
Use Intune like Nudge for iOS

(Even if it's not your MDM)

Milly Marsh

Sr. Apple Device Administrator

@TechM on MacAdmins Slack



Guest Appearances

- **JNUC '19 Panel: Acing Enrollment**
- **JNUC '21: "We Could Be Heroes!"**
Empowering SMEs in a media production environment
- **PSUMac '22: The 7 Habits of Highly Effective Feedback**
Better Results through Powerful User Stories
- **Apple IT Tech Camp '23 @ Los Angeles, San Diego**
Invited to present and discuss the AppleSeed testing template for OS readiness



Fun Facts About Me

- **260-mile, 5-day bike ride with Girl Scouts**
(Santa Barbara to San Diego, beach camping)
- **Technology Committee (1997)**
@ Will Rogers Learning Community
- **Drafted into 2006 Macworld keynote** 🥵
bumped into Steve Jobs + entourage
- **Over 100 flights to/from Guatemala**
attending school, visiting family
- **Crochet as a hobby**
hats, scarves, blankets



Before we begin...

This session is **not** about:

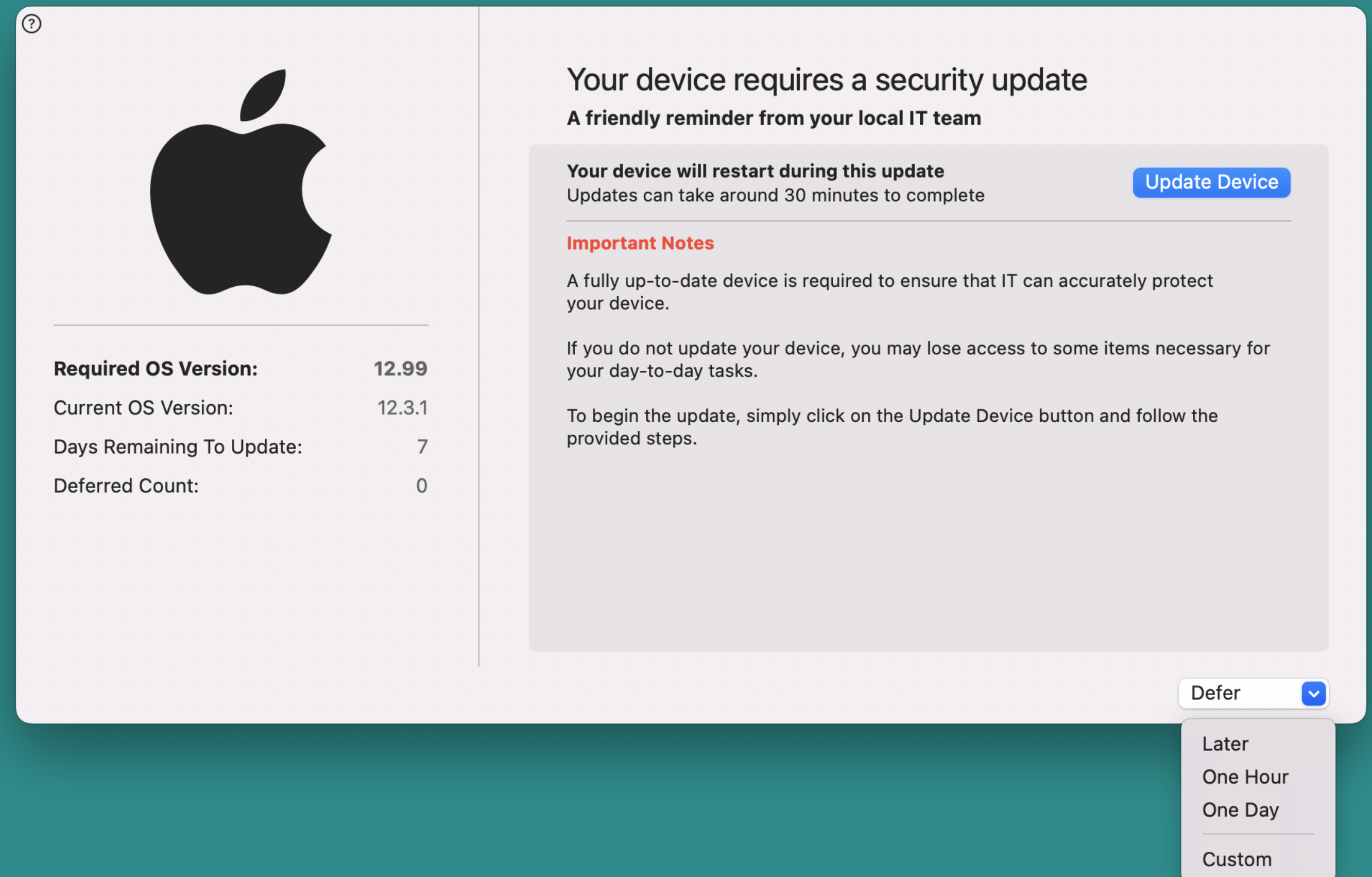
- Supervised Device Enrollment
- BYOD User Enrollment
- Using Intune as MDM
- Forcing an update onto a user's device

This session **is** about:

- Conditional Launch
- App Protection Policies
- Nudging users to update their device
- Reminding them of their responsibility

What is Nudge?

- Reminds users to update macOS
- **Cannot force** updates
- Guides users to Software Update
- Accepts configuration profiles
- Admin sets minimum OS and install deadline
- Progressively more annoying as deadline approaches
- User deferrals are logged



Outline



**Problems with
updating iOS**



Solutions



**User
Experience**



**Implementation
& Caveats**

Problems with updating iOS

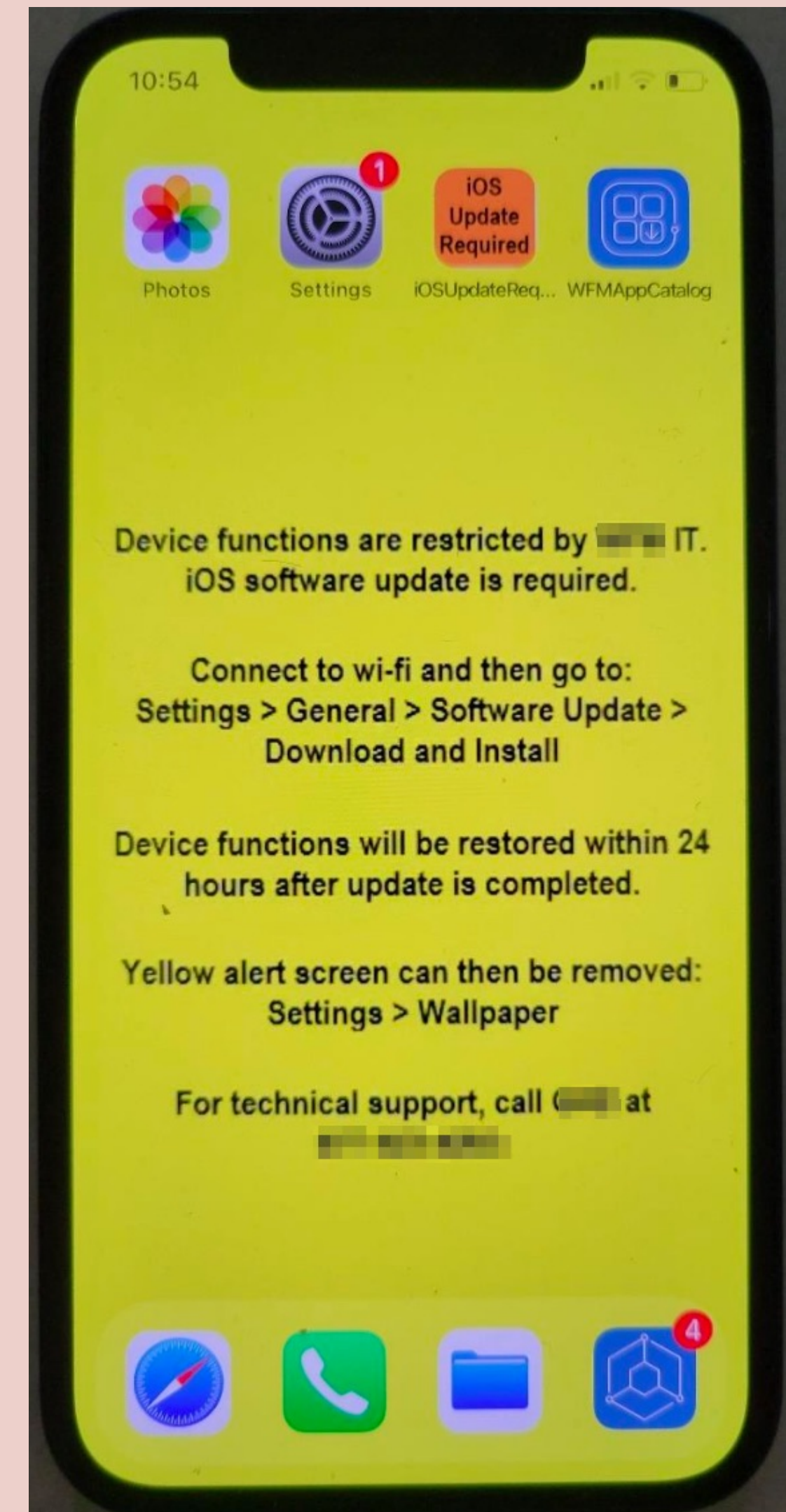
The old ways...

- **Security posture decided in a vacuum**
- **MDM vendor limitations:**
 - **i.e monolithic profile**
- **Change management not enforced**
- **No communication to support teams**



The experience...

- Users had 4 days to update their company device
- Critical functions blocked / hidden:
 - Authenticator, Wallet, Accessibility Modes, Erase All Contents & Settings
- Up to 24hr latency reporting to MDM after user complied with OS update
- Inventory update not 100% consistent
- No data protection on BYOD devices



High user impact

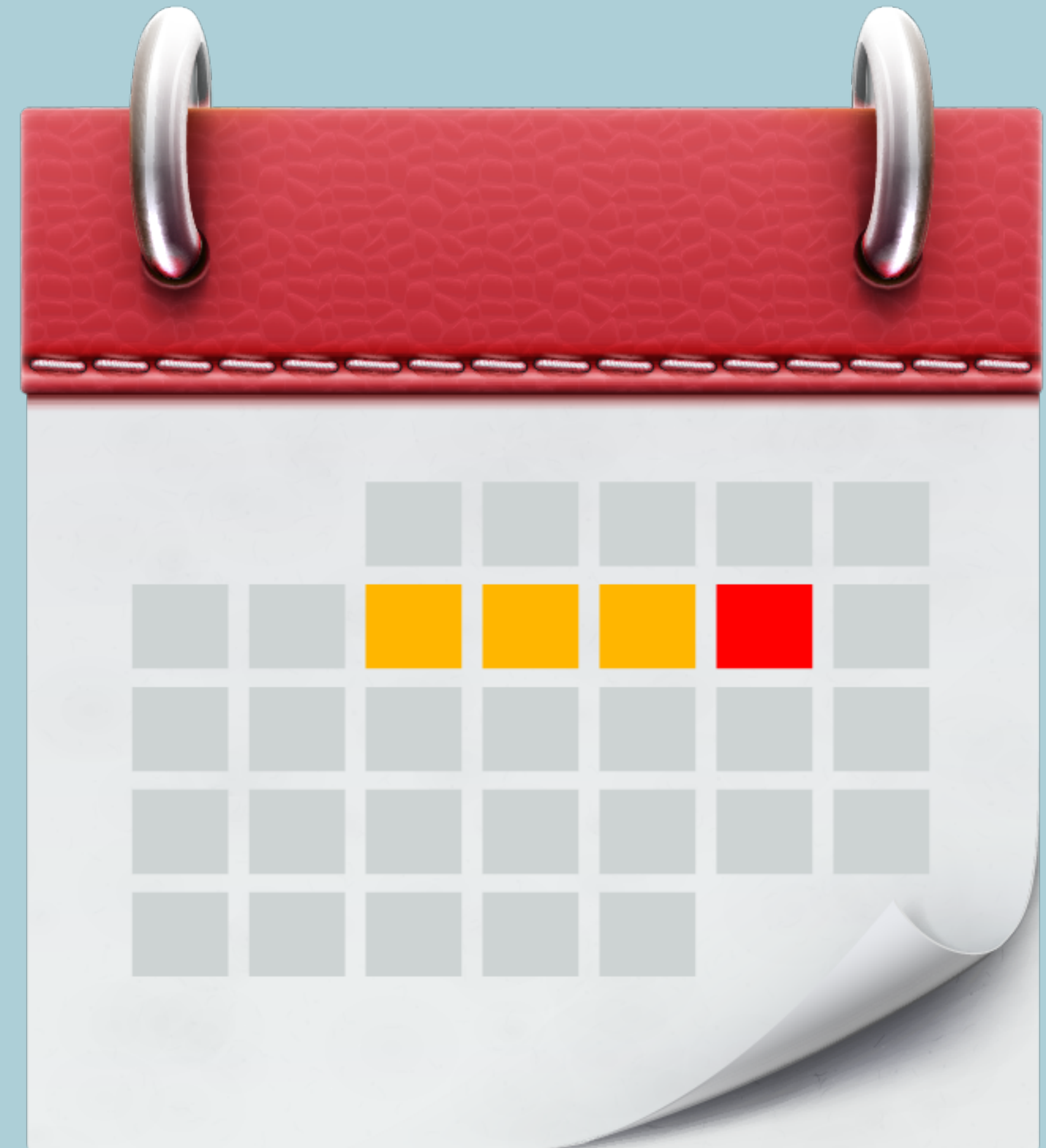
- **Large volume of Help Desk calls**
 - **Frequently misrouted to wireless VAR for “problem with iPhone.”**
 - **Helpdesk lacked access to MDM console**
 - **No KB articles for users to update OS**
 - **High rate of escalations, low rate of first-call resolutions**



Solutions

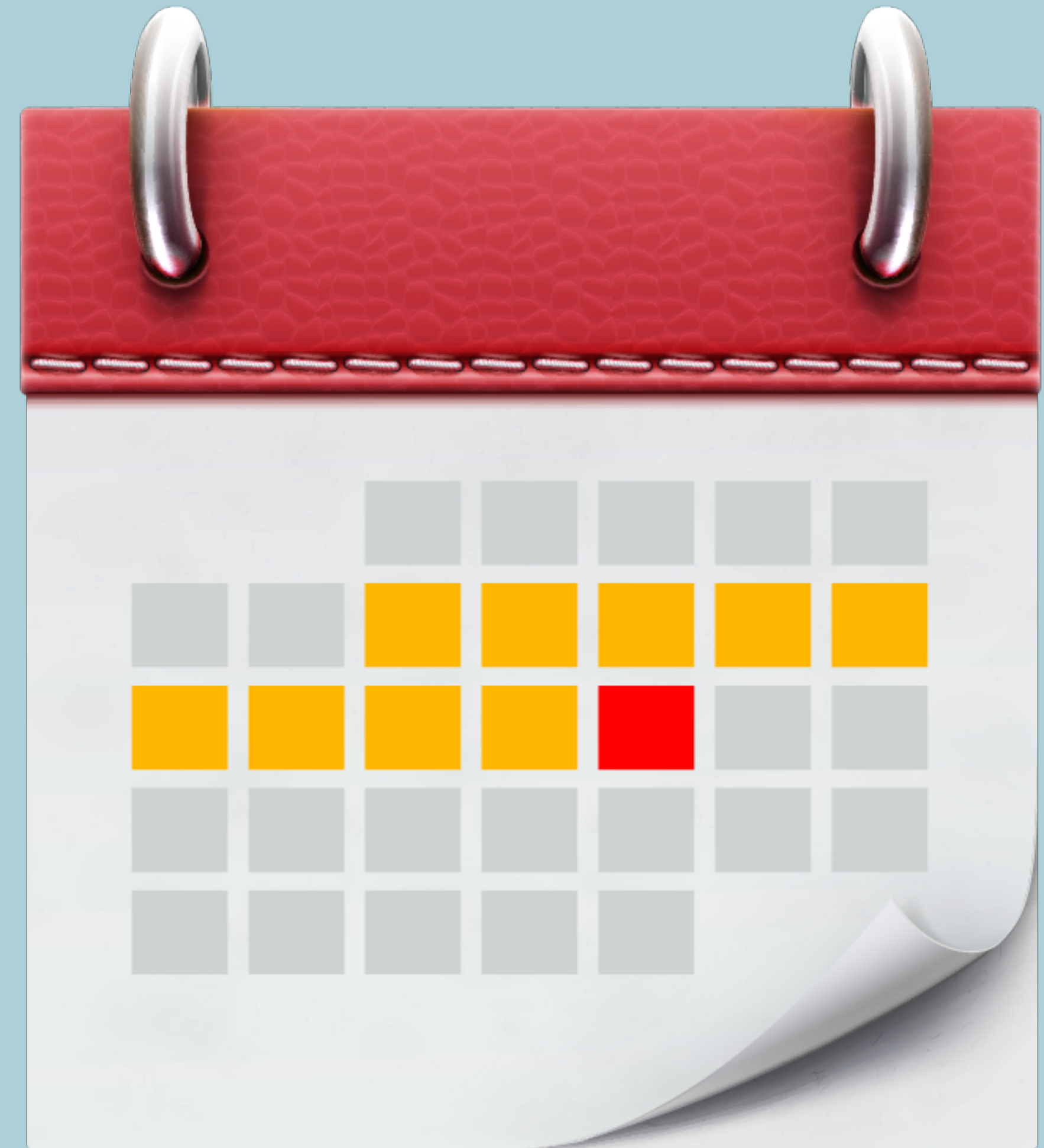
Short-term Relief

➤ Extend grace period to 10 days



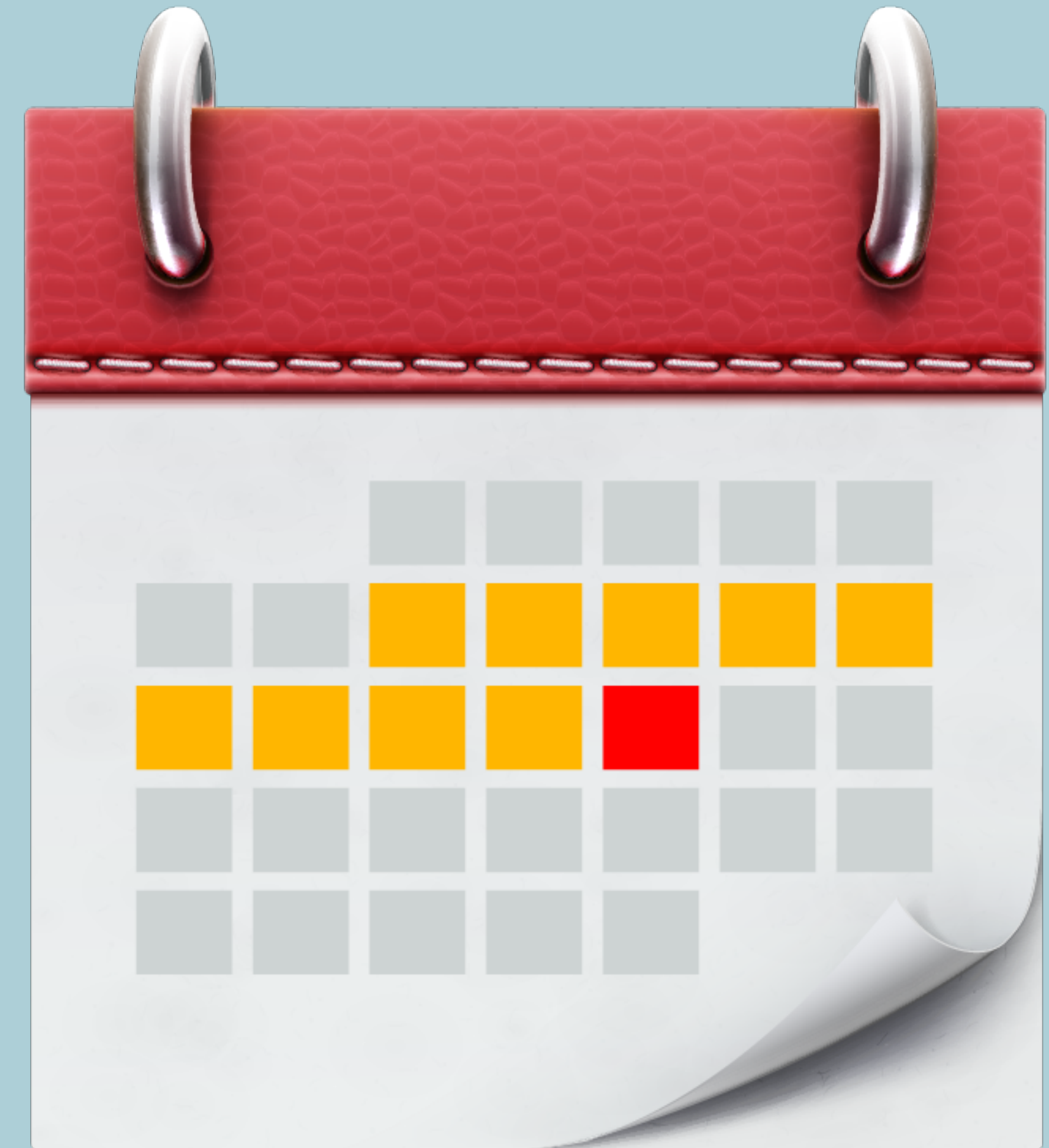
Short-term Relief

- Extend grace period to 10 days



Short-term Relief

- **Extend grace period to 10 days**
- **Share Apple KB HT201222 with all support teams**
- **Audit MDM console for OS update “policies” (configuration profiles)**
- **Explore solutions outside the box**



Hiding in plain sight

- **Intune: Mobile App Management (MAM)**
 - **App Protection Policies**
 - **Conditional Launch**
 - **Data protection for licensed accounts**
 - **Works with Supervised, BYOD, or Unmanaged Devices**



Improvements

- Implemented app protection policy for iOS 16.3.1
- MAM app protection policies are effective on managed and unmanaged iOS devices.
- The user decides on the best time to update their device.
- Significant uptake for entire fleet within 24 hours.



Noteworthy...

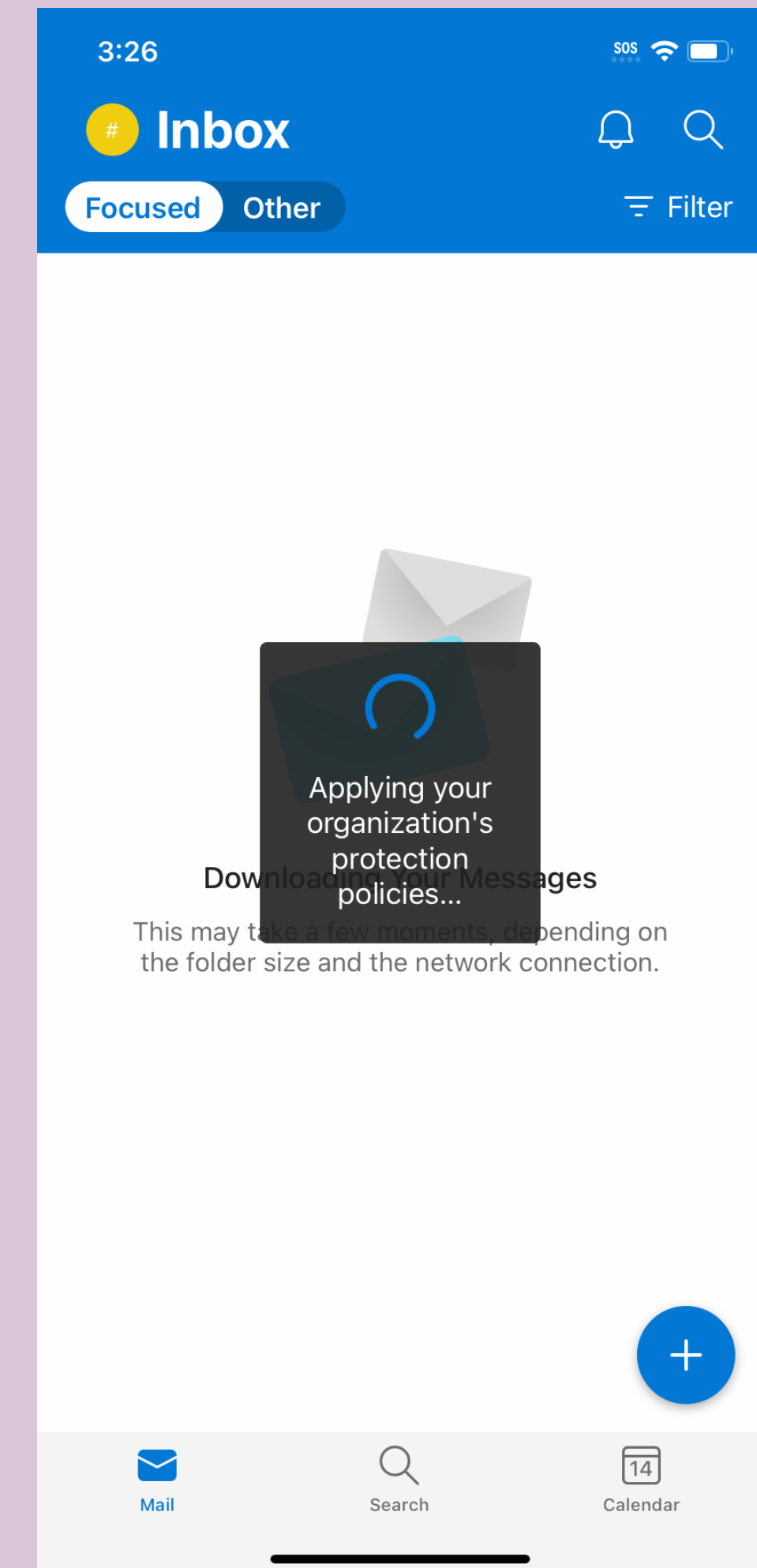
- Our devices are MDM enrolled (just not with Intune)
- We do not employ Software Update deferrals.
- Organizational data in the app is protected when the Block policy goes into effect.
- Essential apps, settings, user preferences untouched.
- Our company is achieving about 87% compliance on managed fleet before “block” is set.
- Ticket volume & escalations reduced by 82%



User Experience

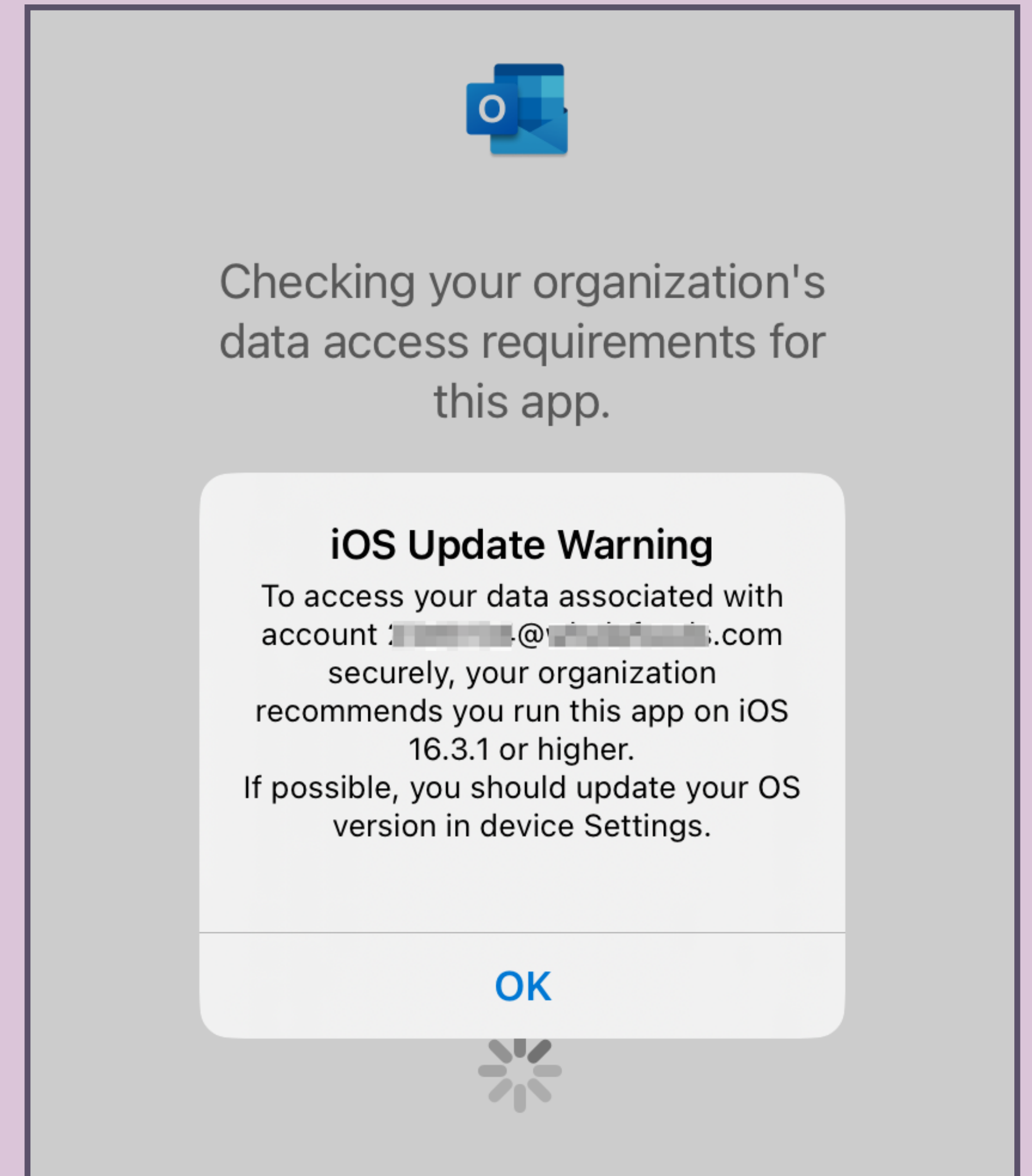
Applying Protection Policies

- **“Conditional Launch”**
- **Applying Organization’s protection policies**
- **App will quit and need to be re-launched**
- **Policies will be checked on app launch and periodically thereafter**



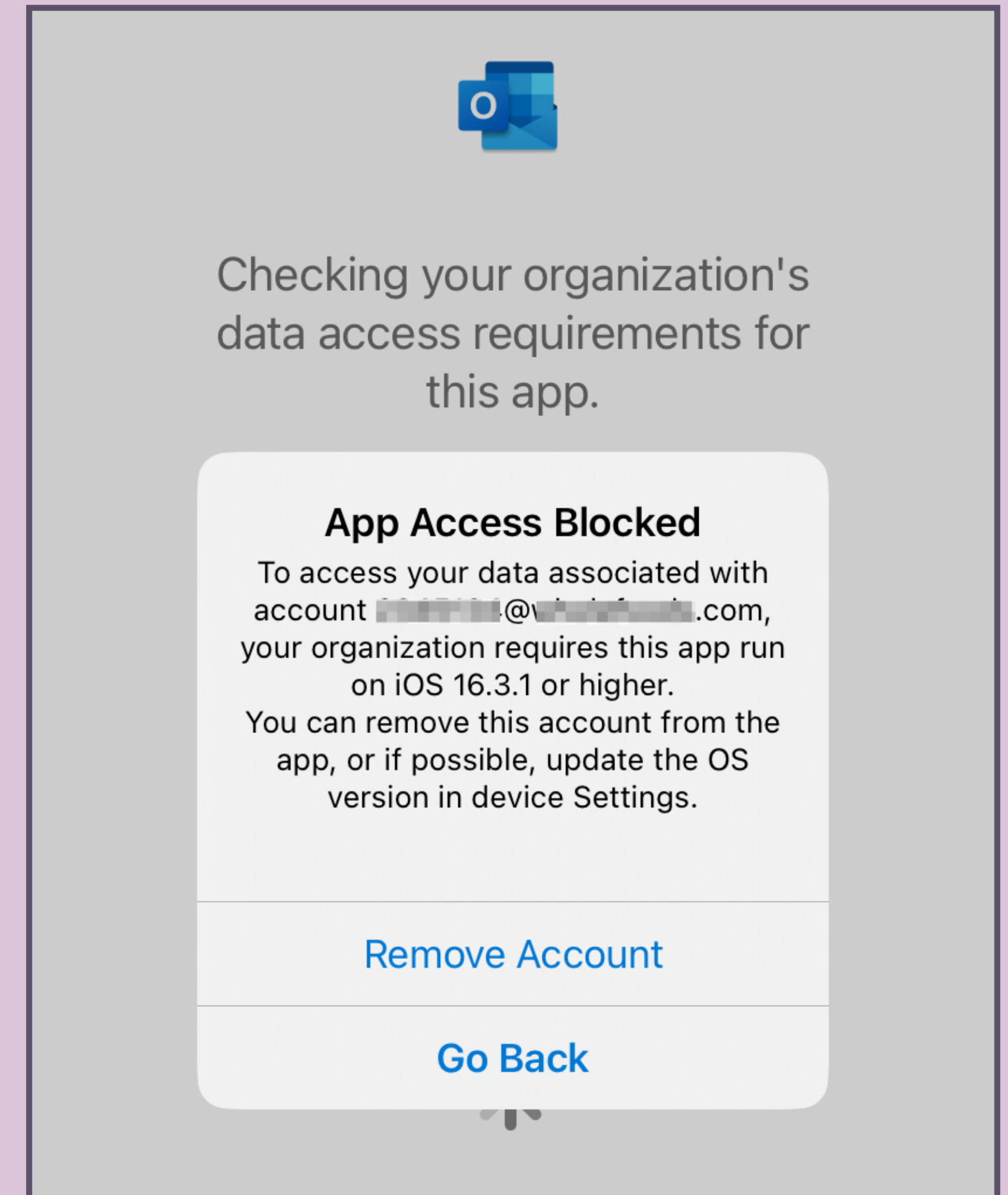
iOS Update Warning ⚠

- **Conditions are checked on app launch**
- **Examples of items that can be checked:**
- **iOS version, app version, device age, PIN age, jailbroken, etc.**
- **In this example, if iOS version requirement is not met, a warning is displayed.**



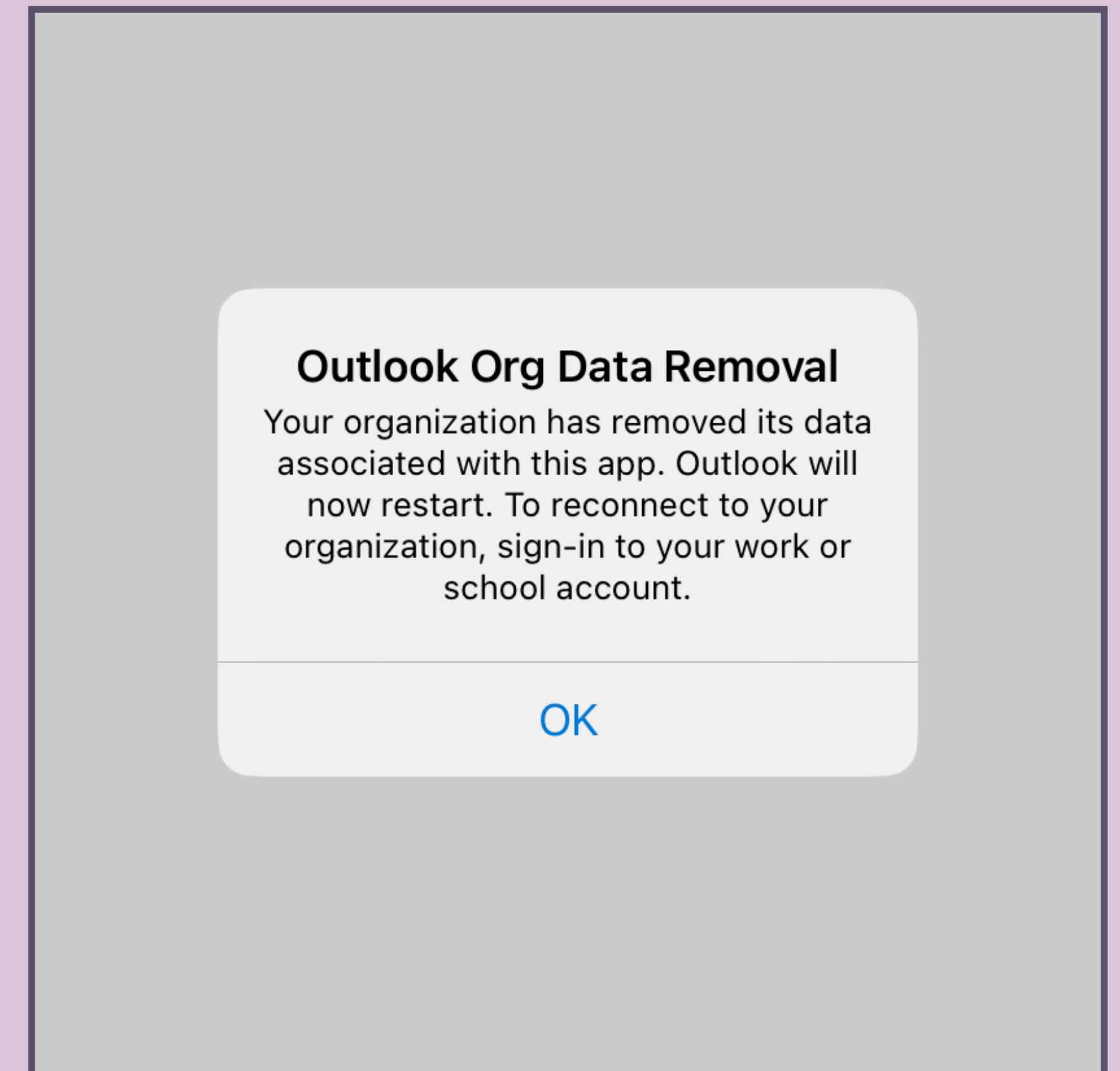
App Access Blocked

- Admin changes Intune policy to “block”
- In this example, iOS version requirement not met — access blocked
- User informed of required action.
- User may remove the enterprise account to continue accessing the app.
- Example: personal accounts configured



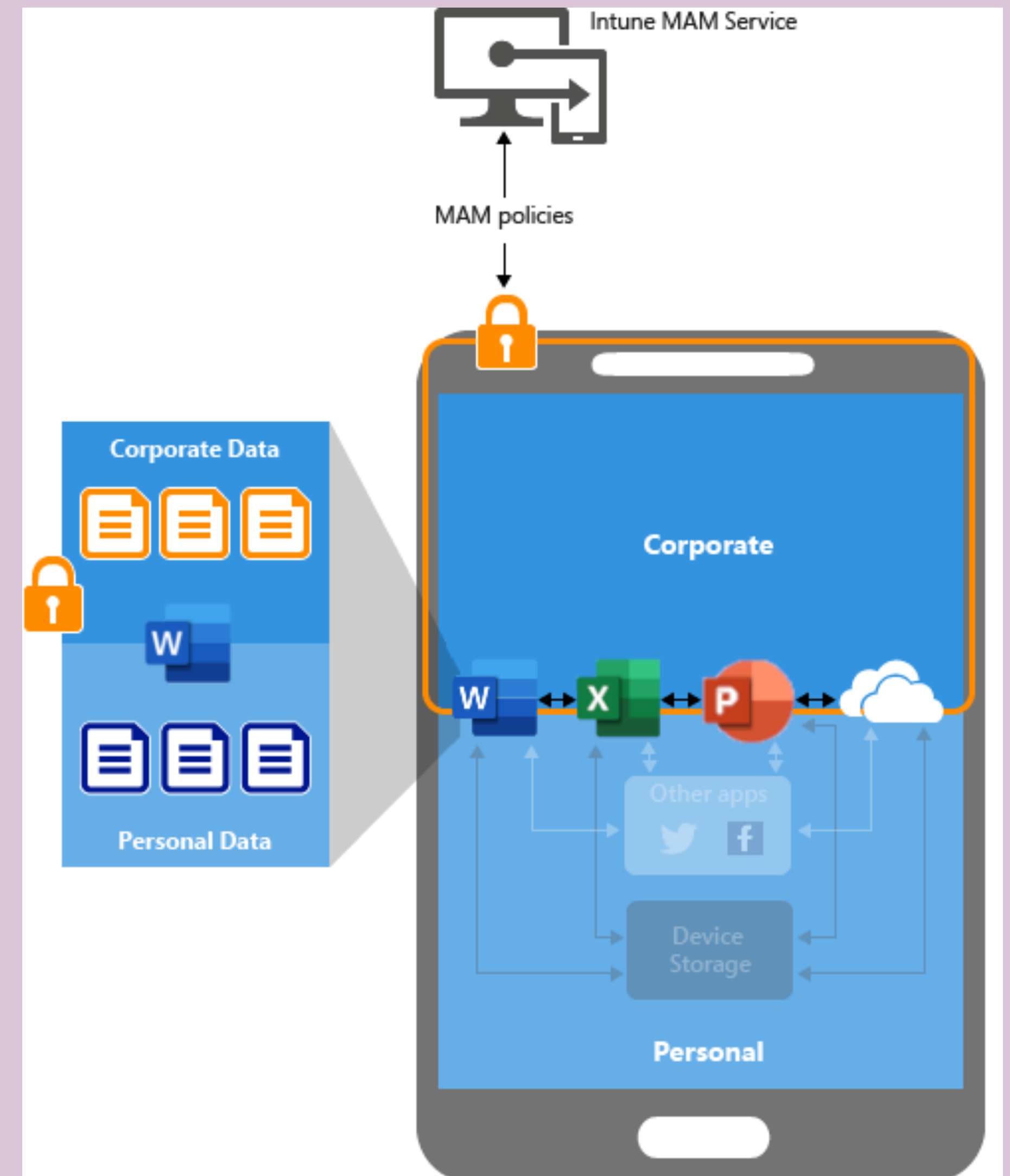
App Org Data Removal 🧽

- **Administrator changes Intune policy to “wipe data”**
- **Only removes organizational accounts**
- **Device is not wiped**
- **App remains installed**



How is this done?

- Org data is protected with Intune app protection policies for O365 apps.
- Policies can be configured for any device — managed or unmanaged.
- Light-touch policies = great results.

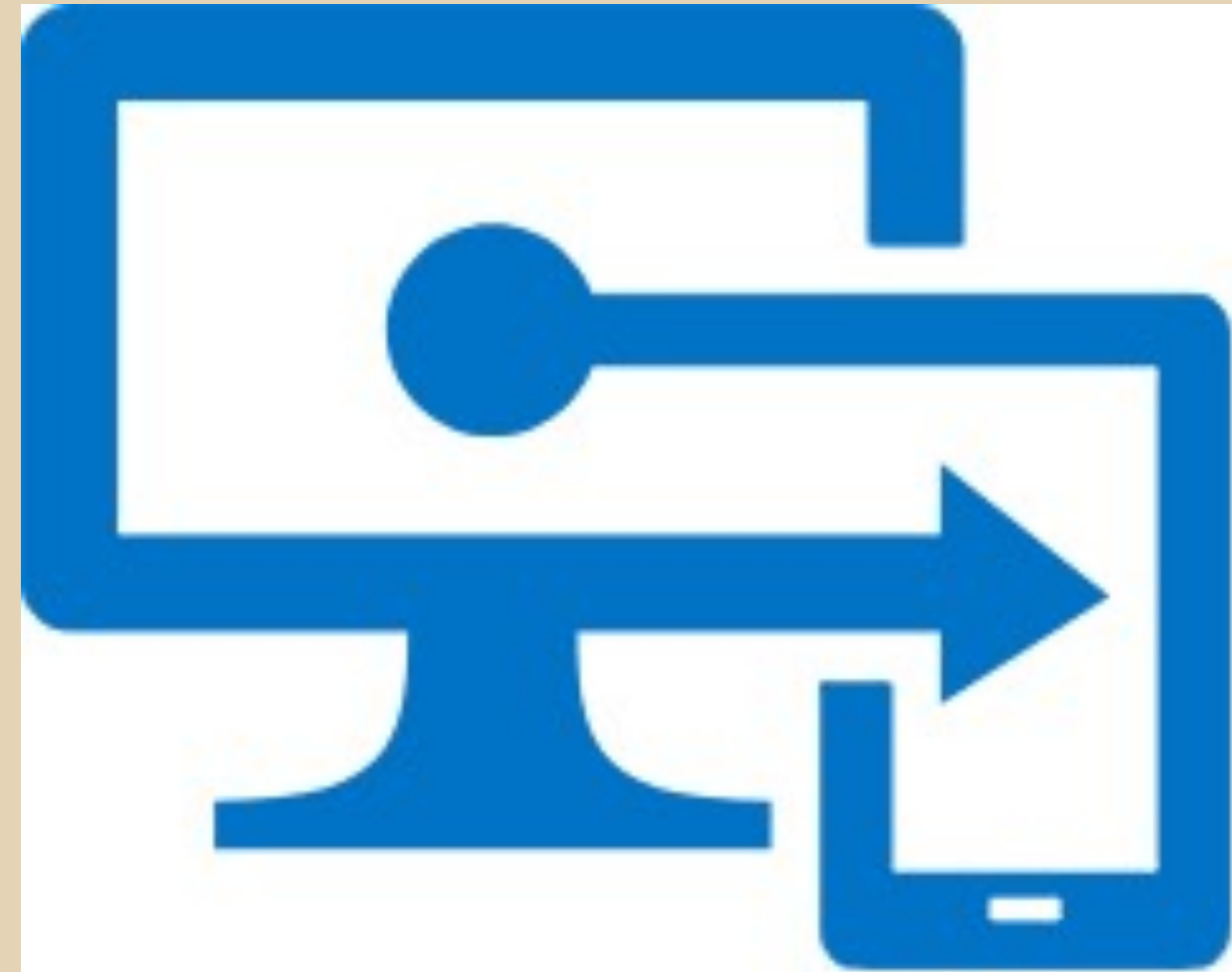


Implementation & Caveats

Implementation: How-To

➤ Requirements:

- Microsoft 365
- E3 or E5 license
- Intune admin account (RBAC)
- Discuss & plan roadmap and desired compliance settings
 - Grace periods, PIN, other settings



Roadmap

1

Plan App Protection Policies

Grace periods, minimum OS

NOTE: MAM cannot detect deferrals!

Don't over-configure; not Conditional Access!

2

Test Scenarios

Run MAM policies on test devices

Observe effect of warn vs. block

Review plan with Cybersecurity

3

Communication Plan

Inform end users

Advise support teams

Write KB articles

4

Deploy to Production

Set up reports

Monitor compliance rates

Raise min. OS as needed


Intune Settings: Conditional Launch


➤ A walkthrough of first-time setup





Apps | App protection policies


Policy

 App protection policies

 App configuration policies

 iOS app provisioning profiles

 S mode supplemental policies

 Policies for Office apps

 Create policy

 Refresh

 Columns








 Export

App protection report: WIP v


Search by policy


Policy	↑↓	Deployed	↑↓	Updated	↑↓	Platform
iOS/iPadOS Warn and Block OS ...		No		7/15/23, 4:39 AM		iOS/iPadOS
iOS MAM Policy Example 01		No		7/15/23, 5:22 PM		iOS/iPadOS


Apps | App protection policies





Policy



 App protection policies


 App configuration policies

 iOS app provisioning profiles

 S mode supplemental policies

 Policies for Office apps



 Create policy 



 Refresh

iOS/iPadOS

Android

Windows Information Protection

 Export  App protection report: WIP v1

	Updated		Platform
	7/15/23, 4:39 AM		iOS/iPadOS
	7/15/23, 5:22 PM		iOS/iPadOS

Apps | App protection policies

1 Basics

2 Apps

3 Data protection

4 Access requirements

5 Conditional launch

6 Assignments

7 Review + create

Name *

Description

Previous

Next

Apps | App protection policies

1 Basics

2 Apps

3 Data protection

4 Access requirements

5 Conditional launch

6 Assignments

7 Review + create

Name *

Nudge for iOS - Warn and Block

Description

This policy will warn users if they are not running the latest version of iOS required by their administrator, and block them from using the apps if their device is too far behind on updates.

Previous

Next

Apps | App protection policies

1 Basics

2 Apps

3 Data protection

4 Access requirements

5 Conditional launch

6 Assignments

7 Review + create

Name *

Nudge for iOS - Warn and Block

Description

This policy will warn users if they are not running the latest version of iOS required by their administrator, and block them from using the apps if their device is too far behind on updates.

Previous

Next

Apps | App protection policies

 Basics

 Apps

 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

Target policy to

Core Microsoft Apps

Selected apps

All Apps

All Microsoft Apps

Core Microsoft Apps

Previous

Next

Apps | App protection policies

 Basics

 Apps

 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

Target policy to


Core Microsoft Apps

Selected apps

All Apps

All Microsoft Apps

Core Microsoft Apps

 We'll continue to add managed apps to your policy as they become available in Intune. [View a list of apps that will be targeted](#)

Previous

Next

Apps | App protection policies


 Basics

Target policy to

Core Microsoft Apps

2 Apps

Selected apps

 We'll continue to add managed apps to your policy as they become available in Intune. [View a list of apps that will be targeted](#)

3

4

5

Conditional launch

6

Assignments

7

Review + create

Core Microsoft Apps


Previous

Next

Apps | App protection policies

 Basics

 Apps

 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

Data Transfer

Backup org data to iTunes and iCloud backups ⓘ

Allow

Block

Send org data to other apps ⓘ

Policy managed apps with OS sharing ✓


Select apps to exempt

Select

Apps | App protection policies

 Basics

 Apps

 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

Data Transfer

Backup org data to iTunes and iCloud backups ⓘ

Allow

Block

Send org data to other apps ⓘ

Policy managed apps with OS sharing



All Apps

None

Policy managed apps


Policy managed apps with OS sharing

Policy managed apps with Open-In/Share fil...

Apps | App protection policies

 Basics

 Apps

 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

Save copies of org data ⓘ

Allow

Block

Allow user to save copies to selected services ⓘ

2 selected


Transfer telecommunication data to ⓘ

Any dialer app

Apps | App protection policies

 Basics

 Apps

 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

☒ OneDrive for Business

☒ SharePoint

☐ Box

☐ Local Storage

☐ Photo Library

2 selected


Transfer telecommunication data to ⓘ

Any dialer app

Apps | App protection policies

 Basics

 Apps


 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

Restrict cut, copy, and paste between other apps 

Policy managed apps with paste in 

Cut and copy character limit for any app

0

Third party keyboards


Allow

Block

Apps | App protection policies

 Basics

 Apps

 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

Encryption

Encrypt org data ⓘ

Require

Not required

Functionality

Sync policy managed app data with native apps or add-ins ⓘ

Allow

Block

Printing org data ⓘ

Allow

Block

Apps | App protection policies

 Basics

 Apps

3 Data protection

4 Access requirements

5 Conditional launch

6 Assignments

7 Review + create

Restrict web content transfer with other apps



Any app



Unmanaged browser protocol 

Org data notifications 

Allow



Previous

Next

Apps | App protection policies

 Basics

 Apps

 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

App PIN when device PIN is set ⓘ

Require

Not required

Work or school account credentials for access ⓘ

Require

Not required

Recheck the access requirements after
(minutes of inactivity) ⓘ

30

Apps | App protection policies

 Basics

 Apps

 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

App PIN when device PIN is set ⓘ

Require

Not required

Work or school account credentials for access ⓘ

Require

Not required

Recheck the access requirements (minutes of inactivity) ⓘ

30

If the policy-managed app is inactive for longer than the number of minutes of inactivity specified, the app will prompt the access requirements to be rechecked after the app is launched.

Apps | App protection policies

 Basics

 Apps

 Data protection

 Access requirements

 Conditional launch

 Assignments

 Review + create

App conditions

Setting	Value
Max PIN attempts	5
Offline grace period	720
Offline grace period	90

Select one



Apps | App protection policies

- ✓ Basics
- ✓ Apps
- ✓ Data protection
- ✓ Access requirements
- 5** Conditional launch
- 6 Assignments
- 7 Review + create

Setting	Value	Action
Jailbroken/rooted d...		Block access ...
Min OS version	16.5	Block access ...
Min OS version	16.5.1 ✓	Warn ...
Select one		

Apps | App protection policies

- ✓ Basics
- ✓ Apps
- ✓ Data protection
- ✓ Access requirements
- 5 Conditional launch**
- 6 Assignments
- 7 Review + create

Setting	Value	Action
Jailbroken/rooted d...		Block access ...
Min OS version	16.5	Block access ...
Min OS version	16.5.1 ✓	Block access ...
Select one		



Delete

Apps | App protection policies

- ✓ Basics
- ✓ Apps
- ✓ Data protection
- ✓ Access requirements
- 5** Conditional launch
- 6 Assignments
- 7 Review + create

Setting	Value	Action
Max OS version		Select one
<p>The value must not be empty.</p> <p>Format: [Major].[Minor] or [Major].[Minor].[Build] or [Major].[Minor].[Build].[Revision]. For iOS, [Major].[Minor].[Build].[Revision]. [RapidSecurityResponse] is also supported.</p> <p>Note: Apps will not perform wipes for RapidSecurityResponse violations, only block or warn is supported.</p> <p>Example: 1.5 or 1.5.50 or 1.5.50.101 or (for iOS) 1.5.50.101.a</p>		

Apps | App protection policies

- ✓ Basics
- ✓ Apps
- ✓ Data protection
- ✓ Access requirements
- 5** Conditional launch
- 6 Assignments
- 7 Review + create

Setting	Value	Action
Max OS version		Select one
<p>The value must not be empty.</p> <p>Format: [Major].[Minor] or [Major].[Minor].[Build] or [Major].[Minor].[Build].[Revision]. For iOS, [Major].[Minor].[Build].[Revision]. <u>[RapidSecurityResponse]</u> is also supported.</p> <p>Note: Apps will not perform wipes for RapidSecurityResponse violations, only block or warn is supported.</p> <p>Example: 1.5 or 1.5.50 or 1.5.50.101 or (for iOS) 1.5.50.101.a</p>		

Apps | App protection policies

- ✓ Basics
- ✓ Apps
- ✓ Data protection
- ✓ Access requirements
- ✓ Conditional launch

6 Assignments

7 Review + create

Included groups

 Add groups

Groups

No groups selected

Excluded groups

 Add groups

Groups

No groups selected

Apps | App protection policies

- ✓ Basics
- ✓ Apps
- ✓ Data protection
- ✓ Access requirements
- ✓ Conditional launch
- ✓ Assignments
- 7 Review + create

Summary

Basics

Name	iOS MAM Policy Example 01
Description	--
Platform	iOS/iPadOS

Apps

Target to apps on all device types	Yes
Device types	--
Public apps	Core Microsoft Apps
Custom apps	--

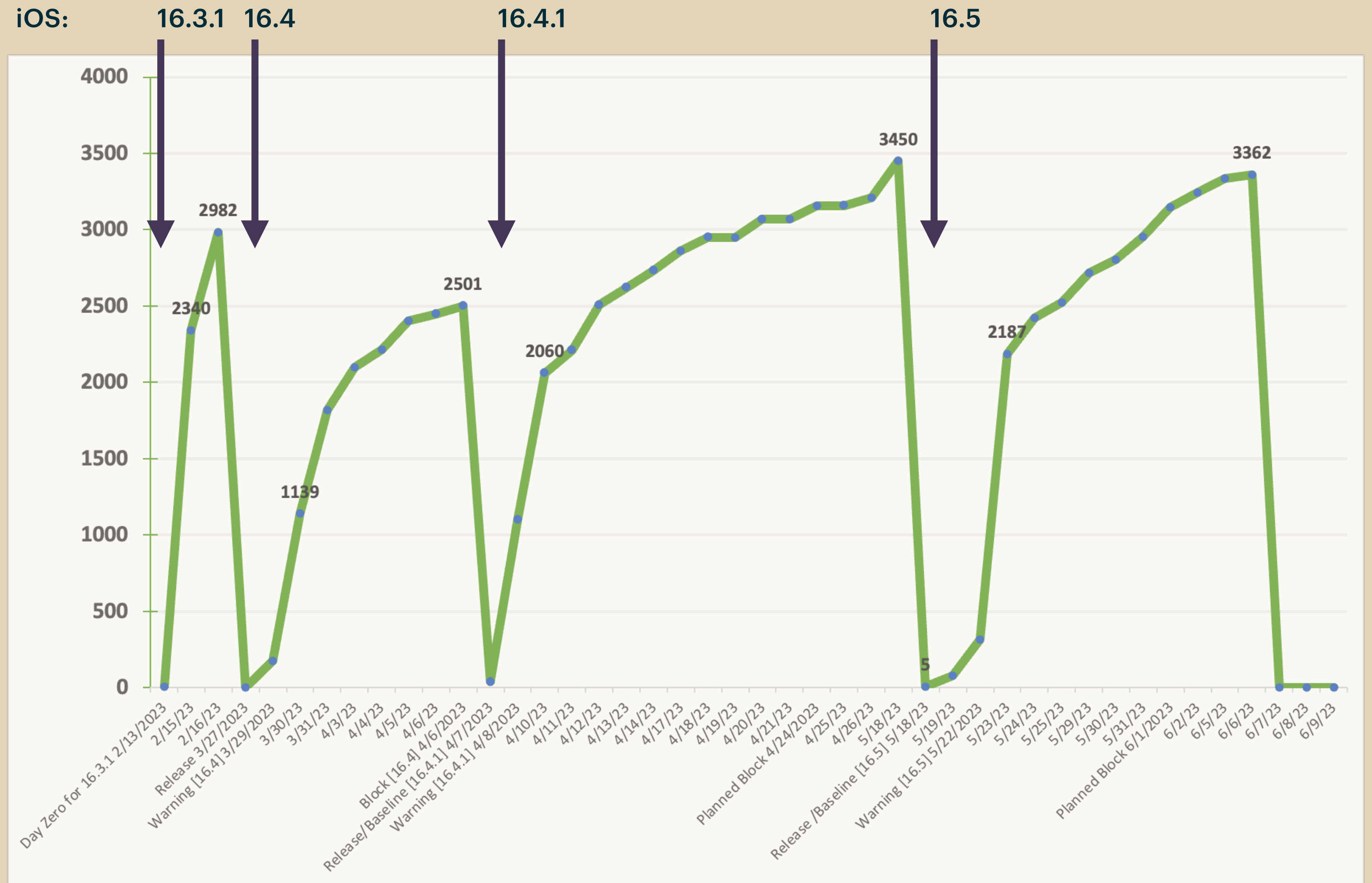
Data protection

Prevent backups	Allow
Send org data to other apps	All Apps
Select apps to exempt	Default: skype;app-settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services;
Select universal links to exempt	http://facetime.apple.com http://maps.apple.com https://facetime.apple.com https://maps.apple.com
Select managed universal links	http://*.appsplatform.us/* http://*.onedrive.com/*

Effect of Intune Warn & Block Notifications

- Graph shows iOS version installed across Managed fleet
- WARN: shown one day after release
- BLOCK: 10 calendar days after WARN.

Device Version - Saturation Report



Compliance Gap:

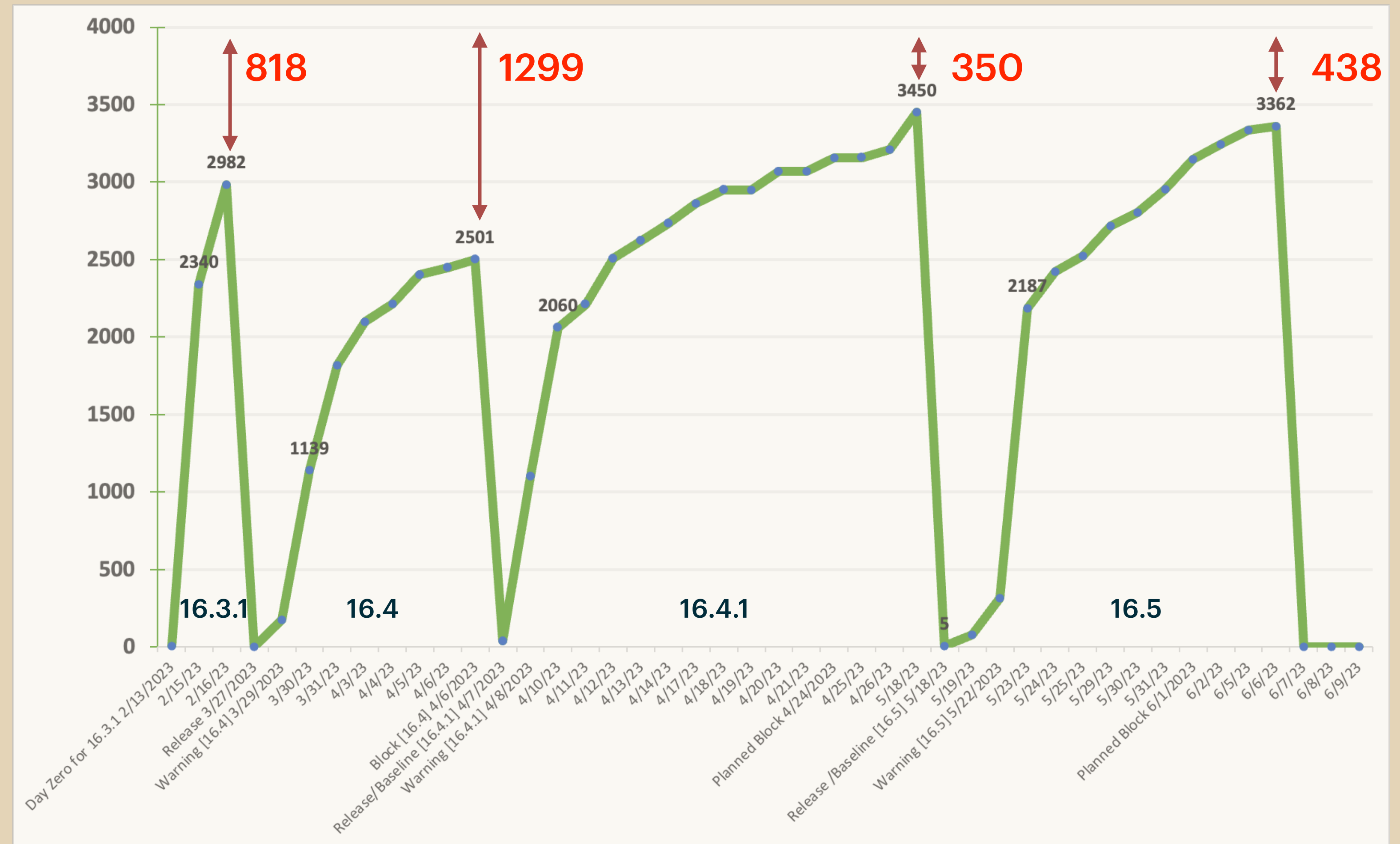
Mail.app users

- Average gap = 500 devices
- ActiveSync still managed by MDM, which prompts users for credentials.

Devices Patched vs. Fleet Total

Red arrows = Mail.app users

iOS:



The last mile...

- **Native Apple apps (Mail, Calendar, Contacts, etc.) do not leverage Intune's SDK.**
- **Block configuration of your org's accounts on native apps**



The last mile...

- **Native Apple apps (Mail, Calendar, Contacts, etc.) do not leverage Intune's SDK.**
- **Block configuration of your org's accounts on native apps**
- **Use Microsoft Device Compliance for BYOD**
- **Dependancies typically lay outside of Apple SMEs area of responsibility.**



Getting to 100%



- **How can Apple help us?**
 - **Forced Software Updates should be a last resort.**
 - **Apple Device Admins need options.**
 - **Provide an MDM method to display notifications similar to Microsoft.**
 - **Messaging about why Organization accounts can't be set up in Mail.**
- **Give us lots of options to support widest range of Apple devices.**
- **File Feedback**

Resources & Special Thanks

➤ Links:

- [Acing Enrollment Panel](#)
- [We could be heroes: Empowering SMEs in media production environments | JNUC 2021](#)
- [2022 Campfire Session Week 5.1: The 7 Habits of Highly Effective Feedback](#)
- [AppleSeed for IT: macOS Testing Template](#)
- [Apple security releases KB HT201222](#)

➤ Resources:

- [Apps you can manage with app protection policies](#)
- [Data Protection with app for devices without enrollment](#)
- [Multi Identity](#)

➤ Special Thanks:

- Erik Gomez <https://github.com/erikng>
- @essbee on MacAdmins Slack
- Brad T Chapman <https://github.com/bradtchapman>

THANK YOU!

github.com/WFHSam/psumac2023

