

A silver MacBook laptop is shown from a three-quarter perspective, open. The screen displays a dark blue background with the title text. The laptop is positioned on the left side of the frame, with its screen angled towards the right.

Guide pratique de la conformité Mac

*Pour les équipes informatiques
qui gèrent des environnements
Apple en pleine croissance.*

Pourquoi la conformité des Mac est-elle aussi importante ?

Les entreprises en pleine croissance qui gèrent des appareils mobiles et Mac ont un double défi à relever : répondre aux exigences de conformité, tout en conservant des opérations informatiques efficaces et gérables. La conformité ne consiste pas seulement à respecter des normes légales ou réglementaires. Elle joue également un rôle essentiel dans le renforcement de la sécurité, la réduction des risques et l'instauration d'un climat de confiance. Mais elle ne doit pas pour autant ajouter de complexité inutile à des équipes informatiques déjà surchargées.

Pour créer un environnement sécurisé et évolutif, la première étape consiste à comprendre l'importance de la conformité Mac.

Fondamentalement, la conformité est guidée par des critères de référence. Dans le domaine de la sécurité informatique, les critères de conformité permettent de déterminer dans quelle mesure une organisation adhère à ces réglementations et ces exigences, et ils proposent des bonnes pratiques pour la protection des données sensibles.

Les contrôles et les critères de référence du CIS, par exemple, sont largement adoptés dans tous les secteurs, et ils forment un socle fondamental de bonnes pratiques de sécurité. S'ils ne sont pas rattachés à une réglementation spécifique, ils servent souvent de base pour l'élaboration de mesures de conformité supplémentaires propres à un secteur ou à une région, comme le RGPD ou l'HIPAA.

Pour les entreprises en pleine croissance, ces critères sont un excellent moyen de réduire les risques, de protéger les données et d'éviter les failles de sécurité au fil du développement de l'environnement. En effet, les infractions aux réglementations en vigueur peuvent entraîner de lourdes amendes et des poursuites, mais aussi nuire considérablement à la réputation d'une entreprise. Correctement appliqués et suivis, ces critères permettent aux organisations de préserver leur sécurité et leur compétitivité dans le monde numérique.



Qu'est-ce que la DDM ?



La gestion déclarative des appareils (DDM) permet aux appareils d'agir de manière proactive et autonome en cas d'anomalie de conformité. Cette capacité renforce la fiabilité des systèmes, tout en réduisant les efforts manuels de mise en conformité.

L'art de maintenir la sécurité des Mac

Si les administrateurs informatiques adorent Apple, c'est en partie parce que le Mac possède de puissantes fonctions de sécurité intégrées.

Pour les petites équipes informatiques chargées de la gestion des Mac et des appareils mobiles, ces protections intégrées sont plus efficaces lorsqu'elles sont gérées de manière centralisée et appliquées automatiquement.

Les ordinateurs Mac sont, par nature, plus stables et plus efficaces que les autres appareils. Et avec les bons outils, le service informatique peut appliquer des mesures de gestion et de sécurité puissantes et flexibles, spécialement conçues pour Apple, sans dégrader l'excellente expérience qui fait la réputation de la marque. En associant une solution MDM de classe mondiale au protocole de gestion déclarative des appareils (DDM) d'Apple, vous pouvez garantir la protection des réseaux et des données de l'entreprise et des employés.

La conformité réglementaire des Mac : les facteurs à prendre en compte

De nombreuses organisations sont soumises aux mêmes exigences de conformité que les grandes entreprises, mais leurs équipes informatiques sont plus réduites et elles disposent de moins de ressources.

La conformité implique de comprendre et appliquer tout un éventail de normes et d'obligations.

Votre organisation doit sans doute se conformer à plusieurs normes de conformité. Ces normes garantissent la sécurité des données de l'entreprise et des employés. Vous devrez faire respecter ces critères, mais aussi les réglementations propres à votre secteur et à la législation nationale.

Combien y a-t-il de règlements ?

Chaque secteur, chaque région possède ses propres réglementations et bonnes pratiques, et certaines se recoupent. Un petit échantillon du monde entier :

ISO

La certification [ISO 27701](#) garantit le traitement adéquat des IPI (informations personnellement identifiables) dans le secteur de la santé à travers le monde.



Les exigences du [NIS2](#) garantissent le respect de la législation européenne en matière de cybersécurité.



Les règlements [DORA](#) traitent de la résilience numérique dans l'UE



[Les lois allemandes sur la sécurité informatique 1.0 et 2.0 \(das IT-Sicherheitsgesetz 1.0 und 2.0\)](#)

réglementent la sécurité informatique en définissant leurs propres exigences de conformité.



Les [critères du CIS](#) (Center for Internet Security) proposent des recommandations de configuration normatives pour assurer la sécurité des organisations.



[Cyber Essentials+](#) définit des standards minimum de cybersécurité pour toutes les organisations au Royaume-Uni.

Il y a beaucoup de réglementations complexes à suivre et à mettre en œuvre.

Une fois que vous avez identifié les obligations propres à votre organisation et à votre environnement d'appareils, l'étape suivante consiste à mettre en place les processus adéquats.

Avec une approche moderne de la gestion des appareils, les équipes informatiques peuvent automatiser une grande partie de ce travail et s'assurer en continu de la conformité de l'ensemble de leur parc.

Avec la gestion des appareils, vous pouvez :

- Appliquer des politiques de configuration et de conformité cohérentes
- Utiliser des groupes dynamiques pour attribuer automatiquement des paramètres et des actions
- Miser sur l'automatisation pour réduire les efforts manuels et maintenir la conformité au niveau des appareils.

À ce stade, tout peut sembler sous contrôle. Vous pensez même pouvoir vous éloigner un instant.

Sauf que...

Que sont les Groupes intelligents ?



Les Groupes intelligents permettent aux équipes informatiques de cibler dynamiquement des ordinateurs gérés, des appareils mobiles ou des utilisateurs selon des critères définis. Ces groupes s'adaptent automatiquement lorsque les appareils ou les utilisateurs remplissent certaines conditions ou cessent de le faire, ce qui réduit la quantité de mises à jour manuelles nécessaires.

Que sont les blueprints de Jamf ?



Les flux de configuration basés sur des règles s'appuient sur le cadre de gestion déclarative des appareils d'Apple pour administrer les réglages, les commandes, les installations d'applications et les restrictions des appareils avec davantage d'efficacité et d'autonomie.

En savoir plus sur les [blueprints de Jamf](#)

Découvrez les processus qui aident les équipes informatiques à maintenir la conformité et la cohérence de leur environnement avec le minimum d'efforts.

...En matière de conformité, la seule constante, c'est le changement.

La technologie, les pratiques commerciales et les réglementations évoluent, et les exigences de conformité évoluent avec elles. L'objectif de la conformité est d'assurer la sécurité et le bon fonctionnement des organisations, même lorsque l'environnement change. Rester en phase avec les risques de sécurité émergents et les attentes réglementaires demande des efforts continus.

Cela implique généralement :

- ✓ Des audits de conformité et des bilans réguliers
- ✓ L'application rapide des mises à jour du système d'exploitation et de sécurité
- ✓ La surveillance continue des menaces de sécurité
- ✓ Des efforts d'adaptation à l'évolution des réglementations et des politiques
- ✓ Une grande réactivité en cas de changements du rôle des utilisateurs ou des besoins d'accès

Vous trouvez la mission difficile ? En effet, c'est souvent le cas.

C'est là qu'une liste de contrôle de conformité structurée devient indispensable.

En suivant une approche claire et détaillée, les équipes informatiques peuvent organiser leurs efforts de conformité et rester en phase avec l'évolution des exigences.

Une liste de contrôle bien définie évite les oublis et veille à la cohérence des contrôles de sécurité, de la surveillance et de la mise en œuvre.

Phase de préparation

- ✓ Créez des comptes et des profils d'utilisateurs.
- ✓ Définissez les règles et les autorisations de votre organisation avec les décideurs.
- ✓ Identifiez les règles de conformité externes auxquelles votre entreprise est soumise, du fait de son secteur et de sa région d'implantation.
- ✓ Vérifiez la compatibilité matérielle et logicielle de votre parc avec tous les outils que vous utiliserez.

Que sont les critères de conformité ?

Les critères de conformité permettent aux équipes informatiques de définir, d'auditer et de mettre en œuvre la conformité de manière structurée et reproductible.

Cette approche :

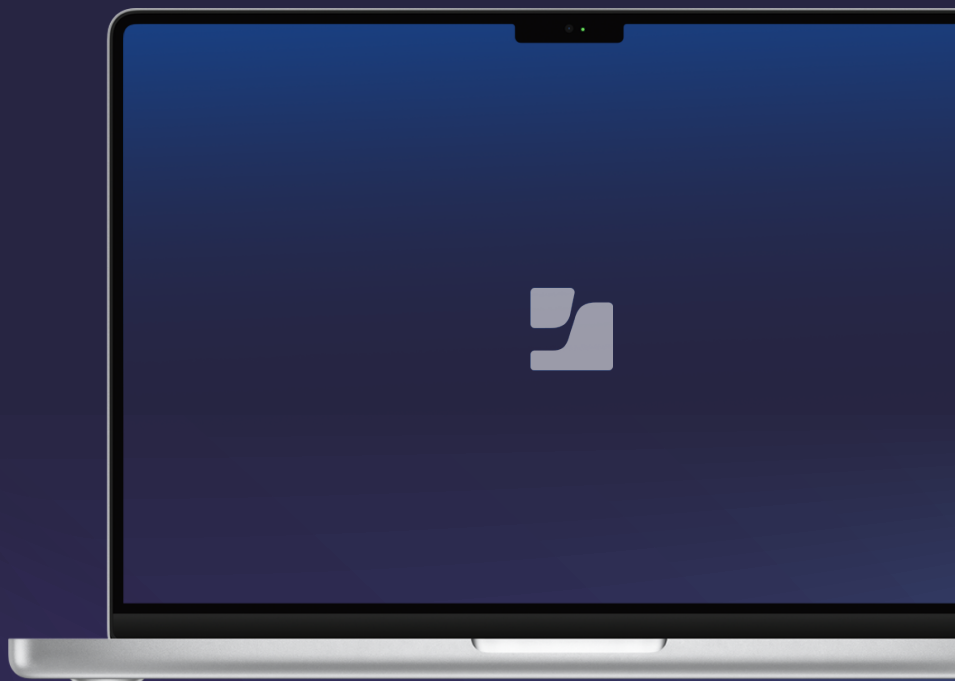
- ✓ Réduit le temps nécessaire pour vérifier la conformité et appliquer les exigences sur l'ensemble du parc d'appareils
- ✓ Simplifie l'application des normes de sécurité et des exigences de configuration complexes
- ✓ Contribue à améliorer la posture de sécurité globale de l'appareil

En automatisant l'application et la maintenance des paramètres de sécurité, les critères de conformité permettent de maintenir dans le temps l'alignement des appareils sur les normes définies.

Un exemple :

Application d'un critère de conformité, par exemple le niveau 1 du CIS

- 1 Sélectionnez le type d'application.
- 2 Définissez le groupe d'appareils concernés.
- 3 Personnalisez les critères si nécessaire.
- 4 Sauvegardez et déployez.



Maintenance et suivi continu

Les critères de conformité offrent une visibilité détaillée sur la conformité globale de l'appareil. Les équipes informatiques peuvent ainsi contrôler la conformité à chaque règle (exigences en matière de mots de passe, par exemple) pour procéder à une inspection approfondie.

Regardez une démo sur les critères de conformité :



Les critères de conformité sont basés sur le projet de conformité de macOS en matière de sécurité (mSCP), un effort commun mené par plusieurs équipes de sécurité informatique au niveau fédéral : Institut national des standards et de la technologie (NIST), Administration nationale de l'aéronautique et de l'espace (NASA), Agence des systèmes d'information de la défense (DISA) et Laboratoire national de Los Alamos (LANL).

Mise en place et configuration

Utilisez le provisionnement automatisé pour fournir à chaque utilisateur un appareil configuré correctement pour son usage et tenir à jour les applications et les paramètres d'accès.

- ✓ Utilisez les critères de conformité pour simplifier et accélérer le processus de configuration en appliquant des exigences basées sur des normes communes, telles que CIS niveau 1 ou 2.
- ✓ Utilisez des modèles de configuration prédéfinis ou créez les vôtres pour accélérer le processus et améliorer sa cohérence. Gagnez du temps et renforcez la sécurité en distribuant des réglages relatifs au code secret, aux fichiers de configuration de service et à la gestion des tâches en arrière-plan.
- ✓ Installez les applications et les mises à jour essentielles en combinant Self Service+ et les Groupes intelligents. Donnez aux utilisateurs la possibilité d'accéder librement aux outils dont ils ont besoin tout en préservant le contrôle du service informatique grâce à l'attribution automatisée.
- ✓ Configurez les paramètres de sécurité de base tels que le chiffrement du disque, les protections du système et les contrôles d'application.

Tests

- ✓ Vérifiez que les applications et les fonctionnalités du système sont opérationnelles.
- ✓ Procédez à des examens et à des audits de sécurité et de conformité.
- ✓ Vous pouvez commencer par introduire ces changements auprès d'un groupe restreint d'employés qui feront des tests sur le terrain.

Réussissez votre lancement

- ✓ Donnez des instructions claires aux utilisateurs.
- ✓ Planifiez une session sur le thème du déploiement pour répondre aux questions et résoudre les problèmes susceptibles de se présenter.
- ✓ Vérifiez que les mises à jour de conformité automatiques sont bien activées pour maintenir l'alignement des systèmes au fil de l'évolution des exigences, et réduire les efforts nécessaires pour rester au fait des protocoles de conformité.

Qu'est-ce que Self Service+?

Self Service+ est un portail destiné aux utilisateurs finaux de macOS. Il permet aux utilisateurs d'accéder à des contenus et des mises à jour préconfigurés dans Jamf Pro. Dans Self Service+, les utilisateurs peuvent :

- 1 Consulter l'état de sécurité de leurs appareils.
- 2 Parcourir, rechercher et installer des applications de l'App Store, des applications tierces, des profils de configuration et des livres.
- 3 Effectuer des tâches liées aux identités telles que la modification des mots de passe.

Bonnes pratiques et considérations futures

Pour un parc d'appareils bien configuré, sécurisé et conforme aux exigences réglementaires comme aux règles internes, choisissez les bons outils et les bons processus.

Avec la bonne approche, rester en conformité ne demande qu'un minimum d'efforts. Quant aux équipes de sécurité, elles pourront facilement produire la documentation et les rapports de conformité nécessaires aux audits et aux examens.

Tenez-vous au courant de l'évolution des lois, des réglementations et des normes de conformité en suivant les annonces des organismes de régulation. Les équipes informatiques sont tenues de connaître l'évolution des exigences réglementaires, mais cet effort peut être considérablement allégé par les mises à jour des cadres et des critères de conformité.

S'il y a une chose à retenir, c'est que les équipes informatiques jouent un rôle essentiel dans la pérennisation des efforts de conformité.

En vous informant et en explorant des ressources telles que cet e-book, vous vous dotez d'outils essentiels pour réussir dans cette mission. Mais vous pouvez également suivre cette check-list.

Enfin, gardez à l'esprit un point essentiel : en plaidant pour des pratiques de conformité efficaces et fiables, vous donnerez à votre organisation les moyens de faire face aux changements à venir.



Découvrez comment Jamf peut simplifier la gestion de la conformité.

[Demander une démo](#)