JAMF NATION LIVE

Compliance made effortless: An easy approach for enhancing your Device-Security with Jamf

Pontus Nord

Sales Engineer
Nordics

René Stiel

Senior Sales Engineer
DACH

Rob Lee

Sales Engineer
UK&I

Agenda

1 | **An overview of types of security compliance and their importance**

Types, Consequences, Benefits, Frameworks

2 | **Compliance Monitoring**

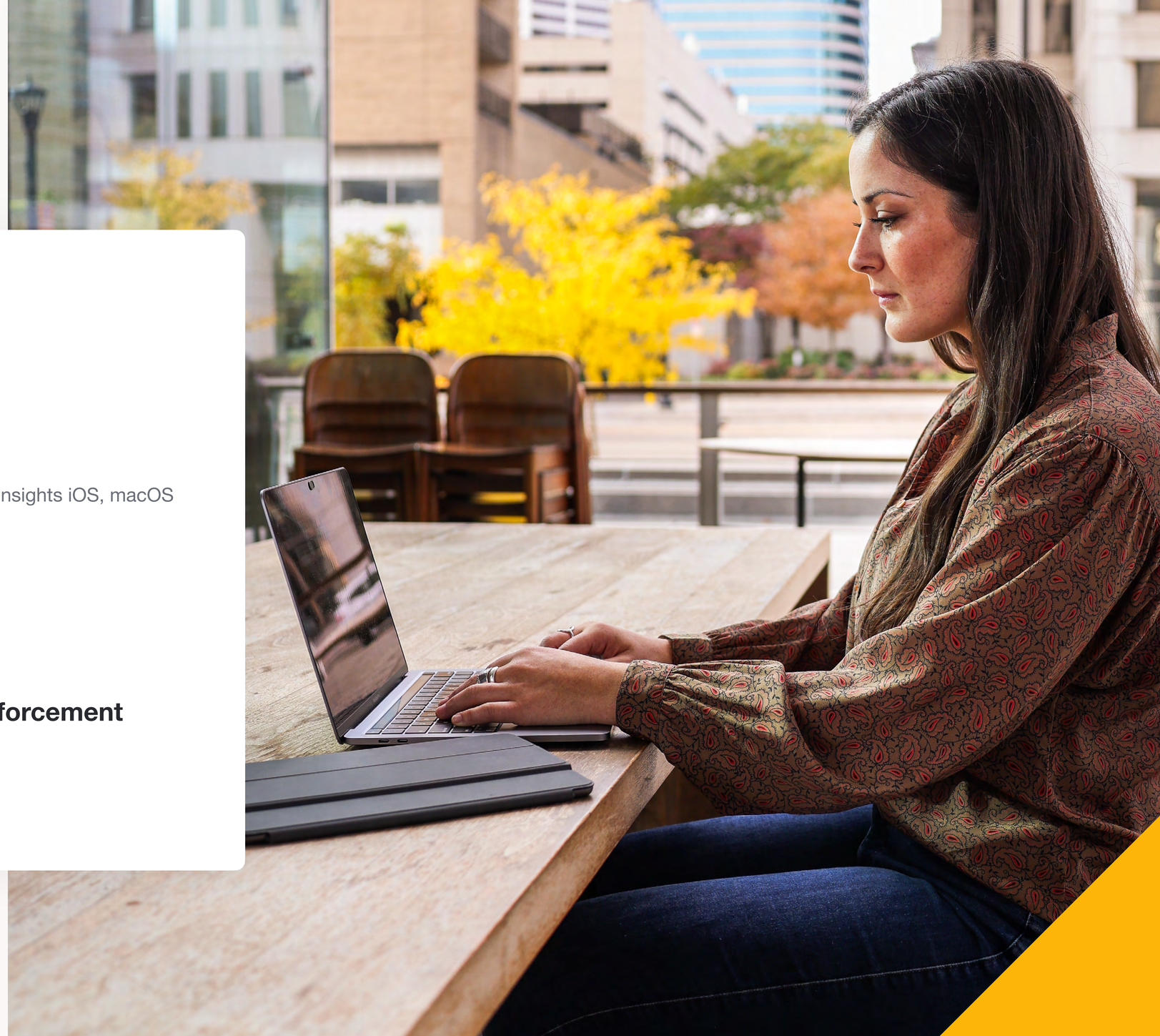
Compliance Dashboard, CVE-Monitoring, App-Insights iOS, macOS

3 | **Compliance with Jamf**

Compliance Editor, Jamf Pro

4 | **Compliance Remediation and Enforcement**

Jamf Pro, Jamf Protect



An overview of types of security compliance and their importance


Adhering to:
Laws
Industry Standards
Data and Security Requirements
JAMF NATION LIVE


Dependent on industry
Device and data
Requirements as a legal entity
JAMF NATION LIVE

Impact on the organization
Workforce and customers

JAMF NATION LIVE

Types of **Compliance**

Legal Regulations

Industry Standards

Security Compliance

Company Rules and Responsibilities

Consequences of **non-compliance**

Data breaches and leakage

Monetary loss (fines, settlements)

Loss of customers, accounts or job

Loss of reputation

Benefits of Compliance

Besides the monetary fines and sanctions, following security compliance in an organization brings several benefits such as;

- Protecting your company's reputation
- Mitigating security risks
- Enhancing customer confidence
- Improving operational efficiency
- Staying ahead of the competition

Compliance Frameworks

Baselines and Benchmarks

A **"security baseline"** is a **set of controls**
that an organisation wants to configure on their devices.

Once these are in place, they must continually check that the controls remain in place
and that the devices are compliant.

This **compliance assessment system** is the **"benchmark".**

Why implement **Baselines and Benchmarks?**

Some government agencies require all computers that interact with their systems and data to be subject to a specific benchmark with few allowances for exceptions. Many regulated industries will also be required to implement a security benchmark.

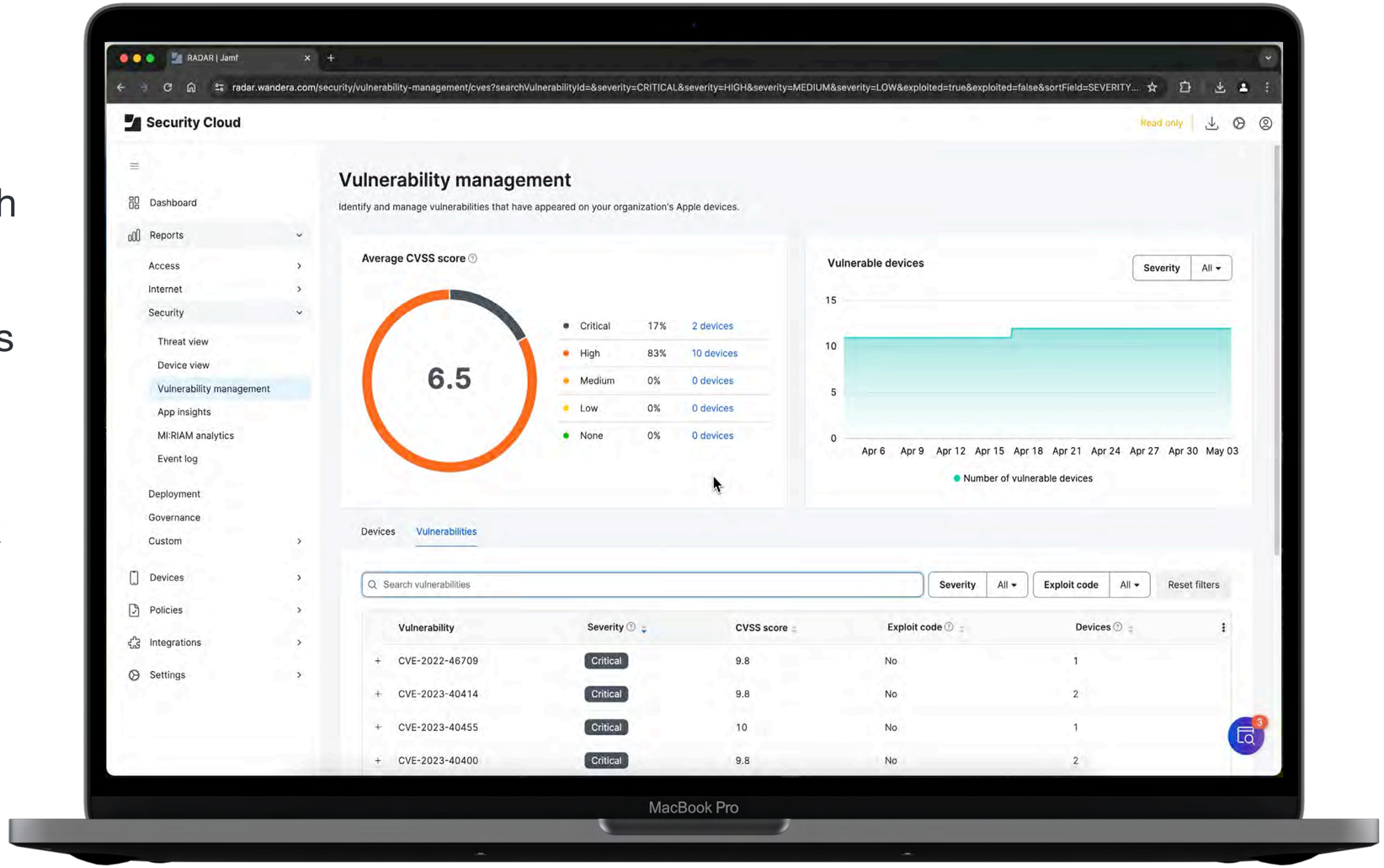
- IT and Information Security departments need to collaborate
- Balance between information security and user productivity
- Different devices with different risk categories

Compliance and Vulnerability Monitoring with Jamf Protect

JAMF NATION LIVE

Vulnerability Management
In Jamf Protect

- Detailed reporting of Apple devices with **known vulnerabilities**
- Built-in **CVE reporting** for OS and apps
- **Automatic risk elevation**, devices running risky OS will have elevated risk status
- Users can be **notified** of update vulnerable systems

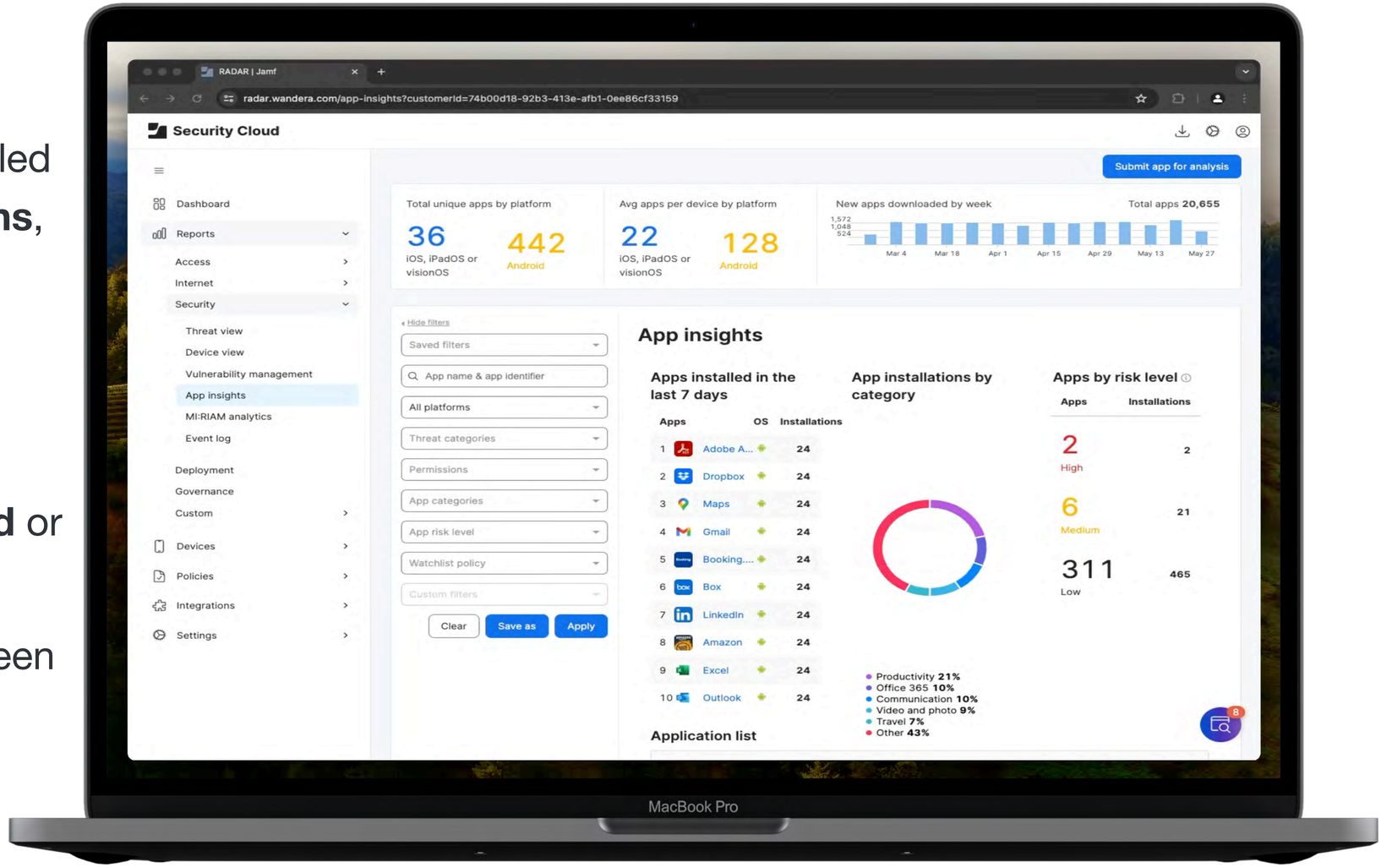


App Insights
In Jamf Protect

- **Returns** information on the apps installed on your devices, including their **versions**, permissions, and the **level of risk** they may pose.

Identify:

- How many users are using an **outdated** or **risky** version of an app
- Which apps are leaking data or have been **side-loaded**

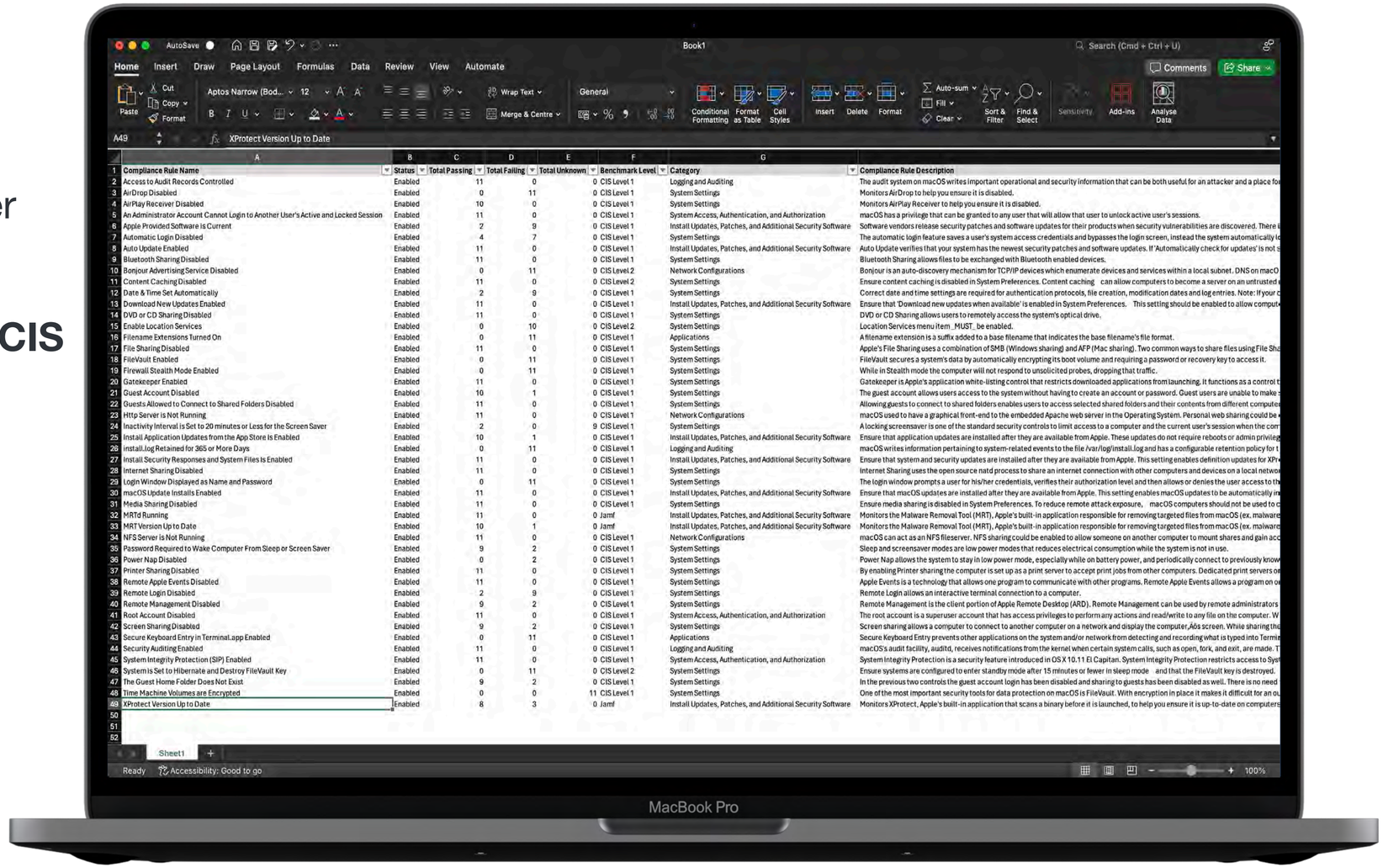


Compliance Baseline
In Jamf Protect

- **New dashboard** with widgets for better visibility
- Compliance baseline rules built on the **CIS benchmark** for macOS Sonoma
- **More visibility** for administrators to ensure their Mac computers stay compliant
- The perfect tool to **monitor** Jamf Compliance Editor's effectiveness

Compliance Baseline
In Jamf Protect

- **New dashboard** with widgets for better visibility
- Compliance baseline rules built on the **CIS benchmark** for macOS Sonoma
- **More visibility** for administrators to ensure their Mac computers stay compliant
- Easily generate **Reporting**



Compliance Rule Name	Status	Total Passing	Total Failing	Total Unknown	Benchmark Level	Category	Compliance Rule Description
Access to Audit Records Controlled	Enabled	11	0	0	CIS Level 1	Logging and Auditing	The audit system on macOS writes important operational and security information that can be both useful for an attacker and a place fo
AirDrop Disabled	Enabled	0	11	0	CIS Level 1	System Settings	Monitors AirDrop to help you ensure it is disabled.
AirPlay Receiver Disabled	Enabled	10	0	0	CIS Level 1	System Settings	Monitors AirPlay Receiver to help you ensure it is disabled.
An Administrator Account Cannot Login to Another User's Active and Locked Session	Enabled	11	0	0	CIS Level 1	System Access, Authentication, and Authorization	macOS has a privilege that can be granted to any user that will allow that user to unlock active user's sessions.
Apple Provided Software is Current	Enabled	2	9	0	CIS Level 1	Install Updates, Patches, and Additional Security Software	Software vendors release security patches and software updates for their products when security vulnerabilities are discovered. There i
Automatic Login Disabled	Enabled	4	7	0	CIS Level 1	System Settings	The automatic login feature saves a user's system access credentials and bypasses the login screen, instead the system automatically l
Auto Update Enabled	Enabled	11	0	0	CIS Level 1	Install Updates, Patches, and Additional Security Software	Auto Update verifies that your system has the newest security patches and software updates. If 'Automatically check for updates' is not s
Bluetooth Sharing Disabled	Enabled	11	0	0	CIS Level 1	System Settings	Bluetooth Sharing allows files to be exchanged with Bluetooth enabled devices.
Bonjour Advertising Service Disabled	Enabled	0	11	0	CIS Level 2	Network Configurations	Bonjour is an auto-discovery mechanism for TCP/IP devices which enumerate devices and services within a local subnet. DNS on macO
Content Caching Disabled	Enabled	11	0	0	CIS Level 2	System Settings	Ensure content caching is disabled in System Preferences. Content caching can allow computers to become a server on an untrusted
Date & Time Set Automatically	Enabled	2	9	0	CIS Level 1	System Settings	Correct date and time settings are required for authentication protocols, file creation, modification dates and log entries. Note: If your c
Download New Updates Enabled	Enabled	11	0	0	CIS Level 1	Install Updates, Patches, and Additional Security Software	Ensure that 'Download new updates when available' is enabled in System Preferences. This setting should be enabled to allow compute
DVD or CD Sharing Disabled	Enabled	11	0	0	CIS Level 1	System Settings	DVD or CD Sharing allows users to remotely access the system's optical drive.
Enable Location Services	Enabled	0	10	0	CIS Level 2	System Settings	Location Services menu item _MUST_ be enabled.
Filename Extensions Turned On	Enabled	0	11	0	CIS Level 1	Applications	A filename extension is a suffix added to a base filename that indicates the base filename's file format.
File Sharing Disabled	Enabled	11	0	0	CIS Level 1	System Settings	Apple's File Sharing uses a combination of SMB (Windows sharing) and AFP (Mac sharing). Two common ways to share files using File Sha
FileVault Enabled	Enabled	0	11	0	CIS Level 1	System Settings	FileVault secures a system's data by automatically encrypting its boot volume and requiring a password or recovery key to access it.
Firewall Stealth Mode Enabled	Enabled	0	11	0	CIS Level 1	System Settings	While in Stealth mode the computer will not respond to unsolicited probes, dropping that traffic.
Gatekeeper Enabled	Enabled	11	0	0	CIS Level 1	System Settings	Gatekeeper is Apple's application white-listing control that restricts downloaded applications from launching. It functions as a control t
Guest Account Disabled	Enabled	10	1	0	CIS Level 1	System Settings	The guest account allows users access to the system without having to create an account or password. Guest users are unable to make
Guests Allowed to Connect to Shared Folders Disabled	Enabled	11	0	0	CIS Level 1	System Settings	Allowing guests to connect to shared folders enables users to access selected shared folders and their contents from different computer
Http Server is Not Running	Enabled	11	0	0	CIS Level 1	Network Configurations	macOS used to have a graphical front-end to the embedded Apache web server in the Operating System. Personal web sharing could be
Inactivity Interval is Set to 20 minutes or Less for the Screen Saver	Enabled	2	0	9	CIS Level 1	System Settings	A locking screensaver is one of the standard security controls to limit access to a computer and the current user's session when the com
Install Application Updates from the App Store is Enabled	Enabled	10	1	0	CIS Level 1	Install Updates, Patches, and Additional Security Software	Ensure that application updates are installed after they are available from Apple. These updates do not require reboots or admin privileg
install.log Retained for 365 or More Days	Enabled	0	11	0	CIS Level 1	Logging and Auditing	macOS writes information pertaining to system-related events to the file /var/log/install.log and has a configurable retention policy for t
Install Security Responses and System Files is Enabled	Enabled	11	0	0	CIS Level 1	Install Updates, Patches, and Additional Security Software	Ensure that system and security updates are installed after they are available from Apple. This setting enables definition updates for XPr
Internet Sharing Disabled	Enabled	11	0	0	CIS Level 1	System Settings	Internet Sharing uses the open source natd process to share an internet connection with other computers and devices on a local netwo
Login Window Displayed as Name and Password	Enabled	0	11	0	CIS Level 1	System Settings	The login window prompts a user for his/her credentials, verifies their authorization level and then allows or denies the user access to th
macOS Update Installs Enabled	Enabled	11	0	0	CIS Level 1	Install Updates, Patches, and Additional Security Software	Ensure that macOS updates are installed after they are available from Apple. This setting enables macOS updates to be automatically in
Media Sharing Disabled	Enabled	11	0	0	CIS Level 1	System Settings	Ensure media sharing is disabled in System Preferences. To reduce remote attack exposure, macOS computers should not be used to c
MRTd Running	Enabled	11	0	0	Jamf	Install Updates, Patches, and Additional Security Software	Monitors the Malware Removal Tool (MRT), Apple's built-in application responsible for removing targeted files from macOS (ex. malware
MRT Version Up to Date	Enabled	10	1	0	Jamf	Install Updates, Patches, and Additional Security Software	Monitors the Malware Removal Tool (MRT), Apple's built-in application responsible for removing targeted files from macOS (ex. malware
NFS Server is Not Running	Enabled	11	0	0	CIS Level 1	Network Configurations	macOS can act as an NFS fileserver. NFS sharing could be enabled to allow someone on another computer to mount shares and gain acc
Password Required to Wake Computer From Sleep or Screen Saver	Enabled	9	2	0	CIS Level 1	System Settings	Sleep and screensaver modes are low power modes that reduces electrical consumption while the system is not in use.
Power Nap Disabled	Enabled	0	2	0	CIS Level 1	System Settings	Power Nap allows the system to stay in low power mode, especially while on battery power, and periodically connect to previously know
Printer Sharing Disabled	Enabled	11	0	0	CIS Level 1	System Settings	By enabling Printer sharing the computer is set up as a print server to accept print jobs from other computers. Dedicated print servers o
Remote Apple Events Disabled	Enabled	11	0	0	CIS Level 1	System Settings	Apple Events is a technology that allows one program to communicate with other programs. Remote Apple Events allows a program on o
Remote Login Disabled	Enabled	2	9	0	CIS Level 1	System Settings	Remote Login allows an interactive terminal connection to a computer.
Remote Management Disabled	Enabled	9	2	0	CIS Level 1	System Settings	Remote Management is the client portion of Apple Remote Desktop (ARD). Remote Management can be used by remote administrators
Root Account Disabled	Enabled	11	0	0	CIS Level 1	System Access, Authentication, and Authorization	The root account is a superuser account that has access privileges to perform any actions and read/write to any file on the computer. W
Screen Sharing Disabled	Enabled	9	2	0	CIS Level 1	System Settings	Screen sharing allows a computer to connect to another computer on a network and display the computer,Ás screen. While sharing the
Secure Keyboard Entry in Terminal.app Enabled	Enabled	0	11	0	CIS Level 1	Applications	Secure Keyboard Entry prevents other applications on the system and/or network from detecting and recording what is typed into Termi
Security Auditing Enabled	Enabled	11	0	0	CIS Level 1	Logging and Auditing	macOS's audit facility, auditd, receives notifications from the kernel when certain system calls, such as open, fork, and exit, are made. T
System Integrity Protection (SIP) Enabled	Enabled	11	0	0	CIS Level 1	System Access, Authentication, and Authorization	System Integrity Protection is a security feature introduced in OS X 10.11 El Capitan. System Integrity Protection restricts access to Syst
System is Set to Hibernate and Destroy FileVault Key	Enabled	0	11	0	CIS Level 2	System Settings	Ensure systems are configured to enter standby mode after 15 minutes or fewer in sleep mode and that the FileVault key is destroyed.
The Guest Home Folder Does Not Exist	Enabled	9	2	0	CIS Level 1	System Settings	In the previous two controls the guest account login has been disabled and sharing to guests has been disabled as well. There is no need
Time Machine Volumes are Encrypted	Enabled	0	0	11	CIS Level 1	System Settings	One of the most important security tools for data protection on macOS is FileVault. With encryption in place it makes it difficult for an ou
XProtect Version Up to Date	Enabled	8	3	0	Jamf	Install Updates, Patches, and Additional Security Software	Monitors XProtect, Apple's built-in application that scans a binary before it is launched, to help you ensure it is up-to-date on computers

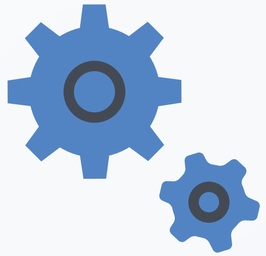
JAMF NATION LIVE

Compliance with Jamf

How do we deploy our compliance baseline?

1.Go to CIS website
2.Go to Solutions > Benchmarks
3.Fill in a form
4.Get an email

5.Access the benchmarks webpage
6.Find the benchmark you want.
7.Download the PDF
8.Read the PDF



9.Create all the scripts/configuration profiles needed
10.Upload them to Jamf Pro
11.Deploy to devices
12.Test them.

Center for Internet Security

CIS Apple macOS 14.0 Sonoma

v1.0.0 - 10-16-2023

JAMF NATION LIVE

2.2.1 Ensure Firewall Is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

A firewall is a piece of software that blocks unwanted incoming connections to a system. Apple has posted general documentation about the application firewall:

Rationale:

A firewall minimizes the threat of unauthorized users gaining access to your system while connected to a network or the Internet.

Impact:

The firewall may block legitimate traffic. Applications that are unsigned will require special handling.

Audit:

Graphical Method:
Perform the following steps to ensure the firewall is enabled:

1. Open `System Settings`
2. Select `Network`
3. Verify that the `Firewall` is `Active`

or

1. Open `System Settings`
2. Select `Privacy & Security`
3. Select `Profiles`
4. Verify that an installed profile has `Firewall` set to `Enabled`

Terminal Method:
Run the following command to verify that the firewall is enabled:

```
$ /usr/bin/sudo /usr/bin/osascript -l JavaScript << EOS
function run() {
    app = Application.currentApplication()
    app.includeStandardAdditions = true;


  let pref1 = app.doShellScript('/usr/bin/defaults read
/Library/Preferences/com.apple.alf globalstate')
  let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.fire
wall')\
  .objectForKey('EnableFirewall'))

    if ( ( ( pref1 == 1 ) || ( pref1 == 2 ) || ( pref2 == "true" ) ) &&
(pref1 != 0 ) ) {
    return("true")
  } else {
    return("false")
  }

}
EOS

true
```

Remediation:

Graphical Method:
Perform the following steps to turn the firewall on:

1. Open `System Settings`
2. Select `Network`
3. Select `Firewall`
4. Set `Firewall` to enabled

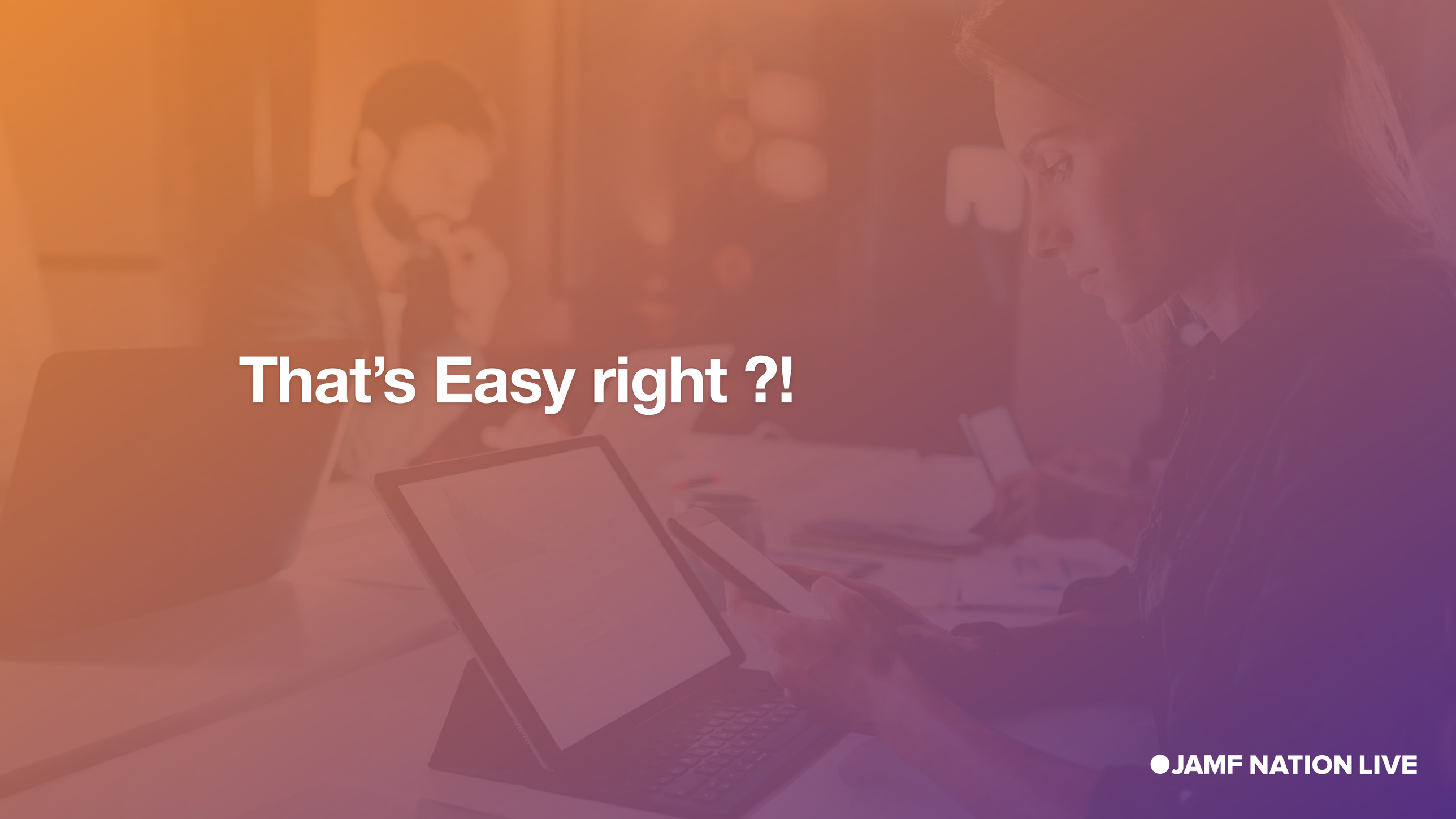
Terminal Method:
Run the following command to enable the firewall:

```
$ /usr/bin/sudo /usr/bin/defaults write /Library/Preferences/com.apple.alf
globalstate -int <value>
```

For the `<value>`, use either `1`, specific services, or `2`, essential services only.

Profile Method:
Create or edit a configuration profile with the following information:

1. The PayloadType string is `com.apple.security.firewall`
2. The key to include is `EnableFirewall`
3. The key must be set to `<true/>`

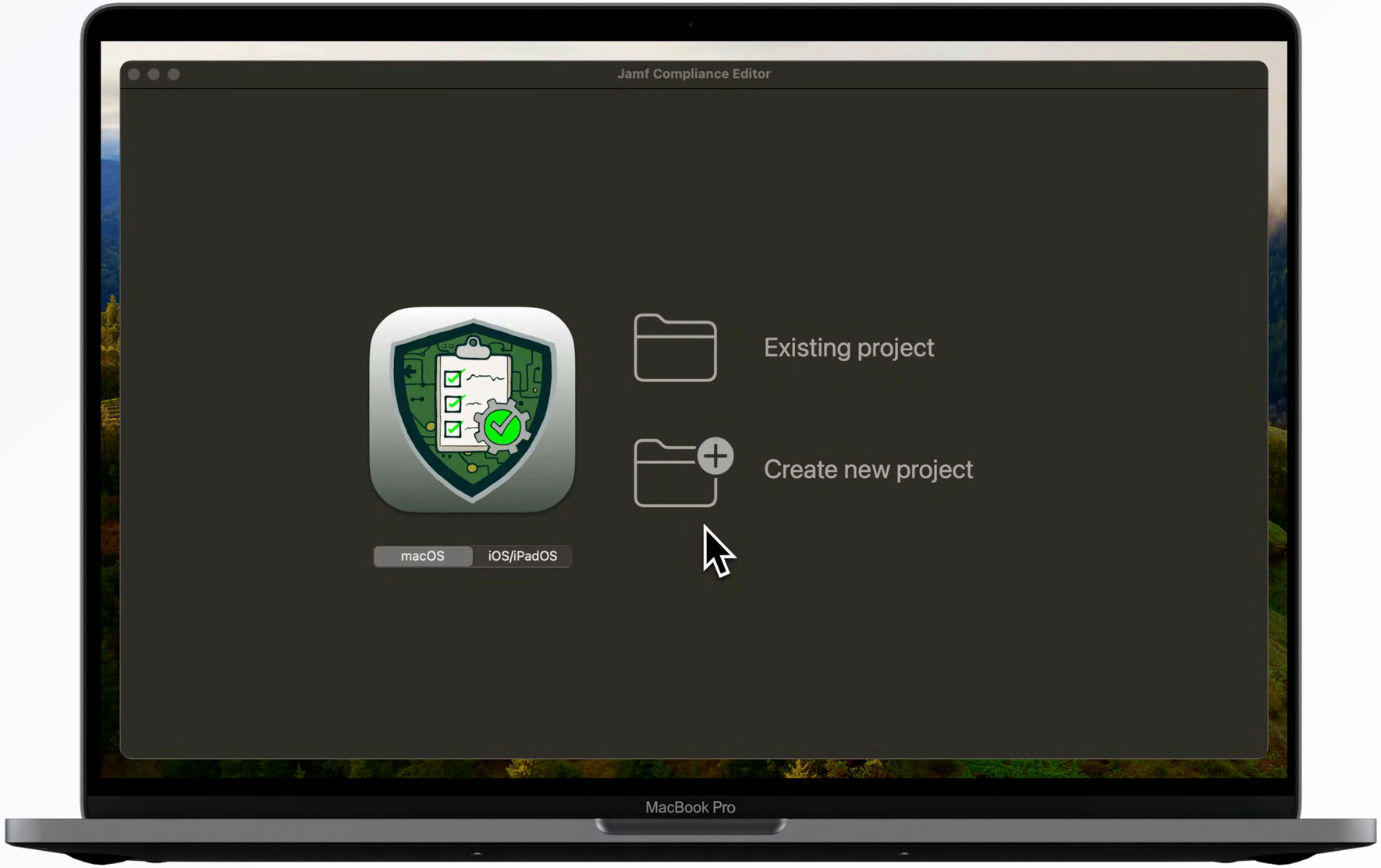

That’s Easy right ?!
JAMF NATION LIVE

Jamf Compliance Editor

- Automatically **generate compliance baselines** for common compliance benchmarks
- **One-click** guidance creation
- Easy to **customize** guidance for any organization's specific needs
- Integrate with **Jamf Pro** for quick deployments
- Generate **detailed reporting**

How do we deploy our compliance baseline?

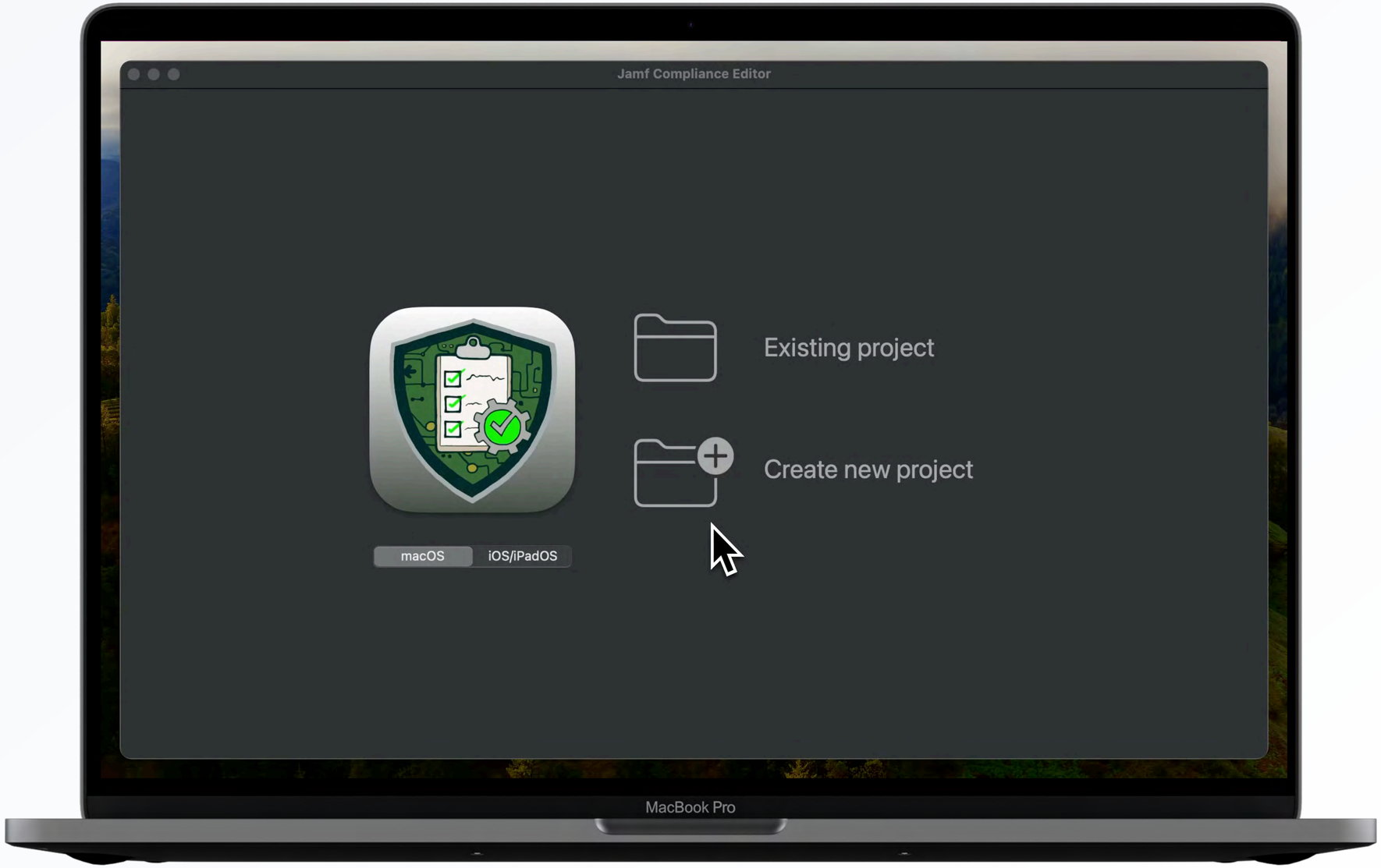
Select your Platform



How do we deploy our compliance baseline?

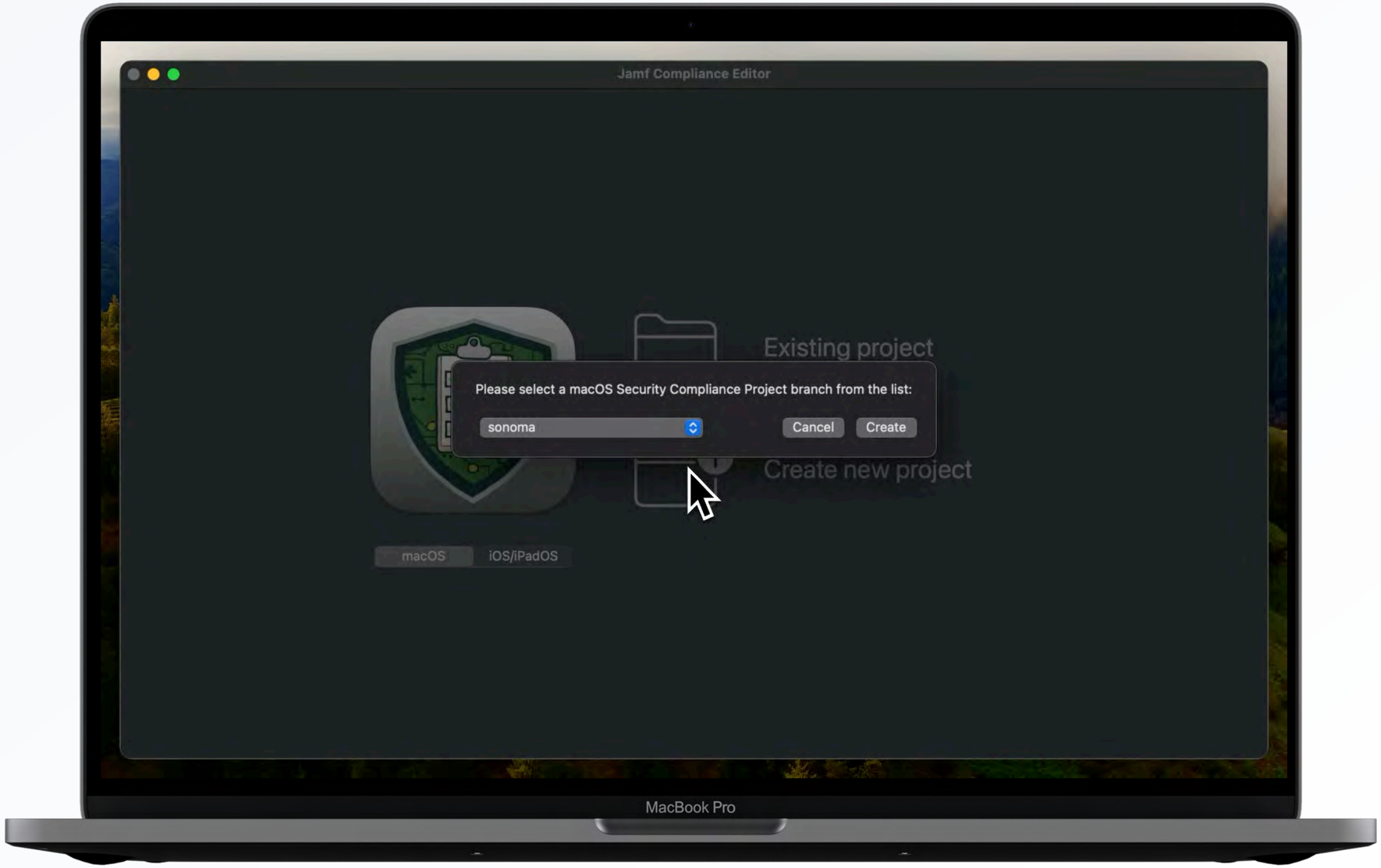
Create a new Project

Select your OS



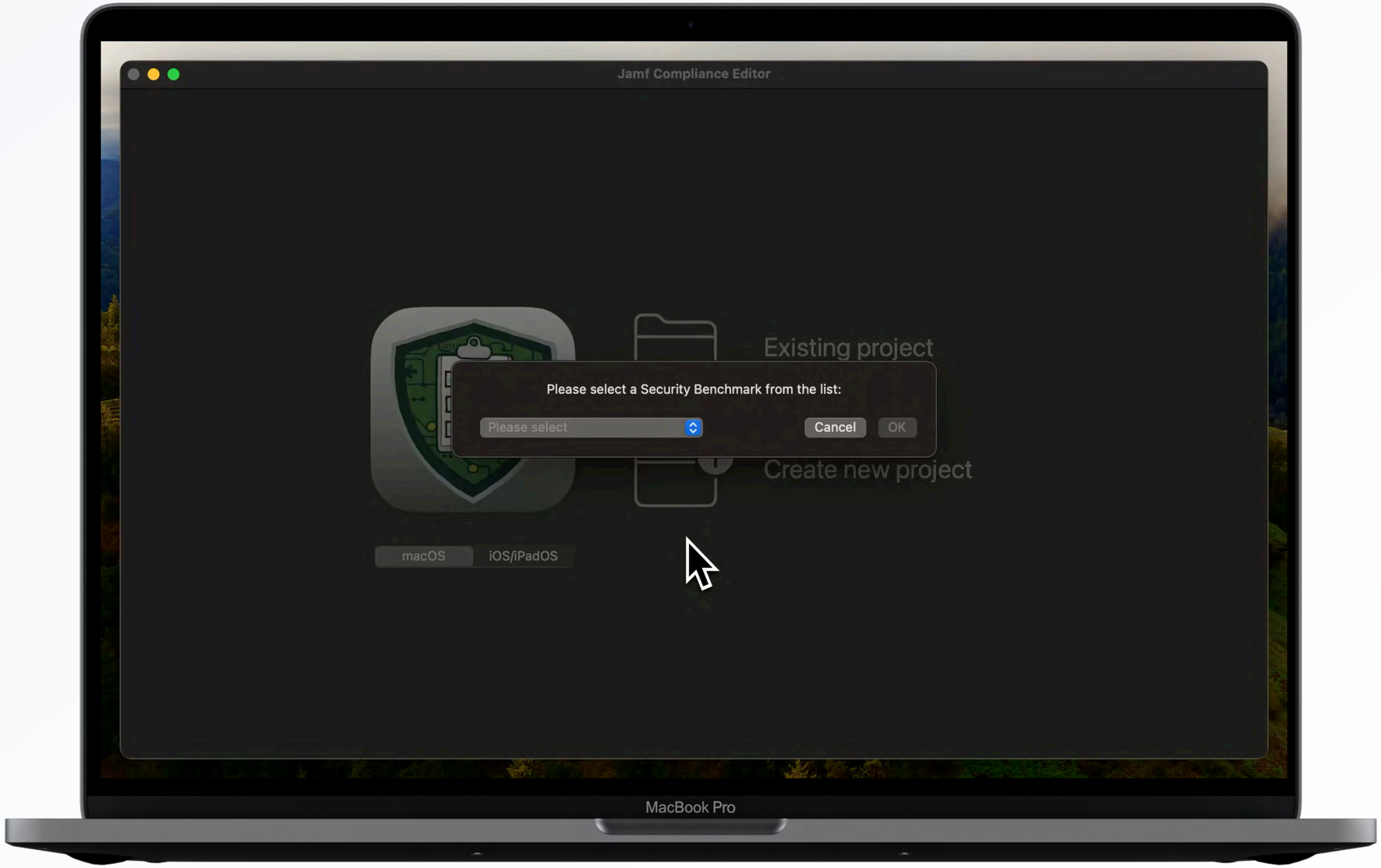
How do we deploy our compliance baseline?

Save your Project



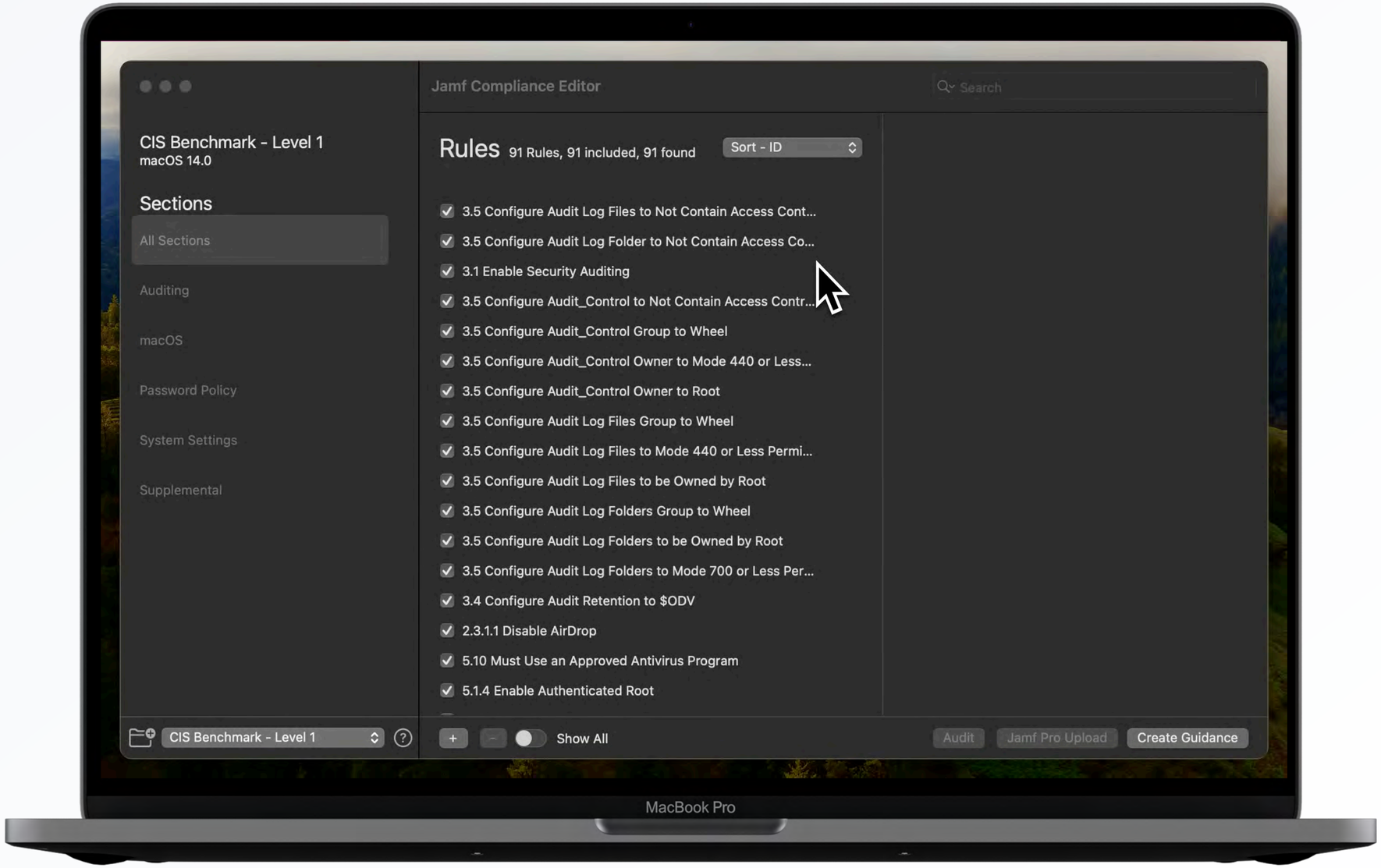
How do we deploy our compliance baseline?

Select your Benchmark



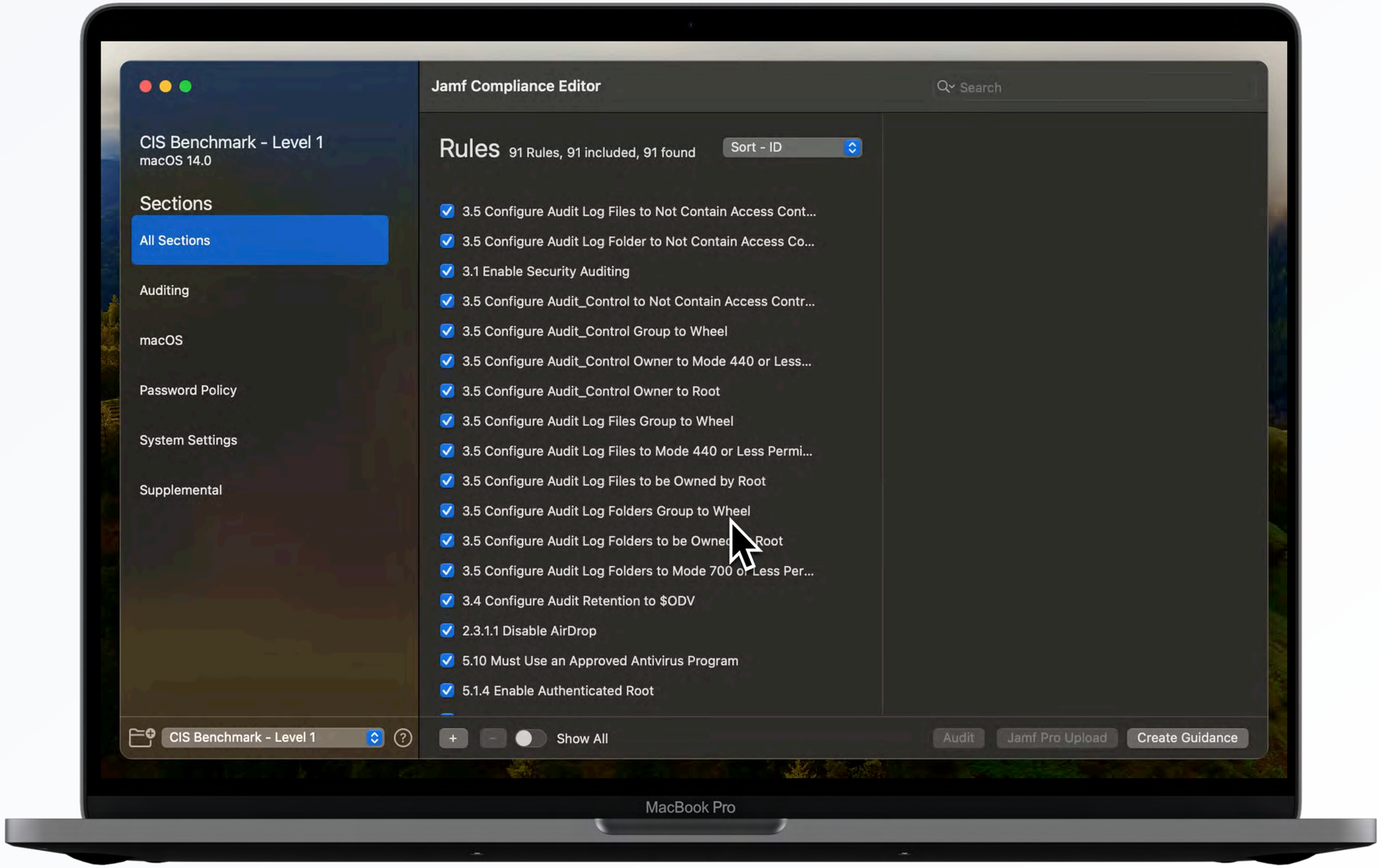
How do we deploy our compliance baseline?

Overview of all Rules



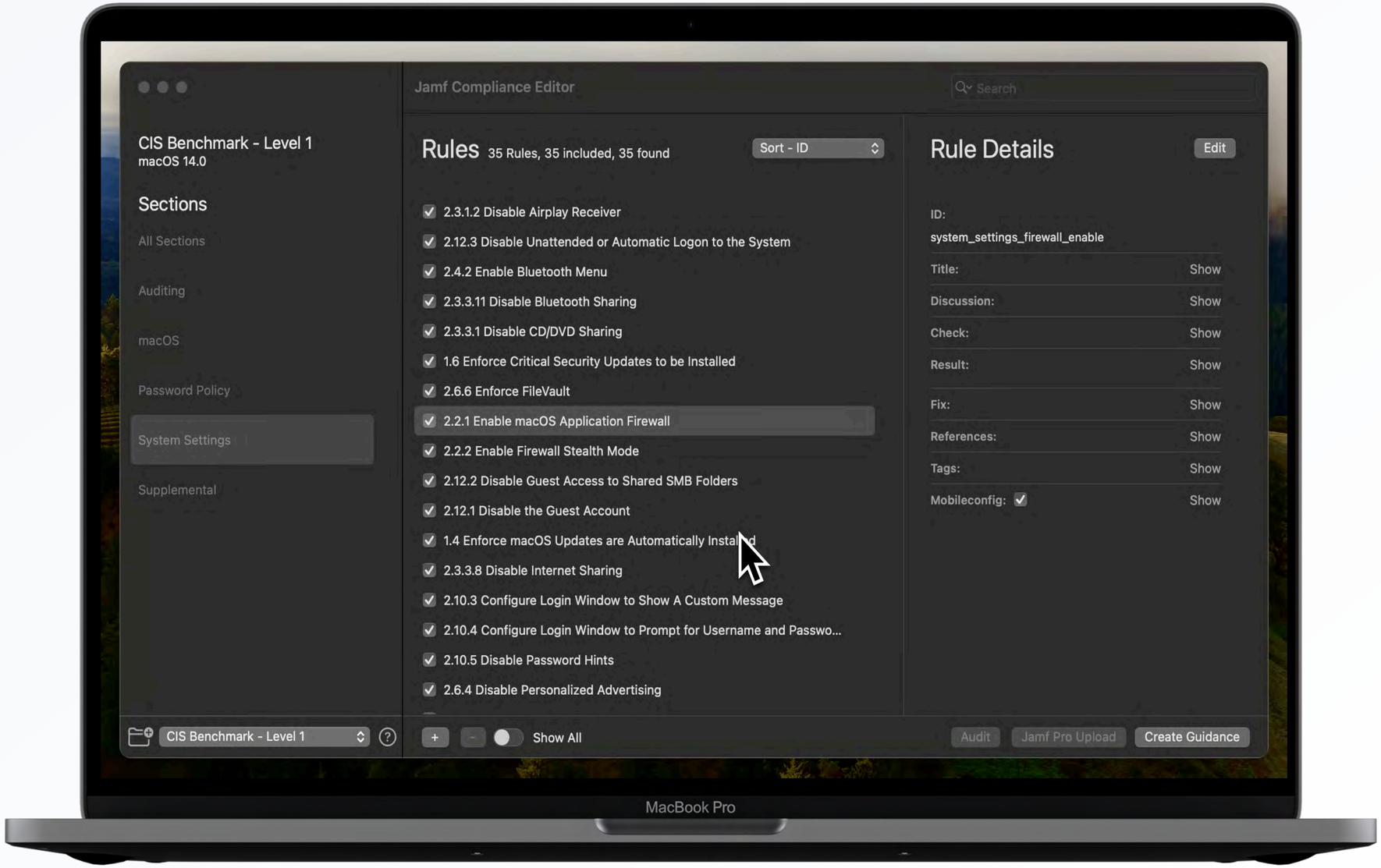
How do we deploy our compliance baseline?

Check specific Rules
e.g. (AirDrop or Firewall)



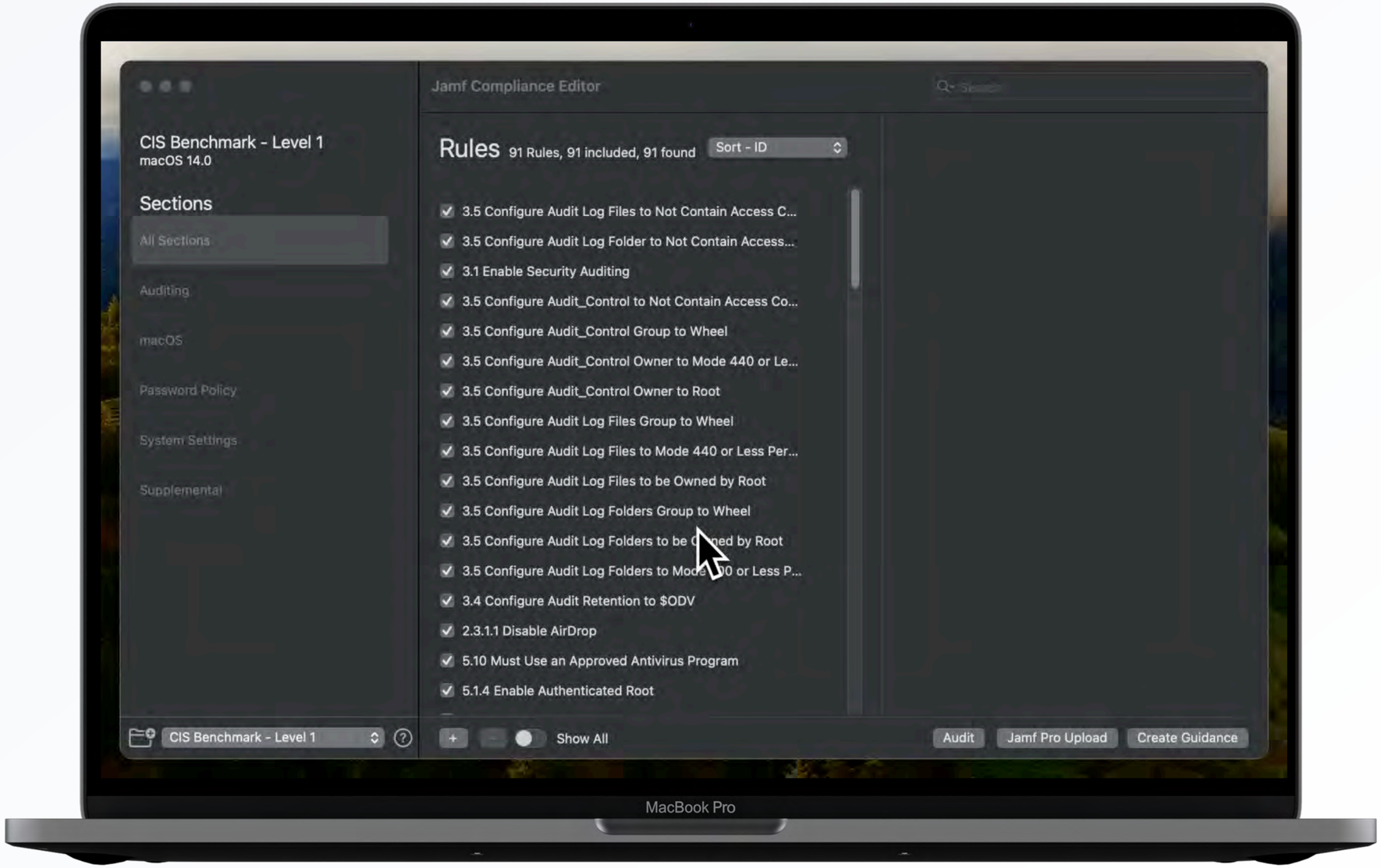
How do we deploy our compliance baseline?

Optional: Edit Rules
e.g. (Screen Saver)



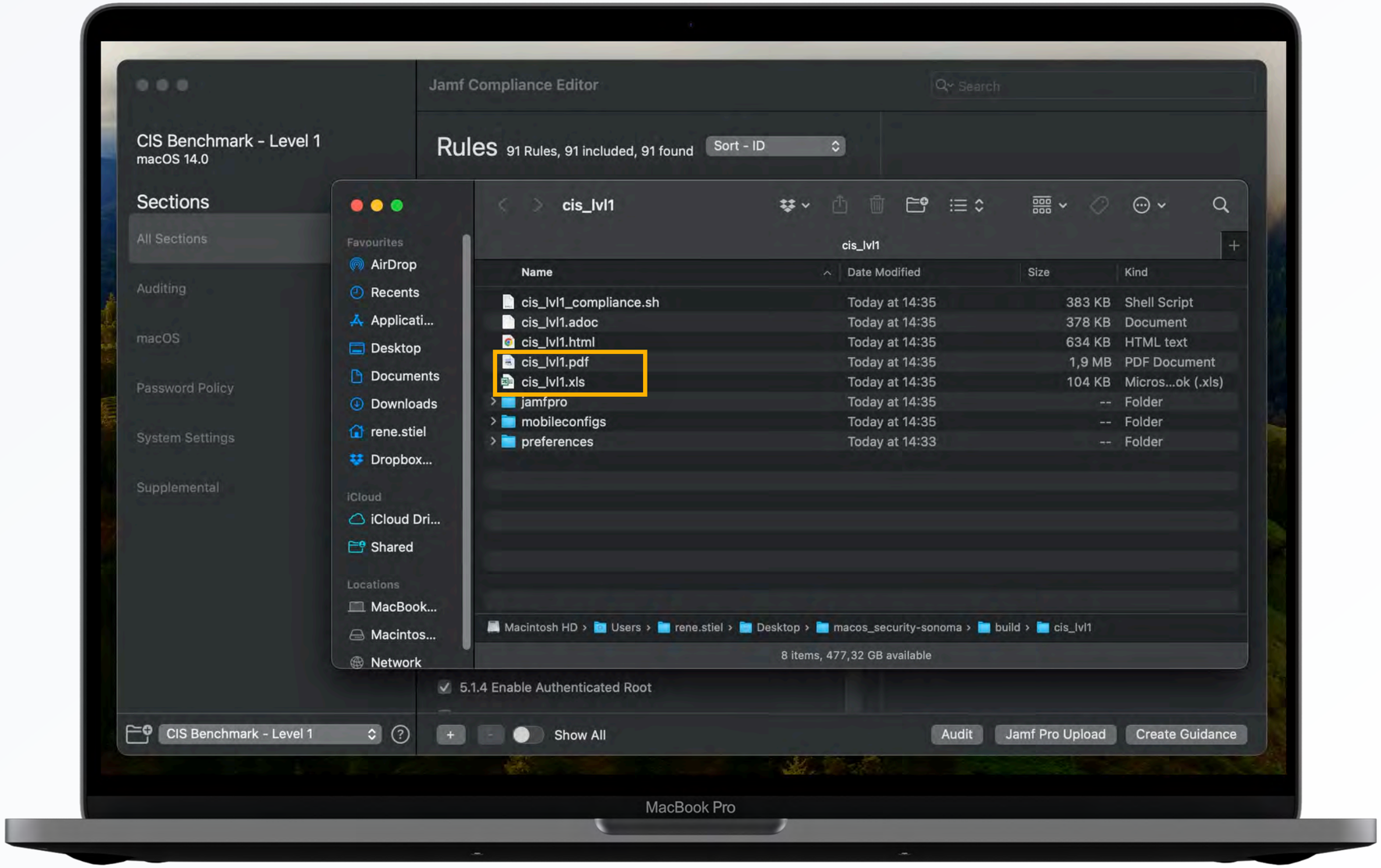
How do we deploy our compliance baseline?

Create your Guidance



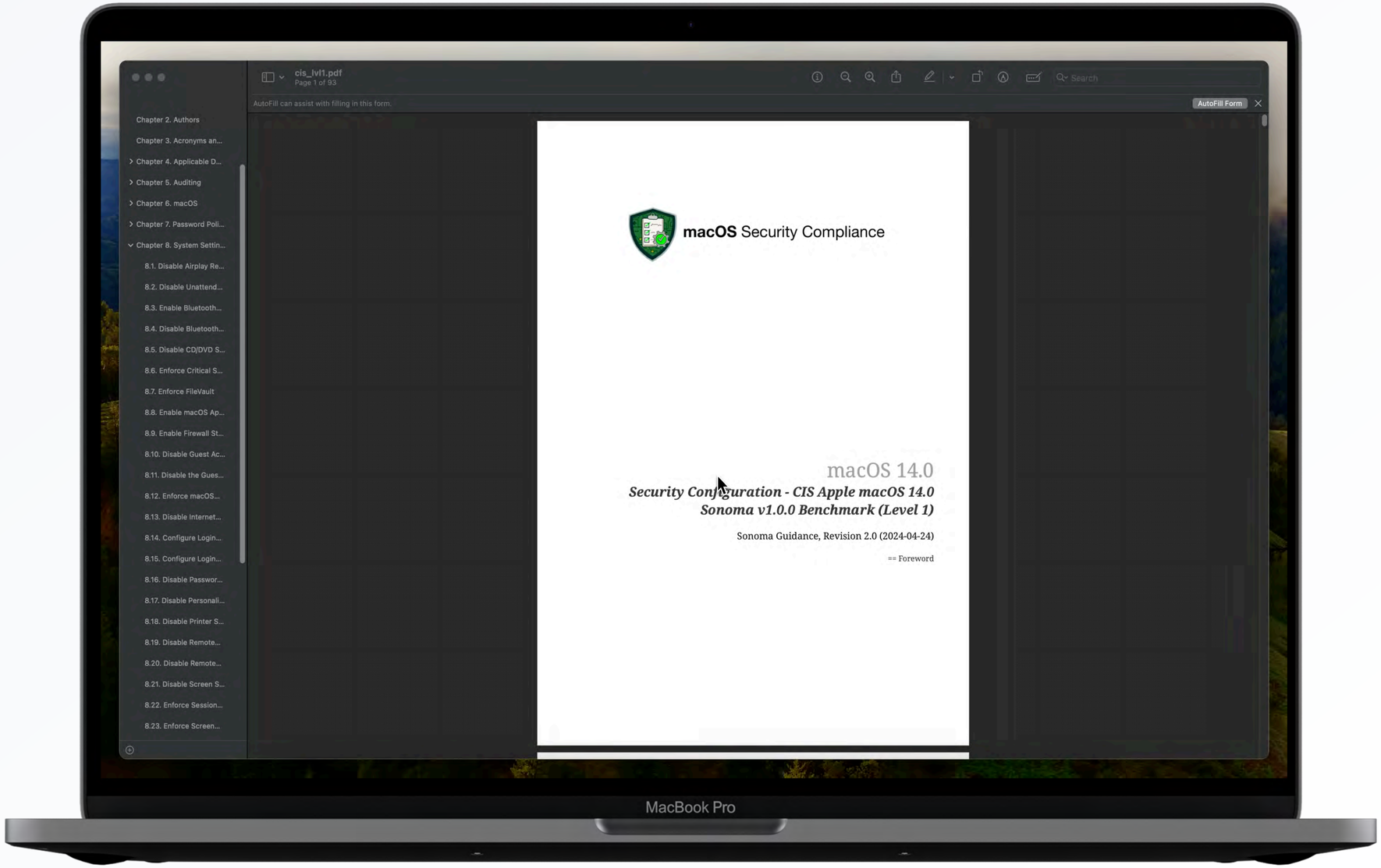
How do we deploy our compliance baseline?

Create your Guidance



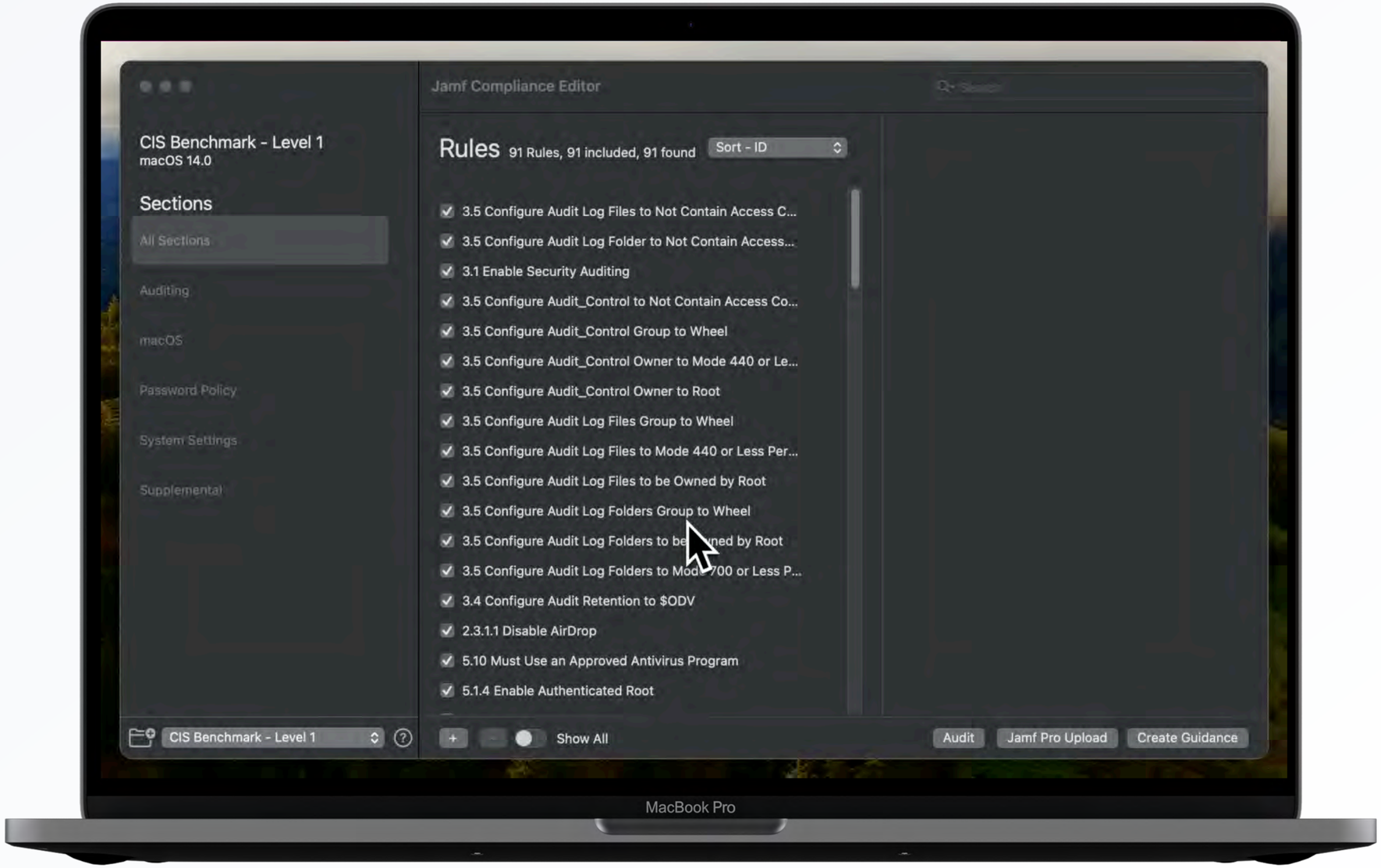
How do we deploy our compliance baseline?

Create your Guidance



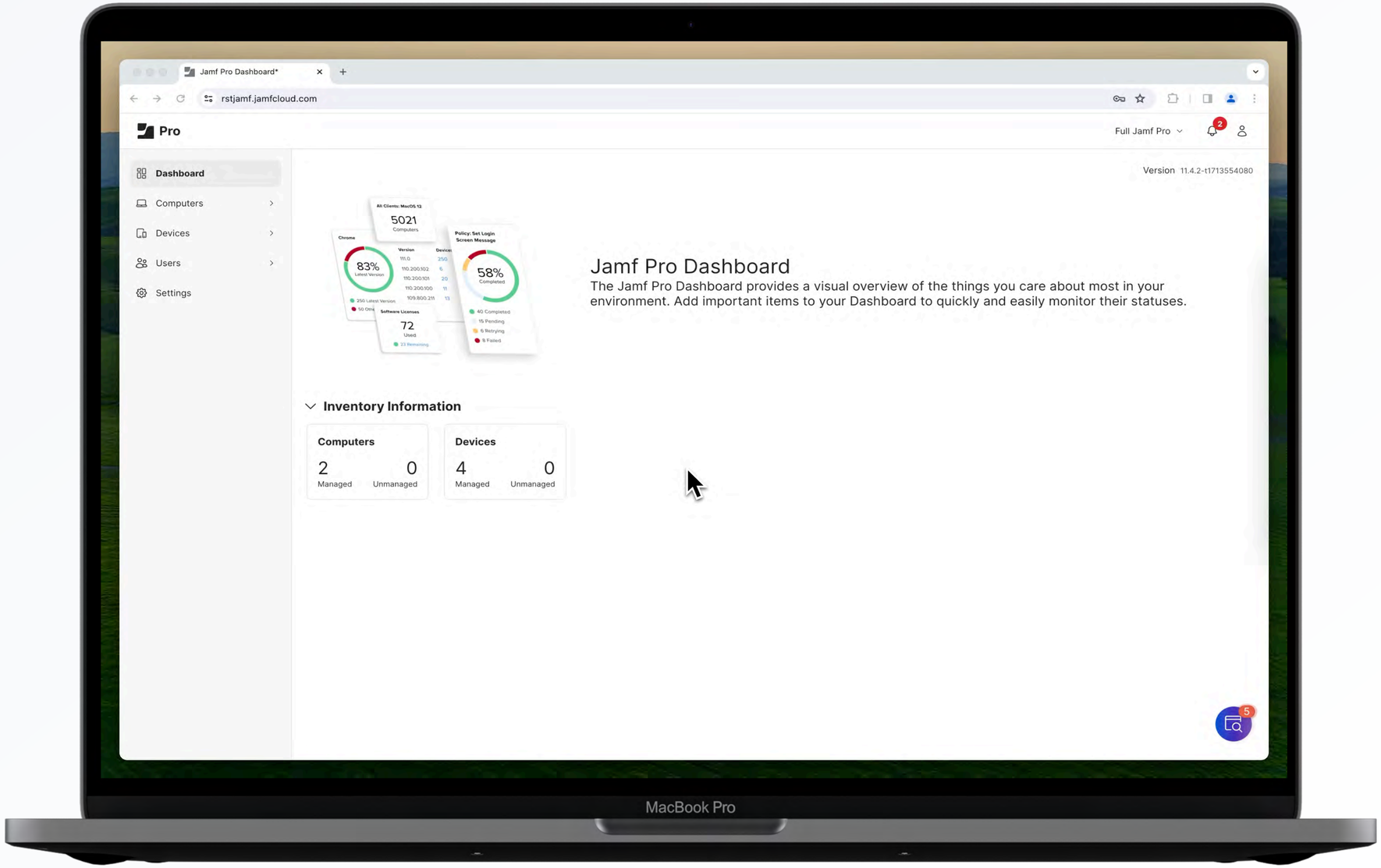
How do we deploy our compliance baseline?

Upload to Jamf Pro



How do we deploy our compliance baseline?

All Profiles and Scripts needed are available in Jamf Pro



Compliance - Remediation and Enforcement

Remediate and Enforce Settings

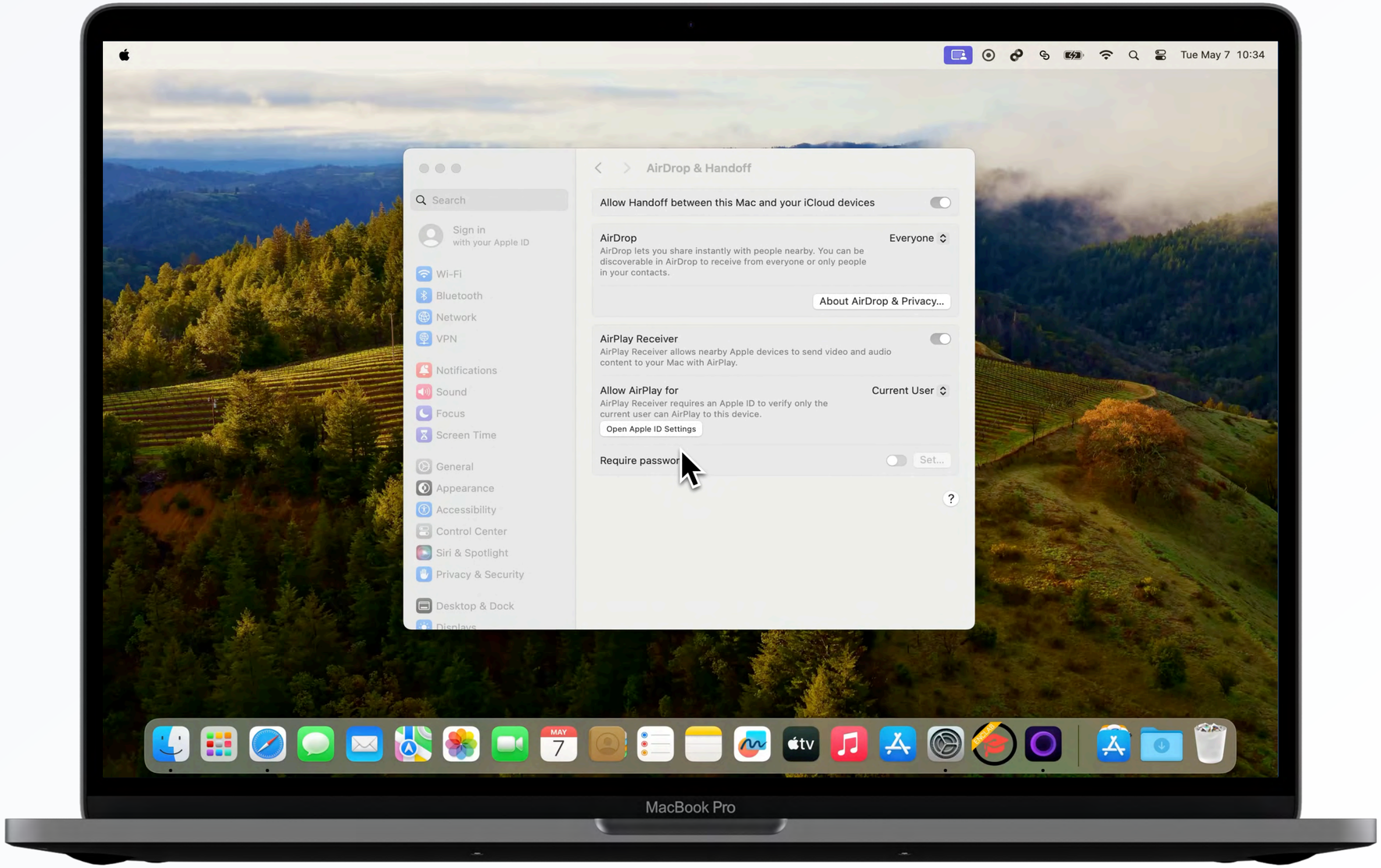
Non-Compliant Device:
Firewall-setting - not enforced

“Standard” User!

Remediate and Enforce Settings

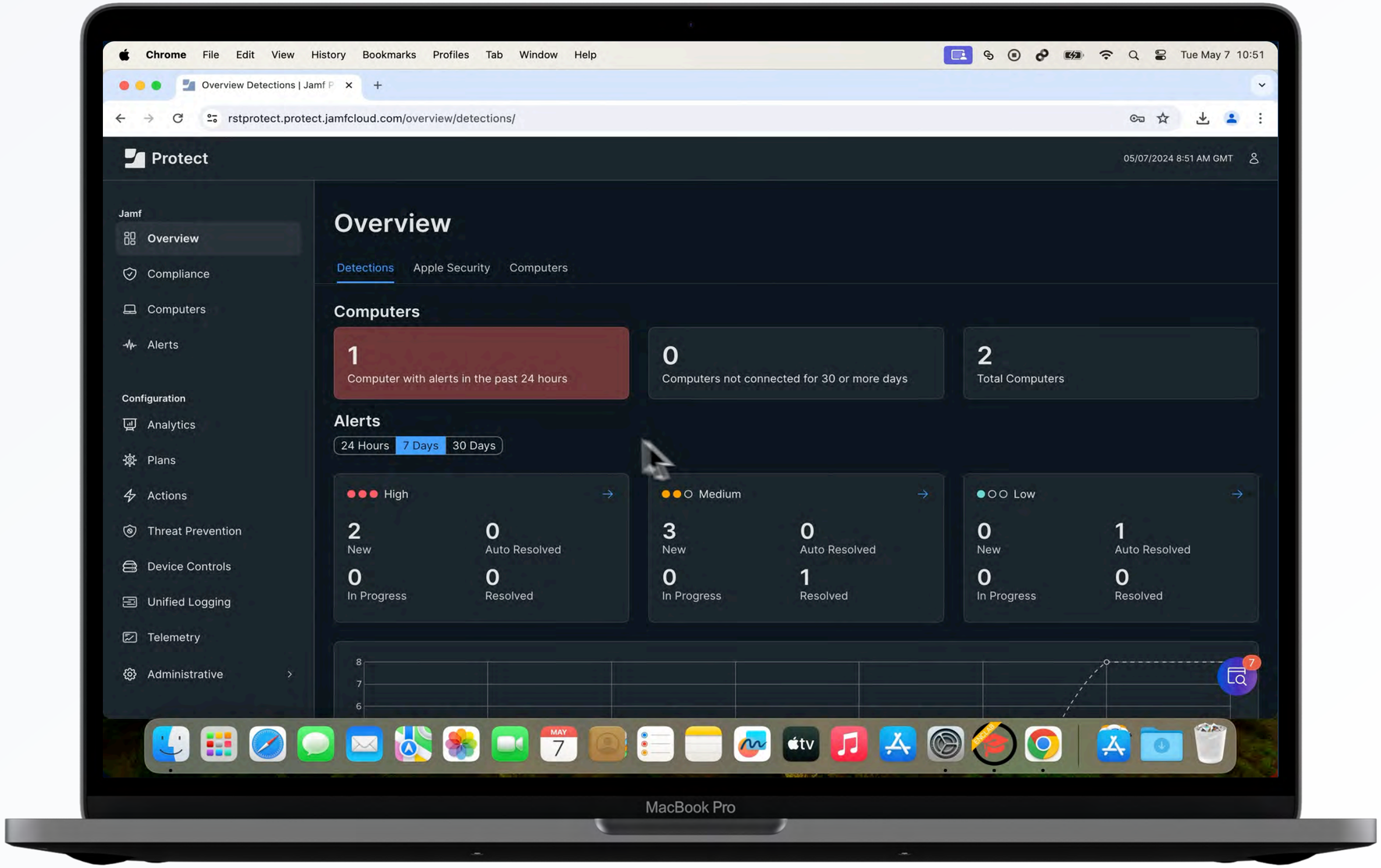
Non-Compliant Device:
Firewall-setting - not enforced

Do the “Admin” thing!

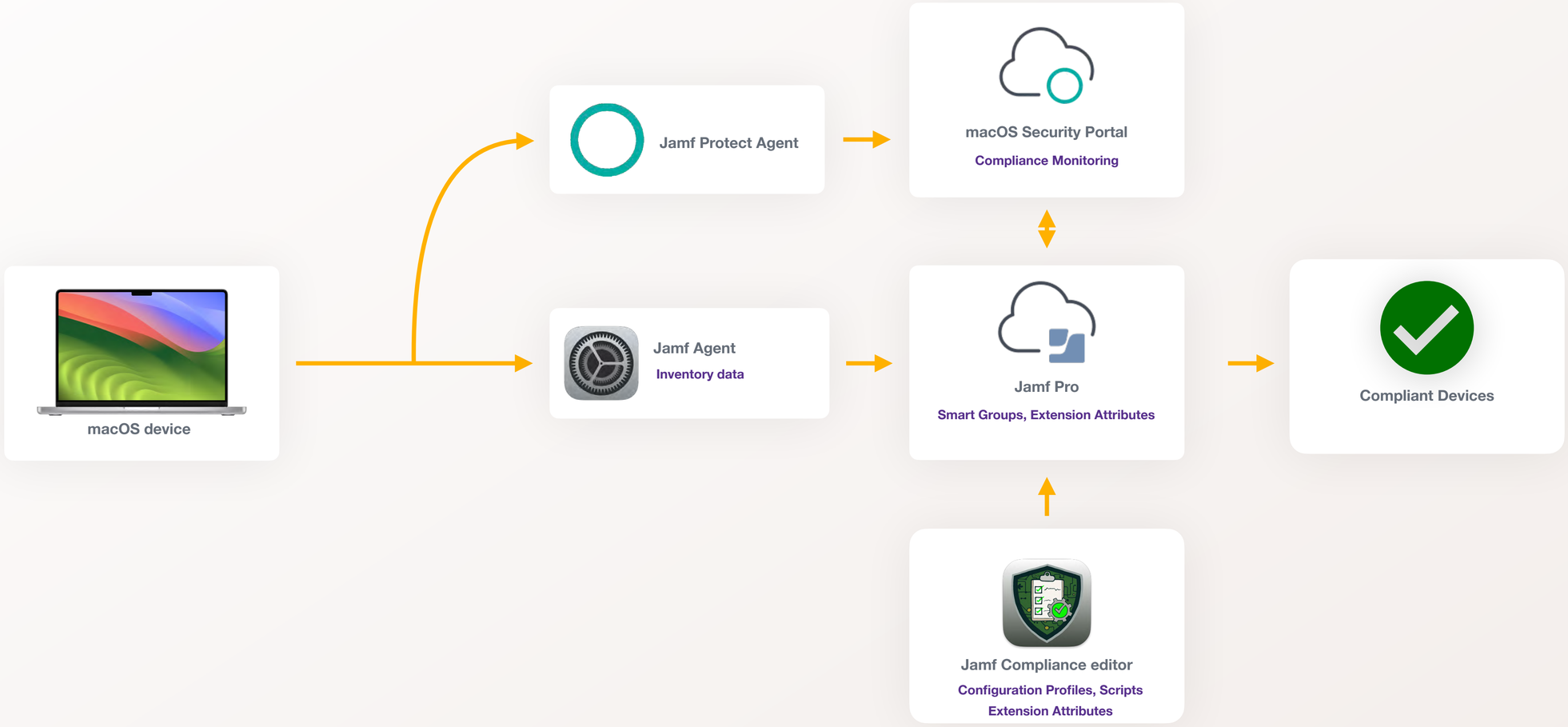


Remediate and Enforce Settings

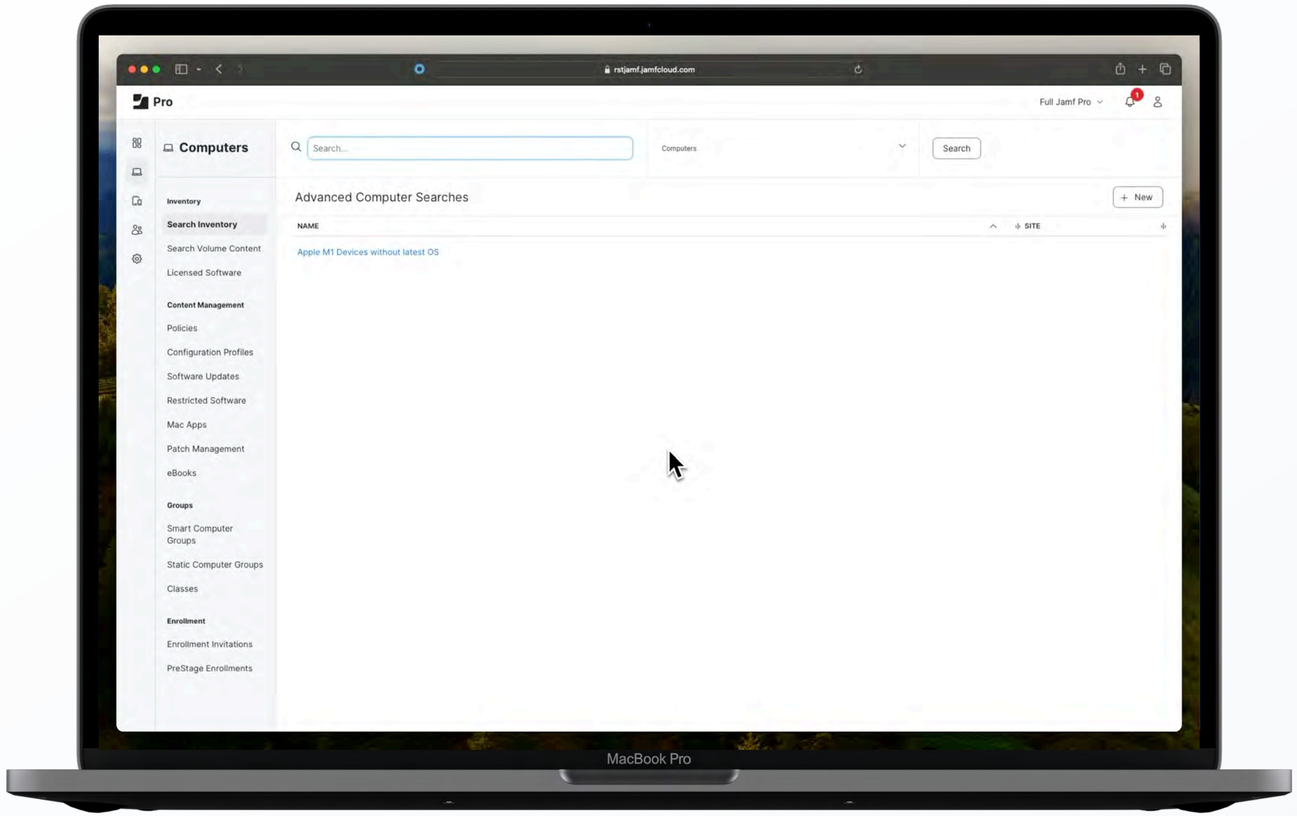
Compliance Monitoring:
Show Non-Compliant devices



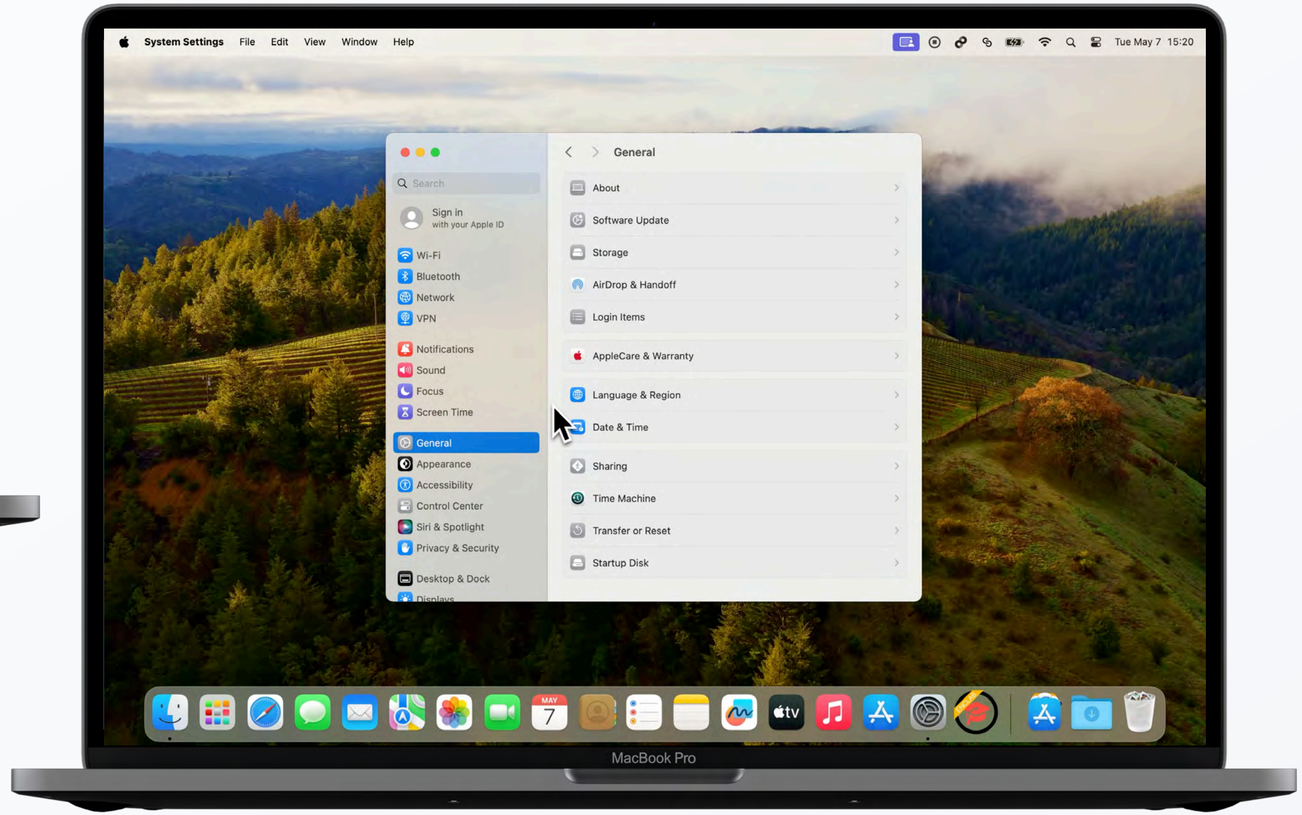
Behind the scenes



Remediate and Enforce Settings

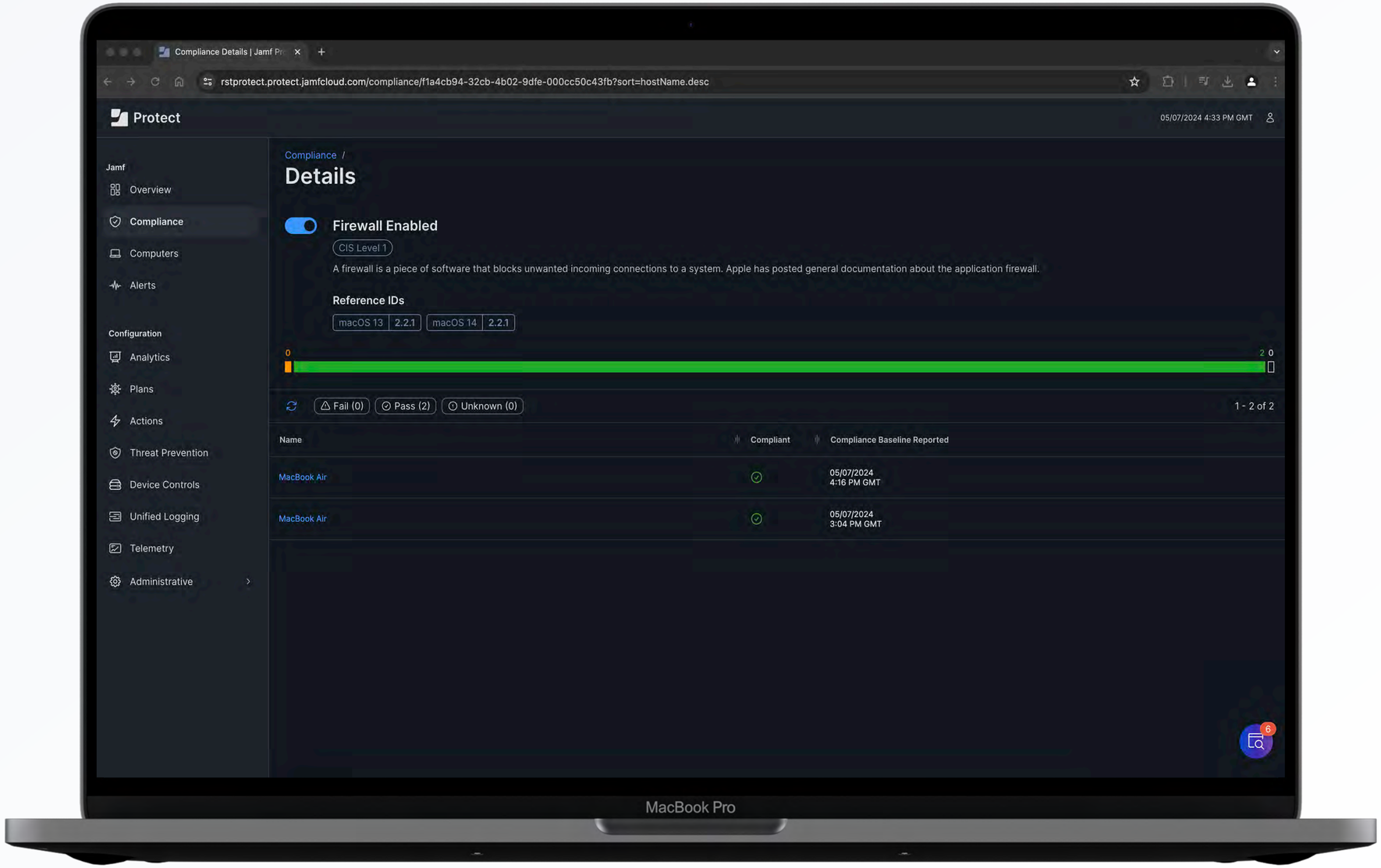


Compliant Device:
Firewall-setting - enforced

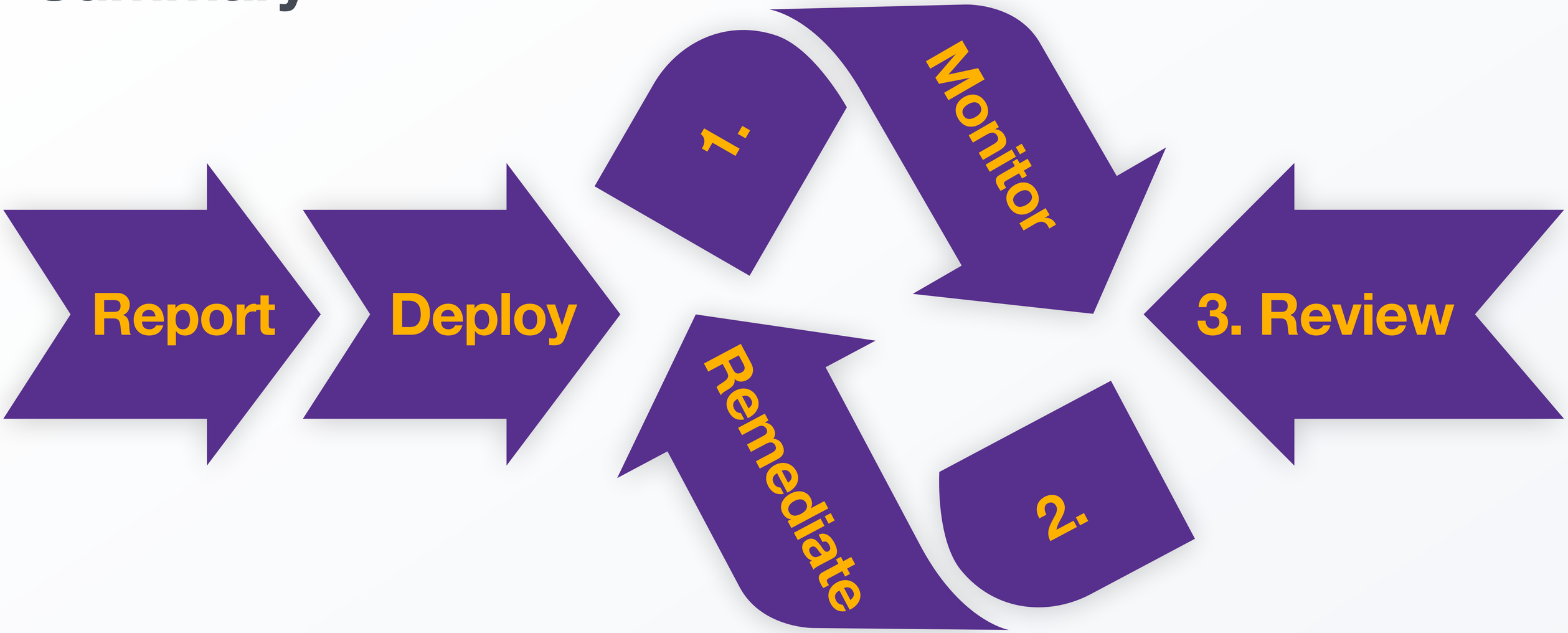


Review Compliance Status

Compliance Review:
Show Compliant devices



Summary



Thank You!

JAMF NATION LIVE