jumpcloud™

Software Update

The Missing Manual

Tom Bridge, JumpCloud

jumpcloud™

Software Update

discoveryd (2): Electric Bugaloo

Tom Bridge, JumpCloud

jumpcloud™

Software Update

Threat Or Menace?

Tom Bridge, JumpCloud

jumpcloud™

Software Update

A Guide to Safe Use

Tom Bridge, JumpCloud

jumpcloud™

Software Update

Where We're Going, Where We've Been

Tom Bridge, JumpCloud

How Do Macs Update in 2023?

Key Resource: Platform Deployment Guide

Key Resource: Platform Security Guide

Key Vocabulary

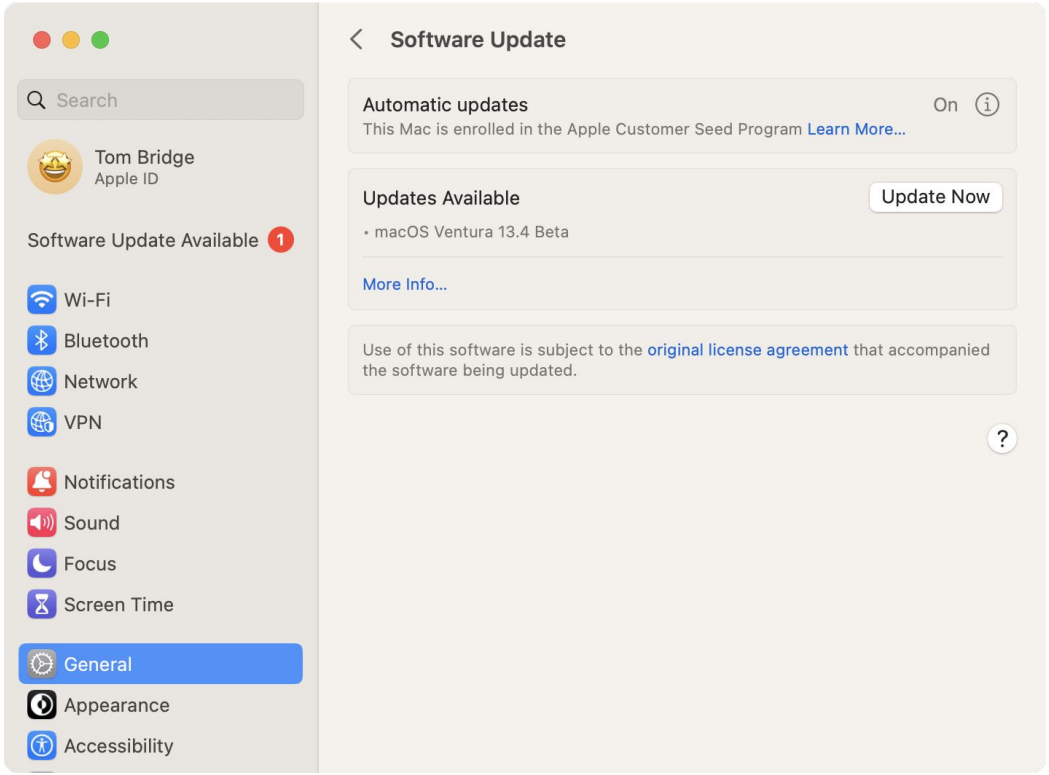
Update: A minor release of macOS - from 13.2.1 to 13.3

Upgrade: A major release of macOS - From 12.x to 13.x

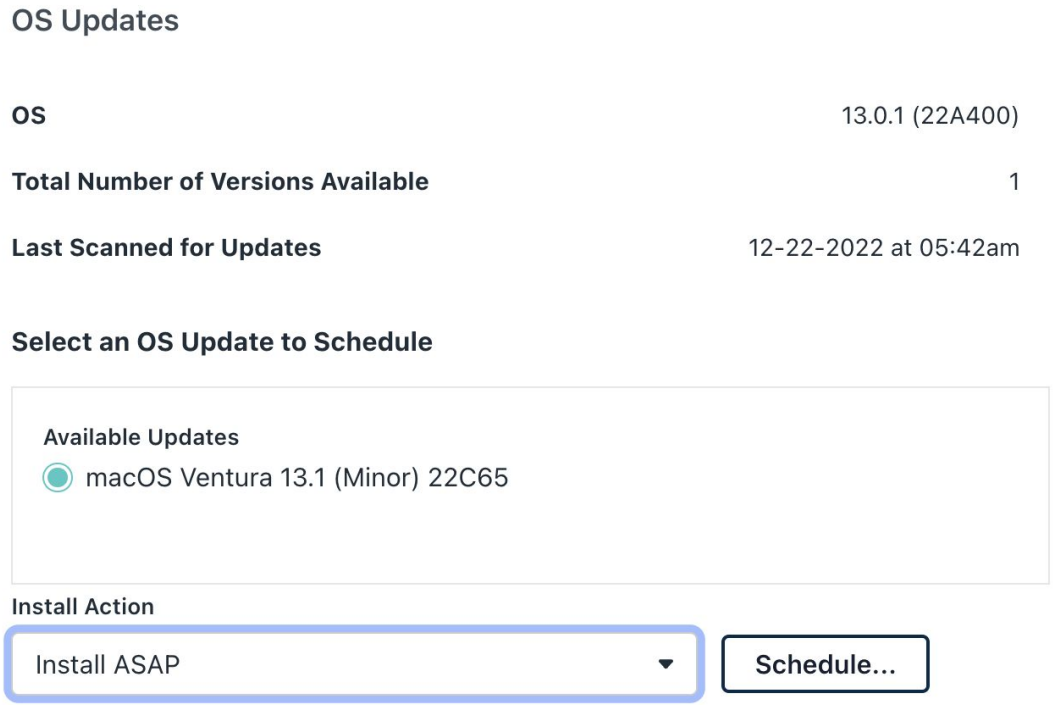
Over the Air (OTA) Update: An update that does not require the entire monolithic installer for macOS. New in macOS 12.3 and later. Specific data necessary to go from current version to the newest version.

Universal Mac Assistant (UMA): An app-driven update to the operating system.

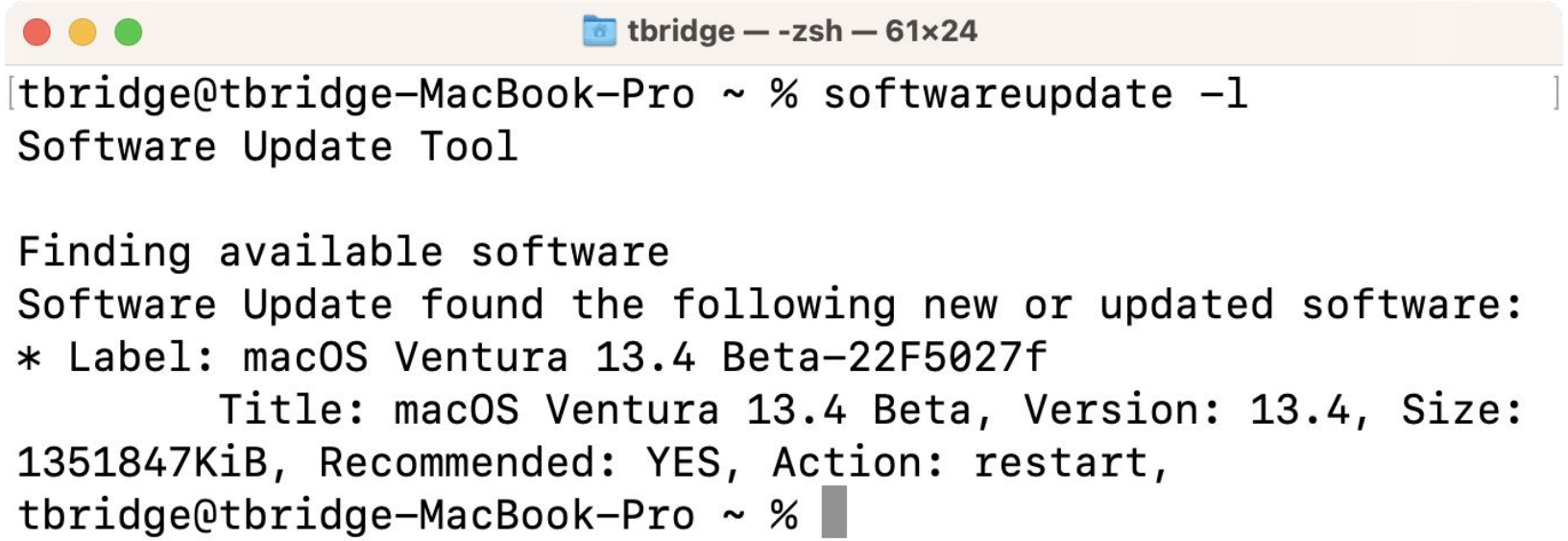
The Update Process - System Settings



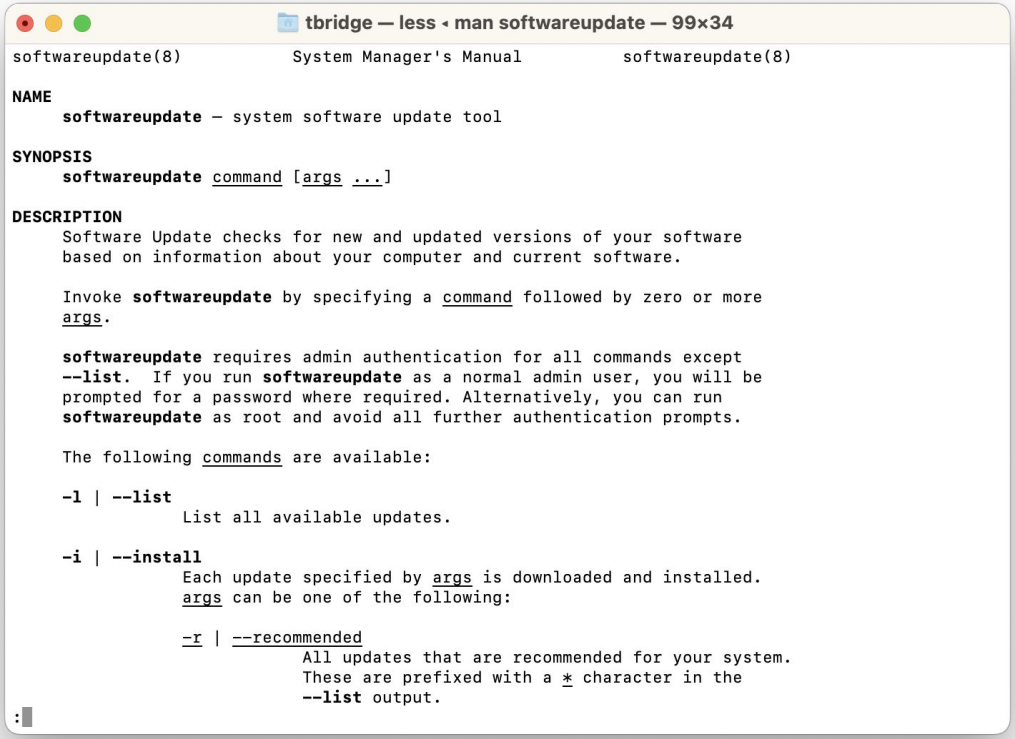
The Update Process - Via MDM



The Update Process - Via Terminal



The Update Process - Via Terminal



jumpcloud™

So you have the bits…

Now what?

The Update Process - Personalization

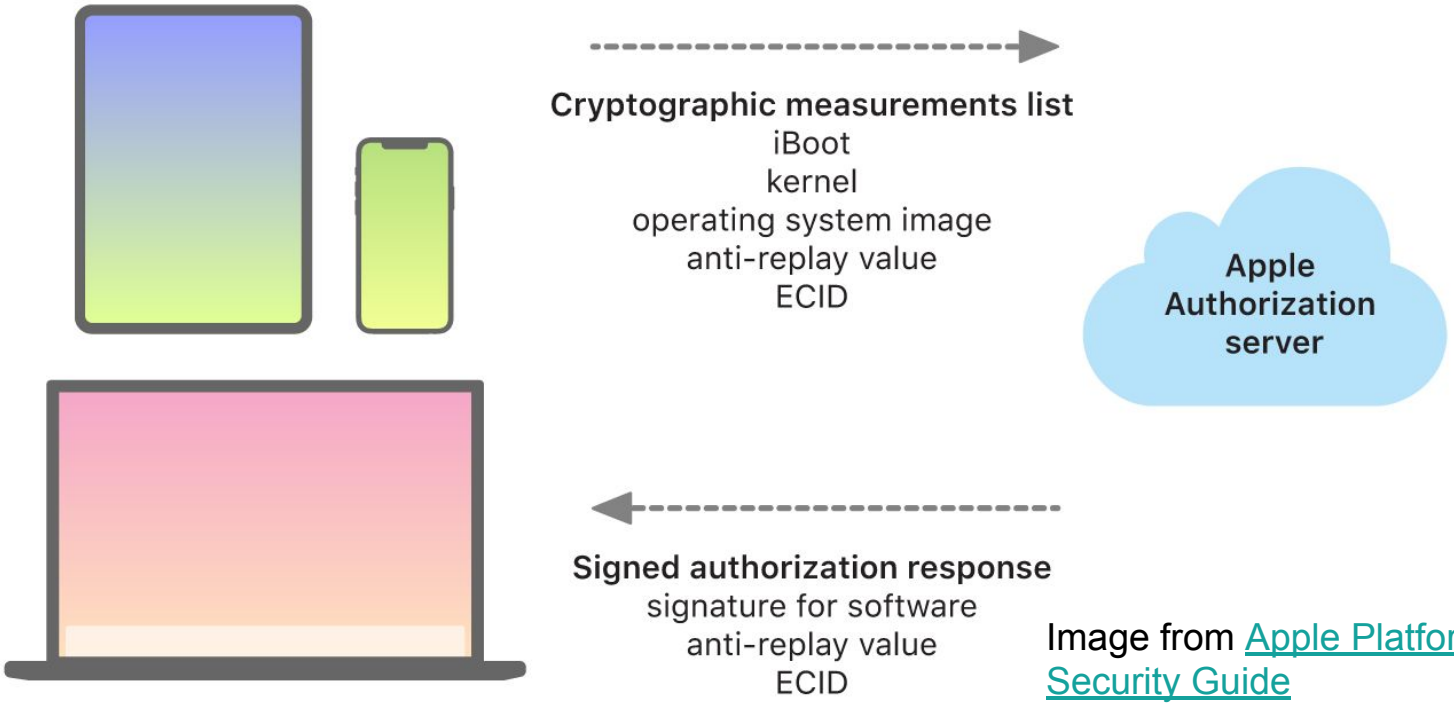


Image from Apple Platform Security Guide

Traffic to and from Apple

- Don’t Attempt to Inspect SSL/TLS Traffic to/from Apple
- Don’t Block Outbound Connections to Apple
- If You Have A Proxy, Skip It for Apple Traffic
- Content Caching is Fine! Reposado Isn’t, Anymore

Knowledge Base Article HT210060: Use Apple Products on Enterprise Networks

A Brief Interlude on History

Software Updates In Recent Apple History

The Past Is Prologue

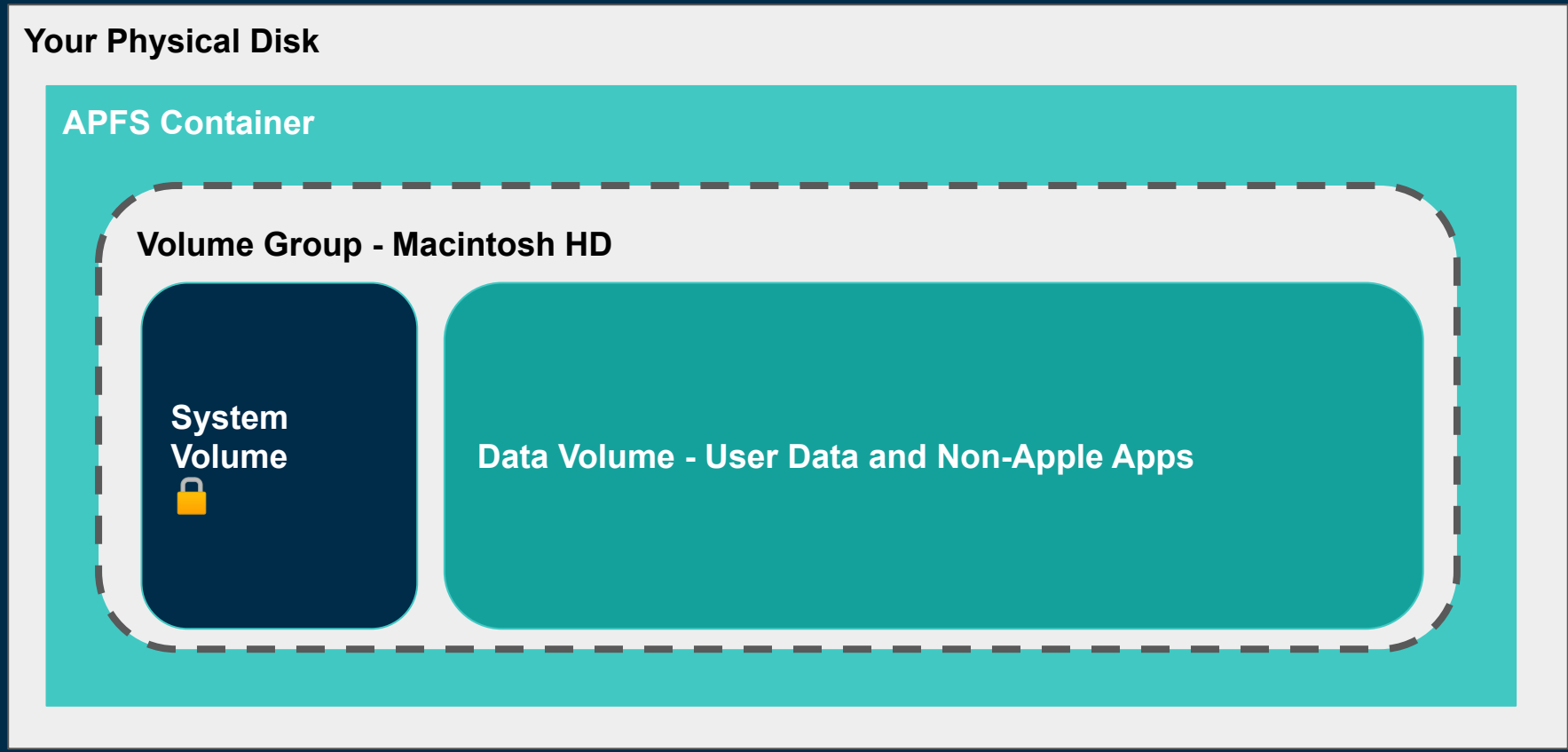
- El Capitan (OS X 10.11) introduces System Integrity Protection (SIP)
- Some directories on disk are read-only without special permissions granted only to Apple

The Past Is Prologue

- Sierra (OS X 10.12) introduces APFS, first for solid state drives
- APFS has a number of improvements over the previous HFS+ filesystem

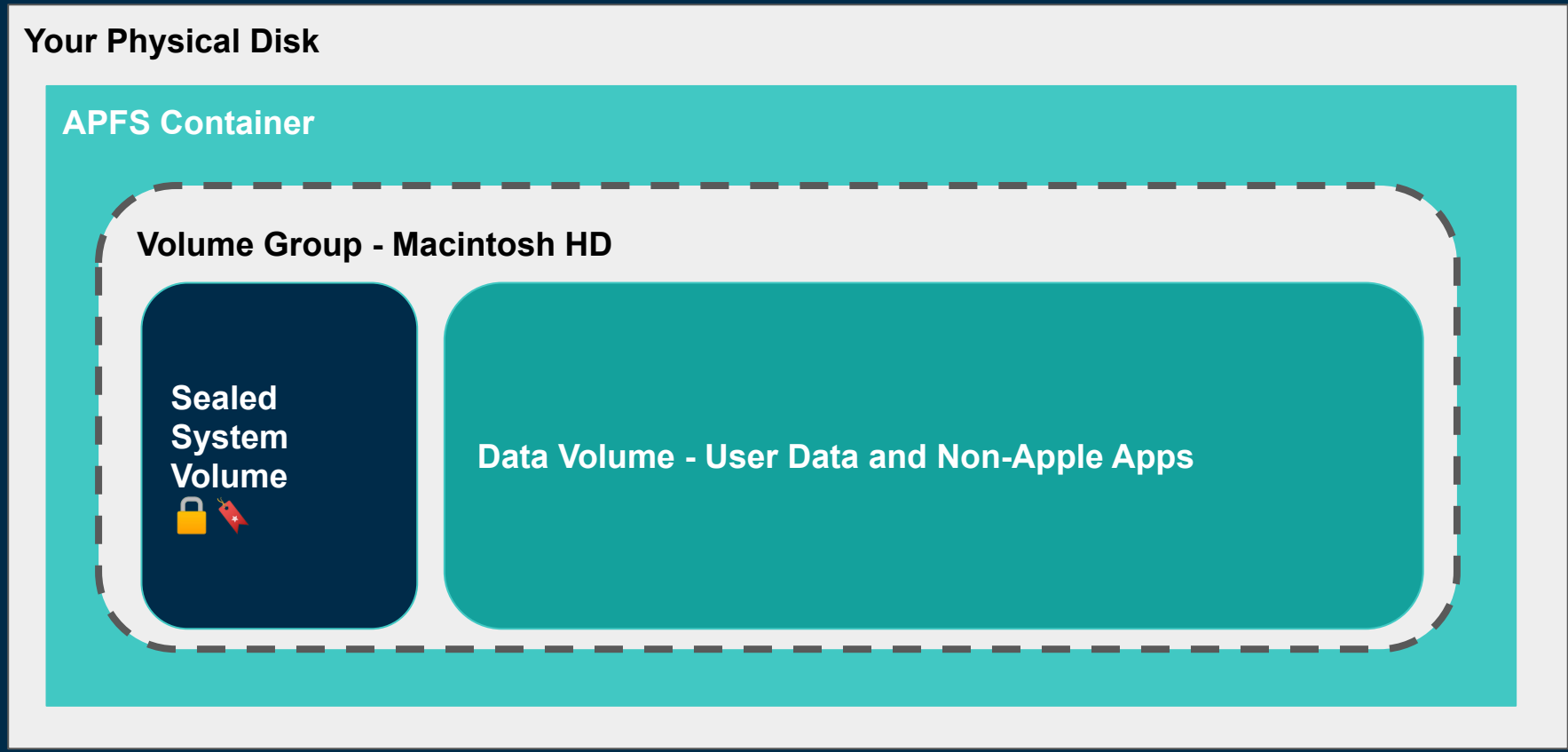
The Past Is Prologue

- Catalina (macOS 10.15) creates an APFS Volume Group and moves the System to a read-only volume.
- Can technically be mounted read-write and changed, but shouldn’t be.
- Software Catalogs are Formally Deprecated.


Your Physical Disk
APFS Container
Volume Group - Macintosh HD
System Volume
Data Volume - User Data and Non-Apple Apps

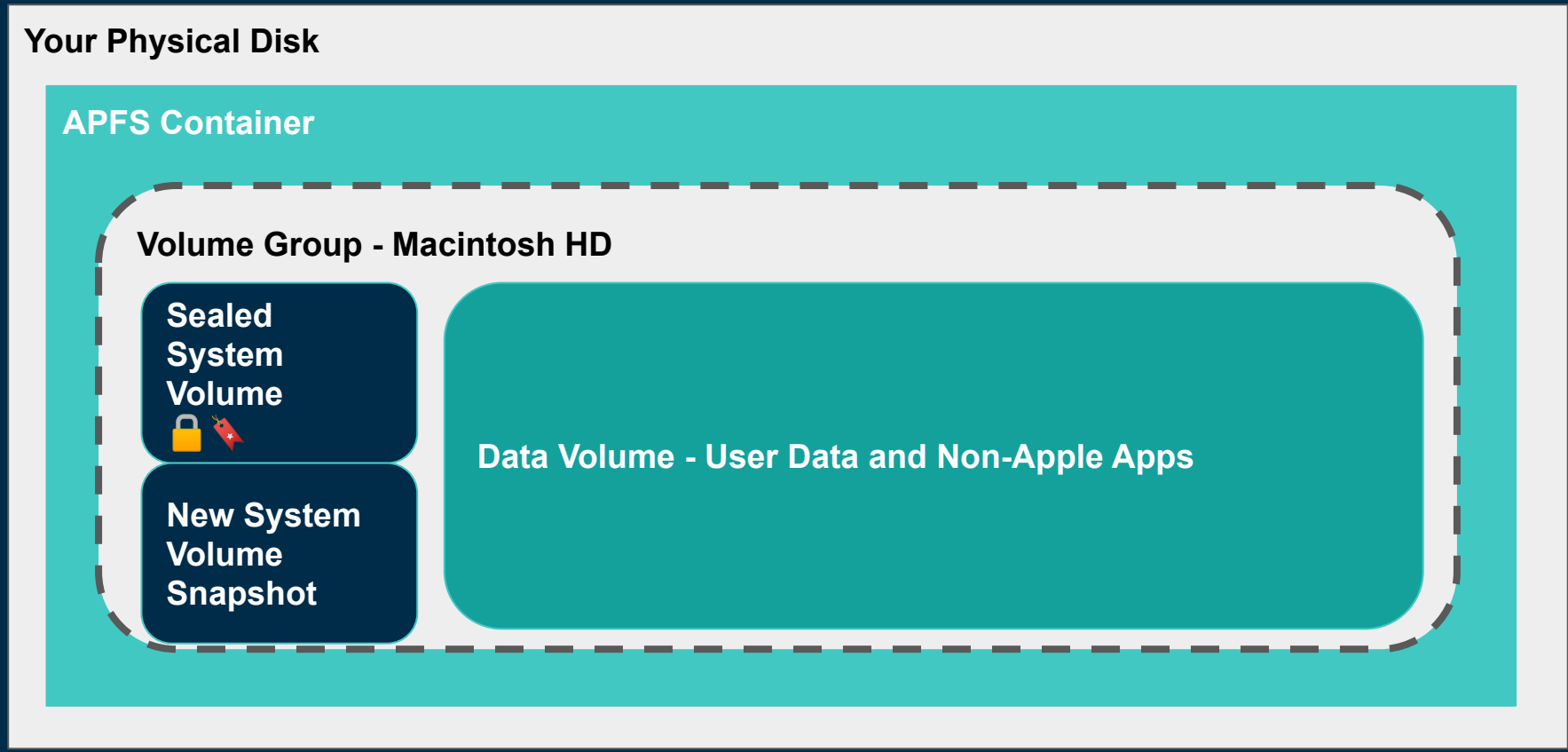
The Past Is Prologue

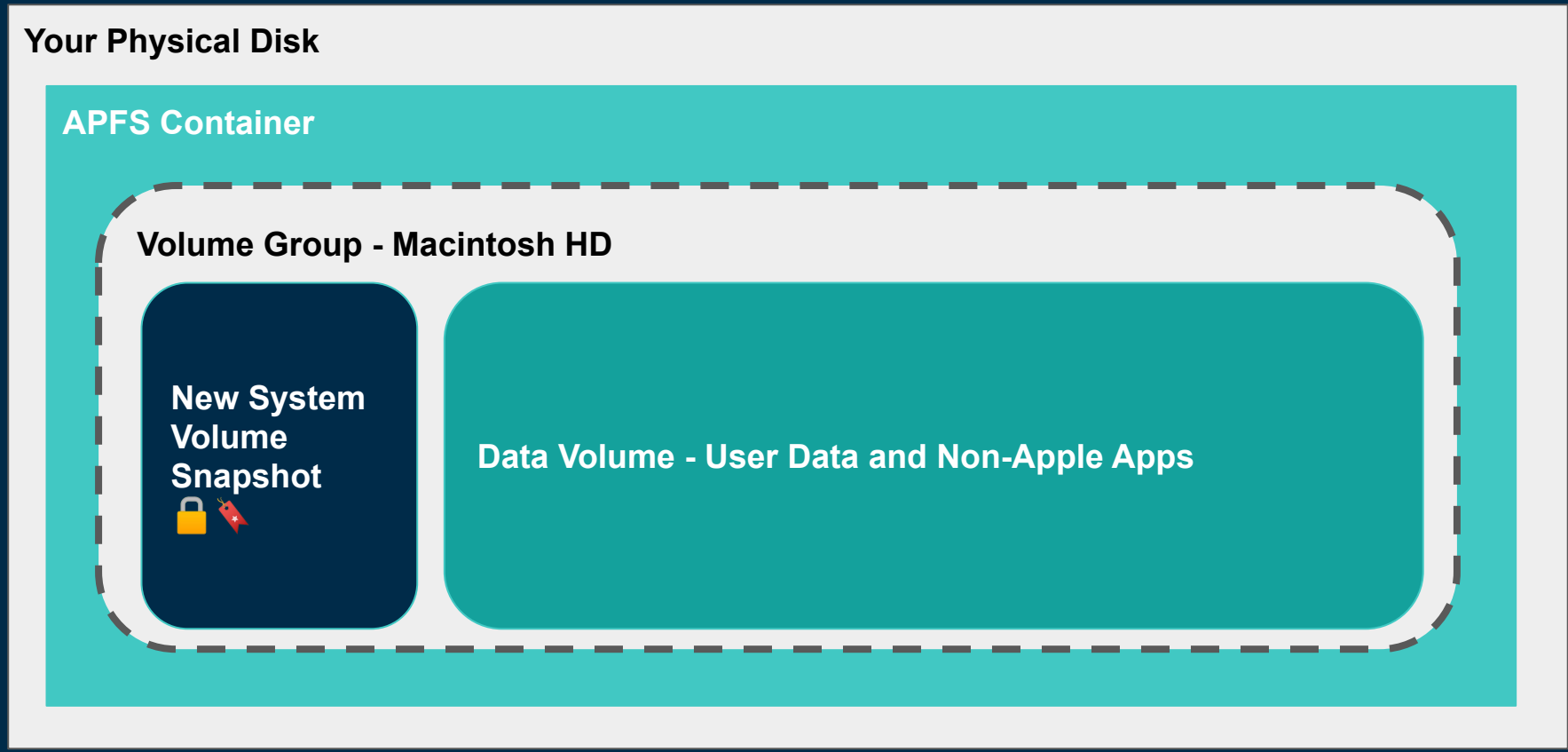
- Big Sur (macOS 11) locks down that System Volume with a cryptographic seal.
- Booting is now accomplished by mounting a snapshot of that APFS volume.


Your Physical Disk
APFS Container
Volume Group - Macintosh HD
Sealed System Volume
Data Volume - User Data and Non-Apple Apps

Okay, but Updates?

Right. Stay on topic, Thomas.


Your Physical Disk
APFS Container
Volume Group - Macintosh HD
Sealed System Volume
New System Volume Snapshot
Data Volume - User Data and Non-Apple Apps

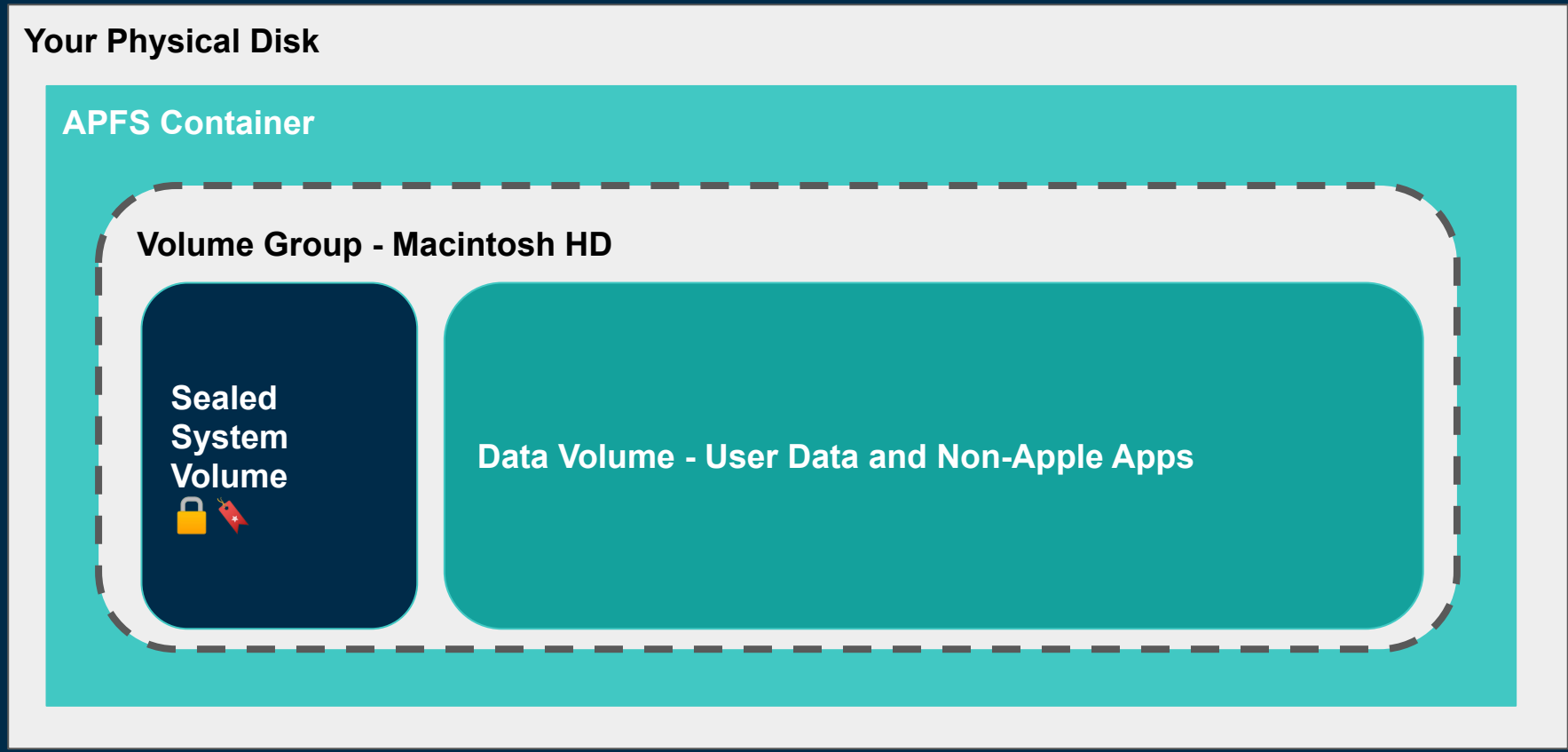

Your Physical Disk
APFS Container
Volume Group - Macintosh HD
New System Volume Snapshot
Data Volume - User Data and Non-Apple Apps

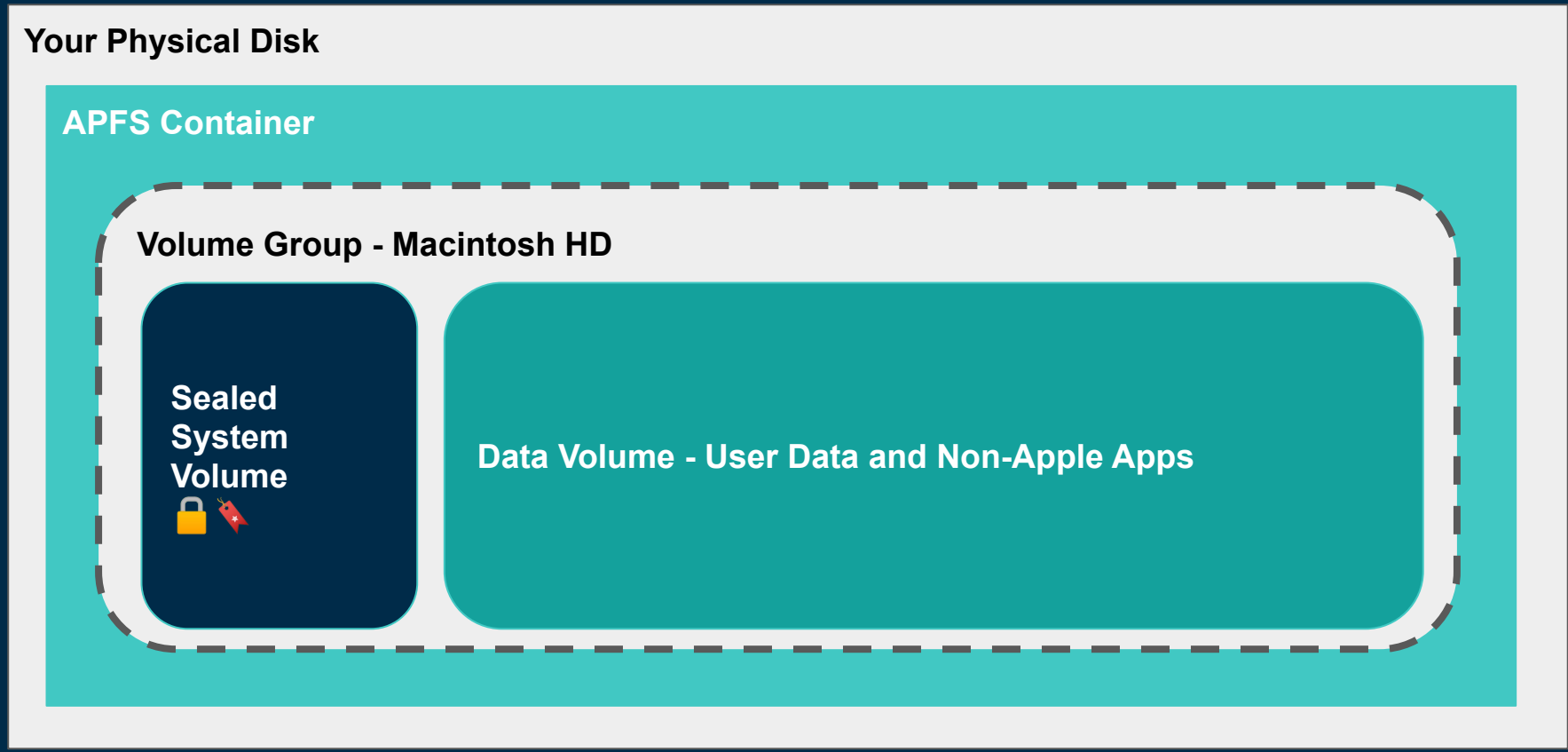
Wait, There's More

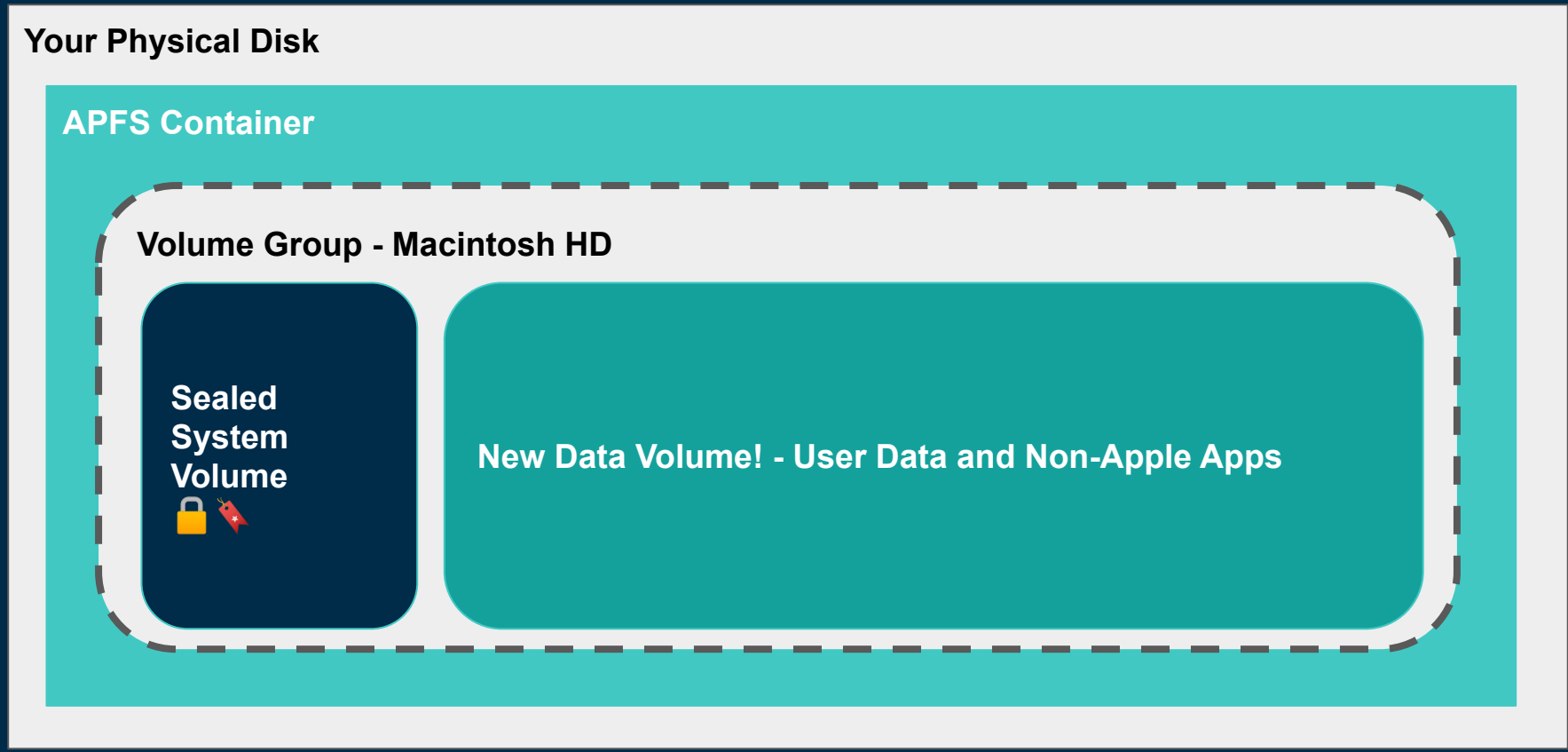
Software Update is also about Hardware!

A Note on Erase All Contents & Settings

macOS 12’s Single Best Feature


Your Physical Disk
APFS Container
Volume Group - Macintosh HD
Sealed System Volume
Data Volume - User Data and Non-Apple Apps


Your Physical Disk
APFS Container
Volume Group - Macintosh HD
Sealed System Volume
Data Volume - User Data and Non-Apple Apps


Your Physical Disk
APFS Container
Volume Group - Macintosh HD
Sealed System Volume
New Data Volume! - User Data and Non-Apple Apps

Booting macOS

Secure Boot is the underpinning of a secure update process

Intel Macs with T2 chips

T2 Boots First

- Validates the Boot ROM
- Validates Bootloader
- Validates Kernel Cache Signature on file
- Validates UEFI Signature on file
- Loads EFI

Intel Chip Boots Next

- Evaluates boot.efi
- Boot.efi reviews macOS Signature

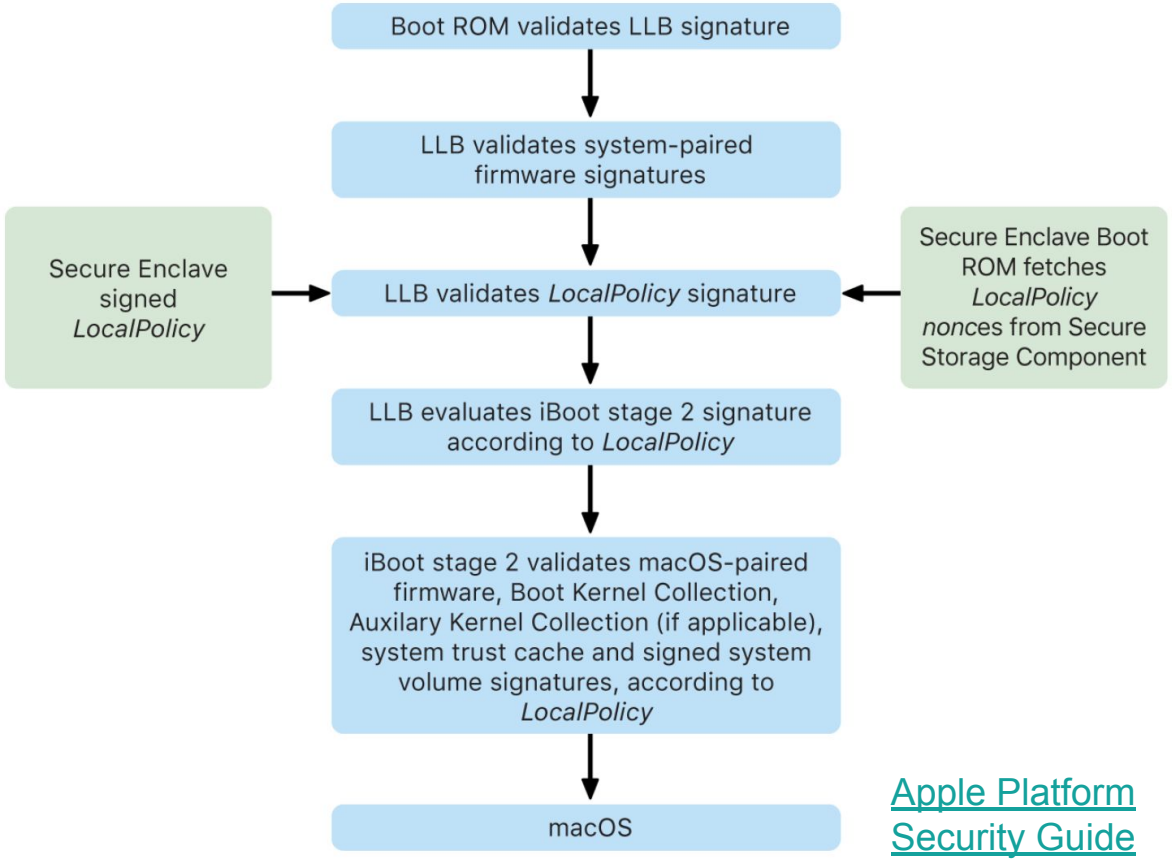
BridgeOS Upgrades on T2 chips

T2 Processors upgrade like other Apple Silicon platforms, through communication with Apple, but occasionally, problems occur with those updates.

Apple Configurator 2 is valuable for **reviving** these devices in the event that something goes wrong that is recoverable.

It can also be used to handle **restoring** things if you need to.

Macs with Apple silicon



[Apple Platform Security Guide]

jumpcloud™

Managing Software Versions

And other lies we tell ourselves

Requirements for Software Update

- You need an MDM to do anything interesting.
- You probably need more than just an MDM.
- Beginning with macOS 14 Sonoma, DDM is very helpful

jumpcloud™

How Do MDM Updates Work?

MDM-Managed Mac

Please do a Scan for OS Updates.

Sure. Why Not.

Your MDM

Tell Me What Updates You Have?

I have this array of available updates.

Please Install This Specific Update In This Way

Yeah, okay, whatever.

jumpcloud™

	Major	Minor
Default	✅	✅
DownloadOnly	✅	✅
InstallASAP	✅	✅
NotifyOnly	✅	✅
InstallLater	❌	✅
InstallForceRestart	✅	✅

Deferrals

Introduced in macOS 12, Deferrals are meant to help admins deploy software updates without direct user involvement.

`MaxUserDeferrals`
`integer`

The maximum number of times the system allows the user to postpone an update before it's installed. The system prompts the user once a day.

This key is only supported when `InstallAction` is `InstallLater` and only supported for minor OS updates (for example, macOS 12.x to 12.y).

`InstallLater` updates happen during system quiet period, which is traditionally 1-5am local time, but is actually influenced by the end user's activity. Generally requires power or a full battery (50%+)

Bootstrap Tokens

- Gathered by your MDM via Command
- Can Unlock the System Volume

```
tbridge@tbridge-MacBook-Pro ~ % diskutil apfs listUsers /
Cryptographic users for disk3s1s1 (4 found)
|
+-- EBC6C064-0000-11AA-AA11-00306543ECAC
|   Type: Personal Recovery User
|   Volume Owner: Yes
|
+-- 2457711A-523C-4604-B75A-F48A571D5036
|   Type: MDM Bootstrap Token External Key
|   Volume Owner: Yes
'
```

- Used by **`InstallLater`** to unlock the system volume during the quiet period.

jumpcloud™

Rapid Security Response

When is an update NOT an update?

What is an RSR update?

- Added to macOS with macOS 13 Ventura
- First update on 1 May 2023
- Updates are styled as 13.3.1 (a) (b) or (n)
- RSR Updates can be removed, by the user
- RSR Update install and removal can be controlled by the admin with an MDM Profile
- JumpCloud Supports Managing RSR Updates with a profile

What is an RSR update?

- Contain special updates for Safari or other Apple apps on iOS or macOS
- Require a reboot to become fully functional
- These updates are very, very fast to install, unlike current updates.
- Based on Cryptex

OS Updates

OS	13.3.1 (22E261)
Total Number of Versions Available	1
Last Scanned for Updates	05-03-2023 at 08:20am

Select an OS Update to Schedule

Available Updates

◯ macOS Security Response (a) 13.3.1 (Minor) 22E772610a

Install Action

Select Install Action ▾ | Schedule...


Manage Rapid Security Response
Allow Rapid Security Response updates
Prevent removal of Rapid Security Response updates

How Should I Think About Rapid Security Response?

These ephemeral updates are for patching the worst flaws.

What is an RSR update?

- **Limited Utility**, but when you need it, you need it.
- **Limited Lifespan**, all updates rolled into the next minor release.
- **Limited Testing**, RSR updates don’t go through the same flow as point release updates.
- **Limited Application**, only applies to non-kernelspace changes

macOS Ventura 13.4.1 (a)

Released July 10, 2023

WebKit

Available for: macOS Ventura 13.4.1

Impact: Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Description: The issue was addressed with improved checks.

CVE-2023-37450: an anonymous researcher

About the security content of Rapid Security Responses for macOS Ventura 13.4.1

jumpcloud™

A Wish List for Software Update Commands

Wish List Items

- Deadlines for install based on Apple release dates.
- Close deferral escape paths.
- Update alerts triggered by MDM should be customizable in time and persistence.
- Install Later should apply to Major Upgrades.
- Takeover the job of Nudge or Super.
- Spot problems that might result in Recovery Mode during the preflight and act appropriately.


WWDC23
Overview
Topics
Sessions
Labs
Activities
Forums
Beyond WWDC

What Changed in Software Update?

"Software Update takes advantage of declarative device management and now allows IT administrators to enforce software updates to specific deadlines with improved user transparency."

– What's New in Managing Apple Devices, 2023

jumpcloud™

How Does DDM Enforcement Work?

Declarative Device Management - Software Update Configurations

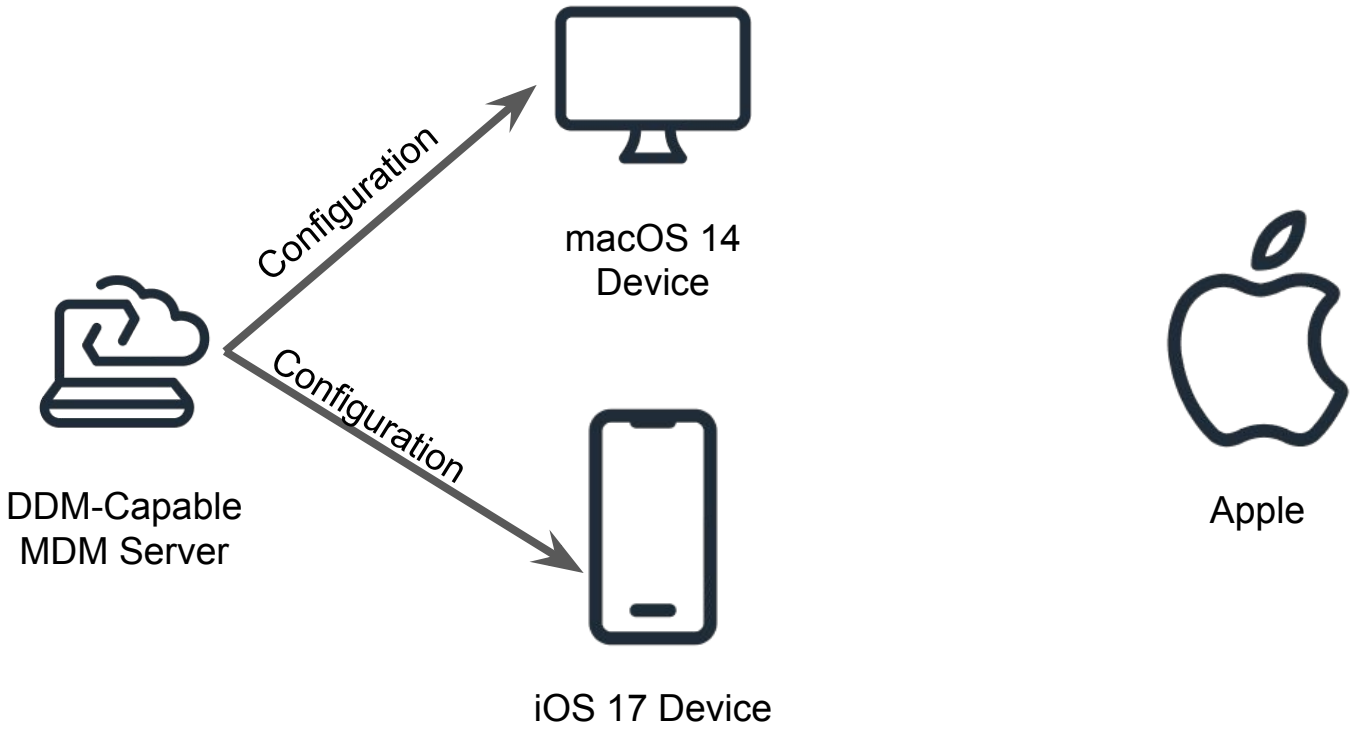
DDM-Capable
MDM Server

macOS 14
Device

iOS 17 Device

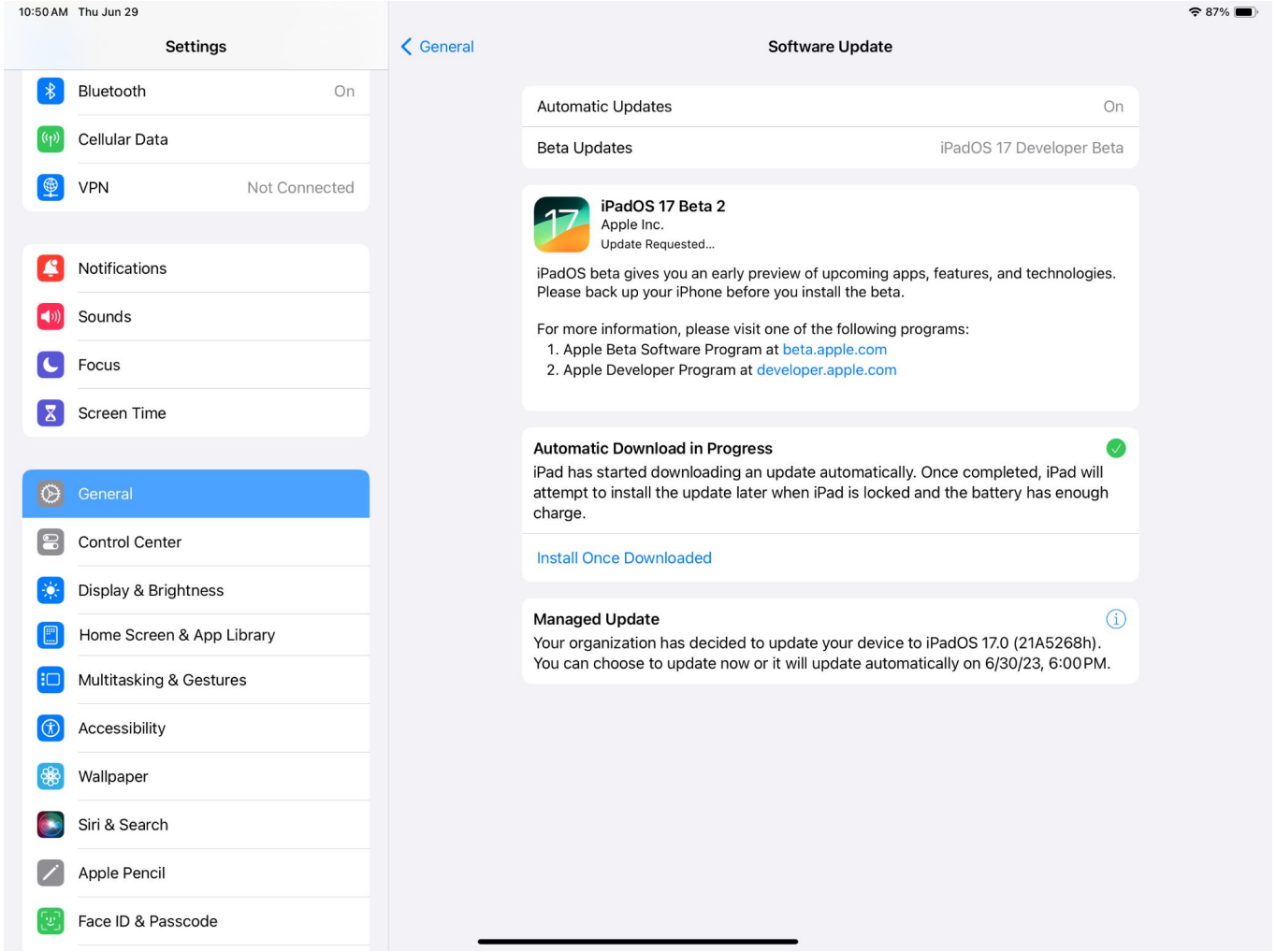
Apple

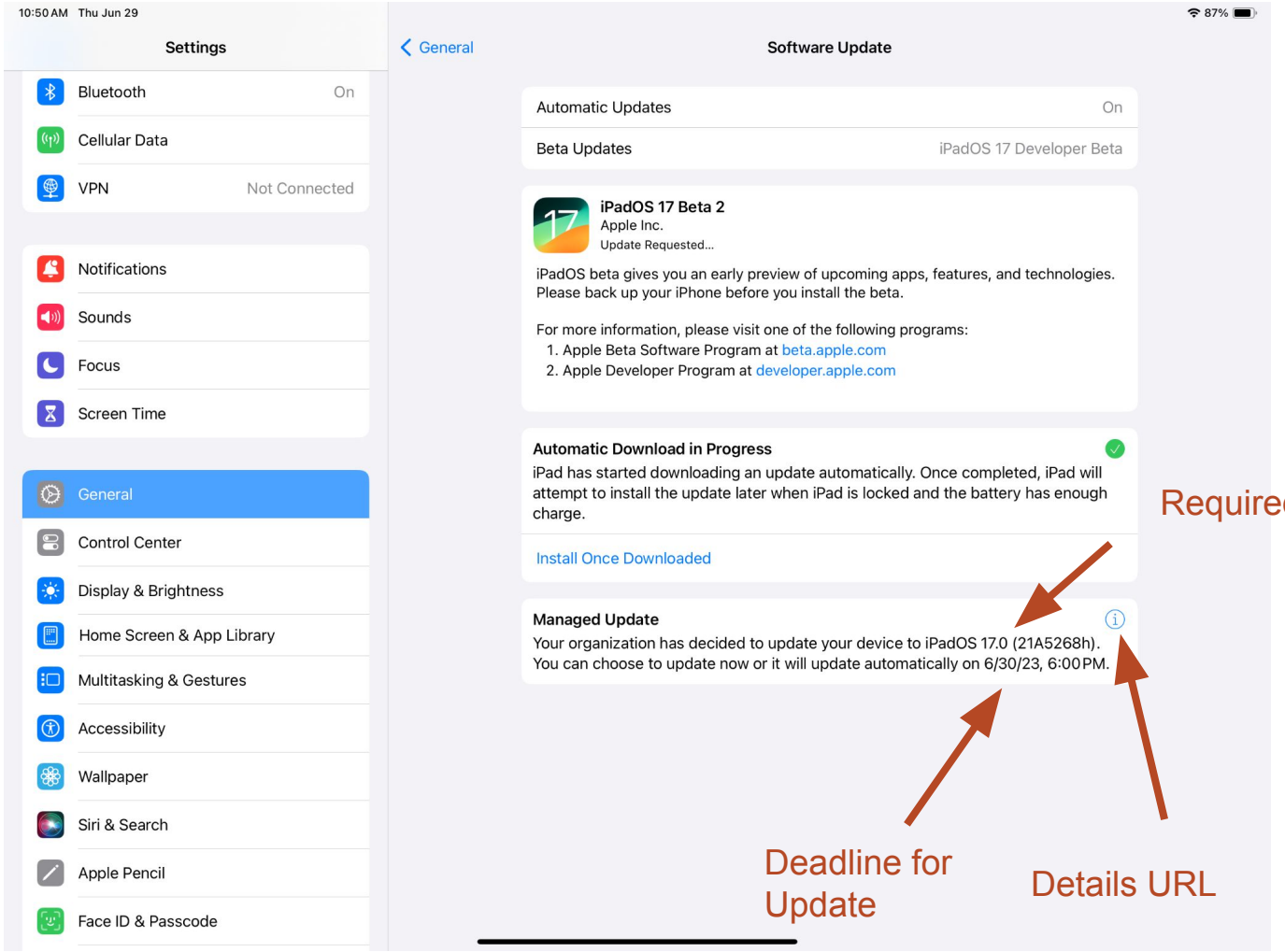
Declarative Device Management - Software Update Configurations



Declarative Device Management - Software Update Configurations

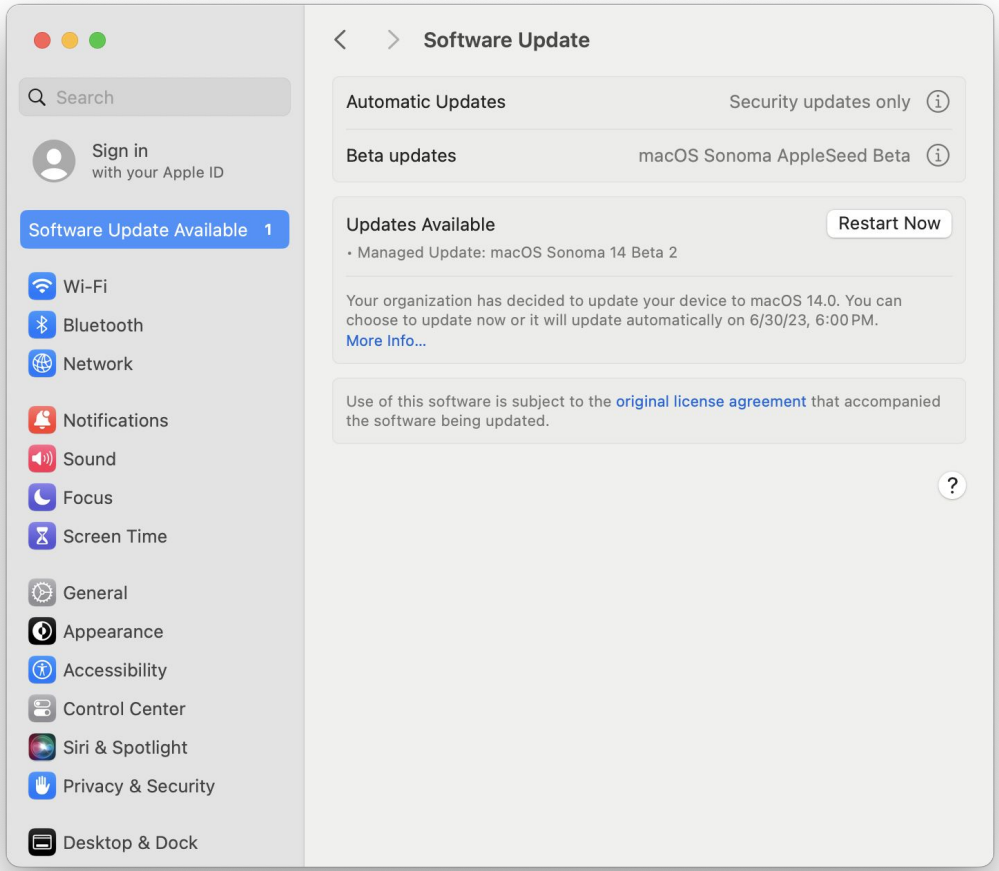
```
{
    "Type":
"com.apple.configuration.softwareupdate.enforcement.specific",
    "Identifier": "tom.ios.enforcement",
    "Payload": {
        "DetailsURL": "https://youtube.com/watch?v=sVdaFQhS86E",
            "TargetLocalDateTime": "2023-06-30T18:00:00",
            "TargetOSVersion": "17.0",
            "TargetBuildVersion": "21A5268h"
    }
}
```

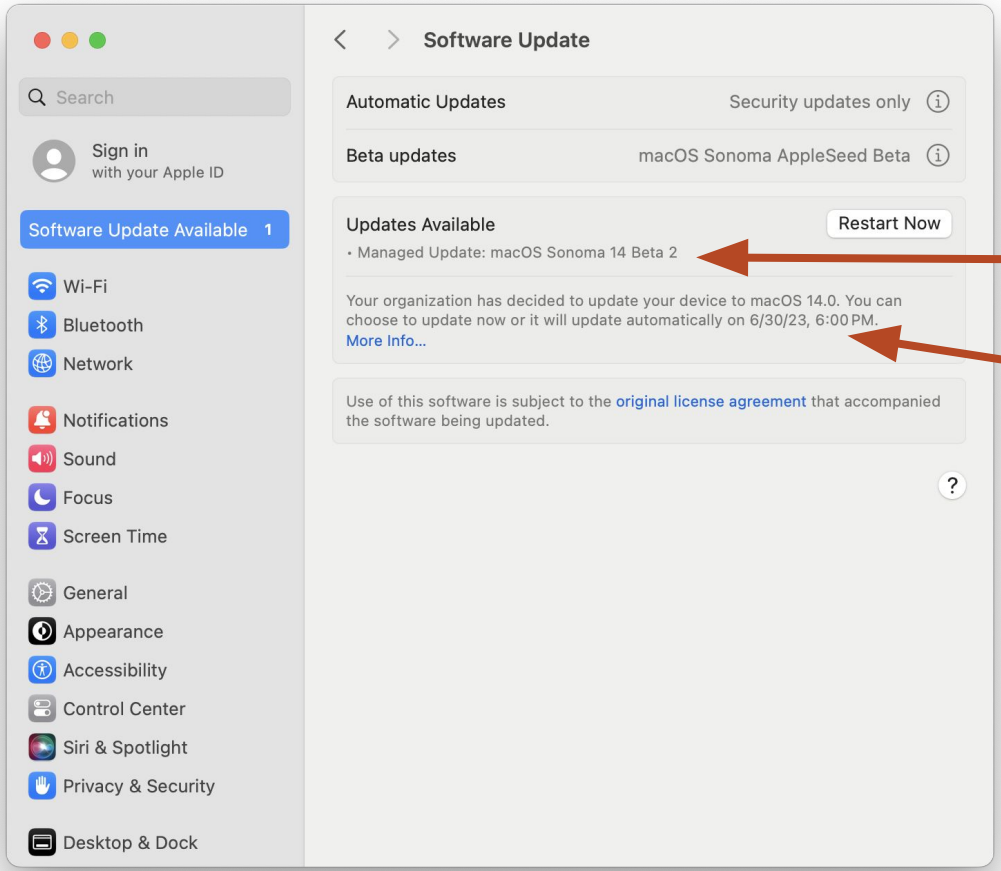


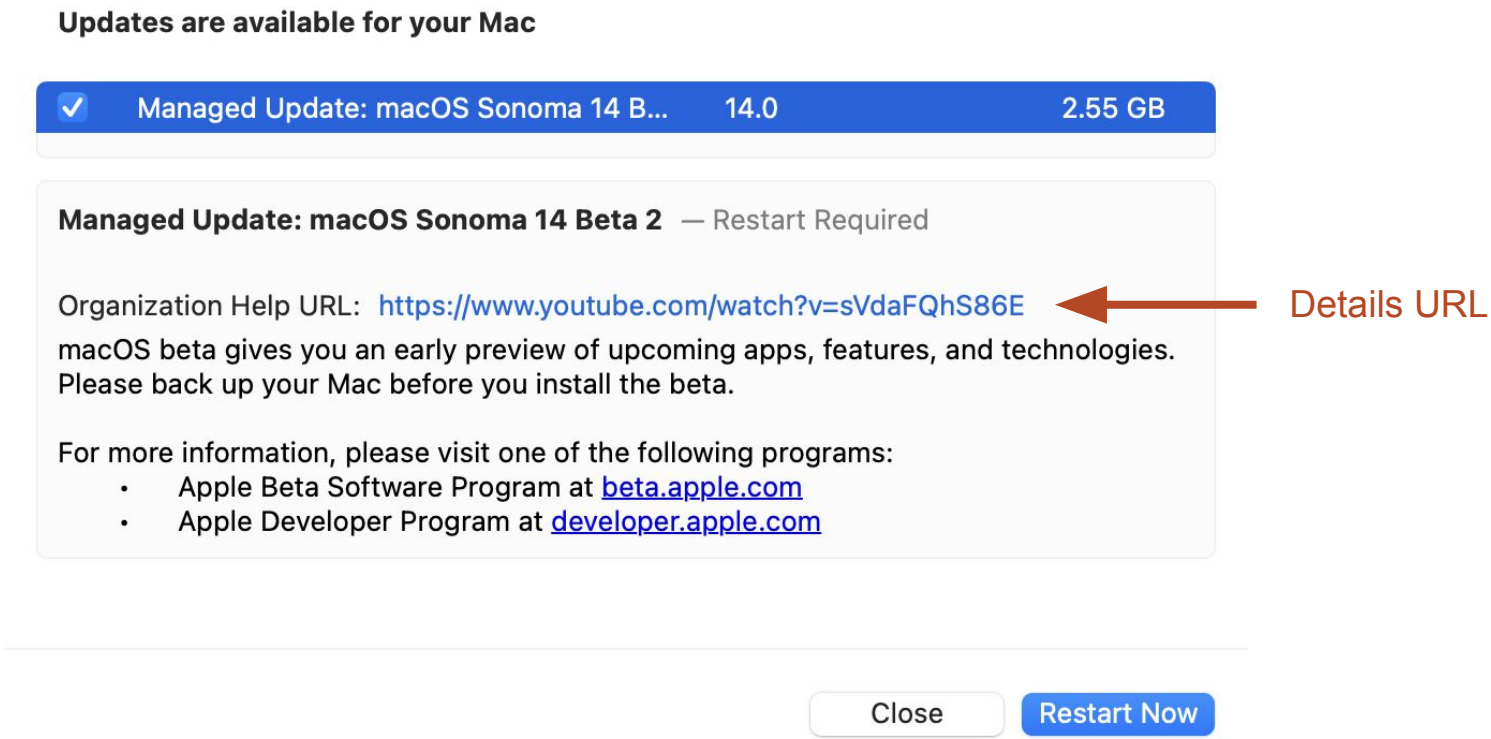


Declarative Device Management - Software Update Configurations

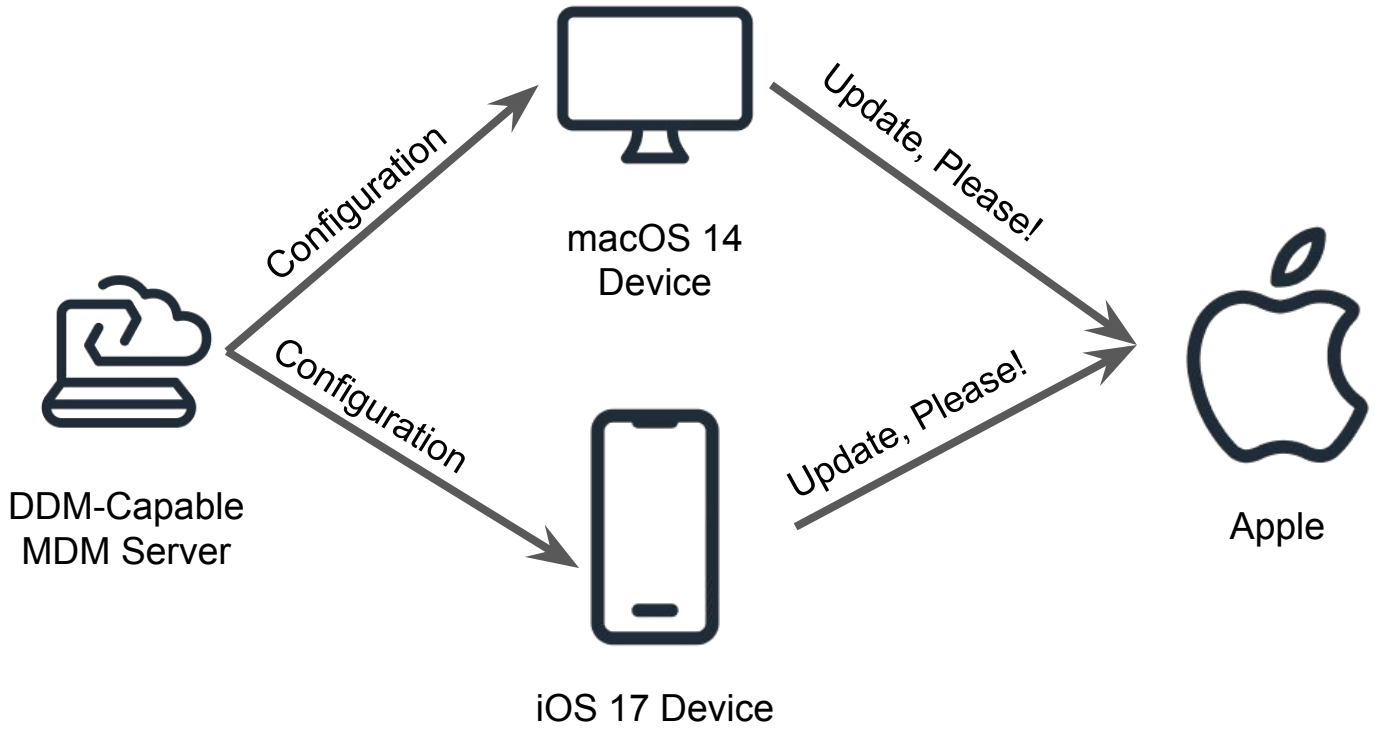
```
{
    "Type":
"com.apple.configuration.softwareupdate.enforcement.specific",
    "Identifier": "tom.beta.enforcement",
    "Payload": {
        "DetailsURL": "https://youtu.be/5IsSpAOD6K8?t=29",
            "TargetLocalDateTime": "2023-06-30T18:00:00",
            "TargetOSVersion": "14.0",
            "TargetBuildVersion": "23A5276g"
    }
}
```







Declarative Device Management - Software Update Configurations



So What Happens When You Ignore The Alerts?

Update available notification

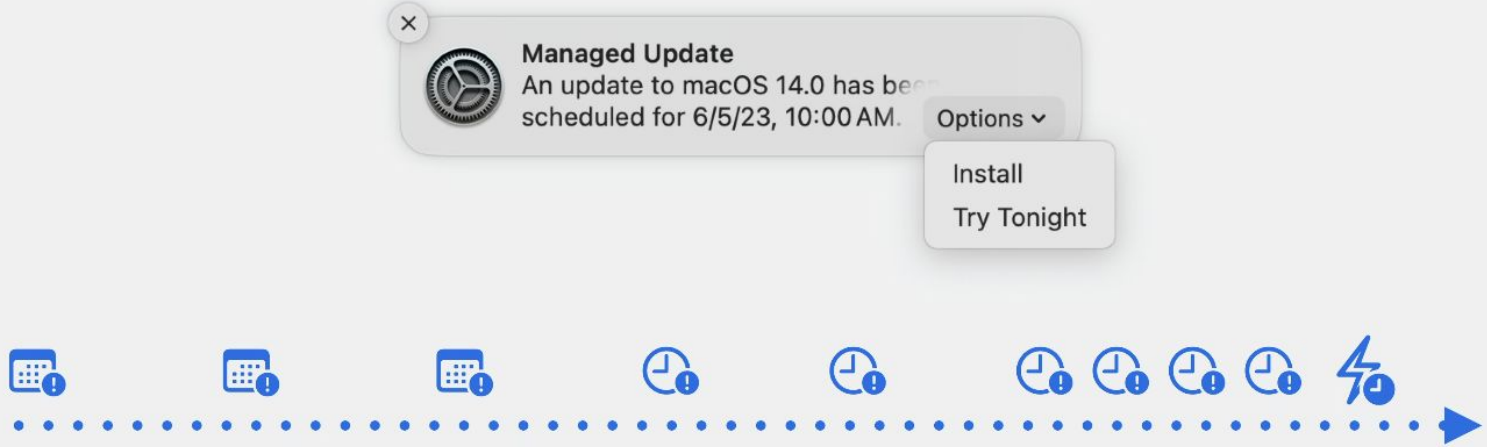


Image from Apple

Update available notification

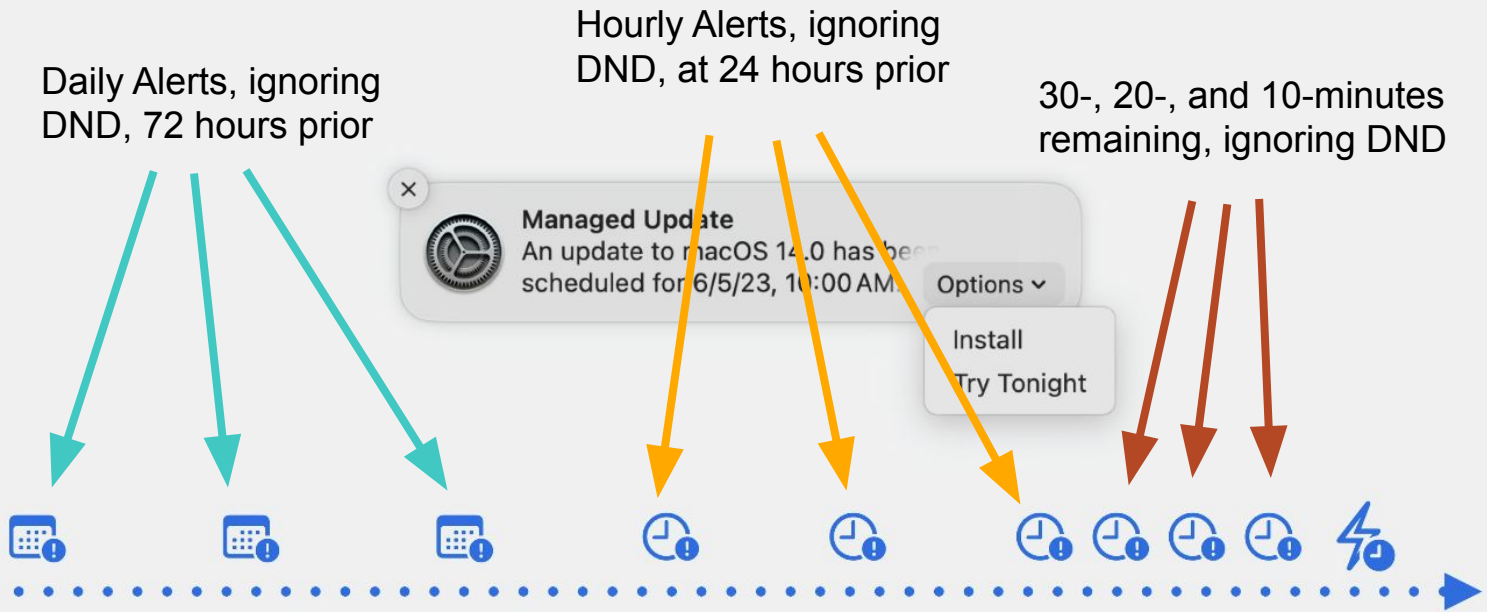
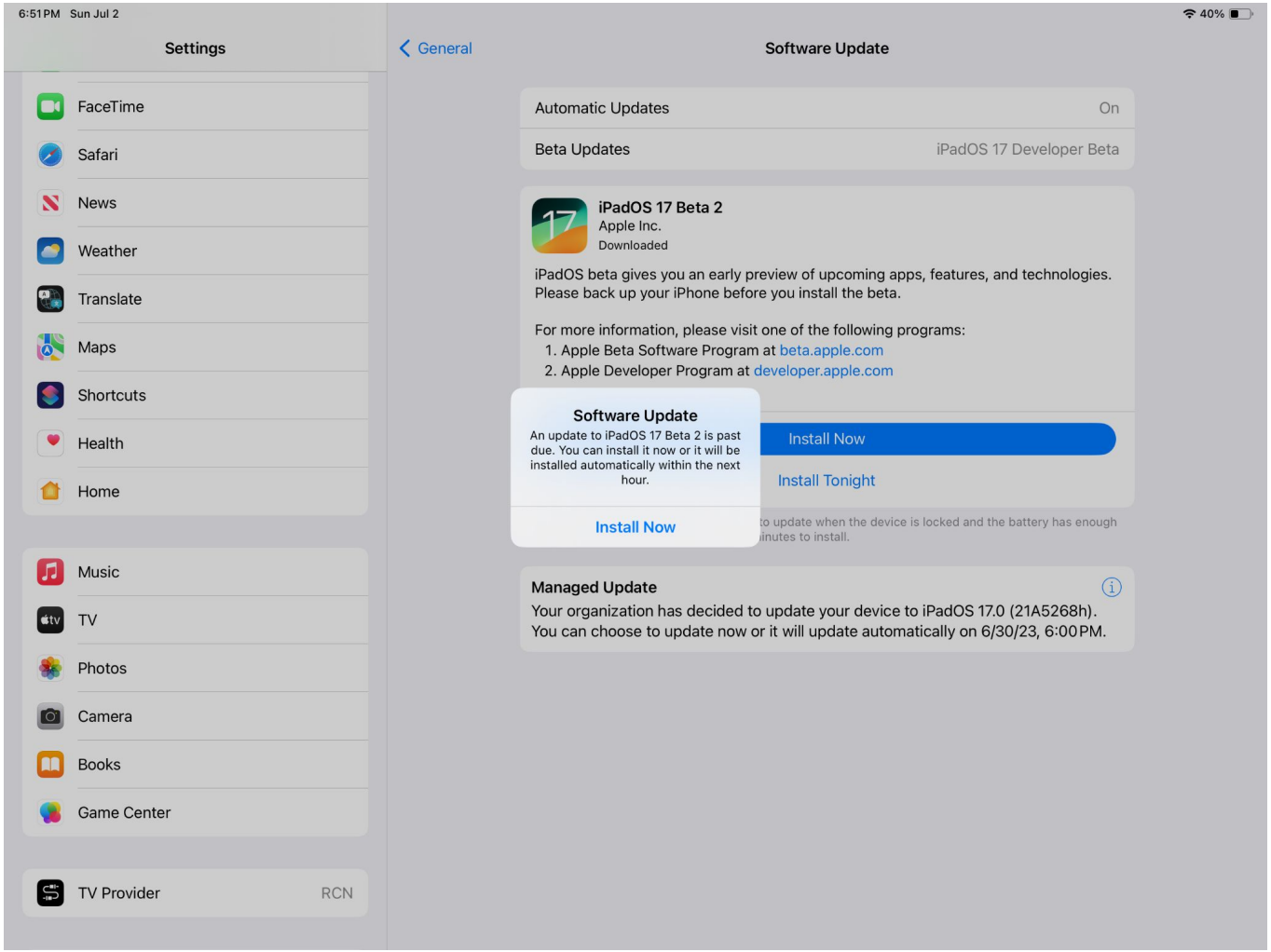


Image from Apple

So What Happens When You Ignore The Deadline?



But What If My User Was on Vacation? What Then?

Other details for using Software Deadlines

- Must be using a DDM-capable management solution
- Must have a Bootstrap Token
- Multiple versions can be specified in a Configuration, each with their own deadline
- A very large number are supported

Wish List Items

- ~~Deadlines for install based on Apple release dates.~~
- ~~Close deferral escape paths.~~
- Update alerts triggered by MDM should be customizable in time and persistence.
- Install Later should apply to Major Upgrades.
- ~~Takeover the job of Nudge or Super.~~
- Spot problems that might result in Recovery Mode during the preflight and act appropriately.

jumpcloud™

Coping Mechanisms

Mac Admins Community to the Rescue!

jumpcloud™

Nudge

Nudge

- LaunchDaemon + Configuration/JSON
- Drives user to apply their own updates
- Can takeover the screen, be customized easily
- Supported by a Jamf Schema
- Used by JumpCloud MDM as part of Patch Management
- Great Community Support in #nudge

jumpcloud™

Super

Super

- Scripts + IBM Notifier
- API Access for Jamf Pro required today
- Other MDMs may be supported in the future
- Combines notifications with API Commands for `ScheduleOSUpdate`

`softwareupdate` CLI

CLI Tools

- Basically, Don’t Do This.

CLI Tools

But if you have to, there's stuff you need to know:

- As of macOS 13, it's not a good idea to use the `sudo launchctl kickstart -k system/com.apple.softwareupdated` construct as an automated, repeated action.
- Authenticated Restarts will required a volume owner's credentials.

jumpcloud™

Feedback as an Art

Tom's Rules for Great Feedback

1. Start from what you expected
2. Then explained what happened instead
3. Describe time & effort savings desired
4. Provide examples and code
5. Center yourself with context
6. Clarity is the true soul of wit

Suggested Topic Areas

1. MDM Commands Not Being Reliable
2. MDM Command Escapes Are Too Easy
3. `InstallLater` doesn't work with Majors
4. `InstallLater` with Deferrals are too unpredictable