Protect Office 365 and more with EMS

Jan Ketil Skanke – Enterprise Mobility MVP

COO and Principal Cloud Architect @CloudWay

Experts Live Netherlands

Jan Ketil Skanke

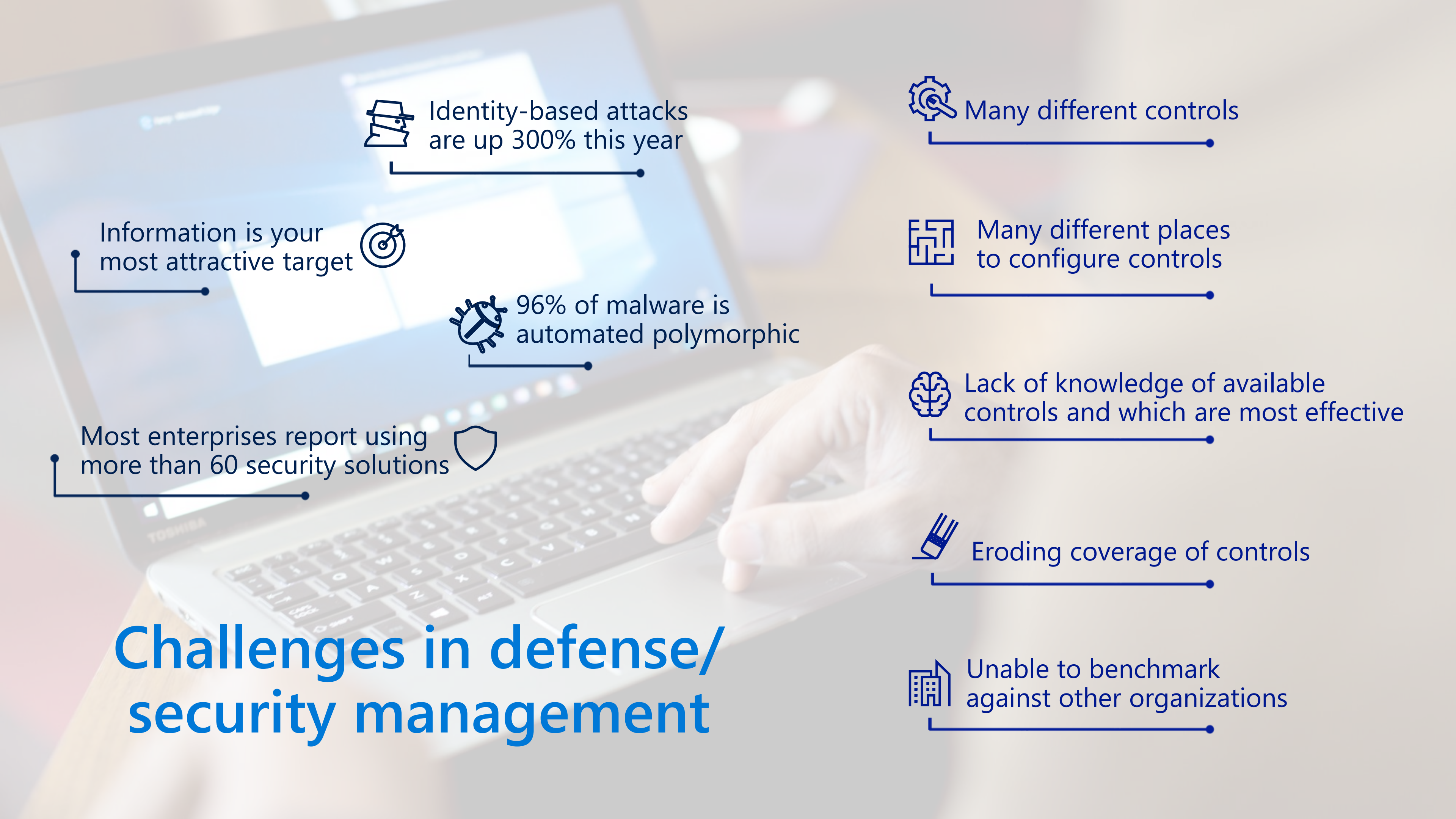
MVP Enterprise Mobility

Partner and Princial Cloud Architect

CloudWay

Twitter: @JankeSkanke

How good is your security?



Challenges in defense/ security management

Identity-based attacks are up 300% this year

Information is your most attractive target

96% of malware is automated polymorphic

Most enterprises report using more than 60 security solutions

Many different controls

Many different places to configure controls

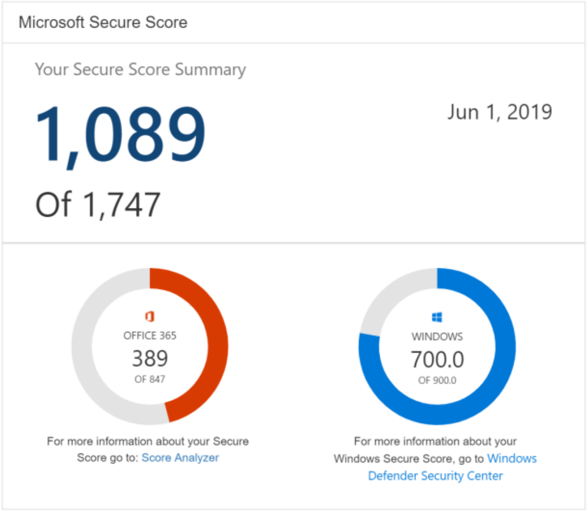
Lack of knowledge of available controls and which are most effective

Eroding coverage of controls

Unable to benchmark against other organizations

Assess your current situation

https//securescore.microsoft.com



Microsoft Secure Score

Your Secure Score Summary

1,089

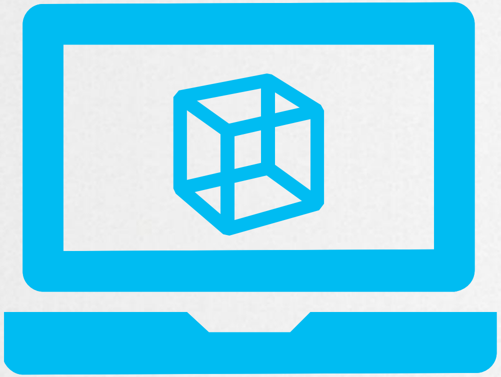
Of 1,747

Jun 1, 2019

For more information about your Secure Score go to: Score Analyzer

For more information about your Windows Secure Score, go to Windows Defender Security Center

Secure Score



Score-based framework

Calculates a security score based on current security settings and behaviours and compares it to a baseline asserted by Microsoft

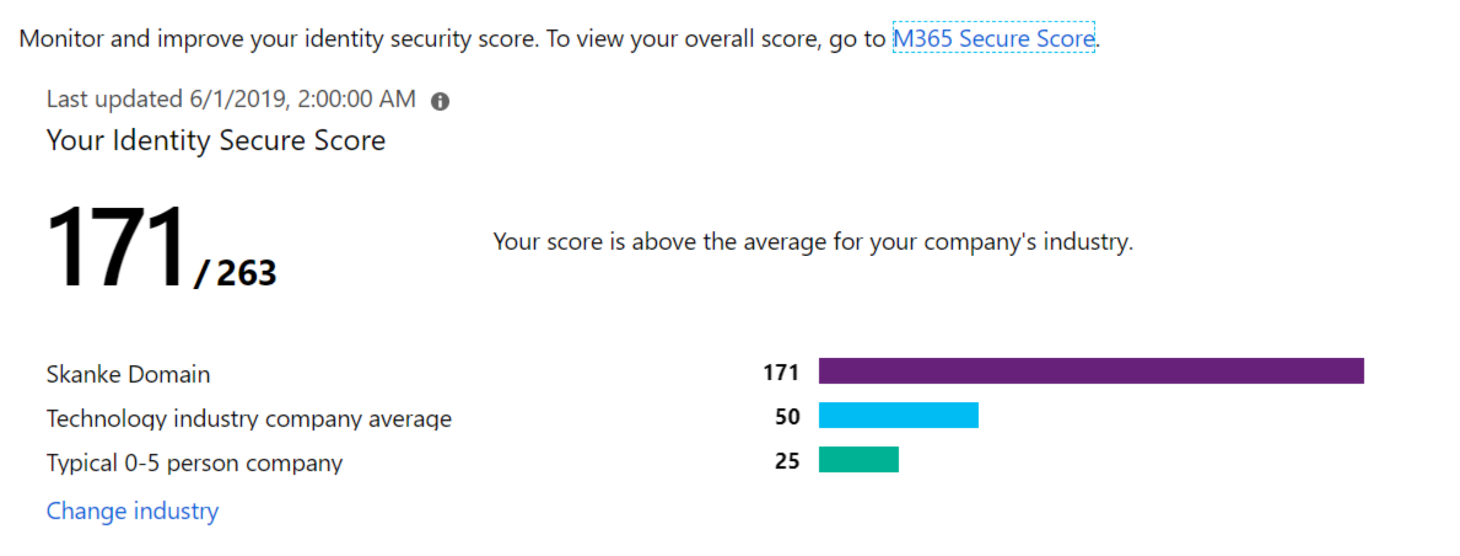
Insights into your security position

One place to understand your security position and what features you have enabled

Guidance to increase your security level

Learn what security features are available to reduce risk while helping you balance productivity and security

Identity Secure Score



Monitor and improve your identity security score. To view your overall score, go to M365 Secure Score.

Last updated 6/1/2019, 2:00:00 AM ⓘ

Your Identity Secure Score

171 / 263

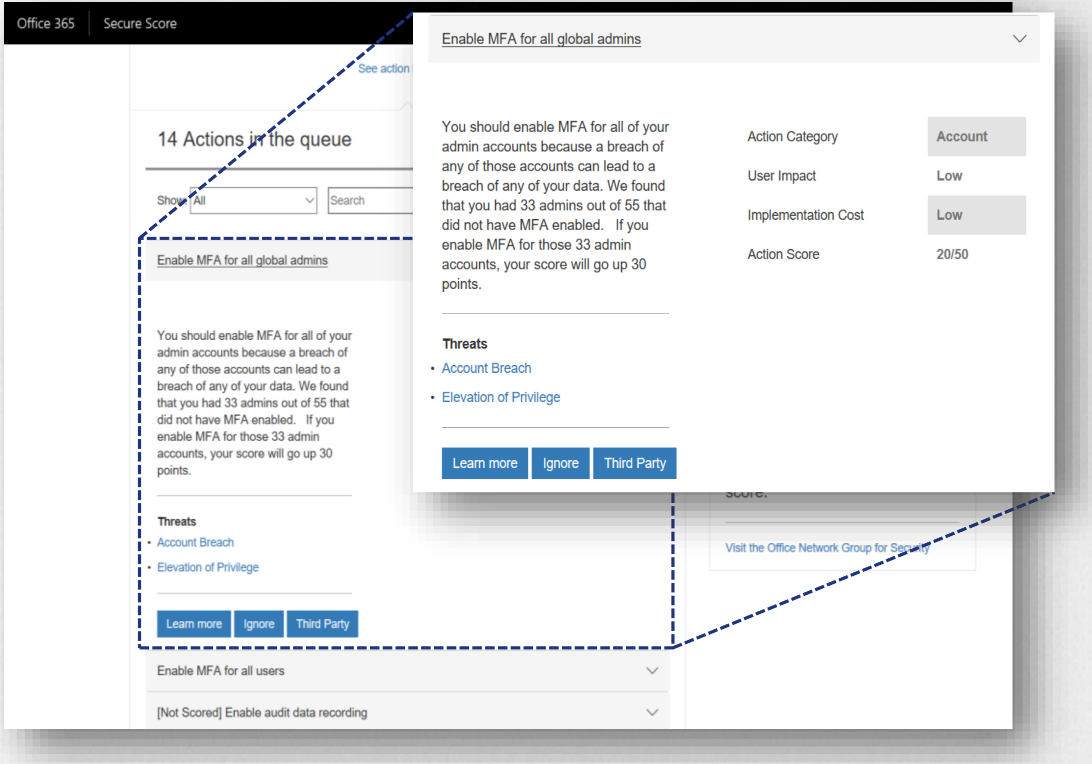
Your score is above the average for your company's industry.

Skanke Domain	171
Technology industry company average	50
Typical 0-5 person company	25

Change industry

Enable controls through Secure Score

Get more details and enable control or take you to where you can enable



Enable MFA for all global admins

You should enable MFA for all of your admin accounts because a breach of any of those accounts can lead to a breach of any of your data. We found that you had 33 admins out of 55 that did not have MFA enabled. If you enable MFA for those 33 admin accounts, your score will go up 30 points.

Action Category	Account
User Impact	Low
Implementation Cost	Low
Action Score	20/50

Threats

- Account Breach
- Elevation of Privilege

Enable MFA for all global admins

You should enable MFA for all of your admin accounts because a breach of any of those accounts can lead to a breach of any of your data. We found that you had 33 admins out of 55 that did not have MFA enabled. If you enable MFA for those 33 admin accounts, your score will go up 30 points.

Threats

- Account Breach
- Elevation of Privilege

Learn more Ignore Third Party

Enable MFA for all users

[Not Scored] Enable audit data recording

score.

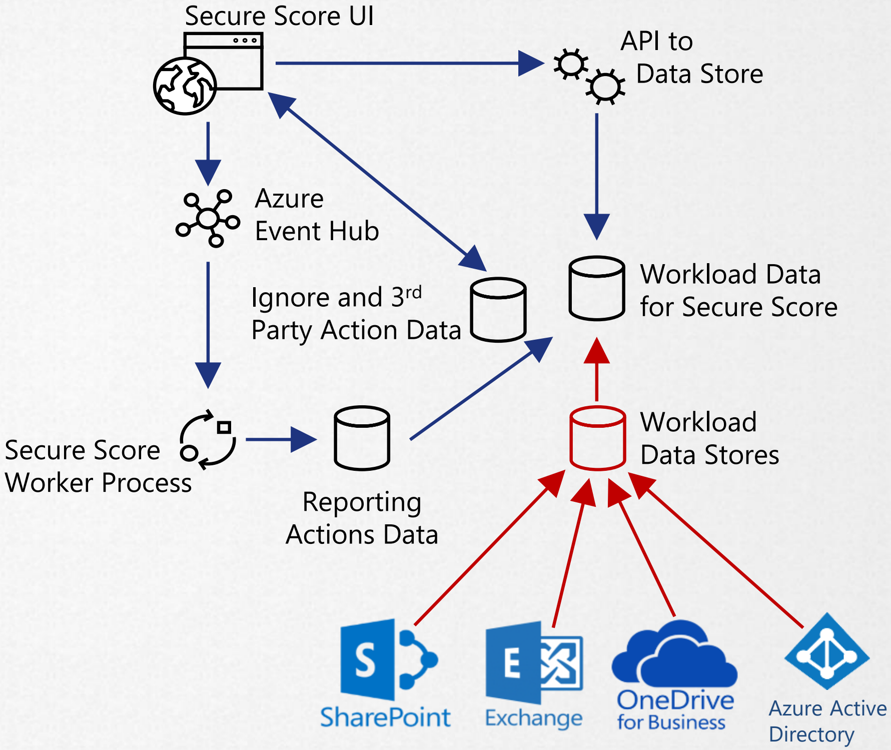
Visit the Office Network Group for Security

How scores get calculated

Nightly process collects telemetry from workloads

Ignore and 3rd party information is stored in another location

Reviewing report data is anonymized and store separately



MICROSOFT 365

Identity Based Approach

COMPAREX A SoftwareONE Company KPN ICT Consulting Sterk in ICT-advies Microsoft

Identity Based Approach

Device Trust

Identity Based Approach

Device Trust

MAM vs MDM?

MICROSOFT 365

Identity Based Approach

Device Trust

MAM vs MDM?

Health and Compliance?

COMPAREX A SoftwareONE Company

KPN ICT Consulting Sterk in ICT-advies

Microsoft

MICROSOFT 365

Identity Based Approach

Device Trust

MAM vs MDM?

Health and Compliance

Data Security

Identity Based Security

Identity driven approach

- **MFA / Conditional Access**

Risk

- **Can we trust their device?**

Who and What are accessing your data?

MICROSOFT 365

Getting the basics rights

Strengthen **your credentials**

MFA reduces compromise by 99.99%

Reduce **your attack surface**

Blocking legacy authentication reduces compromise by 66%.

Automate **threat response**

Implementing risk policies reduces compromise by 96%

Increase **your awareness with auditing and monitor security alerts**

Attackers escape detection inside a victim's network for a median of 101 days. *(Source: FireEye)*

Enable **self-help for more predictable and complete end user security**

60% of enterprises experienced social engineering attacks in 2016. *(Source: Agari)*

COMPAREX A SoftwareONE Company

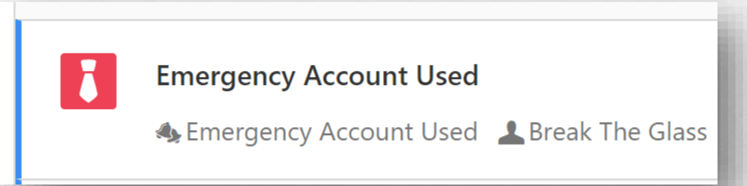
KPN ICT Consulting Sterk in ICT-advies

Microsoft

“Less than 2% of tenant admins have MFA enabled”

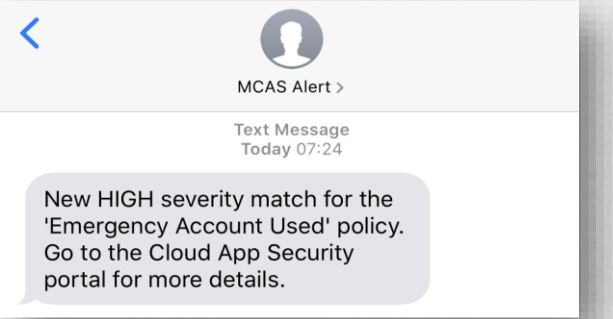
Secure Privileged Access

- Create a “Break The Glass” account
- Setup MFA on “all” Privileged roles
- Use AAD Privileged Identity MGMT
- Monitor usage – Alerting



Emergency Account Used

Emergency Account Used   Break The Glass



MCAS Alert >

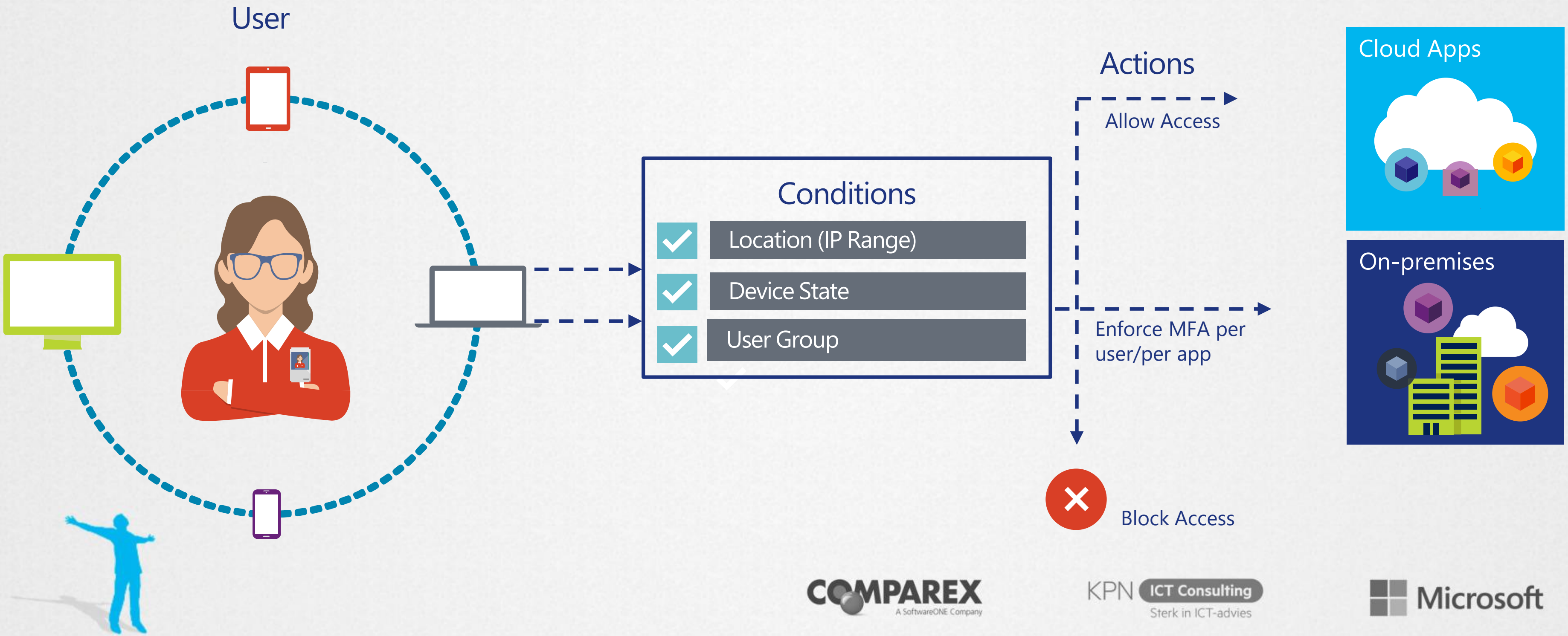
Text Message
Today 07:24

New HIGH severity match for the 'Emergency Account Used' policy. Go to the Cloud App Security portal for more details.

Secure ALL your users

- Enable MFA the Right Way
- Use Conditional Access
- Protect ALL your apps
- Trust on Device Level
- Risk Based Policies
    - MDATP and AAD Identity Protection

Conditional Access



User

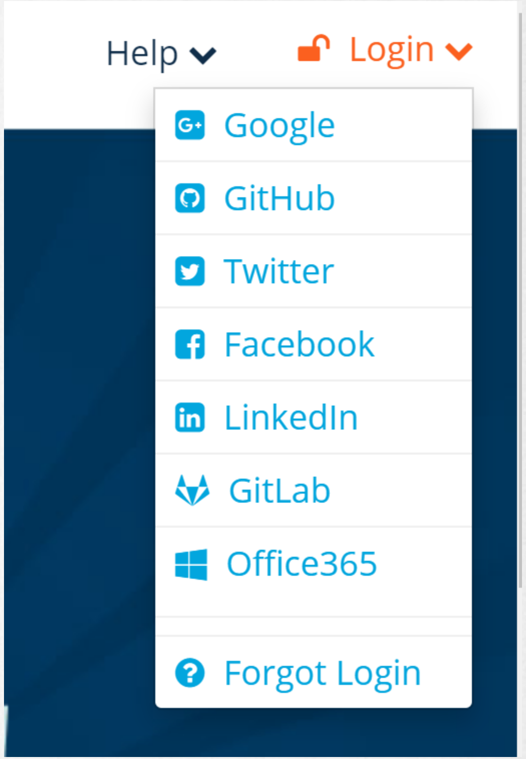
Conditions

- ✓ Location (IP Range)
- ✓ Device State
- ✓ User Group

Actions

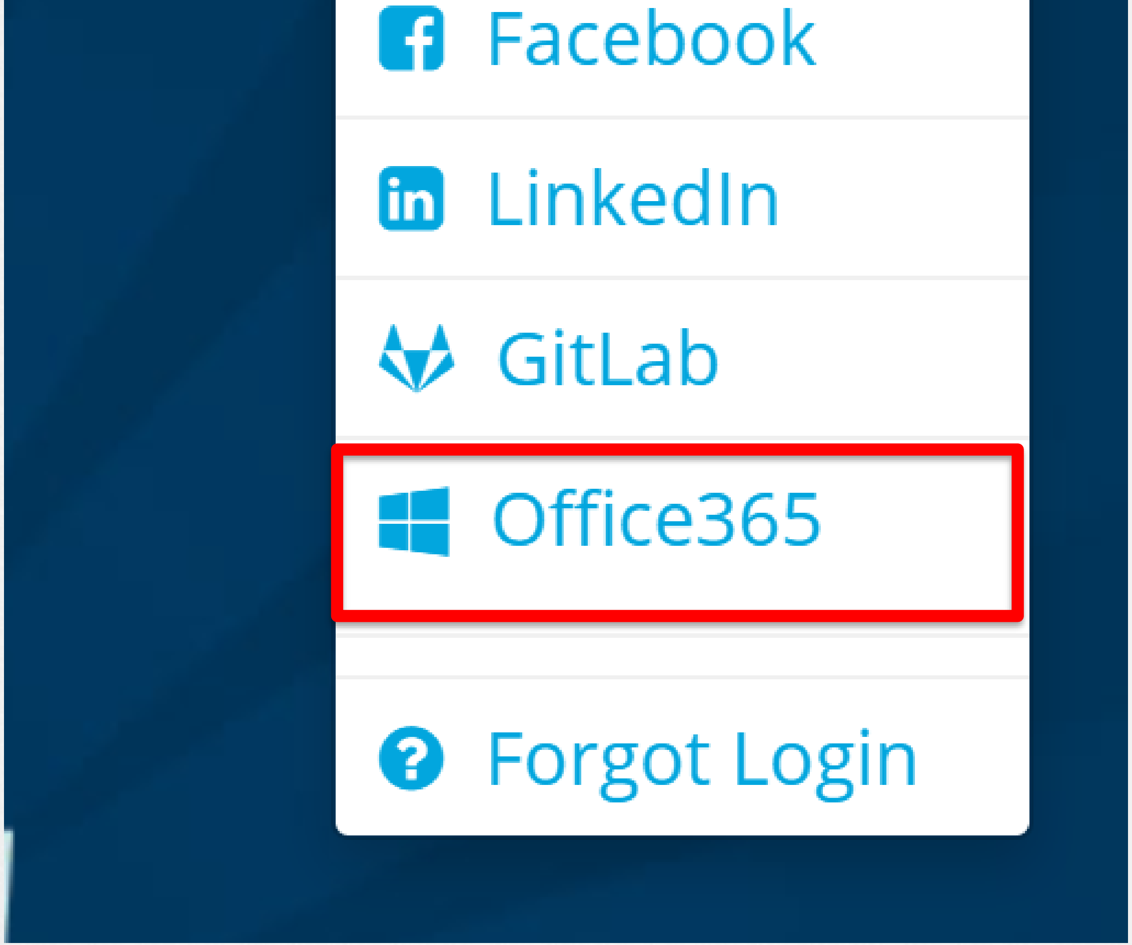
- Allow Access
- Enforce MFA per user/per app
- Block Access

What about those Oauth Apps?



MICROSOFT 365

What about those Oauth Apps?



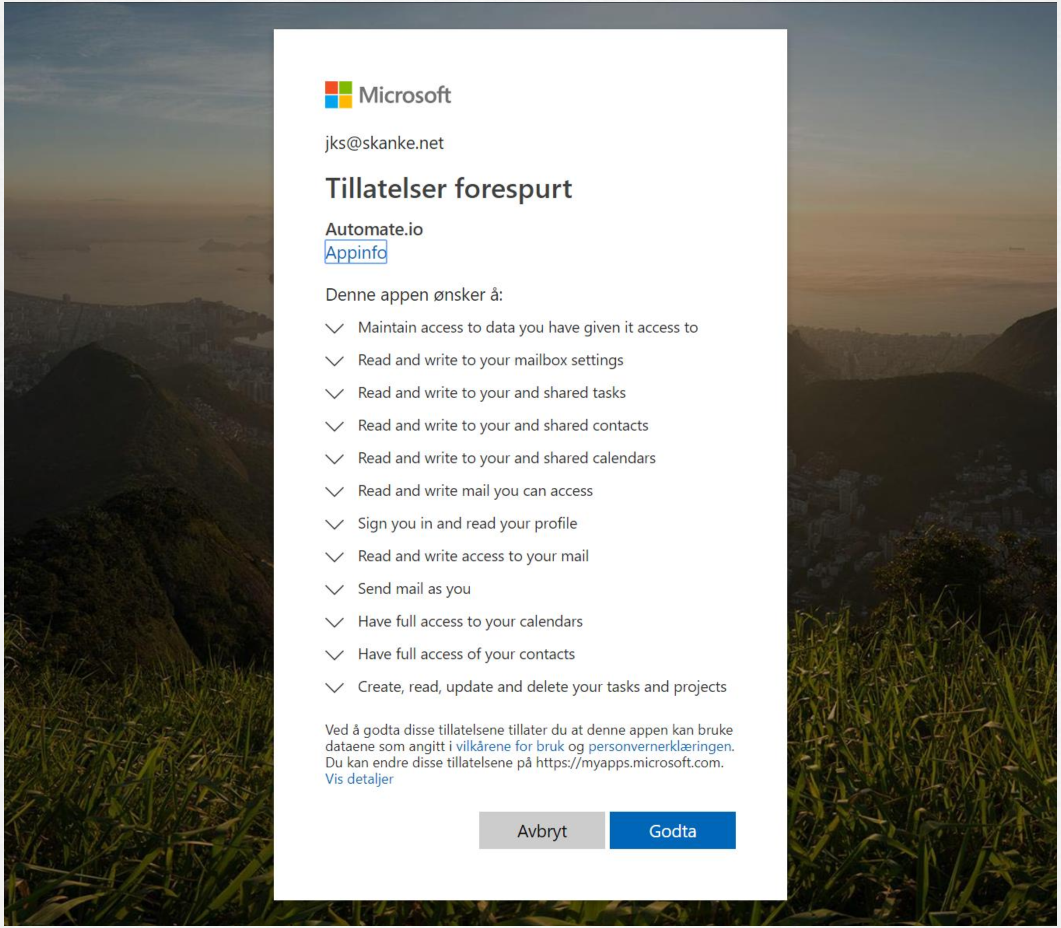
Facebook

LinkedIn

GitLab

Office365

Forgot Login



Microsoft

jks@skanke.net

Tillatelser forespurt

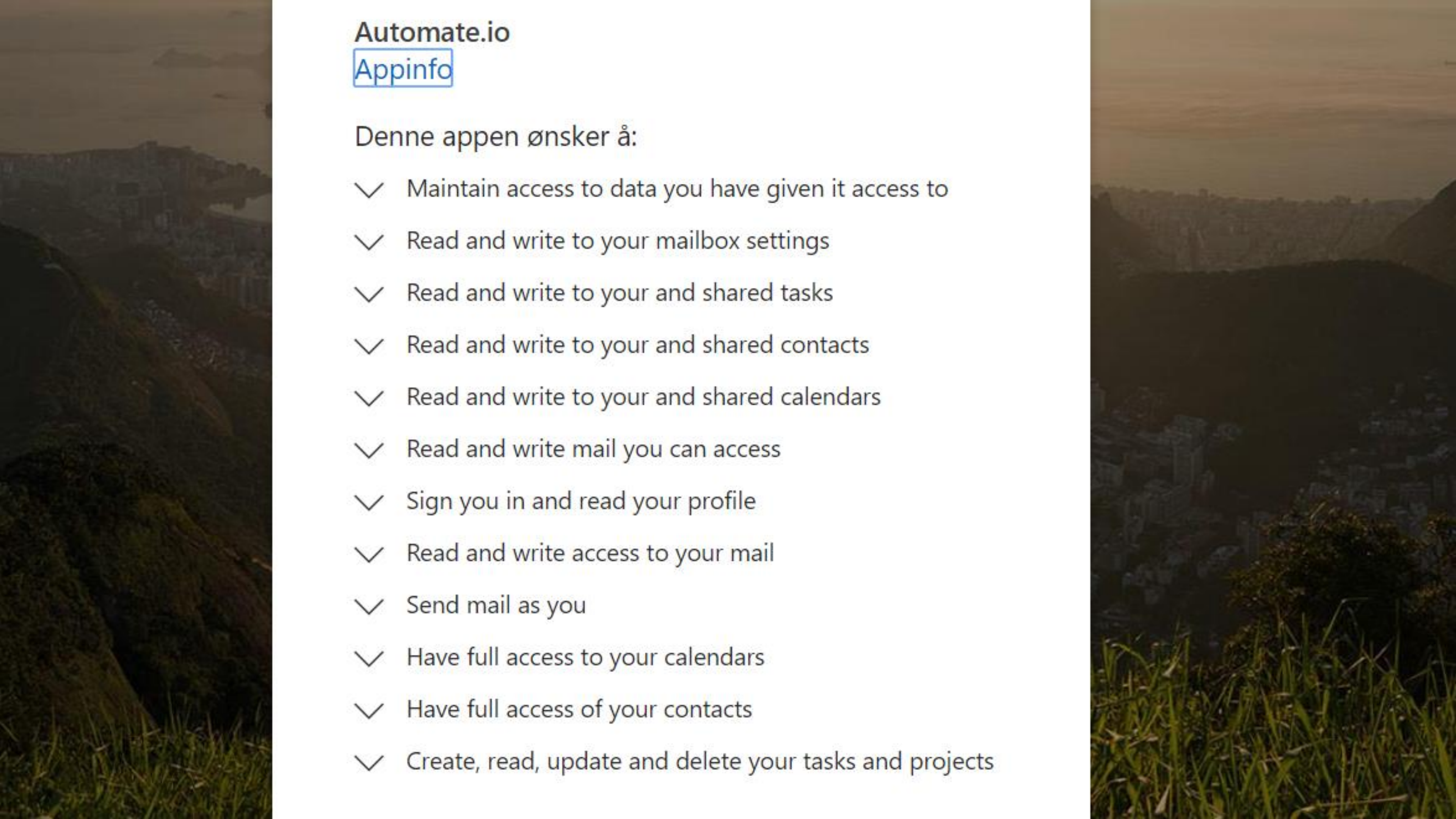
Automate.io

Appinfo

Denne appen ønsker å:

- Maintain access to data you have given it access to
- Read and write to your mailbox settings
- Read and write to your and shared tasks
- Read and write to your and shared contacts
- Read and write to your and shared calendars
- Read and write mail you can access
- Sign you in and read your profile
- Read and write access to your mail
- Send mail as you
- Have full access to your calendars
- Have full access of your contacts
- Create, read, update and delete your tasks and projects

Ved å godta disse tillatelsene tillater du at denne appen kan bruke dataene som angitt i vilkårene for bruk og personvernerklæringen. Du kan endre disse tillatelsene på https://myapps.microsoft.com.
Vis detaljer

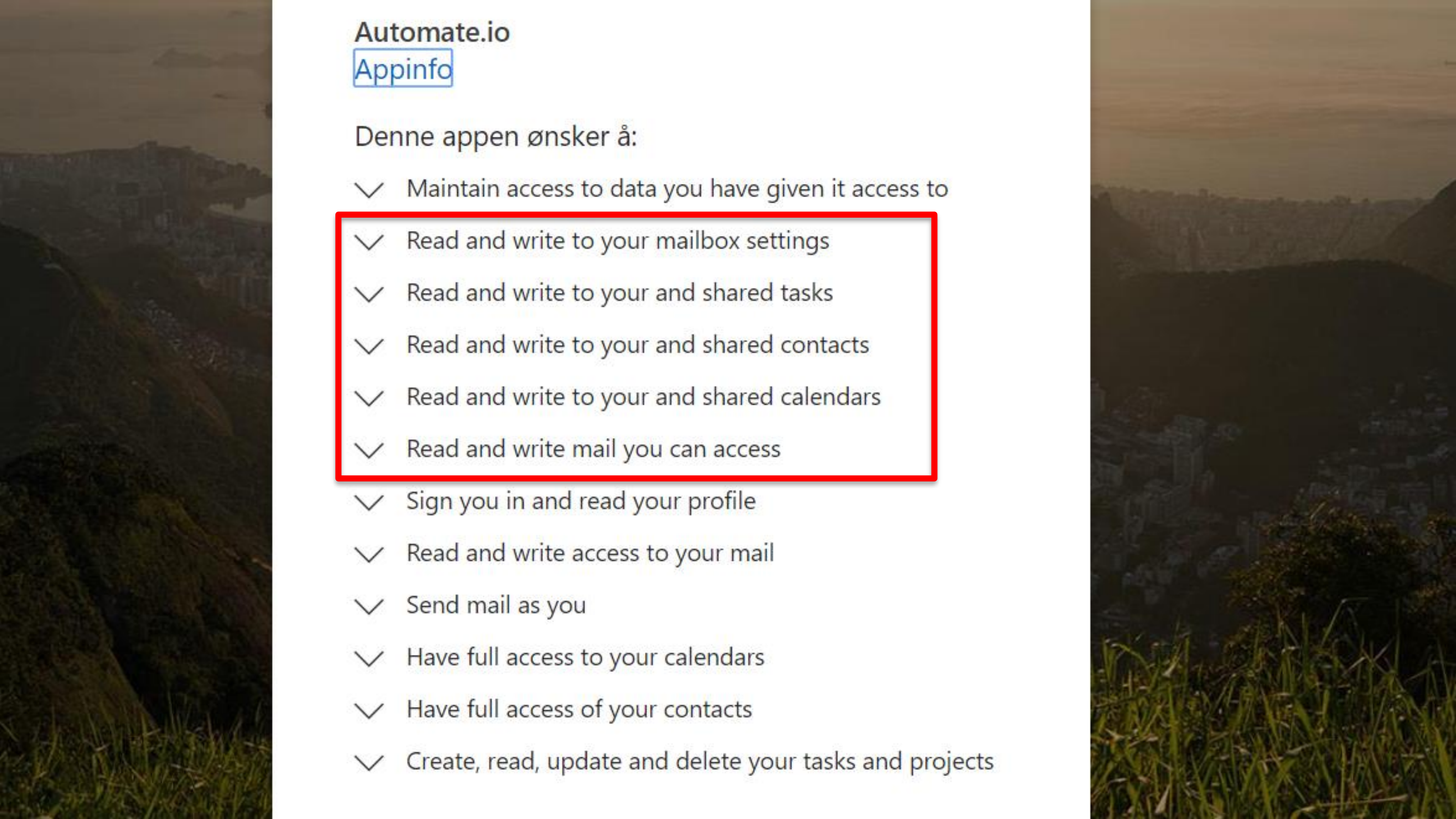


Automate.io

Appinfo

Denne appen ønsker å:

- Maintain access to data you have given it access to
- Read and write to your mailbox settings
- Read and write to your and shared tasks
- Read and write to your and shared contacts
- Read and write to your and shared calendars
- Read and write mail you can access
- Sign you in and read your profile
- Read and write access to your mail
- Send mail as you
- Have full access to your calendars
- Have full access of your contacts
- Create, read, update and delete your tasks and projects

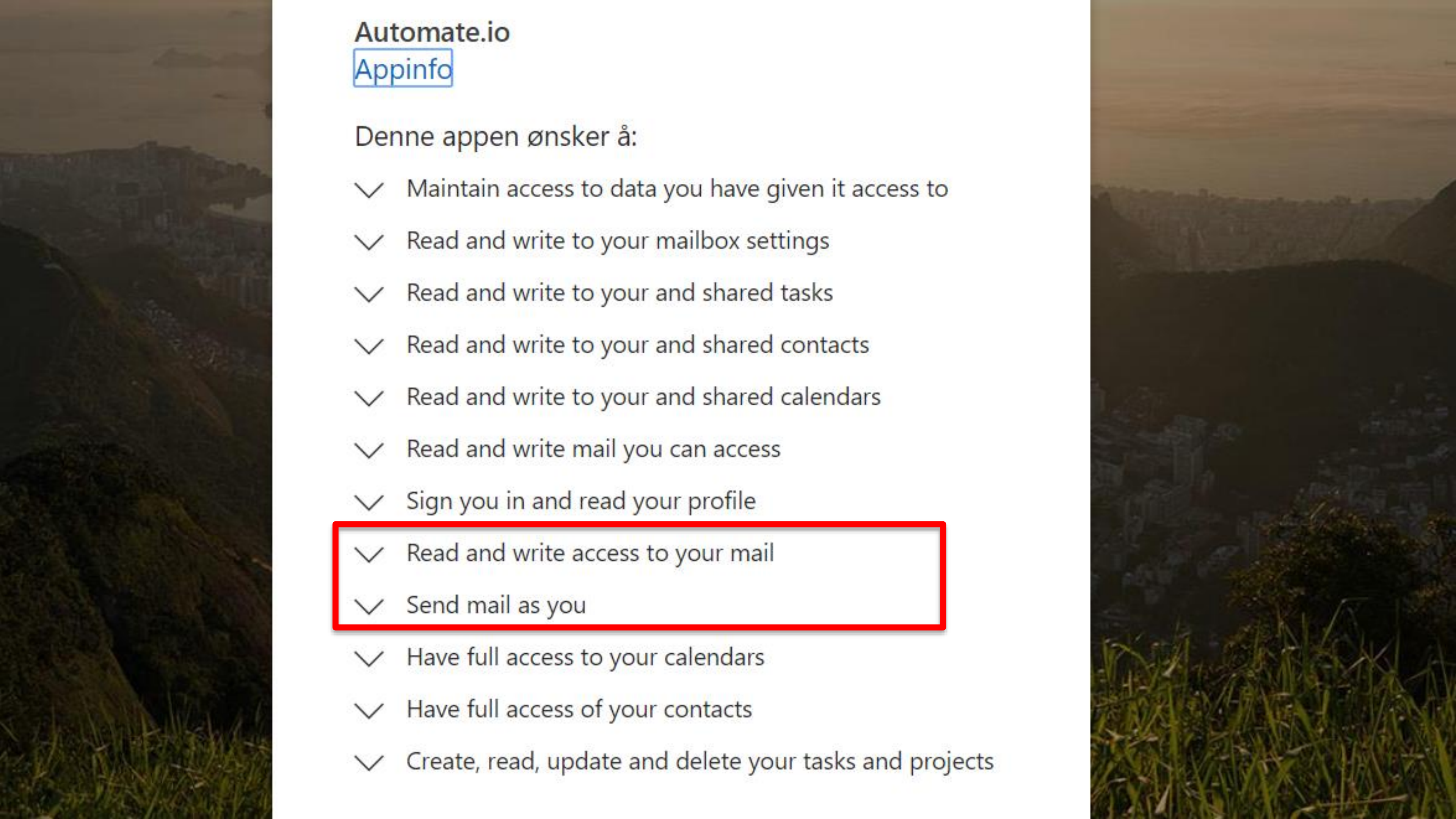


Automate.io

Appinfo

Denne appen ønsker å:

- Maintain access to data you have given it access to
- Read and write to your mailbox settings
- Read and write to your and shared tasks
- Read and write to your and shared contacts
- Read and write to your and shared calendars
- Read and write mail you can access
- Sign you in and read your profile
- Read and write access to your mail
- Send mail as you
- Have full access to your calendars
- Have full access of your contacts
- Create, read, update and delete your tasks and projects

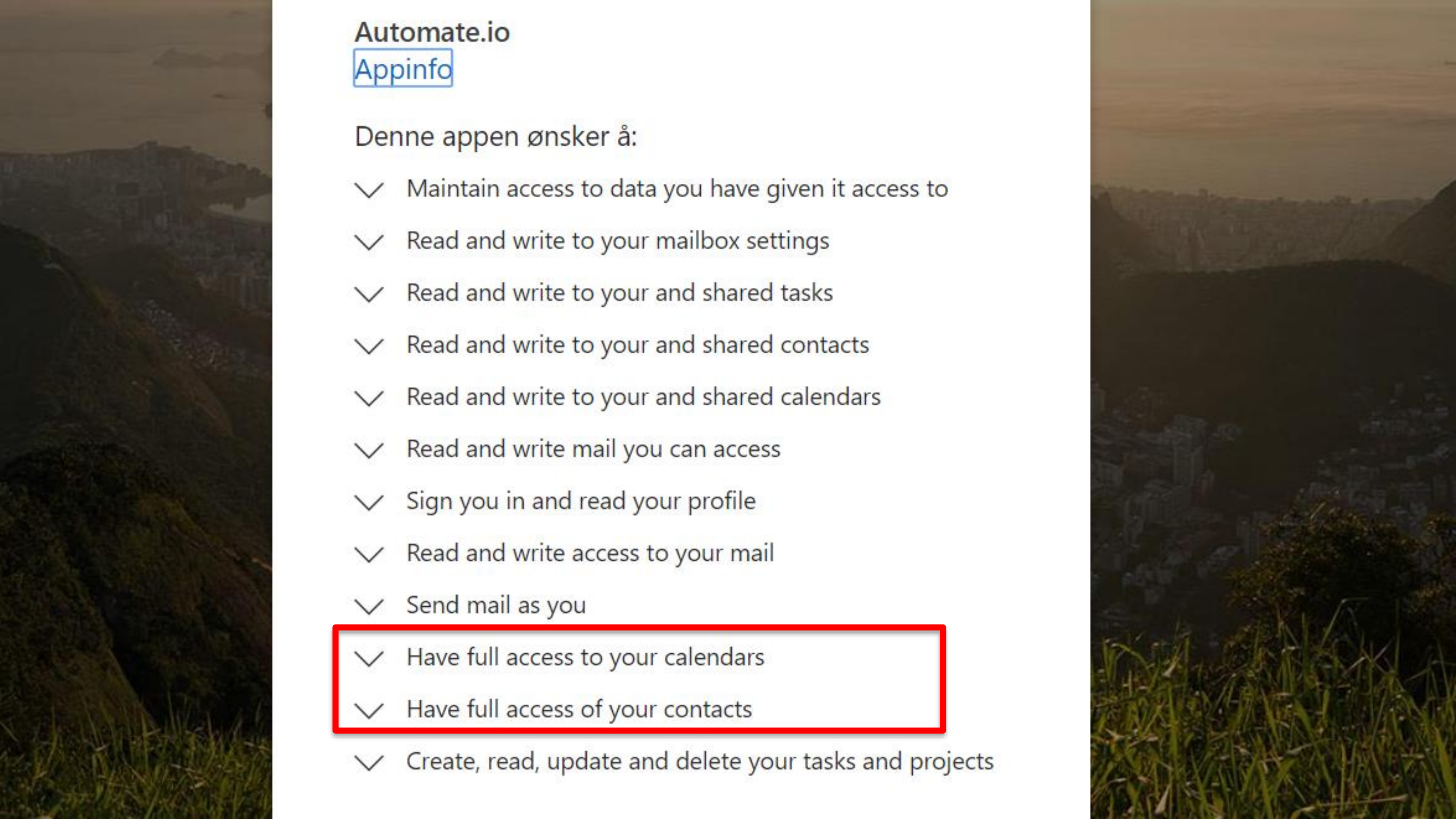


Automate.io

Appinfo

Denne appen ønsker å:

- Maintain access to data you have given it access to
- Read and write to your mailbox settings
- Read and write to your and shared tasks
- Read and write to your and shared contacts
- Read and write to your and shared calendars
- Read and write mail you can access
- Sign you in and read your profile
- Read and write access to your mail
- Send mail as you
- Have full access to your calendars
- Have full access of your contacts
- Create, read, update and delete your tasks and projects



Automate.io

Appinfo

Denne appen ønsker å:

- Maintain access to data you have given it access to
- Read and write to your mailbox settings
- Read and write to your and shared tasks
- Read and write to your and shared contacts
- Read and write to your and shared calendars
- Read and write mail you can access
- Sign you in and read your profile
- Read and write access to your mail
- Send mail as you
- Have full access to your calendars
- Have full access of your contacts
- Create, read, update and delete your tasks and projects

SO WHO IS ACCESSING YOUR COMPANY DATA?

Controlling Oath Apps with MCAS

DEMO

Moving to Device Trust

Configure Conditional Access

Require MFA for all unknown Windows devices
Require Managed App on Mobile

Zero Trust Network:
No need to trust your local network.

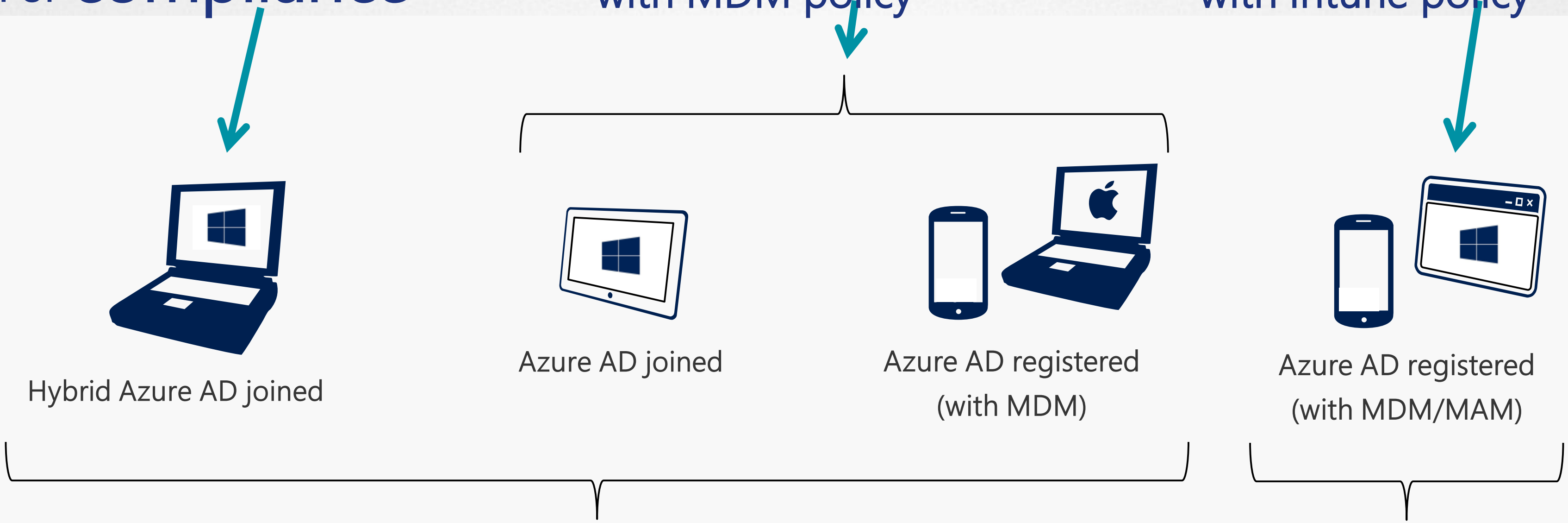
Enable Baseline Policy for Admins

Block Legacy Auth with Policy

Trusted by virtue of domain join or compliance

Trusted if device complies with MDM policy

Trusted if device/app complies with Intune policy



Hybrid Azure AD joined

Azure AD joined

Azure AD registered (with MDM)

Azure AD registered (with MDM/MAM)

Work-owned devices

Personal devices

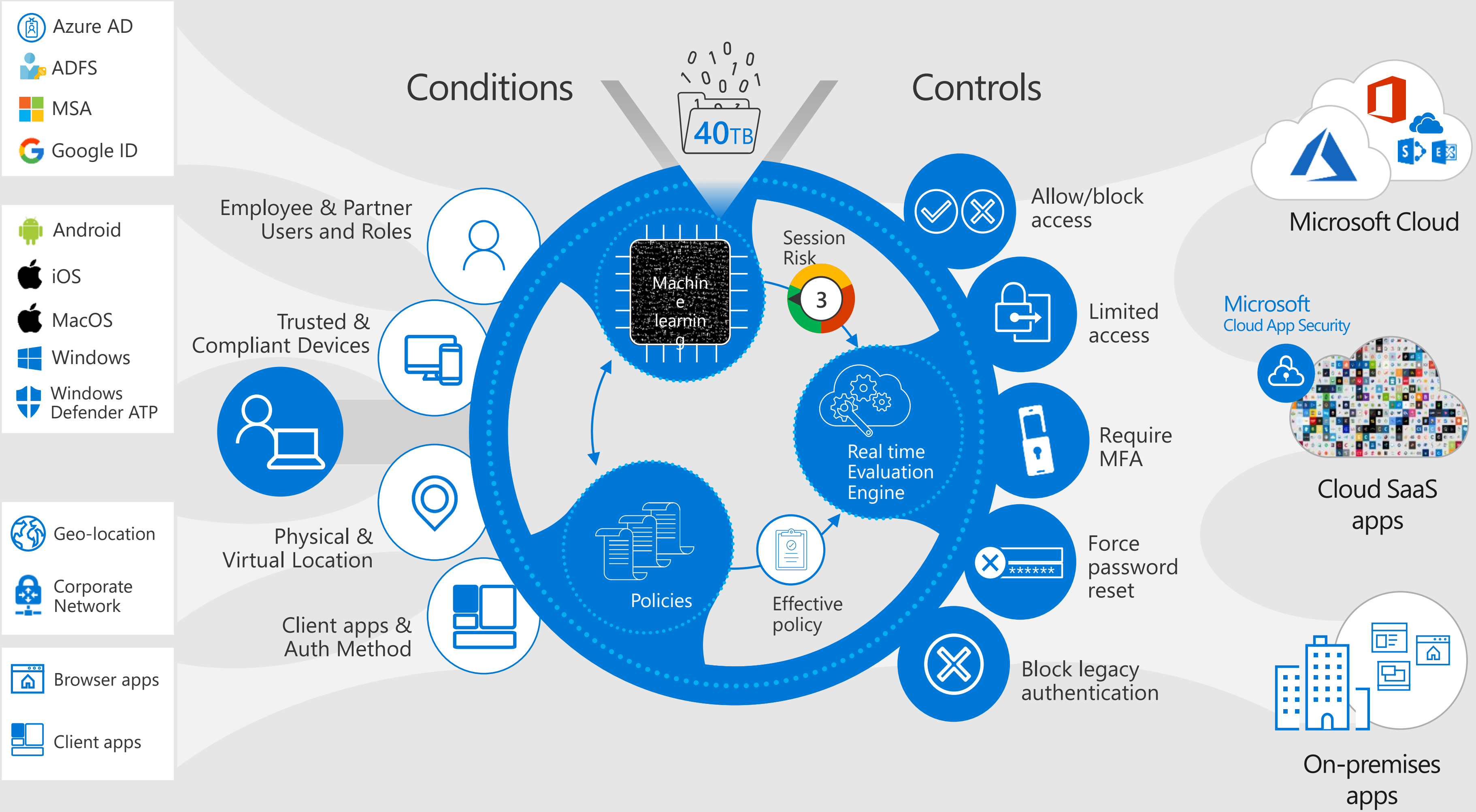
Utilize Microsoft Intune

Setup Configuration Policies

Setup Compliance Policies

Compliant Device

Microsoft Intune



Azure AD

ADFS

MSA

Google ID

Android

iOS

MacOS

Windows

Windows Defender ATP

Geo-location

Corporate Network

Browser apps

Client apps

Conditions

Controls

Employee & Partner Users and Roles

Trusted & Compliant Devices

Physical & Virtual Location

Client apps & Auth Method

Machin e learnin g

Session Risk

Real time Evaluation Engine

Policies

Effective policy

Allow/block access

Limited access

Require MFA

Force password reset

Block legacy authentication

Microsoft Cloud

Microsoft Cloud App Security

Cloud SaaS apps

On-premises apps

Conditional Access

DEMO

Intune App Protection for Mobile Devices

Independent of Mobile Device Management

Why Intune App Protection for Mobile Devices

Independent of Mobile Device Management

Protecting Data at App Level

Why Intune App Protection for Mobile Devices

Independent of Mobile Device Management

Protecting Data at App Level

End User Productivity not Affected

MICROSOFT 365

Why Intune App Protection for Mobile Devices

Independent of Mobile Device Management

Protecting Data at App Level

End User Productivity not Affected

Separate Work from Private

crosoft

MICROSOFT 365

Why Intune App Protection for Mobile Devices

Independent of Mobile Device Management

Protecting Data at App Level

End User Productivity not Affected

Separate Work from Private

crosoft

Without Enrollment

Without Enrollment

Enables BYOD

Without Enrollment

Enables BYOD

Non-intrusive Management

Without Enrollment

- Enables BYOD
- Non-intrusive Management
- Full Privacy

MICROSOFT 365

Without Enrollment

Enables BYOD

Non-intrusive Management

Full Privacy

Works on all iOS and Android Devices

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

MICROSOFT 365

Without Enrollment

Enables BYOD

Non-intrusive Management

Full Privacy

Works on all iOS and Android Devices

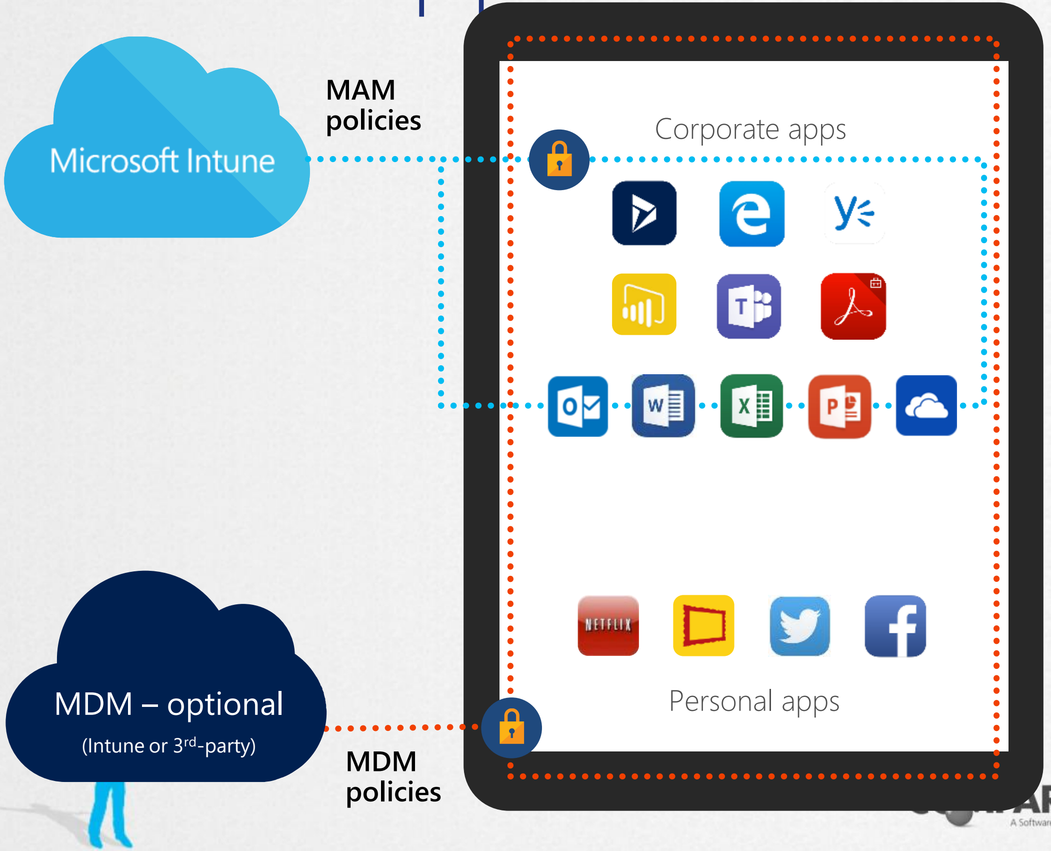
Corporate Data Secured

Without Enrollment

- Enables BYOD
- Non-intrusive Management
- Full Privacy
- Works on all iOS and Android Devices
- Corporate Data Secured

MICROSOFT 365

Intune App Protection Policies (APP)



Comprehensive protection

- App encryption at rest
- App access control – PIN or credentials
- Save as/copy/paste restrictions
- App-level selective wipe

MDM mgmt. by Intune or third-party is optional

Might be a good solution for these scenarios:

- BYOD when MDM is not required
- Extending app access to vendors and partners
- Already have an existing MDM solution

What do we need?

1 App Protection Policies

2 The Broker App(s)

3 Conditional Access Policies

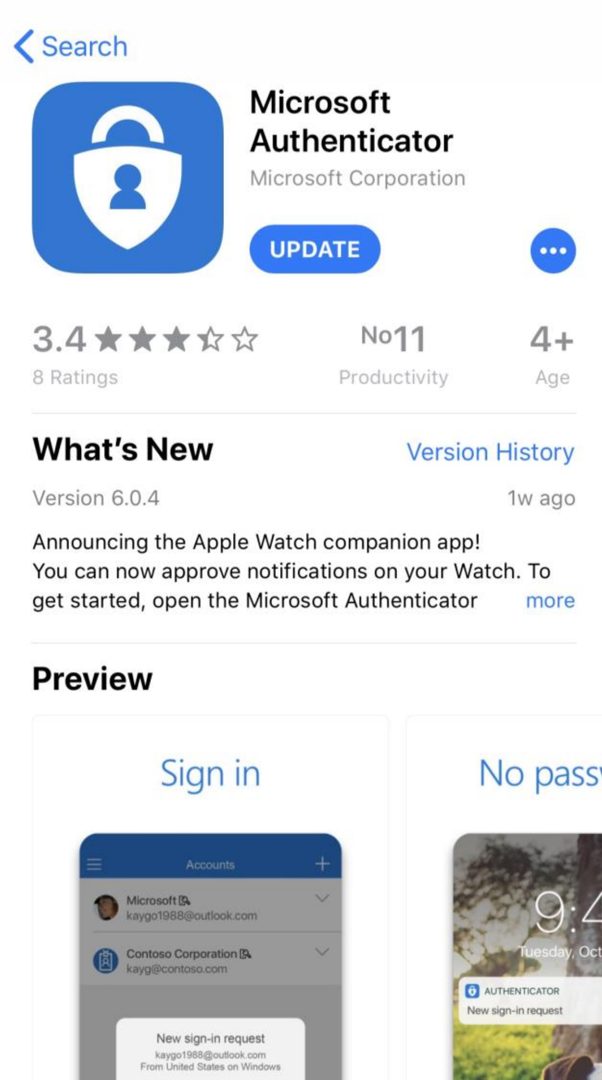
MICROSOFT 365

The Broker App(s)

Registers the device in AAD

Android: Intune Company Portal

iOS: Microsoft Authenticator



< Search

Microsoft Authenticator
Microsoft Corporation

UPDATE

3.4 ★★★★☆ 8 Ratings | No11 Productivity | 4+ Age

What's New Version History

Version 6.0.4 1w ago

Announcing the Apple Watch companion app! You can now approve notifications on your Watch. To get started, open the Microsoft Authenticator more

Preview

Sign in

Accounts

Microsoft
kaygo1988@outlook.com

Contoso Corporation
kayg@contoso.com

New sign-in request
kaygo1988@outlook.com
From United States on Windows

No pass

9:4

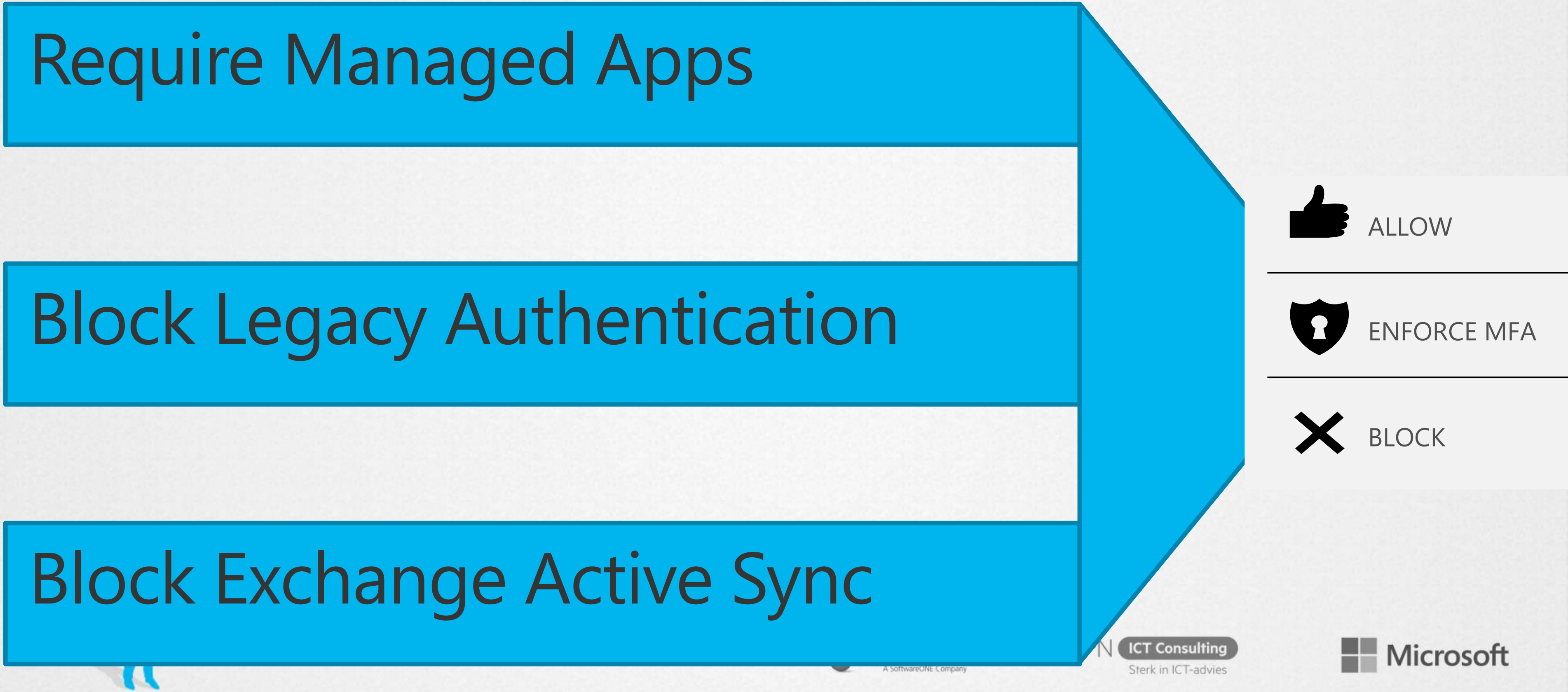
Tuesday, Oct

AUTHENTICATOR
New sign-in request

COMPAREX
A SoftwareONE Company

MICROSOFT 365

Conditional Access Policies



Require Managed Apps

Block Legacy Authentication

Block Exchange Active Sync

👍 ALLOW

🛡 ENFORCE MFA

✕ BLOCK

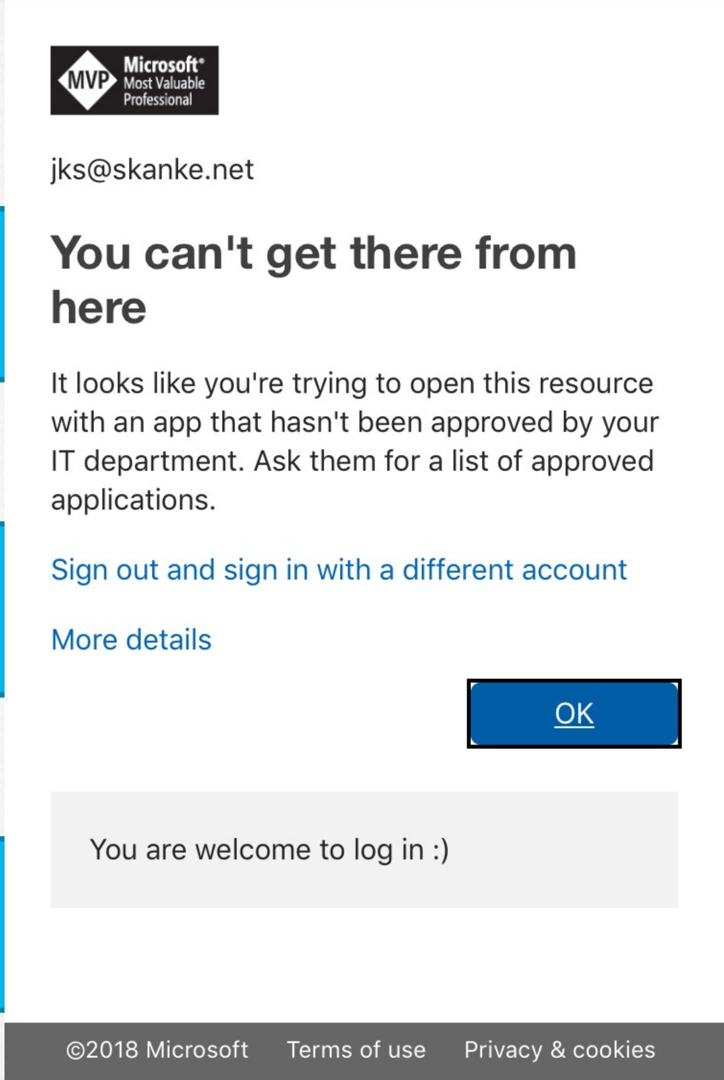
MICROSOFT 365

Require Managed Apps

Block Legacy Authentication

Block Exchange Active Sync

A SoftwareONE Company



jks@skanke.net

You can't get there from here

It looks like you're trying to open this resource with an app that hasn't been approved by your IT department. Ask them for a list of approved applications.

Sign out and sign in with a different account

More details

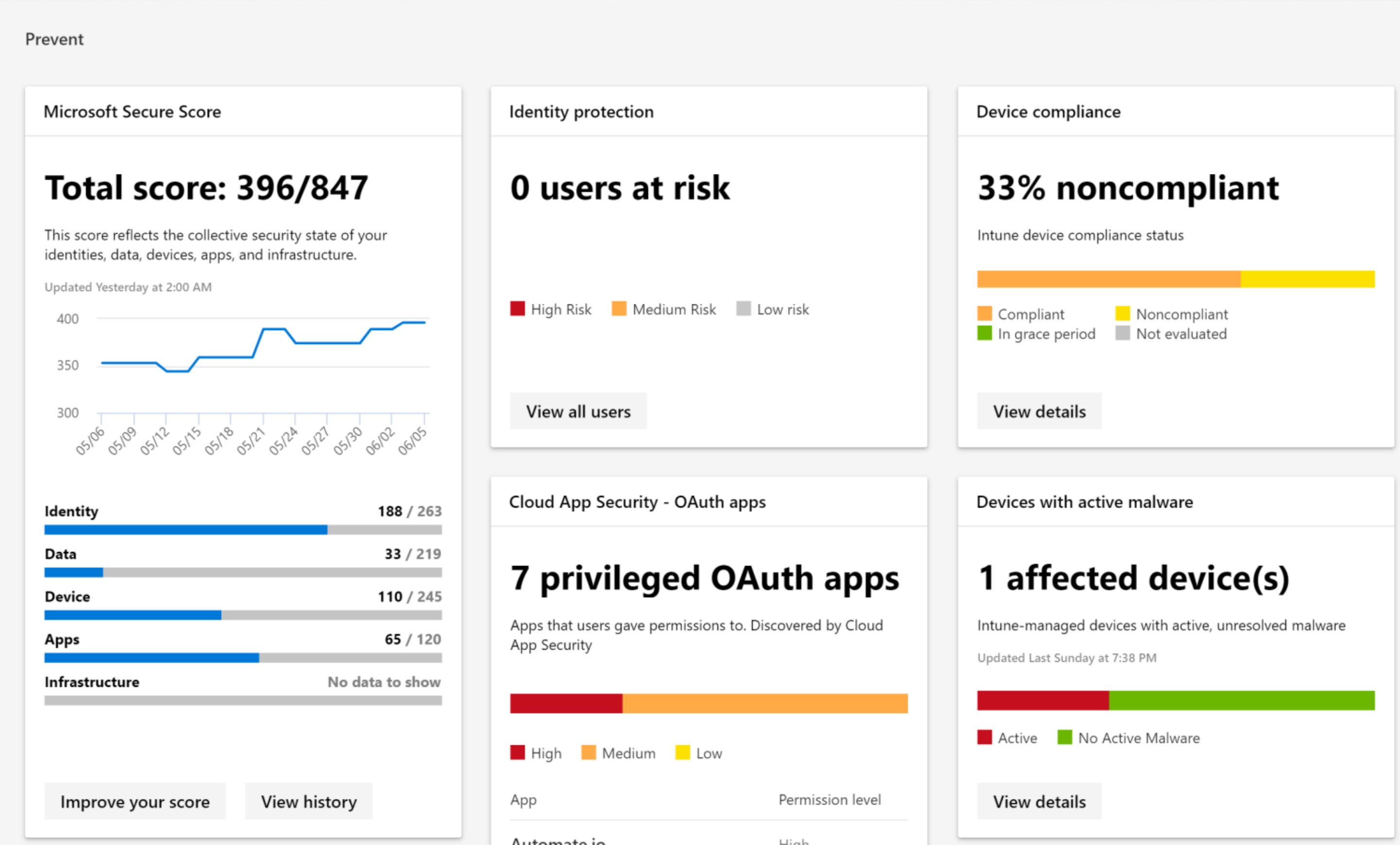
OK

You are welcome to log in :)

©2018 Microsoft Terms of use Privacy & cookies

MICROSOFT 365

security.microsoft.com



Prevent

Microsoft Secure Score

Total score: 396/847

This score reflects the collective security state of your identities, data, devices, apps, and infrastructure.

Updated Yesterday at 2:00 AM

Identity	188 / 263
Data	33 / 219
Device	110 / 245
Apps	65 / 120
Infrastructure	No data to show

Improve your score | View history

Identity protection

0 users at risk

🟥 High Risk 🟧 Medium Risk ⬜ Low risk

View all users

Device compliance

33% noncompliant

Intune device compliance status

🟧 Compliant 🟨 Noncompliant
🟩 In grace period ⬜ Not evaluated

View details

Cloud App Security - OAuth apps

7 privileged OAuth apps

Apps that users gave permissions to. Discovered by Cloud App Security

🟥 High 🟧 Medium 🟨 Low

App	Permission level
Automate.io	High

Devices with active malware

1 affected device(s)

Intune-managed devices with active, unresolved malware

Updated Last Sunday at 7:38 PM

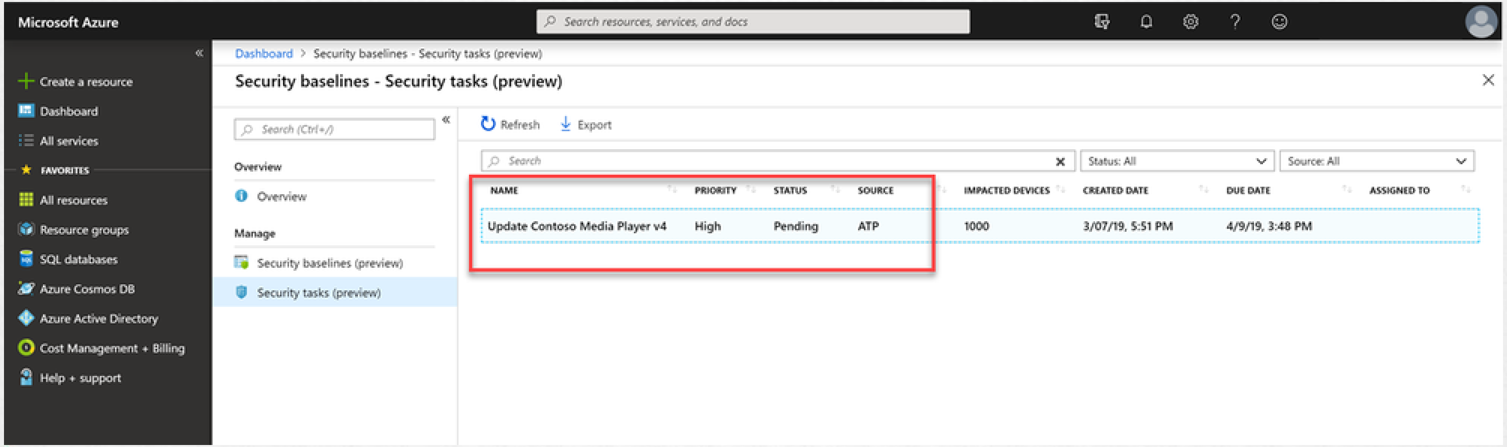
🟥 Active 🟩 No Active Malware

View details

Intune Security Tasks

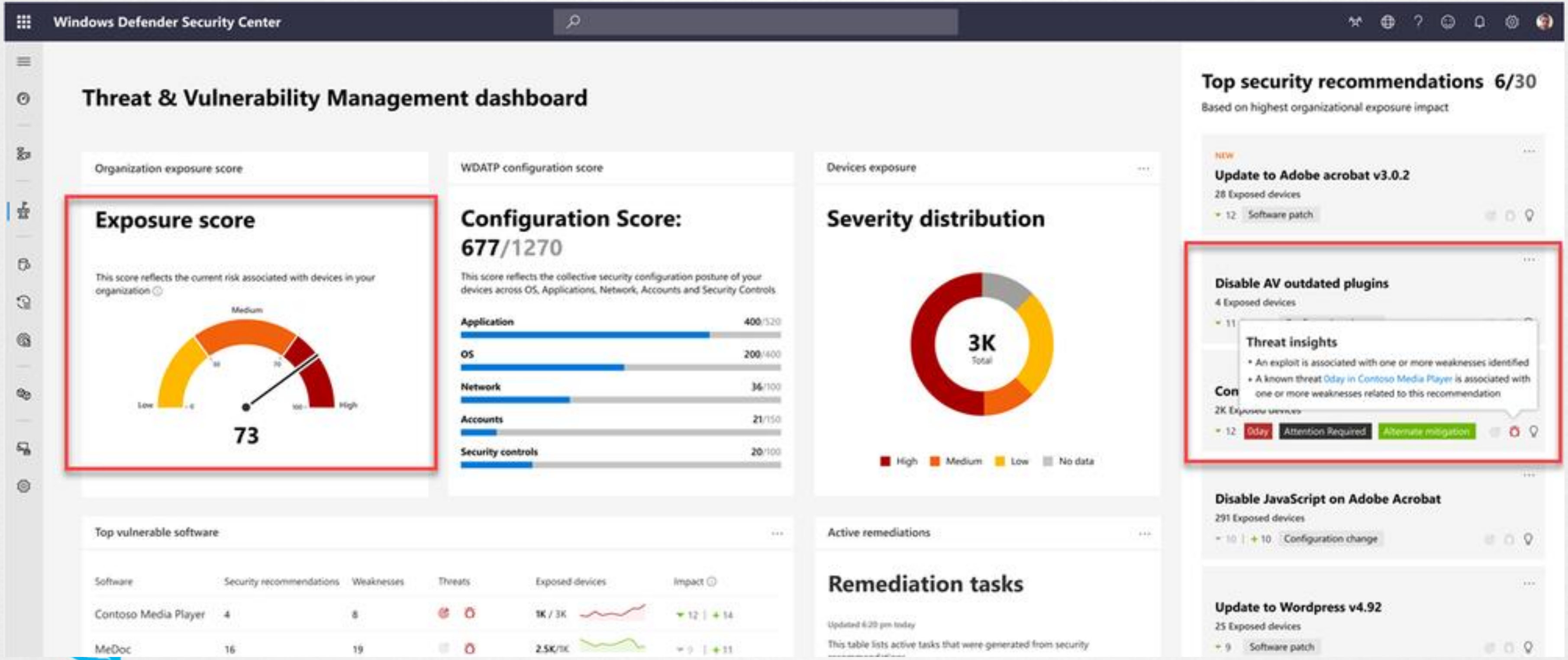
Intune Admin get tasks assigned from SecOps

Integrated with Microsoft Defender ATP



Security baselines - Security tasks (preview)

NAME	PRIORITY	STATUS	SOURCE	IMPACTED DEVICES	CREATED DATE	DUE DATE	ASSIGNED TO
Update Contoso Media Player v4	High	Pending	ATP	1000	3/07/19, 5:51 PM	4/9/19, 3:48 PM	



Windows Defender Security Center

Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current risk associated with devices in your organization ⓘ

WDATP configuration score

Configuration Score: 677/1270

This score reflects the collective security configuration posture of your devices across OS, Applications, Network, Accounts and Security Controls

Application	400/520
OS	200/400
Network	36/100
Accounts	21/150
Security controls	20/100

Devices exposure

Severity distribution

Top vulnerable software

Software	Security recommendations	Weaknesses	Threats	Exposed devices	Impact ⓘ
Contoso Media Player	4	8		1K / 3K	▾ 12 | + 14
MeDoc	16	19		2.5K/1K	▾ 9 | + 11

Active remediations

Remediation tasks

Updated 6:20 pm today

This table lists active tasks that were generated from security recommendations

Top security recommendations 6/30

Based on highest organizational exposure impact

NEW

Update to Adobe acrobat v3.0.2

28 Exposed devices

▾ 12 Software patch

Disable AV outdated plugins

4 Exposed devices

▾ 11

Threat insights

- An exploit is associated with one or more weaknesses identified
- A known threat 0day in Contoso Media Player is associated with one or more weaknesses related to this recommendation

Con

2K Exposed devices

▾ 12 0day Attention Required Alternate mitigation

Disable JavaScript on Adobe Acrobat

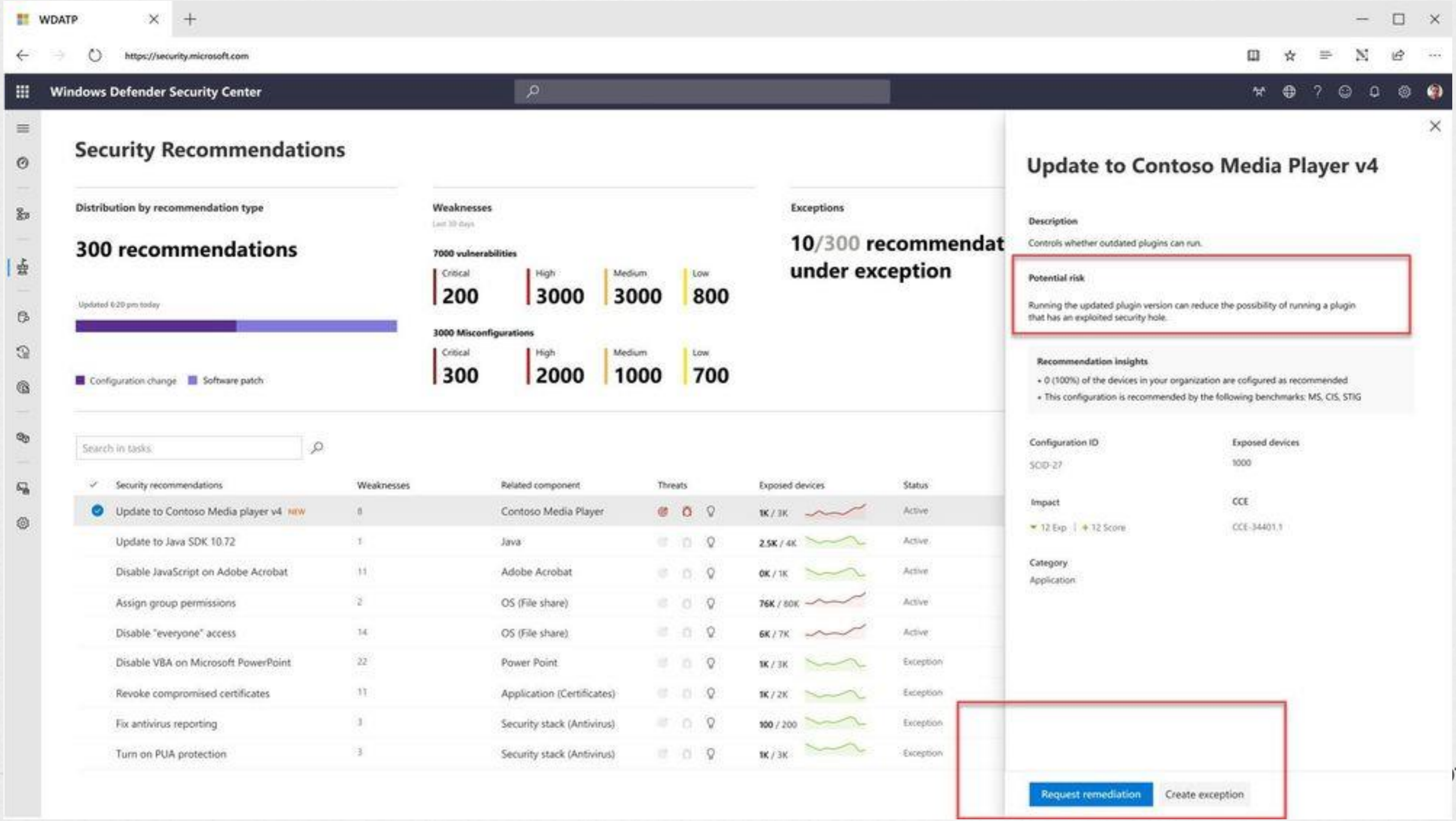
291 Exposed devices

▾ 10 | + 10 Configuration change

Update to Wordpress v4.92

25 Exposed devices

▾ 9 Software patch



WDATP
https://security.microsoft.com
Windows Defender Security Center

Security Recommendations

Distribution by recommendation type

300 recommendations

Updated 6:20 pm today

■ Configuration change ■ Software patch

Weaknesses

Last 30 days

7000 vulnerabilities

Critical	High	Medium	Low
200	3000	3000	800

3000 Misconfigurations

Critical	High	Medium	Low
300	2000	1000	700

Exceptions

10/300 recommendat under exception

Search in tasks

✓	Security recommendations	Weaknesses	Related component	Threats	Exposed devices	Status
●	Update to Contoso Media player v4 NEW	8	Contoso Media Player		1K / 3K	Active
	Update to Java SDK 10.72	1	Java		2.5K / 4K	Active
	Disable JavaScript on Adobe Acrobat	11	Adobe Acrobat		0K / 1K	Active
	Assign group permissions	2	OS (File share)		76K / 80K	Active
	Disable "everyone" access	14	OS (File share)		6K / 7K	Active
	Disable VBA on Microsoft PowerPoint	22	Power Point		1K / 3K	Exception
	Revoke compromised certificates	11	Application (Certificates)		1K / 2K	Exception
	Fix antivirus reporting	3	Security stack (Antivirus)		100 / 200	Exception
	Turn on PUA protection	3	Security stack (Antivirus)		1K / 3K	Exception

Update to Contoso Media Player v4

Description

Controls whether outdated plugins can run.

Potential risk

Running the updated plugin version can reduce the possibility of running a plugin that has an exploited security hole.

Recommendation insights

- 0 (100%) of the devices in your organization are cofigured as recommended
- This configuration is recommended by the following benchmarks: MS, CIS, STIG

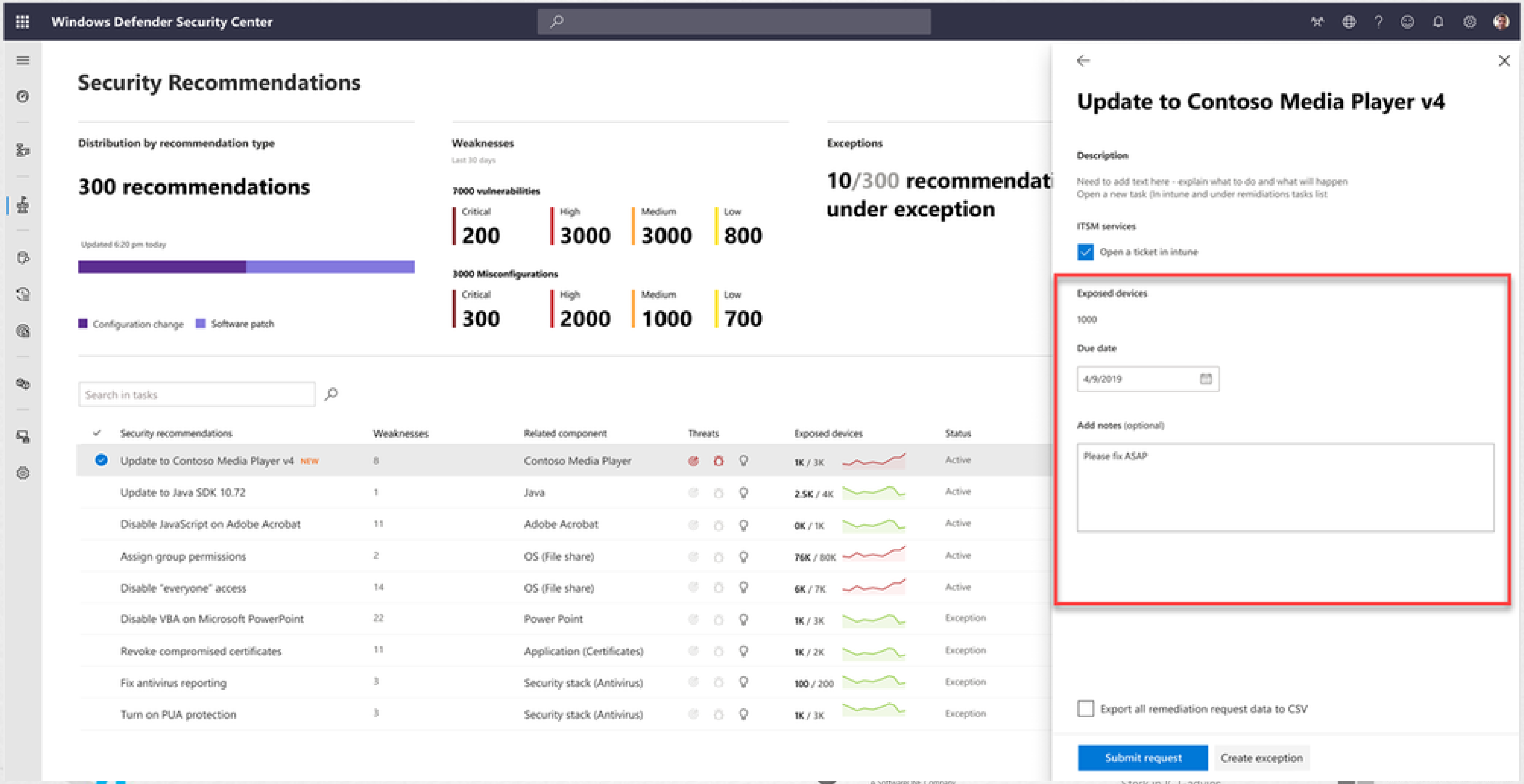
Configuration ID: SCID-27

Exposed devices: 1000

Impact: ▼ 12 Exp | + 12 Score

CCE: CCE-34401.1

Category: Application



Windows Defender Security Center

Security Recommendations

Distribution by recommendation type

300 recommendations

Updated 6:20 pm today

▮ Configuration change ▮ Software patch

Weaknesses

Last 30 days

7000 vulnerabilities

Critical	High	Medium	Low
200	3000	3000	800

3000 Misconfigurations

Critical	High	Medium	Low
300	2000	1000	700

Exceptions

10/300 recommendati under exception

Search in tasks

✓	Security recommendations	Weaknesses	Related component	Threats	Exposed devices	Status
●	Update to Contoso Media Player v4 NEW	8	Contoso Media Player		1K / 3K	Active
	Update to Java SDK 10.72	1	Java		2.5K / 4K	Active
	Disable JavaScript on Adobe Acrobat	11	Adobe Acrobat		0K / 1K	Active
	Assign group permissions	2	OS (File share)		76K / 80K	Active
	Disable "everyone" access	14	OS (File share)		6K / 7K	Active
	Disable VBA on Microsoft PowerPoint	22	Power Point		1K / 3K	Exception
	Revoke compromised certificates	11	Application (Certificates)		1K / 2K	Exception
	Fix antivirus reporting	3	Security stack (Antivirus)		100 / 200	Exception
	Turn on PUA protection	3	Security stack (Antivirus)		1K / 3K	Exception

Update to Contoso Media Player v4

Description

Need to add text here - explain what to do and what will happen
Open a new task (In intune and under remidiations tasks list

ITSM services

☑ Open a ticket in intune

Exposed devices

1000

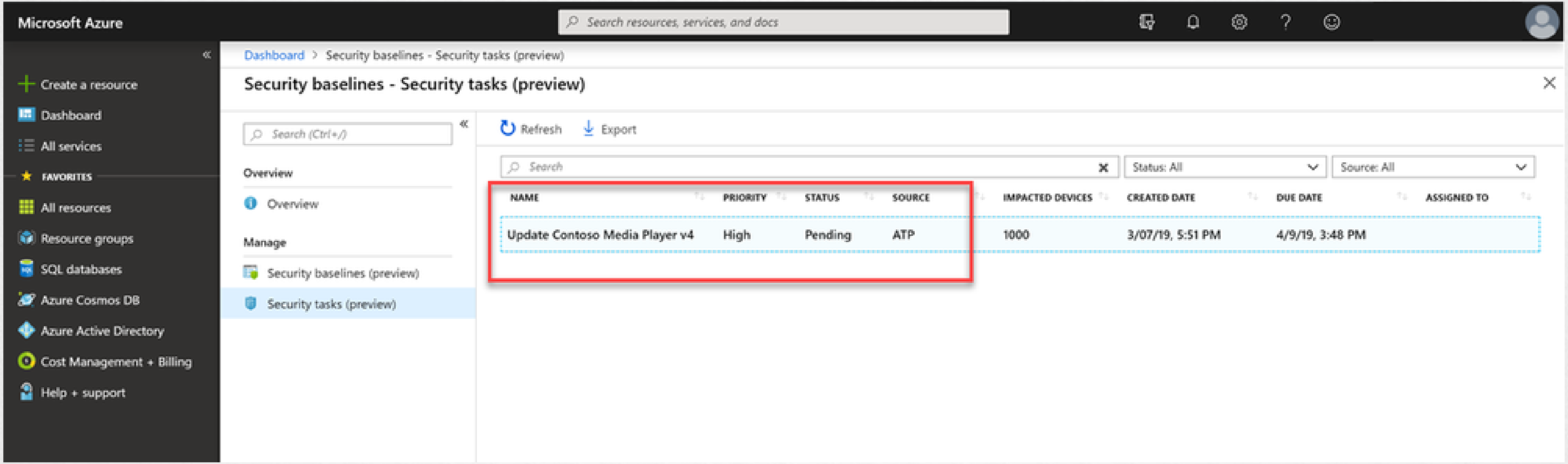
Due date

4/9/2019

Add notes (optional)

Please fix ASAP

☐ Export all remediation request data to CSV



Dashboard > Security baselines - Security tasks (preview)

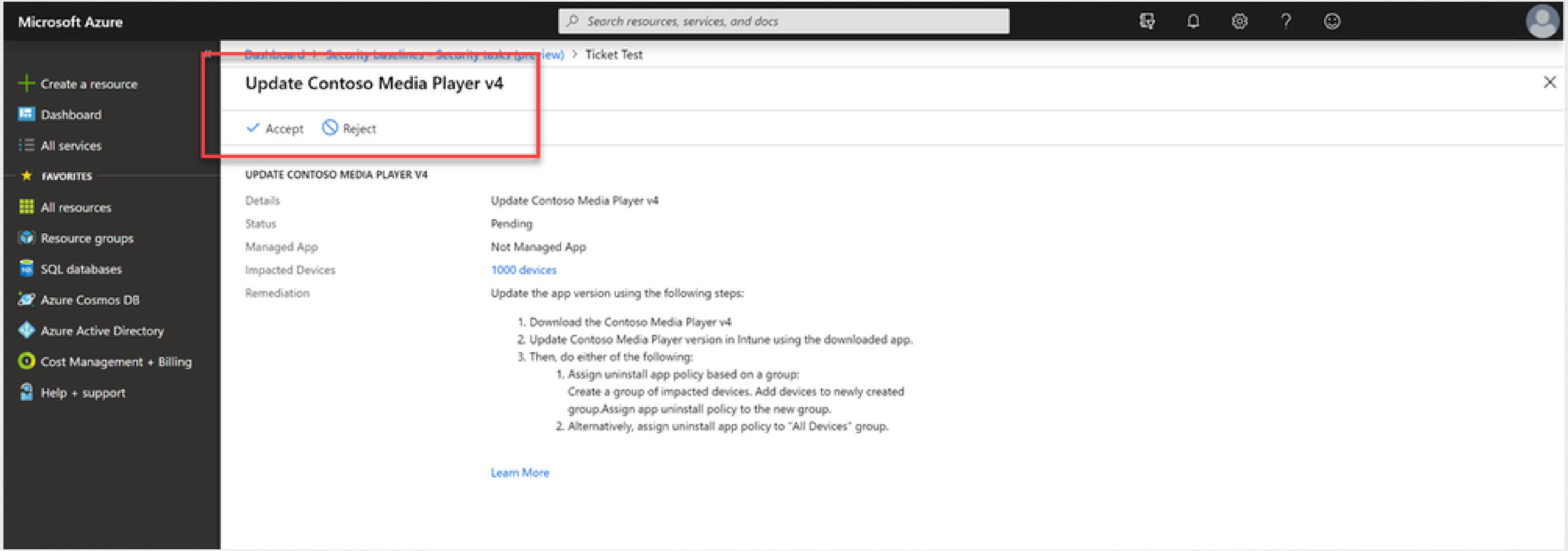
Security baselines - Security tasks (preview)

Status: All

Source: All

NAME	PRIORITY	STATUS	SOURCE	IMPACTED DEVICES	CREATED DATE	DUE DATE	ASSIGNED TO
Update Contoso Media Player v4	High	Pending	ATP	1000	3/07/19, 5:51 PM	4/9/19, 3:48 PM	

MICROSOFT 365



Update Contoso Media Player v4

✓ Accept ⃠ Reject

UPDATE CONTOSO MEDIA PLAYER V4

Details Update Contoso Media Player v4

Status Pending

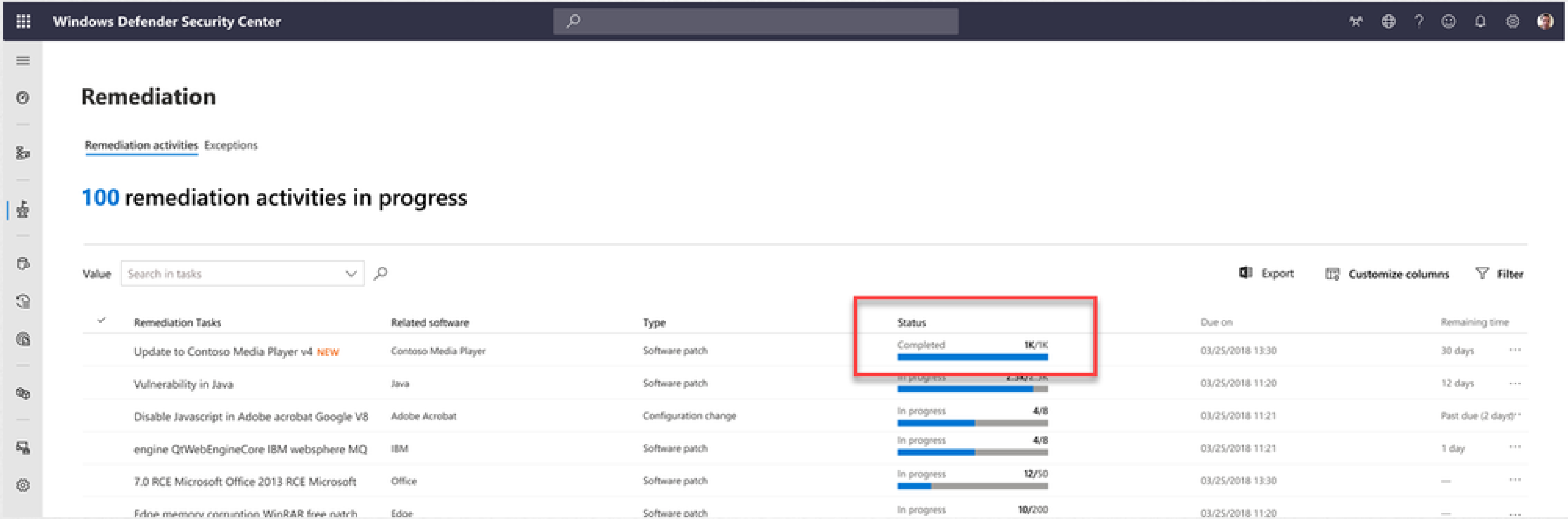
Managed App Not Managed App

Impacted Devices 1000 devices

Remediation Update the app version using the following steps:

1. Download the Contoso Media Player v4
2. Update Contoso Media Player version in Intune using the downloaded app.
3. Then, do either of the following:
   1. Assign uninstall app policy based on a group:
      Create a group of impacted devices. Add devices to newly created group.Assign app uninstall policy to the new group.
   2. Alternatively, assign uninstall app policy to "All Devices" group.

Learn More

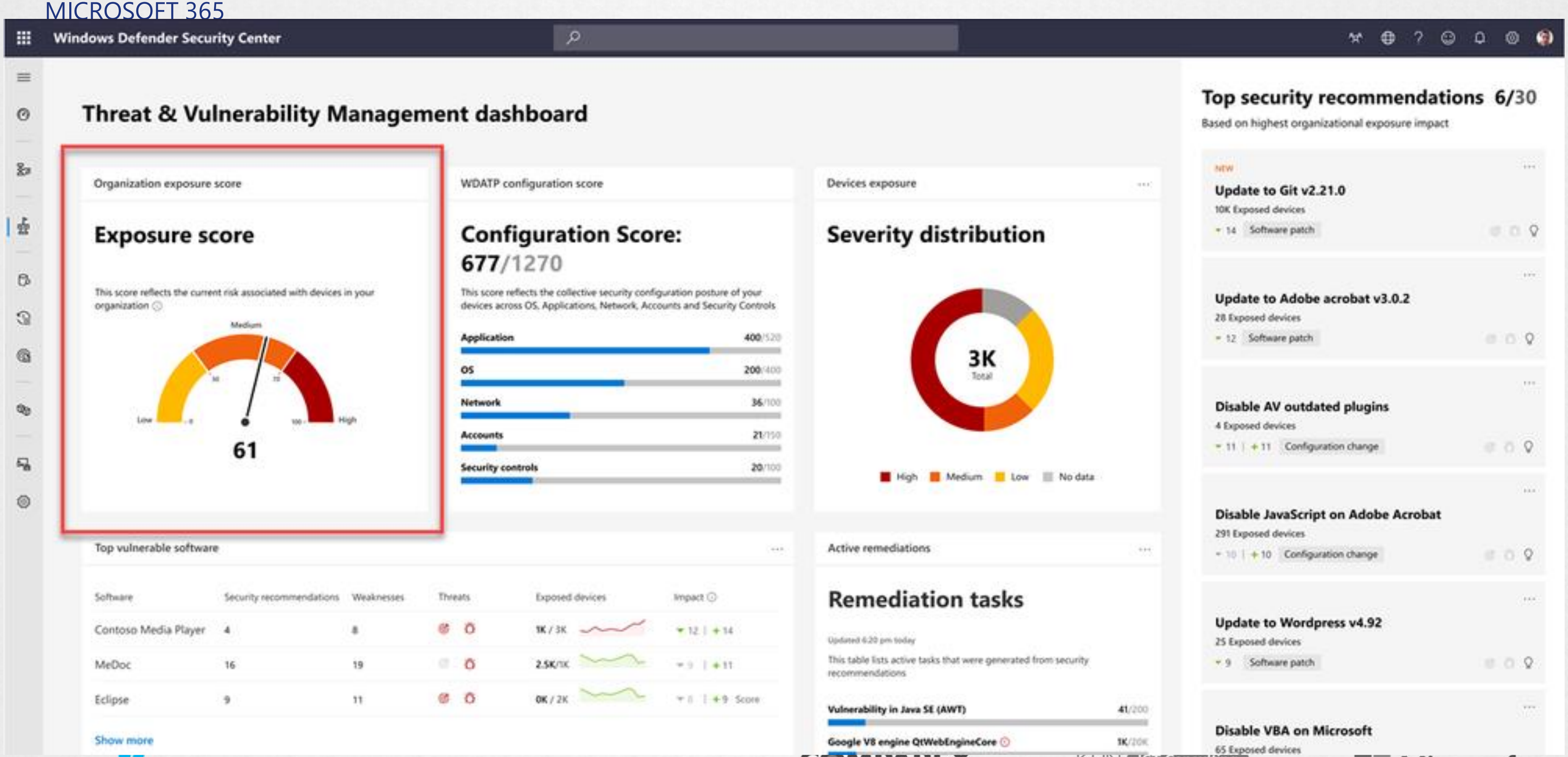


Remediation

Remediation activities Exceptions

100 remediation activities in progress

Remediation Tasks	Related software	Type	Status	Due on	Remaining time
Update to Contoso Media Player v4 NEW	Contoso Media Player	Software patch	Completed 1K/1K	03/25/2018 13:30	30 days
Vulnerability in Java	Java	Software patch	In progress [illegible]	03/25/2018 11:20	12 days
Disable Javascript in Adobe acrobat Google V8	Adobe Acrobat	Configuration change	In progress 4/8	03/25/2018 11:21	Past due (2 days)
engine QtWebEngineCore IBM websphere MQ	IBM	Software patch	In progress 4/8	03/25/2018 11:21	1 day
7.0 RCE Microsoft Office 2013 RCE Microsoft	Office	Software patch	In progress 12/50	03/25/2018 13:30	—
Edge memory corruption WinRAR free patch	Edge	Software patch	In progress 10/200	03/25/2018 11:20	—



Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current risk associated with devices in your organization

61

WDATP configuration score

Configuration Score: 677/1270

This score reflects the collective security configuration posture of your devices across OS, Applications, Network, Accounts and Security Controls

Application	400/520
OS	200/400
Network	36/100
Accounts	21/150
Security controls	20/100

Devices exposure

Severity distribution

Top vulnerable software

Software	Security recommendations	Weaknesses	Threats	Exposed devices	Impact
Contoso Media Player	4	8		1K / 3K	▼ 12 | + 14
MeDoc	16	19		2.5K/1K	▼ 9 | + 11
Eclipse	9	11		0K / 2K	▼ 8 | + 9 Score

Show more

Active remediations

Remediation tasks

Updated 6:20 pm today

This table lists active tasks that were generated from security recommendations

Vulnerability in Java SE (AWT)	41/200
Google V8 engine QtWebEngineCore	1K/20K

Top security recommendations 6/30

Based on highest organizational exposure impact

NEW

Update to Git v2.21.0
10K Exposed devices
▼ 14 Software patch

Update to Adobe acrobat v3.0.2
28 Exposed devices
▼ 12 Software patch

Disable AV outdated plugins
4 Exposed devices
▼ 11 | + 11 Configuration change

Disable JavaScript on Adobe Acrobat
291 Exposed devices
▼ 10 | + 10 Configuration change

Update to Wordpress v4.92
25 Exposed devices
▼ 9 Software patch

Disable VBA on Microsoft
65 Exposed devices

DEMO

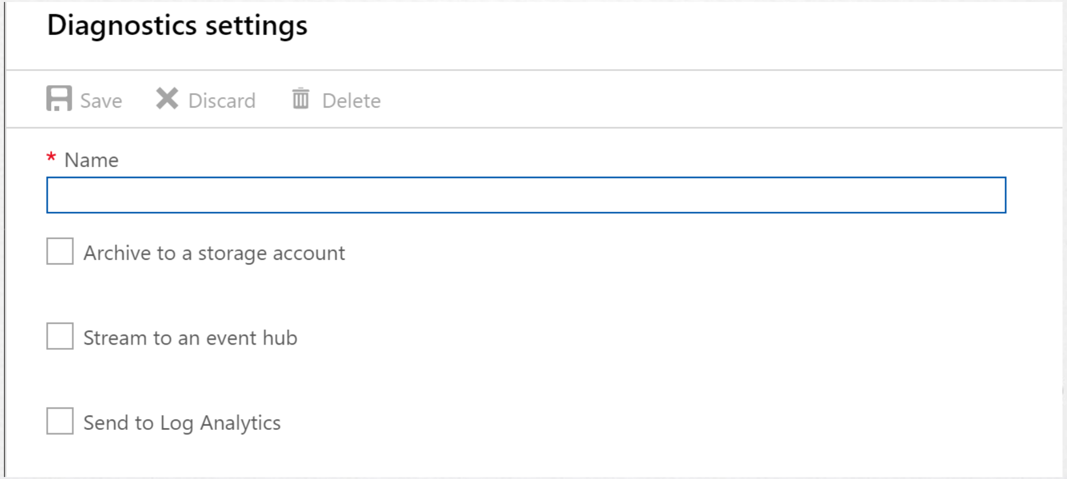
MICROSOFT 365

Log Analytics

Export logs to Log Analytics

Store logs in Storage Account

Stream to Event Hub (forward to SIEM)



Diagnostics settings

* Name

□ Archive to a storage account

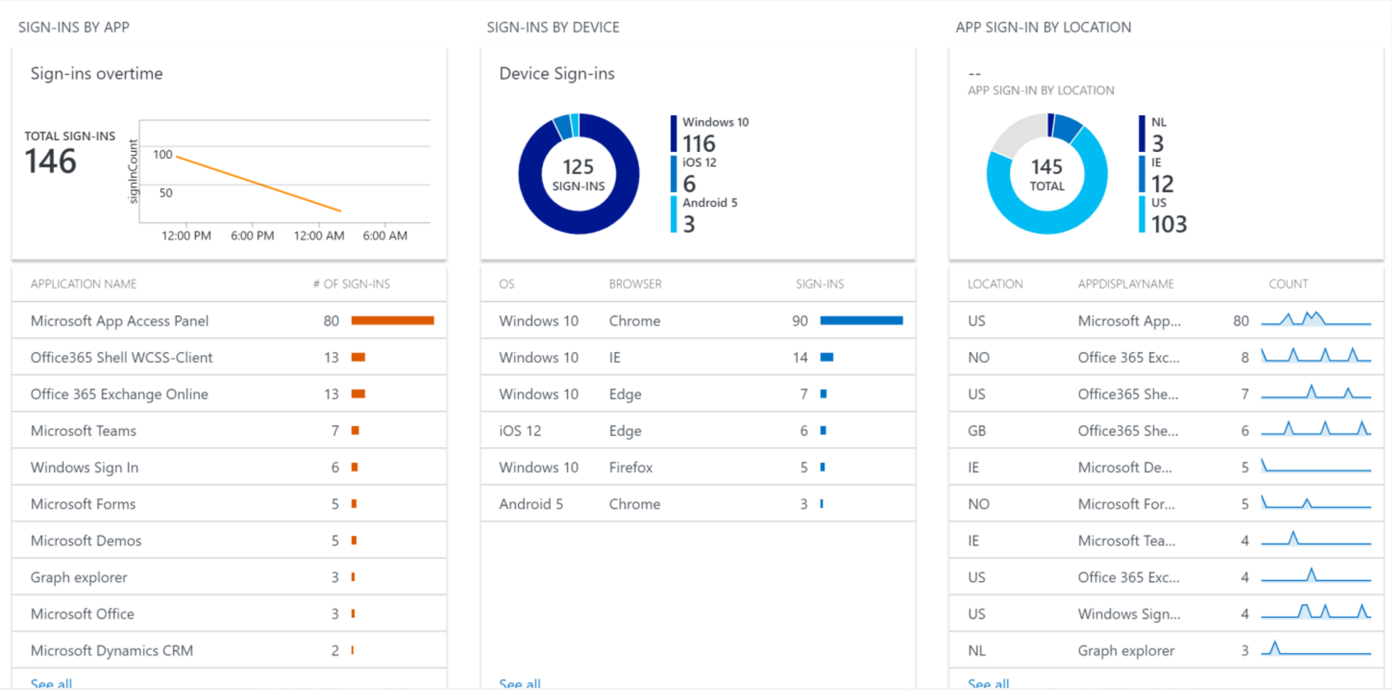
□ Stream to an event hub

□ Send to Log Analytics

Microsoft

MICROSOFT 365

Logs logs logs



SIGN-INS BY APP

Sign-ins overtime

APPLICATION NAME	# OF SIGN-INS
Microsoft App Access Panel	80
Office365 Shell WCSS-Client	13
Office 365 Exchange Online	13
Microsoft Teams	7
Windows Sign In	6
Microsoft Forms	5
Microsoft Demos	5
Graph explorer	3
Microsoft Office	3
Microsoft Dynamics CRM	2

See all

SIGN-INS BY DEVICE

Device Sign-ins

OS	BROWSER	SIGN-INS
Windows 10	Chrome	90
Windows 10	IE	14
Windows 10	Edge	7
iOS 12	Edge	6
Windows 10	Firefox	5
Android 5	Chrome	3

See all

APP SIGN-IN BY LOCATION

--
APP SIGN-IN BY LOCATION

LOCATION	APPDISPLAYNAME	COUNT
US	Microsoft App...	80
NO	Office 365 Exc...	8
US	Office365 She...	7
GB	Office365 She...	6
IE	Microsoft De...	5
NO	Microsoft For...	5
IE	Microsoft Tea...	4
US	Office 365 Exc...	4
US	Windows Sign...	4
NL	Graph explorer	3

See all

COMPAREX
A SoftwareONE Company

KPN ICT Consulting
Sterk in ICT-advies

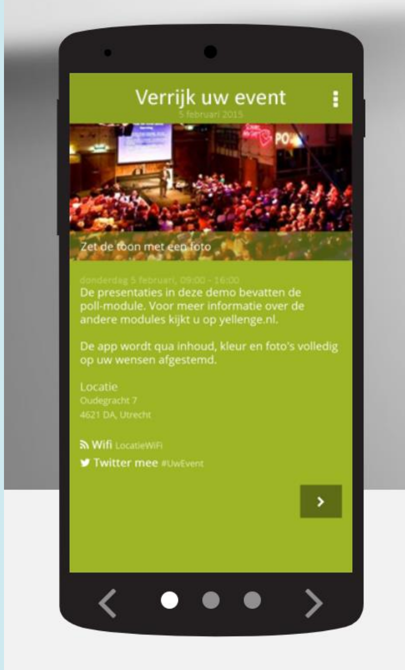
Microsoft

DEMO

Thank You

Remember to evaluate my session

Yellenge



Verrijk uw event

5 februari 2015

Zet de toon met een foto

donderdag 5 februari, 09:00 - 16:00

De presentaties in deze demo bevatten de poll-module. Voor meer informatie over de andere modules kijkt u op yellenge.nl.

De app wordt qua inhoud, kleur en foto's volledig op uw wensen afgestemd.

Locatie
Oudegracht 7
4621 DA, Utrecht

Wifi LocatieWiFi

Twitter mee #UwEvent

Experts Live Netherlands