Guide avancé de la gestion d'iOS/iPadOS

Le paysage de la sécurité

La cybersécurité continue de s'améliorer.
Selon le récent rapport Global Digital Trust Insights 2023 de PwC, la cybersécurité s'est améliorée à bien des égards depuis 2020 : parmi les 3 522 cadres dirigeants interrogés, issus d'un large éventail de secteurs et de différentes régions du monde, 70 % ont lancé des initiatives pour renforcer la cybersécurité en 2021.

Nous avons encore un long chemin à parcourir.
38 % des personnes interrogées pensent avoir complètement atténué les risques liés à la mise en place du télétravail et du travail hybride, par exemple. Et elles sont 48 % à affirmer les avoir complètement atténués. 35 % ont également indiqué avoir entièrement résolu les problèmes liés à l'adoption rapide du cloud.

Pourtant, **elles ne sont que 3 % à avoir entièrement atténué les cyber-risques émergents**. Seuls 5 % des répondants disent optimiser les cinq aspects du workflow de sécurité : identification, protection, détection, réponse et restauration.

Et les technologies mobiles ne font qu'accentuer les inquiétudes : des logiciels malveillants dissimulés dans des applications apparemment inoffensives ont d'ailleurs fait la une des journaux. Les systèmes traditionnels de sécurité et de gestion reposant sur des pare-feu sont mal adaptés aux appareils mobiles. En effet, ceux-ci ont par nature la capacité à accéder à distance aux outils de travail. Si l'on ajoute à cela la pratique croissante du BYOD dans les organisations, les inquiétudes deviennent d'autant plus légitimes.

Comment les administrateurs informatiques et les responsables de la sécurité de l'information peuvent-ils garantir la mise en place des protocoles de sécurité dans tous les domaines de l'environnement numérique, iOS et iPadOS inclus ?

Seuls

3 %

indiquent avoir pleinement atténué les cyber-risques émergents

Une bonne gestion d'iOS est une gestion sécurisée

Ce guide de gestion d'iOS et d'iPadOS fait suite à notre e-book Introduction à la gestion de l'iPhone et de l'iPad. Il détaille le rôle clé de la gestion des appareils iOS et iPadOS pour la sécurité de votre flotte Apple. Une gestion adéquate ne couvre pas à elle seule tout le paysage de sécurité. En revanche, c'est la base sur laquelle toutes les organisations doivent s'appuyer.

Pour en savoir plus sur la gestion de la sécurité, lisez la suite. Nous aborderons également les capacités, les workflows et les réglages nécessaires pour gérer en toute sécurité votre flotte d'iOS et d'iPadOS et bien couvrir les fondamentaux.

Certificats PKI et push

Certificats PKI

Un certificat PKI est un fichier texte qui contient des données d'identification sur les utilisateurs et les appareils. Très simplement, il confirme la sécurité de l'appareil mobile et sécurise les informations passant d'un endroit à l'autre grâce au chiffrement.

Le chiffrement par certificats permet de sécuriser toutes les communications, mais pas seulement. Il permet aussi de révoquer immédiatement l'accès des personnes qui quittent l'entreprise ou des appareils qui ne sont plus conformes.

Les certifications peuvent avoir de nombreux usages : authentification unique (SSO), profils d'inscription, gestion des appareils avec le binaire Jamf, profils de configuration et plus encore. Les administrateurs peuvent les déployer manuellement via un portail web. L'opération peut également être automatisée à l'aide d'un outil tiers tel que Jamf Connect, ou via une demande directe – dans ce cas, l'appareil communique avec le serveur via Jamf Pro.

Vous pouvez télécharger le certificat intégré de l'autorité de certification (CA) intégrée, le révoquer et le renouveler. Vous pouvez enfin créer un certificat intégré à partir d'une demande de signature de certificat (CSR) et créer une sauvegarde.

Certificats push

Un certificat push est un fichier chiffré généré par Apple qui établit la confiance entre un service tiers comme Jamf Pro et le service de notification push d'Apple (APNs). Le certificat push est créé par Apple, mais nécessite un service tiers (Jamf, par exemple), APNs. Il est utilisé avec un identifiant Apple d'entreprise plutôt qu'un identifiant Apple personnel.

Les certificats Push autorisent la communication entre le serveur Jamf Pro et APNs. APNs contrôle les informations échangées par les appareils, et notamment celles qui proviennent des applications. C'est avec les notifications push que les appareils reçoivent des communications.

Comme il s'agit d'un fichier chiffré généré par Apple, vous pouvez désinstaller une application à distance sur la base des informations de sécurité qu'il contient.

Comment obtenir les certificats

Sous iOS, les certificats sont stockés dans le trousseau de l'éditeur. Vous pouvez afficher une liste de certificats en les exportant dans un fichier .csv, .txt. ou XML. Jamf Pro facilite ce processus : il accompagne l'administrateur informatique dans la création d'un certificat push (.pem) et son importation dans Jamf Pro. Vous aurez besoin d'un identifiant Jamf et d'un identifiant Apple valides, et il est essentiel que les administrateurs maintiennent ces certificats à jour. En effet, dans le cas contraire, APNs perdra la connectivité avec les serveurs et les terminaux de gestion des appareils mobiles (MDM).

Accès conditionnel

Nous l'évoquions plus haut, la plupart des organisations ne peuvent plus se contenter de créer un réseau et protéger les appareils et les utilisateurs au moyen d'un pare-feu. Les appareils mobiles notamment, souvent utilisés à domicile, en déplacement ou en avion, échappent à ce type de contrôle.

L'accès conditionnel est un composant du cloud Microsoft. Il permet à une organisation de définir des paramètres pour sécuriser ses données dans plusieurs lieux différents. Il évalue les risques dans l'instant pour accorder ou non l'accès aux données de l'organisation – e-mails, OneDrive, Word et Excel, mais aussi les applications cloud comme Jamf Pro.

L'accès est réservé aux utilisateurs de confiance équipés d'un appareil vérifié : un atout de poids pour la gestion et la sécurité, quel que soit le lieu de travail.

Les iPhone et iPad de l'entreprise sont gérés par Jamf et enregistrés auprès de Microsoft Intune via un connecteur cloud ou un connecteur manuel. Le partenariat solide entre Jamf et Microsoft garantit un fonctionnement simple et fluide : Jamf envoie l'inventaire des appareils iOS et iPadOS à Intune. Intune évalue la conformité et génère un rapport. Azure AD applique les contrôles d'accès.

Conformité des appareils

La conformité des appareils comporte de nombreux composants délicats, mais parmi eux les appareils mobiles sont indéniablement les plus difficiles à appréhender. Tout d'abord, ces appareils entrent dans l'entreprise de différentes manières. Ils peuvent avoir été achetés directement auprès d'Apple ou par l'intermédiaire de revendeurs autorisés. Il peut également s'agir d'appareils personnels inscrits dans un programme BYOD. Deuxièmement, en raison des fonctions remplies par les personnes qui utilisent des iPad et des iPhone d'entreprise au quotidien, les organisations doivent souvent remplir des obligations de conformité supplémentaires. Dans un tel contexte, les appareils ne devront pas être soumis aux mêmes mesures pour respecter les exigences de votre organisation.

Les établissements de santé, souvent de grandes utilisatrices d'iPhone et d'iPad dans des contextes cliniques, doivent se conformer à la loi HIPAA. Les établissements d'enseignement supérieur sont soumis à la FERPA. Quant aux établissements d'enseignement primaire et secondaire, ils doivent satisfaire des exigences rigoureuses de conformité en matière de sécurité, imposées par le gouvernement fédéral.

Ces organisations doivent donc se munir d'un programme de gestion de la conformité des appareils complet et bien conçu. C'est absolument essentiel pour la cybersécurité, la sécurité des données et la sécurité des utilisateurs. Et pour faire appliquer ces règles, il est indispensable de faire appel à un leader du secteur de la gestion des appareils mobiles. Vous voulez en savoir plus sur la création d'une règle de conformité complète ? Apprendre à garantir la sécurité de vos appareils, de vos utilisateurs et des données de votre entreprise ? Lisez Introduction à la gestion de la conformité.

Scripts, profils de configuration et chiffrement : une collaboration harmonieuse

Scripts

L'automatisation des activités courantes est un puissant atout pour la sécurité : elle élimine l'erreur humaine et évite d'oublier des tâches essentielles. Cela peut se faire par le biais de scripts. Les scripts permettent d'automatiser de nombreuses tâches et donnent aux administrateurs davantage de contrôle sur leurs applications.

Le tout est de commencer modestement et de s'entraîner. Vous aimeriez automatiser une tâche en particulier ? Faites appel à Jamf Nation et aux autres forums d'administrateurs Mac : des collègues ont sans doute déjà créé des scripts intéressants.

Vous voulez vous plonger dans des scripts et des tâches spécifiques ? Lisez Automatiser les tâches courantes avec les scripts Apple et Jamf.

Profils de configuration

Les profils de configuration offrent à l'administrateur un moyen essentiel de renforcer son contrôle par le biais de scripts. Le plus souvent, les profils de configuration servent à appliquer des codes d'accès, configurer des réseaux Wi-Fi enregistrés, etc.

Les profils de configuration sont des fichiers XML portant l'extension .mobileconfig. Ils permettent de définir facilement les réglages et les restrictions à appliquer à des appareils et des utilisateurs. Ils utilisent généralement le service de notification push d'Apple (APNs).

Les profils de configuration peuvent appliquer des protocoles de sécurité touchant aux codes secrets, aux comportements, etc. En cela, ils sont un puissant outil de sécurité.

Les profils de configuration sont intégrés à Apple Configurator 2, au Gestionnaire de profils et à votre fournisseur de MDM. Ils peuvent être déployés sur les appareils et les utilisateurs inscrits dans la MDM.

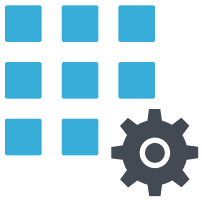
Les administrateurs peuvent également configurer les applications en fonction d'informations détaillées et de protocoles de sécurité.

Chiffrement

Les profils de configuration et les scripts sont des outils puissants, mais tout ce qui peut contrôler les actions d'un appareil doit être absolument sécurisé. Le chiffrement des disques garantit la sécurité des informations. Il chiffre le code et les scripts, qui deviennent quasiment illisibles.

Apple utilise une technologie appelée Protection des données pour le chiffrement. Certaines applications système (Messages, Mail, Calendrier, Contacts, Photos) et valeurs de données de santé utilisent la protection des données par défaut. Les apps tierces bénéficient automatiquement de cette protection.

Gestion des applications



Les apps restent l'aspect le plus important de l'expérience de l'utilisateur final. On comprend donc que leur administration représente un aspect essentiel de la gestion et de la sécurisation des appareils. De l'approvisionnement à l'hébergement, en passant par la mise à jour et le déploiement, une bonne gestion des apps est essentielle pour sécuriser une flotte Apple. Et elle favorise la productivité des utilisateurs finaux.

Configuration des applications gérées
App Config permet aux organisations disposant de solutions MDM de transmettre à distance des données à un appareil autorisé. Ces données servent, par exemple, à personnaliser l'expérience utilisateur ou le comportement de l'application.

En créant une application unique qui peut être déployée et personnalisée selon les besoins de tous vos utilisateurs, vous réduisez à la fois le coût de développement et la maintenance à long terme.

Les apps compatibles avec App Config conservent leur mode de fonctionnement d'origine pour les cas d'utilisation grand public. Mans dans un contexte d'entreprise, elles peuvent être étendues pour prendre en charge des workflows ou des environnements plus personnalisés. De plus, App Config permet de personnaliser l'interface utilisateur. Les administrateurs ont toutes les cartes en main pour adapter une application à leurs besoins. App Config donne enfin accès à des informations sur les utilisateurs et les appareils.

Apps et livres
Apps and Books est un moyen de distribuer et de révoquer collectivement des applications ou des livres iOS à des utilisateurs finaux, par l'intermédiaire d'Apple Business Manager ou d'Apple School Manager (les entreprises doivent utiliser l'un de ces outils pour accéder à Apps and Books).

La distribution des apps de l'App Store se fait par le biais d'un workflow simple et géré. Les administrateurs informatiques peuvent attribuer des applications à des groupes d'utilisateurs, en fonction des critères définis dans votre MDM.

Les apps iOS doivent répondre aux standards d'Apple pour être disponibles dans l'App Store. Elles sont donc intrinsèquement plus sûres que les applications tierces vendues en dehors de l'App Store. Pour préserver votre posture de sécurité, vous devez :

Acheter et obtenir des licences d'applications et de livres par lots auprès d'Apple.

Les distribuer aux utilisateurs via leur identifiant Apple ID, ou directement sur les appareils, sans identifiant

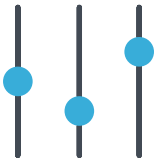
Vous pouvez lier un jeton (fourni par Apple) à votre solution de MDM Apple pour faciliter l'attribution et la distribution des ressources, et ainsi cibler les bons utilisateurs.

Quand la distribution gérée est appliquée au niveau de l'appareil, les identifiants gérés permettent de diffuser du contenu sans identifiants Apple. Cette approche est recommandée pour les appareils inscrits par les utilisateurs. Elle empêche les applications d'apparaître dans le compte App Store personnel de l'utilisateur : l'entreprise garde le contrôle sur la mise à jour et la gestion des applications professionnelles.

En revanche, quand la distribution gérée est attribuée à l'utilisateur, le contenu est installé sur l'appareil géré, mais la licence est attribuée directement à l'utilisateur. Pour cela, il faut disposer d'un identifiant Apple, qu'il soit géré ou personnel. Les utilisateurs auront également été inscrits auprès du système d'achat en volume, de manière à leur attribuer des licences avant de distribuer le contenu. De cette façon, vous pouvez :

Programmer la mise à jour automatique des applications

Forcez automatiquement les apps à se mettre à jour



Forcez manuellement les apps à se mettre à jour

Distribuer une mise à jour d'application (application spécifique seulement).

Workflows des règles d'application des correctifs
La plupart des administrateurs Apple savent déployer manuellement des règles de correctifs. Jamf propose des workflows qui prennent en charge la correction des bugs. Cet aspect est vital pour la sécurité des réseaux : les bugs présents dans les apps tierces représentent en effet un moyen très courant d'infiltrer des environnements autrement sécurisés.

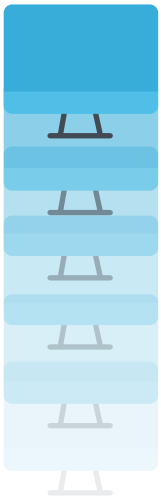
En ayant une vision complète de votre environnement d'applications, vous saurez lesquelles doivent être mises à jour, et sur quelles machines. App Installer, qui peut s'exécuter en arrière-plan, automatise ce processus.

Et le BYOD ?

Combinez l'inscription des utilisateurs basée sur le profil ou le compte avec la gestion des appareils mobiles Jamf. Ainsi armé, vous pourrez sécuriser et gérer tous les appareils appartenant aux employés. Avec l'accès basé sur l'identité, les administrateurs gèrent et protègent les appareils en fonction des personnes qui les utilisent.

Pour en savoir plus sur la création d'un programme BYOD sûr et bien géré, lisez Jamf et Apple : une meilleure approche du BYOD.

Actions groupées



Les actions groupées offrent un autre moyen d'effectuer plusieurs tâches fastidieuses sur de nombreux appareils en une opération. Avec Jamf Pro, les administrateurs peuvent appliquer des actions groupées à n'importe quel groupe intelligent ou statique, aux résultats d'une recherche d'appareils ou à des listes d'utilisation de licences. Les actions groupées peuvent être de toute nature. Quelques exemples : commandes à distance, modification d'un panneau latéral ou envoi d'e-mails aux utilisateurs.

Pour votre environnement, c'est un gage de sécurité. Qu'il s'agisse de gérer cinq appareils ou 5 000, les actions groupées éliminent pratiquement tous les risques qu'un appareil soit laissé de côté et devienne une faille de sécurité.

Solutions de sécurité Jamf pour iOS et iPadOS

Une chose est claire : une gestion vigilante des appareils iPadOS et iOS est indispensable pour une bonne sécurité. Mais il est important de rappeler qu'elle n'est qu'une base. Le puzzle de la sécurité a besoin d'une dernière pièce : des outils de sécurité spécifiques. À ce sujet, nous vous recommandons de lire Une introduction à la protection contre les menaces sur mobile.

Défense et protection contre les menaces mobiles

Les solutions de sécurité Jamf pour la défense contre les menaces et la protection des terminaux vont plus loin que les antivirus de base. La solution complète de défense contre les menaces mobiles utilise un moteur sophistiqué de machine learning et de renseignement sur les menaces, MI:RIAM, pour identifier et prévenir les nouvelles menaces. Elle protège les appareils au sein du réseau, recueille des informations en temps réel et préserve âprement la confidentialité des utilisateurs.

Vous découvrirez également d'autres systèmes de sécurité stratégiques : la gestion des identités et des accès, la prévention et la correction des menaces, le filtrage de contenu et l'accès réseau Zero-Trust (ZTNA). Tous ont pour but d'assurer la sécurité des utilisateurs, des appareils et des données de l'entreprise.

Quels sont les avantages de Jamf

Jamf Pro et Jamf School

Pour une base solide et sécurisée, essayez Jamf Pro – la référence en matière de gestion des appareils Apple – ou Jamf School, la MDM des écoles et des groupements scolaires. N'hésitez pas à nous contacter pour en savoir plus et demander une version d'essai, ou adressez-vous à votre revendeur habituel.

La sécurité au-delà de la gestion des appareils

Lisez notre rapport sur l'état de la sécurité Apple en entreprise, basé sur les témoignages de 1 500 professionnels de l'informatique et de la sécurité de l'information. Il aborde l'utilisation des appareils et les approches actuelles, les défis de sécurité et l'avenir de la protection des terminaux.

Trusted Access

Trusted Access est la solution de Jamf pour porter la sécurité au-delà de la gestion. Trusted Access propose un workflow qui réunit gestion des appareils, identité des utilisateurs et protection des terminaux. Il aide les organisations à créer une excellente expérience de travail en laquelle elles pourront avoir confiance et qui fera le bonheur des utilisateurs.

Seuls les utilisateurs de confiance, équipés d'appareils inscrits et sûrs, peuvent accéder aux données de l'entreprise. Associé à Jamf, Trusted Access augmente considérablement la sécurité du lieu de travail moderne tout en simplifiant la tâche de vos utilisateurs, où qu'ils soient.

Explorez les offres de sécurité de pointe de Jamf dédiées aux Mac, et découvrez comment nous pouvons vous accompagner dans la gestion et la protection de votre flotte Mac !

Sur Jamf.com/solutions, vous pourrez approfondir :

- **La gestion des identités et des accès**
- **La gestion des appareils**
- **La protection des terminaux**
- **La prévention et la correction des menaces**
- **Le filtrage du contenu et l'Internet sécurisé**
- **L'accès réseau Zero-Trust (ZTNA)**
- **La visibilité et la conformité de la sécurité**

Et si vous êtes prêt à confier à Jamf la gestion et la sécurité de vos Mac, **demandez une version d'essai gratuite dès aujourd'hui !**

Source :
1. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html