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 comme vous le faites pour votre flotte Mac. À l'issue de cette lecture, vous saurez comment aligner la protection des appareils mobiles sur la solution de sécurité des terminaux qui protège votre flotte Mac et ses données, pour unifier vos défenses.

Nous allons explorer :

L'état de la sécurité sur mobile

Avec les progrès de la technologie, les gens utilisent de plus en plus d'appareils mobiles. Ces appareils offrent les capacités d'un ordinateur de bureau dans un format compact, léger et économe en énergie. Utilisables toute la journée et bénéficiant de connexions réseau rapides, ils donnent accès en permanence à un large éventail d'applications et de services.

Dans le contexte professionnel, les appareils mobiles estompent les frontières des lieux de travail. La connectivité permanente au réseau affranchit les utilisateurs des plateformes en fournissant un accès en temps réel à des services basés sur le cloud. Pour une entreprise, fournir un appareil mobile à chaque employé a un coût significatif. Mais la généralisation des appareils mobiles personnels a permis l'émergence de différents modèles de propriété : appareils d'entreprise avec inscription personnelle (COPE), programmes de choix des employés et utilisation des appareils personnels au travail (« Bring Your Own Device », ou BYOD). Le BYOD offre de nombreux avantages aux entreprises. Quant aux utilisateurs, ils accomplissent leurs tâches professionnelles à l'aide de la plateforme et de l'appareil qu'ils préfèrent.

Mais cette généralisation et la dépendance croissante à l'égard des mobiles ont des conséquences plus lourdes sur le plan de la sécurité. Voici les plus courantes en entreprise :

- Risques supplémentaires de fuites de données
- Accès non autorisé aux informations privées de l'utilisateur
- Absence d'équivalence entre la sécurité des appareils mobiles et des Mac
- Difficulté d'évaluation et de maintien de la conformité
- Violations de données provoquées par la compromission des appareils

Les organisations pèchent souvent par excès de confiance dans leur sécurité. 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.

Quand la réponse est « non », une autre question s'impose : et quand le PDG utilise une tablette pendant ses déplacements ? Cette tablette, que ses enfants utilisent peut-être pour faire leurs devoirs, peut être configurée pour accéder aux e-mails privés de l'entreprise. Pensez aussi aux smartphones utilisés par les membres des conseils d'administration et les cadres dirigeants pour planifier des réunions et discuter d'opérations commerciales confidentielles. Essentiels à la communication au sein des organisations, ces appareils peuvent servir de vecteurs dans des attaques de phishing ciblé.

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 professionnelle :

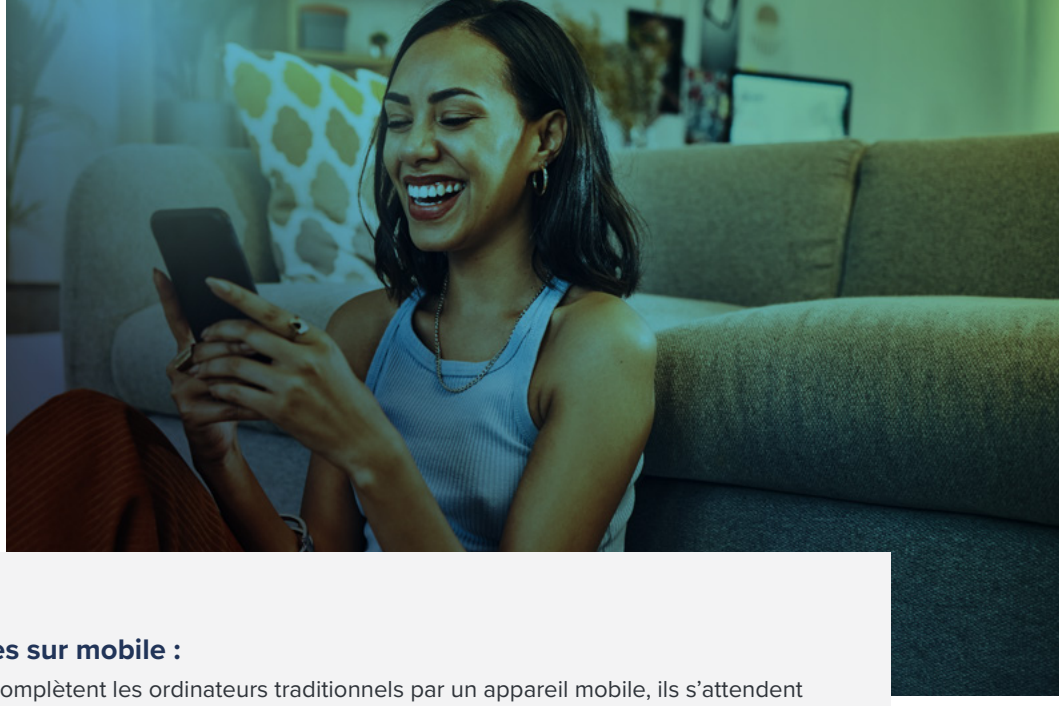
Les appareils mobiles, à commencer par les smartphones, sont devenus indispensables au travail. Grâce à eux, les utilisateurs accèdent partout aux applications métier et se connectent aux réseaux : les pratiques de travail deviennent plus intelligentes et plus efficaces.

La popularité des applications de travail mobiles :

Les applications professionnelles doivent leur popularité à leur souplesse et leur polyvalence dans les environnements de travail dynamiques. Leurs avantages pratiques, leurs capacités de personnalisation, leur ergonomie et leur rentabilité les rendent indispensables.

Workflows polyvalents :

Les appareils mobiles sont le support de workflows efficaces dans de nombreuses tâches professionnelles. Appels en visioconférence, messagerie d'entreprise, édition de documents en collaboration et traitement d'e-mails professionnels : toutes ces tâches sont simples sur un appareil mobile.



Attentes de performances sur mobile :

Les nombreux utilisateurs qui complètent les ordinateurs traditionnels par un appareil mobile, ils s'attendent à ce que la technologie mobile soit une extension simple, naturelle et efficace des outils de travail.

Innovation sur le lieu de travail :

Parce qu'ils favorisent la satisfaction, la productivité et la fidélisation des employés, les appareils mobiles jouent un rôle crucial dans l'innovation sur le lieu de travail. Ils offrent aux organisations des moyens plus simples et plus efficaces d'accomplir des tâches et s'adaptent en souplesse aux évolutions des environnements de travail.

Croissance constante de la mobilité :

Les appareils mobiles continuent de dominer le marché : ils servent principalement à accéder à Internet et à accomplir des tâches professionnelles, comme en témoigne la croissance constante de la part de marché du mobile. Selon Statcounter GlobalStats, « la répartition de l'utilisation entre mobile, bureau et tablette est de 58,72 %, 39,18 % et 2,1 % dans le monde ».

Tendances du télétravail et des pratiques hybrides : La demande en espaces de travail flexibles, accélérée par l'adoption de solutions de télétravail en 2020, encourage encore l'utilisation généralisée des appareils mobiles. La mobilité est un facteur clé des environnements de travail à distance et hybrides, fortement privilégiés par les employés. FlexJobs a en effet constaté que 97 % des employés interrogés souhaitaient pouvoir choisir le télétravail, de façon totale ou partielle.

Modèles de propriété des appareils mobiles dans le monde :

La grande majorité de la population mondiale possède aujourd'hui un téléphone mobile, les smartphones représentant une part importante de ces appareils. Selon Statistica, en 2023, 90,97 % de la population mondiale possède un téléphone mobile, qui est un smartphone dans 85,88 % des cas.

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.

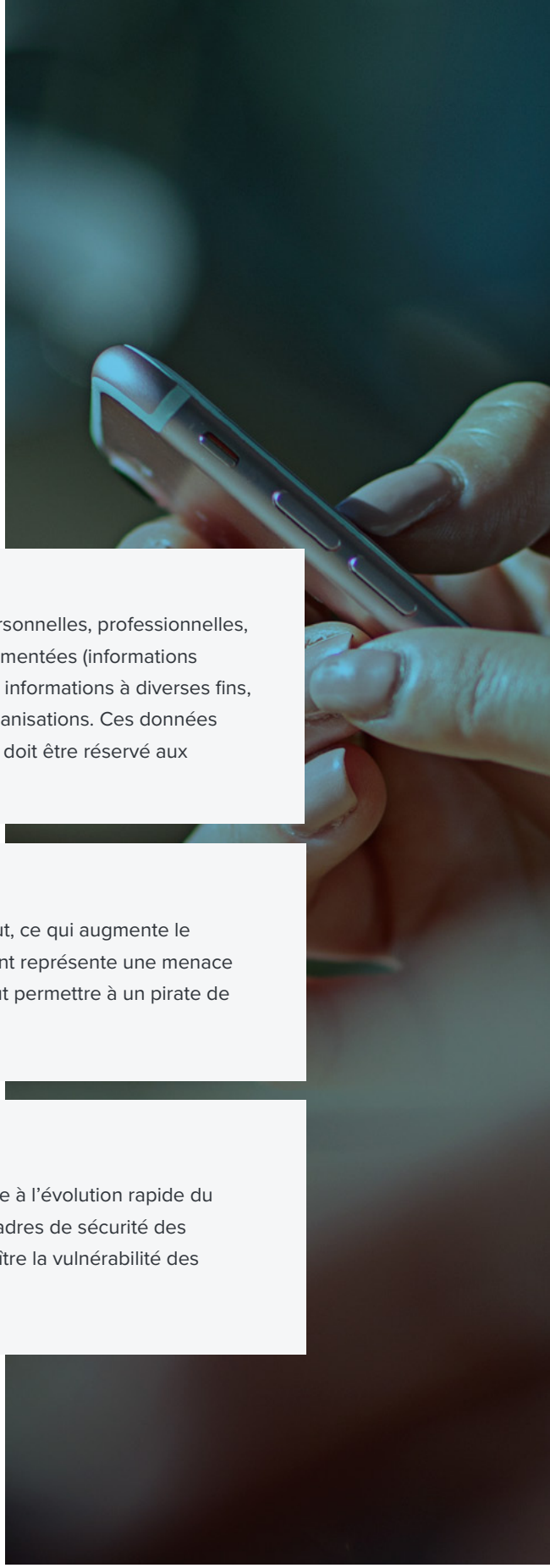
Mais c'est là qu'émerge le défi : le paysage de la mobilité, traditionnellement axé sur le consommateur particulier, considère les correctifs OS comme des mises à jour urgentes à installer dès leur publication. Les utilisateurs peuvent choisir le moment où ils installent les mises à jour et le font généralement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



1

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.

2

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.

3

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 est un concept essentiel dans le contexte de la mobilité – comme dans le domaine plus large de la sécurité et de la gestion. On le décrit d'ailleurs souvent comme un bras de fer entre les équipes informatiques et les équipes de sécurité. Mais la réalité est qu'une solution MDM ne suffit pas. Pour mettre en place une solution de sécurité mobile réellement efficace, les organisations doivent envisager la gestion et la sécurité comme deux composant étroitement liés.

Le défi consiste à trouver le bon équilibre. L'accumulation de solutions de sécurité peut dégrader l'expérience utilisateur, mais une négligence dans la sécurité mobile peut mettre en péril des actifs précieux. Il ne s'agit pas de faire un choix, mais bien d'adopter l'équilibre entre gestion et sécurité comme principe directeur d'une sécurité mobile efficace et flexible.

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		✓

L’approche holistique : les leçons du paradigme Mac

Si votre entreprise sécurise ses ordinateurs Mac, pourquoi ne sécuriserait-elle pas également les appareils mobiles ?

Quels que soient le secteur d’activité et la région du monde, des organisations du monde entier adoptent les appareils Apple au travail. Pensez-y : il y a moins de deux ans, selon Apple Statistics, le constructeur affichait un chiffre d’affaires de 365,8 milliards de dollars ! Les ventes combinées de l’iPhone (51,9 %) et de l’iPad (8,8 %) représentaient 60,7 % de ce chiffre. À elle seule, l’Apple Watch s’est vendue plus que l’iPad et le Mac (9,8 %), comptant pour 10,4 % du chiffre d’affaires total.

Les appareils mobiles font l’objet d’une demande croissante, tous systèmes d’exploitation confondus – iOS, iPadOS, Windows, Android et ChromeOS.

Il faut souligner que les stratégies employées pour protéger ces différents systèmes d’exploitation présentent plus de similitudes que de différences. Ils ne sont pas identiques, mais on peut dégager certains parallèles. L’expérience utilisateur Apple, par exemple, est réputée pour son équilibrage idéal entre sécurité, gestion et confidentialité – une approche qui peut être directement appliquée à la sécurité mobile. On peut alors envisager une stratégie globale visant à protéger tous les terminaux de votre flotte contre les menaces.

Apple est à la base d’une sécurité Mac efficace. La sécurité est au cœur du développement matériel et logiciel de l’entreprise, qui intègre dès le départ à tous ses composants des protections de sécurité et de confidentialité. Et l’utilisation des cadres natifs d’Apple vient renforcer cette base. Les développeurs qui respectent ces cadres garantissent la confidentialité, l’intégrité et la disponibilité des données à chaque interaction avec un appareil.

La conception de ces cadres a fait l’objet d’une réflexion approfondie et s’aligne sur les principes fondamentaux d’Apple de convivialité et de simplicité. Soulignons d’ailleurs que ces principes répondent à une critique fréquemment émise à l’encontre des mesures de sécurité, à savoir qu’elles nuisent à l’efficacité et au confort des utilisateurs. Une fois de plus, tout est question d’équilibre.

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 ne protègent pas toujours contre les menaces mobiles émergentes et donnent un faux sentiment de sécurité.

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 les Mac 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
- Améliore l'expérience des employés
- Renforce la confiance des employés
- 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 peuvent s'inspirer de leur plan de conformité Mac pour élaborer celui des utilisateurs mobiles. 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 mobile avec le même sérieux que la conformité Mac, les organisations vont protéger leurs terminaux mobiles 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 Mac et des 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 doit 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 représente l'objectif ultime : une technologie sécurisée et fiable pour l'entreprise, mais aussi simple et conviviale pour l'utilisateur. Notre vision : une gestion et une protection transparentes, dans tous les contextes. Nous appelons cette approche **Trusted Access**.

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

Lancez-vous

Vous pouvez également contacter votre revendeur pour essayer Jamf gratuitement.