compared to the organization 100%

User score in the last two weeks

Top 90% in your organization

Alerts and risky activities that contributed to the score (last 7 days)

View all user alerts (36)

Yesterday

+2 4/16/21, 10:51:53 AM
Access file: file https://demoonevinn.sharepoint.com/sites/ProjectDel...

4/12/21

+50 4/12/21, 7:46:44 PM
Potential ransomware activity

+30 4/16/21, 1:43:02 PM
Activity from infrequent country

+30 4/15/21, 11:28:03 AM
Impossible travel activity

+30 4/15/21, 11:16:50 AM
User and IP address reconnaissance (SMB)

4/12/21

+50 4/12/21, 7:46:44 PM
Potential ransomware activity

Dashboard
Discover
Investigate
Control
Policies
Templates
Alerts 83

Alerts

Save as default settings | Restore default settings

Send alert as email
anders.olsson@onevinn.se

Send alert as text message

Send alerts to Power Automate
Select playbook...

Governance actions

All apps — Confirm user compromised, Notify user

Notify user
CC additional users
anders@demoonevinn.net

Suspend user
For Azure Active Directory users

Confirm user compromised
For Azure Active Directory users

Office 365

This policy was modified 7 months ago

After the policy is created, it takes a week to learn your baseline before this policy generates al...
We secure your data as described in our privacy statement and online service terms.

Update Cancel

Peter Davidsson
Manager
Management

SENSITIVE

User threat

Investigation priority
480

Open alerts
36

Identity risk level
No user risk

User exposure

First seen
Oct 20, 2020

Last seen
Apr 14, 2021

Accounts
3

Devices
8

Logon Types
3

Locations
5

Matched files
5

Investigation priority score

Score is based on the last 7 days

480

Alerts ..... Score: 480
Risky activities ..... Score: 0

User's score compared to the organization

User score in the last two weeks

Top 90% i

Alerts and risky activities that contributed to the score (last 7 days) View all user alerts (36)

Yesterday

+2
4/16/21, 10:51:53 AM
Access file: file https://demoonevinn.sharepoint.com/sites/ProjectDel...

4/12/21

+50
4/12/21, 7:46:44 PM
Potential ransomware activity

+30
4/16/21, 1:43:02 PM
Activity from infrequent country

+30
4/15/21, 11:28:03 AM
Impossible travel activity

+30
4/15/21, 11:16:50 AM
User and IP address reconnaissance (SMB)

4/12/21

+50
4/12/21, 7:46:44 PM
Potential ransomware activity

DEMO BY onevinn

onevinn

peter.davidsson@demoonevinn.net

Your account is at risk

To help you—and only you—get back into peter.davidsson@demoonevinn.net, we need to verify your identity.

Cancel Verify

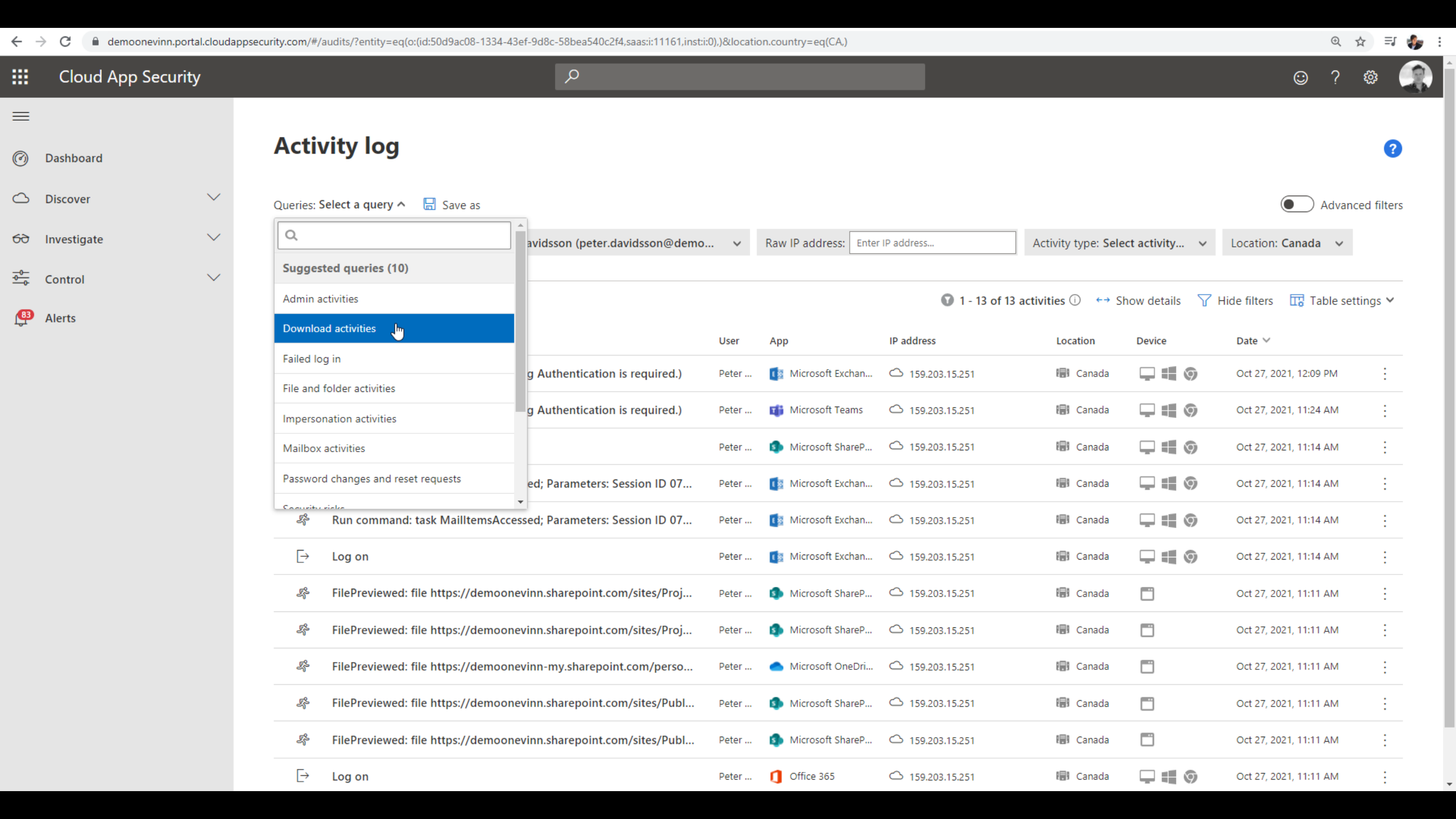
Welcome to a demo by Onevinn

Terms of use Privacy & cookies ...

NORDIC
– VIRTUAL SUMMIT –

Investigations from the portals

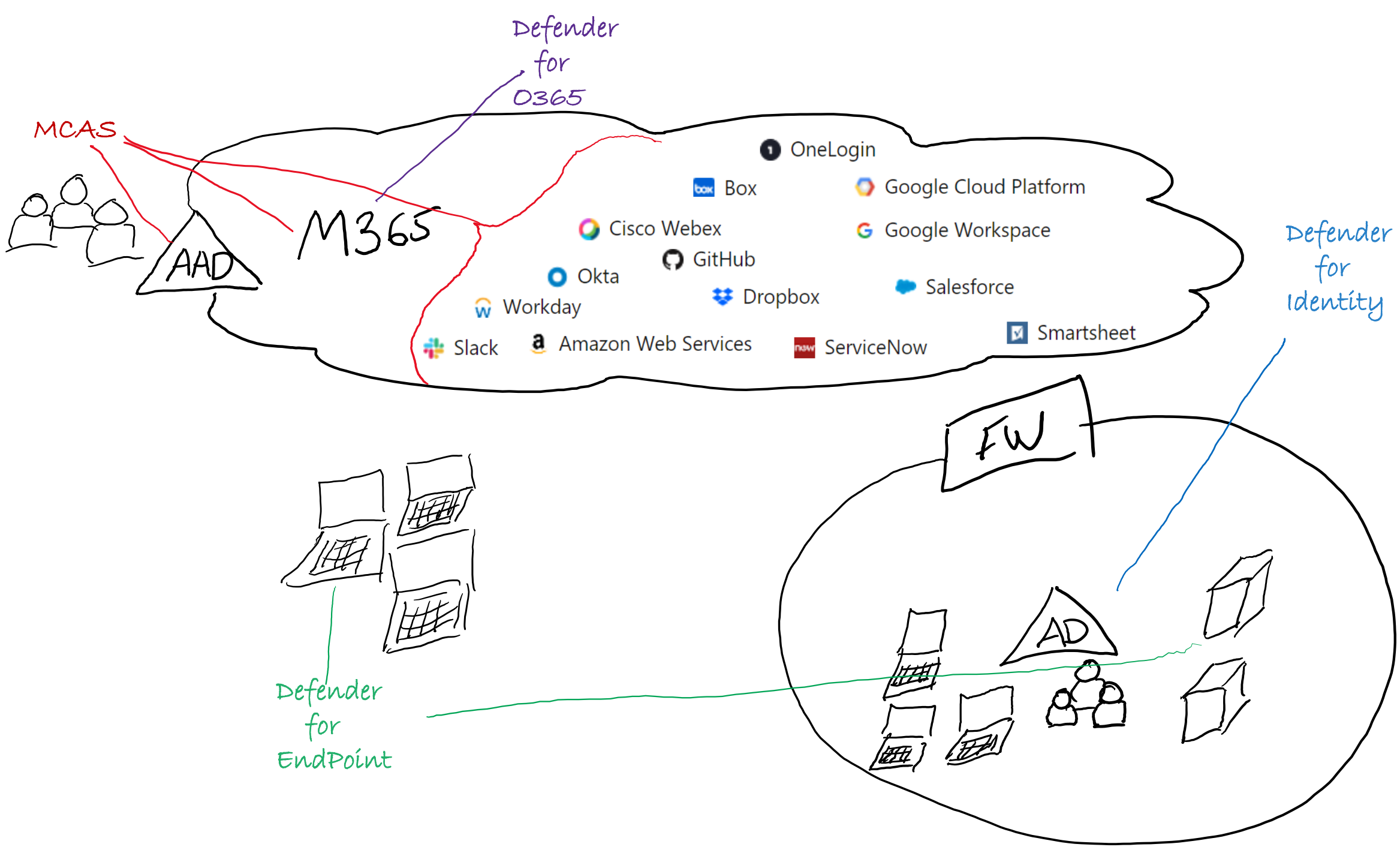
Where to look for what....

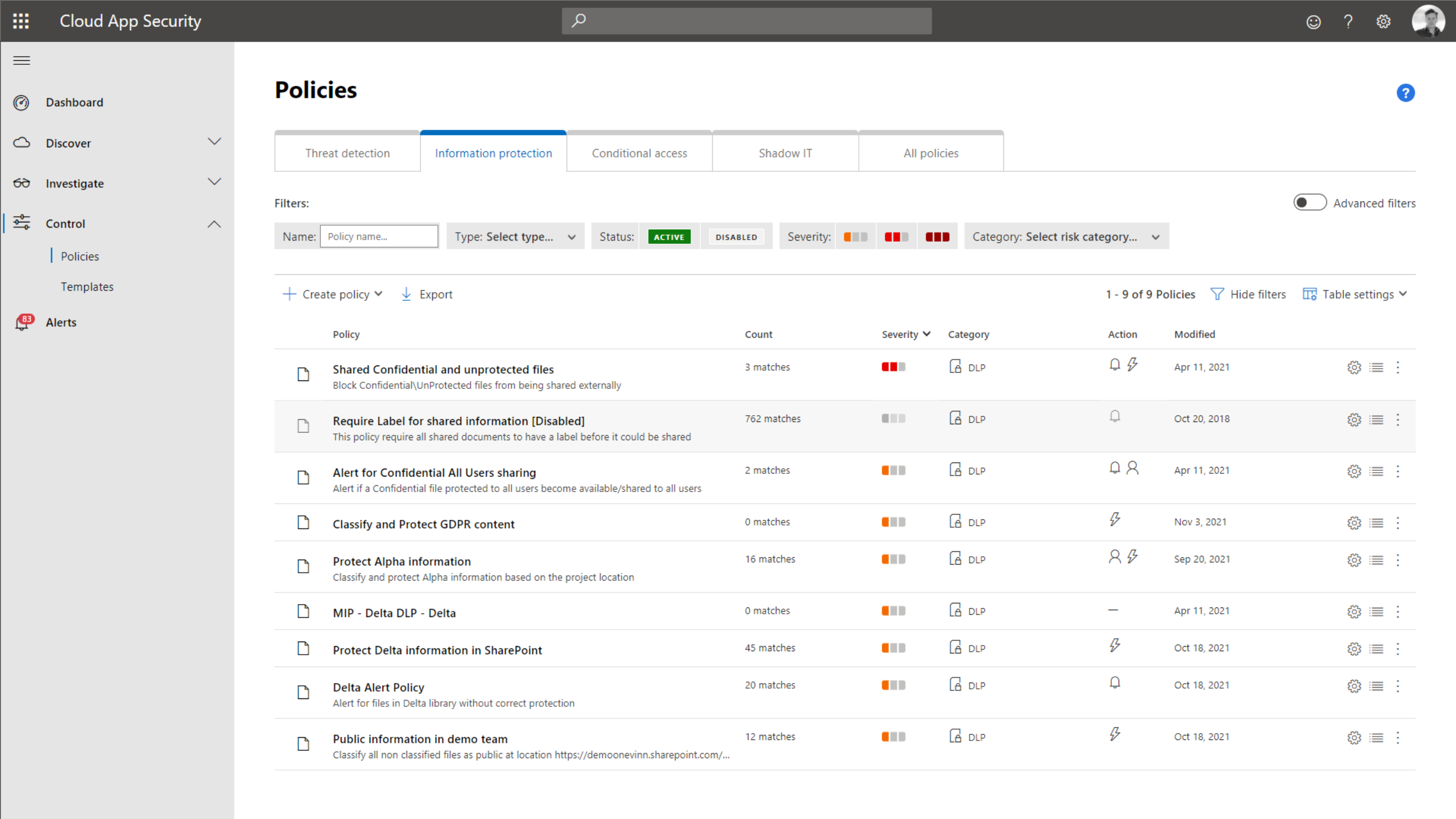

demoonevinn.portal.cloudappsecurity.com/#/audits/?entity=eq(o:(id:50d9ac08-1334-43ef-9d8c-58bea540c2f4,saas:i:11161,inst:i:0),)&location.country=eq(CA,)
Cloud App Security
Dashboard
Discover
Investigate
Control
Alerts
Activity log
Queries: Select a query
Save as
Advanced filters
Suggested queries (10)
Admin activities
Download activities
Failed log in
File and folder activities
Impersonation activities
Mailbox activities
Password changes and reset requests
Raw IP address:
Enter IP address...
Activity type: Select activity...
Location: Canada
1 - 13 of 13 activities
Show details
Hide filters
Table settings
User
App
IP address
Location
Device
Date
Run command: task MailItemsAccessed; Parameters: Session ID 07...
Log on
FilePreviewed: file https://demoonevinn.sharepoint.com/sites/Proj...
FilePreviewed: file https://demoonevinn.sharepoint.com/sites/Proj...
FilePreviewed: file https://demoonevinn-my.sharepoint.com/perso...
FilePreviewed: file https://demoonevinn.sharepoint.com/sites/Publ...
FilePreviewed: file https://demoonevinn.sharepoint.com/sites/Publ...
Log on

NORDIC
– VIRTUAL SUMMIT –

Information Protection

Identify and protect sensitive information


Defender for O365
MCAS
AAD
M365
OneLogin
Box
Google Cloud Platform
Cisco Webex
Google Workspace
GitHub
Okta
Dropbox
Salesforce
Workday
Slack
Amazon Web Services
ServiceNow
Smartsheet
Defender for Identity
FW
AD
Defender for EndPoint



Dashboard
Discover
Investigate
Control
Policies
Templates
Alerts 83

Policies

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 - 9 of 9 Policies | Hide filters | Table settings

Policy	Count	Severity	Category	Action	Modified
Shared Confidential and unprotected files Block Confidential\UnProtected files from being shared externally	3 matches		DLP		Apr 11, 2021
Require Label for shared information [Disabled] This policy require all shared documents to have a label before it could be shared	762 matches		DLP		Oct 20, 2018
Alert for Confidential All Users sharing Alert if a Confidential file protected to all users become available/shared to all users	2 matches		DLP		Apr 11, 2021
Classify and Protect GDPR content	0 matches		DLP		Nov 3, 2021
Protect Alpha information Classify and protect Alpha information based on the project location	16 matches		DLP		Sep 20, 2021
MIP - Delta DLP - Delta	0 matches		DLP	—	Apr 11, 2021
Protect Delta information in SharePoint	45 matches		DLP		Oct 18, 2021
Delta Alert Policy Alert for files in Delta library without correct protection	20 matches		DLP		Oct 18, 2021
Public information in demo team Classify all non classified files as public at location https://demoonevinn.sharepoint.com/...	12 matches		DLP		Oct 18, 2021

Dashboard
Discover
Investigate
Control
Policies
Templates
Alerts 83

Governance actions

Microsoft OneDrive for Business — Apply sensitivity label

- [ ] Send policy-match digest to file owner
- [ ] Notify specific users
- [ ] Make private
- [ ] Remove external users
- [ ] Inherit parent permissions
- [ ] Put in user quarantine
- [ ] Put in admin quarantine Configure a quarantine folder to enable this option
- [ ] Trash
- [ ] Remove a collaborator
- [x] Apply sensitivity label

Select an Microsoft Information Protection sensitivity label to apply to matching files:

Confidential-Recipients (all users) Encrypt

- Non Business
- Public
- Business
- Confidential-UnProtected
- Confidential-Internal View Only
- Confidential-Internal edit, copy and print
- Confidential-Internal Full Control
- Confidential-Custom Permission
- Confidential-Recipients (all users) Encrypt
- Confidential-Recipient Do Not Forward

Micr — Apply sensitivity label

Dashboard
Discover
Investigate
Control
Policies
Templates
Alerts 83

Policies

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 - 9 of 9 Policies | Hide filters | Table settings

Policy	Count	Severity	Category	Action	Modified
Shared Confidential and unprotected files Block Confidential\UnProtected files from being shared externally	3 matches		DLP		Apr 11, 2021
Require Label for shared information [Disabled] This policy require all shared documents to have a label before it could be shared	762 matches		DLP		Oct 20, 2018
Alert for Confidential All Users sharing Alert if a Confidential file protected to all users become available/shared to all users	2 matches		DLP		Apr 11, 2021
Classify and Protect GDPR content	0 matches		DLP		Nov 3, 2021
Protect Alpha information Classify and protect Alpha information based on the project location	16 matches		DLP		Sep 20, 2021
MIP - Delta DLP - Delta	0 matches		DLP	—	Apr 11, 2021
Protect Delta information in SharePoint	45 matches		DLP		Oct 18, 2021
Delta Alert Policy Alert for files in Delta library without correct protection	20 matches		DLP		Oct 18, 2021
Public information in demo team Classify all non classified files as public at location https://demoonevinn.sharepoint.com/...	12 matches		DLP		Oct 18, 2021

Dashboard
Discover
Investigate
Control
Policies
Templates
Alerts 83

all file owners

Inspection method

None

Alerts

Create an alert for each matching file

Governance actions

Microsoft OneDrive for Business

Microsoft SharePoint Online — Apply sensitivity label

Send policy-match digest to file owner

Notify specific users

Make private

Remove external users

Inherit parent permissions

Put in user quarantine

Put in admin quarantine Configure a quarantine folder to enable this option

Trash

Remove a collaborator

Apply sensitivity label

Select an Microsoft Information Protection sensitivity label to apply to matching files:

Confidential-Project Delta

Cloud App Security

Dashboard
Discover
Investigate
Control
Policies
Templates
Alerts 83

all file owners

Search

Teams
Your teams
Public team
Company internal
Project Delta
General
Project Alpha
Project X
Hidden teams
Join or create a team

Activity
Chat
Teams
Calendar
Calls
Files
Apps
Help

General Posts Files Wiki

New Upload Sync Copy link All Documents*

Documents > General

Name	Sensitivity	Modified By
Budget November.xlsx	Confidential \ Project Delta	Peter Davidsson
Business changes draft.pptx	Confidential \ Project Delta	SharePoint-program
Business Changes.pptx	Confidential \ Project Delta	SharePoint-program
Business presentation 2020.pp...	Secret \ Cooperation with Onevinn and	Anders Olsson
Conf Delta info.docx	Confidential \ Project Delta	Anders Olsson
Delta info for the business.docx	Business	Anders Olsson
Delta news.docx	Confidential \ Project Delta	Peter Davidsson
Finance changes.xlsx	Secret \ Internal Edit permission	Peter Davidsson

Put in admin quarantine Configure a quarantine folder to enable this option

Trash

Remove a collaborator

Apply sensitivity label

Select an Microsoft Information Protection sensitivity label to apply to matching files:

Confidential-Project Delta

NORDIC
– VIRTUAL SUMMIT –

Information Protection

Meet regulation about data handling

Block cloud storage for classified information

Prevent data leakage by blocking downloads

Dashboard > Conditional Access >

AO - MCAS for Office365

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 *

AO - MCAS for Office365

Assignments

Users and groups

Specific users included

Cloud apps or actions

1 app included

Conditions

2 conditions selected

Access controls

Grant

0 controls selected

Session

Use Conditional Access App Control

Enable policy

Report-only | On | Off

Save

Session

Control user access based on session controls to enable limited experiences within specific cloud applications.
Learn more

- [ ] Use app enforced restrictions
- [x] Use Conditional Access App Control

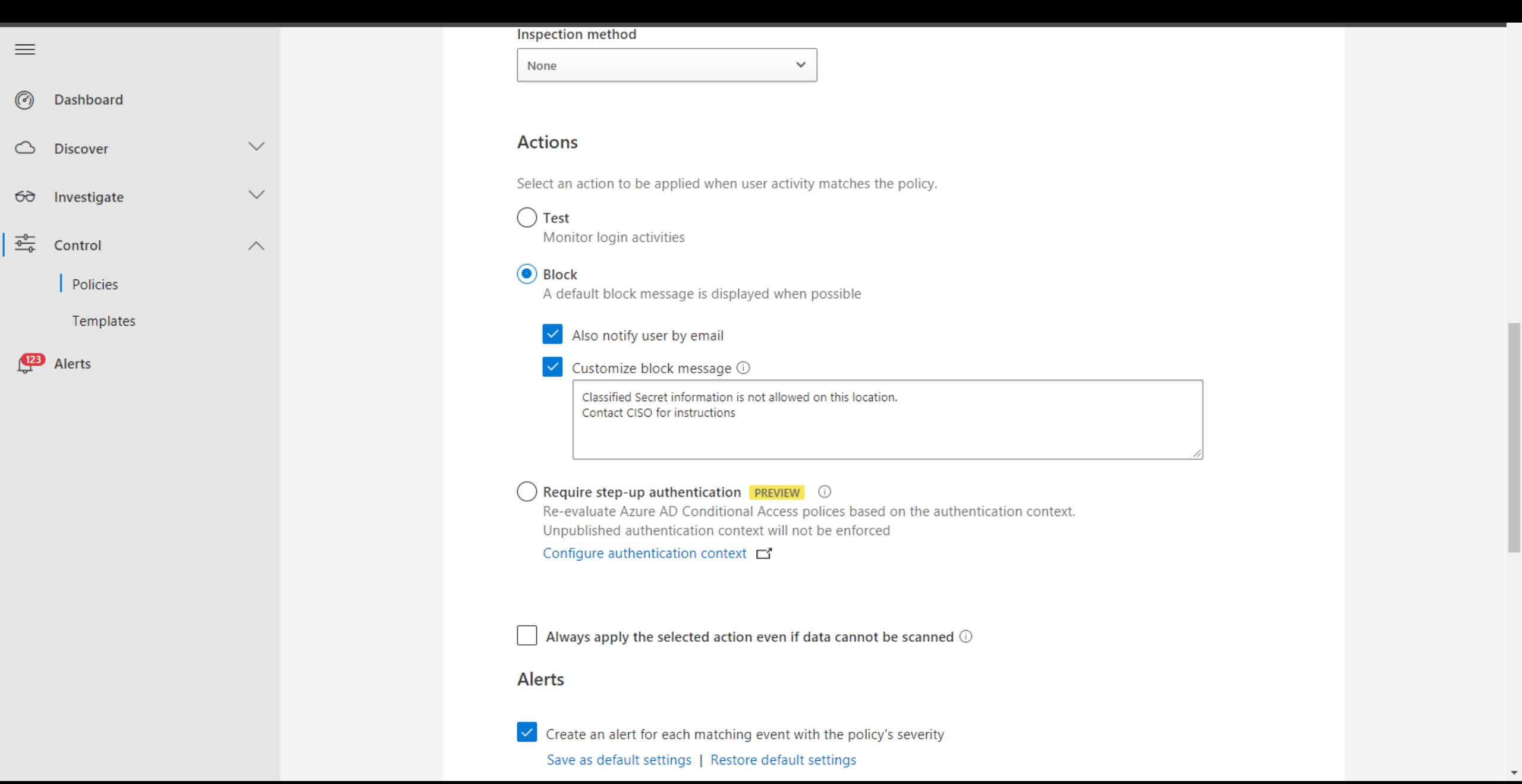
Use custom policy...

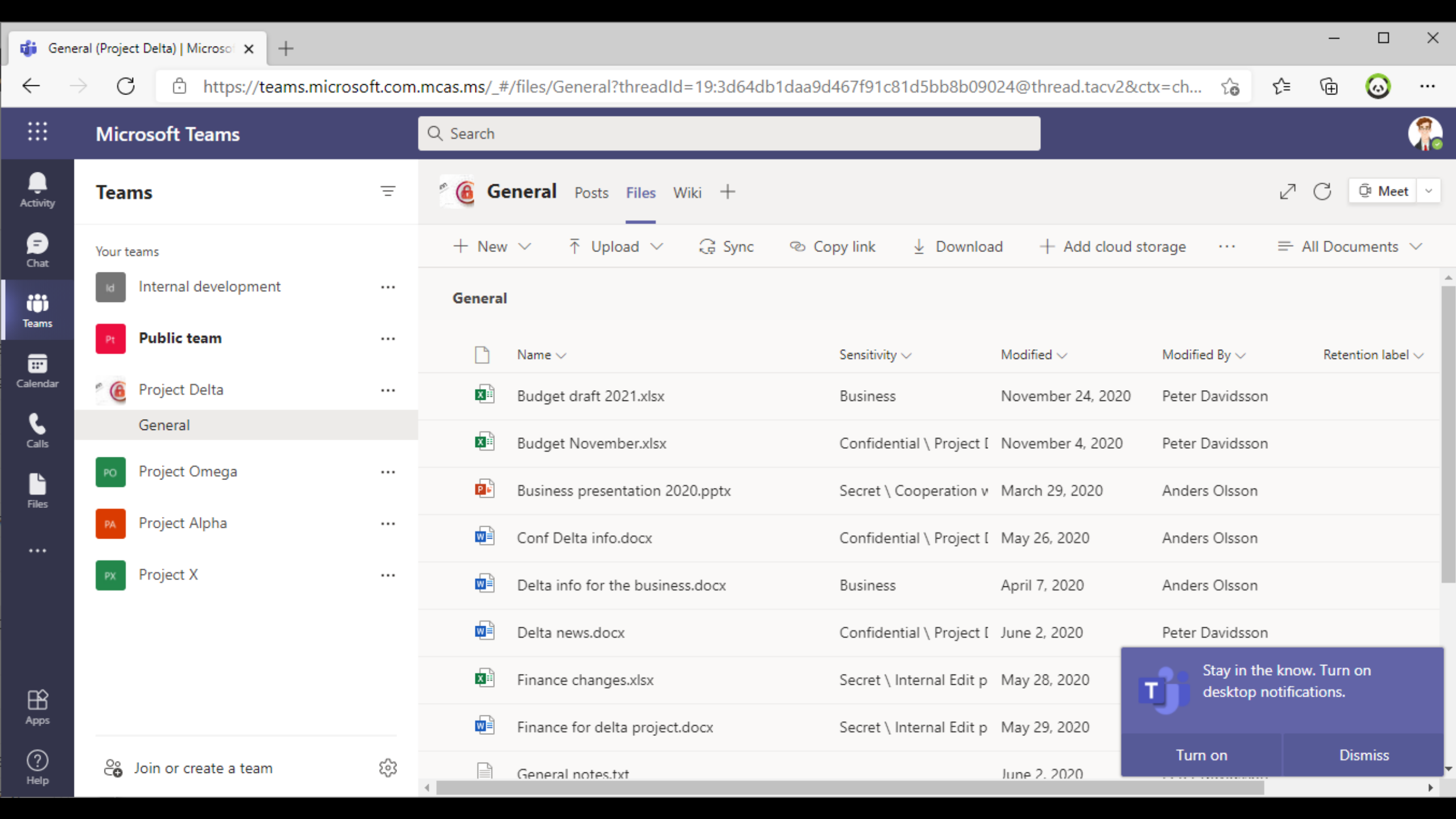
Custom policies need to be configured in Cloud App Security portal. This control works instantly for featured apps and can be self onboarded for any app. Click here to learn more about both scenarios.

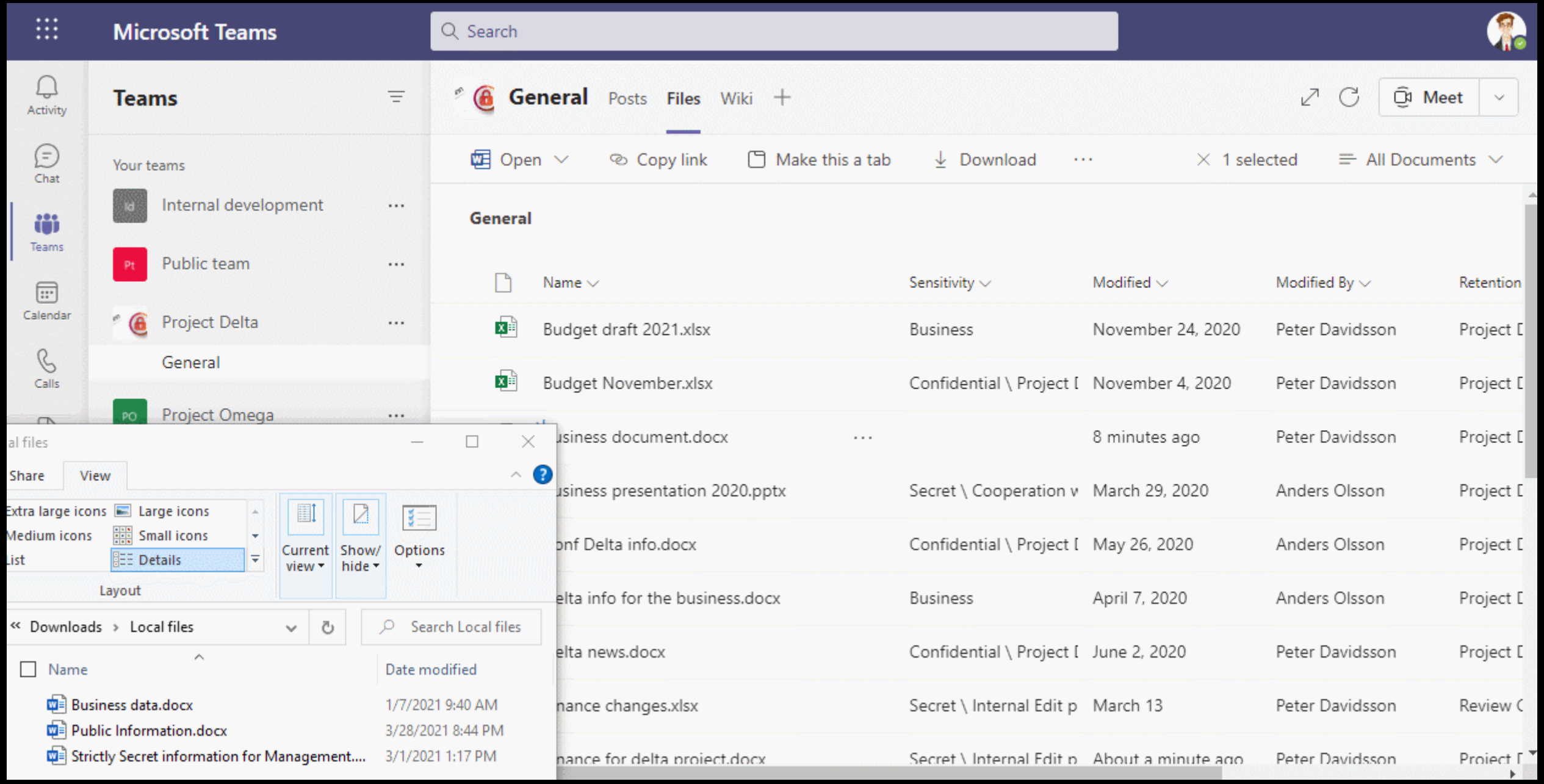
Configure custom policy

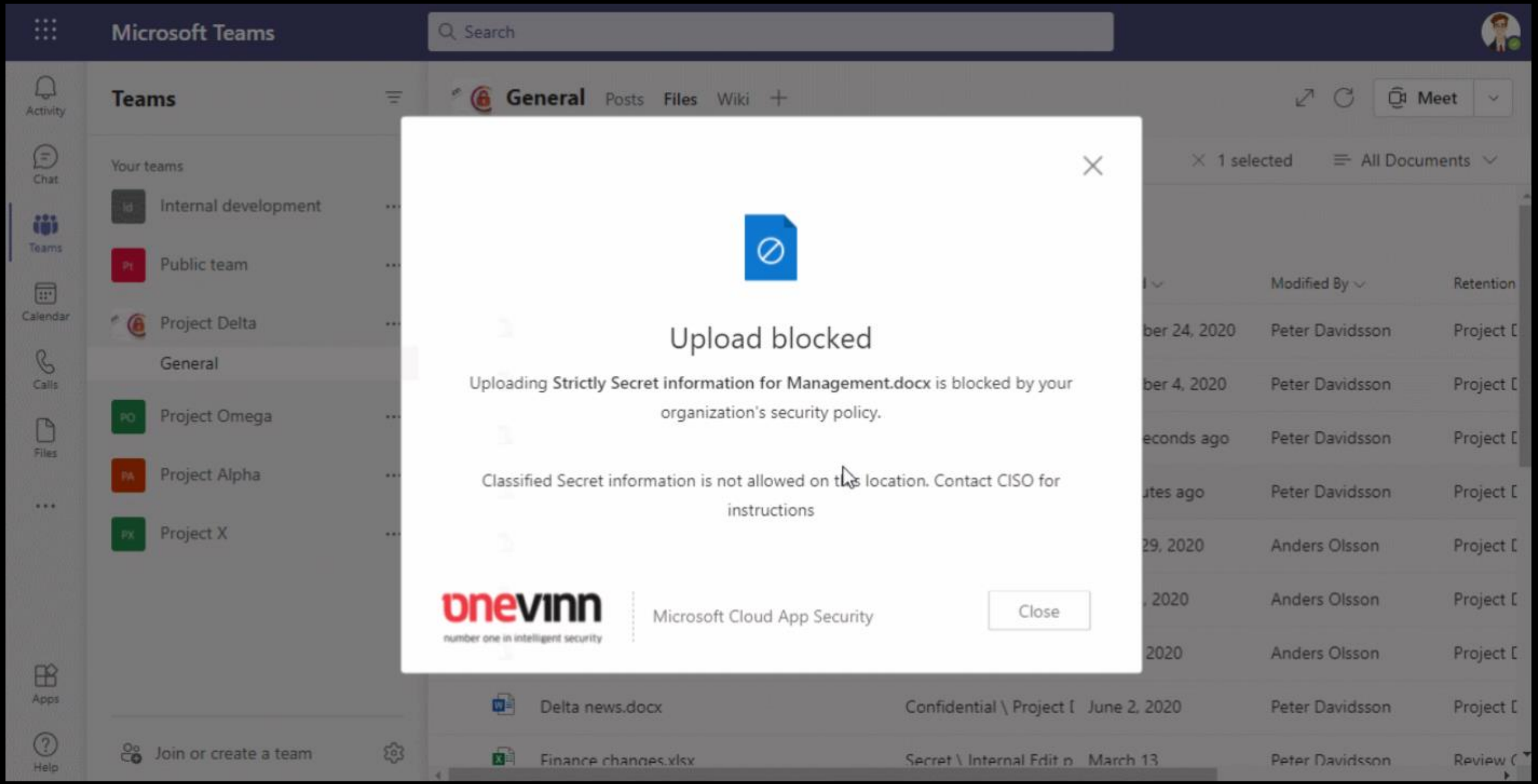
- [ ] Sign-in frequency
- [ ] Persistent browser session

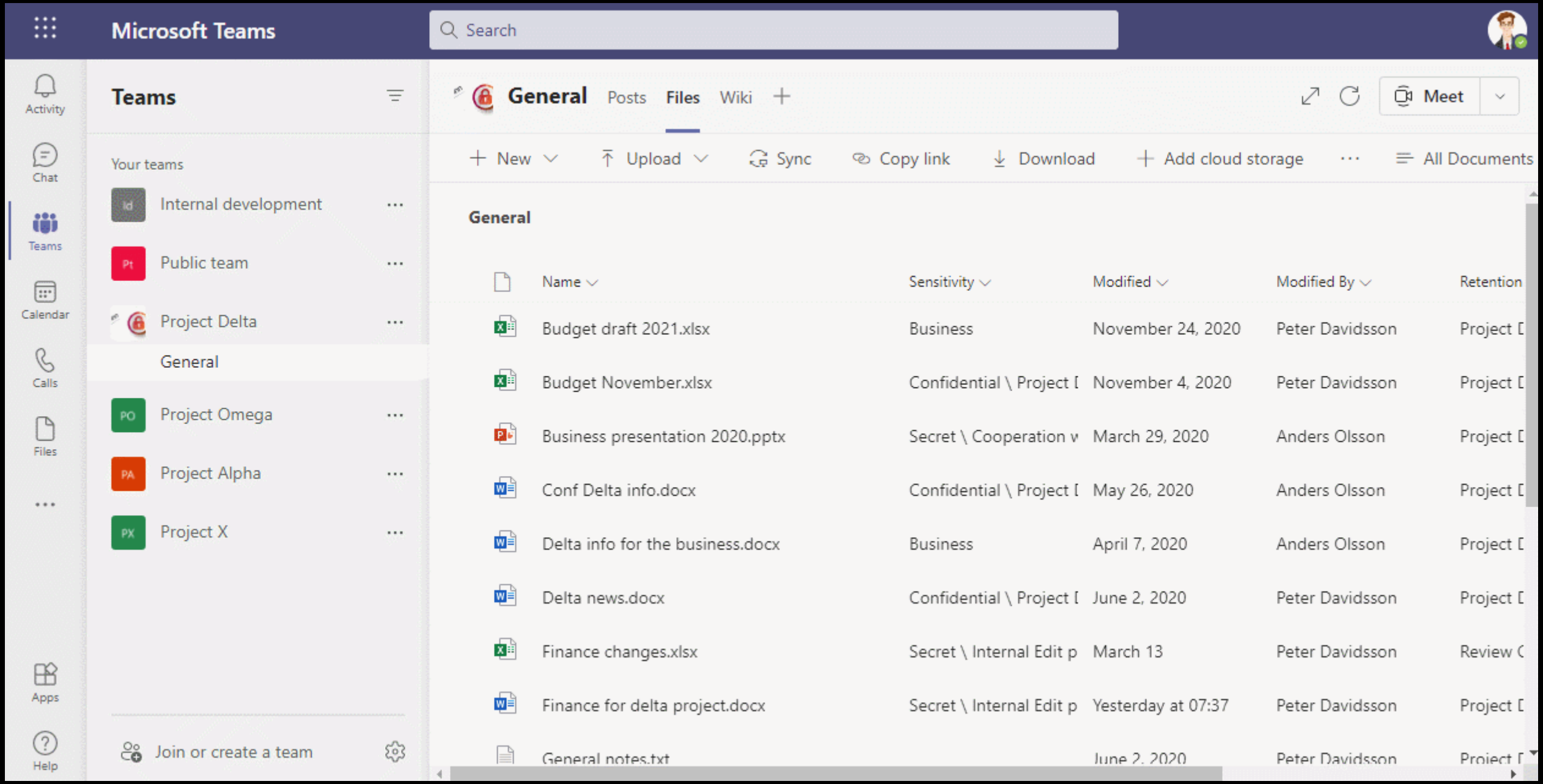
Select


Dashboard
Discover
Investigate
Control
Policies
Templates
123
Alerts
Inspection method
None
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
Also notify user by email
Customize block message
Classified Secret information is not allowed on this location.
Contact CISO for instructions
Require step-up authentication
PREVIEW
Re-evaluate Azure AD Conditional Access polices based on the authentication context.
Unpublished authentication context will not be enforced
Configure authentication context
Always apply the selected action even if data cannot be scanned
Alerts
Create an alert for each matching event with the policy's severity
Save as default settings | Restore default settings


General (Project Delta) | Microso
https://teams.microsoft.com.mcas.ms/_#/files/General?threadId=19:3d64db1daa9d467f91c81d5bb8b09024@thread.tacv2&ctx=ch...
Microsoft Teams
Search
Activity
Chat
Teams
Calendar
Calls
Files
Apps
Help
Teams
Your teams
Internal development
Public team
Project Delta
General
Project Omega
Project Alpha
Project X
Join or create a team
General
Posts
Files
Wiki
Meet
New
Upload
Sync
Copy link
Download
Add cloud storage
All Documents
General
Name
Sensitivity
Modified
Modified By
Retention label
Budget draft 2021.xlsx
Business
November 24, 2020
Peter Davidsson
Budget November.xlsx
Confidential \ Project [
November 4, 2020
Peter Davidsson
Business presentation 2020.pptx
Secret \ Cooperation v
March 29, 2020
Anders Olsson
Conf Delta info.docx
Confidential \ Project [
May 26, 2020
Anders Olsson
Delta info for the business.docx
Business
April 7, 2020
Anders Olsson
Delta news.docx
Confidential \ Project [
June 2, 2020
Peter Davidsson
Finance changes.xlsx
Secret \ Internal Edit p
May 28, 2020
Finance for delta project.docx
Secret \ Internal Edit p
May 29, 2020
General notes.txt
June 2, 2020
Stay in the know. Turn on desktop notifications.
Turn on
Dismiss


Microsoft Teams
Search
Activity
Chat
Teams
Calendar
Calls
Teams
Your teams
Internal development
Public team
Project Delta
General
Project Omega
General
Posts
Files
Wiki
Meet
Open
Copy link
Make this a tab
Download
1 selected
All Documents
General
Name
Sensitivity
Modified
Modified By
Retention
Budget draft 2021.xlsx
Business
November 24, 2020
Peter Davidsson
Budget November.xlsx
Confidential \ Project [
November 4, 2020
Peter Davidsson
usiness document.docx
8 minutes ago
Peter Davidsson
usiness presentation 2020.pptx
Secret \ Cooperation v
March 29, 2020
Anders Olsson
onf Delta info.docx
Confidential \ Project [
May 26, 2020
Anders Olsson
elta info for the business.docx
Business
April 7, 2020
Anders Olsson
elta news.docx
Confidential \ Project [
June 2, 2020
Peter Davidsson
nance changes.xlsx
Secret \ Internal Edit p
March 13
Peter Davidsson
nance for delta project.docx
Secret \ Internal Edit p
About a minute ago
Peter Davidsson
al files
Share
View
Extra large icons
Large icons
Medium icons
Small icons
List
Details
Layout
Current view
Show/ hide
Options
Downloads
Local files
Search Local files
Name
Date modified
Business data.docx
1/7/2021 9:40 AM
Public Information.docx
3/28/2021 8:44 PM
Strictly Secret information for Management....
3/1/2021 1:17 PM


Microsoft Teams
Search
Activity
Chat
Teams
Calendar
Calls
Files
Apps
Help
Teams
Your teams
Internal development
Public team
Project Delta
General
Project Omega
Project Alpha
Project X
Join or create a team
General
Posts
Files
Wiki
Meet
1 selected
All Documents
Modified By
Retention
Upload blocked
Uploading Strictly Secret information for Management.docx is blocked by your organization's security policy.
Classified Secret information is not allowed on this location. Contact CISO for instructions
onevinn
number one in intelligent security
Microsoft Cloud App Security
Close
Delta news.docx
Confidential \ Project [
June 2, 2020
Peter Davidsson
Project [
Finance changes.xlsx
Secret \ Internal Edit p
March 13
Peter Davidsson
Review C


Microsoft Teams
Search
Activity
Chat
Teams
Calendar
Calls
Files
Apps
Help
Teams
Your teams
Internal development
Public team
Project Delta
General
Project Omega
Project Alpha
Project X
Join or create a team
General
Posts
Files
Wiki
Meet
New
Upload
Sync
Copy link
Download
Add cloud storage
All Documents
General
Name
Sensitivity
Modified
Modified By
Retention
Budget draft 2021.xlsx
Business
November 24, 2020
Peter Davidsson
Budget November.xlsx
Confidential \ Project [
November 4, 2020
Peter Davidsson
Business presentation 2020.pptx
Secret \ Cooperation v
March 29, 2020
Anders Olsson
Conf Delta info.docx
Confidential \ Project [
May 26, 2020
Anders Olsson
Delta info for the business.docx
Business
April 7, 2020
Anders Olsson
Delta news.docx
Confidential \ Project [
June 2, 2020
Peter Davidsson
Finance changes.xlsx
Secret \ Internal Edit p
March 13
Peter Davidsson
Finance for delta project.docx
Secret \ Internal Edit p
Yesterday at 07:37
Peter Davidsson
General notes.txt
June 2, 2020
Peter Davidsson

NORDIC
– VIRTUAL SUMMIT –

Information Protection

Prevent password sharing

Microsoft Teams

Search

Activity
Chat
Teams
Calendar
Calls
Files
Apps
Help

Teams

Your teams

- Internal development
- Public team
- Project Delta
- Project Omega
- Project Alpha
  - General
- Project X

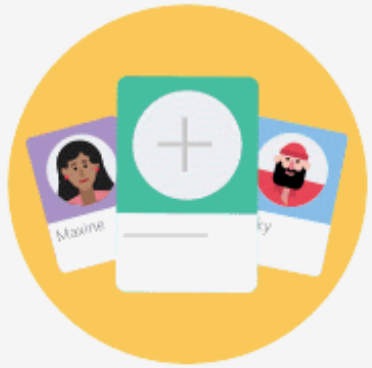
Join or create a team

PA General Posts Files Wiki +

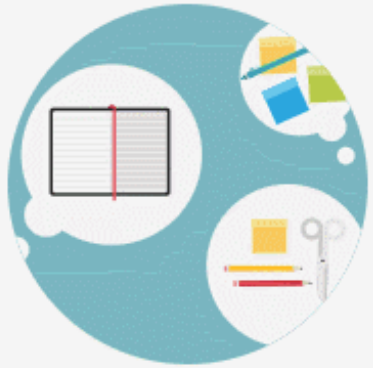
Team | Secret internal site

Meet

Here are some things to get going...



Add more people



Create more channels

Open the FAQ

Peter Davidsson 1/26 1:45 PM
Welcome to project Alpha

Reply

New conversation

Thanks for listening!

- Anders Olsson
- IT/Information Security Advisor
- Twitter @AndersPsYnet
- MVP

NORDIC — VIRTUAL SUMMIT —