jamf

Votre solution de sécurité mobile va-t-elle au-delà de la MDM ?

Cochez toutes les affirmations qui décrivent votre situation, puis calculez le total ci-dessous.

1.

DÉFENSE CONTRE LES MENACES

Les menaces qui pèsent sur les appareils mobiles ne disparaissent pas une fois qu'ils sont inscrits.

- [ ] Nous comptons sur la MDM pour protéger les appareils, sans lui ajouter de solution de protection contre les menaces mobiles.
- [ ] Si un utilisateur clique sur un lien d'hameçonnage sur son iPhone ou son iPad, nous n'avons qu'une capacité limitée à le détecter ou à réagir automatiquement.
- [ ] Nous n'avons pas de moyen simple d'identifier les applications qui augmentent les risques de sécurité sur les appareils gérés.
- [ ] Nous ne disposons que d'une visibilité et d'une protection limitées sur les réseaux Wi-Fi non sécurisés et les autres menaces mobiles liées au réseau.

2.

CONFORMITÉ ET ÉTAT DES APPAREILS

On ne peut régler un problème sur lequel on n'a pas de visibilité continue.

- [ ] Nous n'avons pas de vue en temps réel des appareils mobiles qui sont conformes à un instant T.
- [ ] Il nous est difficile de détecter les dérives de configuration avant qu'elles n'aient des répercussions sur les utilisateurs ou la conformité.
- [ ] Ce sont généralement les utilisateurs qui portent à notre connaissance les problèmes affectant les appareils mobiles.
- [ ] Nous ne pouvons pas garantir le respect systématique des exigences relatives aux versions du système d'exploitation et des applications sur tous les appareils mobiles.

3.

MISES À JOUR ET GESTION DES FAILLES

Chaque mise à jour retardée introduit un risque inutile.

- [ ] Nous ne pouvons pas garantir que tous les appareils mobiles disposent de la version la plus récente de leur système d'exploitation.
- [ ] Les mises à jour essentielles des applications doivent toujours être installées par les utilisateurs.
- [ ] Les échéances de mise à jour ne sont pas systématiquement respectées sur l'ensemble de notre parc d'appareils mobiles.
- [ ] Il arrive parfois que des appareils ne soient plus conformes parce que les mises à jour ne sont pas installées à temps.

4.

IDENTITÉS ET ACCÈS

L'identité ne représente qu'une partie du dispositif de sécurité.

- [ ] Notre plateforme d'identité n'évalue pas la posture de sécurité des appareils mobiles au moment de l'authentification.
- [ ] Un appareil mobile compromis ou non conforme pourrait tout de même accéder aux applications professionnelles.
- [ ] Les politiques d'accès partent du principe que les appareils inscrits sont fiables, quel que soit leur état de sécurité réel.
- [ ] Nous n'empêchons pas systématiquement l'accès des appareils mobiles à risque ou non conformes.

Pourquoi ces questions sont-elles aussi importantes ?

La gestion des appareils mobiles est un fondement indispensable, mais configurer les appareils ne suffit pas à assurer leur sécurité face au paysage des menaces d'aujourd'hui. Il faut combiner la protection contre les menaces, la conformité en continu, les mises à jour régulières et le contrôle des accès basé sur l'identité pour réduire efficacement les risques.

Plus vous avez coché d'affirmations, plus il est probable que votre environnement présente des failles de sécurité qui sortent du contrôle de la gestion des appareils.

Votre résultat

De 0 à 4 → **Des bases solides**

Votre stratégie de sécurité mobile couvre bon nombre des fonctionnalités dont les équipes informatiques modernes ont besoin. Cet article peut vous aider à valider votre approche et suggérer de nouvelles pistes pour renforcer votre environnement.

De 5 à 9 → **Une marge d'amélioration**

Votre environnement présente plusieurs failles de sécurité courantes qui peuvent exposer vos opérations à des risques croissants au fil du temps. De nombreuses entreprises se retrouvent dans cette situation lorsque leur parc mobile se développe. Découvrez comment le protéger efficacement sans ajouter de complexité inutile.

De 10 à 16 → **L'heure est venue de moderniser votre approche**

La gestion des appareils doit assumer des responsabilités pour lesquelles elle n'a pas été conçue. En enrichissant votre stratégie d'outils de protection contre les menaces, de conformité continue et d'accès basé sur l'identité, vous pourrez réduire les risques de votre environnement tout en simplifiant les opérations. Ce document propose une feuille de route concrète pour moderniser votre stratégie de sécurité mobile.

Prêt à aller plus loin que la MDM ?

Découvrez comment faire converger la gestion des appareils mobiles, la protection contre les menaces et la conformité au sein d'une stratégie de sécurité moderne pour protéger iPhone et iPad.

Obtenir l'article

jamf

www.jamf.com/fr/