jamf

Gérer et sécuriser vos terminaux les plus vulnérables : les appareils mobiles.

Lorsque l'on parle d'appareils mobiles, on pense aux ordinateurs portables, aux tablettes et aux smartphones. Ils entrent effectivement tous dans la catégorie « mobile », mais nous allons nous intéresser spécialement aux smartphones et aux tablettes. Des millions d'utilisateurs dans le monde s'appuient sur ces appareils pour accomplir leurs tâches professionnelles, scolaires ou personnelles au quotidien. Mais cette dépendance suscite de vives inquiétudes sur le plan de la sécurité.

Vous pouvez maintenir la sécurité et la conformité de vos terminaux mobiles tout en offrant une expérience utilisateur mémorable. Après avoir lu ce guide, vous aurez toutes les cartes en main pour appliquer à vos appareils mobiles les mêmes standards de sécurité que ceux du reste de votre parc, de façon efficace et performante.

L'état de la sécurité sur mobile

Les appareils mobiles offrent aux organisations la possibilité d'uniformiser les opérations de leurs différentes fonctions. Particulièrement faciles d'utilisation, ils permettent d'accéder aux applications et aux ressources partout, ce qui les rend indispensables pour aider les équipes de première ligne et celles du siège à rester connectées et productives.

Découvrons ensemble :

L'état de la sécurité mobile

Le paysage des déploiements mobiles en entreprise

L'approche holistique de la gestion et de la sécurité des appareils mobiles

Les clés de l'unification de la gestion et de la sécurité Mac et mobiles

Les organisations doivent souvent prendre en charge différents modèles de propriété pour les appareils mobiles : déploiements partagés ou individuels pour les travailleurs de première ligne (personnel infirmier, vendeurs, etc.), COPE (appareil d'entreprise géré par l'employé) et BYOD (utilisation de l'appareil personnel au travail). Les équipes informatiques chargées du déploiement et de la gestion doivent appliquer à chaque modèle des configurations de sécurité sur mesure. Sur un appareil partagé et étroitement contrôlé comme sur un appareil personnel régi par des impératifs de protection de la vie privée, il faut également améliorer l'expérience utilisateur dans son ensemble.

La généralisation et la dépendance croissante à l'égard des mobiles ont de lourdes conséquences en matière de sécurité. Voici les plus courantes en entreprise :

- Risques supplémentaires de fuites de données
- Accès non autorisé aux informations privées de l'utilisateur
- Expérience utilisateur en décalage par rapport à l'appareil mobile
- Mise en œuvre et maintien de la conformité

Il existe toujours un fossé entre les règles de sécurité conçues pour protéger les ordinateurs et leur application sur les appareils mobiles. Ces lacunes peuvent affaiblir la posture de sécurité de ces derniers – et donc celle de l'organisation dans son ensemble. Il faut également tenir compte de la complexité introduite par la prise en charge de plusieurs plateformes, qui affecte la vitesse des déploiements mobiles à plusieurs titres. La délivrance des appareils d'entreprise comme la sécurisation des données professionnelles sur les appareils personnels deviennent de vrais enjeux. Et tout cela sans porter atteinte à la vie privée de l'utilisateur ni à l'ergonomie de son appareil.

Il est également essentiel de savoir si votre organisation limite l'utilisation des appareils mobiles qui ne sont pas couverts par un programme BYOD. Si vous pensez que votre organisation est à l'abri des menaces mobiles, vous devez réévaluer la situation. Commencez par vous demander si vous autorisez l'utilisation des appareils mobiles personnels.

Les appareils peuvent contenir des données sensibles ou jouer un rôle clé dans des workflows essentiels pour l'entreprise. Pensez, par exemple, aux appareils mobiles utilisés par les directeurs et les vice-présidents. Souvent utilisés pour les communications professionnelles, ces appareils sont également des vecteurs d'attaque attrayants. Pensez également aux appareils déployés pour des cas d'utilisation spécifiques, comme les iPad des commerciaux de terrain ou ceux des ouvriers d'un atelier de fabrication. Ces appareils sont « sur le terrain », mais ils doivent aussi répondre à des exigences spécifiques de conformité et de facilité d'utilisation.

Les moteurs de la mobilité

La mobilité en entreprise est étroitement liée à l'évolution de nos méthodes de travail. Elle a fait émerger des défis importants qui ont imposé un changement rapide des modèles d'organisation. Cette transformation a été motivée par différents facteurs :

- La migration des opérations vers les services cloud
- La distribution croissante des équipes
- La prévalence croissante des applications mobiles natives

Le développement et l'utilisation des applications métier mobiles épousent l'évolution des environnements de travail dans lesquels les appareils mobiles sont devenus indispensables. Cela s'explique principalement par leurs qualités pratiques, leur polyvalence, leur ergonomie et leur rentabilité.

Il s'agit de souligner l'importance des appareils mobiles et des applications professionnelles dans le contexte d'un lieu de travail moderne et global :

Les appareils mobiles au service de l'efficacité au travail :

Essentiels pour accéder partout aux applications et aux réseaux de l'entreprise, les appareils mobiles permettent de travailler de manière plus intelligente et efficace.

Popularité des applications mobiles :

Les appareils mobiles prennent en charge des workflows critiques et abritent des données sensibles, et sont de ce fait des cibles de choix pour les pirates. Les appareils utilisés par les cadres ou les équipes de terrain doivent concilier convivialité et conformité.

Des workflows polyvalents :

Les appareils mobiles permettent de créer des workflows efficaces : visioconférences, messagerie, gestion des stocks, accès aux informations sur les clients, édition de documents et e-mails, tout cela en déplacement.

Attentes de performances sur mobile :

De nombreux utilisateurs utilisent des appareils mobiles en plus, voire à la place, de leur ordinateur de bureau. Ils s'attendent donc à ce que les technologies mobiles soient tout aussi simples et efficaces que les autres outils de travail.

Innovation sur le lieu de travail :

Les appareils mobiles favorisent l'innovation sur le lieu de travail en dopant la satisfaction, la productivité et la fidélité des employés. Les gains d'efficacité qu'ils permettent aident les entreprises à s'adapter au changement.

Croissance continue des mobiles :

Les appareils mobiles dominent l'utilisation d'Internet et les usages professionnels, avec une part de marché mondiale de 62,22 % en 2024, loin devant les ordinateurs de bureau et les tablettes, selon Statcounter GlobalStats.

Environnements de travail à distance et hybrides :

L'adoption du mobile reste cruciale pour le télétravail et les pratiques hybrides, surtout lorsque l'on sait que 95 % des employés privilégient les options à distance. Les appareils mobiles favorisent la collaboration et la mobilité, quelle que soit la localisation.

Pénétration mondiale des appareils mobiles :

En 2024, 7,4 milliards de personnes dans le monde possédaient un téléphone mobile, dont 71 % de smartphone (environ 6,7 milliards d'abonnements), ce qui souligne l'ampleur de l'adoption mondiale de la téléphonie mobile.

Le paysage des déploiements mobiles en entreprise

Par le passé, les organisations choisissaient délibérément de centraliser leurs besoins métier sur une plateforme unique – Microsoft Windows la plupart du temps. Elles devaient acquérir des machines compatibles avec le système d'exploitation (OS) choisi. Grâce à des accords d'entreprise avec Microsoft, les organisations pouvaient retarder le déploiement de la version la plus récente de Windows jusqu'à ce qu'elles soient prêtes pour la transition. Les précédentes versions de l'OS restaient prises en charge pendant une période prolongée, précisément pour répondre aux besoins de ces organisations.

Mais c'est là qu'émerge le défi : le paysage de la mobilité, traditionnellement axé sur le consommateur particulier, considère les correctifs OS comme des mises à jour urgentes à installer dès leur publication. Les utilisateurs peuvent choisir le moment où ils installent les mises à jour et le font généralement dès leur sortie. C'est d'ailleurs ce qui freine les entreprises, confrontées à :

- Un panel divers d'OS mobiles
- Hétérogénéité de la prise en charge des versions de chaque OS
- Évolution des méthodes de déploiement selon les types d'OS
- Prise en charge incomplète retardant les mises à niveau
- Variabilité de la prise en charge des applications professionnelles selon les versions d'OS
- Manque de coordination dans les mises à jour et la prise en charge des fonctionnalités par les développeurs
- Diversité des modèles de propriété qui ont un impact sur la gestion (par exemple, BYOD ou COPE)
- Inégalité de la prise en charge des fonctionnalités dans les solutions MDM (frameworks natifs et non natifs)
- Niveaux de sécurité variables selon les types d'OS
- Limitation de l'application des politiques à des fins de conformité

Des inquiétudes croissantes

Nous avons évoqué les problèmes de sécurité liés à l'adoption rapide des appareils mobiles en entreprise. Dans cette section, nous allons nous pencher sur les menaces qui ciblent les appareils mobiles et les risques associés à leur utilisation. Nous aborderons également sur les idées reçues concernant la sécurité des appareils mobiles sur le lieu de travail.

Le premier problème découle de la nature mobile de ces appareils, cibles attrayantes pour les acteurs malveillants pour plusieurs raisons :

Stockage de données précieuses :
Les appareils mobiles contiennent une grande quantité de données personnelles, professionnelles, sensibles (informations personnellement identifiants, ou IPP) voire réglementées (informations médicales, par exemple). Les acteurs malveillants peuvent exploiter ces informations à diverses fins, en particulier dans le cadre d'attaques contre des personnes ou les organisations. Ces données doivent être protégées par plusieurs couches de sécurité, et leur accès doit être réservé aux utilisateurs autorisés.

Risque de perte et de vol :
Les appareils mobiles sont précisément conçus pour être utilisés partout, ce qui augmente le risque de perte ou de vol. Et le vol d'un appareil par un acteur malveillant représente une menace directe pour la sécurité des données. Un bref moment d'inattention peut permettre à un pirate de compromettre un appareil ou d'y introduire une vulnérabilité.

Idées reçues sur la sécurité :
Certains pensent qu'il faut diversifier les solutions de sécurité. Mais face à l'évolution rapide du paysage des menaces mobiles, il faut une prise en charge native des cadres de sécurité des terminaux. Sans une prise en charge complète, une solution peut accroître la vulnérabilité des appareils en laissant des vecteurs d'attaque ouverts.

Trouver le juste équilibre entre protection et gestion

L'équilibre entre gestion des appareils et sécurité est au cœur de l'optimisation des technologies mobiles destinées aux employés de première ligne. Si les priorités de l'administration informatique et celles de la sécurité peuvent sembler en conflit, la réalité est qu'on ne peut se contenter de se concentrer sur l'une ou sur l'autre. Les organisations doivent étroitement intégrer ces deux aspects pour créer une solution de sécurité mobile axée sur la performance et l'efficacité.

Le défi consiste à trouver le bon équilibre. Des mesures de sécurité rigides qui verrouillent les appareils peuvent entraver l'expérience des utilisateurs et leur productivité sur le terrain. De la même façon, des mesures de sécurité laxistes mettent en péril les données et les opérations. Il ne s'agit pas de choisir entre la sécurité et la productivité, mais bien d'aligner les deux, en veillant à ce qu'elles s'harmonisent pour soutenir les équipes de première ligne et protéger les actifs de l'organisation.

Enjeux	Surprotection	Sous-gestion
Performances compromises		✔
Simplicité d'utilisation		✔
Informatique fantôme (les employés inquiets pour leur vie privée peuvent être tentés d'utiliser des appareils personnels)		✔
Contournement des mesures de sécurité de l'entreprise		✔
Sape le potentiel de l'espace de travail mobile		✔
Conformité aux exigences réglementaires	✔	
Atténuation des menaces mobiles en constante évolution	✔	
Les données professionnelles sont séparées des données personnelles dans un volume chiffré	✔	
Garantit l'application des correctifs à intervalles réguliers	✔	
Rationalise le déploiement des terminaux mobiles	✔	
Empêche l'accès non autorisé aux ressources d'entreprise	✔	
Préserve la confidentialité des utilisateurs tout en protégeant les ressources de l'entreprise		✔

Plusieurs stratégies peuvent aider les organisations à adopter une approche de la sécurité mobile qui respecte la vie privée des utilisateurs :

1 Privilégier des workflows de sécurité intuitifs : Intégrez la convivialité aux processus de sécurité. C'est aussi bénéfique pour les utilisateurs que pour les équipes chargées de gérer et de sécuriser les appareils mobiles.

2. Opter pour une sécurité centrée sur les données :
Au lieu de cibler uniquement la sécurité des appareils, centrez la sécurité sur les données. Oui, il est important de protéger les appareils, mais ils sont remplaçables. Les données sensibles, en revanche, doivent toujours être protégées.

3 Adopter différents modèles de propriété :
Soyez ouvert aux différents modèles de propriété et adaptez les mesures de sécurité pour protéger les ressources accessibles depuis les appareils des utilisateurs. La stratégie de sécurité ne doit ignorer aucun appareil pour éviter l'apparition de vulnérabilités.

4 Protection complète des données :
Garantissez la sécurité des données sous toutes leurs formes. Autrement dit : chiffrez les volumes, séparez les données professionnelles des données personnelles, et sécurisez les données transmises via n'importe quelle connexion réseau.

5 Adopter des technologies mobiles modernes :
Choisissez des technologies conçues pour répondre aux exigences des appareils mobiles d'aujourd'hui. Les outils de sécurité traditionnels sont souvent impuissants contre les menaces mobiles émergentes, et leurs protections sont généralement lacunaires.

6. Mettre en œuvre le split-tunneling :
L'efficacité des appareils mobiles est vitale. Sécurisez la circulation des données professionnelles tout en autorisant les données personnelles à contourner les protocoles de sécurité de l'entreprise. Cette approche du split-tunneling préserve à la fois la sécurité des données et la confidentialité des utilisateurs en BYOD.

Traiter les mobiles comme des ordinateurs porte ses fruits

Quelles sont les implications de l'intégration croissante entre macOS et iOS pour l'avenir de la sécurité des terminaux ?

Comparer un OS de bureau comme macOS à un appareil mobile a nécessairement des limites, mais il reste que chaque nouvelle itération de macOS et d'iOS resserre la convergence entre ces systèmes d'exploitation. Chaque nouvelle version renforce l'importance de cette intégration.

Mais toute la question est de savoir comment les organisations peuvent en tirer parti. Voici comment cette intégration englobe différents types d'appareils :

- Atténuation rapide des lacunes de sécurité
- Rétablissement transparent de la productivité
- Amélioration de l'expérience des employés
- Confiance des employés renforcée
- Mise en conformité à l'échelle de l'infrastructure
- Meilleur alignement sur les règles de l'organisation
- Processus de sécurité multi-couches complet
- Gestion bilatérale des applications
- Stratégie de défense en profondeur, quel que soit le modèle de propriété
- Des solutions de sécurité et de gestion à la fois flexibles et robustes qui se conjuguent pour une prise en charge complète

Conformité des mobiles

La conformité n'est pas l'apanage des secteurs réglementés. Si elle est essentielle dans la finance, la santé et l'éducation, elle englobe également le respect des règles établies au sein d'une organisation pour répondre à ses besoins tout en minimisant les risques pour la continuité des activités. On comprend mieux pourquoi il est essentiel d'appliquer des règles pour encadrer la mobilité à l'échelle de l'organisation, comme on le fait déjà pour les Mac. C'est ce qui permettra d'établir une stratégie de sécurité mobile globale pour l'ensemble de votre flotte d'appareils.

Prenons l'exemple suivant : les appareils mobiles sont exposés à des risques accrus de vol, de perte ou de compromission dans le contexte du télétravail – un véritable danger pour les données sensibles de l'entreprise. Avec les workflows MDM, l'équipe informatique peut appliquer des normes de chiffrement et des protocoles d'authentification sécurisés via des configurations de sécurité standardisées. En outre, les capacités d'effacement à distance permettent d'effacer en toute sécurité les données des appareils compromis.

Les organisations ont tout intérêt à élaborer un plan de conformité pour les utilisateurs mobiles, quel que soit le type d'usage.

Cette base solide permettra de faire face aux risques inhérents. Cette approche est essentielle pour atténuer les risques émergents liés, **par exemple, à des applications mobiles récentes, quand un site web mature est déjà conforme à des réglementations** telles que la loi californienne sur la confidentialité des consommateurs (CCPA).

La conformité consiste également à atténuer et à identifier les problèmes avant qu'ils ne deviennent des vulnérabilités critiques ou des infractions réglementaires. Dans ce contexte, la sécurité (surveillance) et la gestion (application) se conjuguent pour faciliter la détection et l'atténuation des menaces, en veillant à la conformité des appareils mobiles.

Les appareils mobiles sont très polyvalents, et l'utilisateur peut, par inadvertance, utiliser des services professionnels pour des tâches personnelles et inversement. Ces deux scénarios présentent des risques : mélange de données, compromission de la confidentialité, violations de données professionnelles et infractions à la réglementation.

En traitant la conformité des mobiles avec le même sérieux que les autres terminaux, les entreprises offrent à tous les terminaux qui accèdent à ses ressources le même niveau de protection contre les menaces les plus récentes. Mais les avantages ne s'arrêtent pas là : elles vont conserver un inventaire précis des appareils et un suivi de leur affectation et de leur utilisation, des accès aux données de l'entreprise et des mesures de sécurité déployées – comme pour Mac.

Dernier élément à prendre en compte : la formation continue des utilisateurs en matière de sécurité. Cet aspect est souvent négligé, mais il est vital dans un plan de sécurité mobile complet. Il doit **armer les utilisateurs de connaissances sur les bonnes pratiques de sécurité**, les workflows sécurisés et les procédures à suivre face à une menace de sécurité. Cette formation est une mesure de protection à part entière qui complète les mesures de gestion et de sécurité technique.

En d'autres termes, la cybersécurité ne relève pas uniquement de l'informatique ou de l'entreprise : elle est l'affaire de tous.

Les clés pour unifier la gestion et la sécurité des appareils mobiles

Résumons les choses clairement : la clé de la sécurité réside dans l'unification de la gestion et de la sécurité dans l'ensemble de votre flotte.

1 Convergence :
Une stratégie réussie repose sur l'intégration transparente de la gestion et la sécurité, des protocoles de sécurité robustes, au sein d'un espace de travail moderne et centré sur la mobilité.

2. Exhaustivité :
Pour relever les défis de la sécurité mobile, il faut une solution globale plutôt que des approches traditionnelles fragmentaires qui multiplient les outils sans en tirer une véritable efficacité.

3. Cohérence :
Pour assurer l'uniformité de la protection, il faut mesurer des critères de référence sur l'ensemble des appareils et les maintenir sous surveillance constante. Au moindre écart suspect, il faut déterminer si des menaces, des vulnérabilités ou des anomalies de sécurité méritent une enquête.

4. Simplicité d'utilisation :
La stratégie doit donner la priorité à l'expérience utilisateur et l'harmoniser avec la protection. L'objectif : atteindre l'équilibre délicat entre efficacité et simplicité pour les équipes informatiques, les équipes de sécurité et les utilisateurs finaux.

5 Réponse :
Les menaces de sécurité doivent être prises en charge sans délai. La hiérarchisation, l'investigation et la résolution doivent englober tous les types d'appareils, les différentes plateformes et l'ensemble de l'infrastructure.

6. Équilibre :
Trouver le juste équilibre, c'est assurer la sécurité sans compromettre l'expérience de l'utilisateur, et réaffirmer la possibilité de faire converger la sécurité et la satisfaction de l'utilisateur.

Nous imaginons un avenir où chaque appareil bénéficie d'une protection sans compromis ni concessions. Cette vision décrit notre objectif ultime : des protections équilibrées et complètes pour les données et la vie privée, étendues à chaque appareil de votre infrastructure.

Jamf peut vous aider à évaluer les besoins de sécurité de votre organisation et à déterminer comment gérer et protéger tous vos terminaux.

jamf

www.jamf.com/fr

© 2025 Jamf, LLC. Tous droits réservés.

Lancez-vous

Vous pouvez également contacter votre revendeur pour essayer Jamf gratuitement.