

Compliance leicht gemacht:

**Ein einfacher Ansatz zur Verbesserung
der Geräte-Compliance mit Jamf**



René Stiel

Senior Sales Engineer
DACH

Agenda

1 | Ein Überblick: Compliance-Vorschriften und Ihre Bedeutung

Arten, Konsequenzen, Vorteile, Frameworks

2 | Compliance Monitoring

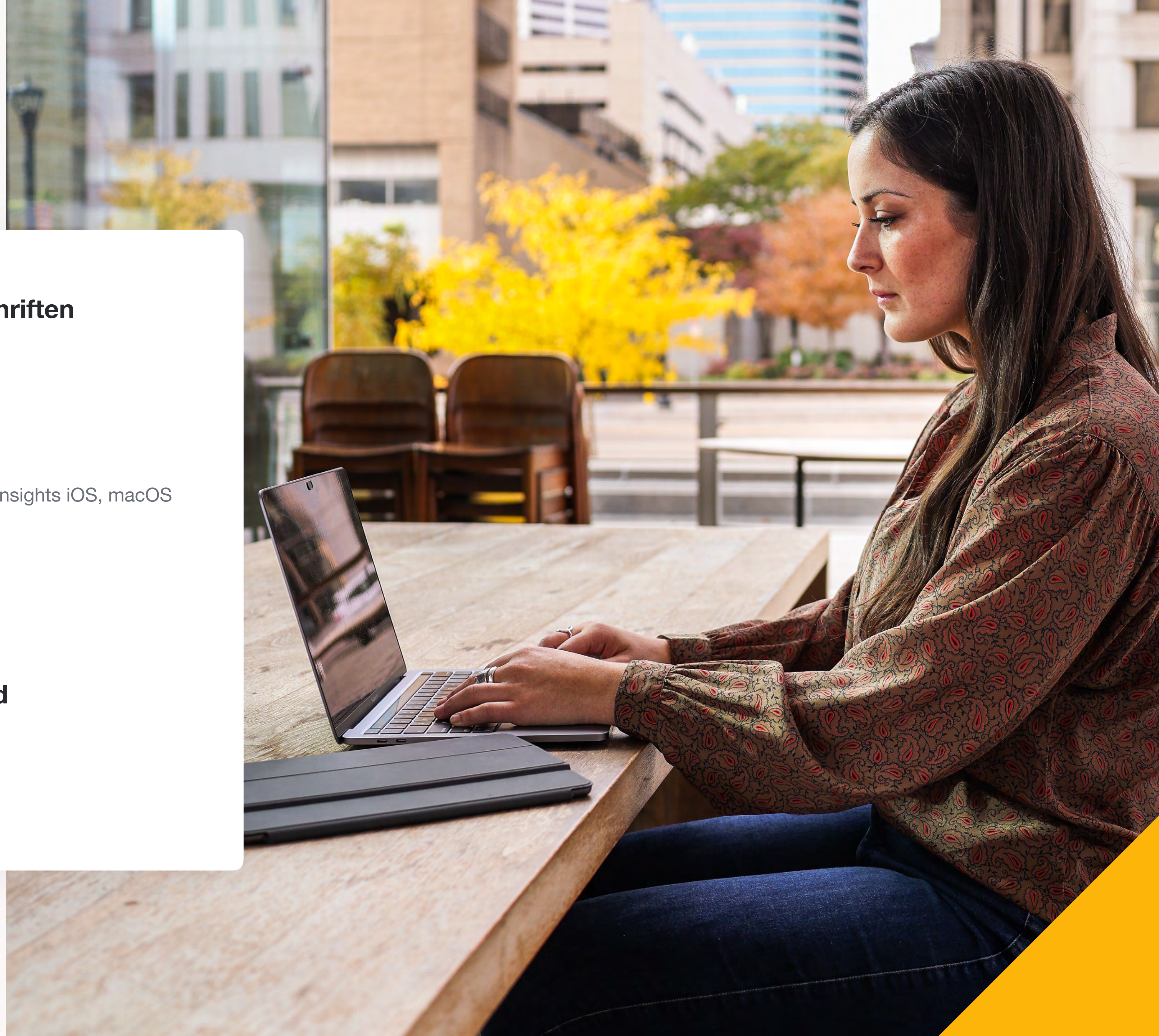
Compliance Dashboard, CVE-Monitoring, App-Insights iOS, macOS

3 | Compliance mit Jamf

Compliance Editor, Jamf Pro

4 | Compliance-Mängel beheben und Vorgaben erzwingen

Jamf Pro, Jamf Protect



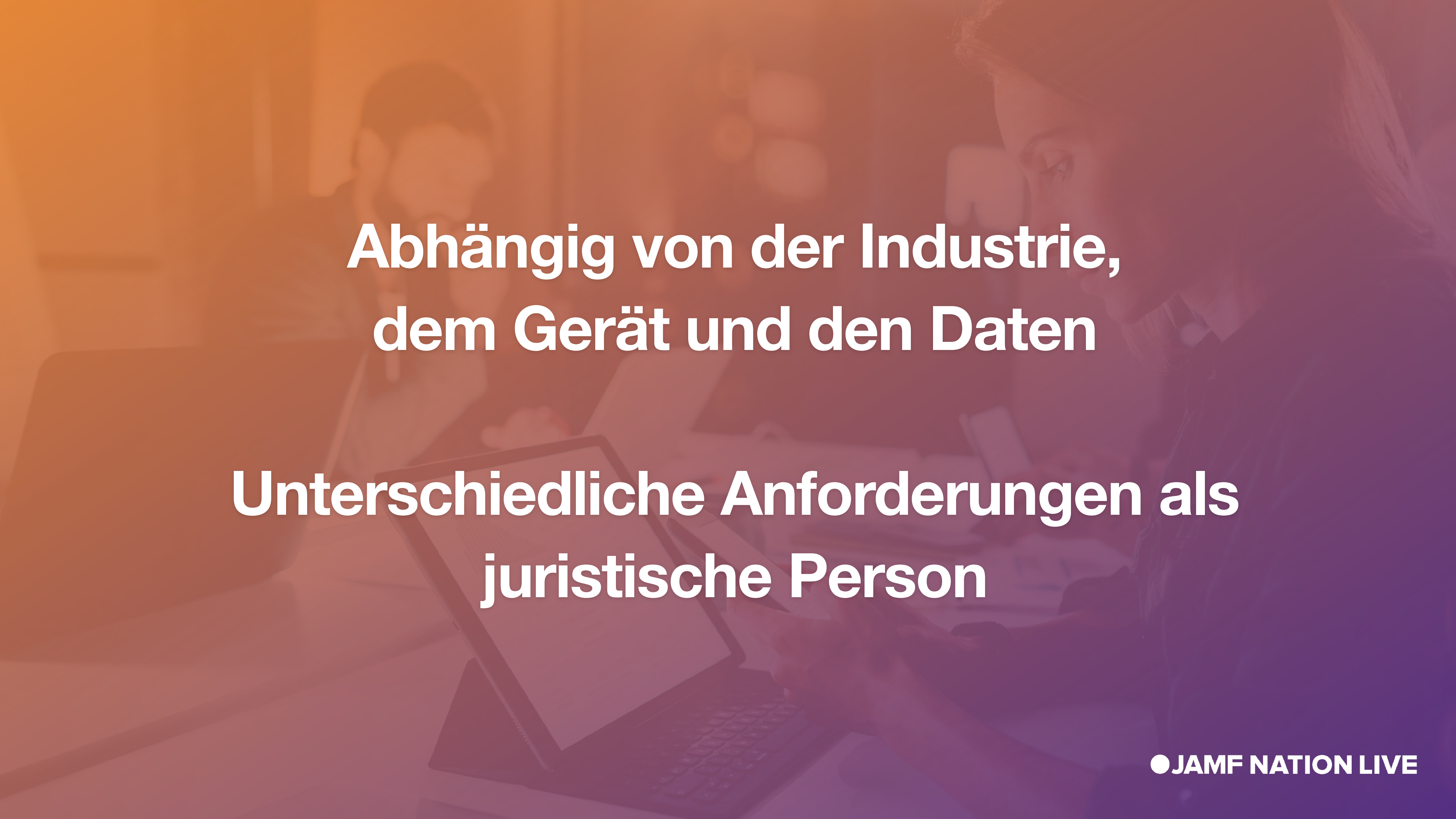
Ein Überblick: Compliance- Vorschriften und ihre Bedeutung



Einhaltung von Gesetzen

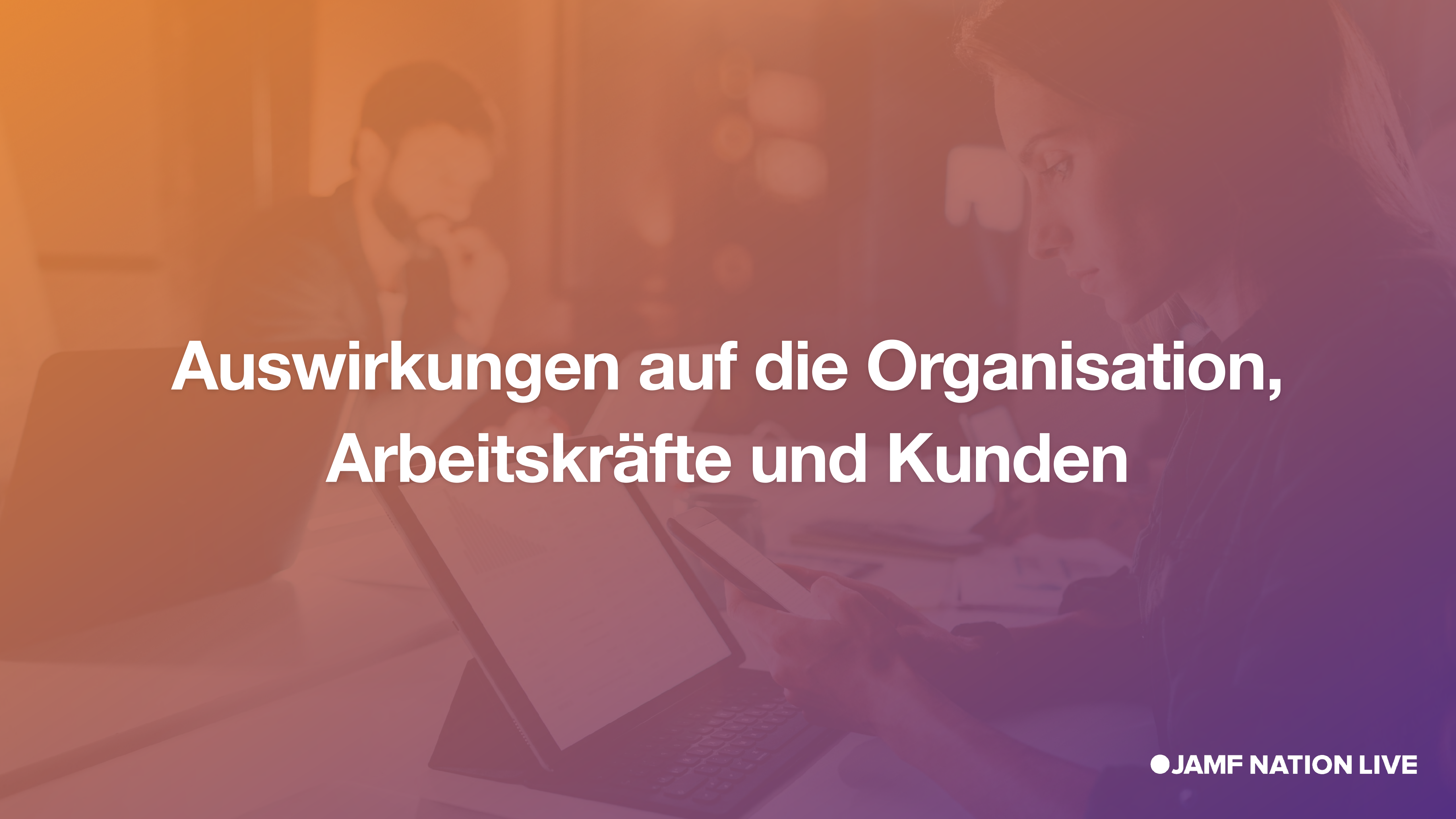
Industriestandards

Datenschutz- und Sicherheitsanforderungen



**Abhängig von der Industrie,
dem Gerät und den Daten**

**Unterschiedliche Anforderungen als
juristische Person**



Auswirkungen auf die Organisation, Arbeitskräfte und Kunden

Arten der Compliance



Gesetzliche Bestimmungen



Industrie-Normen



Security Compliance Richtlinien



Unternehmensregeln und Verantwortlichkeiten

Konsequenzen von Non-Compliance



**Datenschutzverstöße und
Datenverluste**



**Monetäre Verluste
(Geldbußen, Sanktionen)**



**Verlust von Kunden
oder Arbeitsplätzen**



Verlust der Reputation

Vorteile der Compliance

Abgesehen von der Vermeidung von Geldstrafen und Sanktionen bringt die Einhaltung der Sicherheitsvorschriften in einem Unternehmen mehrere Vorteile mit sich, wie z.B.:

- ▶ **Schutz der Reputation Ihres Unternehmens**
- ▶ **Abmilderung von Sicherheitsrisiken**
- ▶ **Stärkung des Kundenvertrauens**
- ▶ **Verbesserung der betrieblichen Effizienz**
- ▶ **Dem Wettbewerb immer einen Schritt voraus**



Compliance Frameworks



Baselines und Benchmarks

Eine "**security baseline**" ist eine **Reihe von Sicherheitsrichtlinien (Prüfkatalog)**, die ein Unternehmen auf seinen Geräten konfigurieren möchte.

Sobald diese eingerichtet sind, müssen sie laufend überprüfen, ob die Richtlinien bestehen bleiben und die Geräte den Vorschriften entsprechen.

Dieses **System zur Bewertung der Einhaltung der Vorschriften** ist der "**benchmark**".



Warum sollten **Baselines** und **Benchmarks** eingeführt werden?

Einige Regierungsbehörden verlangen, dass alle Computer, die mit ihren Systemen und Daten interagieren, einem bestimmten Benchmark unterliegen, der nur wenige Ausnahmen zulässt. Viele regulierte Industrien werden auch verpflichtet sein einen Sicherheits-Benchmark einzuführen.

- ▶ **IT- und Informations-Sicherheitsabteilungen müssen zusammenarbeiten**
- ▶ **Gleichgewicht zwischen Informationssicherheit und Benutzerproduktivität**
- ▶ **Verschiedene Geräte mit unterschiedlichen Risikokategorien**

Aufklärung der Endnutzer

In Compliance-Schulungen können sich die Mitarbeiter mit den Gesetzen und Vorschriften vertraut machen, die für ihre Arbeit gelten. Es gibt viele Arten von Compliance-Schulungsprogrammen, von denen einige branchenübergreifend gelten und andere wiederum berufs- oder branchenspezifisch sind.

- ▶ **Compliance-Schulungen sind oft verpflichtend und zeitkritisch**
- ▶ **Damit ein Unternehmen und seine Mitarbeiter die Gesetze einhalten können, müssen sie Schulungsprogramme in der Regel innerhalb eines bestimmten Zeitrahmens absolvieren**
- ▶ **Die Schulungen müssen mindestens jährlich wiederholt bzw. aufgefrischt werden**

74 %

**der Datenschutzverletzungen
waren auf den Faktor Mensch
zurückzuführen**

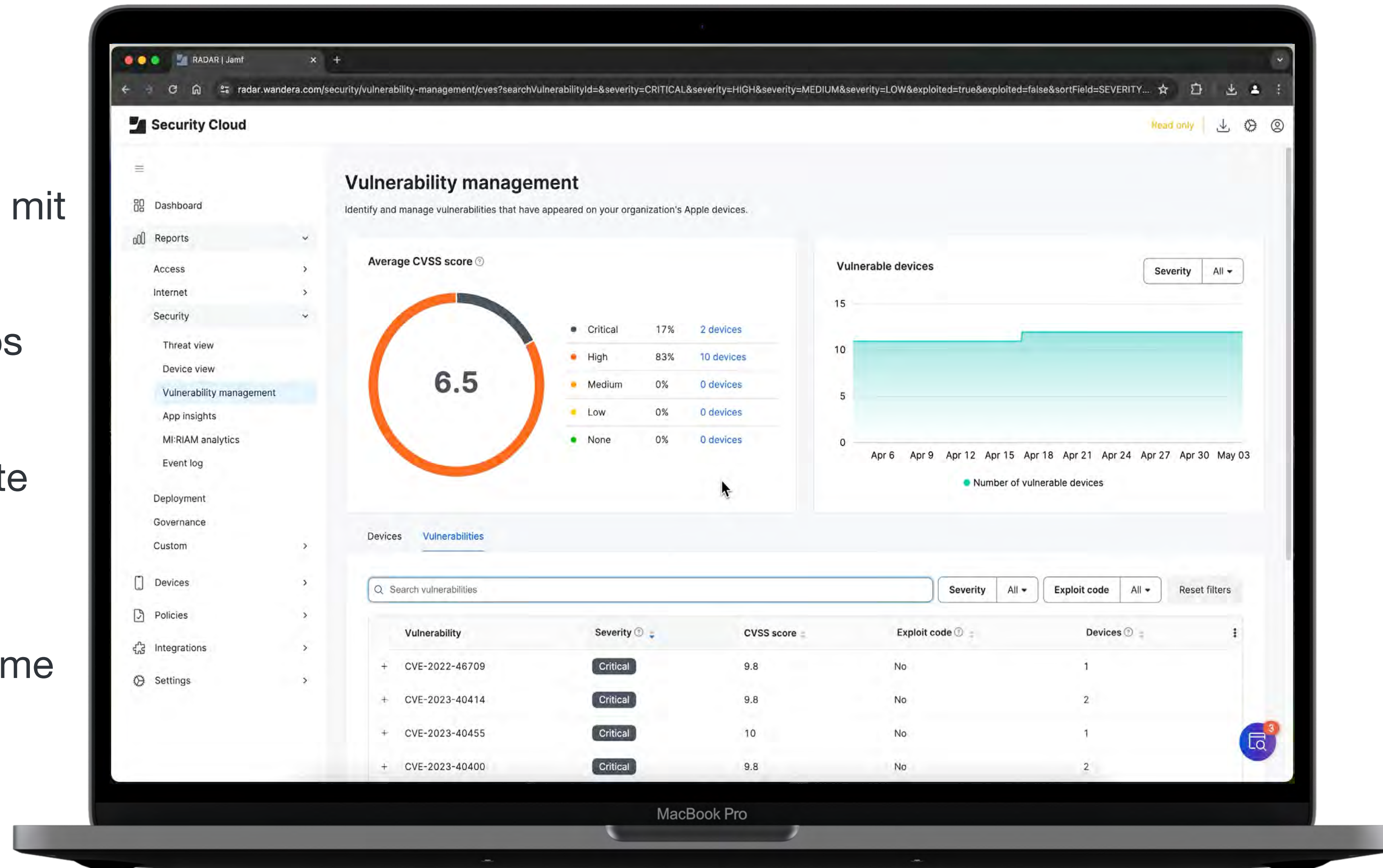
Bericht über die Untersuchung von
Datenschutzverletzungen 2023, Verizon



Compliance und Schwachstellen-Monitoring mit Jamf Protect

Schwachstellen-Management in Jamf Protect

- ▶ Detaillierte Berichte über Apple-Geräte mit **bekannten Sicherheitslücken**
- ▶ Built-in **CVE reporting** für OS und Apps
- ▶ **Automatische Risikoerhöhung**, Geräte mit risikobehafteten Betriebssystemen erhalten einen erhöhten Risikostatus
- ▶ Benutzer können über unsichere Systeme **benachrichtigt** werden

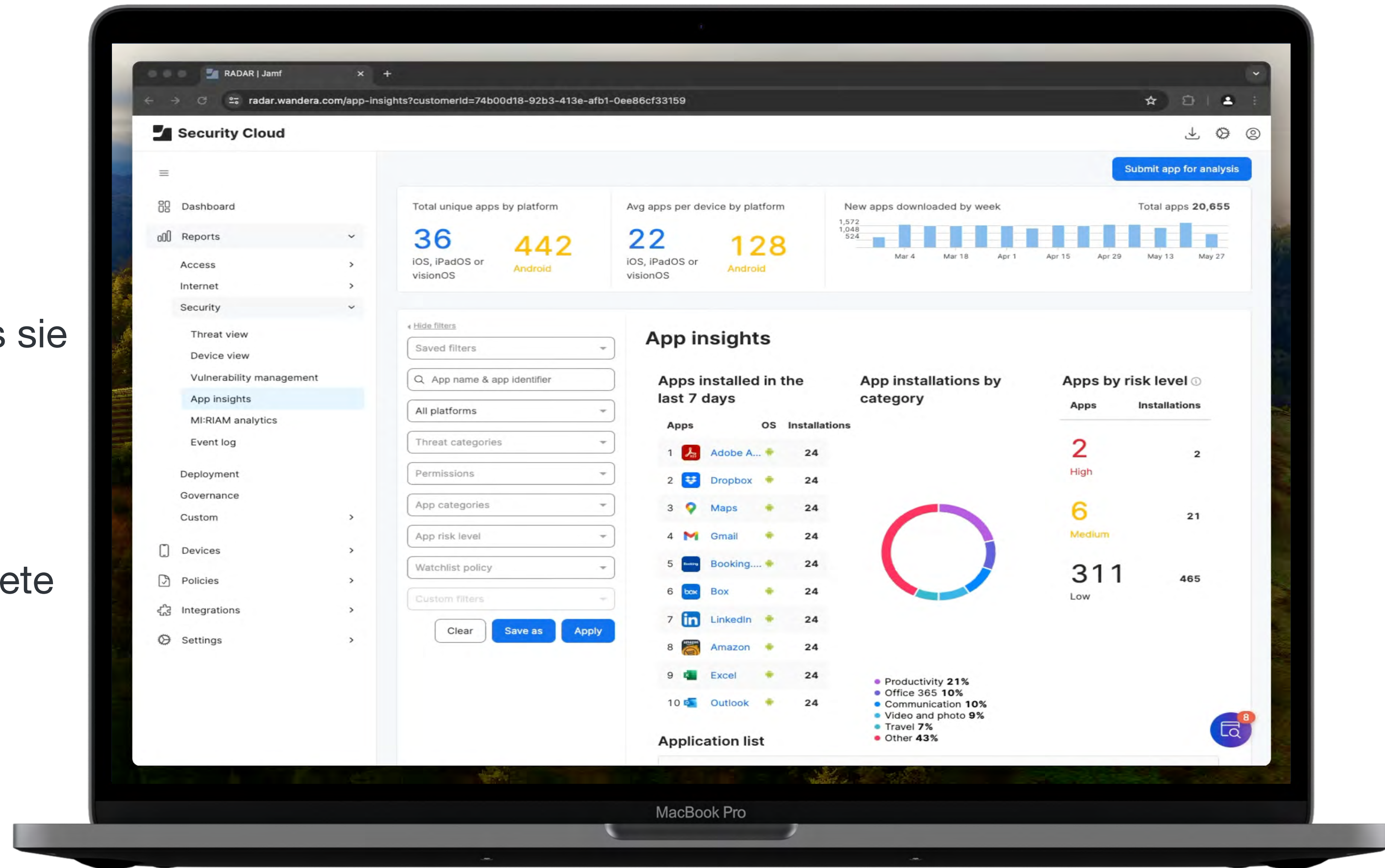


App Insights in Jamf Protect

- ▶ Gibt **Informationen** über die auf Ihren Geräten installierten Apps zurück, einschließlich ihrer **Versionen**, **Berechtigungen** und des **Risikos**, das sie darstellen können.

Identifizieren:

- ▶ Wie viele Nutzer verwenden eine veraltete oder riskante Version einer App?
- ▶ Welche Apps **greifen Daten ab** - oder wurden **side-loaded**



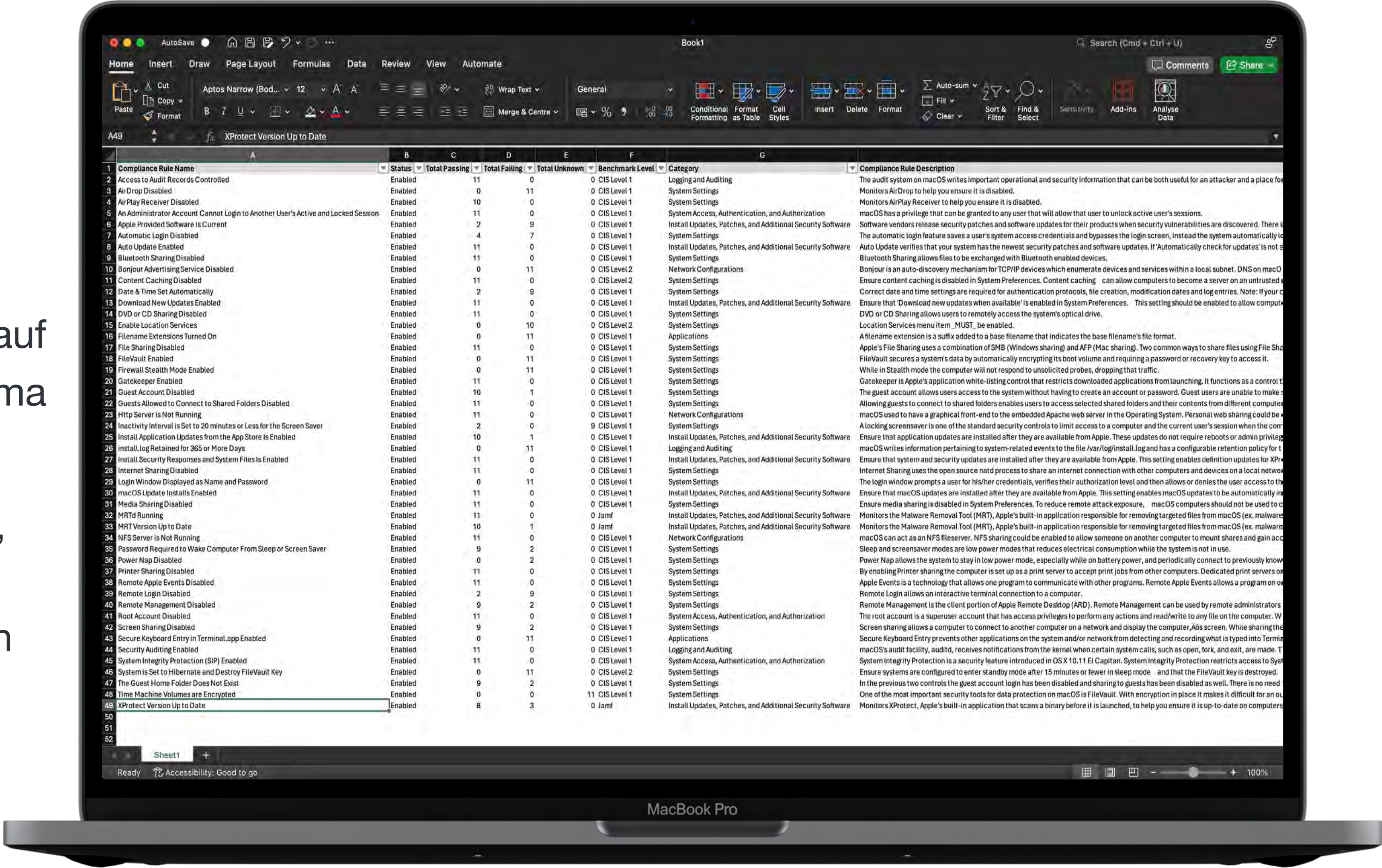
Compliance Baseline in Jamf Protect

- ▶ **Neues Dashboard** mit Widgets zur besseren Übersicht
- ▶ Compliance-Baseline Regel basierend auf dem **CIS benchmark** für macOS Sonoma
- ▶ **Mehr Transparenz** für Administratoren, um sicherzustellen, dass ihre Mac-Computer den Vorschriften entsprechen
- ▶ Das perfekte Werkzeug zur **Überwachung** der Wirksamkeit des Jamf Compliance Editors



Compliance Baseline in Jamf Protect

- ▶ **Neues Dashboard** mit Widgets zur besseren Übersicht
- ▶ Compliance-Baseline Regel basierend auf dem **CIS benchmark** für macOS Sonoma
- ▶ **Mehr Transparenz** für Administratoren, um sicherzustellen, dass ihre Mac-Computer den Vorschriften entsprechen
- ▶ Einfaches **Erstellen von Berichten**



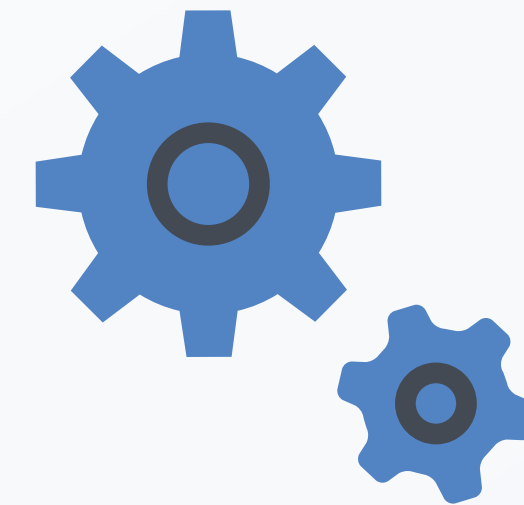
Compliance mit Jamf

Wie setzen wir unsere Compliance-Baseline durch?

1. Zur CIS-Website gehen
2. Lösungen > Benchmarks
3. Formular ausfüllen
4. Eine E-Mail erhalten



5. Benchmark-Webseite besuchen
6. Gewünschten Benchmark suchen
7. PDF herunterladen
8. PDF lesen



9. Alle benötigten Skripte/Configs erstellen
10. In Jamf Pro hochladen
11. Auf Geräte verteilen
12. Testen

Center for Internet Security

CIS Apple macOS 14.0 Sonoma

v1.0.0 - 10-16-2023

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>
```

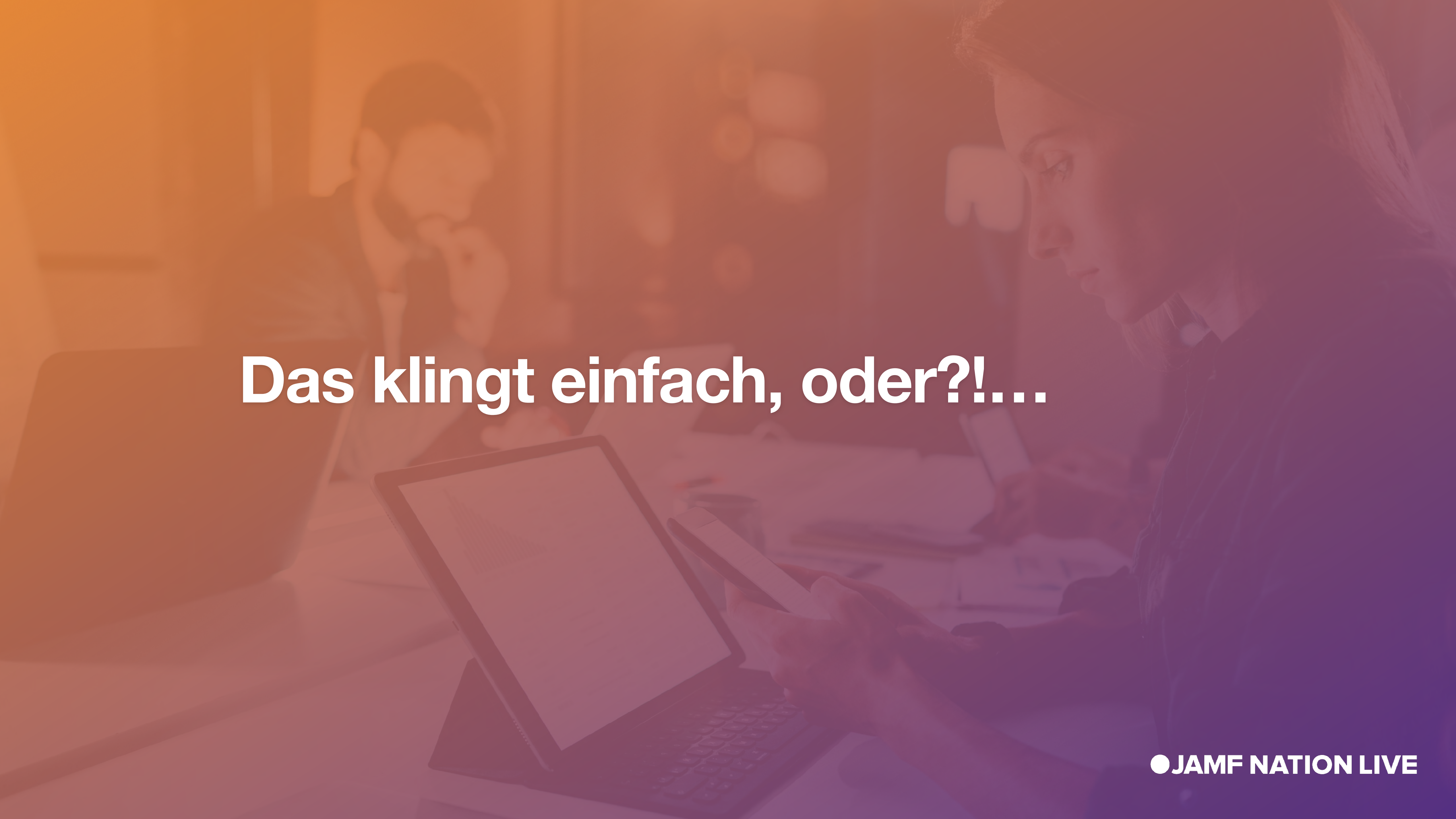
For the <value>, use either 1, specific services, or 2, essential services only.

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/>`





Das klingt einfach, oder?!...

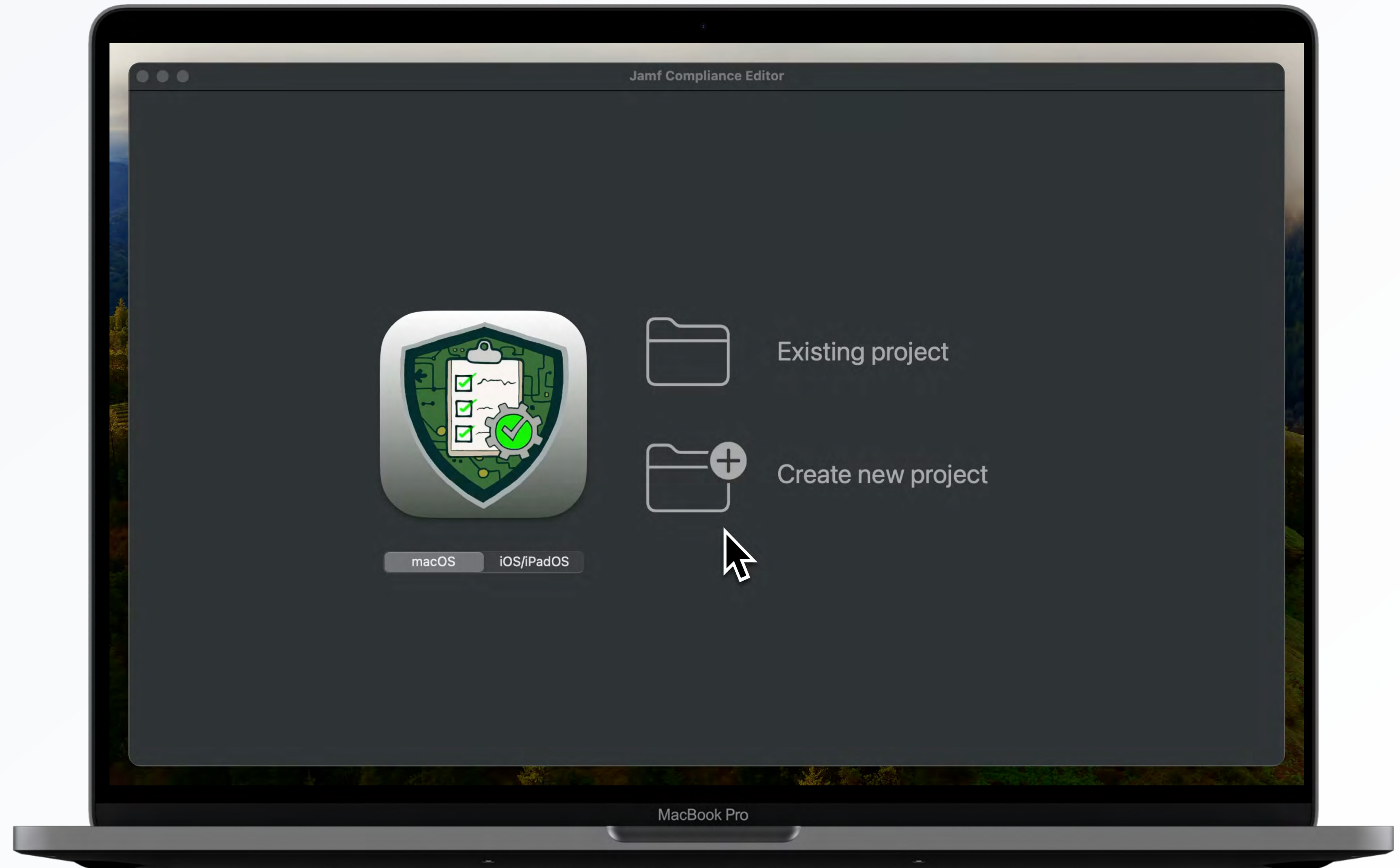
Jamf Compliance Editor

- ▶ **Automatische Erstellung** von **Baselines** für gängige **Compliance-Benchmarks**
- ▶ **Ein-Klick** Leitlinien Erstellung
- ▶ Leicht **anpassbare** Leitlinien für die spezifischen Bedürfnisse jeder Organisation
- ▶ Integration mit **Jamf Pro** für schnelle Verteilung/Durchsetzung
- ▶ **Detaillierte Berichte** erstellen



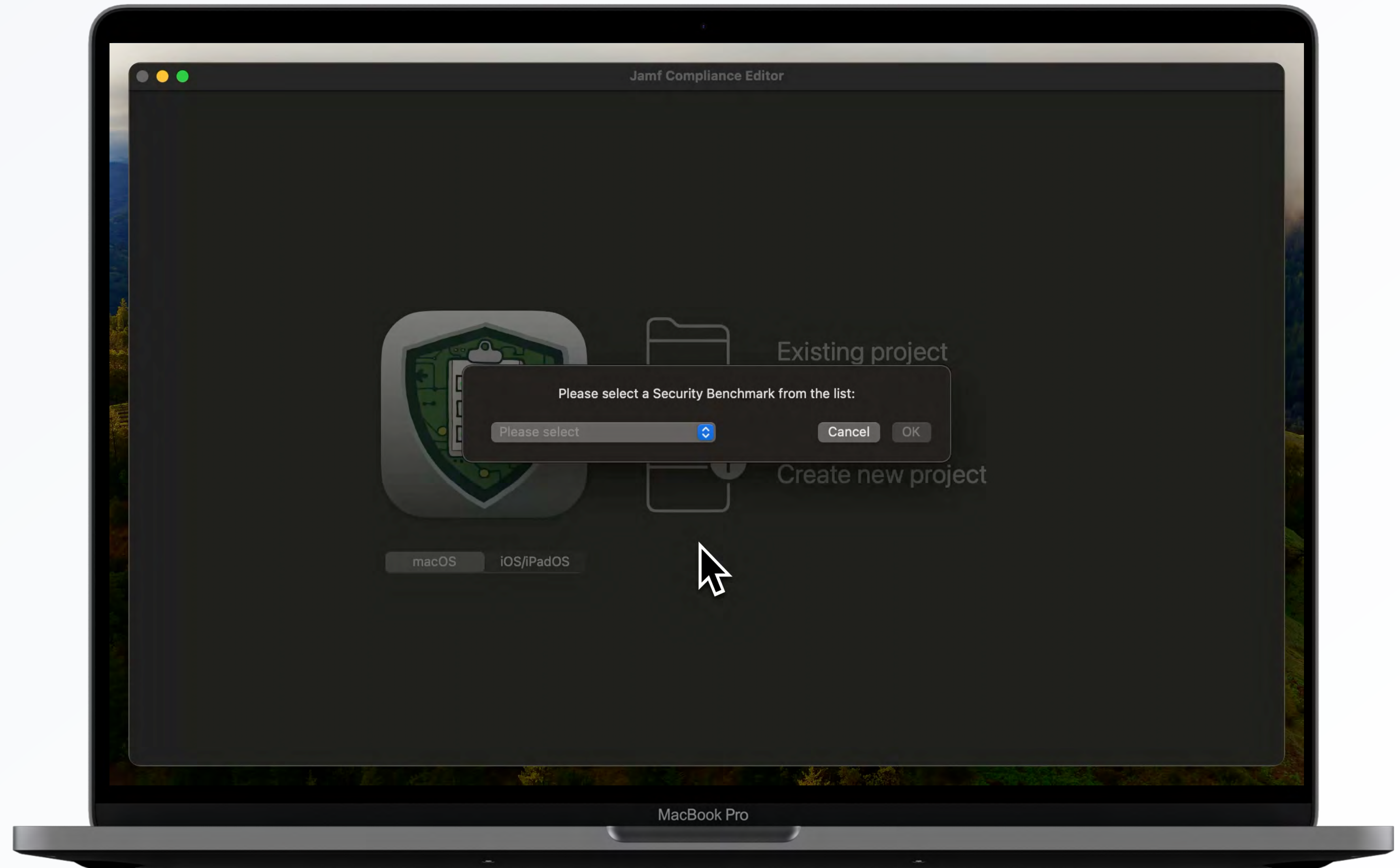
Wie stellen wir unsere Compliance-Baseline bereit?

Neues Projekt erstellen
OS auswählen



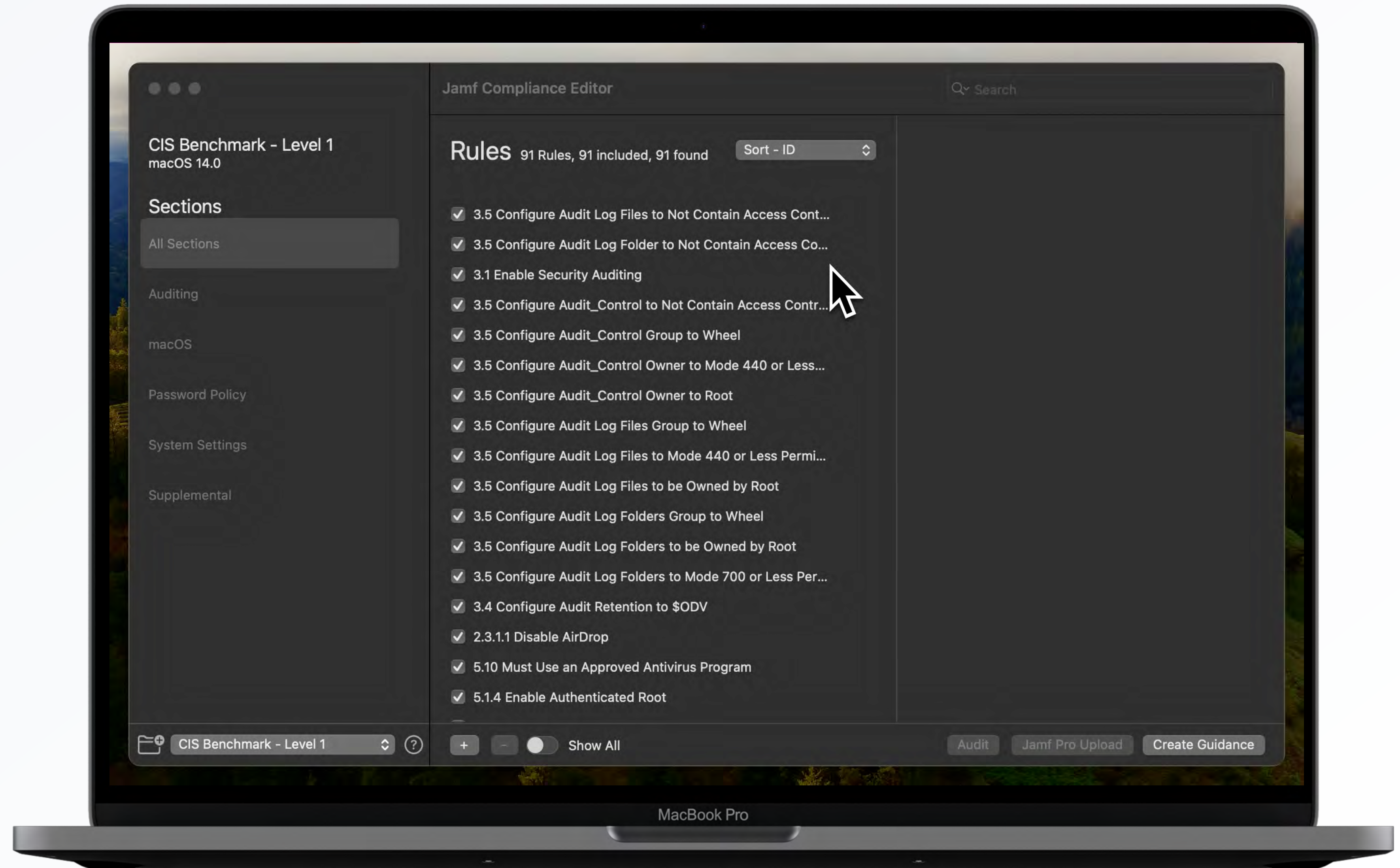
Wie stellen wir unsere Compliance-Baseline bereit?

Benchmark auswählen



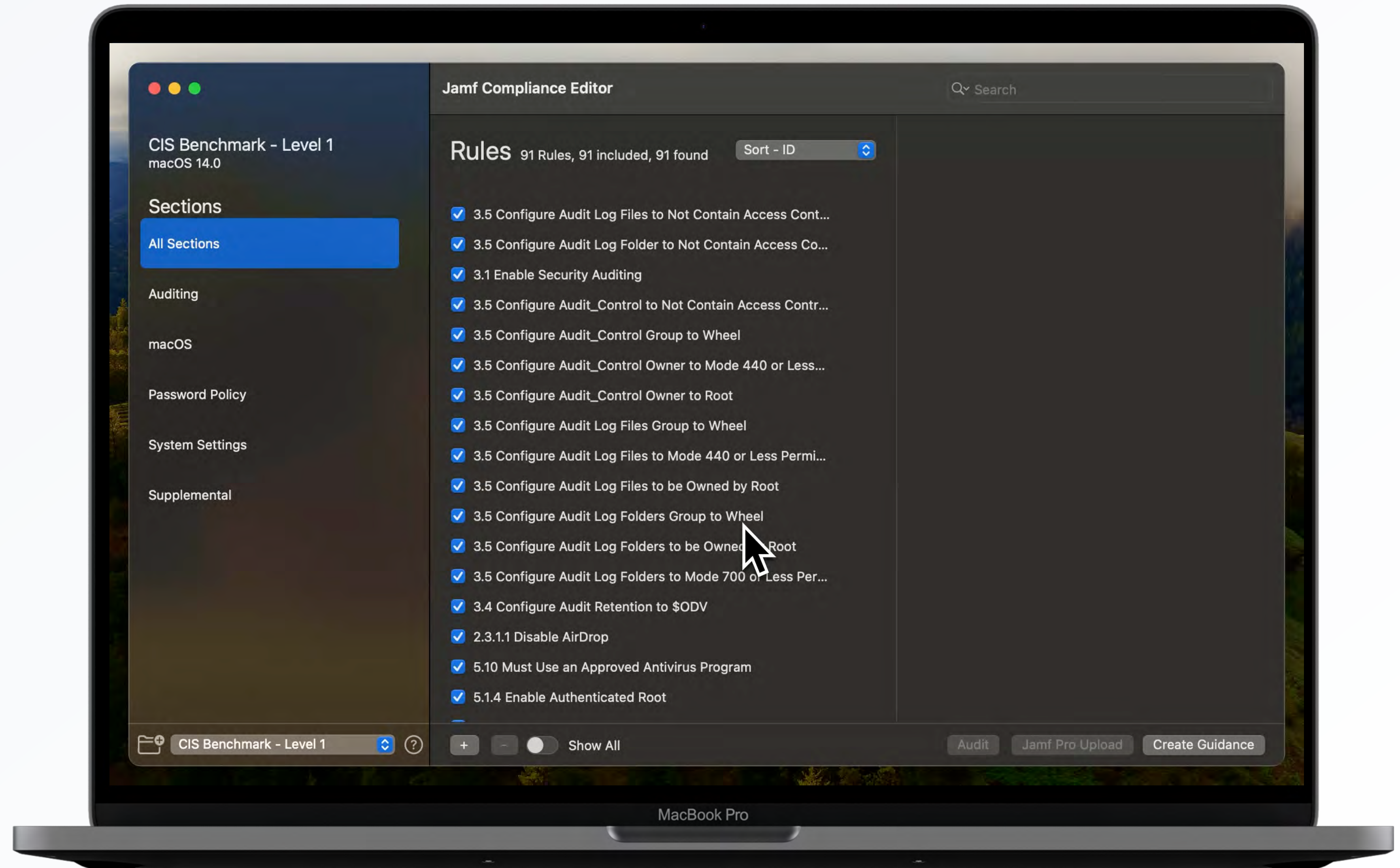
Wie stellen wir unsere Compliance-Baseline bereit?

Übersicht aller Regeln



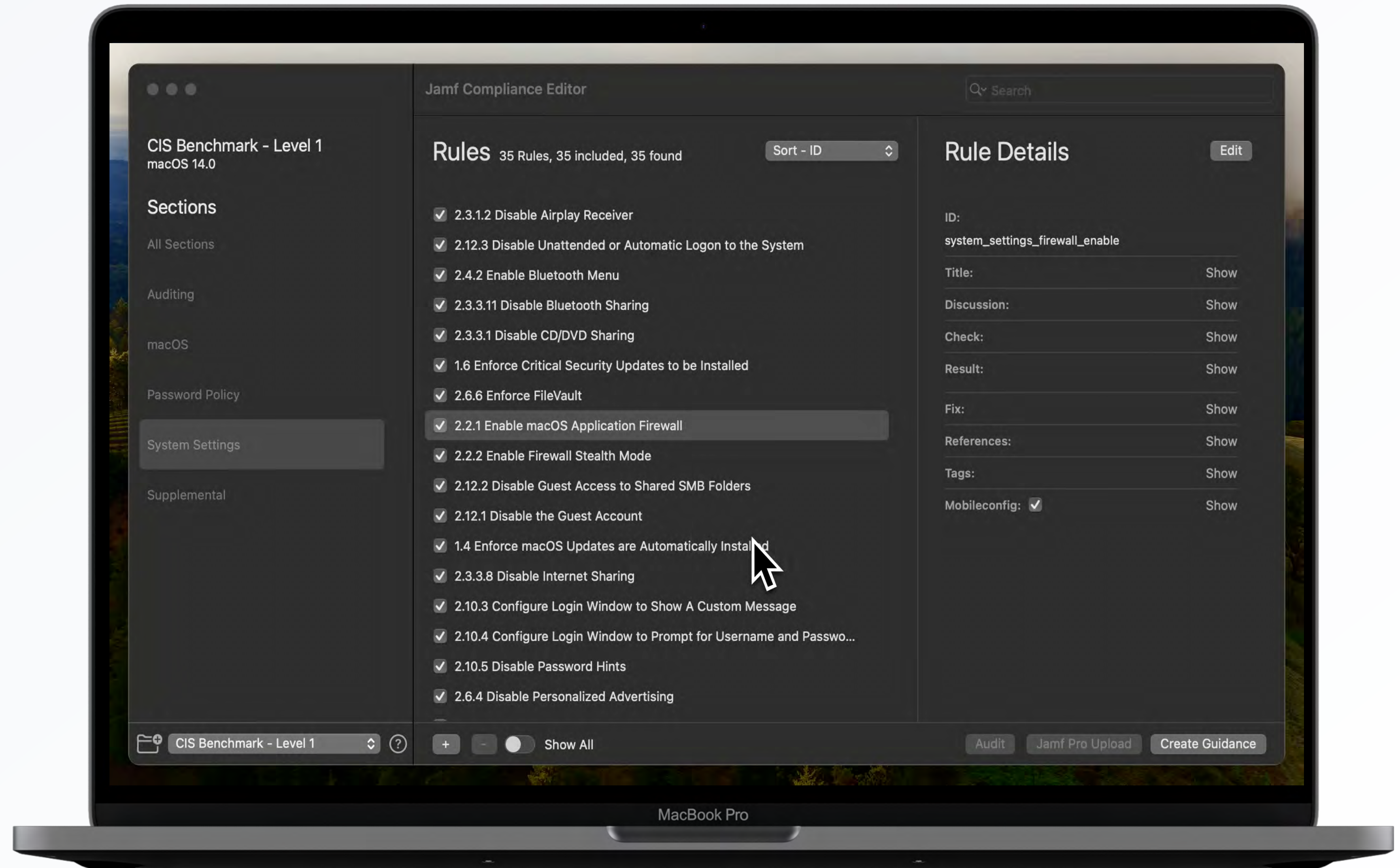
Wie stellen wir unsere Compliance-Baseline bereit?

Einzelne Regeln prüfen
z.B. (AirDrop or Firewall)



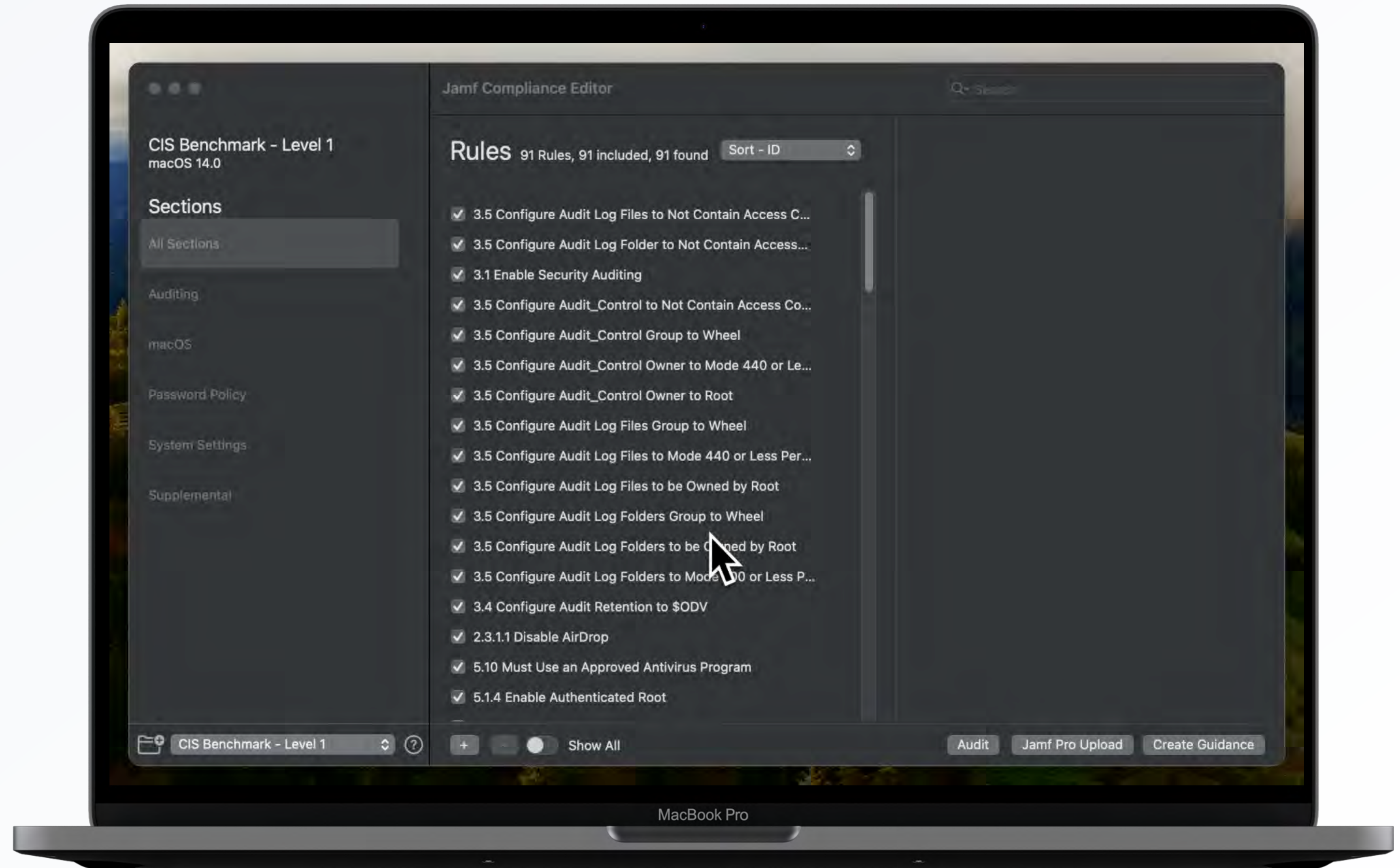
Wie stellen wir unsere Compliance-Baseline bereit?

Optional: Regeln bearbeiten
z.B. (Screen Saver)



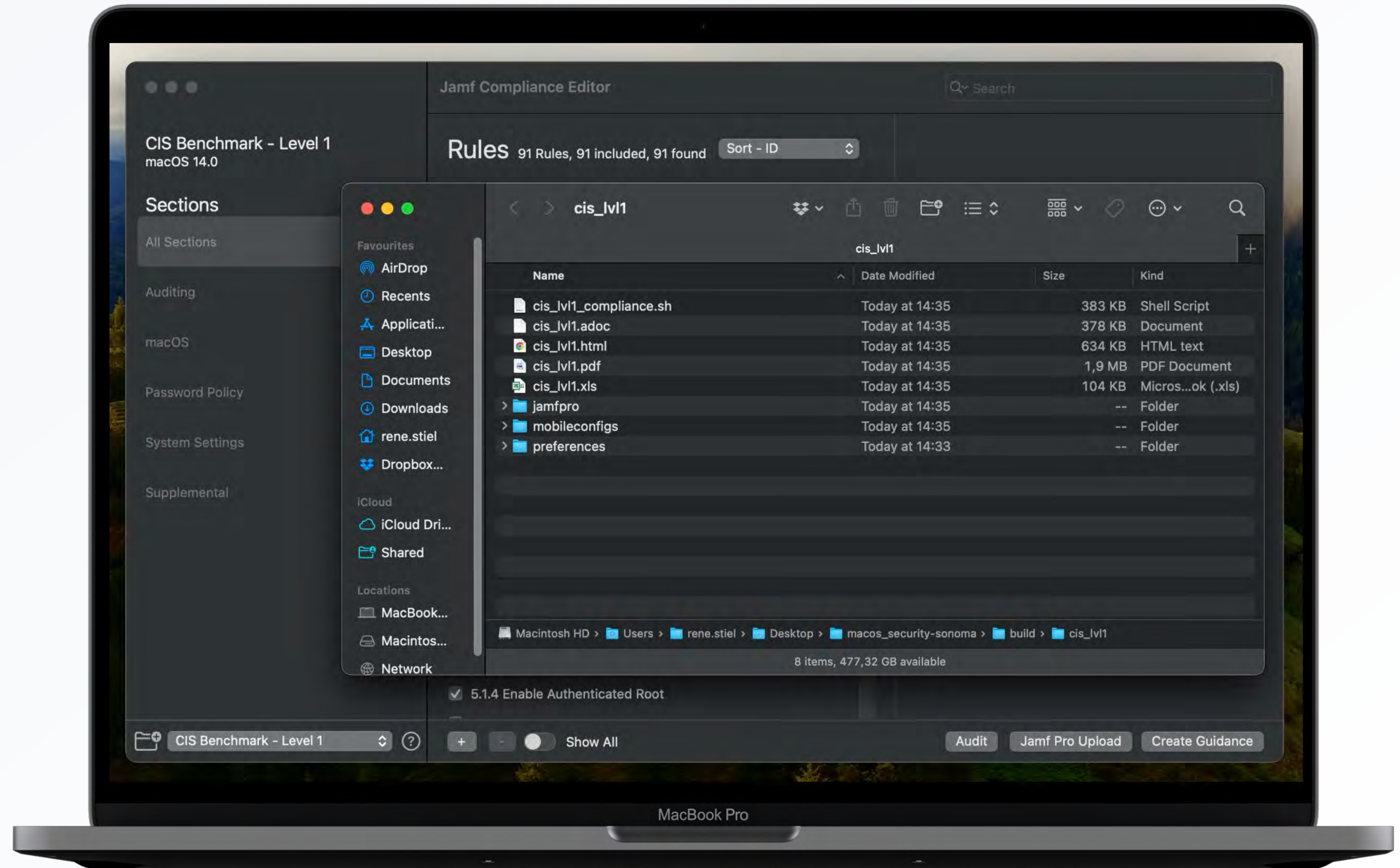
Wie stellen wir unsere Compliance-Baseline bereit?

Leitfaden erstellen



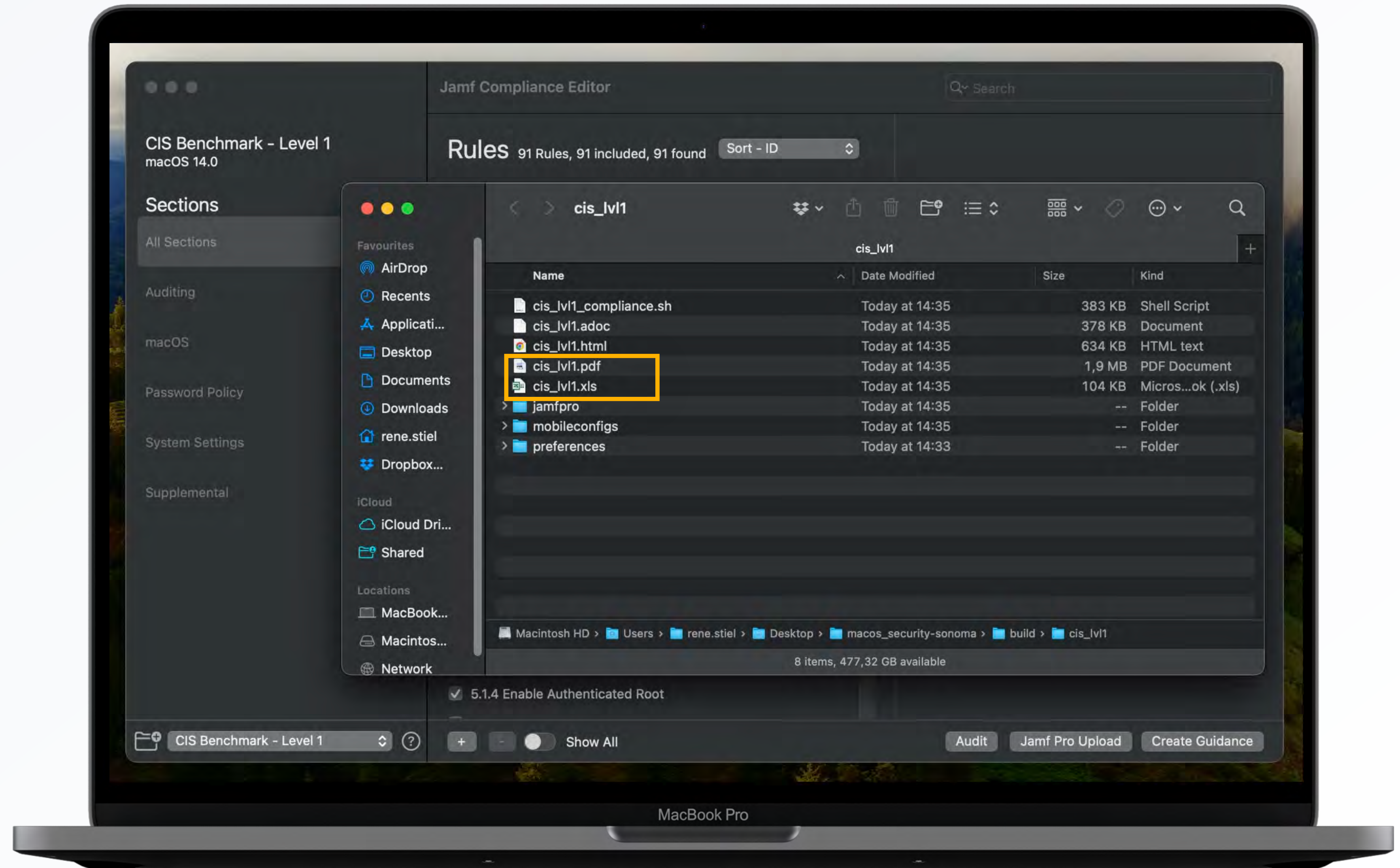
Wie stellen wir unsere Compliance-Baseline bereit?

Leitfaden erstellen



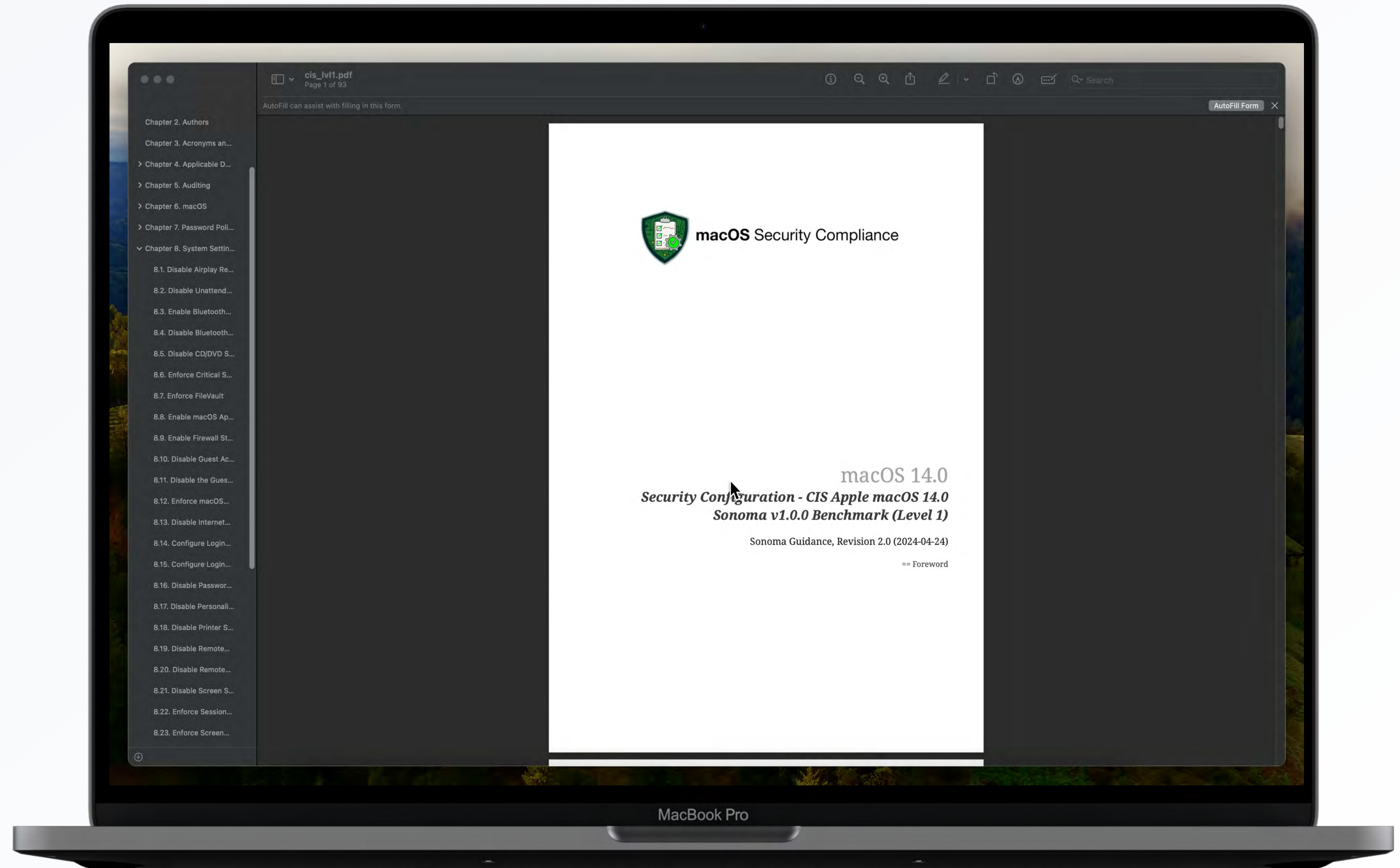
Wie stellen wir unsere Compliance-Baseline bereit?

Leitfaden erstellen



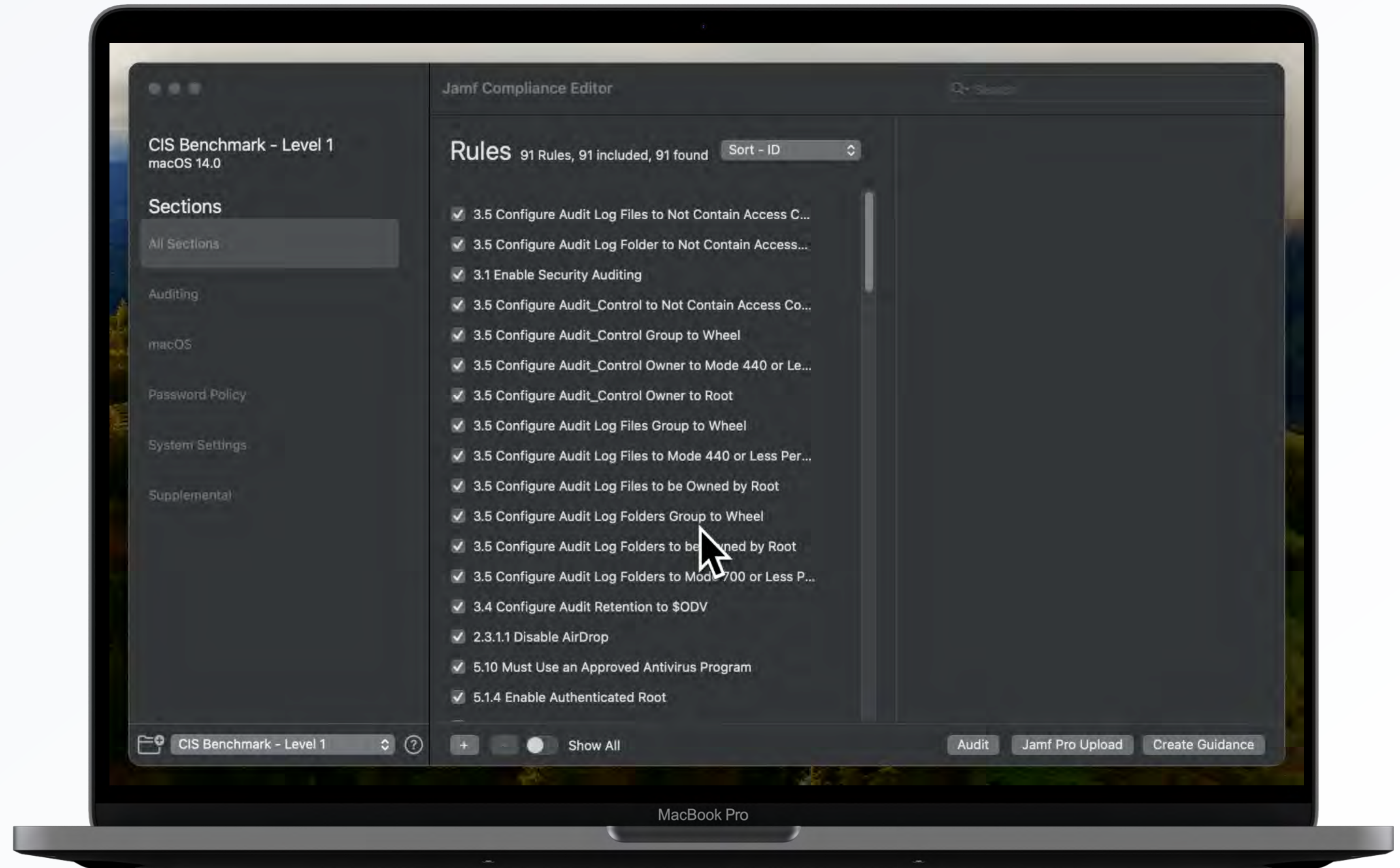
Wie stellen wir unsere Compliance-Baseline bereit?

Leitfaden erstellen



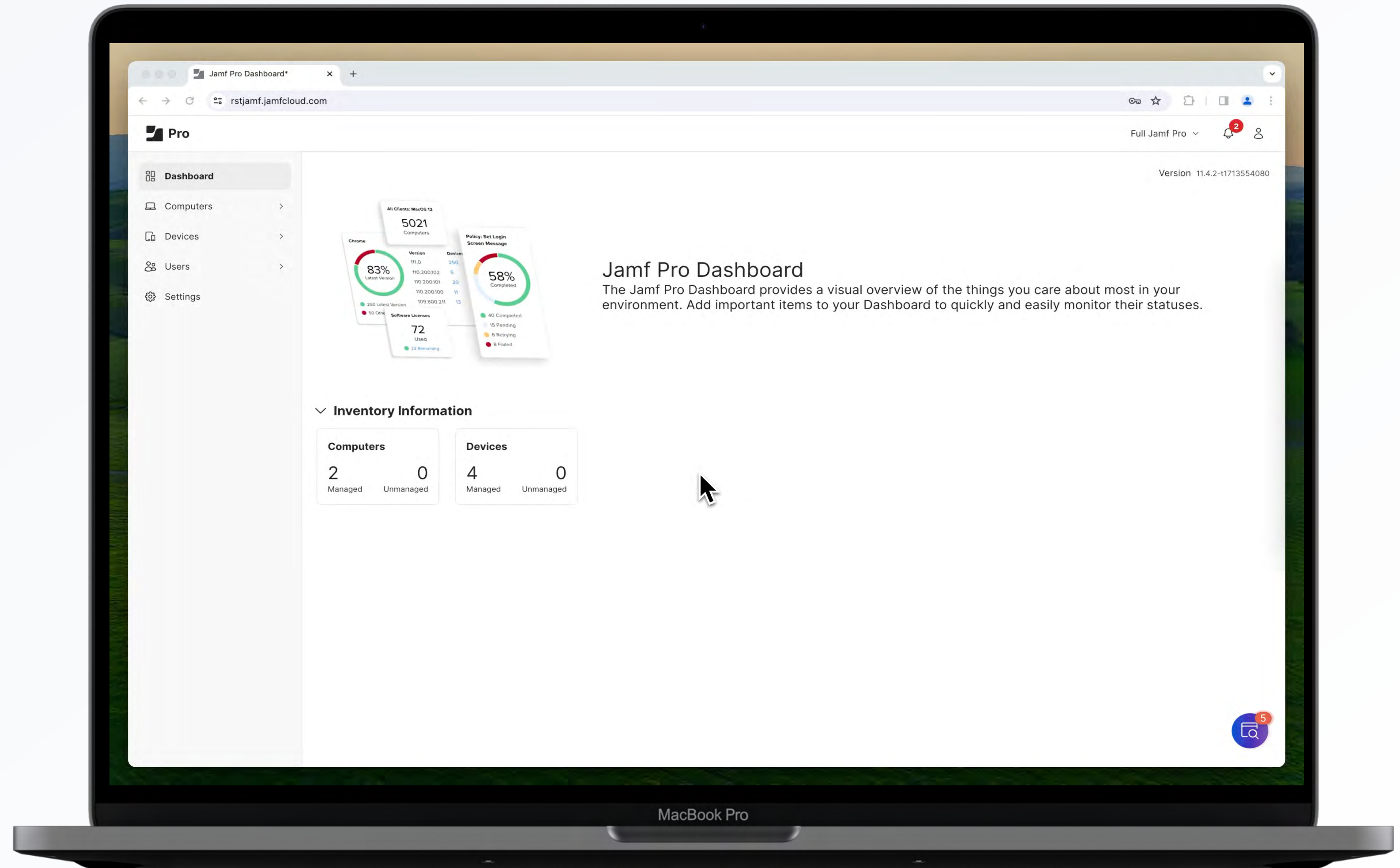
Wie stellen wir unsere Compliance-Baseline bereit?

In Jamf Pro hochladen



Wie stellen wir unsere Compliance-Baseline bereit?

Alle Profile und Skripte sind
in Jamf Pro verfügbar

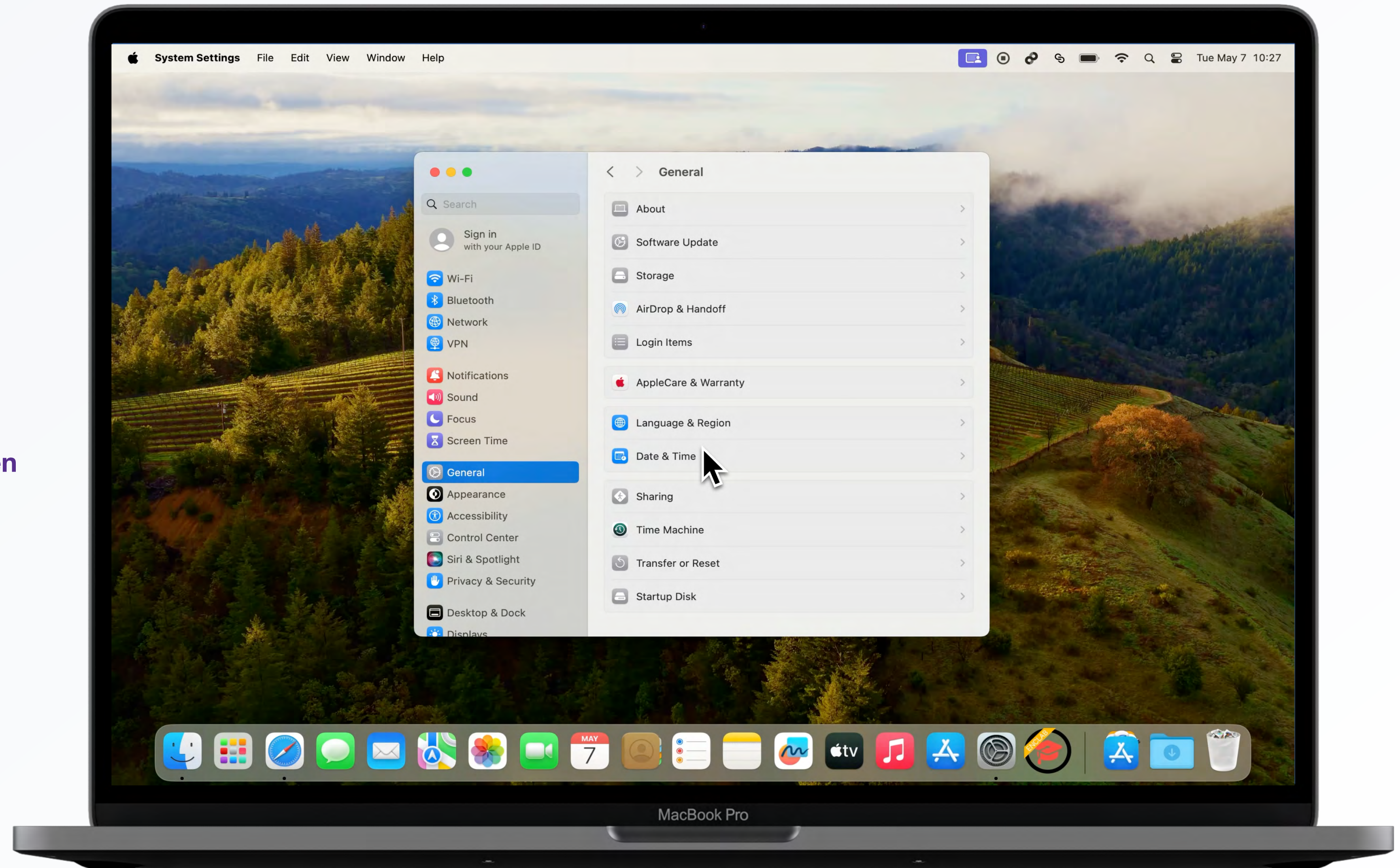


Compliance - Mängel beheben und Vorgaben erzwingen

Compliance - Mängel beheben und Vorgaben erzwingen

Nicht-Konformes Gerät:
Firewall-Einstellung nicht erzwungen

“Standard” Benutzer!



Compliance - Mängel beheben und Vorgaben erzwingen

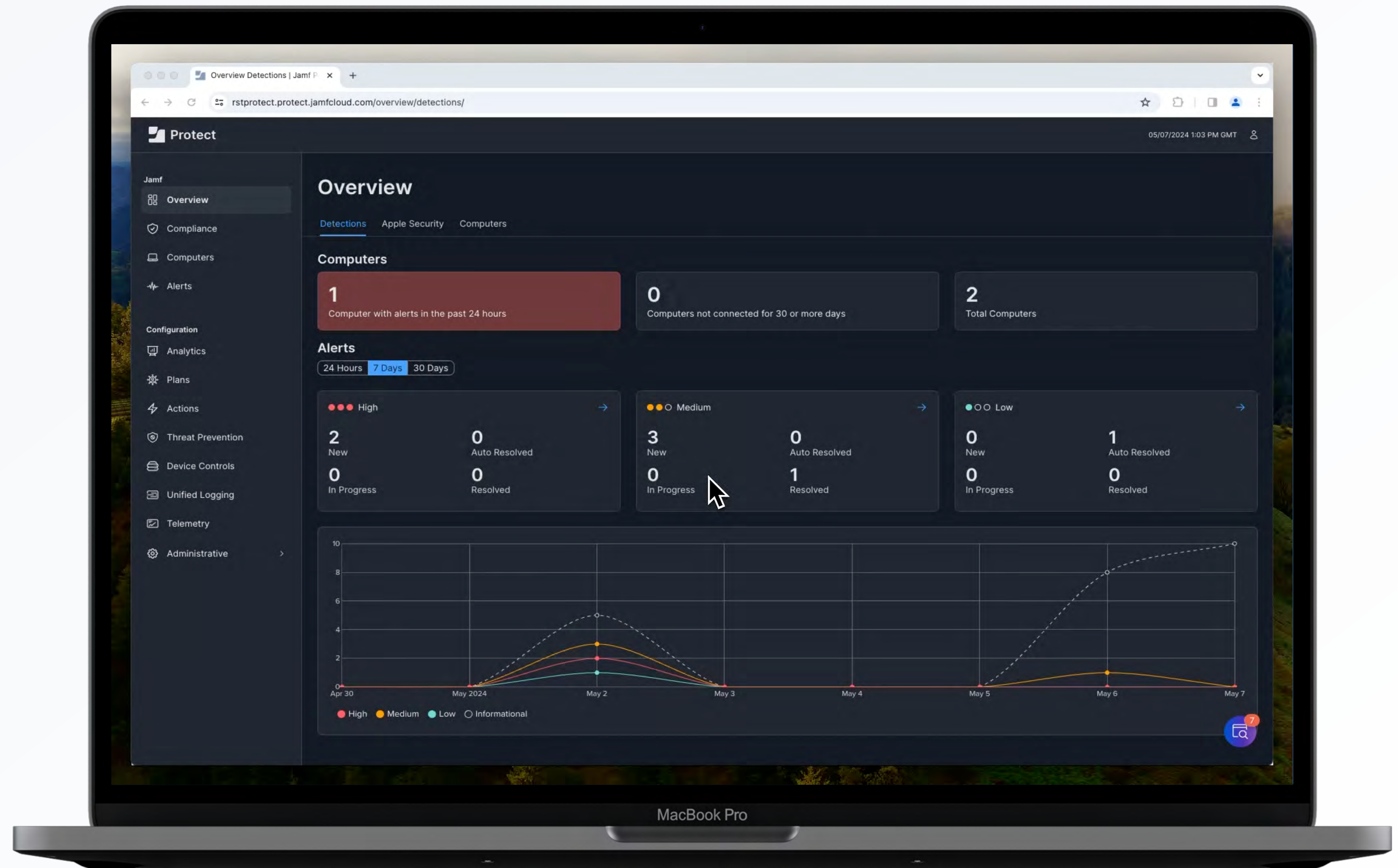
Nicht-Konformes Gerät:
Firewall-Einstellung nicht erzwungen

Mach das “Admin” Ding!



Compliance - Mängel beheben und Vorgaben erzwingen

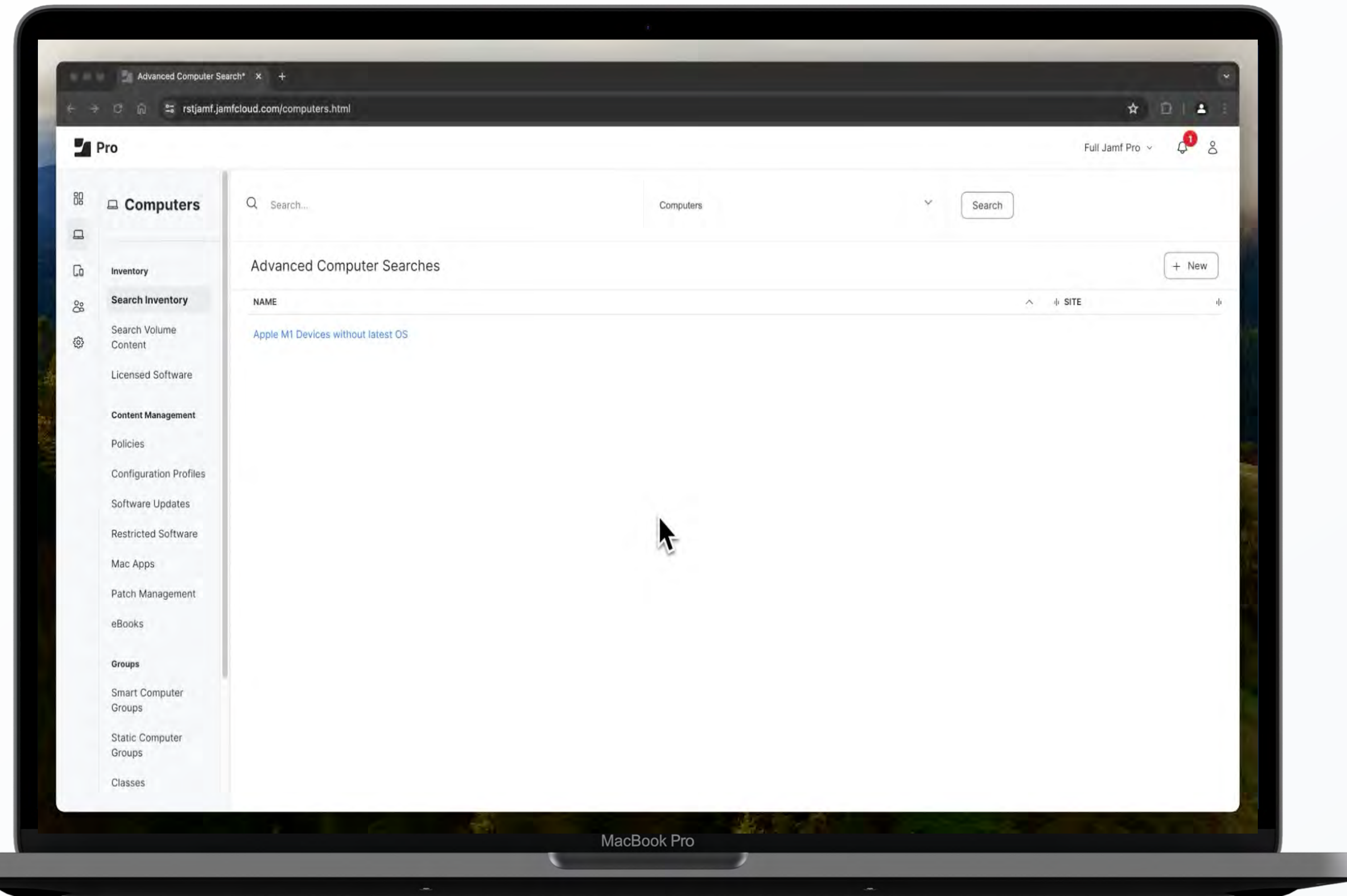
Compliance Monitoring:
Nicht-Konforme Geräte anzeigen



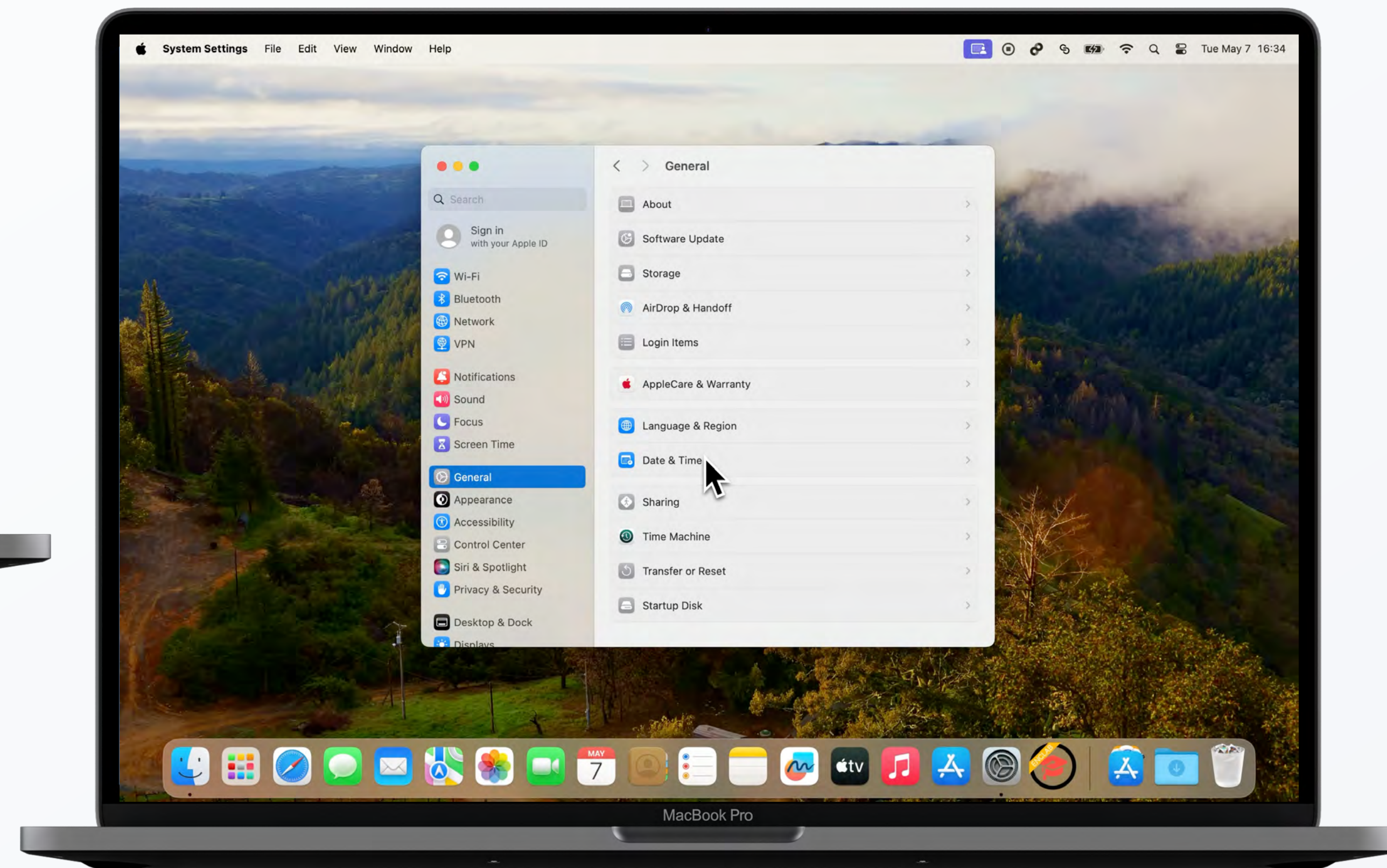
Hinter den Kulissen



Compliance - Mängel beheben und Vorgaben erzwingen

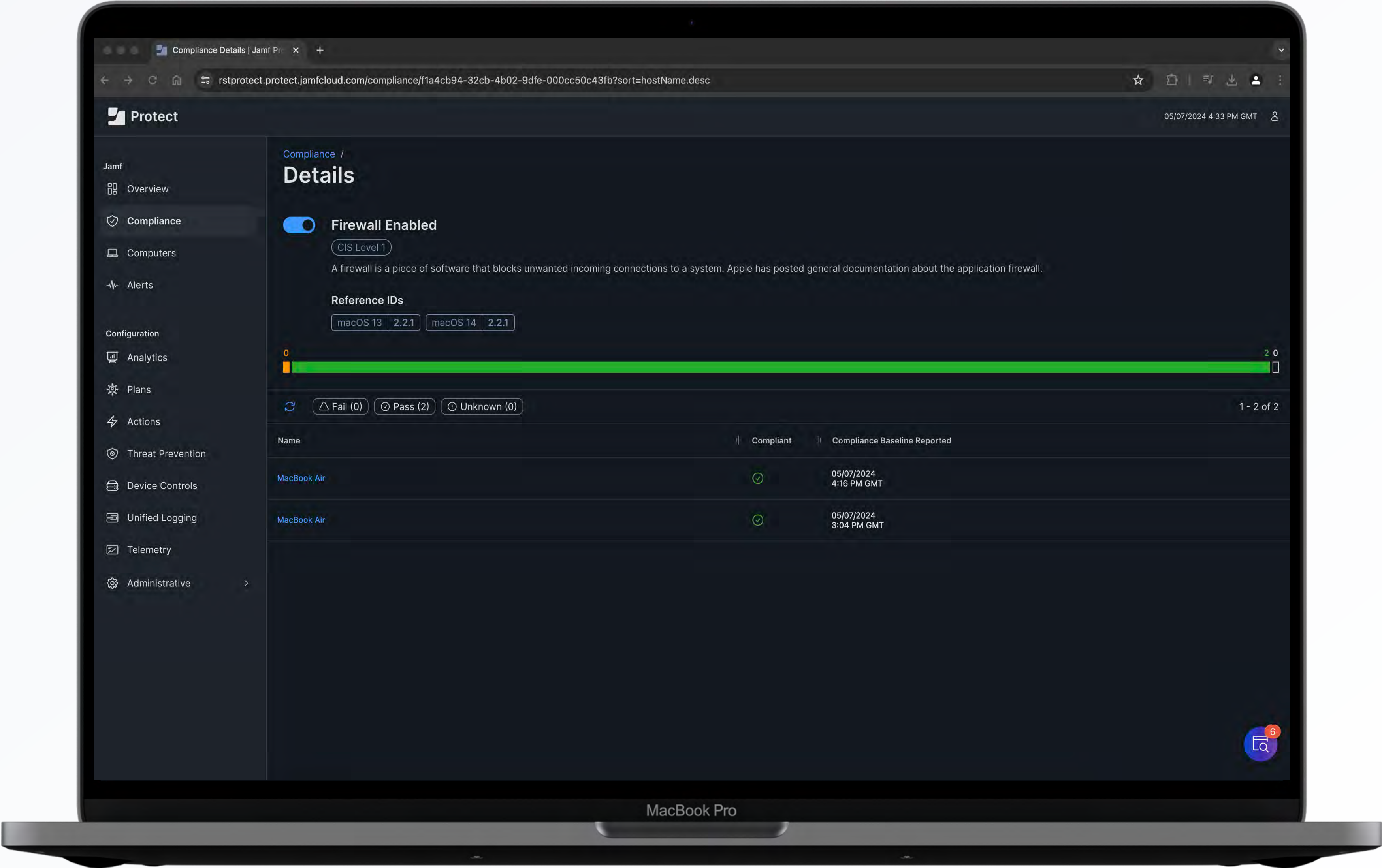


Konformes Gerät:
Firewall-Einstellung - erzwungen

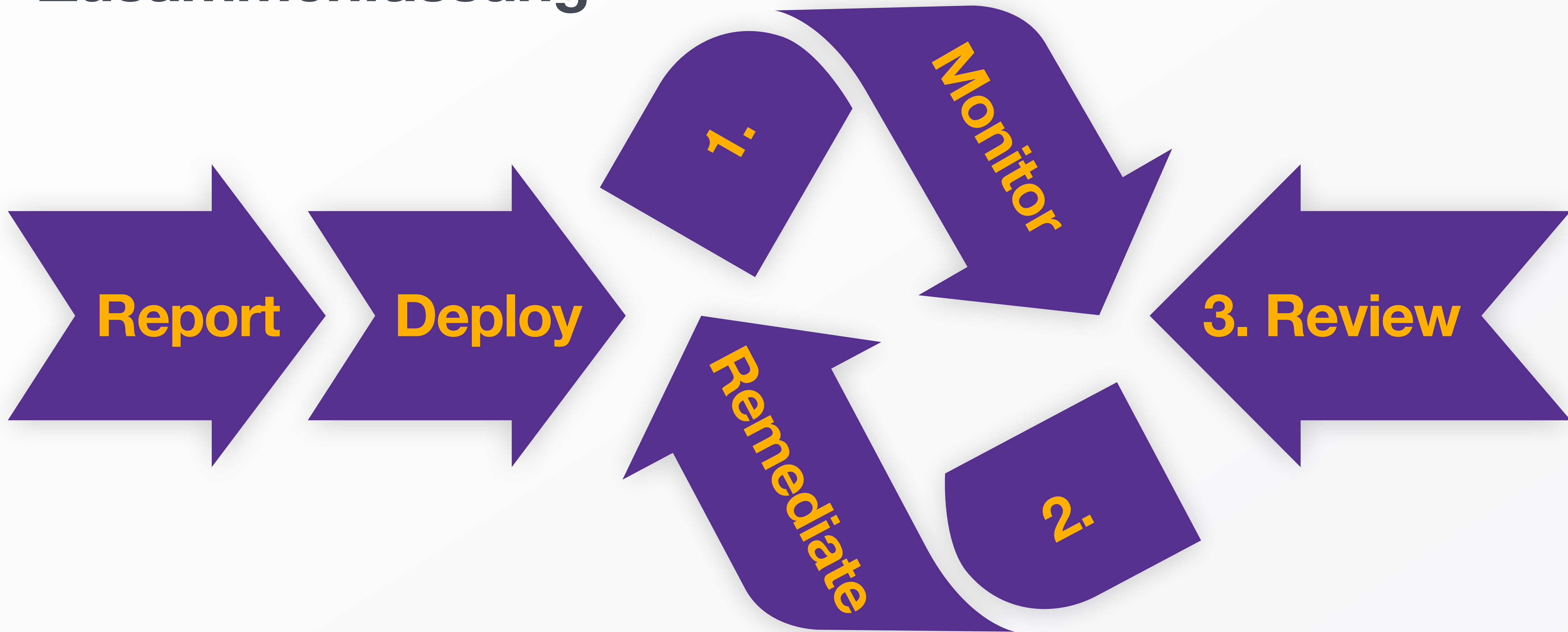


Compliance-Status überprüfen

Compliance Überprüfung:
Konforme Geräte anzeigen



Zusammenfassung



● JAMF NATION LIVE

