jamf

La check-list de conformité des Mac

La conformité ne concerne pas seulement le respect des exigences réglementaires. Elle est aussi un moyen de renforcer la sécurité, de réduire les risques et d'instaurer la confiance.

Pourquoi la conformité des Mac est-elle aussi importante ?

La plupart des organisations, quels que soient leur taille et leur secteur d'activité, doivent respecter des réglementations et des obligations de conformité, en particulier lorsqu'elles traitent des données sensibles.

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 du CIS, par exemple, sont des recommandations émises par le Center for Internet Security (CIS). Sans caractère obligatoire, ils sont néanmoins largement adoptés, car ils facilitent le respect d'exigences réglementaires telles que le RGPD ou la HIPAA.

Les organisations ont tout intérêt à respecter ces critères pour les risques de sécurité, renforcer la confiance des clients et éviter les sanctions. 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.

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.

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

La conformité d'une organisation est un enjeu multifacette.

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.

DORA

Les règlements **DORA** traitent de la résilience numérique dans l'UE

CIS

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

NIS2

Les exigences du **NIS2** garantissent le respect de la législation européenne en matière de cybersécurité.

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.

CYBER ESSENTIALS

Cyber Essentials+ définit des standards minimum de cybersécurité pour toutes les organisations au Royaume-Uni.

Vous en conviendrez, cela fait beaucoup de réglementations complexes à suivre et à mettre en œuvre !

Mais vous prenez votre courage à deux mains, vous faites des recherches et vous déterminez quelles réglementations s'appliquent à votre organisation et à votre environnement informatique. Désormais, grâce à votre solution MDM de classe mondiale et à votre propre processus d'assurance qualité approfondi, vous pouvez automatiser la mise en conformité de vos appareils et la contrôler en continu.

La gestion des appareils met à votre disposition :

- **Des profils de configuration, des déclarations de conformité et blueprints soigneusement conçus**
- **Des groupes intelligents pour attribuer dynamiquement des profils et envoyer des commandes ciblées**
- **Des possibilités d'automatisation pour gagner du temps et assurer une conformité immédiate des appareils.**

Bravo, vous pouvez vous déconnecter, et peut-être faire enfin cette petite sieste dont vous avez besoin depuis longtemps.

Sauf que...

...la conformité est un domaine en évolution constante.

Internet, l'informatique, les pratiques commerciales et les lois évoluent, et vos configurations de conformité doivent s'y adapter. La conformité a pour but d'assurer la sécurité et le bon fonctionnement des entreprises. Le suivi des problèmes de sécurité et informatiques émergents est un aspect important de cette démarche.

Pour cela, il faut :

- **Des audits de conformité et des bilans réglementaires réguliers**
- **Des mises à jour rapides de l'OS**
- **Une surveillance proactive des cybermenaces**
- **Une adaptation constante à l'évolution des règles de conformité**
- **Des réactions rapides en cas de changement dans le personnel et les règles susceptible d'avoir un impact sur l'accès aux données.**

Si tout cela vous semble vraiment insurmontable, c'est parfaitement naturel.

Heureusement, il y a la check-list de conformité des Mac, et il y a Jamf.

En suivant une check-list structurée, le service informatique peut uniformiser les processus de conformité pour garder une longueur d'avance sur l'évolution des règles. Pour rester constamment à jour, le plus judicieux est d'établir une liste complète d'étapes détaillées et spécifiques pour vérifier que les configurations de sécurité, les mesures de surveillance et les contrôles appropriés sont en place.

Et pour mettre à profit cette liste, il faut des solutions de premier ordre qui faciliteront le suivi, la supervision, les vérifications et les mises à jour.

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.**

Qu’est-ce que la fonctionnalité Critères de conformité ?

Intégrés à Jamf Pro, les critères de conformité permettent au service informatique de définir, auditer et faire respecter la conformité.

Cette fonctionnalité :

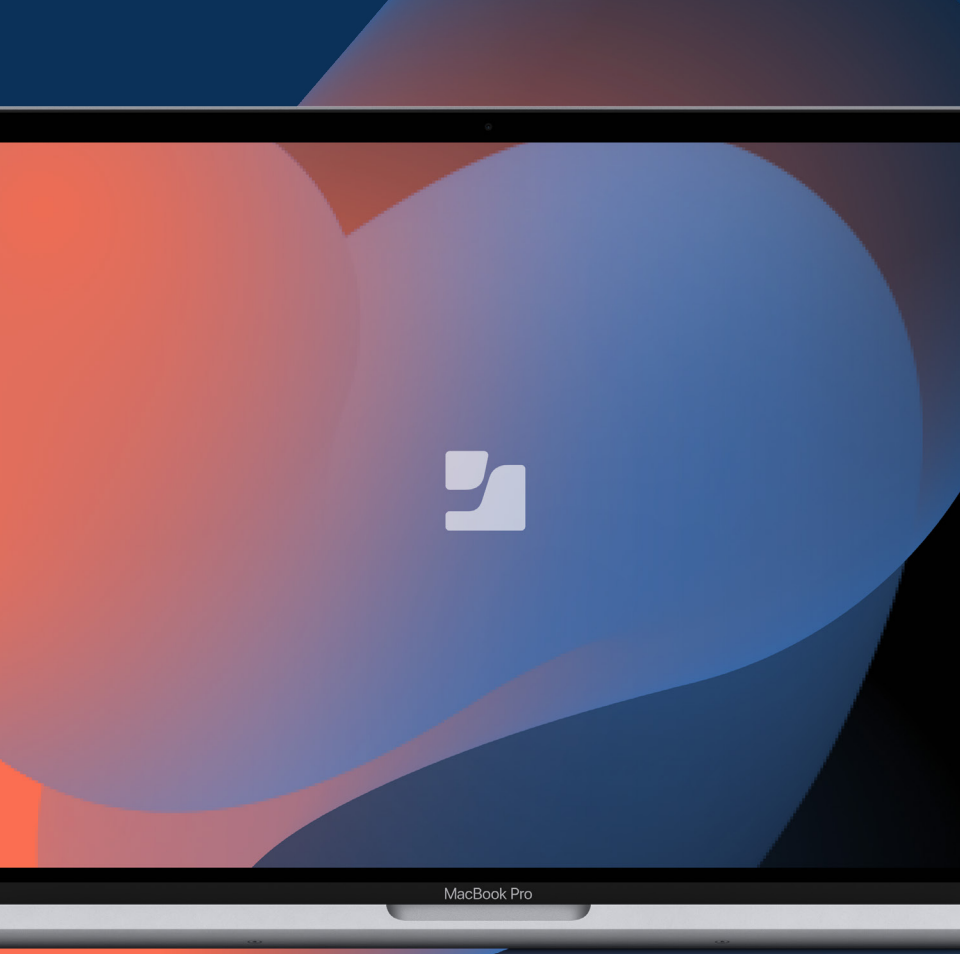
- **Réduit à quelques minutes seulement le temps nécessaire à un administrateur informatique pour auditer et appliquer des critères de conformité à son parc d’appareils, un processus qui prend normalement plusieurs semaines.**
- **Dissimule la complexité des normes de conformité, des règles et des contrôles de configuration derrière une interface utilisateur conviviale et un workflow simple.**
- **Améliore la position de sécurité des appareils du parc des clients.**

La fonctionnalité Critères de conformité crée automatiquement les profils, les règles, les scripts, les attributs d’extension, etc. Elle génère des configurations Jamf Pro qui modifient et maintiennent les réglages des appareils pour garantir la conformité au critère sélectionné.

Exemple :

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

1. **Sélectionnez le type d’application.**
2. **Ciblez des ordinateurs.**
3. **Personnalisez les critères si nécessaire.**
4. **Sauvegardez et déployez.**



Les critères de conformité ont été intégrés au Projet Conformité sécurité macOS (mSCP). Il s'agit d'un effort commun mené par plusieurs équipes de sécurité informatique opérationnelles 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).

Maintenance et suivi continus

Le tableau de bord des critères de conformité affiche tous les critères créés ainsi que leur statut. Des vues plus détaillées affichent la conformité de tous les appareils par règle de conformité (par exemple, longueur minimale des mots de passe) pour offrir un maximum de visibilité aux administrateurs.

Regardez une démo sur les critères de conformité :

Mise en place et configuration

Utilisez l'approvisionnement automatisé avec la MDM et la DDM pour que chaque appareil reçoive exactement ce dont son utilisateur a besoin et que les applications et les réglages d'accès soient tenus à jour de manière proactive.

- ✓ **Utilisez les critères de conformité Jamf pour simplifier et accélérer votre workflow. Exploitez les spécifications créées par Jamf sur la base de critères communs tels que le niveau 1 ou 2 du CIS, ou établissez des critères personnalisés.**
- ✓ **Utilisez l'un des six modèles de démarrage rapide proposés dans la fenêtre Blueprints de Jamf, ou créez le vôtre. 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 des applications et des mises à jour essentielles grâce à Self Service+ (qui permet à certains groupes d'utilisateurs de télécharger des applications et des ressources utiles à leur rôle) et aux groupes intelligents.**
- ✓ **Configurez les réglages de sécurité (FileVault, Gatekeeper, etc.).**

Tests

- ✓ **Vérifiez que les applications et les fonctionnalités du système sont opérationnelles.**
- ✓ **Réalisez des audits de sécurité : Jamf Protect conserve des journaux d'audit qui peuvent aider le service informatique dans cette tâche.**
- ✓ **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 vous recevez bien les mises à jour automatisées sur les réglages de conformité via Jamf ; vous resterez ainsi au courant des nouveaux développements de nombreux protocoles de conformité clés.**

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 de gestion des 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 le bon partenaire : Jamf.

Jamf garantit la conformité du parc d'appareils avec un minimum d'efforts des administrateurs informatiques. Quant aux équipes de sécurité, elles peuvent générer de la documentation et des rapports de conformité pour les présenter aux auditeurs.

Tenez-vous au courant de l'évolution des lois, des règlements et des normes de conformité en suivant les annonces des organismes de régulation. Les administrateurs Apple devraient toujours se tenir au courant des développements à venir dans le domaine de la conformité, mais Jamf met à jour les blueprints et les critères de conformité en cas d'évolution.

S'il y a une chose à retenir, c'est que les administrateurs 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.

Et par-dessus tout, plaidez toujours en faveur de stratégies et de tactiques de conformité plus rapides et plus fiables. Grâce à votre travail, votre organisation pourra affronter avec sérénité l'avenir et les changements qui se profilent à l'horizon.

Découvrez comment Jamf peut faciliter la conformité.

jamf

Demande une démo