Repenser la sécurité des terminaux pour le travail moderne

La sécurité des terminaux consiste généralement à protéger votre flotte d'appareils contre les menaces de cybersécurité.

Certes, c'est un aspect essentiel, **mais cela ne suffit pas à répondre à l'ensemble des besoins de votre entreprise en matière dans le domaine.** La sécurité des terminaux est un ensemble de capacités visant à protéger vos appareils (et vos utilisateurs) contre un paysage de menaces en constante évolution. Et vous devez choisir les bons outils pour vos appareils.

Beaucoup plus.

Vous découvrez l'écosystème Apple ? C'est la première fois que vous devez gérer la sécurité des terminaux dans le contexte des menaces ciblant Mac ou les appareils mobiles ? Ne vous inquiétez pas : Jamf est là pour vous aider à adopter une approche moderne de la gestion et de la sécurité des terminaux. Vous verrez également ce que cela signifie pour votre environnement distant ou hybride et pour l'utilisateur final, et pourrez les comparer aux solutions et concepts traditionnels. Vous comprendrez alors pourquoi ils ne sont tout simplement pas adaptés à ces plateformes modernes.

Dans ce document, nous explorons :

Qu'est-ce qui peut mal tourner ?

Pour de nombreuses entreprises, il peut être intimidant d'aborder la gestion et la sécurisation des terminaux Apple – surtout sans nuire à l'expérience de l'utilisateur final. Si l'on se souvient que pour mille appareils déployés, deux cents d'entre eux ont une configuration non sécurisée, il y a de quoi s'inquiéter.

Et si cela ne vous inquiète pas, le problème est plus grave encore. Il faut également avoir une image plus large des menaces qui pèsent sur les entreprises. Pensez simplement au vol de données : celles-ci peuvent être tout simplement exfiltrées à l'aide d'une clé USB. Les vols d'identifiants sont également fréquents, que ce soit via des attaques de phishing ou l'exploitation de vulnérabilités au niveau des apps ou de l'OS, lorsque les correctifs ne sont pas appliqués à temps.

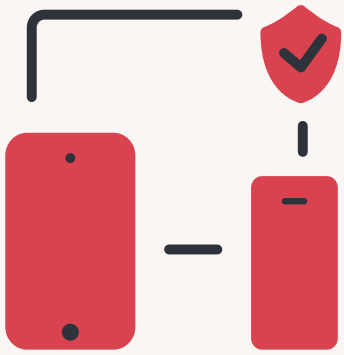
Atténuer les risques tout en gérant correctement les appareils : voilà le yin et le yang. Un équilibre entre deux aspects apparemment sans rapport qui, lorsqu'ils fonctionnent en harmonie, assurent la conformité.

En outre, aligner la sécurité et la gestion sur la conformité, pour appliquer des règles d'utilisation acceptable (AUP) notamment, permet d'éviter d'autres formes de dommages. Ceux-ci ne sont pas de nature purement technique mais peuvent avoir des conséquences désastreuses. Les entreprises peuvent en effet enfreindre malgré elles les réglementations de leur secteur. Et lorsqu'une fuite de données est rendue publique, les dommages pour la marque et la réputation d'une organisation peuvent être considérables.

39 % des organisations autorisaient l'utilisation d'appareils présentant des vulnérabilités d'OS connues dans un environnement de production, sans limiter leurs privilèges ni leur accès aux données, **contre 28 % en 2020.**

– Jamf Security 360, Rapport annuel sur les tendances

Appliquer des bonnes pratiques de sécurité aux appareils



Par où commencer pour protéger efficacement les appareils de manière claire, concise et organisée ? Tout commence par un cadre. Il doit reposer sur trois piliers centraux qui fournissent plusieurs couches de protection, conformément à une stratégie de défense en profondeur qui vous protège de divers écueils :

Manque de visibilité sur la santé des terminaux : les appareils non gérés représentent une menace importante pour les ressources et les données de l'entreprise et des utilisateurs finaux. En effet, leur état est souvent mal connu, ce qui présente un vrai risque pour la confidentialité des données.

Menaces et vulnérabilités non contrôlées : les menaces connues et inconnues, qu'elles proviennent de logiciels malveillants ou du réseau, ont un impact sur la sécurité et l'intégrité des données. Il faut disposer d'un moyen de communiquer régulièrement avec les terminaux : les équipes informatiques ou de sécurité doivent pouvoir vérifier qu'ils sont à jour, conformes et équipés de tous les correctifs avant qu'il ne soit trop tard.

Risques et problèmes de sécurité introduits par les utilisateurs : les comportements à risque mettent en danger la sécurité de vos appareils et la confidentialité de vos utilisateurs. Pensez notamment au téléchargement d'applications suspectes ou aux infractions aux règles d'utilisation acceptables.

Chacun de ces piliers détermine les modalités de mise en œuvre des contrôles de sécurité, des bonnes pratiques et des directives de sécurité des terminaux. L'objectif : protéger votre flotte Apple (macOS et iOS) contre les menaces modernes, tout en protégeant les données et en respectant la vie privée des utilisateurs.

En outre, ces piliers sont intimement liés à l'autre dimension qu'est la gestion. L'intégration entre la sécurité et la gestion forme un workflow complet qui permet de maintenir les terminaux à jour et de contrôler en permanence leur conformité, afin que l'organisation soit prête à atténuer les menaces détectées dans un cycle itératif.

1 Mettre en place des fondamentaux de sécurité

La normalisation de la sécurité des terminaux aide les organisations à identifier les besoins propres à leur flotte d'appareils. Elle informe directement la gestion en donnant la priorité à l'hygiène des appareils. Et en codifiant les bonnes pratiques de sécurité dans les règles de l'organisation, on peut aligner les besoins sur les normes de renforcement, afin de traiter les risques de façon claire et rapide.

Les applications doivent être évaluées avant leur déploiement et constamment tenues à jour, de même que les OS.
Les avantages sont multiples : applications et OS sont conformes aux bonnes pratiques de sécurité, les équipes informatiques et de sécurité administrent des logiciels qui répondent aux besoins de l'entreprise au lieu d'y nuire, les vulnérabilités sont réduites au minimum et l'assistance organisationnelle est rationalisée.

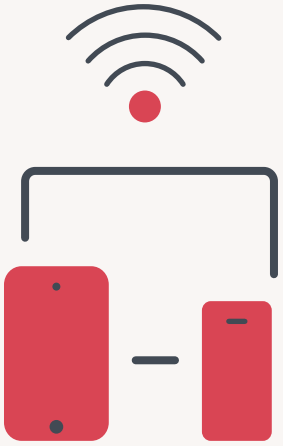
La gestion des privilèges et des autorisations des utilisateurs représente un aspect essentiel de cette démarche. En limitant les droits d'accès selon le principe du moindre privilège et en gérant les réglages des appareils, les utilisateurs accèdent uniquement aux données et aux tâches indispensables à leur travail. Tous les autres droits sont désactivés pour éviter les abus.

2 Protéger les appareils contre les menaces modernes

Au lieu de les isoler, il est essentiel d'intégrer la sécurité des points d'extrémité à la gestion. C'est comme cela que vous pourrez protéger les ordinateurs et les mobiles Apple, les utilisateurs et les données, contre les menaces modernes qui ciblent les appareils et les réseaux. Les données de renseignement sur les menaces doivent être partagées entre la gestion et la sécurité – toutes deux alignées sur le Cadre de sécurité des terminaux (ESF) d'Apple. Cette approche centralise les règles de gestion, déclenche automatiquement des workflows pour corriger les problèmes et alerte les équipes informatiques et de sécurité.

Les menaces CVE font l'objet d'une veille constante. Des analyses basées sur les signatures classent les menaces connues et les empêchent de nuire à vos terminaux. De même, l'analyse comportementale et le ML avancé identifient et atténuent les menaces inconnues ou les attaques de type « zero-day » avant qu'elles n'aient une chance de compromettre vos terminaux. Grâce à une surveillance constante et à des rapports détaillés sur l'état de santé des appareils, les solutions de sécurité tiennent les équipes informatiques et de sécurité informées en permanence. En outre, des fonctionnalités d'alertes en temps réel mobilisent les équipes d'assistance lorsqu'un terminal doit être isolé ou corrigé.

Enfin, le partage de renseignements entre gestion et sécurité apporte aux organisations de précieuses données de conformité. Avec un tel niveau d'information, les équipes d'assistance atténuent les risques identifiés et peuvent rétablir la conformité des terminaux que des problèmes de sécurité plus importants apparaissent. Elles évitent ainsi les mouvements latéraux ou les vols de données pouvant porter atteinte à la réputation de l'entreprise ou mettre en jeu sa responsabilité légale.



7 % des appareils compromis accédaient à des services de stockage dans le Cloud (tels que OneDrive, Google Drive et DropBox) et 25 % à des services d'e-mail (dont Gmail et Outlook).

Source : Jamf Security 360,
Rapport annuel sur les tendances

3 Gestion des risques initiés par les utilisateurs

Les utilisateurs représentent de loin la plus grande menace pour la sécurité des terminaux. Que les actions soient malveillantes ou involontaires, le résultat est souvent le même : les comportements à risque constituent une véritable menace pour la sécurité de votre flotte Apple et des données organisationnelles critiques ou sensibles.

L'alignement de la sécurité et de la gestion cible également les comportements potentiellement risqués des utilisateurs. Il s'appuie sur l'analyse comportementale pour identifier, par exemple, les téléchargements malveillants ou l'accès à des sites web utilisés dans des attaques de phishing, que l'appareil appartienne à l'entreprise ou à l'employé.

Les processus de sécurité sécurisent les terminaux tandis que la gestion assure le respect des règles de l'organisation, concernant notamment l'utilisation acceptable.

En ce qui concerne la protection de la vie privée, les environnements informatiques modernes prennent souvent en charge plusieurs modèles de propriété, dont le BYOD (utilisation professionnelle des appareils personnels). Il s'agit d'offrir le même niveau de protection aux appareils personnels qu'à ceux de l'entreprise. Mais la gestion et la sécurité doivent être souples trouver le juste équilibre entre protection de la vie privée et sécurité.

1 sur 10

C'est le nombre de personnes qui cliquent sur des liens d'hameçonnage sur mobile

Source : Wandera, une société Jamf

Le nombre d'utilisateurs mobiles victimes d'attaques de phishing a augmenté de 160 % par rapport à l'année dernière.

Source : Wandera, une société Jamf

Pourquoi faut-il ajouter des outils de sécurité aux fonctionnalités Apple natives ?

Les appareils Apple font partie des plus sûrs dès leur sortie de l'emballage. En raison de ses bases Unix et d'une tradition de renforcement de la sécurité et de la confidentialité, Mac possède des logiciels et des technologies de protection natifs qui limitent son exposition aux menaces de sécurité :

XProtect : logiciel antivirus qui détecte les logiciels malveillants en s'appuyant sur les signatures.

Outil de suppression des logiciels malveillants (MRT) : suppression automatisée des logiciels malveillants détectés.

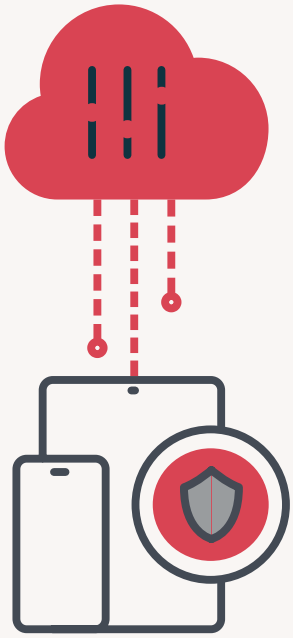
Notarisation : service d'analyse des apps qui remet un ticket numérique aux logiciels jugés exempts de logiciels malveillants.

Gatekeeper : fonctionne avec la notarisation pour garantir que seuls des logiciels fiables s'exécutent sur votre Mac.

Sandbox (mise en conteneur) : limite les dommages causés à votre Mac en cas de compromission des données utilisateur

App Store : méthode sécurisée de distribution d'applications fiables, gérée par Apple.

Autrement dit : les équipes informatiques et de sécurité ont-elles une visibilité sur les dernières menaces visant les Mac de votre organisation ? Sans une solution de sécurité et de gestion spécialement conçue pour cela, la réponse est un **non** catégorique. La quantité et la diversité des menaces visant Apple exigent des stratégies de défense à plusieurs niveaux. Il faut également prendre en charge divers modèles de propriété avec souplesse et centraliser les capacités de gestion centralisée. C'est le minimum pour répondre aux exigences croissantes du paysage actuel des menaces.

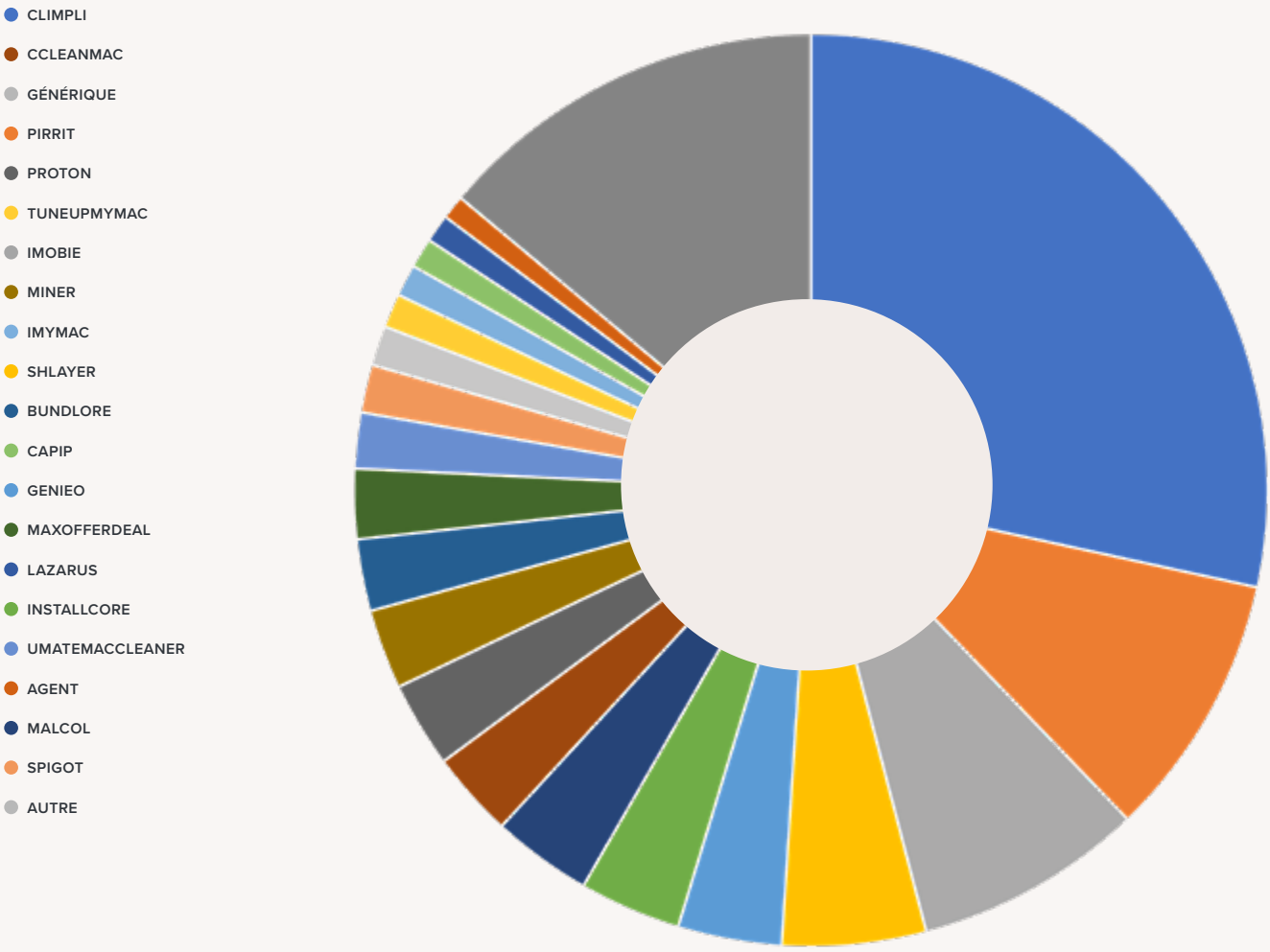


Fait amusant :

En 2021, **6 % des organisations** ont été confrontées à l'installation de logiciels malveillants sur un appareil à distance, **contre 3 % en 2020.**

Source : Jamf Security 360, Rapport annuel sur les tendances

Part des différentes familles de logiciels malveillants Mac détectées en 2021



Source : Jamf Threat Labs

Les couches de défense

Nous avons abordé les risques pesant sur les données de l'entreprise, ainsi que les trois piliers d'une stratégie de défense moderne et stratifiée – la gestion et la sécurité constituant les deux piliers de votre plan de sécurité des terminaux.

Poursuivons sur cette voie en incorporant des concepts, des composants, des technologies et des pratiques supplémentaires pour élaborer un plan de sécurité des terminaux qui réponde aux besoins uniques de votre organisation. Nous cherchons à assurer la sécurité de l'ensemble de votre flotte en intégrant les meilleures solutions du marché, conçues spécifiquement pour les terminaux Apple et adaptées aux programmes de choix des utilisateurs.

L'essentiel est de faire de l'intégration une extension naturelle de la sécurité et de la gestion. Il s'agit de travailler avec les workflows existants de sécurité de l'information et de les développer, tout en améliorant l'expérience utilisateur – et non en la détériorant.

Choix de l'utilisateur

COPE, BYOD, CYOD... Que ce soit l'entreprise ou l'employé qui choisisse et/ou possède l'appareil, la sécurité et la gestion des terminaux doivent rester au même niveau pour sécuriser les données et prévenir les menaces. Il faut donc une solution qui soit à la fois puissante et suffisamment souple pour atténuer les risques tout en permettant aux utilisateurs de travailler confortablement sur n'importe quel appareil, où qu'ils soient.

Opter pour la solution de référence

Ne vous contentez pas d'une solution qui offre une prise en charge minimale de l'écosystème Apple simplement parce qu'elle gère également les appareils Windows. Le gain apparent en termes de frais administratifs ne fait pas le poids face aux meilleures solutions. Adaptées spécifiquement aux appareils Apple, elles prennent en charge toutes les fonctionnalités dès le premier jour. C'est à vous, et non à vos logiciels de sécurité ou de gestion, de décider quand et comment gérer vos terminaux.

Intégration aux workflows de sécurité de l'information existants.

Il n'est pas nécessaire de réinventer la roue, surtout si vous disposez de workflows bien établis qui répondent aux besoins de votre organisation et à ceux de vos utilisateurs. C'est l'un des domaines où l'intégration s'avère payante pour les équipes informatiques et de sécurité. Elle leur permet de combiner leurs workflows existants aux meilleures solutions du marché afin de renforcer la sécurité et la gestion de base, sans avoir à tout repenser en raison d'une incompatibilité ou d'un manque de soutien de la part des développeurs.

Faire de l'expérience utilisateur une solution clé

Soyons réalistes, les utilisateurs en sont souvent réduits à faire ce qu'on leur dit. Dans le paysage informatique moderne, avec la généralisation du télétravail et des programmes BYOD, il faut voir les utilisateurs finaux comme une partie de la solution – et non comme un maillon faible à protéger.

La sécurité des terminaux est fondamentale

N'oubliez pas le yin et le yang : la sécurité des terminaux ne s'arrête pas à l'antivirus installé sur votre Mac ou au VPN configuré sur votre appareil iOS. Dans le paysage moderne des menaces, la sécurité (yin) et la gestion (yang) collaborent étroitement comme une solution unifiée et axée sur Apple. Elles servent de base à la myriade de technologies, de pratiques et de règles qui composent votre plan de défense en profondeur tout en assurant la conformité des terminaux.

Les idées fausses sur les solutions tout-en-un

On parle de pile centralisée quand deux solutions fonctionnent ensemble comme une unité cohésive (encore une fois, pensez au yin et au yang), offrant des avantages globaux par un effet de synergie. Ne nous y trompons pas : ce n'est pas une solution unique qui fait le gros du travail à la place des deux autres comme la « fenêtre unique » pourrait le faire croire. Ces solutions à taille unique gèrent souvent plusieurs OS, mais au prix d'une prise en charge incomplète de chacun d'eux. Et quand il s'agit de la sécurité des terminaux Apple, le manque d'efficacité est criant.

L'intégration entre les solutions = une approche gagnant-gagnant

Pour unifier la gestion et de la sécurité en une seule force impénétrable, il faut d'abord partager les données exploitées par les deux équipes. De plus, en intégrant tous les outils et workflows au sein d'une solution unique, les équipes d'assistance ont moins de problèmes à résoudre et peuvent recentrer leurs efforts sur l'autonomie des utilisateurs. Collecte de données, évaluation de l'état des appareils, génération de rapports, gestion des alertes en temps réel... tout peut être géré simplement. Des workflows permettent de trier et corriger les problèmes détectés ou suspectés avant que la situation ne se dégrade, entraînant par exemple une violation de données.

Sécurité ou performance ? Pourquoi pas les deux ?!

La sécurité est souvent considérée à travers le prisme du compromis. Pour obtenir une plus grande protection, les acteurs doivent renoncer à certaines libertés. Mais les nouvelles technologies inversent cette approche. L'accès réseau Zero-Trust (ZTNA) et ses règles tenant compte du contexte, notamment, refusent leur confiance aux terminaux et à leurs connexions. Le ZTNA s'attache plutôt à protéger les données contre les accès non autorisés et les menaces pensant sur leur intégrité. Il assure à la fois la sécurité et les performances sans compromettre l'expérience utilisateur.

Le nombre d'organisations ayant une application potentiellement indésirable installée dans leur flotte a plus que **doublé**, **passant de 5 % à 11 %.**

36 % des organisations ont rencontré **des indicateurs de trafic malveillant** sur un **appareil mobile en 2021 »**, ce qui soulève une question : **vos équipes informatiques et de sécurité sont-elles en mesure de réagir rapidement aux indicateurs de compromission ?**

Le saviez-vous ?

34 % des appareils compromis ont accédé à des services de conférence **tels que Zoom, Skype et Microsoft Teams** en 2021. Ce chiffre est passé à **64 %.**

Source : Jamf Security 360,
Rapport annuel sur les tendances

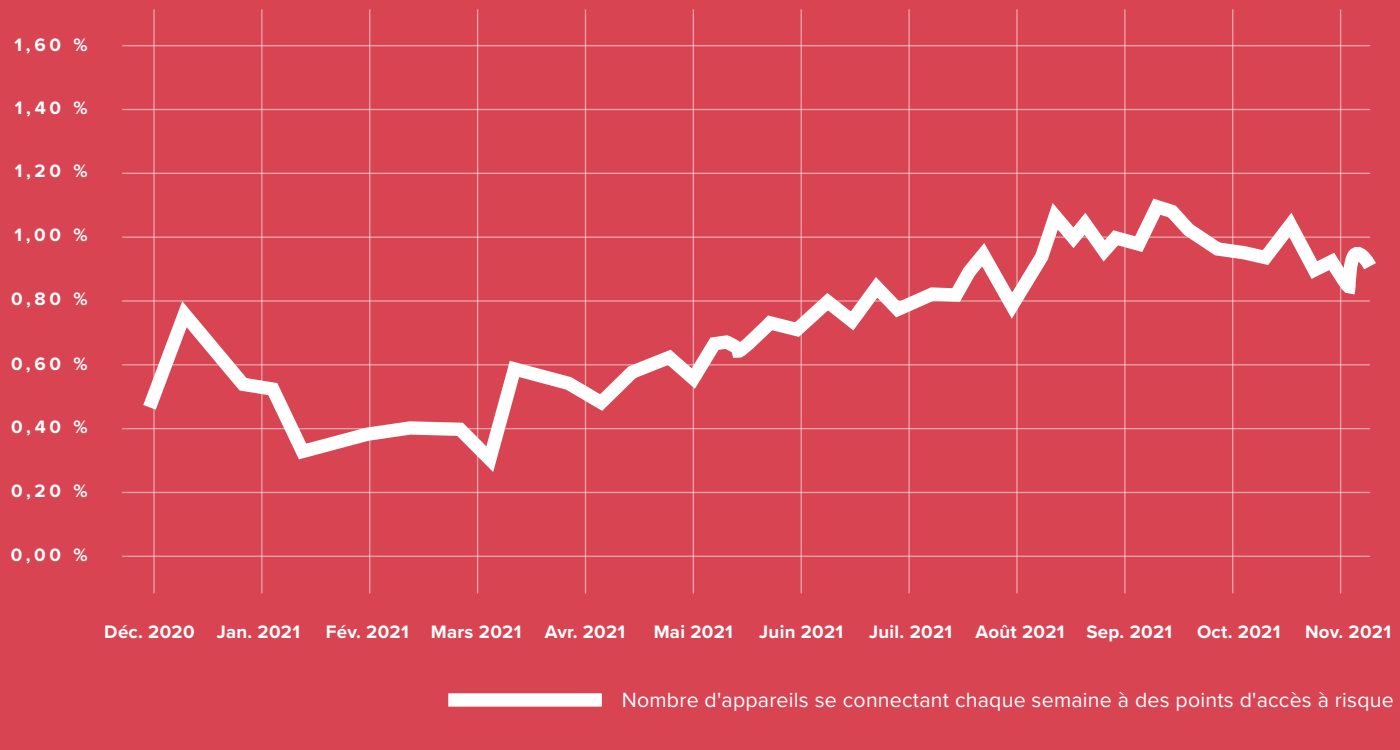
Autonomiser vos utilisateurs

L'utilisateur est important. La technologie devrait être le prolongement de l'utilisateur. Elle doit l'autonomiser, sans freiner sa productivité de quelque manière que ce soit, s'adapter aux contextes dans lesquels il se sent le plus à l'aise. Après tout, le confort rend heureux, et un utilisateur heureux sera toujours plus productif qu'un utilisateur malheureux. C'est d'autant plus le cas si l'on tient compte des environnements de travail modernes, caractérisés par les programmes de choix des employés et les initiatives BYOD. Cette évolution s'accompagne d'un transfert de l'infrastructure vers le Cloud, au service d'un environnement de travail hybride.

Selon les données de Jamf Threat Labs, « le nombre d'utilisateurs mobiles victimes d'attaques de phishing a augmenté de 160 % par rapport à l'année dernière. »

Source : Jamf Security 360, Rapport annuel sur les tendances

Nombre d'appareils se connectant chaque semaine à des points d'accès à risque



Source : Jamf Security 360, Rapport annuel sur les tendances

Principaux points à retenir :

- Évaluez vos terminaux afin de déterminer quelles protections modernes sont nécessaires pour répondre aux exigences de sécurité.
- Adoptez un cadre spécialement conçu pour protéger les appareils Apple, qui servira de base à votre stratégie de sécurité des terminaux.
- Arrêtez les logiciels malveillants, identifiez les vulnérabilités et surveillez les comportements suspects et à risque tout en atténuant les risques. Déployez des correctifs au moyen de workflows basés sur des règles afin de maintenir la conformité des appareils.
- Mettez en place et entretenez des fondamentaux de sécurité qui serviront de référence pour l'état des appareils
- Étendez les protections natives d'Apple pour donner aux équipes de sécurité une visibilité sur les menaces ciblant votre entreprise
- Intégrez la sécurité et la gestion pour déployer des solutions transparentes et atténuer rapidement les menaces détectées
- Choisissez les solutions de référence du marché. Elles doivent prendre pleinement en charge l'écosystème Apple dès la publication des nouvelles versions et s'aligner sur les cadres conçus par Apple. Les utilisateurs pourront ainsi profiter d'une excellente expérience et le service informatique gérera les mises à niveau selon son propre calendrier.
- Préservez l'expérience Apple et les performances tout en renforçant la sécurité
- Accompagnez tous les modèles d'appartenance des appareils pour optimiser la sécurité des utilisateurs, des appareils et des données – sans compromis sur le respect de la vie privée.
- Autonomisez les utilisateurs pour qu'ils soient productifs avec l'appareil qu'ils préfèrent, à l'endroit où ils se sentent le plus à l'aise pour travailler.

Découvrez la solution complète de Jamf. Spécialement conçue pour protéger les utilisateurs Apple contre les actes malveillants, elle minimise également l'impact sur la qualité d'expérience.
Ou demandez une version d'essai et voyez comment vous pouvez protéger vos utilisateurs.

Demander une version d'essai