jamf

Jamf Nation
meet-up

PARIS 2024

La conformité sans effort : Une approche simple pour améliorer la sécurité des appareils avec Jamf

MATTHIEU CASTEL

Team Leader, Sales Engineering
France

Programme

1 | Présentation des types de conformité de sécurité et leur importance

Types, conséquences, avantages, cadres

2 | Surveillance de la conformité

Tableau de bord de la conformité, Surveillance des CVE, App Insights iOS, macOS

3 | Conformité avec Jamf

Compliance Editor, Jamf Pro

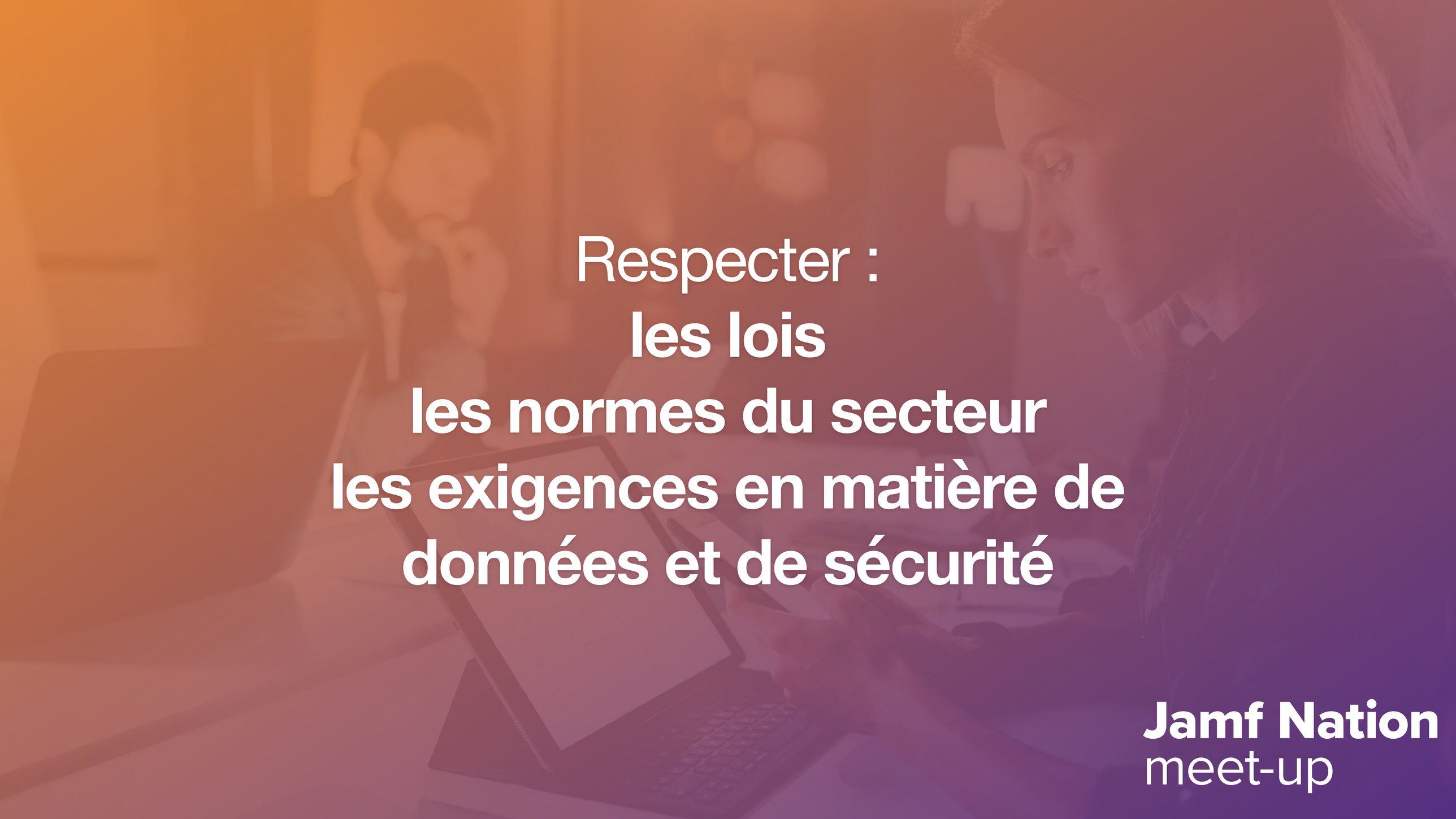
4 | Correction et mise en conformité

Jamf Pro, Jamf Protect

jamf

Jamf Nation
meet-up

Présentation des types de conformité de sécurité et leur importance



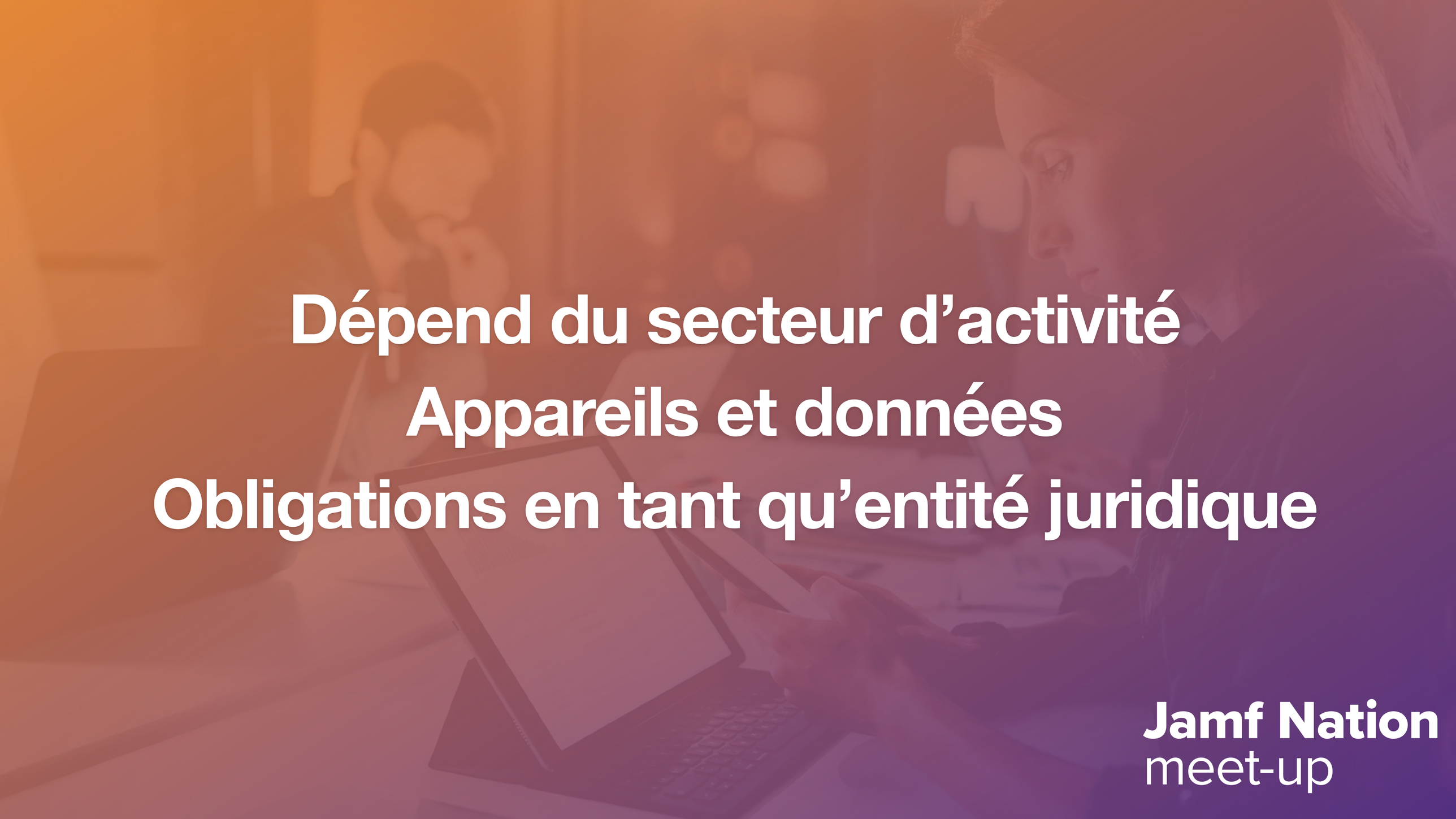
Respecter :

les lois

les normes du secteur

les exigences en matière de données et de sécurité

Jamf Nation
meet-up



Dépend du secteur d’activité
Appareils et données
Obligations en tant qu’entité juridique

Jamf Nation
meet-up

Impact sur l’organisation
Personnel et clients

Jamf Nation
meet-up

Types de **conformité**

Réglementations légales

Normes de l'industrie

Conformité de sécurité

Règles et responsabilités de l'entreprise

jamf

Conséquences de la **non-conformité**

Violations et fuites de données

Pertes financières (amendes et dédommagements)

Perte de clients, de comptes ou d'emplois

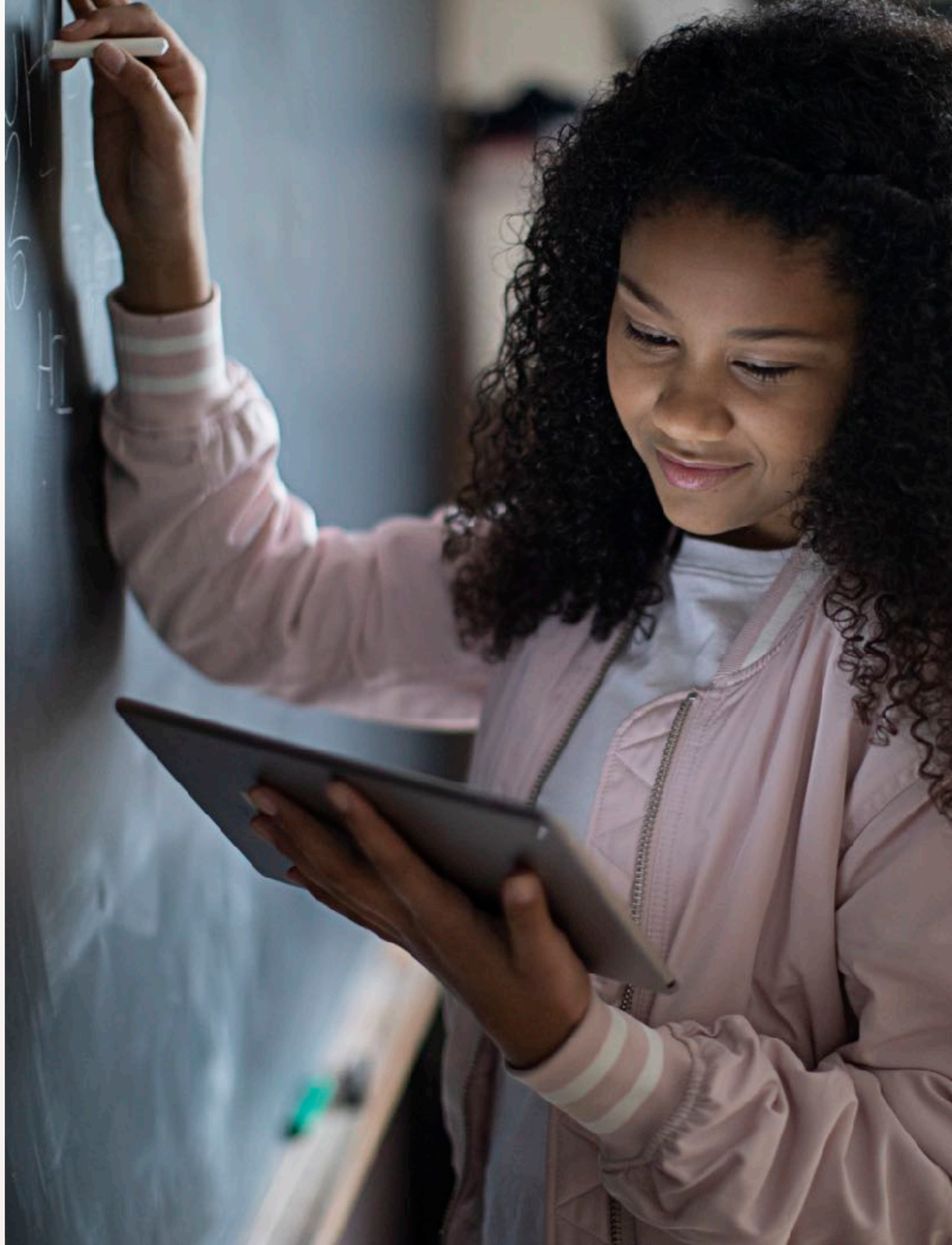
Mauvaise réputation

jamf

Avantages de la conformité

Outre l’intérêt financier d’éviter les amendes et les sanctions, la conformité de sécurité au sein d’une organisation présente plusieurs avantages :

- Protéger la réputation de votre entreprise
- Atténuer les risques de sécurité
- Renforcer la confiance des clients
- Améliorer l’efficacité opérationnelle
- Garder une longueur d'avance sur la concurrence



jamf

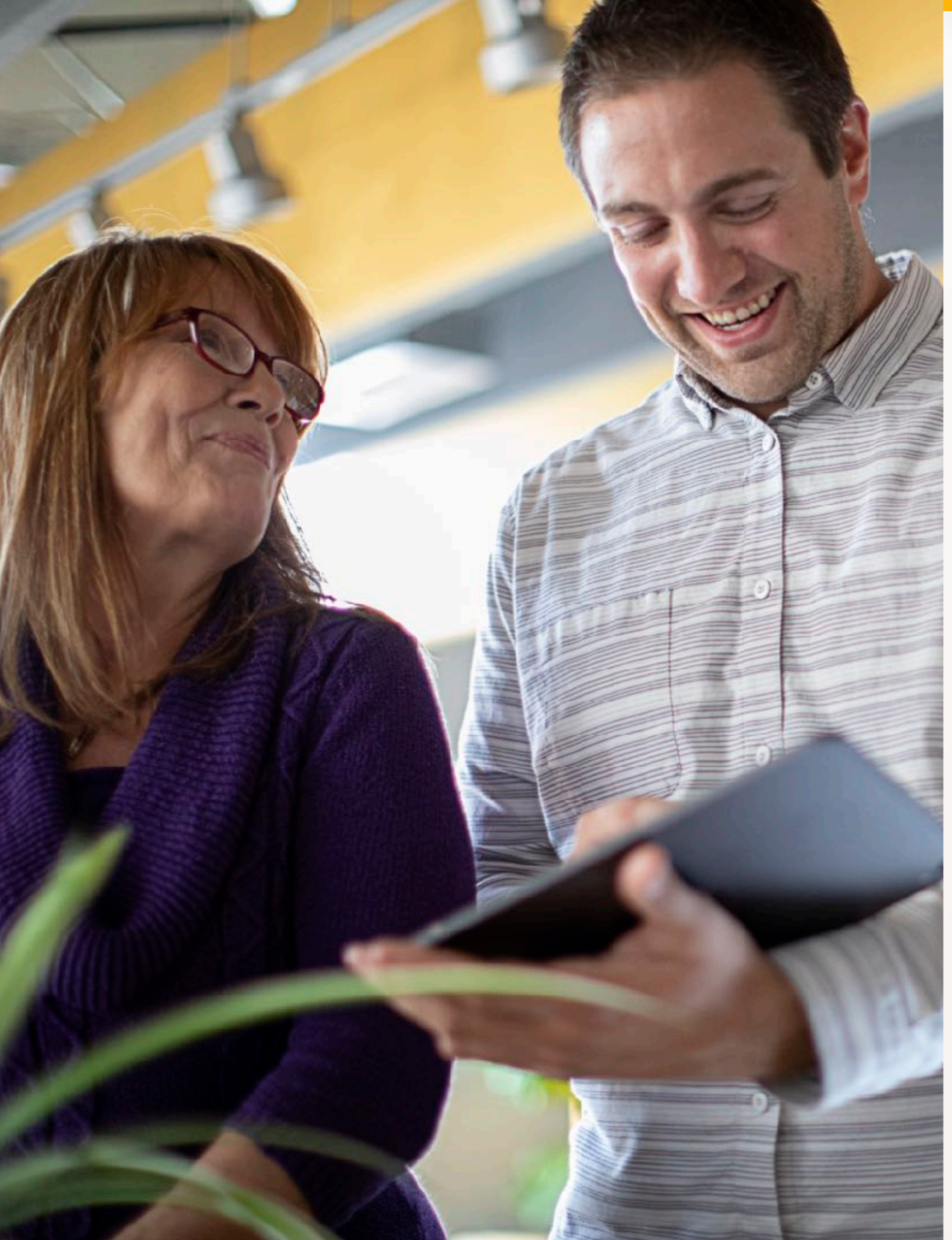
Cadres de conformité

Bases de référence et critères

Un « **référentiel de sécurité** » est un **ensemble de contrôles** qu'une organisation veut mettre en œuvre sur ses appareils.

Une fois qu'ils sont en place, il faut constamment vérifier qu'ils sont appliqués et que les appareils sont conformes.

Ce **système d'évaluation de la conformité** est ce qu'on appelle le « **critère** ».



Pourquoi mettre en œuvre des **niveaux de référence et des critères ?**

Certaines administrations exigent que tous les ordinateurs qui interagissent avec leurs systèmes et leurs données respectent des critères spécifiques, et les exceptions sont rares. De nombreux secteurs réglementés devront également mettre en place des critères de sécurité.

- Les services informatiques et de sécurité doivent collaborer
- Équilibre entre la sécurité informatique et la productivité des utilisateurs
- Différents appareils avec différentes catégories de risques

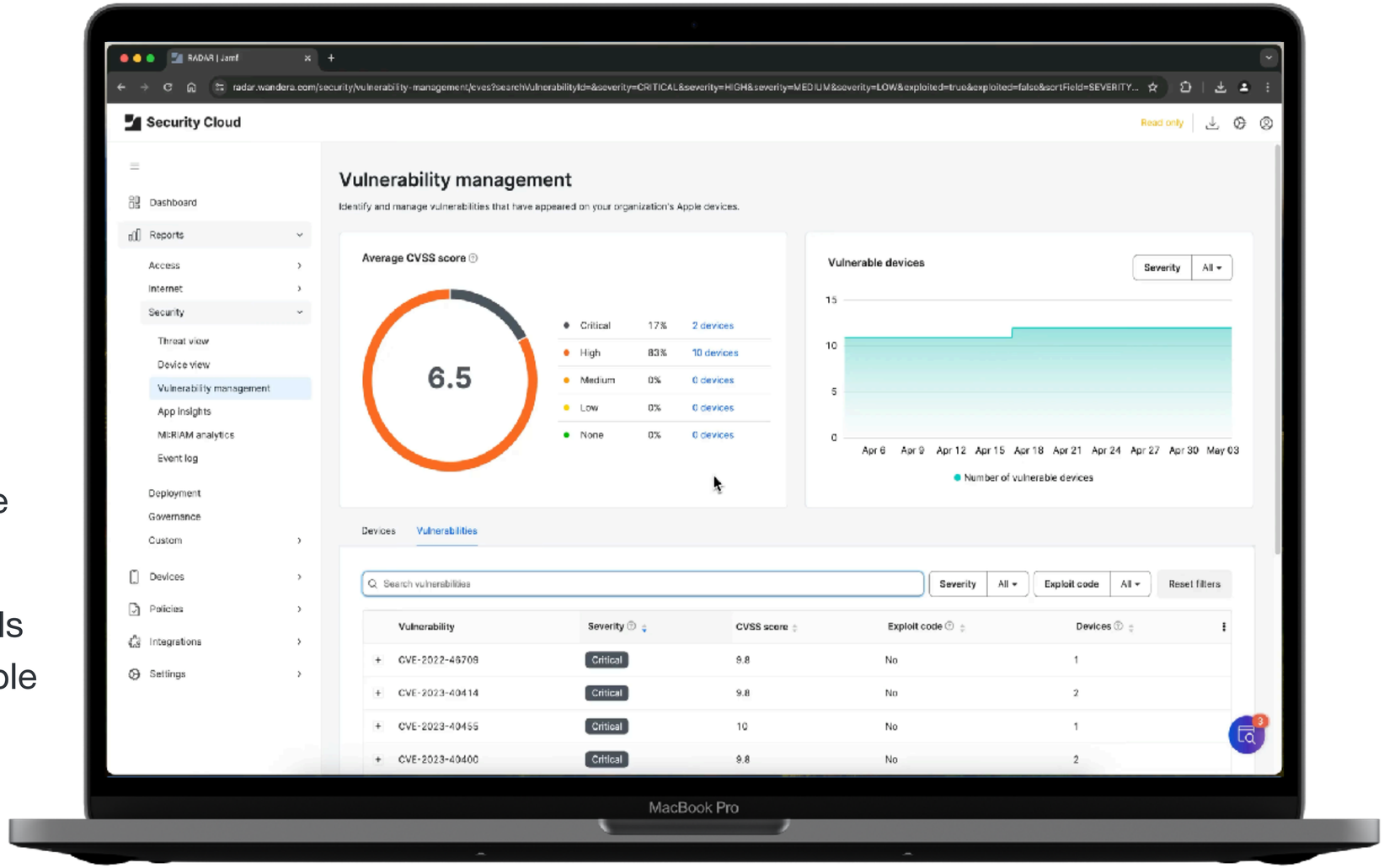
jamf

Jamf Nation
meet-up

Conformité et surveillance de la vulnérabilité avec Jamf Protect

Gestion des vulnérabilités
dans Jamf Protect

- Rapports détaillés sur les appareils Apple présentant des **vulnérabilités connues**
- **Rapports CVE** intégrés pour les OS et les applications
- **Élévation automatique du risque** : les appareils fonctionnant sous un OS à risque auront un statut de risque élevé**.**
- Les utilisateurs peuvent être **informés** qu'ils doivent mettre à jour leur système vulnérable



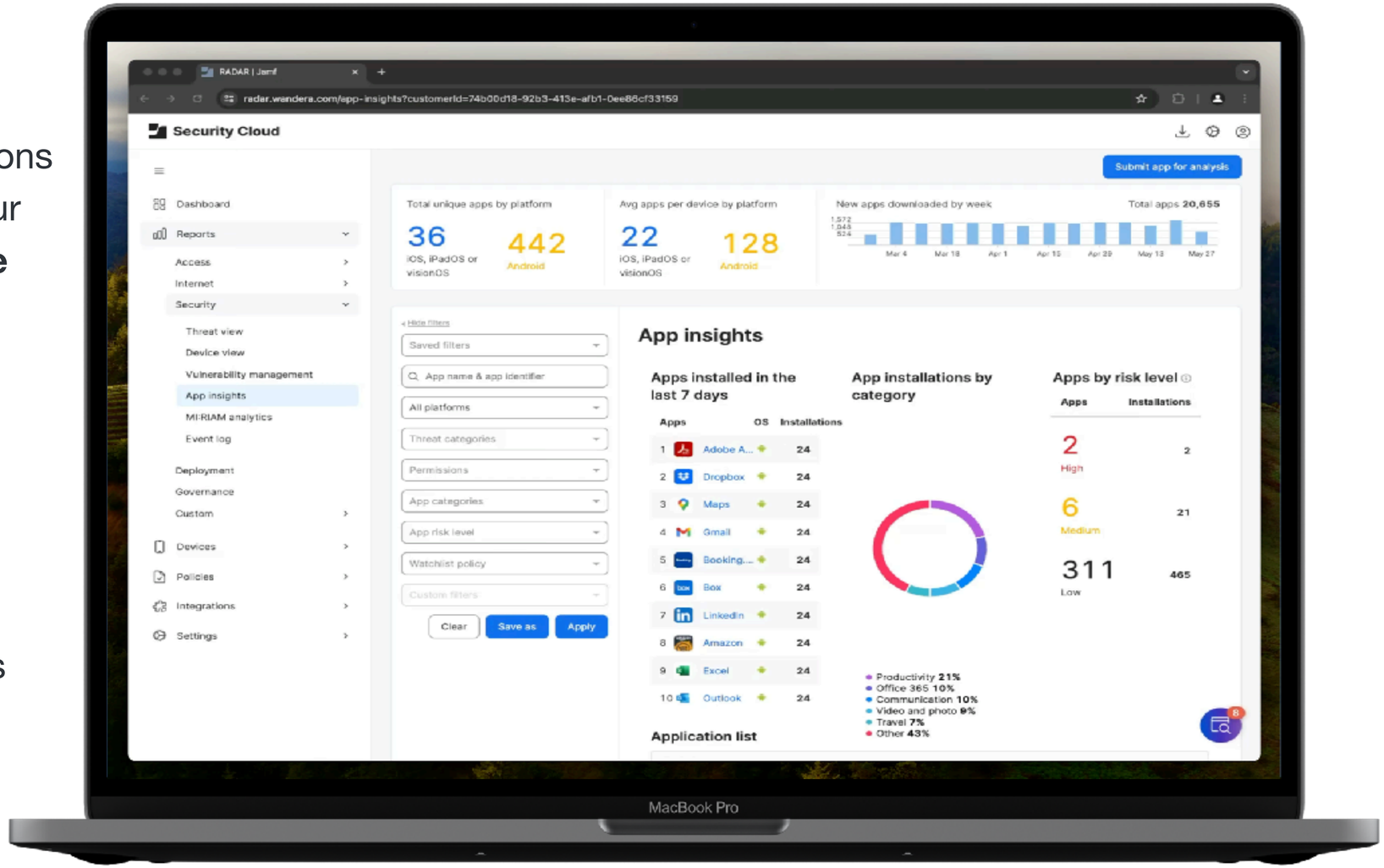
jamf

App Insights
dans Jamf Protect

- **Renvoie** des informations sur les applications installées sur vos appareils, notamment leur **version**, leurs autorisations et le **niveau de risque** qu'elles peuvent présenter**.**

Détermine :

- Le nombre d'utilisateurs qui utilisent une version **obsolète** ou **à risque** d'une application
- Quelles applications exfiltrent des données ou ont été **installées par sideloading**



jamf

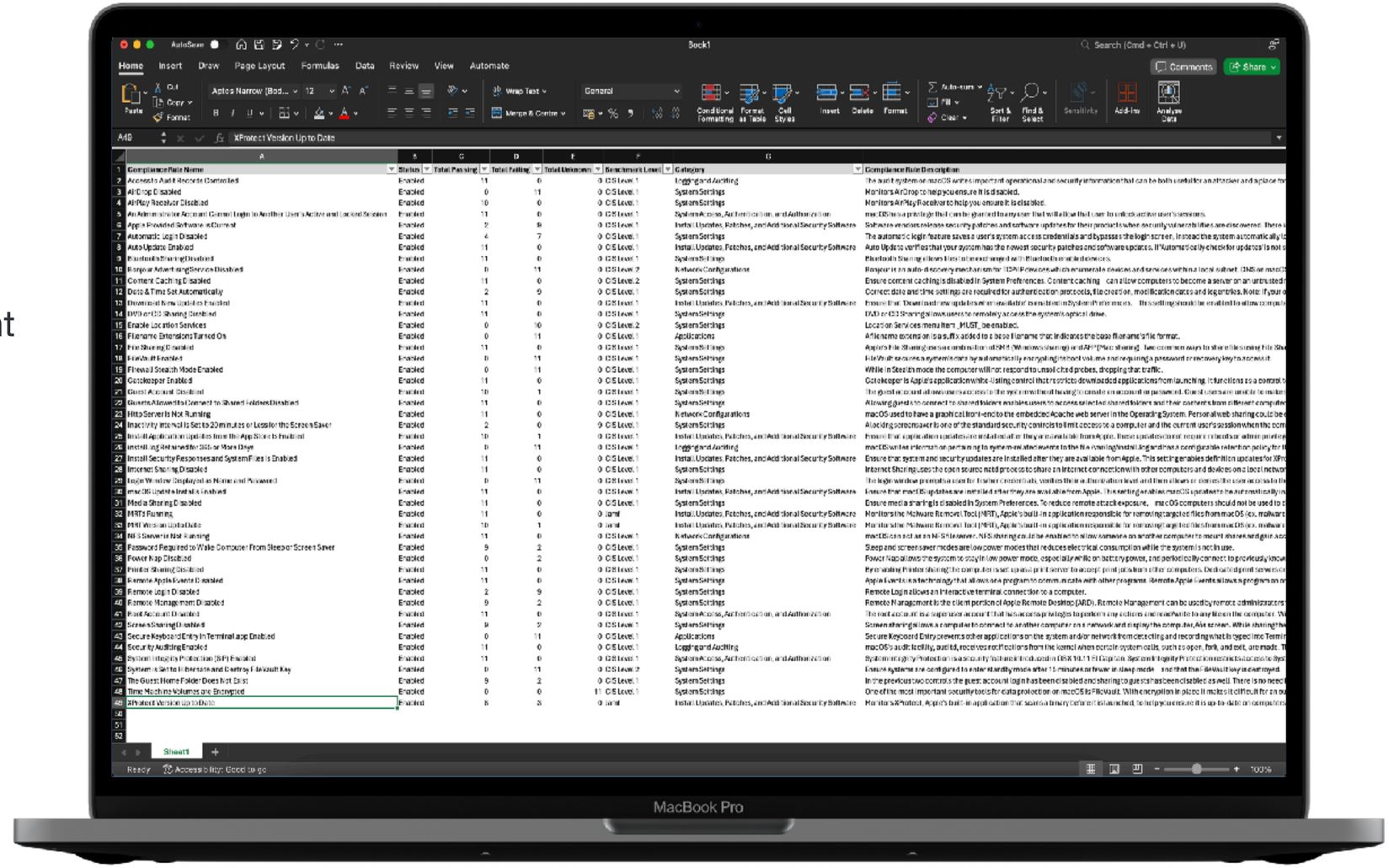
Référence de conformité dans Jamf Protect

- **Nouveau tableau de bord** avec des widgets pour une meilleure visibilité
- Règles de référence de conformité reflétant les **critères du CIS** pour macOS Sonoma
- **Plus de visibilité** pour les administrateurs afin de garantir la conformité des ordinateurs Mac
- L'outil idéal pour **contrôler** l'efficacité de Jamf Compliance Editor

jamf

Référence de conformité
dans Jamf Protect

- **Nouveau tableau de bord** avec des widgets pour une meilleure visibilité
- Règles de référence de conformité reflétant les **critères du CIS** pour macOS Sonoma
- **Plus de visibilité** pour les administrateurs afin de garantir la conformité des ordinateurs Mac
- Création facile de **rapports**



jamf

Jamf Nation
meet-up

Conformité avec Jamf

Comment déployer un référentiel de conformité ?

1. Rendez-vous sur le site web du CIS
2. Accédez à Solutions > Benchmarks
3. Remplissez le formulaire
4. Recevez l’e-mail

5. Accédez à la page web des critères de référence
6. Localisez le critère de référence qui vous intéresse
7. Téléchargez le PDF
8. Lisez le PDF

9. Créer tous les scripts et profils de configuration nécessaires.
10. Importez-les dans Jamf Pro
11. Déployez-les sur les appareils
12. Testez-les

jamf

Center for Internet Security

CIS Apple macOS 14.0 Sonoma

v1.0.0 - 10-16-2023

Jamf Nation
meet-up

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.

jamf

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/>`

jamf

Rien de plus simple !

Jamf Nation
meet-up

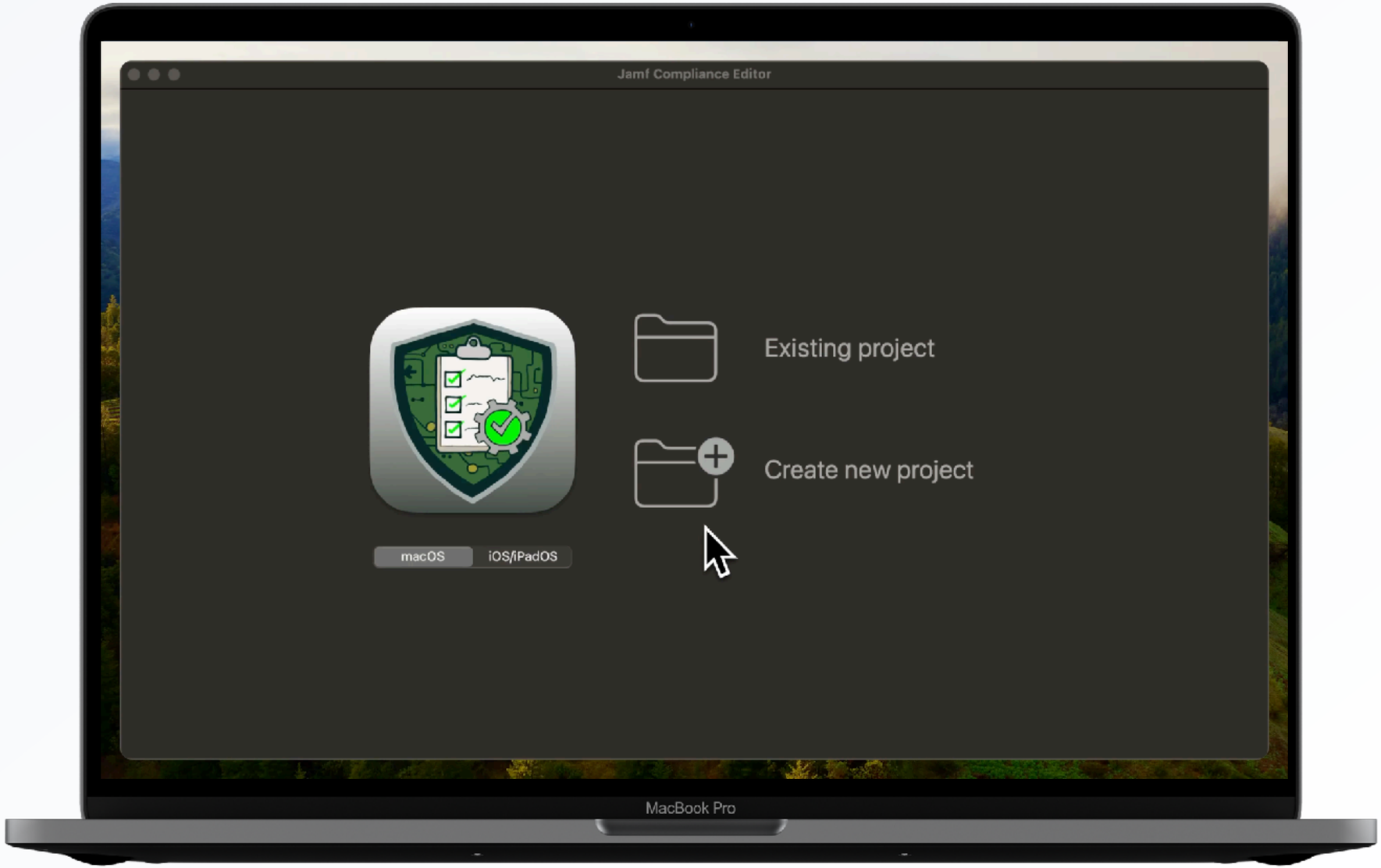
Jamf Compliance Editor

- **Générez automatiquement des références de conformité** pour les critères les plus courants.
- Assistance à la création **en un clic**
- Des directives faciles à **adapter** aux besoins spécifiques de chaque organisation
- S’intègre à **Jamf Pro** pour des déploiements rapides
- Générez des **rapports détaillés**

jamf

Comment déployer un référentiel de conformité ?

Sélectionnez votre plateforme

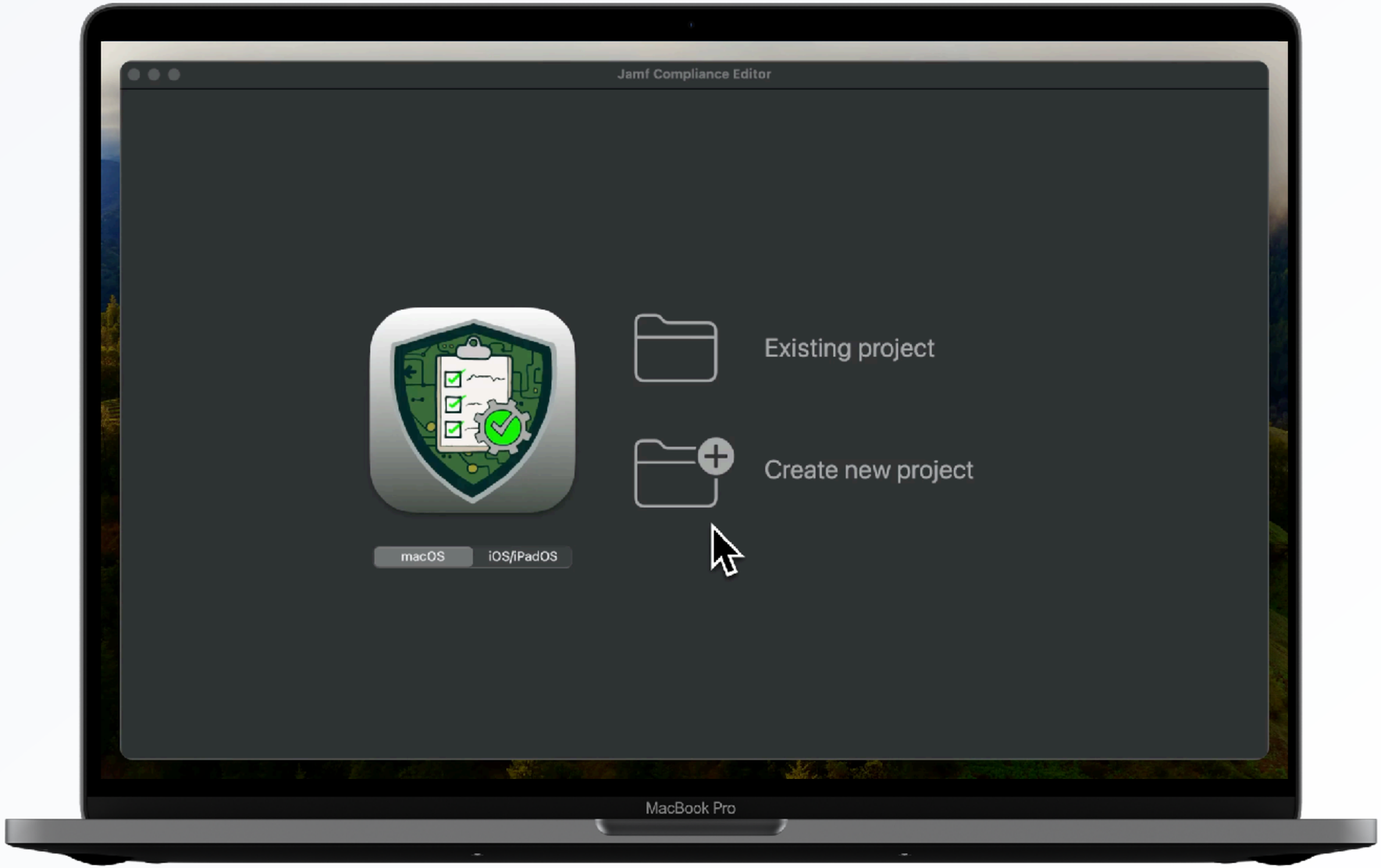


jamf

Comment déployer un référentiel de conformité ?

Créez un nouveau projet

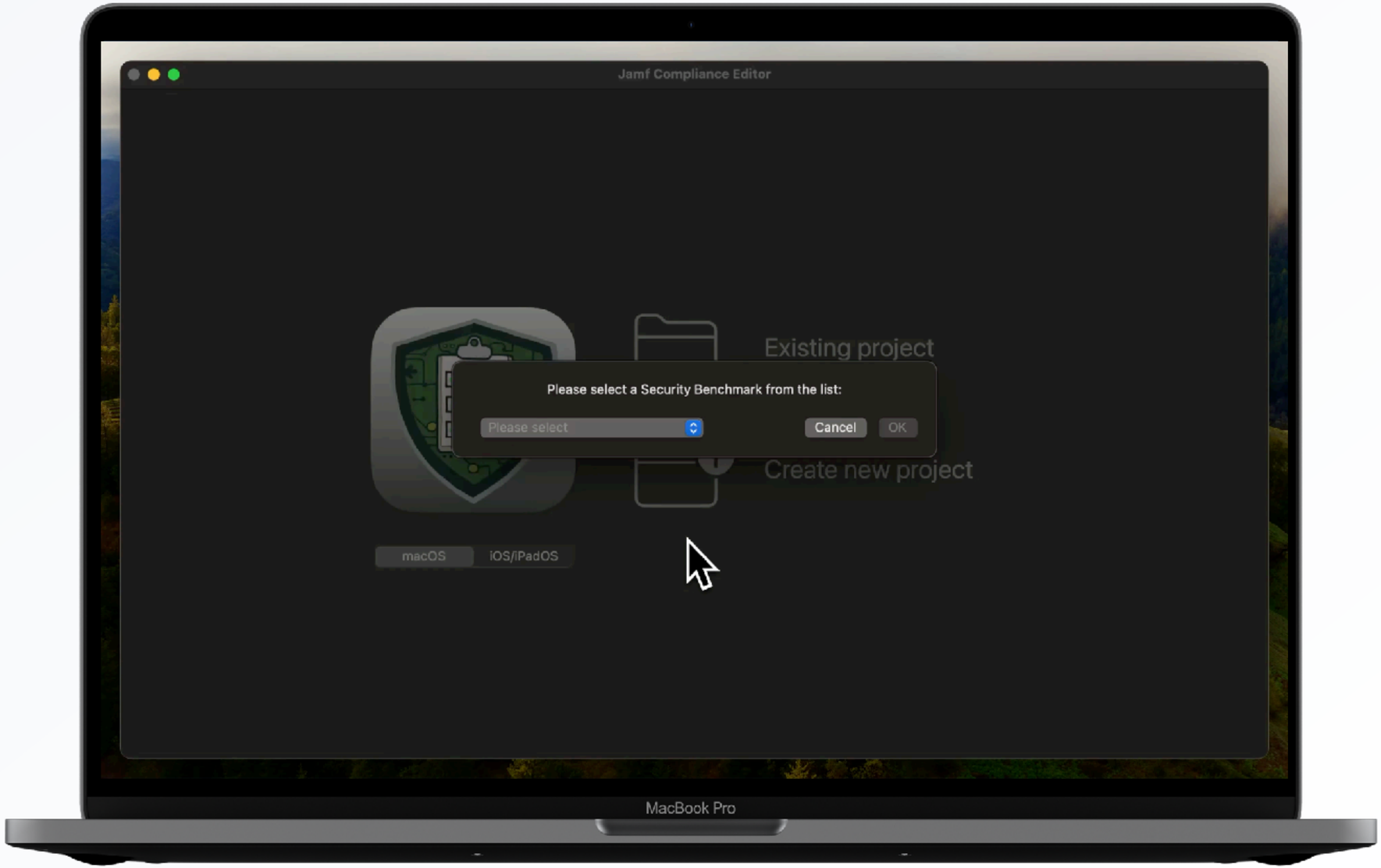
Sélectionnez votre OS



jamf

Comment déployer un référentiel de conformité ?

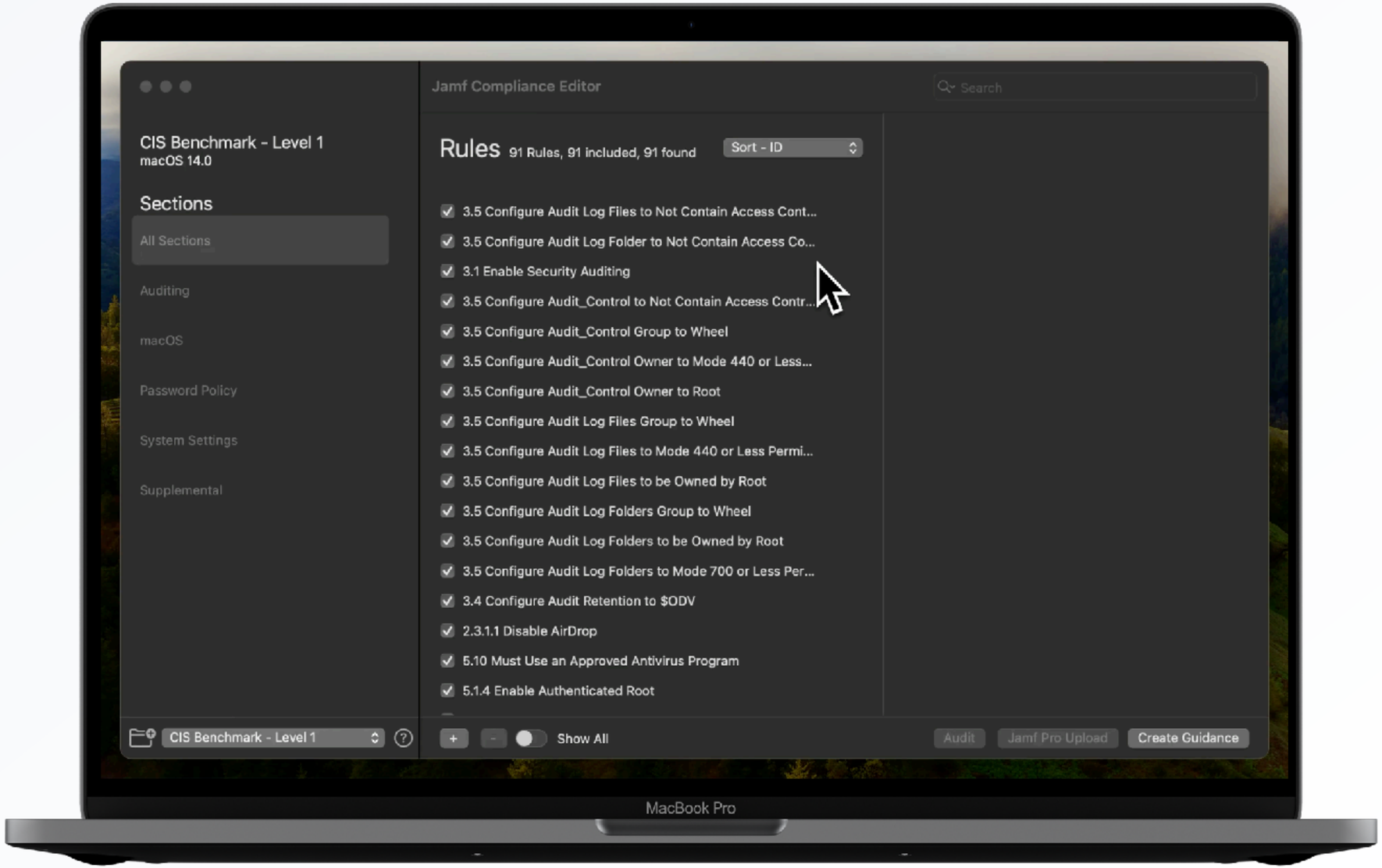
Sélectionnez vos critères de référence



jamf

Comment déployer un référentiel de conformité ?

Vue d’ensemble des règles

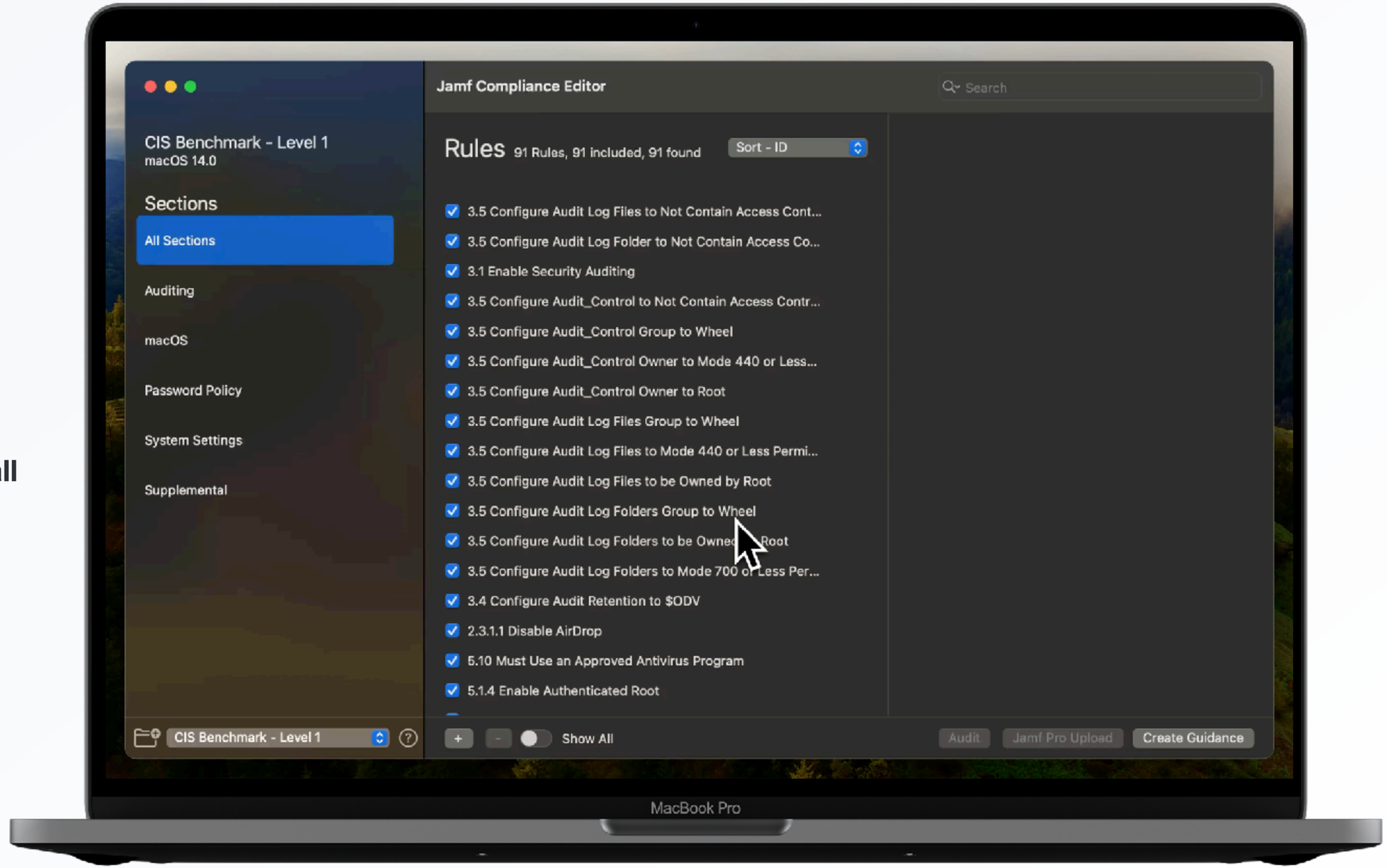


jamf

Comment déployer un référentiel de conformité ?

Vérification de règles spécifiques

par exemple, AirDrop ou Firewall

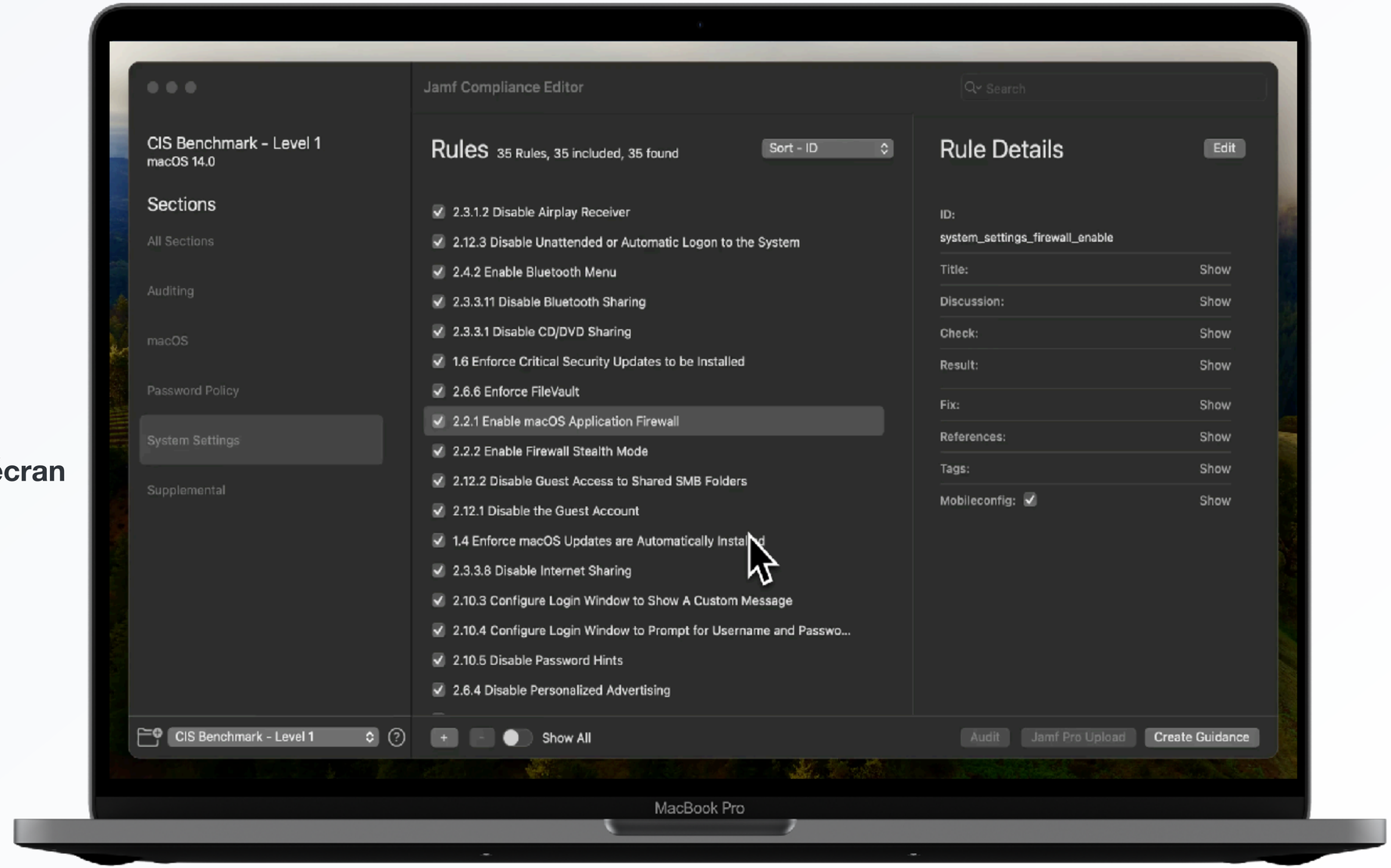


jamf

Comment déployer un référentiel de conformité ?

Optionnel : modifiez des règles

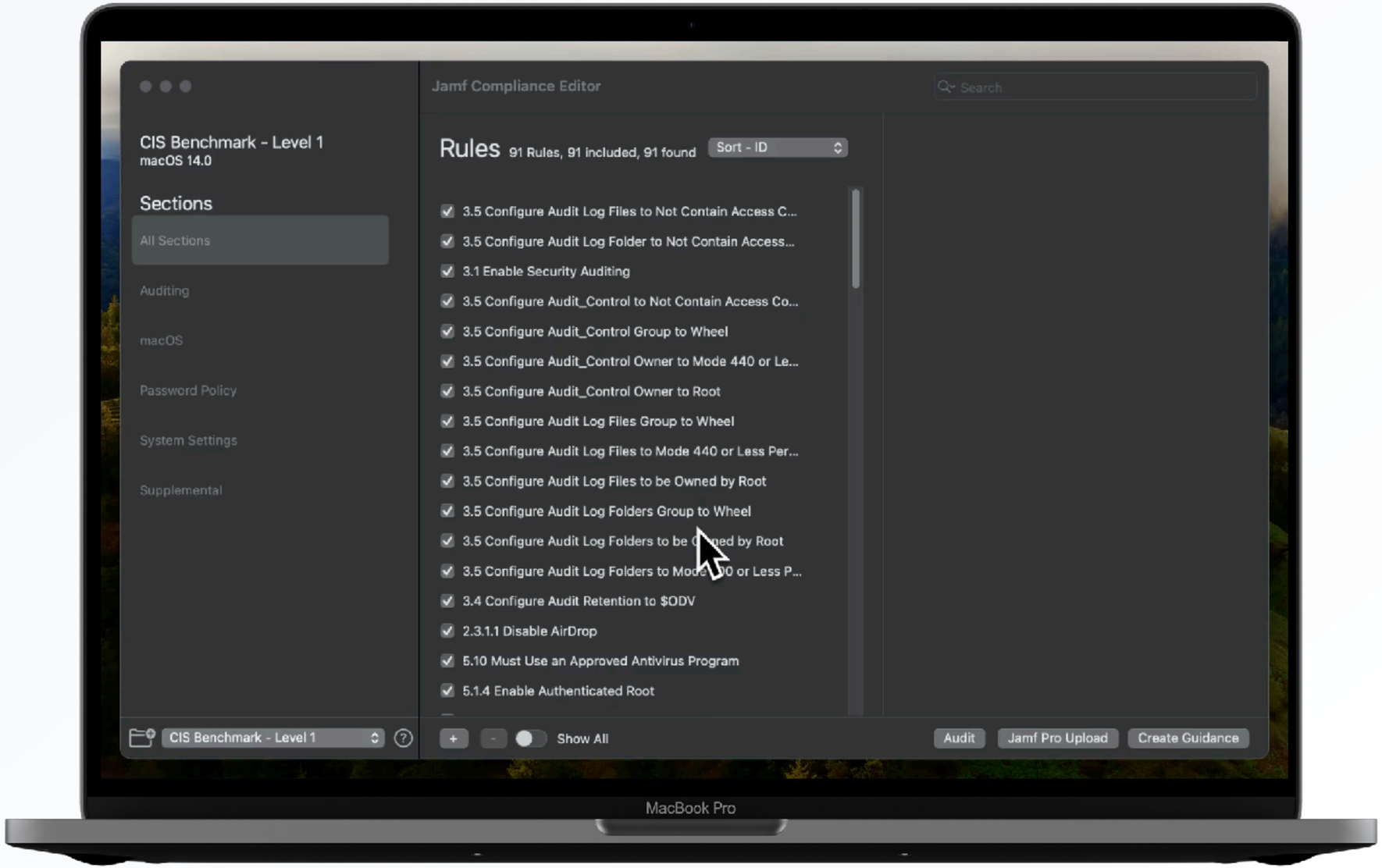
par exemple, l'économiseur d'écran



jamf

Comment déployer un référentiel de conformité ?

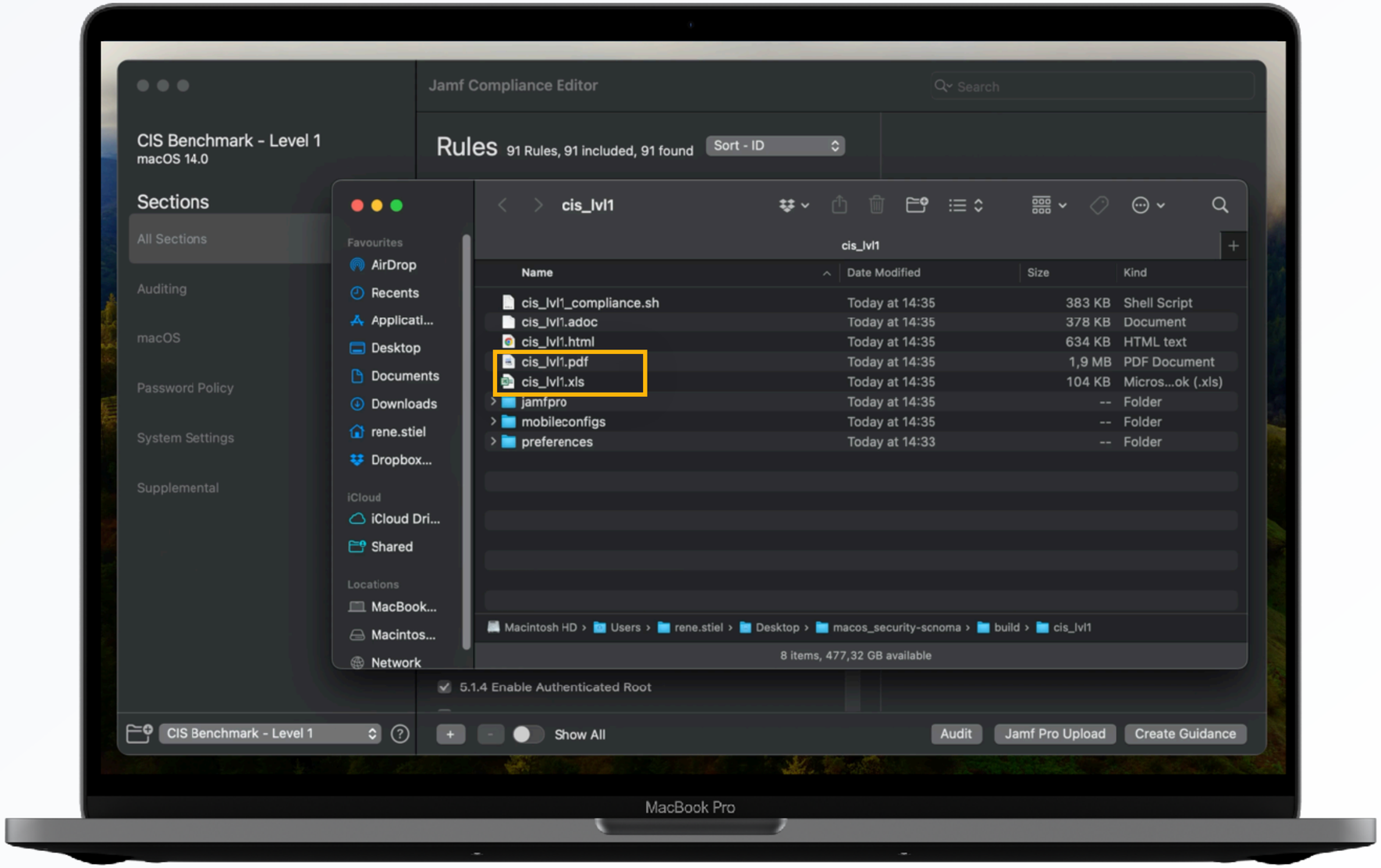
Créez votre directive



jamf

Comment déployer un référentiel de conformité ?

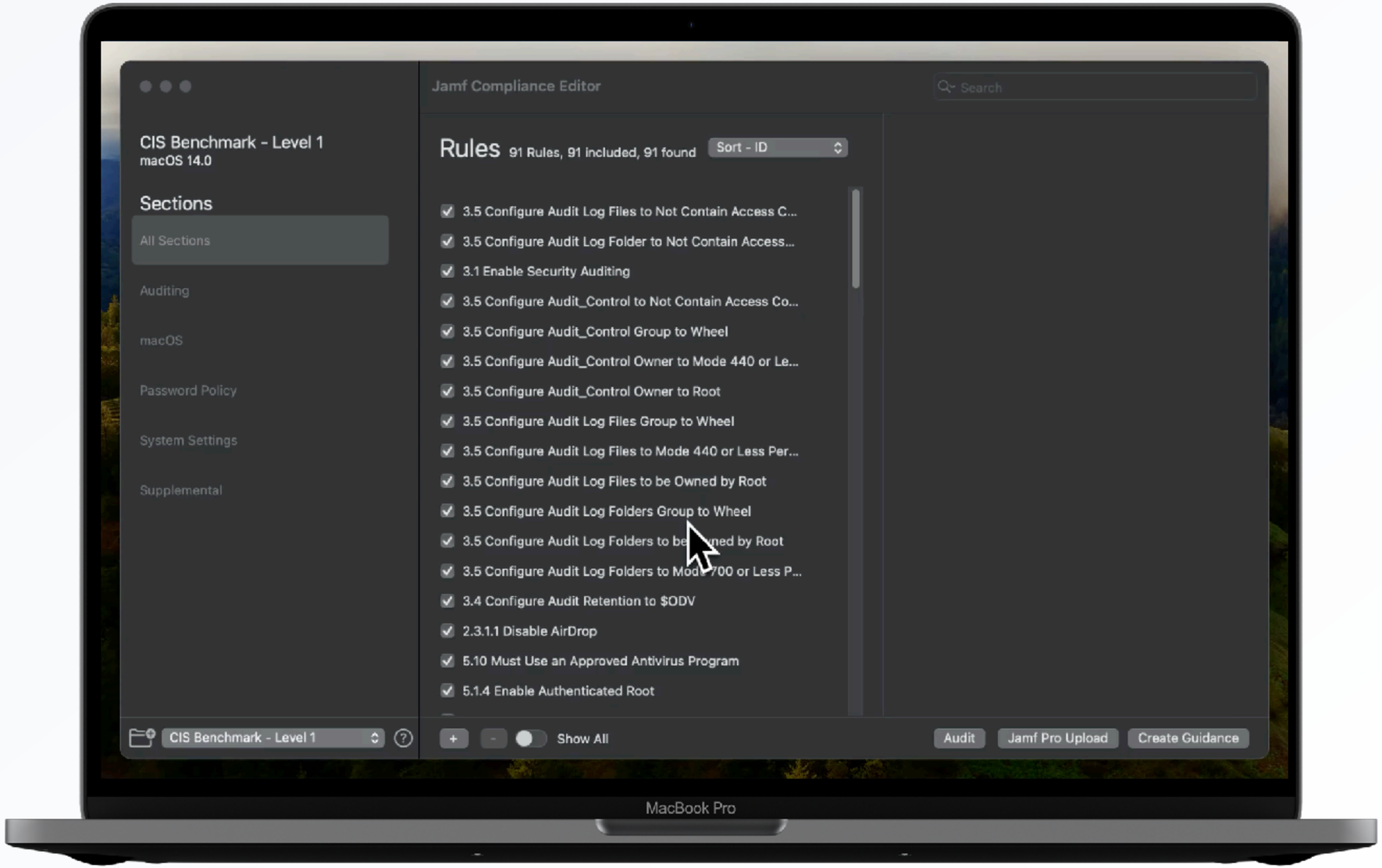
Créez votre directive



jamf

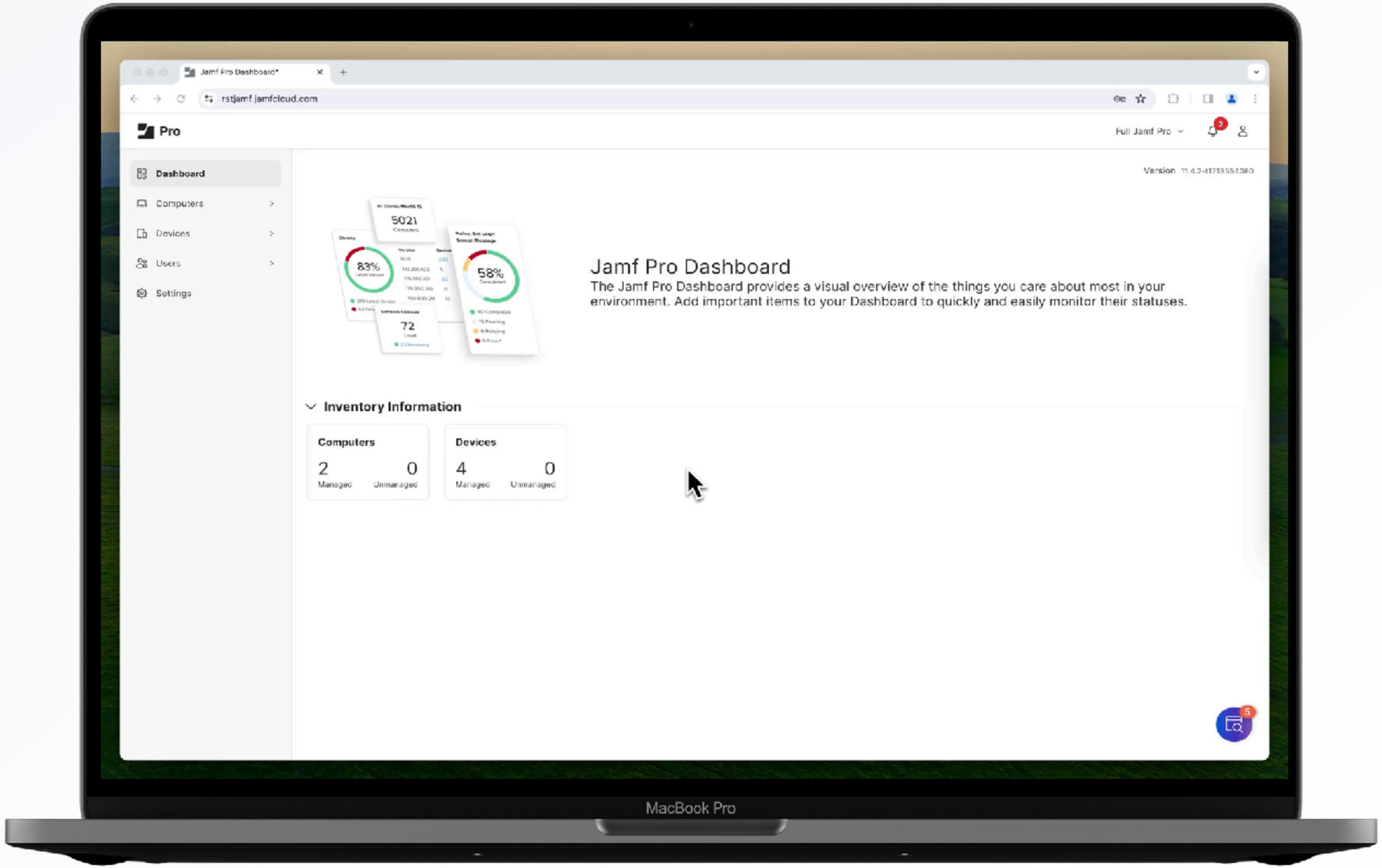
Comment déployer un référentiel de conformité ?

Importez-la dans Jamf Pro



Comment déployer un référentiel de conformité ?

Tous les profils et les scripts nécessaires sont disponibles dans Jamf Pro



jamf

Jamf Nation
meet-up

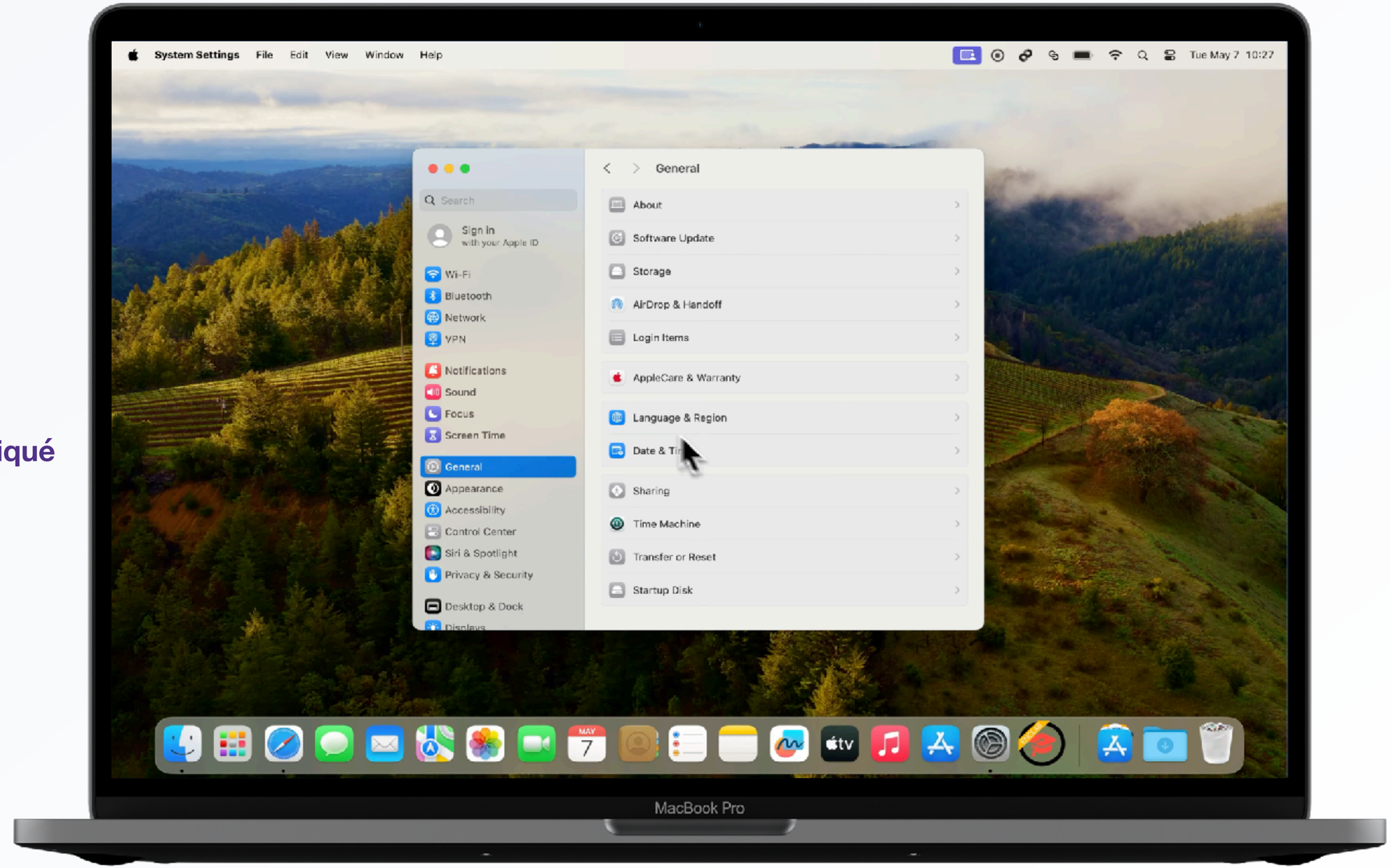
Conformité
Correction et application des règles

Corriger et appliquer les réglages

Appareil non conforme :

Réglage du pare-feu : non appliqué

Utilisateur « standard » !



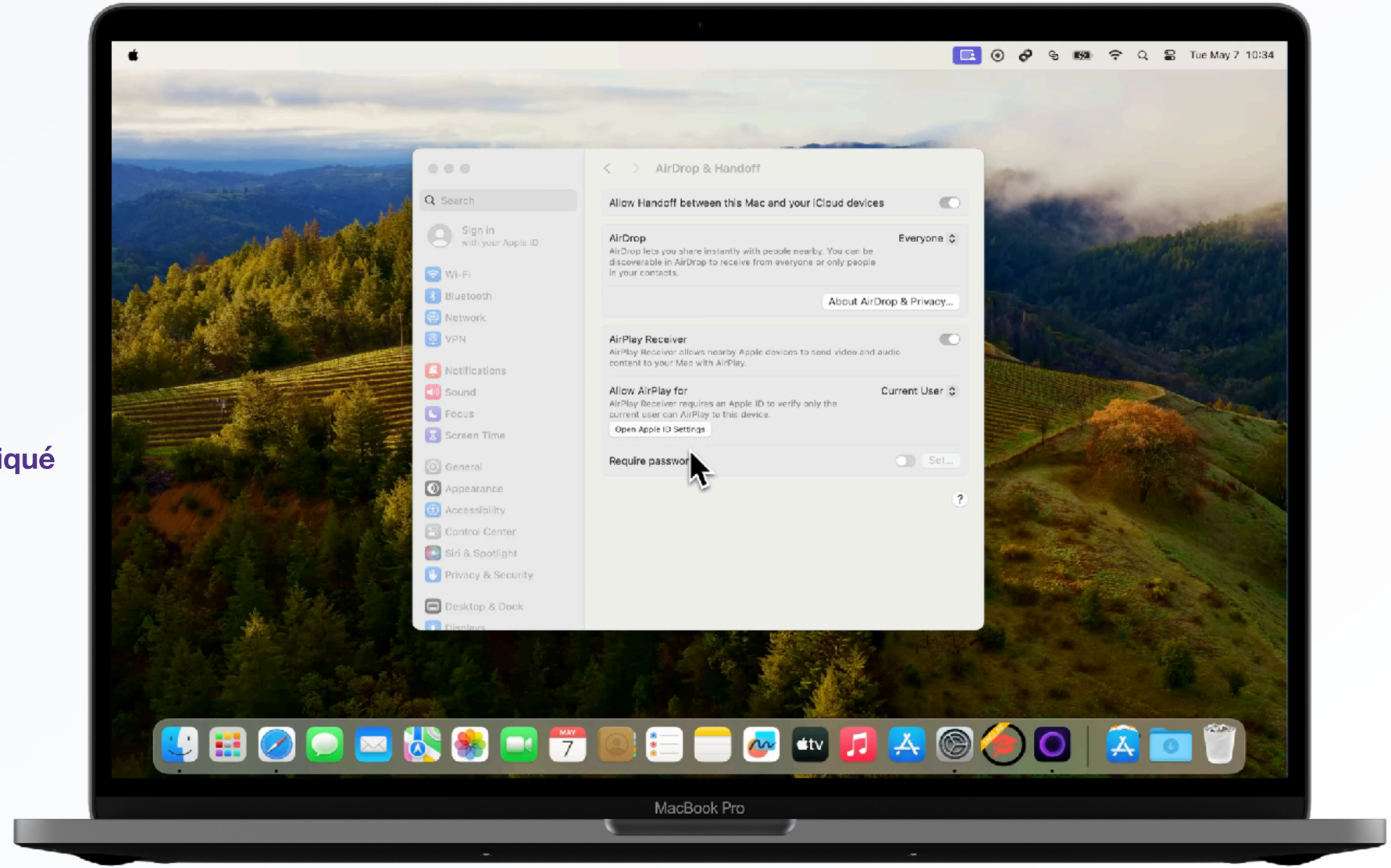
jamf

Corriger et appliquer les réglages

Appareil non conforme :

Réglage du pare-feu : non appliqué

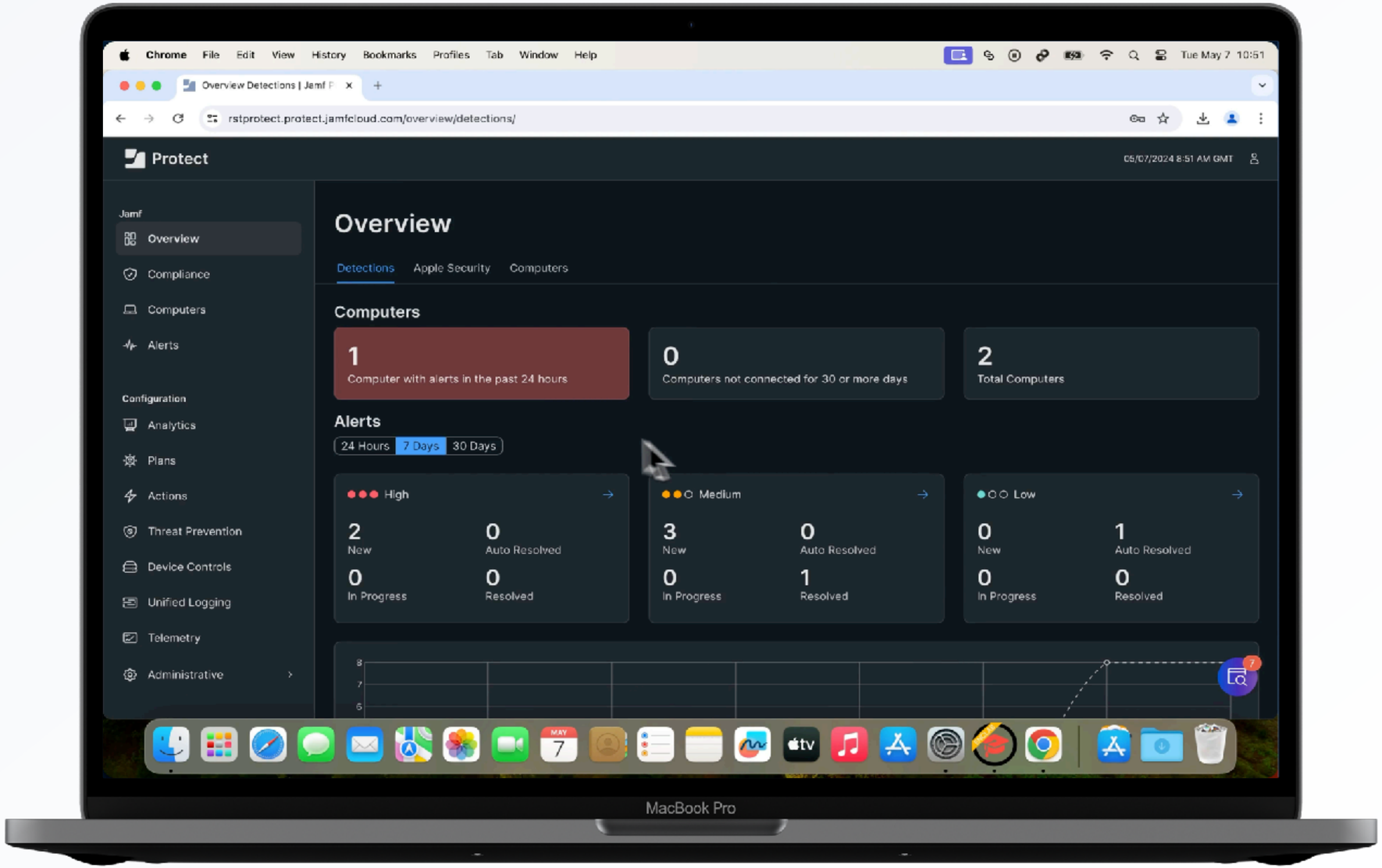
Agissez comme un « admin » !



jamf

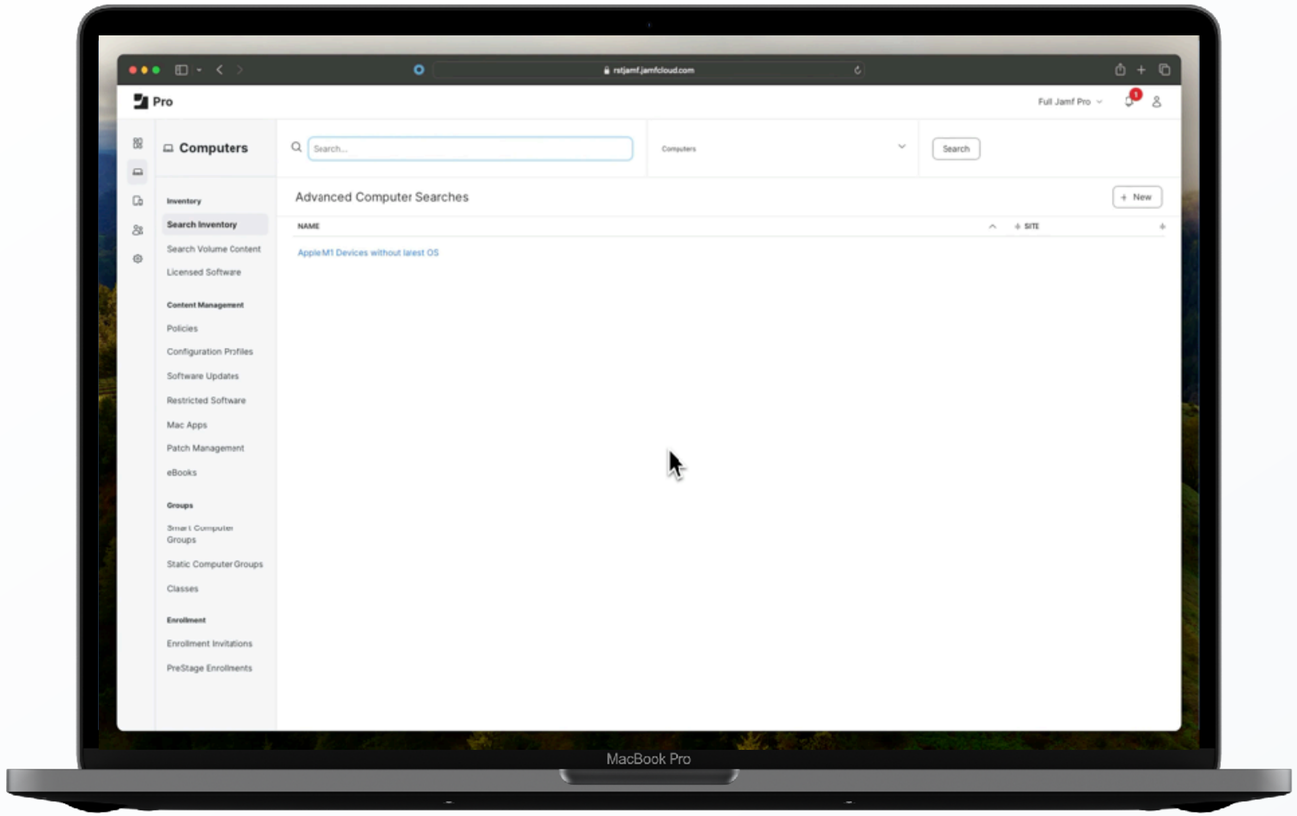
Corriger et appliquer les réglages

Surveillance de la conformité :
Afficher les appareils non conformes

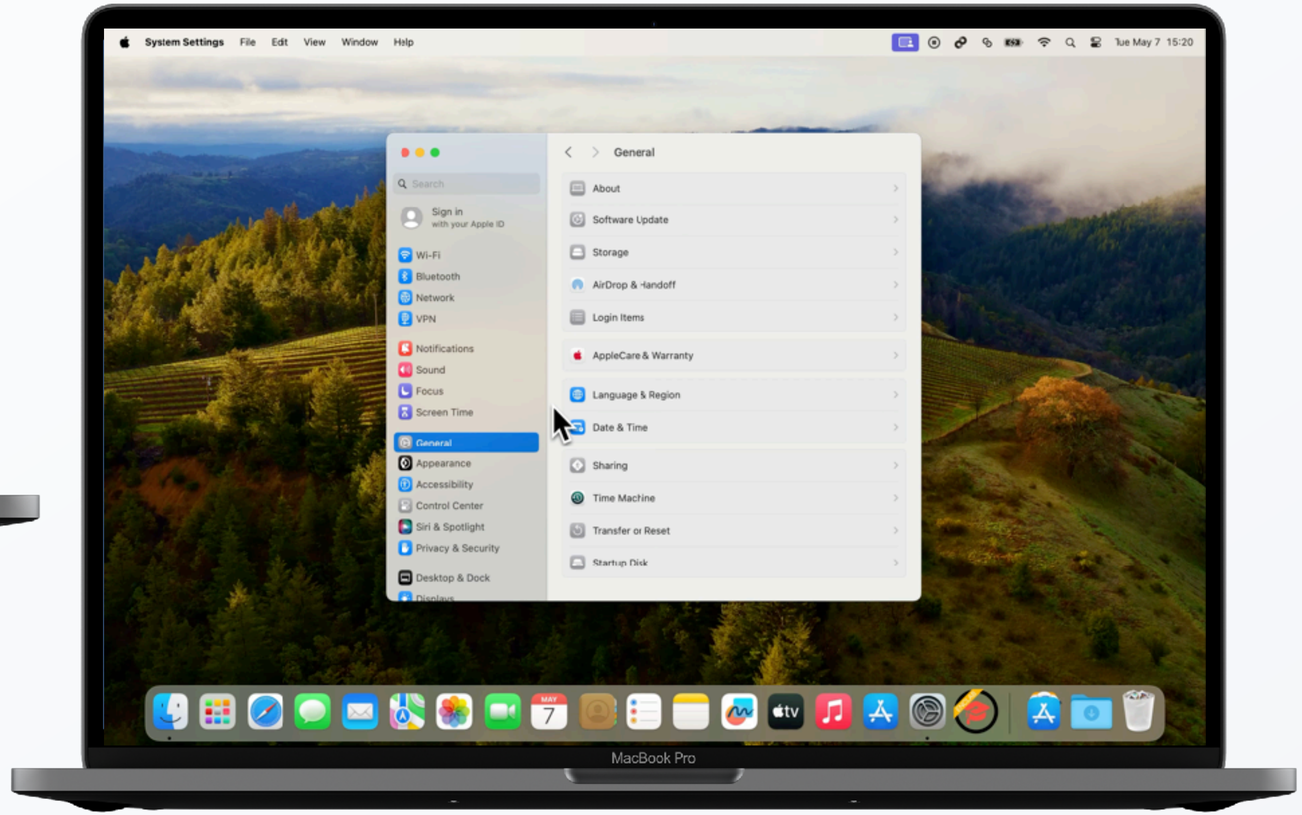


jamf

Corriger et appliquer les réglages



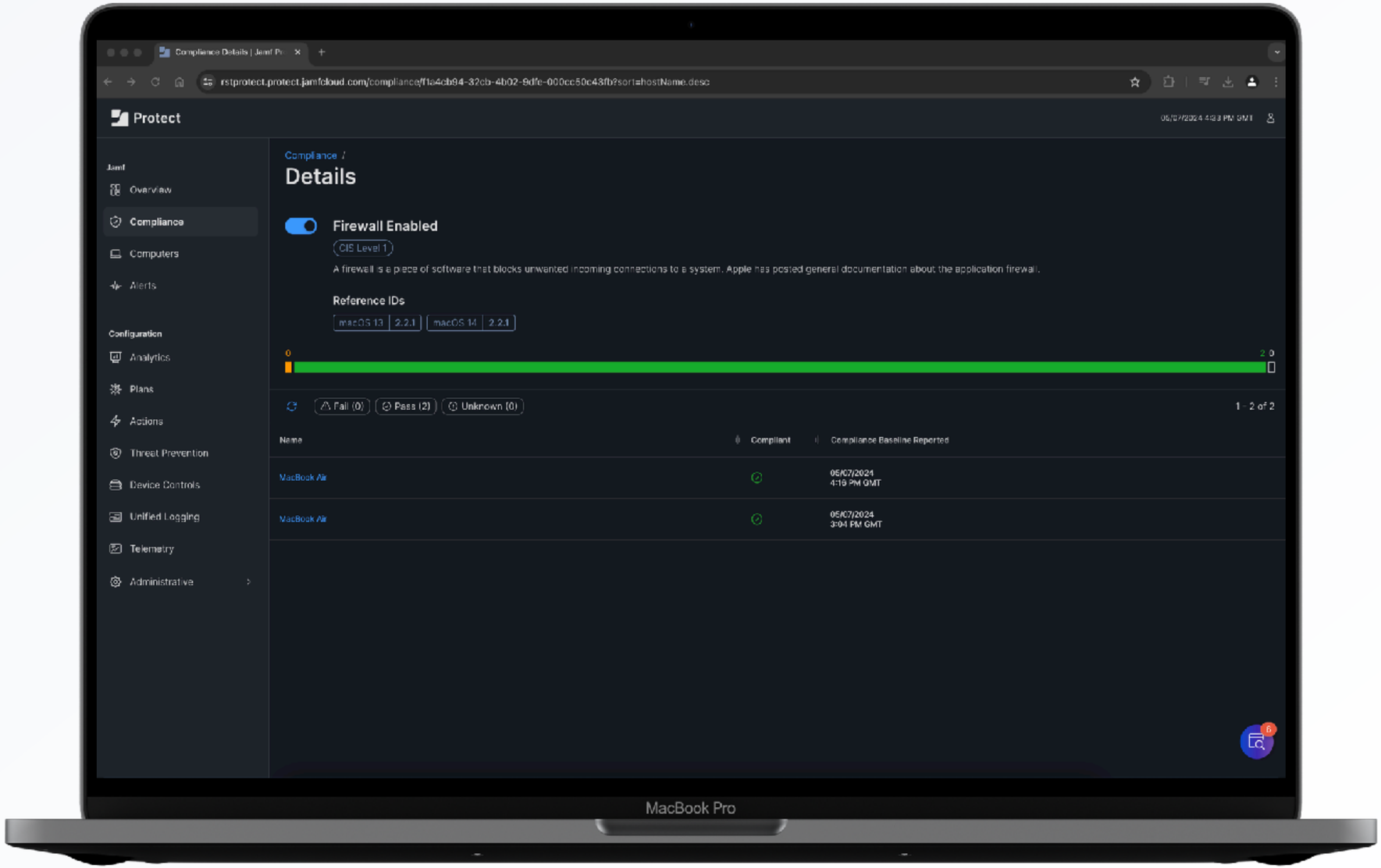
Appareil conforme :
Réglage du pare-feu : appliqué



jamf

Examen de l’état de conformité

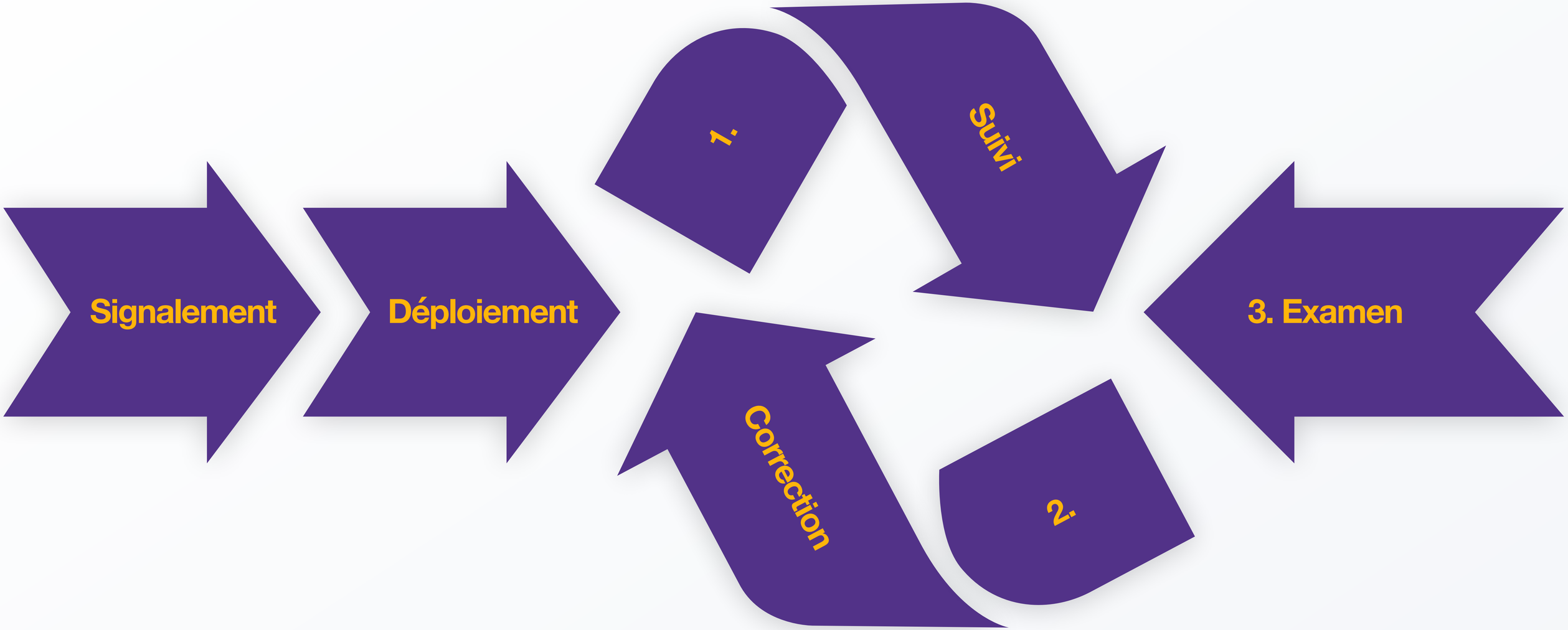
Examen de conformité :
Afficher les appareils conformes



En coulisses

jamf

Résumé



jamf