DON'T BOTHER YOUR USERS WITH MOBILE DEVICE MANAGEMENT, EMBRACE MODERN!

Peter Daalmans

Modern Workplace Consultant| Microsoft MVP | MCT

https://daalmansconsulting.com

peter@daalmansconsulting.com

About me – Peter Daalmans

Trainer, architect, author, lead Workplace Ninja User Group NL

@PDaalmans
@DaalmansConsult

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

https://modernmanagement.blog
https://www.daalmansconsulting.com

https://enterprisemobility.tips
https://www.youtube.com/c/EnterpriseMobilityTips

Daalmans
consulting

Mastering System Center 2012 Configuration Manager
Mastering System Center 2012 R2 Configuration Manager
Microsoft Enterprise Mobility Suite
Planning and Implementation
By Kent Agerlund and Peter Daalmans
Mastering System Center Configuration Manager
Microsoft 365 Security for IT Pros
Michael Van Horenbeeck
Available Now
First Edition (2021)
Microsoft 365 Security for IT Pros
Michael Van Horenbeeck
Second Edition (2022)

MVP

Microsoft
MCT

?
THE ADMINISTRATOR

ALSO THOSE MANY DIFFERENT MOBILE DEVICES?

Complex PIN

Restrictive settings

Check for compliance

MANY GOOD REASONS FOR CORPORATE DEVICES

Use cases MDM

More Control	App Deployment	Kiosk scenarios	VPN / E-mail / Wi-Fi
Corp Owned device	Certificates	Compliance	More?

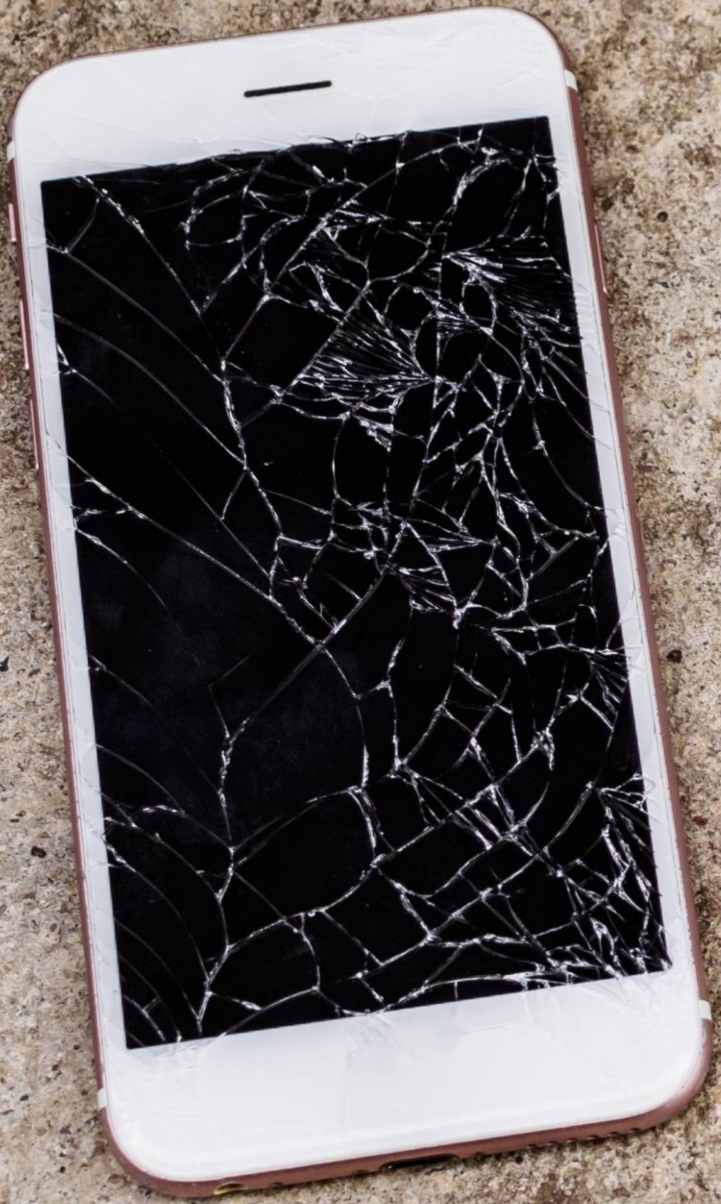
BUT WHAT ABOUT BYOD?

LOCKING IT DOWN?

WHAT WAS THE EIGHT DIGIT PIN AGAIN?

WHAT WAS
MY PIN??

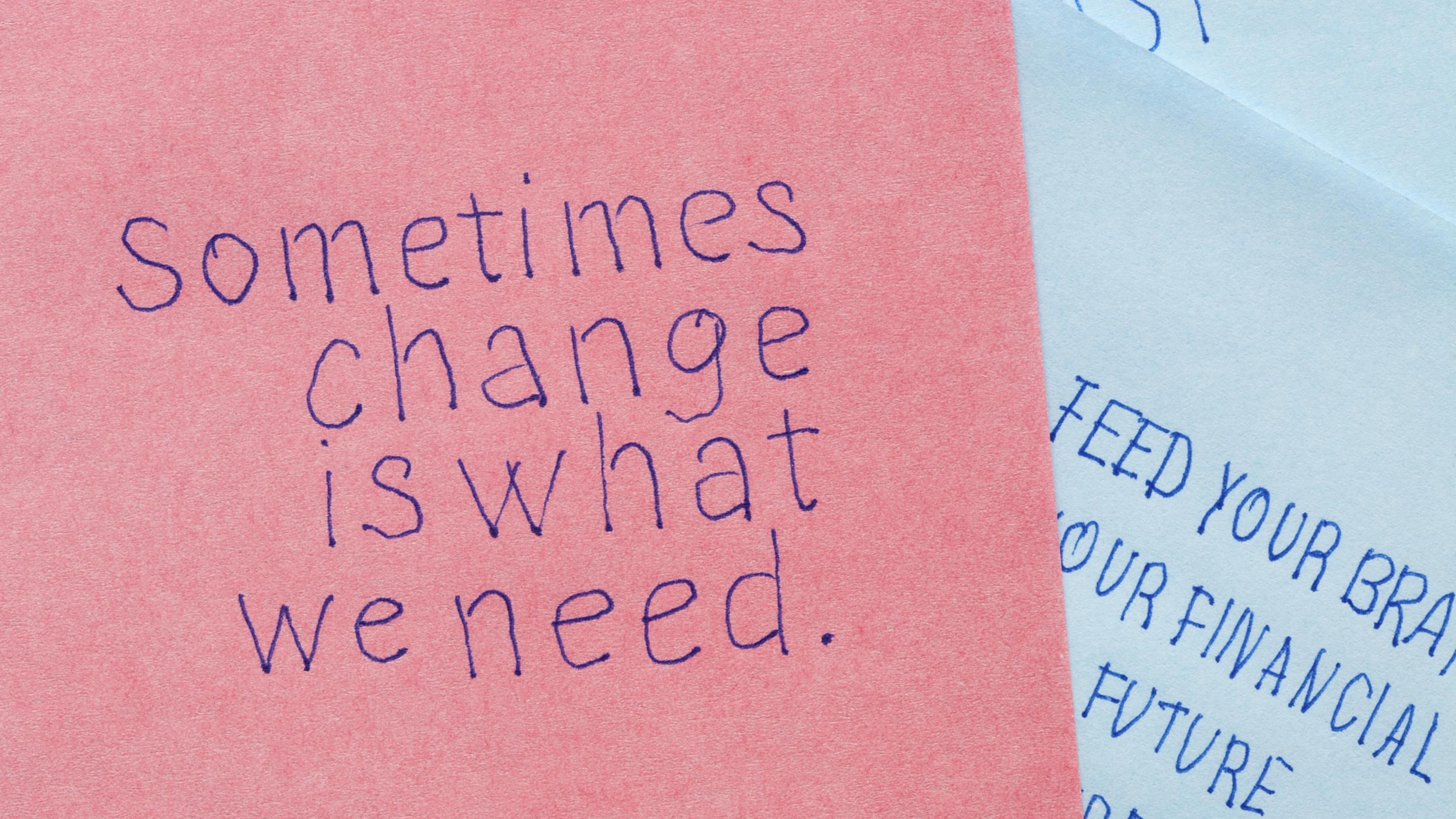
Phone is being erased



FRUSTRATION

=

BROKEN DEVICES



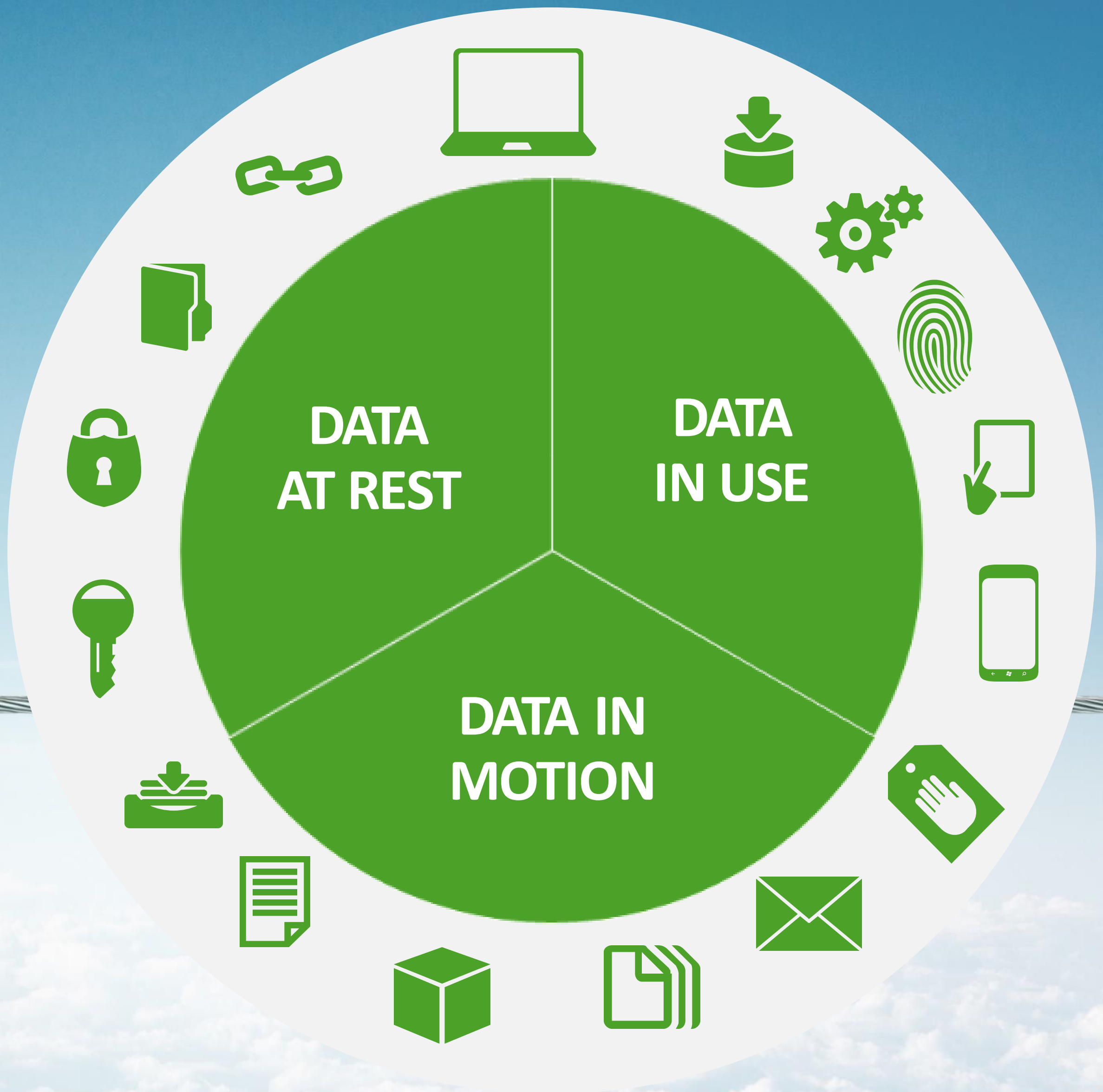
sometimes
change
is what
we need.

FEED YOUR BRA
OUR FINANCIAL
FUTURE

LOOK AT

FOCUS ON

PREVENT



DATA AT REST

DATA IN USE

DATA IN MOTION

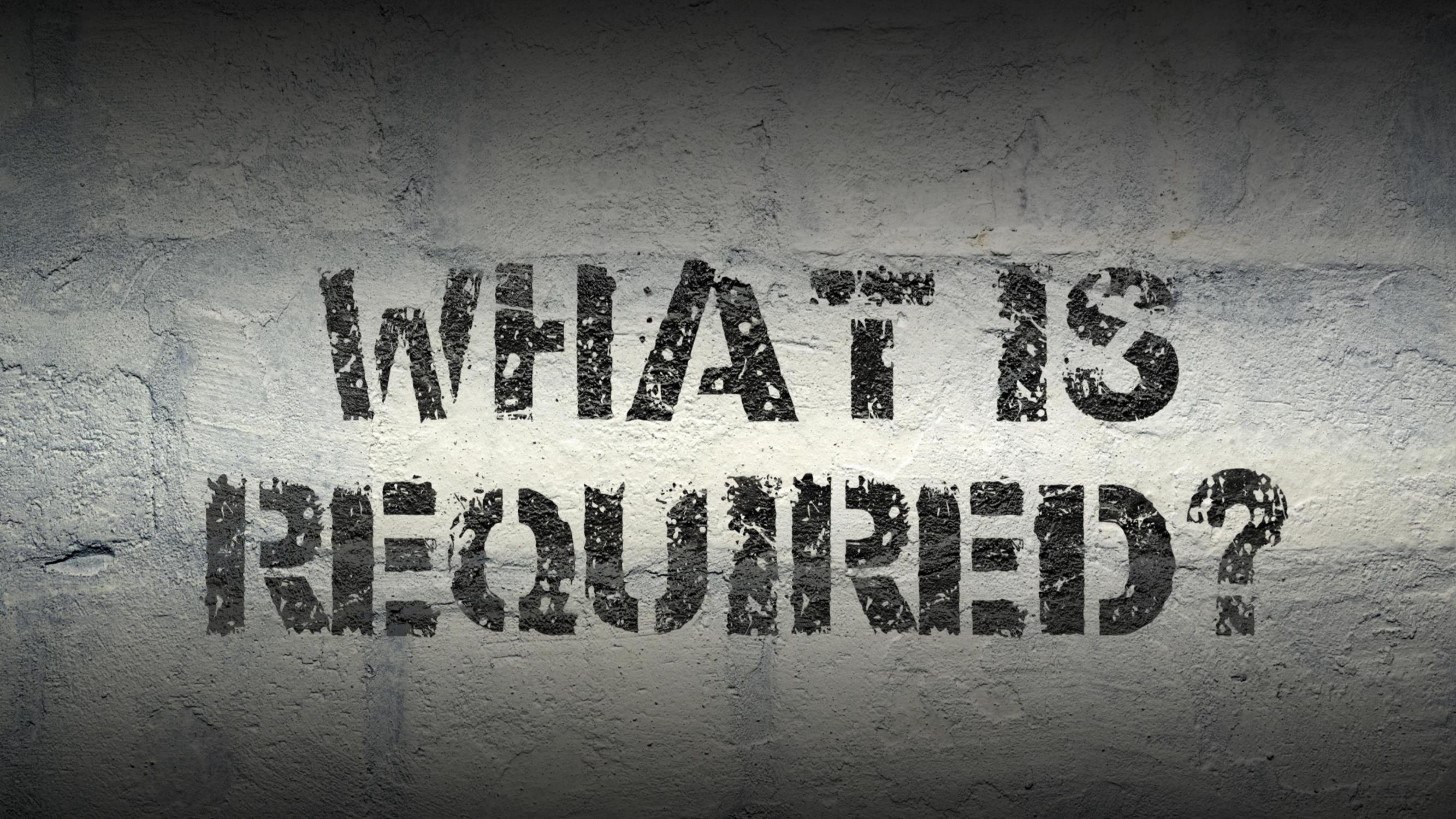
HOW ARE WE GOING TO ACHIEVE THIS?

WITHOUT LOCKING DOWN THE DEVICE

OR USERS SHOOTING HOLES OR FINDING ALTERNATIVES

MEET APP PROTECTION WITHOUT ENROLLMENT

WHERE WE FOCUS ON

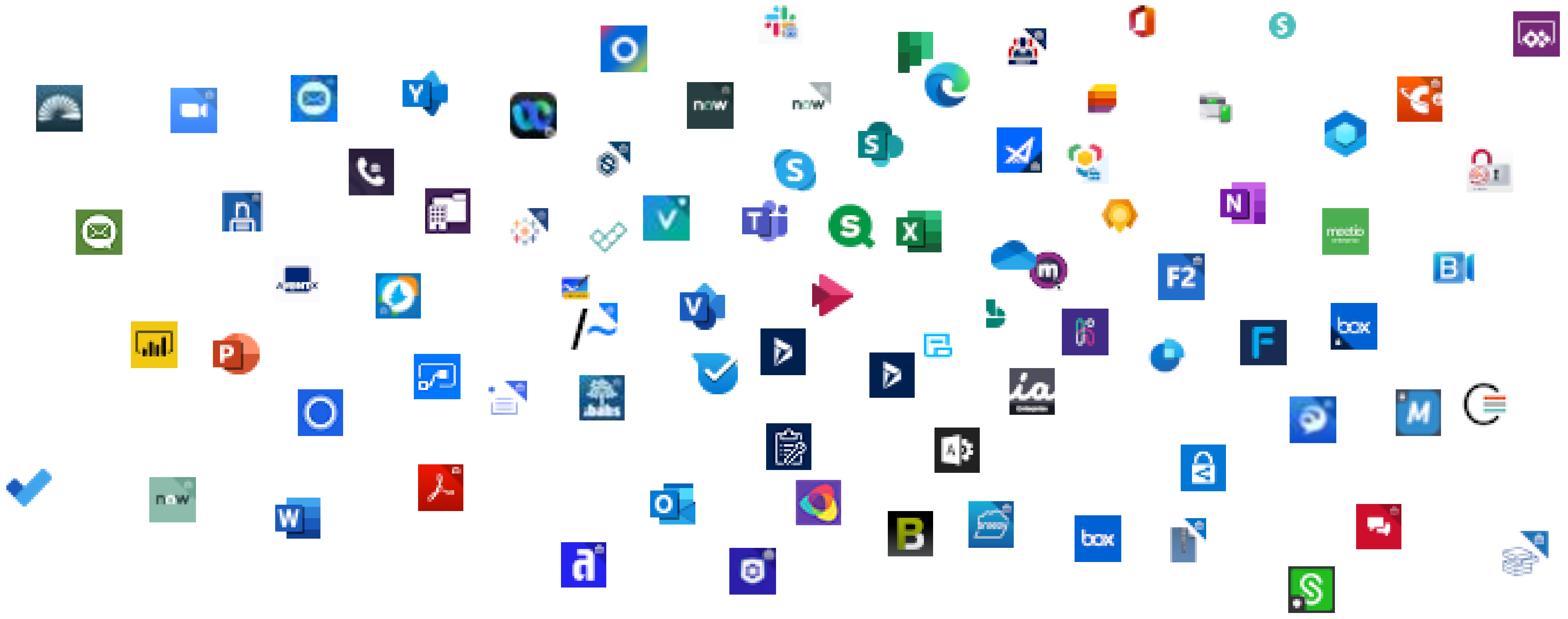


WHAT IS
REQUIRED?

What is required?

131 iOS apps

99 Android apps



Protect data at the app level

Data control / separation

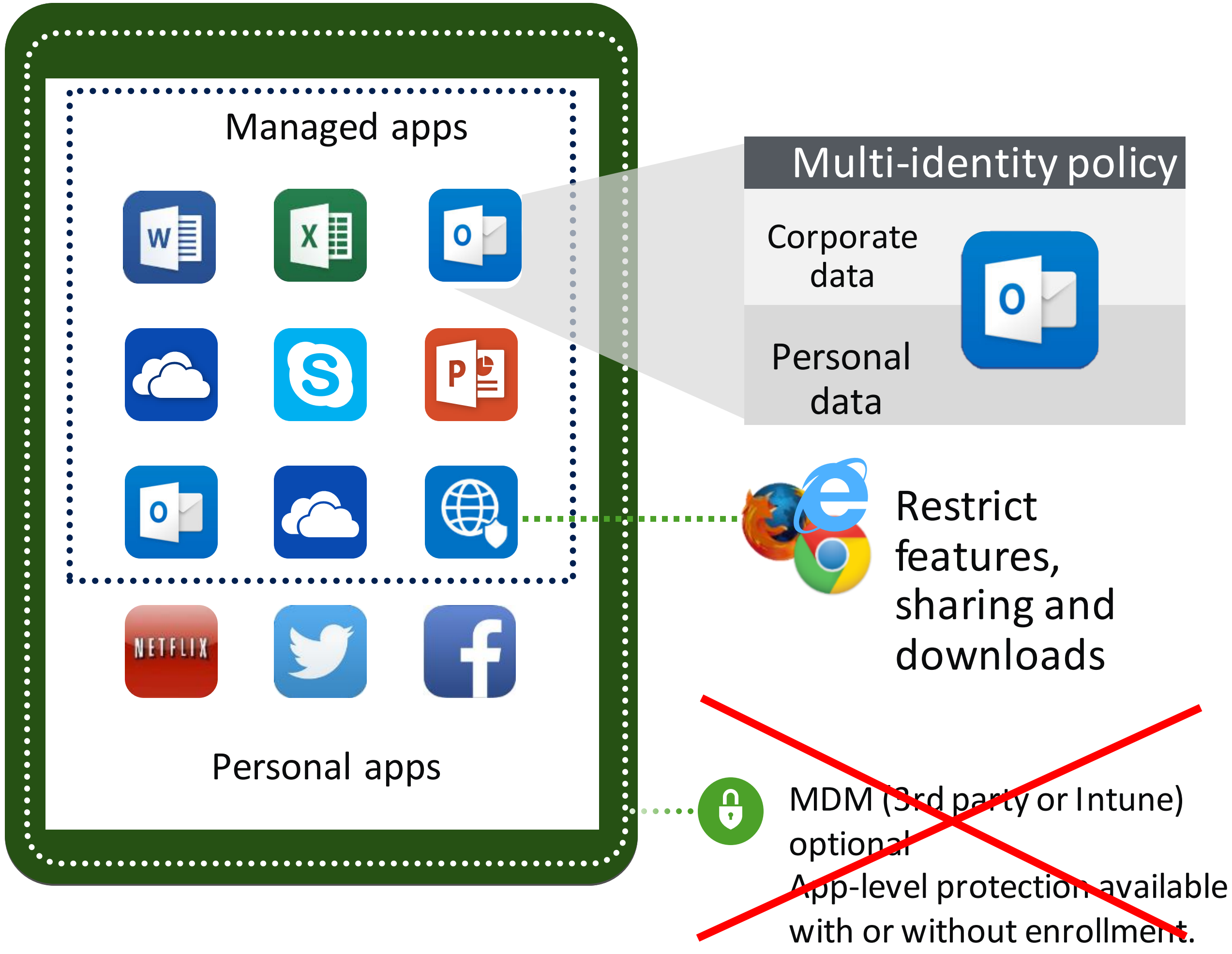
Control company data after it has been accessed, and separate it from personal data.

Conditional Launch

Jailbreak/root detection, version control, threat detection, etc.

Restrict apps and URLs

Restrict access to specific applications or URL addresses on mobile devices.



Managed apps

Personal apps

Multi-identity policy

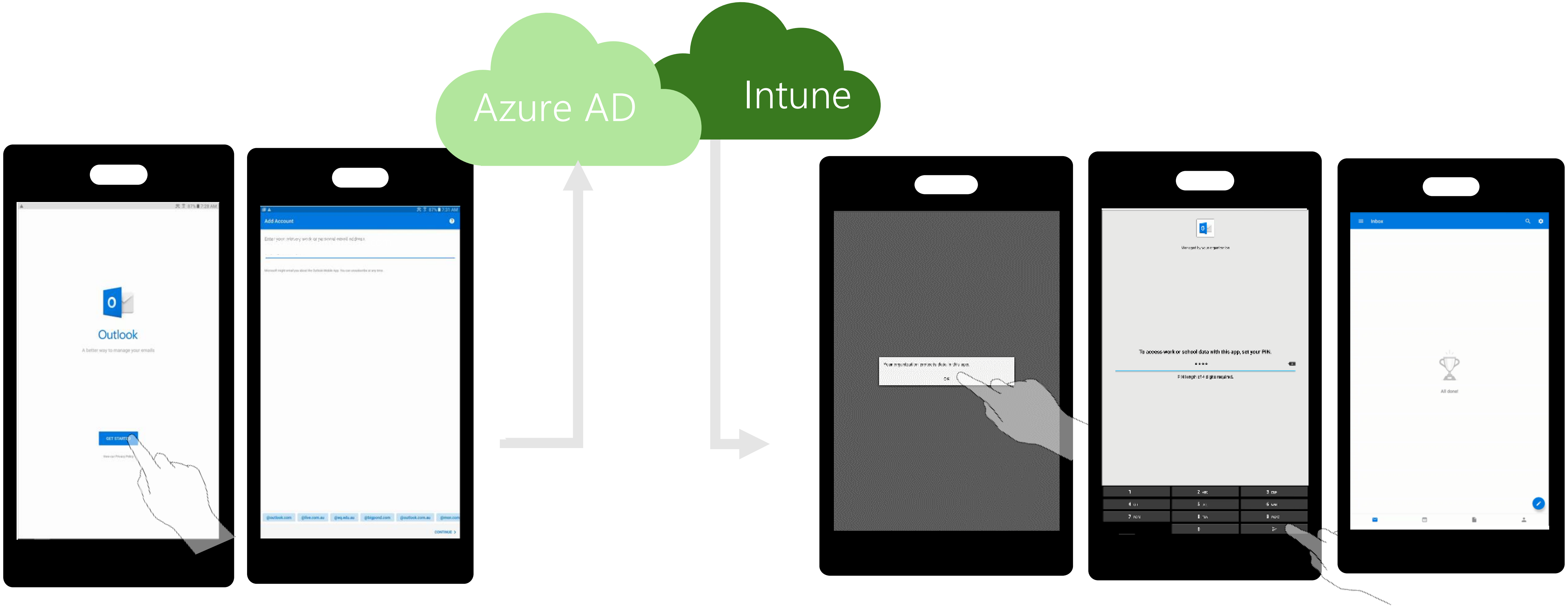
Corporate data

Personal data

Restrict features, sharing and downloads

~~MDM (3rd party or Intune) optional~~
~~App-level protection available with or without enrollment.~~

Modern Management (App Protection WE)



Enter your primary work or personal email address

Microsoft might email you about the Outlook Mobile App. You can unsubscribe at any time.

Your organization protects data in this app.

Managed by your organization

To access work or school data with this app, set your PIN.

PIN length of 4 digits required.

CAPABILITIES

App Protection Policy Settings

Data Relocation

- Android / iCloud Backup
- Transfer Data to other Apps
- Prevent Save As
- Restrict Cut Copy Paste
- Encrypt Data
- Web Links – Browser
- Disable Printing / 3rd party keyboards
- Block Screen capture [1]

Access

- Require PIN
- Complexity, Length
- Fingerprint, Facial Recognition
- Corporate ID
- Check-in frequency
- Offline Period

Lifecycle

- Min OS, Min patch version [1], Device Model(s), Device manufactures
- SafetyNet device attestation, require threat scan on apps [1]
- Min App Version, SDK Version
- Jailbroken/Rooted Devices
- Max PIN attempts

Remote Selective Wipe/Block Access/Reset PIN

1 Android Only
2 iOS Only

When are policies applied?

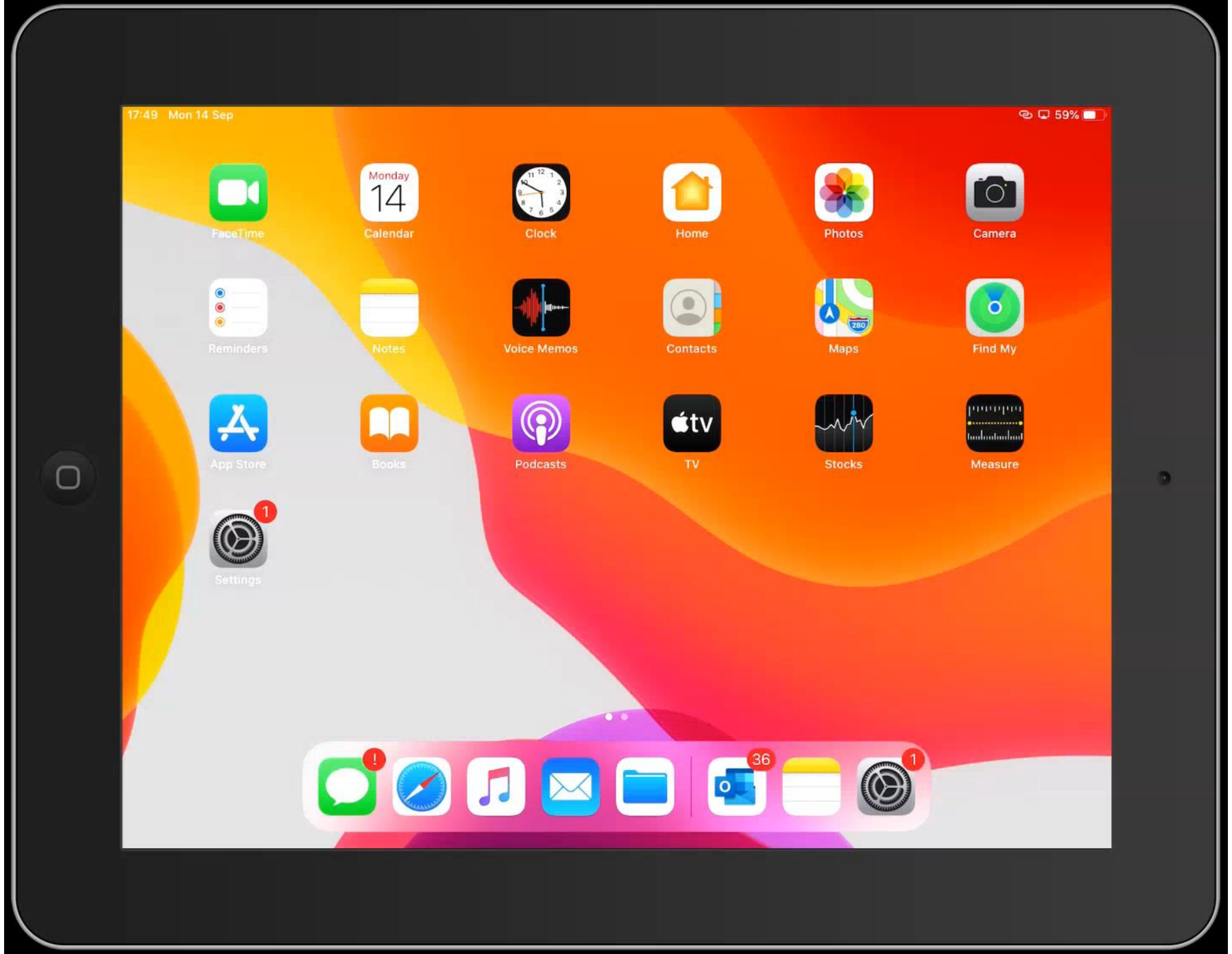
Check-in

- Initial App Sign-in
- Every 8 hours
- Unless there is a policy applied, then every 30 minutes

Selective Wipe

- Instantly when user signs out
- At next Check-in (IT Admin Driven)

- Front end
- Back end


17:49 Mon 14 Sep
59%
Monday
14
FaceTime
Calendar
Clock
Home
Photos
Camera
Reminders
Notes
Voice Memos
Contacts
Maps
Find My
App Store
Books
Podcasts
TV
Stocks
Measure
1
Settings
!
36
1

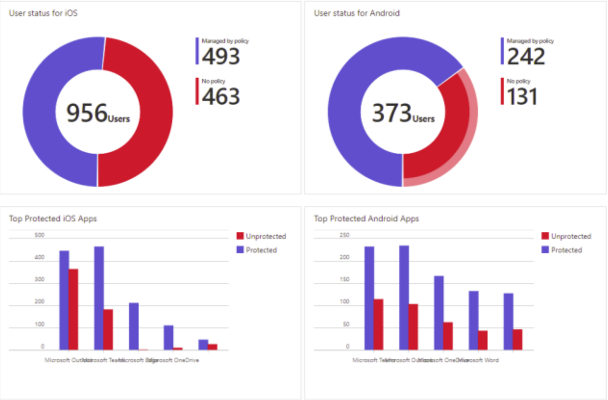
SO THE APP IS PROTECTED,

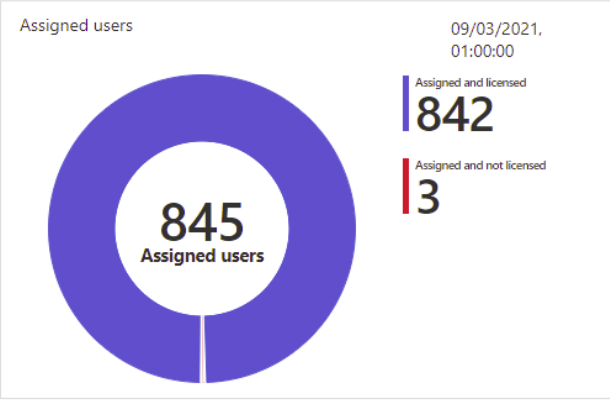
HOW CAN WE ENFORCE IT?

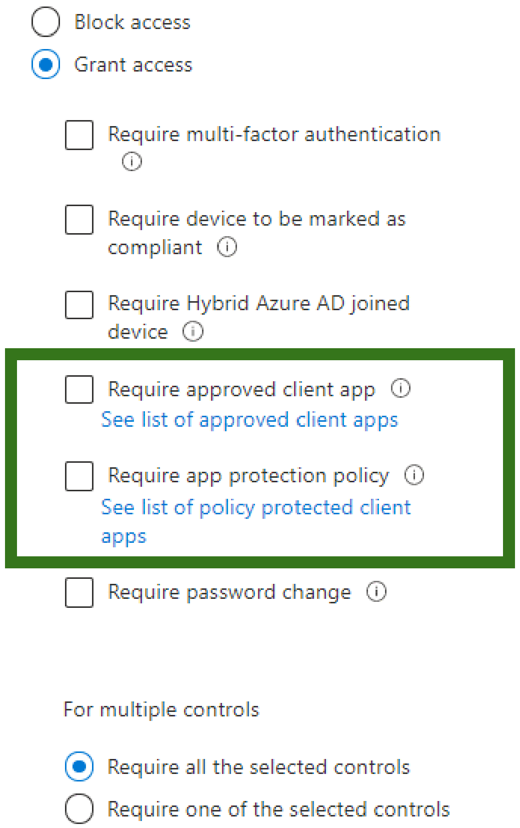
Requiring app (protection)

- Sometimes apps are not protected but have access;
  - Due to time outs – no App Protection policy applied yet.
  - Issues with App Protection Policy targeting
  - Due to licensing issues

- With Require App Protection Policy enable you can block access if an App is not yet protected by an App Protection Policy.







○ Block access
● Grant access

□ Require multi-factor authentication ⓘ

□ Require device to be marked as compliant ⓘ

□ Require Hybrid Azure AD joined device ⓘ

□ Require approved client app ⓘ
See list of approved client apps

□ Require app protection policy ⓘ
See list of policy protected client apps

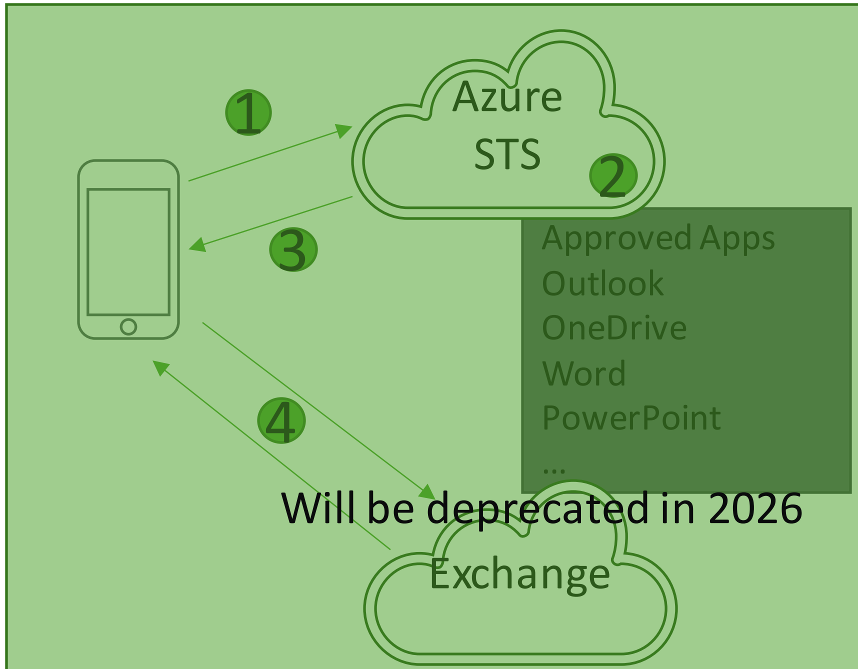
□ Require password change ⓘ

For multiple controls

● Require all the selected controls
○ Require one of the selected controls

Two options to enforce app (protection)

Require approved client apps

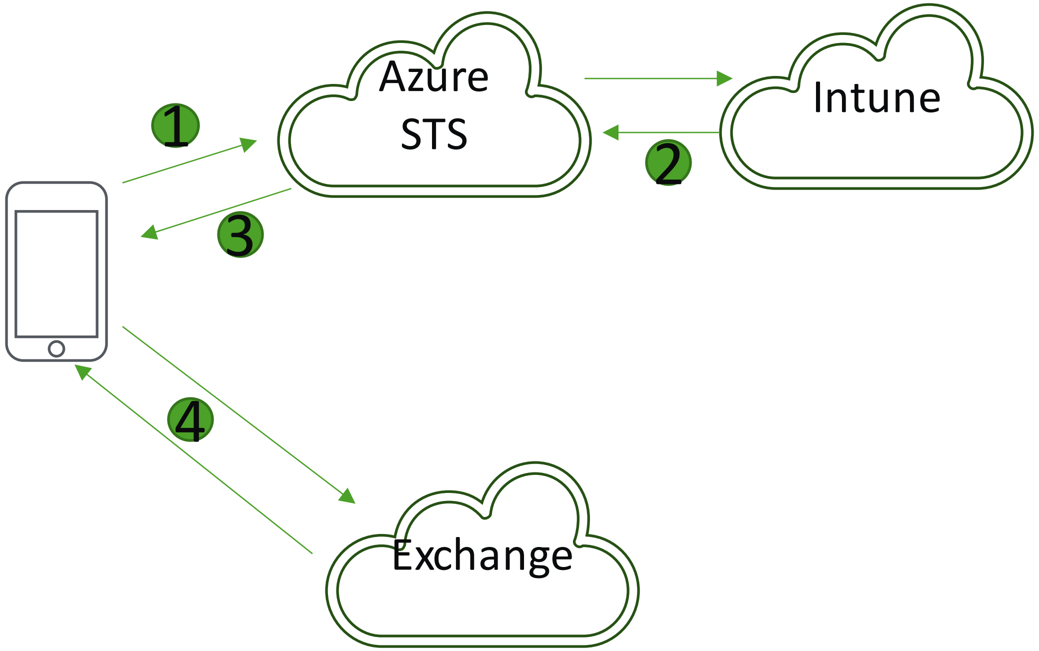


Approved Apps
Outlook
OneDrive
Word
PowerPoint
…

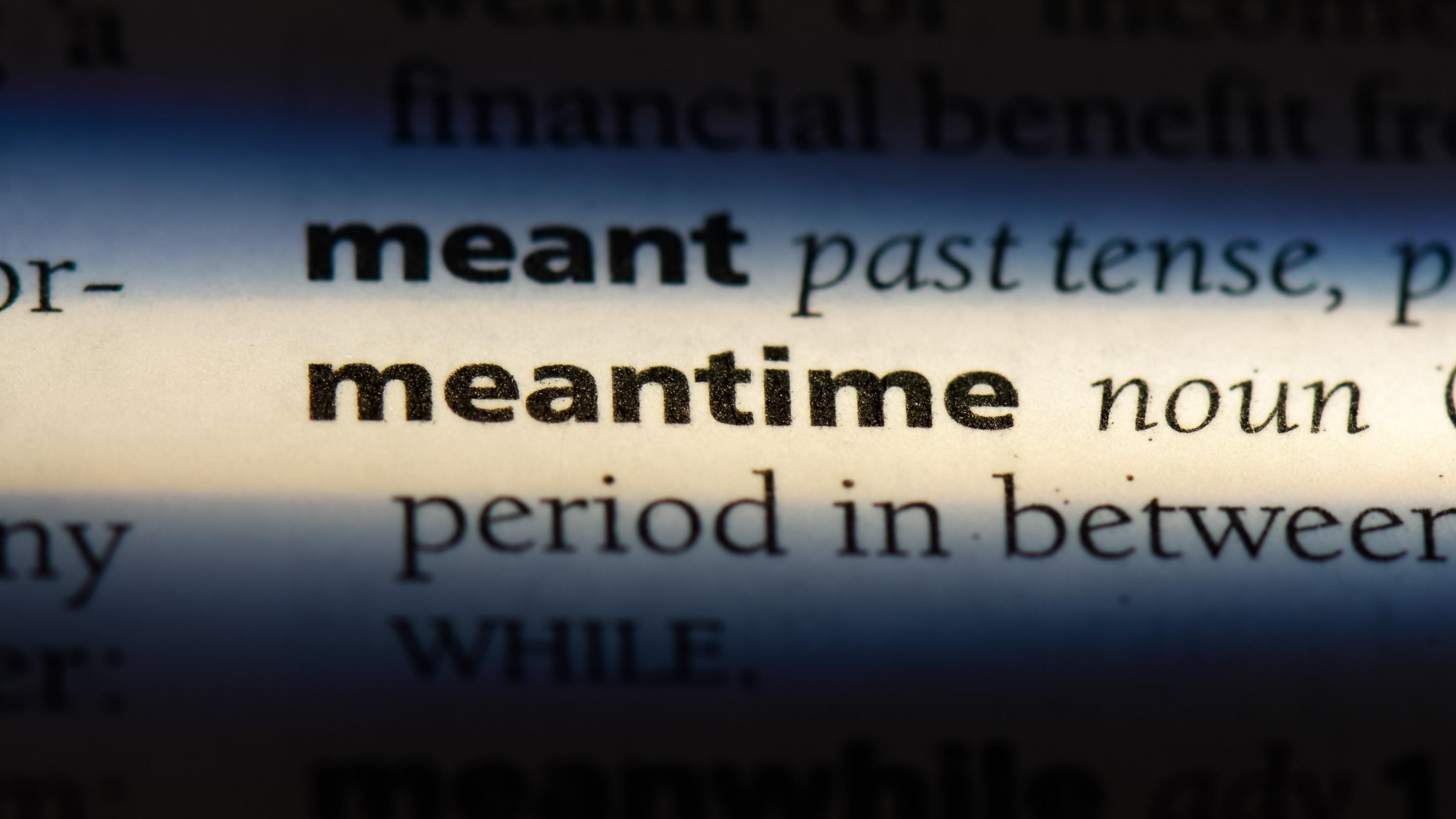
Will be deprecated in 2026

1. User logs into AAD
2. AADs STS service checks to see if this is an approved app.
3. If approved app, STS provides access token
4. Exchange data available

Require app protection policy



1. User logs into AAD
2. **AADs STS checks to see if Intune has reported the app protection policy applied.**
3. If policy applied, STS provides access token
4. Exchange data available



a

or-

ny

er:

financial benefit fr

meant *past tense, p*

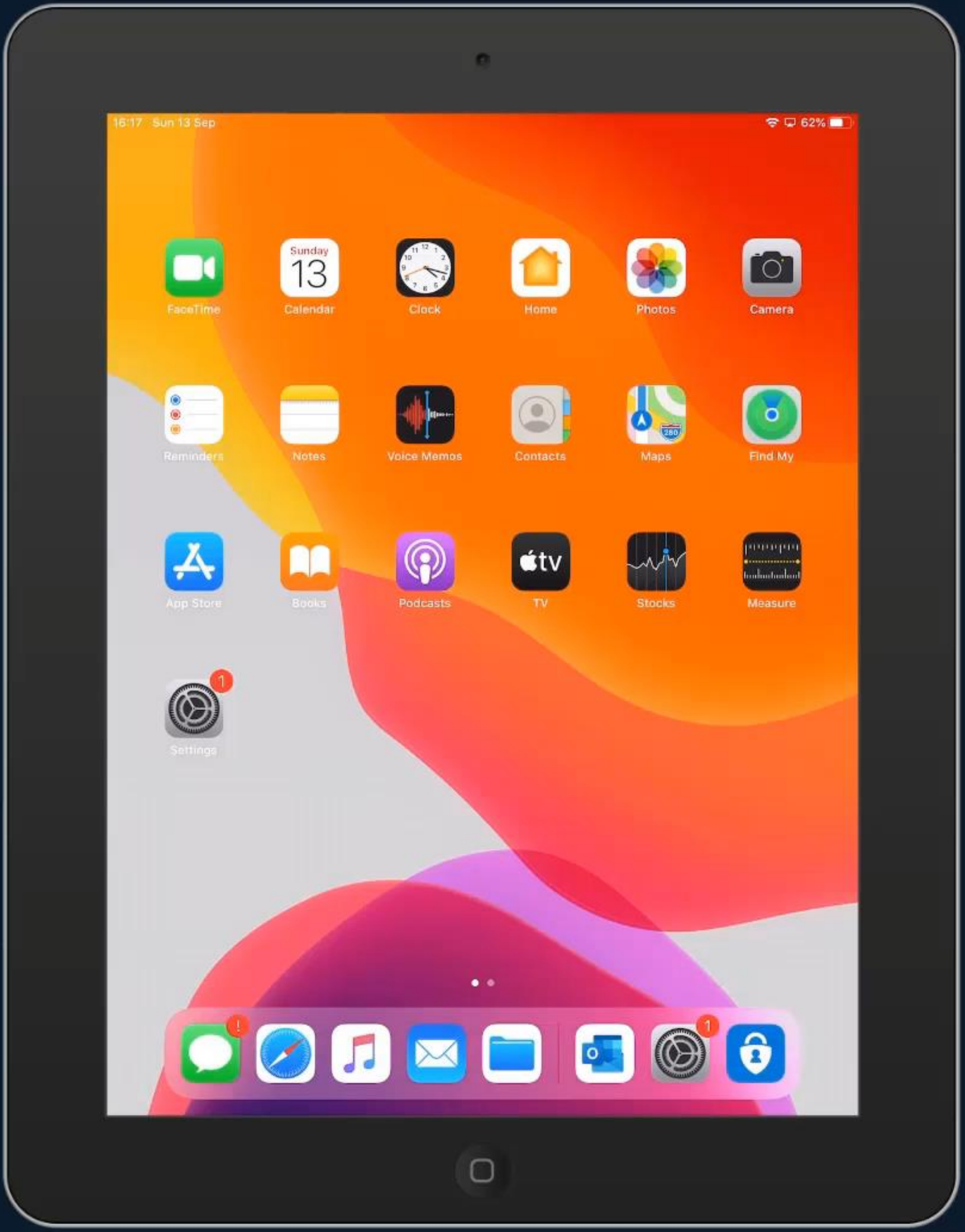
meantime *noun* (

period in between

WHILE.

meanwhile *adv*

DEMO


16:17 Sun 13 Sep
62%
FaceTime
Sunday
13
Calendar
Clock
Home
Photos
Camera
Reminders
Notes
Voice Memos
Contacts
Maps
Find My
App Store
Books
Podcasts
tv
TV
Stocks
Measure
1
Settings
1
1

SPYWARE
ALERT

ADDING EXTRA LAYER

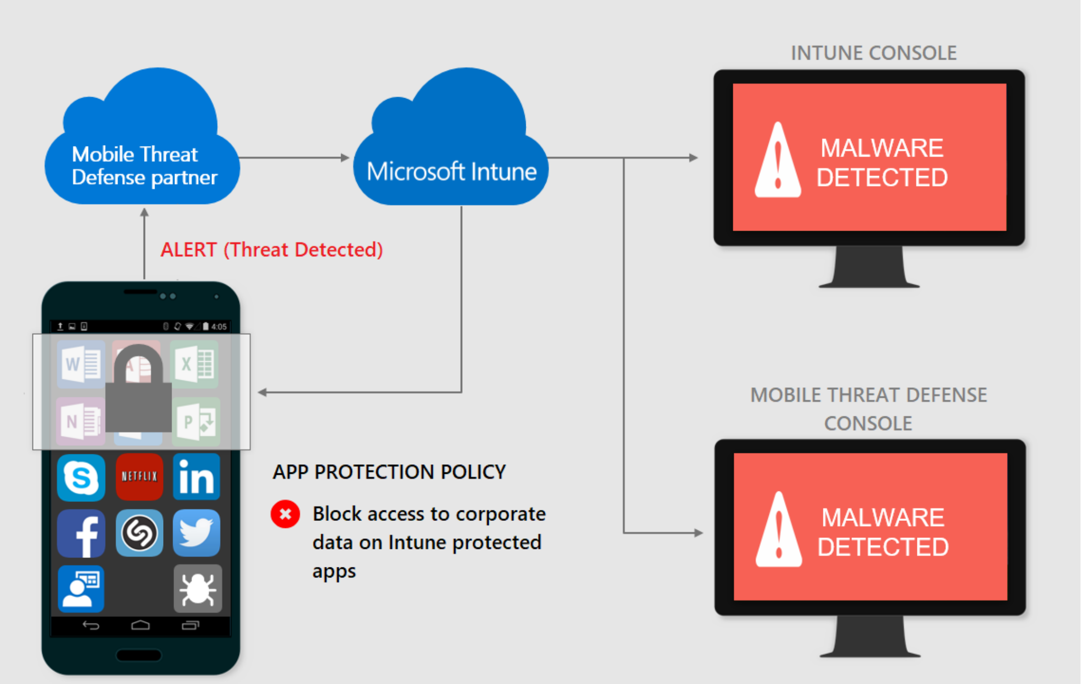
App Protection without enrollment

integrates with

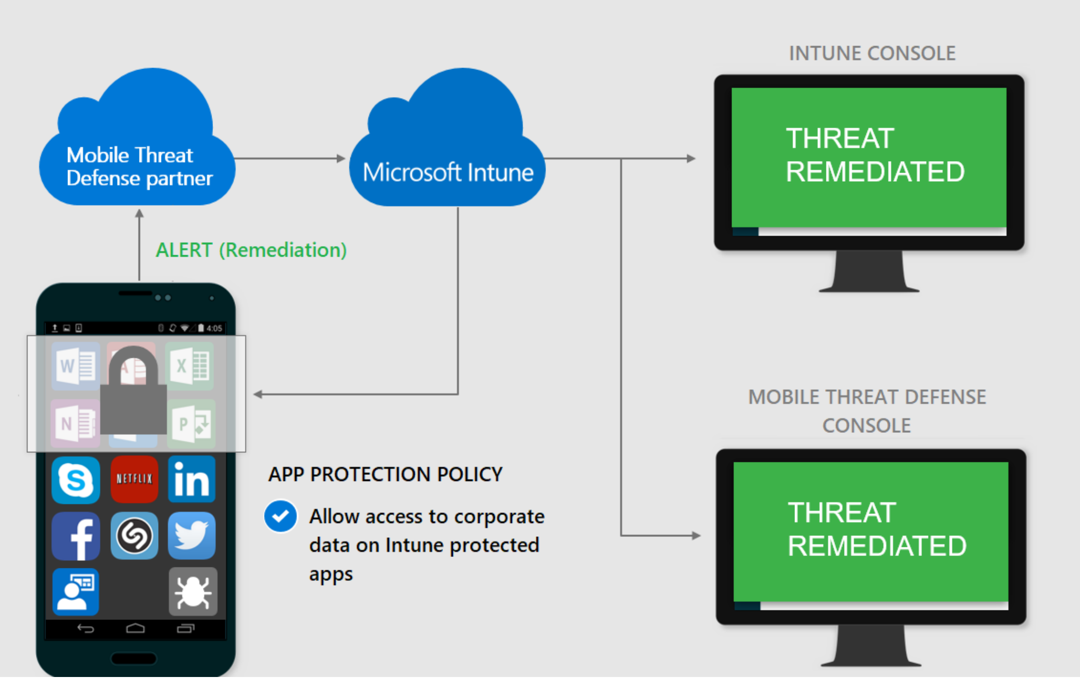
Mobile Threat Defense partners

Mobile Threat Defense – Partners

- Why have additional security tools on mobile devices?
- Supports both scenarios
  - MDM
  - Without Enrollment



Mobile Threat Defense partner
Microsoft Intune
INTUNE CONSOLE
MALWARE DETECTED
ALERT (Threat Detected)
MOBILE THREAT DEFENSE CONSOLE
MALWARE DETECTED
APP PROTECTION POLICY
Block access to corporate data on Intune protected apps



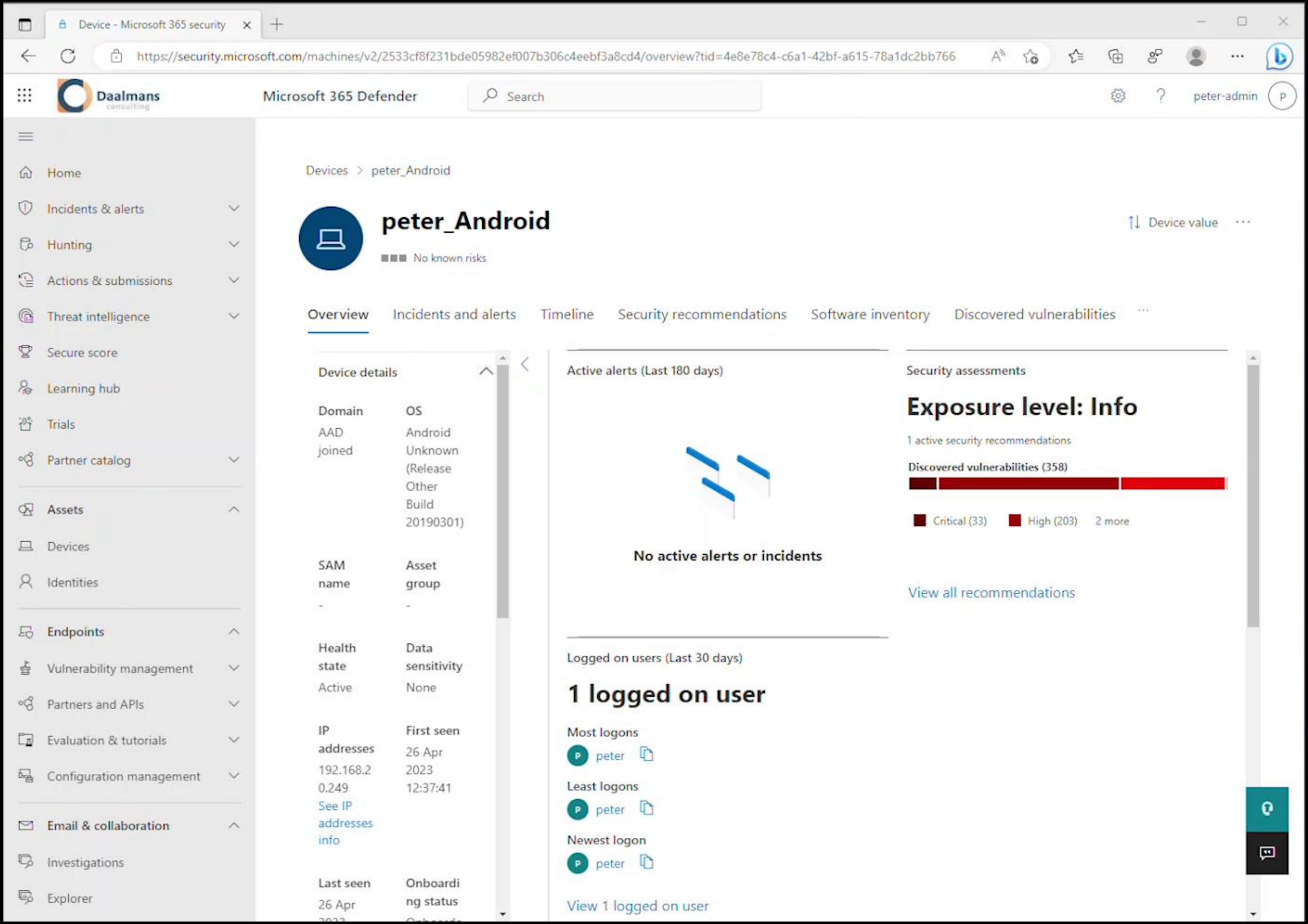
Mobile Threat Defense partner
Microsoft Intune
INTUNE CONSOLE
THREAT REMEDIATED
ALERT (Remediation)
MOBILE THREAT DEFENSE CONSOLE
THREAT REMEDIATED
APP PROTECTION POLICY
Allow access to corporate data on Intune protected apps

Mobile Threat Defense – Partners

- App protection policy support for additional partners since Oct 2019
- Block or selectively wipe a user’s corporate data based on the health of the device
- Use data from Microsoft Threat Defense partners or Microsoft Defender for Endpoint
  - Better Mobile
  - BlackBerry Protect Mobile
  - Check Point Harmony Mobile
  - Lookout for Work
  - Microsoft Defender for Endpoint
  - MVISION Mobile
  - Pradeo
  - SentinelOne
  - Sophos Mobile
  - Symantec Endpoint Protection Mobile
  - Trend Micro Mobile Security as a Service
  - Wandera Mobile Threat Defense
  - Zimperium

DEMO

Help a threat!



Devices > peter_Android

peter_Android

No known risks

Device details

Domain: AAD joined

OS: Android Unknown (Release Other Build 20190301)

SAM name: -

Asset group: -

Health state: Active

Data sensitivity: None

IP addresses: 192.168.20.249

See IP addresses info

First seen: 26 Apr 2023 12:37:41

Last seen: 26 Apr

Onboarding status

Active alerts (Last 180 days)

No active alerts or incidents

Logged on users (Last 30 days)

1 logged on user

Most logons: peter

Least logons: peter

Newest logon: peter

View 1 logged on user

Security assessments

Exposure level: Info

1 active security recommendations

Discovered vulnerabilities (358)

Critical (33) High (203) 2 more

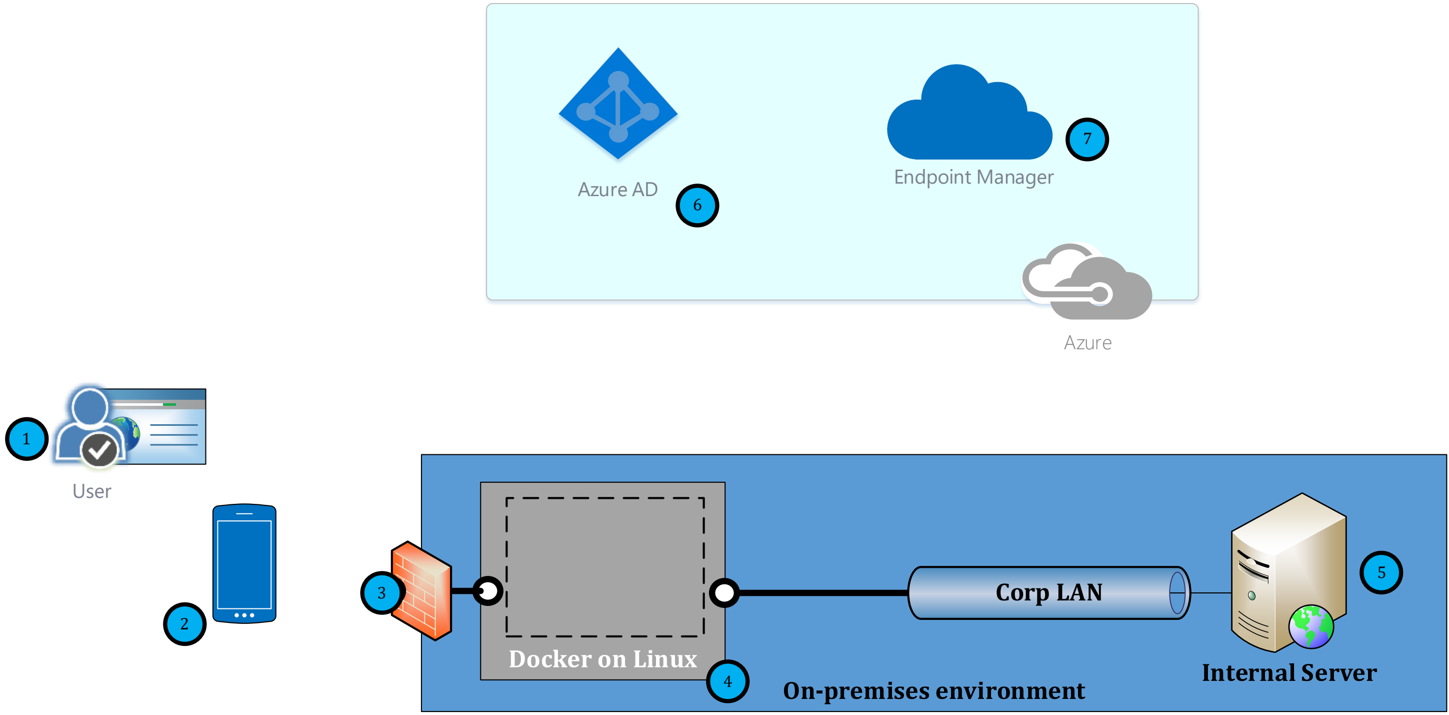
View all recommendations

Microsoft Tunnel for MAM

Access via Microsoft Tunnel

- VPN solution from Microsoft for Microsoft Intune (iOS/Android)

- User logs on via an App or Edge
- Edge is managed by Intune and is connecting to Microsoft Tunnel
- Microsoft Tunnel needs to be published via Proxy/Firewall
- Microsoft manages the Tunnel SW (Docker on Linux)
- Internal server accessible
- Azure AD Controls access via CA
- Microsoft Intune configures App/Edge + Microsoft Tunnel



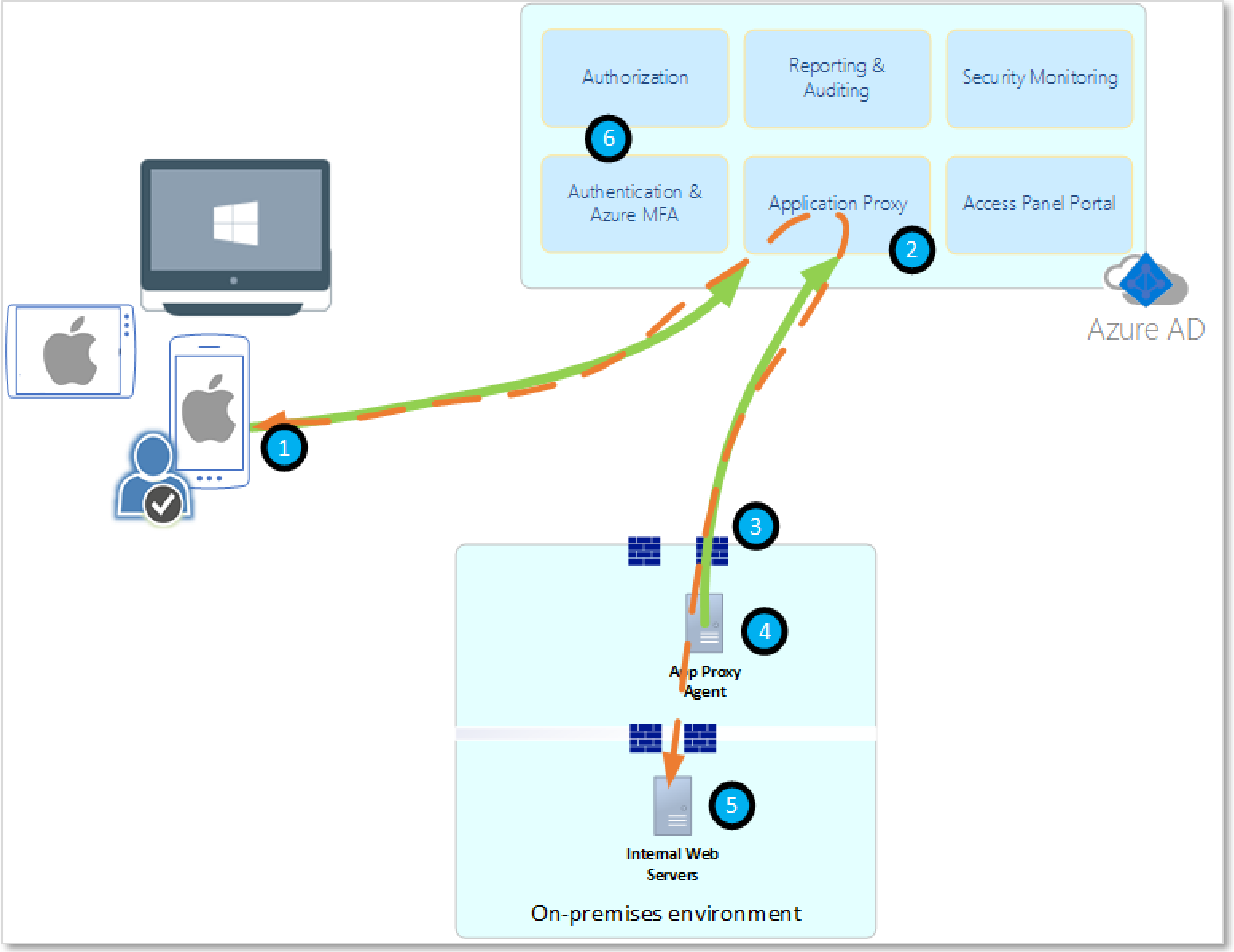
Microsoft Tunnel – What is it and how to set it up | Marius Sandbu (msandbu.org)

Access via Azure App Proxy

Access using Azure AD App Proxy

- Azure App Proxy part of Azure AD allows publishing internal web services. (all platforms)

- User logs on via a Browser
- User is redirected to Azure AD app proxy
  - User authenticates to Azure AD if preauth is enabled.
  - DDOS Out of the box
- Only outgoing ports need to be opened
- Agent needs to be installed
- Internal web service
- Conditional Access



Differences between solutions

Microsoft Tunnel	Azure AD App Proxy
Can be used for only iOS and Android	Can be used for all platforms
All ports are supported	Only port 80 and 443
Port 443 needs to be opened to setup the tunnel	No ports need to be opened to access server
Managed / updated by Microsoft	Managed / updated by Microsoft
MAM and MDM managed devices	Can be used without (pre) authentication / unmanaged device
Defender app or Tunnel capable app required	No extra apps required on device

DEMO

troubleshooting
fix
service
technical
house
maintenance
tool
inspecting
man
profession
expert
computer
management
information
programmer
plumber
success
data
equipment
heating
plumbing
idea
technology
assistance
troubleshooter
hardware
communication
advice
engine
repairman
installing
digital
handyman
check
worker
internet
trouble
solve
question
occupation
control
workman
job
work
professional
industry
consulting
working
repair
inspection
solution
support
problem
server
engineer
technician
upkeep
system
network
fixing
tech
help
software
education
business
workshop
virus
teamwork
mechanic
wrench

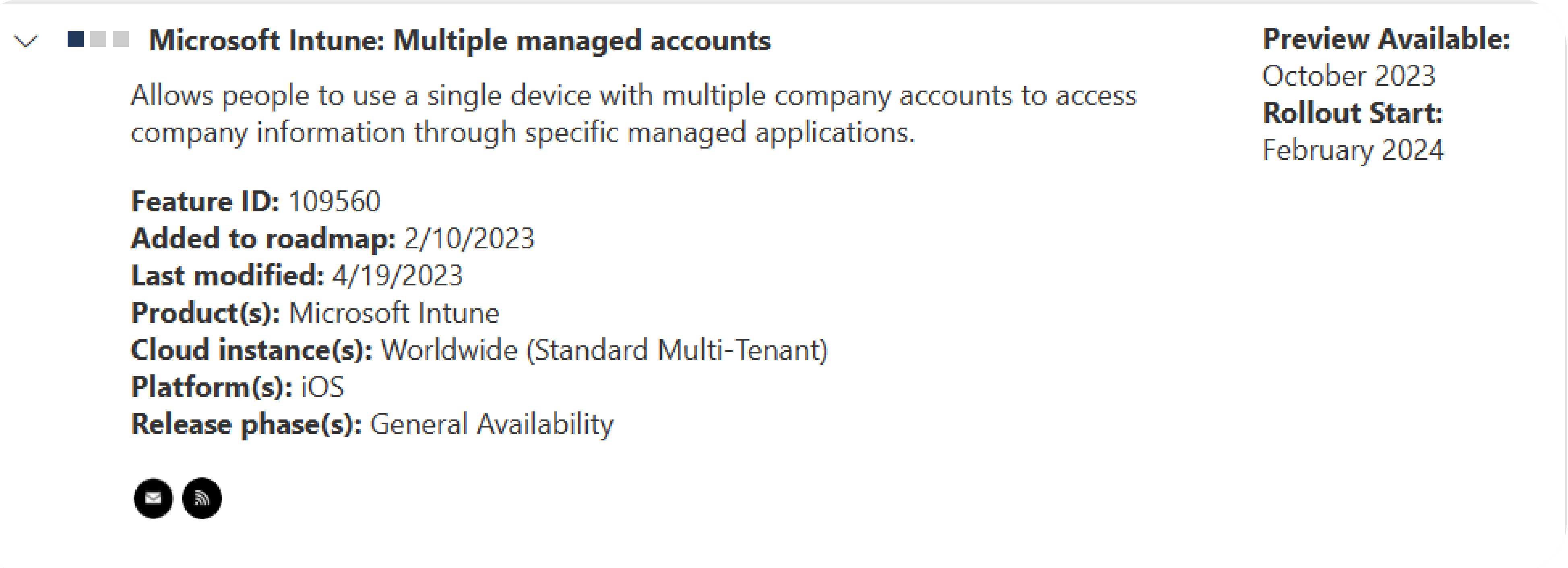
Microsoft Edge is your friend

- **about:IntuneHelp**
  - Collect Intune Diagnostics
  - Review current state
  - Review Intune App Status

DEMO

PLANS FOR THE
COMING YEAR

What’s coming up?



Microsoft Intune: Multiple managed accounts

Allows people to use a single device with multiple company accounts to access company information through specific managed applications.

Feature ID: 109560
Added to roadmap: 2/10/2023
Last modified: 4/19/2023
Product(s): Microsoft Intune
Cloud instance(s): Worldwide (Standard Multi-Tenant)
Platform(s): iOS
Release phase(s): General Availability

Preview Available:
October 2023
Rollout Start:
February 2024

CONCLUSION

WHAT’S NEXT?

EMBRACE MODERN

GOOD SECURITY

HAPPY USERS

Ask questions and share knowledge at:

Reddit: http://www.reddit.com/r/Intune
Reddit: http://www.reddit.com/r/SCCM
Facebook group: Microsoft Enterprise Mobility +Security

YouTube: youtube.com/c/EnterpriseMobilityTips

Join the communities:

Workplace Ninja’s network: https://wpninja.eu
Workplace Ninja User Group NL: https://wpninja.nl
MC2MC Community BE: https://mc2mc.be
MMS: https://mmsmoa.com

Do you have an NDA with Microsoft?

Yes?

Join the Microsoft Customer Connection

https://aka.ms/joinccp

teşekkür ederim

mulțumesc

اركش

MERCI

grazas

thank you

dankie

dankeschön

نونمم

Благодарю вас

gratias ago

dank u

谢谢

tack

kiitos

ありがとう

gracias

GRAZIE

gràcies

OBRIGADO

dankon