

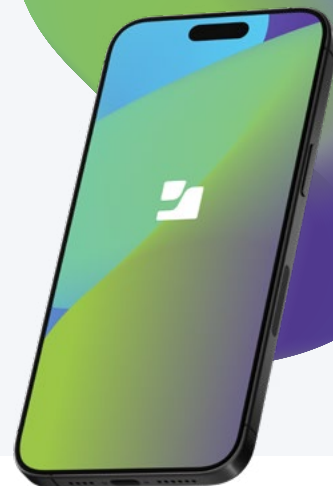
# Guide d'achat de la sécurité mobile

## Assurez la protection de tous vos terminaux

Les équipes mobiles font face à des menaces en constante évolution.

Pour maximiser les chances de succès d'un déploiement mobile, il faut une visibilité détaillée et des actions décisives.

Les employés travaillent de plus en plus souvent à distance de leur bureau ou hors des locaux de leur entreprise, et ils utilisent pour cela des appareils mobiles. La protection de ces terminaux modernes dispersés est d'autant plus délicate que les utilisateurs sont visés par de nouveaux vecteurs de menace.



Les cybermenaces ne pèsent pas seulement sur nos ordinateurs. Le risque pour les appareils mobiles est réel.

- **40 %** des appareils mobiles utilisés au travail présentent une vulnérabilité connue.
- Les employés ont **50 %** plus de risque d'être victimes d'une attaque de phishing sur un appareil mobile que sur un ordinateur portable.
- **1 %** des travailleurs mobiles sont touchés par des logiciels malveillants, et les pirates utilisent des menaces persistantes avancées (APT) pour cibler les utilisateurs avec une précision impressionnante.

La **sécurité des mobiles** est donc indispensable pour protéger les équipes mobiles, leurs appareils et les données de l'entreprise. Un programme de sécurité mobile robuste doit comprendre plusieurs aspects clés :

- Prévention des mauvaises configurations de sécurité
- Blocage des attaques
- Détection des compromissions grâce à des outils robustes d'analyse criminalistique et de réponse aux incidents

## Caractéristiques principales

De quelles fonctions de sécurité devez-vous envisager d'équiper votre parc mobile ?

### Gestion des configurations sécurisées



#### Renforcement des appareils mobiles

- Mettez en place une bonne hygiène de sécurité
- Effectuez des audits de conformité
- Détectez les vulnérabilités de configuration

#### Gestion des correctifs

- Hiérarchisez l'application des correctifs grâce à des rapports détaillés sur les vulnérabilités
- Atténuez les vulnérabilités des OS et des applications

#### Prévention des pertes de données

- Contrôlez la circulation des données d'entreprise entre les applications
- Limitez l'accès aux applications en fonction de l'état de l'utilisateur ou de l'appareil

#### Règles d'utilisation acceptables

- Limitez l'utilisation du Web grâce à des règles dynamiques basées sur des catégories.
- Appliquez les RUA par utilisateur, groupe, région ou configuration globale

### Prévention des attaques



#### Logiciels malveillants et autres risques liés aux applications

- Bloquez les logiciels malveillants
- Identifiez les applications vulnérables et à risque.
- Prévenez les fuites de données sensibles dans les applications
- Surveillez l'utilisation des applications provenant de boutiques d'applications alternatives

#### Attaques de l'homme du milieu

- Identifiez les points d'accès indésirables et les attaques de protocole
- Empêchez les attaques de l'homme du milieu en utilisant des tunnels chiffrés

#### Menaces sur le Web

- Prévenez les tentatives de phishing et les attaques zero-day
- Bloquez le trafic réseau malveillant, les tentatives de commande et contrôle (C2) et l'exfiltration de données
- Neutralisez le cryptojacking, le spam et autres menaces basées sur le Web

### Accès sécurisé



#### Protégez les données en transit

- Créez des tunnels chiffrés vers les applications et les données clés de l'entreprise

#### Contrôlez l'utilisation des applications stratégiques

- Obtenez des rapports sur toutes les applications utilisées par les employés mobiles

#### Appliquez des règles d'accès en temps réel

- Établissez des règles d'accès intégrant des informations sur l'utilisateur et un contrôle de la posture de l'appareil.

### Détection et prise en charge des menaces



#### Collectez des données télémétriques riches

- Rassemblez des journaux détaillés pour les analyser hors ligne

#### Détection des anomalies

- Recherchez les menaces et les anomalies pouvant trahir une activité malveillante
- Intégrez les indicateurs de compromission et les découvertes aux renseignements sur les menaces pour améliorer les détections suivantes.

#### Correction des menaces

- Interdisez l'accès aux applications et aux données stratégiques en cas de détection d'une compromission
- Supprimez les logiciels malveillants pour rétablir la productivité de l'utilisateur

## Créez un environnement Trusted Access avec Jamf

Jamf aide les organisations à protéger leurs actifs les plus précieux. Pour cela, la solution veille à ce que seuls les utilisateurs autorisés, munis d'appareils inscrits et conformes aux règles de sécurité de l'organisation, puissent accéder aux applications métier sécurisées.



## Choisissez judicieusement vos capacités de sécurité mobile

Le paysage des menaces évolue constamment, tout comme nos méthodes de travail. Les protections efficaces d'hier ne garantissent plus notre sécurité aujourd'hui. Voici une sélection de facteurs essentiels pour bien choisir votre solution de sécurité mobile.

### Étudiez les capacités de la solution.

Il est important d'examiner les fonctionnalités réelles de la solution. En effet, la simple mention d'une fonction de « sécurité mobile » ne suffit pas. Votre solution doit couvrir les menaces propres aux appareils mobiles, sans se contenter de calquer sur ces appareils les concepts de sécurité des ordinateurs.

### La sécurité passe par la gestion des appareils.

Une solution de sécurité isolée ne répondra pas nécessairement à tous vos besoins, et un logiciel de sécurité ne suffit pas. La gestion des appareils joue un rôle clé dans leur sécurité. Comme vous le savez, on ne peut pas sécuriser ce que l'on ne voit pas. Votre logiciel de gestion est là pour maintenir les appareils en conformité et corriger les problèmes éventuels.

### L'expérience utilisateur a une grande importance.

Les employés utilisent des appareils mobiles parce qu'ils leur permettent d'être productifs. Les règles de sécurité qui entravent leurs fonctionnalités, loin d'aider les utilisateurs, les incitent souvent à trouver des raccourcis officieux pour les éviter.

Les appareils mobiles ont évolué et ce sont aujourd'hui des outils de travail indispensables à la productivité des utilisateurs. Lorsqu'une règle déclenche une action sur un appareil, il est impératif que le workflow de correction permette à l'utilisateur de reprendre le travail le plus rapidement possible.

Tous les appareils n'ont pas besoin des mêmes outils de sécurité. Tenez compte du scénario de déploiement et des cas d'utilisation avant d'installer des outils et de configurer des règles. Par exemple :

- Réfléchissez à la manière dont vos employés utilisent leurs appareils. Le rôle qu'ils occupent dans l'entreprise influe sur leur niveau de risque. Par exemple :
  - Un employé standard ayant accès à certaines données sensibles et au web a besoin d'une protection contre les menaces courantes. Ses appareils doivent être maintenus en conformité et protégés contre le phishing et les logiciels malveillants. Le filtrage du contenu, la défense contre les menaces et l'accès réseau Zero Trust renforceront encore sa sécurité.
- Pour un employé sans bureau, dans le commerce de détail notamment, le filtrage du contenu et la sécurité des applications sont très appréciables. Si son appareil n'a pas accès à un navigateur, le risque de phishing est moindre.
- Les cadres et les personnes qui ont accès à des données stratégiques sont souvent la cible d'attaques. Ils ont besoin de protections supplémentaires et doivent souvent remplir des obligations réglementaires.