Guide avancé de la gestion des Mac

Le paysage de la sécurité

La cybersécurité continue de se renforcer.
Selon le récent rapport Global Digital Trust Insights 2023 de PwC, la cybersécurité s'est améliorée sur plusieurs plans depuis 2020. Cette étude a interrogé 3 522 cadres dirigeants issus d'un large éventail de secteurs et de régions du monde. D'après les réponses, 70 % d'entre eux ont initié des améliorations en matière de 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. Elles sont 48 % à affirmer les avoir modérément atténués. Et 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.

Malheureusement, une faille suffit aux cybercriminels pour faire des ravages.
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 ?

Seules les

38 %

indiquent avoir pleinement atténué les cyber-risques émergents

Une bonne gestion des Mac est une gestion sécurisée

Ce guide de gestion de Mac fait suite à notre e-book Introduction à la gestion des Mac. Il détaille le rôle clé de la gestion des appareils macOS 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 de Mac 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 machines, les utilisateurs et les appareils. Très simplement, il confirme la sécurité de l'ordinateur et sécurise les informations passant d'un endroit à l'autre grâce au chiffrement.

Jamf Pro vous laisse le choix : autorité de certification (CA) intégrée, intégration d'une CA tierce de confiance (DigiCert, Venafi ou Active Directory Certificate Services) ou configuration de votre propre PKI. Pour cette dernière option, vous aurez besoin d'un accès à une CA externe prenant en charge le protocole SCEP (Simple Certificate Enrollment Protocol). La CA peut délivrer des certificats à la fois aux ordinateurs et aux appareils mobiles. Avec Jamf Pro, vous pouvez télécharger le certificat intégré de la (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.

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.

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.

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. Les certifications Push sont valables un an et doivent être renouvelées avec l'identifiant Apple utilisé lors de leur création.

Comment obtenir les certificats

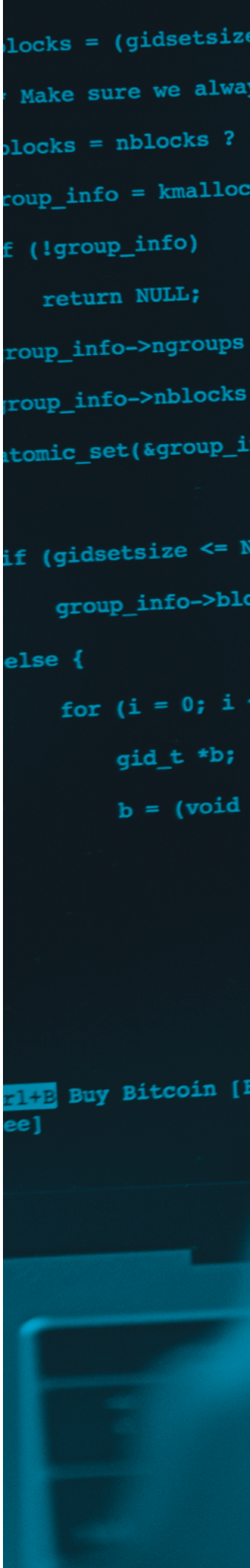
Vous pouvez afficher une liste de certificats en les exportant dans un fichier .csv, .txt ou XML. Jamf Pro facilite ce processus : il accompagne l'administrateur informatique dans la création d'un certificat push (.pem) et son importation dans Jamf Pro. Vous aurez besoin d'un identifiant Jamf et d'un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

Accès conditionnel

Aujourd'hui, la nouvelle norme est celle du télétravail – à la maison, dans un café ou même à bord d'un avion. Dans ce contexte, les entreprises ne peuvent plus protéger les appareils et les utilisateurs derrière le pare-feu de leur réseau.

L'accès conditionnel 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 Mac 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 macOS à Intune. Intune évalue la conformité et génère un rapport. Azure AD applique les contrôles d'accès.

Vous voulez en savoir plus sur la création d'une règle de conformité complète pour Mac ? 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.

TeamViewer : accès administratif à distance pour Mac

TeamViewer est une solution rapide et sécurisée pour accéder à distance aux ordinateurs et aux réseaux. Il établit une connexion de partage d'écran à distance entre un administrateur Jamf Pro et l'ordinateur d'un utilisateur final.

Cet outil est un atout de poids pour la sécurité et la conformité : les administrateurs peuvent visualiser, évaluer et résoudre rapidement les problèmes sans qu'aucune information ne se perde dans le processus. Et les problèmes sont résolus bien plus rapidement. Quand ces problèmes ont un impact sur la sécurité, la vitesse est un facteur déterminant.

Vous devrez ajouter une configuration d'intégration TeamViewer à votre instance Jamf Pro pour bénéficier de cette fonctionnalité.

API Jamf

L'API Jamf vise à rendre Jamf plus accessible. Elle permet d'intégrer Jamf Pro à la pile technologique de l'entreprise pour créer un système cohérent où la gestion des Mac est intégrée. Cela fluidifie également la connectivité entre Jamf et les autres fournisseurs. C'est encore l'API qui rend possible Jamf Protect/Jamf Connect, les applications Jamf School Parent et Jamf Teacher, etc.

L'API Jamf applique un schéma d'authentification par jeton. Cette pratique renforce la posture de sécurité des appareils en interface avec des applications et des intégrations tierces. Il s'agit d'une interface RESTful : elle respecte des normes de communication logicielle sécurisées.

Workflow

1. En utilisant l'authentification de base, demandez un jeton de porteur en envoyant un POST à `/v1/auth/token.`

2. Vous devriez recevoir une réponse comprenant un jeton et une date d'expiration, comme dans l'exemple suivant :

```
{
    "token": "eyJhbGciOiJIUzUxMiJ9...",
    "expires": "2022-01-24T21:35:20.373Z"
}
```

3. Le jeton précédemment généré peut servir à émettre des appels vers un autre point de terminaison de l'API Jamf Pro. Pour ce faire, incluez-le dans un en-tête utilisant le format Authorization: `Bearer TOKEN VALUE.`

Les intégrations permettent d'avoir une vision plus globale des capacités de Jamf. Elles assurent une connexion étanche avec Jamf Protect, qui combine des capacités de protection des terminaux à une prévention des menaces réseau pour Mac. Elles constituent un puissant allié pour les administrateurs chargés de prévenir les logiciels malveillants pour macOS, de protéger les Mac contre des événements spécifiques, de surveiller les terminaux et de corriger rapidement les problèmes.

Webhooks

Avec les webhooks, un administrateur Mac peut s'abonner à un événement spécifique sur une instance Jamf Pro. Lorsque l'événement en question se produit, une charge utile HTTP POST est envoyée à l'URL spécifiée. Les administrateurs peuvent ainsi utiliser les événements en temps réel de Jamf Pro pour créer des workflows personnalisés à l'aide du langage de programmation de leur choix.

Les webhooks renforcent la cybersécurité en informant les administrateurs en temps réel des événements qui surviennent dans leurs instances. Ces flux peuvent être envoyés en XML ou JSON. Ils facilitent encore la création de charges utiles génériques – ComputerAdded (nouvel ordinateur enrôlé), ComputerCheckin (vérification des tâches) ou ComputerPatchPolicyCompleted (lorsqu'une règle de correction est terminée), par exemple.

Points de distribution

Les points de distribution sont des serveurs qui hébergent des fichiers destinés à être distribués aux ordinateurs (et aux appareils mobiles). Paquets, scripts, applications et livres internes peuvent être distribués à l'aide d'un point de distribution.

Jamf Pro prend en charge les points de distribution de partage de fichiers et un point de distribution cloud. Jamf contacte les points de distribution locaux pour trouver des applications et les déployer sur des appareils ou des utilisateurs via le partage de fichiers. Les administrateurs peuvent recourir au point de distribution Jamf hébergé dans le cloud : Jamf Cloud Distribution Service (JCDS).

Les points de distribution peuvent être le maillon faible de la sécurité organisationnelle : ils se trouvent le plus souvent dans le Cloud, et les utilisateurs sont dispersés dans le monde entier. La distribution des fichiers aux Mac doit impérativement se faire via un point de distribution parfaitement sécurisé.

Comment les points de distribution fonctionnent-ils avec Jamf ?

Par défaut, le premier point de distribution que vous ajoutez à Jamf Pro est le point de distribution principal. Tous les autres points de distribution dépendent du premier, qui reste la source d'autorité pour tous les fichiers pendant la réplication. Les points de distribution veillent à ce que les fichiers soient envoyés au bon appareil ou utilisateur, de la bonne manière.

Scripts, profils de configuration et chiffrement des disques : 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 Mac.

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.

Les profils de configuration sont des fichiers XML (.mobileconfig). Ils permettent de définir facilement les réglages et les restrictions à appliquer à des appareils et des utilisateurs. Ils utilisent généralement APNs. Lorsqu'ils créent un profil de configuration d'ordinateur, les administrateurs doivent aussi impérativement spécifier à quel niveau ce profil doit être appliqué : celui de la machine ou de l'utilisateur. À chaque niveau correspond un ensemble unique de charges utiles, dont certaines sont toutefois communes aux deux niveaux.

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 Jamf Pro. Ils peuvent être déployés sur les appareils et les utilisateurs gérés par la MDM. Il existe deux façons de distribuer un profil de configuration : l'installer automatiquement (sans intervention de l'utilisateur) ou le rendre disponible en Self Service.

Chiffrement du disque

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 en les protégeant par un mot de passe. Il chiffre le code et les scripts, qui deviennent quasiment illisibles. Et c'est intégré au Mac.

Le chiffrement des disques permet également aux administrateurs de Mac de gérer et d'activer FileVault sur les ordinateurs. FileVault encode les informations sur les Mac, empêchant quiconque de les lire sans code secret.

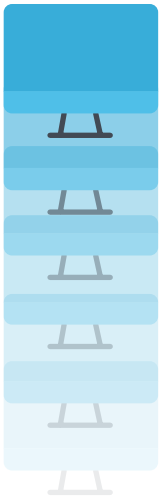
Attributs d’extension

Les attributs d'extension sont des champs personnalisés qui permettent de collecter presque tous les types de données d'inventaire des appareils. Vous pouvez utiliser des attributs LDAP personnalisés pour créer des attributs d'extension. Et si vous le souhaitez, vous pouvez obtenir des attributs d'extension plus sophistiqués grâce aux scripts.

Comment les utiliser
Une fois que les données des attributs d'extension se trouvent dans l'inventaire, les administrateurs peuvent créer, dans Jamf Pro, des groupes intelligents d'utilisateurs et/ou d'appareils en fonction d'un ou plusieurs attributs. Les administrateurs informatiques peuvent naturellement créer eux-mêmes des attributs d'extension selon leurs besoins. Mais ils peuvent aussi s'appuyer sur les modèles fournis par Jamf Pro, qui simplifient et accélèrent le processus de création.

L'utilisation combinée des attributs d'extension et des groupes intelligents de Jamf Pro est un puissant outil pour la sécurité de votre flotte : vous pouvez par exemple appliquer une action spécifiques aux appareils dont l'OS doit être mis à jour. Avec les attributs d'extension, vous aurez également une vision plus cohérente des données dans votre instance. Les problèmes de conformité et les points faibles du système vous apparaîtront ainsi plus clairement.

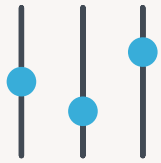
Actions groupées



Les actions groupées offrent un autre moyen d'effectuer plusieurs tâches fastidieuses sur de nombreux ordinateurs 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'ordinateurs 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 ordinateurs ou 5 000, les actions groupées éliminent pratiquement tous les risques qu'un appareil soit laissé de côté et devienne une faille de sécurité.

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 Mac. 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.

Aujourd'hui, les applications les plus utilisées ne se trouvent pas dans le Mac App Store, loin s'en faut. App Installers offre aux administrateurs Mac un moyen pratique et performant d'obtenir, héberger, mettre à jour et distribuer automatiquement des applications aux ordinateurs ou aux utilisateurs. Les applications obsolètes représentent un problème de sécurité majeur.

Pour y remédier, Jamf propose des outils pour faciliter les mises à jour :

App Installers
App Installers est une collection de paquets d'installation gérés et fournis par Jamf. Alternative rationalisée aux workflows de mise à jour des applications tierces, App Installers simplifie le déploiement

Côté sécurité, App Installers valide également l'intégrité des définitions des correctifs avant d'autoriser leur déploiement. Une fois vérifiée, la nouvelle version de l'app est déployée automatiquement sur tous les Mac compatibles.

Jamf obtient les paquets, les repackage et les héberge. Ce catalogue d'applications Jamf comprend une liste de plus de 1 000 logiciels macOS tiers pris en charge dans Jamf Pro.

App Installers doit faire partie d'un groupe intelligent dans Jamf Pro. Dans un groupe intelligent, si un ordinateur cible est équipé d'un logiciel, App Installers déploiera automatiquement la mise à jour à la parution d'une nouvelle version.

Workflows 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 Installers, qui peut s'exécuter en arrière-plan, automatise ce processus.

Title Editor
Title Editor est un service hébergé par Jamf qui étend les capacités de gestion des correctifs de Jamf Pro pour les appareils macOS. Cet outil permet de personnaliser les titres de logiciels, de remplacer les définitions de correctifs existantes et de créer des définitions de correctifs personnalisées.

Solutions de sécurité Jamf pour Mac

Une chose est claire : une gestion vigilante des appareils Mac 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. Pour une vue d'ensemble, lisez Introduction à la protection des terminaux Mac.

Protection des terminaux avec Jamf Protect

Jamf Protect n'est pas un simple outil antivirus. C'est une solution complète de sécurité des terminaux. Ses fonctions de détection basée sur le comportement anticipent et reconnaissent les comportements souvent utilisés dans les attaques.

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

Pour une base solide et sécurisée, essayez Jamf Pro – la référence en matière de gestion des appareils Apple. 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 sécurité 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**
- **Le filtrage du contenu et l'Internet sécurisé**
- **La protection des terminaux**
- **L'accès réseau Zero-Trust (ZTNA)**
- **La prévention et la correction des menaces**
- **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