Checklist de gestion et de sécurité des Mac pour les équipes informatiques en croissance

Une série d'étapes pratiques pour aider les équipes informatiques à déployer, configurer et sécuriser les Mac en toute confiance.

1. Déploiement et configuration

- [ ] Inscrire automatiquement les appareils via Apple Business Manager
- [ ] Appliquer les profils de configuration requis
- [ ] Utiliser le « provisionnement sans intervention » dans la mesure du possible
- [ ] Fournir aux utilisateurs des instructions d'intégration claires.

2. Configuration et profils de référence

- [ ] Appliquer le chiffrement FileVault
- [ ] Activer le verrouillage d'activation
- [ ] Appliquer une configuration de référence sécurisée
- [ ] Définir les autorisations et les restrictions du système
- [ ] Définir des versions minimales du système d'exploitation

3. Mises à jour des applications et du système d'exploitation

- [ ] Déployer automatiquement les applications requises
- [ ] Maintenir les applications à jour et appliquer les correctifs
- [ ] Planifier les mises à jour du système d'exploitation de manière à minimiser les interruptions
- [ ] Vérifier l'application des mises à jour dans l'ensemble des parcs

4. Identité et accès

- [ ] Intégrer les Mac au fournisseur d'identité dans le cloud
- [ ] Exiger une authentification forte pour les utilisateurs
- [ ] Appliquer des contrôles d'accès sensibles au contexte
- [ ] Aligner les niveaux d'accès sur les rôles des utilisateurs

5. Sécurité des points de terminaison

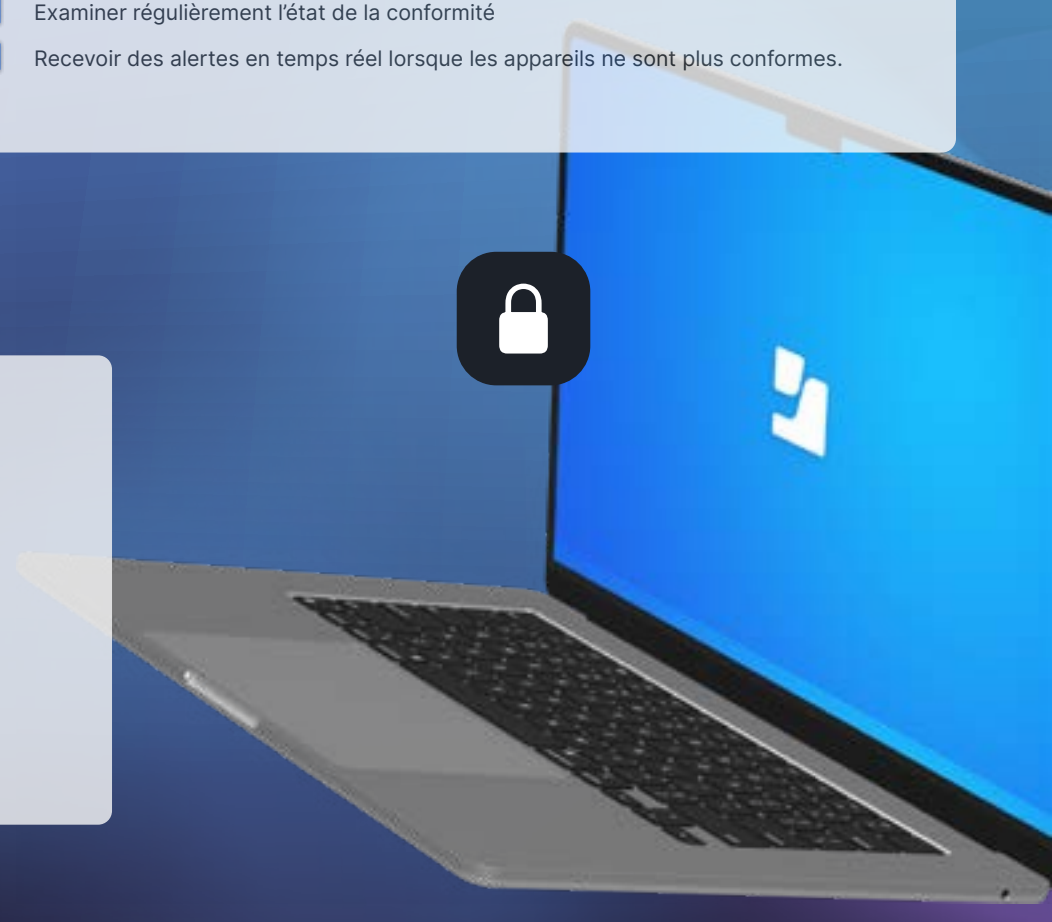
- [ ] Mettre en place la prévention des menaces optimisée par l'IA et le ML
- [ ] Utiliser la détection et le blocage sur l'appareil
- [ ] Surveiller les activités à risque sur les points de terminaison
- [ ] Réagir rapidement aux incidents
- [ ] Limiter l'accès aux ressources sensibles

6. Conformité et surveillance

- [ ] Comparer l'état des appareils aux critères du cadre que vous aurez choisi
- [ ] Utiliser des workflows automatisés pour appliquer des règles
- [ ] Examiner régulièrement l'état de la conformité
- [ ] Recevoir des alertes en temps réel lorsque les appareils ne sont plus conformes.

7. Sensibiliser et former les utilisateurs

- [ ] Former les utilisateurs à reconnaître l'hameçonnage
- [ ] Promouvoir un comportement et des pratiques sécuritaires
- [ ] Encourager le signalement rapide des activités suspectes
- [ ] Renforcer la formation au moment de l'intégration



En unifiant la gestion et la sécurité, les équipes informatiques peuvent réduire la complexité des opérations et mieux protéger leur parc de Mac au fil de sa croissance.

Télécharger

Téléchargez le Guide complet de la gestion et de la sécurité des Mac pour les entreprises.

jamf

www.jamf.com/fr/