jamf

LIVRE BLANC

Combler le fossé : la sécurité sur macOS

Confidentialité et sécurité sont natives sous Mac, mais aucun système d'exploitation n'est parfait.

Tous les systèmes d'exploitation ont besoin d'être sécurisés, et macOS ne déroge pas à la règle. Apple a beaucoup investi pour offrir des fonctions natives de confidentialité et de sécurité. Malheureusement, les attaques visant la plateforme Mac prennent de la valeur avec sa présence grandissante dans l'entreprise : elle devient une cible convoitée pour les logiciels malveillants, les intrusions et la recherche de vulnérabilités. En effet, de plus en plus d'entreprises laissent à leurs employés le choix de leur appareil de travail, et Apple a souvent leur faveur. Une chose est rapidement devenue claire : comme toute autre plateforme, Mac a besoin d'une sécurité et d'une visibilité supplémentaires.

Plusieurs fournisseurs de sécurité offrent des solutions de protection pour Mac. Mais dans bien des cas, elles reposent sur un modèle de sécurité spécifique fermé et sur les produits Windows du fournisseur, sans exploiter les cadres modernes que propose macOS. Avec un système d'exploitation en constante évolution, il devient difficile de rester à jour. La bonne pratique consiste plutôt à étendre le modèle de sécurité macOS existant, à combler les lacunes et à ajouter des outils spécifiques à macOS. Les équipes de sécurité seraient alors armées pour protéger efficacement leur organisation contre les menaces.

Et si les systèmes d'exploitation Apple protègent à la fois l'utilisateur et sa vie privée, la facilité d'utilisation et la productivité ont toujours été des priorités absolues. L'expérience Apple est fortement axée sur l'utilisateur plutôt que sur l'entreprise dans laquelle il opère. Il en va de même pour de nombreuses fonctionnalités de sécurité et de confidentialité sur MacOS.

Notre livre blanc offre un aperçu de l'état actuel de la sécurité sur MacOS. Nous y donnons ensuite des conseils pour améliorer la base de sécurité Apple de manière efficace, utile et conviviale.

Vous découvrirez :

- Des informations sur les fonctionnalités de sécurité macOS intégrées
- Comment Jamf améliore ces fonctionnalités dans l'entreprise
- Comment Jamf étend la détection des menaces au-delà des signatures et des fonctionnalités intégrées
- D'autres possibilités d'extension du modèle de sécurité Apple pour renforcer la sécurité des entreprises

Applications sur macOS

Apple a consacré beaucoup d'efforts à la conception de fonctionnalités de sécurité, afin de protéger l'utilisateur et les applications tierces qu'il utilise. Dans cette section, nous allons présenter plusieurs de ces fonctionnalités et voir comment les améliorer et les étendre de manière stratégique. Pour de plus amples informations sur les fonctionnalités de sécurité Apple, consultez le guide de sécurité sur la plateforme complète sur **support.apple.com/guide/security**.

Établissez la confiance avec Gatekeeper.

L'App Store est la méthode privilégiée et la plus fiable d'Apple pour installer des applications tierces. Il permet en effet à Apple de les examiner et de filtrer celles qui ne répondent pas à leurs normes en matière de respect de la vie privée, de sécurité ou d'expérience utilisateur. Mais dans cette démarche, Apple limite les capacités des applications de l'App Store, et de nombreuses applications stratégiques d'entreprise ne sont pas adaptées à ce type de distribution.

Quand l'App Store n'est pas une option, Apple permet aux développeurs MacOS de distribuer leurs applications directement via des téléchargements hébergés et des méthodes de distribution classiques. Pour faciliter ces distributions « ad hoc » sans faciliter la propagation de logiciels, Apple a introduit d'autres contrôles dans le système d'exploitation macOS. Gatekeeper est le nom de la fonctionnalité qui se trouve au centre des contrôles d'Apple. Au départ, c'était une option pour autoriser l'exécution de programmes fonction de leur tolérance au risque. Aujourd'hui, c'est un vaste ensemble d'exigences strictes et de mesures d'atténuation des risques. Les niveaux d'acceptation de base existent toujours : ils autorisent le téléchargement d'applications sur l'App Store ou l'« App Store et développeurs identifiés ». Mais il reste très difficile d'exécuter du code problématique ou risqué.

Notez, d'ailleurs, que ces contrôles ne s'appliquent qu'aux applications téléchargées sur Internet. Apple ajoute des métadonnées appelées « attribut de quarantaine » au fichier téléchargé à des fins de suivi. Lorsqu'un programme est exécuté, Gatekeeper effectue une série de contrôles et vérifie notamment l'attribut de quarantaine pour déterminer s'il peut s'exécuter. Parmi les vérifications élémentaires, Gatekeeper détermine si l'application est signée par un développeur légitime ou si elle a été distribuée par l'App Store, en fonction du paramètre mentionné précédemment.

Si l'application est signée par un développeur, le dispositif recherche le certificat dans une base de données de signatures révoquées et s'assure que le signataire n'a jamais été associé à des logiciels malveillants. Au besoin, Apple peut rapidement révoquer un certificat et mettre fin à la diffusion généralisée d'une application suspecte. Depuis macOS Catalina, il faut également que l'application soit notariée par Apple pour passer la vérification de Gatekeeper. Pour ce faire, son éditeur doit l'envoyer à Apple pour analyse. Si l'analyse réussit, des données notariées sont associées à l'application et signalent qu'elle a passé ce niveau d'inspection supplémentaire.

La confiance ultime est donnée par l'utilisateur.

Dans un souci de simplicité d'utilisation, macOS permet à l'utilisateur final d'ignorer la décision de Gatekeeper dans de nombreuses situations. Il lui suffit de faire un clic droit sur l'application et de sélectionner « ouvrir » ou « ouvrir avec ». Au lieu de refuser catégoriquement de lancer l'application, un message avertit simplement l'utilisateur qu'il lance une application inconnue ou potentiellement malveillante, mais Gatekeeper ne lui interdit pas de le faire. Observons toutefois qu'un utilisateur ne peut pas autoriser l'exécution de logiciels malveillants définitivement identifiés comme tels par XProtect.

Après la première exécution de l'application, le composant de quarantaine est mis à jour pour éviter à Gatekeeper de reproduire la procédure la fois suivante.

Bloquez les menaces avec XProtect et MRT.

La suite de technologies Gatekeeper comprend également XProtect et Malware Removal Tool (MRT), les mécanismes de détection d'Apple basés sur les signatures. Ils analysent les fichiers sur le système d'exploitation à la recherche de caractéristiques typiques des logiciels malveillants connus. XProtect se déclenche au lancement d'une application et MRT analyse le système de fichiers à intervalles réguliers.

XProtect s'appuie sur moteur de lecture de signatures binaires appelé Yara. Yara prend en charge des définitions de signatures binaires souples et puissantes et exploite un moteur d'exécution efficace. Afin de vérifier une application, XProtect analyse chaque téléchargement de fichier exécutable lors de son exécution initiale puis à chaque mise à jour. S'il détecte une signature connue, le programme n'est pas autorisé à s'exécuter. Le fichier de signatures indésirables connues est fourni par Apple sous forme de mises à jour indépendantes de macOS. Apple définit et fournit ces signatures à sa discrétion, indépendamment du moteur d'exécution de Yara lui-même. Comme dans le cas de Gatekeeper, l'analyse n'a lieu que lorsqu'une application possède l'attribut étendu de quarantaine approprié, lequel est mis à jour après la première exécution réussie de l'application.

MRT, quant à lui, s'exécute à intervalles définis plutôt qu'au moment de l'exécution du programme. Il analyse le système de fichiers à la recherche de noms de fichiers spécifiques et d'artefacts associés à des logiciels malveillants antérieurs. Ceux qu'il détecte sont supprimés. Cette fonctionnalité est largement destinée à détecter et corriger les menaces connues qui peuvent déjà avoir infecté les machines macOS.

Étendez Gatekeeper à toute l'entreprise.

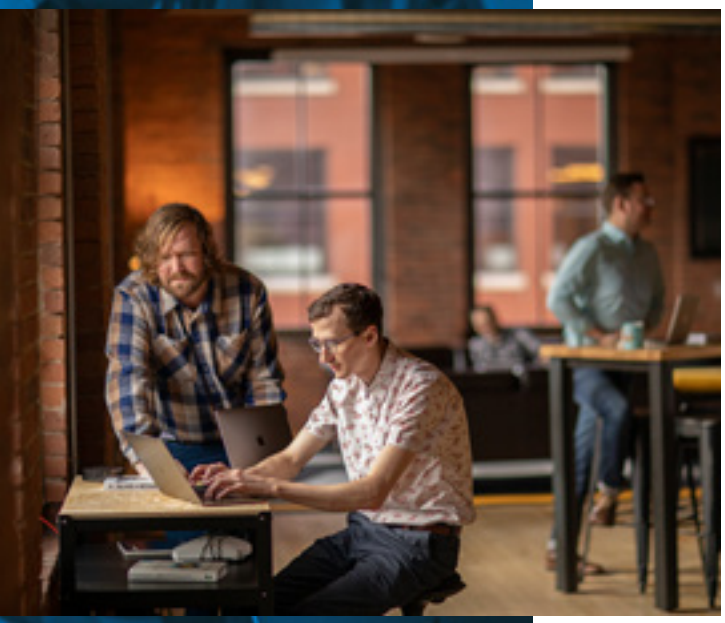
Gatekeeper fonctionne efficacement comme prévu. Il bloque le lancement des applications non fiables et avertit l'utilisateur lorsqu'il reconnaît une application suspecte ou malveillante. Les administrateurs informatiques et de la sécurité doivent avoir une visibilité sur les tentatives d'exécution de logiciels non fiables sur un équipement de l'entreprise. Plus important encore, ils doivent être informés si un utilisateur décide de lancer une application au moyen du clic droit pour contourner les contrôles de sécurité de l'entreprise. Jamf Protect, une solution de sécurité des terminaux spécialement conçue pour Mac, répond à ces besoins. Elle surveille les indicateurs d'action de Gatekeeper et communique les résultats à un emplacement central. Ces informations permettent ensuite au service informatique et aux équipes de sécurité d'évaluer les risques avec précision et de prendre des décisions en connaissance de cause.

En plus d'apporter de la visibilité sur les activités de Gatekeeper, Jamf Protect permet également aux entreprises de s'approprier le modèle de confiance du développeur. Elles peuvent en effet enregistrer des informations de signature supplémentaires comme non fiables dans l'environnement de l'entreprise. Jamf Protect utilise la dernière version de l'API de sécurité des terminaux d'Apple et bloque dès le départ l'exécution de toute application figurant sur la liste rouge de l'entreprise. Cette liste peut cibler des applications spécifiques (grâce à l'identifiant de l'application) mais aussi des fournisseurs (grâce à l'identifiant de l'équipe de développement).

Il faut également savoir que macOS ne fournit pas de signatures ni de filtres pour une variété de « grayware », ces logiciels potentiellement indésirables ou non sanctionnés. Parmi ceux-ci figurent de nombreux logiciels publicitaires et applications de minage de cryptomonnaies, au comportement indésirable et potentiellement invasif. Ces programmes sont souvent signés en toute légitimité par un développeur Apple. Au moment de l'installation, l'utilisateur accepte que ses informations soient collectées ou que ses ressources

soient utilisées, généralement à son insu. Pour ces raisons, dans de nombreux cas, Apple n'intervient pas dans le fonctionnement de ces applications.

Mais l'entreprise calcule le risque selon d'autres critères et requiert bien souvent une approche plus stricte et ciblée. Jamf Protect possède donc son propre ensemble de règles Yara gérées, de signatures binaires et de certificats de développeurs non fiables. Ces mécanismes sont utilisés pour analyser les processus lors de leur exécution, indépendamment de l'attribut étendu de quarantaine. Grâce à cela, lorsque de nouvelles signatures sont ajoutées et que l'entreprise met à jour sa position de sécurité, les applications existantes sont à nouveau inspectées à leur lancement suivant.



Pour produire ce flux de données sur les menaces et les logiciels malveillants connus ciblant les Mac, Jamf s'appuie ses recherches approfondies ainsi que sur des données tierces. Certaines entreprises souhaitent exercer un contrôle encore plus fin sur les logiciels exécutés dans leur environnement. À cette fin, elles peuvent ajouter à la liste des applications bloquées par Jamf Protect leur propre liste de hashs binaires, TeamIDs, etc. Lorsqu'une application correspondant au comportement ou à la signature d'un logiciel malveillant connu s'exécute sur macOS 10.15 (Catalina) ou version ultérieure, Jamf Protect empêche son exécution, met en quarantaine le fichier incriminé et signale le blocage. Pensée comme un complément de haut niveau à la fonctionnalité de Gatekeeper/XProtect, cette opération se déroule en dehors de leur champ d'action. Jamf Protect identifie les logiciels malveillants connus sans tenir compte du composant de quarantaine pour détecter également les binaires potentiellement dangereux. La solution conserve à cet effet un ensemble beaucoup plus large de connaissances sur les menaces.

Étendez le modèle de confiance de l'App Store avec le Self Service.

Dans certaines situations, il peut être utile d'encadrer les programmes accessibles à vos utilisateurs en regroupant, dans une boutique d'applications en libre-service, des ressources informatiques approuvées.

Pour faciliter un accès sécurisé et instantané aux ressources, Jamf Self Service permet au service informatique de créer son propre catalogue d'applications d'entreprise. Les utilisateurs peuvent ainsi installer des applications, mettre à jour les configurations et résoudre les problèmes courants par eux-mêmes, sans faire appel à l'assistance.

Contrôlez et surveillez le comportement des applications.

Limitez et identifiez le comportement des applications grâce aux contrôles de confidentialité.

Les contrôles de confidentialité intégrés ont été introduits dans macOS Mojave. Ces contrôles exigent des utilisateurs (ou des entreprises) qu'ils autorisent l'accès de chaque application à des actions et à des dossiers spécifiques. Une fois l'autorisation accordée, l'application pourra effectuer les opérations en question sans consulter l'utilisateur. Les applications doivent donc être explicitement autorisées à accéder aux parties potentiellement sensibles du système d'exploitation (webcam, micro, saisies, téléchargements). Cette fonction amène les utilisateurs à prendre conscience qu'ils autorisent les applications à accéder à des données privées.

Allez au-delà des contrôles pour auditer et analyser les comportements des applications

Certes, les contrôles de confidentialité limitent ce que les applications sont autorisées à faire. Mais les utilisateurs font toujours des erreurs et certaines autorisations peuvent être employées de manière abusive. Nous avons vu que Jamf Protect offre une visibilité sur les actions des fonctionnalités de sécurité intégrées d'Apple et sur les capacités classiques de prévention des logiciels malveillants et publicitaires. L'objectif : informer et protéger les entreprises. Mais chez Jamf, nous pensons qu'une solution de protection des points terminaux ne doit pas s'arrêter là. Jamf Protect offre également des fonctions d'audit et de surveillance traditionnellement réservées aux produits EDR (Endpoint Detection and Response). Elles adoptent une approche « Apple first » et tiennent compte des normes de confidentialité et de sécurité attendues par les utilisateurs de MacOS.

L'ingénierie de détection de Jamf Protect

Au cœur de l'agent Jamf Protect se trouve un capteur léger en mode utilisateur (sans kext d'accompagnement). Celui-ci exploite l'un des moteurs d'exécution logique propres à Apple, le GameplayKit. Il est assez inhabituel d'utiliser un moteur de jeu pour analyser les événements de sécurité. Pourtant, cela permet à Jamf de rester étroitement intégré à l'écosystème Apple et d'analyser les données sur l'appareil jusqu'à ce qu'il soit nécessaire de les collecter ou de les signaler. Autre avantage, les moteurs de jeu sont conçus pour gérer un grand nombre d'événements en temps réel : un outil parfait pour analyser les activités qui se déroulent sur l'appareil. Par comparaison, pensez aux nombreuses solutions de sécurité qui ont été développées pour la plateforme Windows avant d'être adaptées tant bien que mal pour MacOS, ou encore à celles qui doivent collecter les données pour les analyser dans le cloud.

GameplayKit présente un autre intérêt : comme Yara, il sépare le moteur d'exécution des définitions de détection, qui peuvent donc être mises à jour et enrichies sans qu'il faille mettre à jour l'agent principal. En outre, les définitions de détection sont également spécifiques à Apple. Elles s'appuient sur NSPredicate, un puissant langage logique qui prend en charge une syntaxe de requête classique ainsi que les expressions régulières. Le modèle de données de Jamf Protect a été spécifiquement conçu pour tirer parti des riches fonctionnalités de NSPredicate, notamment sa capacité à appeler des fonctions natives et à enchaîner des modèles de données. Cette approche ouvre des possibilités d'action qui seraient bien plus lourdes à mettre en œuvre par d'autres moyens plus conventionnels. Le modèle de données de Jamf Protect et NSPredicate permet par exemple de :

- Déclencher une alerte si un fichier se supprime lui-même, une technique courante pour couvrir ses traces. Ce cas d'utilisation apparemment simple implique d'analyser à la fois le fichier supprimé et le processus de suppression, sans opération de jointure coûteuse ni détection codée en dur.
- Envoyer une alerte en cas de persistance, sous forme de démon de lancement, d'un binaire non signé ou présentant une signature suspecte. Pour cela, il faut analyser un fichier de configuration, extraire chemin binaire intégré du contenu et exploiter les métadonnées de ce fichier binaire.
- Envoyer une alerte si une application Microsoft Office a créé un fichier enfant inattendu, afin d'identifier l'exploitation des macros Office. Cet exemple met en évidence la capacité à comprendre les relations enfants/parents et découvrir les cas d'abus de fonctionnalités des applications.

- Envoyer une alerte si d'autres activités « parasites » peuvent être symptomatiques d'attaques. Cette classe d'activité nécessite l'accès aux relations enfants/parents, à celles des groupes de processus et aux paramètres de la ligne de commande, entre autres. Le but est de découvrir les cas d'abus d'opérations par ailleurs anodines (curl, ssh, python, etc.).
- Suivre l'utilisation de l'USB dans l'entreprise et signaler les métadonnées des fichiers écrits sur des supports amovibles.

Pour mieux comprendre l'impact de ces types de détections, Jamf Protect analyse les attaques identifiées selon la structure MITRE ATT&CK™, le cas échéant. Actuellement, la solution couvre des cas d'utilisation de l'ensemble de la structure et détecte les techniques des catégories suivantes :

- Persistance
- Accès initial
- Commande et contrôle
- Contournement de défense
- Découverte
- Acquisition de privilèges
- Accès aux certificats

Simplification de la collecte et de l'interprétation du journal unifié

La plupart des analystes de sécurité et des administrateurs informatiques s'appuient fortement sur les journaux des terminaux pour réaliser des audits de conformité ou combler les lacunes d'autres contrôles de sécurité. Lorsque macOS a abandonné les fichiers syslog pour la journalisation unifiée, il est devenu plus difficile de collecter, d'inventorier et d'inspecter ces informations à l'échelle de l'entreprise. L'application macOS Console.app offre une excellente visibilité sur l'infrastructure de journal unifié sur un Mac local. Malheureusement, elle ne permet pas à une organisation de centraliser facilement ces données.

Avec Jamf Protect, les journaux des clients peuvent être transmis en continu vers un système d'enregistrement dès leur inscription dans le journal unifié. Pour collecter uniquement les données ciblées, les administrateurs de Jamf Protect utilisent le même langage de filtrage de prédicats (NSPredicate) que celui de l'utilitaire en ligne de commande intégré, « log stream ». De cette façon, l'élaboration d'un système d'enregistrement des données de journal Mac se résume à une simple configuration, sans collecte fastidieuse machine par machine. Prenons l'exemple des connexions et déconnexions, de ssh, d'AirDrop et des événements d'autorisations. Si des données sont enregistrées dans le journal unifié, Jamf Protect peut les collecter.

S'aligner sur les normes Apple

Prise en charge le jour de sortie

Pour interagir avec macOS et recueillir les données nécessaires aux décisions de sécurité, Jamf Protect s'appuie sur les technologies natives d'Apple. Ces technologies comprennent des cadres émergents comme l'API de sécurité des terminaux d'Apple et le cadre d'audit OpenBSM sur les versions antérieures. En utilisant ces mécanismes, Jamf Protect minimise son impact sur les appareils. Surtout, la solution s'adapte sans problème aux modifications apportées par les correctifs ou les nouvelles versions majeures de macOS. L'application rapide et fréquente des correctifs reste le premier protocole de sécurité. Certains outils de sécurité respectent strictement le principe de prise en charge des nouvelles versions le jour de leur sortie. Ce principe est indispensable à ce protocole et constituent un élément crucial d'une stratégie de sécurité globale de défense en profondeur.

L'expérience utilisateur en tant que fonctionnalité Jamf Protect surveille en permanence l'activité des applications et des utilisateurs pour détecter les menaces potentielles. Mais sa mission n'est pas de rechercher délibérément les logiciels malveillants dormants ou liés à Microsoft Windows. En effet, lorsqu'il faut analyser des fichiers résidant sur le système de fichiers à la recherche d'une longue liste de signatures de logiciels malveillants, l'expérience utilisateur en souffre considérablement. L'approche de Jamf s'aligne sur celle de Gatekeeper/XProtect : les menaces sont identifiées au moment de leur exécution potentielle afin de préserver l'expérience de l'utilisateur et sa productivité.

Confidentialité

Jamf Protect analyse les données sur l'appareil et ne collecte d'informations pertinentes que lorsqu'il est configuré pour le faire – généralement en cas de détection d'une activité potentiellement malveillante ou présentant un grand intérêt. Cela limite la quantité de données utilisateur extraites de l'appareil et stockées dans le cloud : les besoins des entreprises et la vie privée des utilisateurs sont une fois de plus équitablement protégés. Lorsqu'une activité malveillante est détectée, ses caractéristiques et les données associées sont transmises à la console en cloud Jamf Protect ou au SIEM (systèmes de gestion des informations et des événements de sécurité) qui a été configuré. Toute autre donnée spécifiquement demandée est également transmise à Jamf Protect ou au SIEM. Toutes les données inutiles sont filtrées : l'analyste de sécurité chargé de surveiller et d'enquêter sur les incidents reçoit uniquement une compilation de haute qualité des données d'intérêt.

Autres extensions du modèle de sécurité Apple

Bonnes pratiques : renforcement de macOS

Apple fournit des systèmes d'exploitation comptant parmi les plus sûrs et les plus fiables du marché. Mais dans un environnement d'entreprise, il est normal de se vouloir mettre en œuvre des mesures supplémentaires pour optimiser macOS.

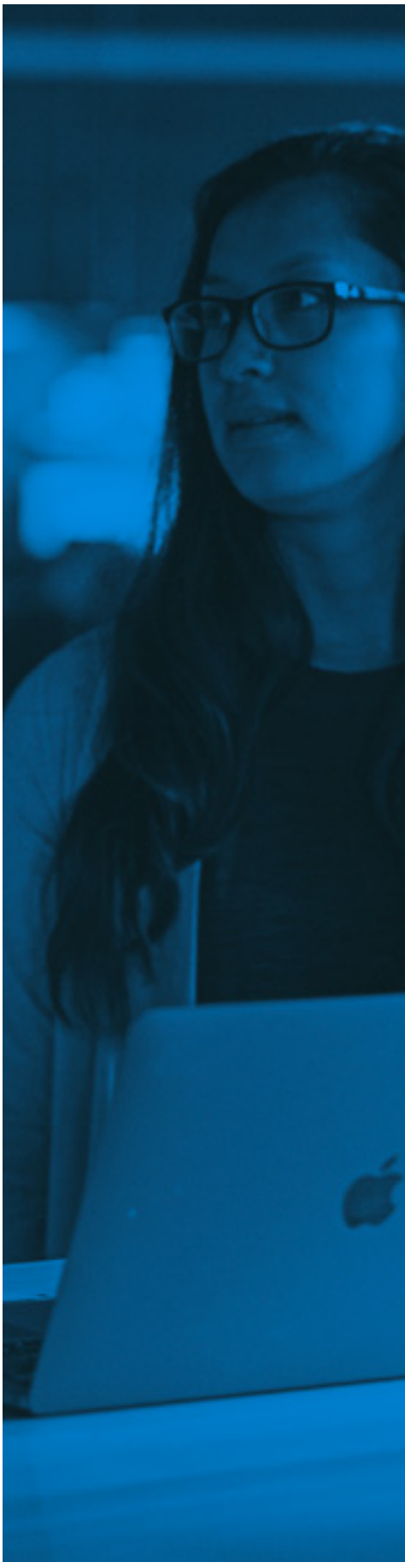
En premier lieu, le mieux est de s'appuyer sur le cadre de gestion des appareils mobiles (MDM) d'Apple pour automatiser la gestion à grande échelle. Non seulement la MDM vous aidera à mieux protéger votre organisation, mais elle vous soulagera d'une grande partie de l'effort de gestion et de sécurisation de votre parc informatique.

Introduite avec OS X 10.7 (« Lion »), le cadre MDM propose une myriade de workflows pour adapter les fonctionnalités de l'appareil aux besoins spécifiques de l'entreprise. Les profils de configuration et les commandes de gestion, notamment, sont couramment employés pour assurer la sécurité des équipes, où qu'elles opèrent.
Améliorez la sécurité grâce à la MDM en l'associant à la puissance d'Apple Business Manager : cette solution gratuite d'Apple pour les entreprises permet, entre autres, d'automatiser l'achat et la gestion du matériel.

Démarrez avec Apple...

Au fil des ans, Apple s'est forgé une réputation d'entreprise axée sur la sécurité et macOS est un fidèle reflet de cette vision. Chaque nouveau Mac ajouté à l'environnement d'une organisation bénéficie de fonctionnalités natives : chiffrement FileVault 2, authentification à deux facteurs, fonction de verrouillage/effacement à distance et possibilité d'appliquer des normes de code d'accès.

Les plateformes de gestion modernes, comme Jamf Pro, s'appuient sur la MDM pour repousser les limites de ces fonctionnalités. Elles permettent de personnaliser la mise en œuvre et l'encadrement de pratiques de sécurité telles que le chiffrement, et délivrent de précieux rapports.



...optimisez avec Jamf.

La MDM est une pierre angulaire de choix pour tout type d'entreprise. Mais les équipes se demandent souvent comment renforcer encore leur posture de sécurité et la protection de la vie privée de leurs employés. Et c'est là que Jamf entre en jeu.

Ce n'est pas un secret : à une certaine échelle, la gestion des appareils épuise les ressources de l'équipe. L'augmentation des effectifs entraîne la multiplication des équipements, et donc l'intensification des activités informatiques.

Du moins, c'était le cas avant les plateformes de gestion de flotte telles que Jamf Pro.

Des technologies brevetées, comme les groupes intelligents, aident à organiser les appareils de l'entreprise et à exécuter automatiquement des fonctions de gestion. Les équipes informatiques gagnent du temps dans la gestion des appareils et peuvent le consacrer à d'autres tâches informatiques. Les groupes intelligents surveillent les inventaires d'appareils pour ajouter et retirer des équipements d'un groupe prédéfini en temps réel lorsque leur statut change.

Gestion des identités moderne sur macOS

L'approche moderne de la sécurité repose sur l'identité : un accès sécurisé et personnalisé pour les utilisateurs finaux. Les méthodes traditionnelles s'appuient sur les services de répertoires locaux, sortes de registres centralisant des informations sur les employés (nom, service, etc.). Avec l'évolution des besoins en matière de sécurité et de déploiement évoluent, les entreprises doivent intégrer à leur stratégie une nouvelle approche de la gestion des identités et des accès. En s'appuyant sur une pile complète de gestion des identités basée sur le cloud, les entreprises unifient toutes les identités – matérielles et logicielles. Cette unification débloque des fonctionnalités et des workflows avancés qui ont un véritable pouvoir de transformation sur l'entreprise.

L'authentification unique (SSO) basée sur le cloud exploite les informations des services de répertoire et impose la saisie d'identifiants sécurisés pour autoriser l'accès aux ressources de l'entreprise.

Jamf Connect élargit ces formes courantes de gestion des identités.

Jamf Connect unifie les identités sur l'ensemble des applications de l'entreprise et sur le Mac de l'utilisateur à l'aide de workflows d'authentification transparents. Grâce à leur identité cloud unique, les utilisateurs finaux accèdent facilement et rapidement aux ressources dont ils ont besoin pour être productifs.
Jamf Connect offre de nombreux outils stratégiques aux entreprises :

- Rationalisation de l'approvisionnement et de l'authentification pour une prise en charge complète des employés sur site et à distance
- Synchronisation automatique des identités des utilisateurs et des identifiants des appareils
- Capacités complètes de gestion des identités pour l'ensemble des services et des appareils
- Une solution d'accès réseau zero-trust (ZTNA) pour remplacer les VPN (réseaux privés virtuels) traditionnels et répondre aux besoins des grandes entreprises modernes et hybrides.

Traiter et corriger les menaces sur Mac

Les tableaux de bord de Jamf Pro offrent aux entreprises une visibilité sur l'état de leurs appareils Mac et mettent en évidence le matériel qui nécessite une attention particulière. Grâce à la fonctionnalité brevetée de groupe intelligent, les administrateurs informatiques ciblent les appareils à mettre à jour ou à corriger pour renforcer leur posture de sécurité. Tout cela se fait à distance et peut être automatisé : le service informatique n'a jamais besoin d'intervenir physiquement sur l'appareil.

En associant Jamf Protect à Jamf Pro, le traitement des menaces est encore plus efficace. Grâce à la technologie de groupe intelligent, les commandes de MDM et de Jamf Pro peuvent être orchestrées pour répondre à une alerte d'activité émise par Jamf Protect. L'éventail des interventions est large : isolement automatisé du réseau, évocation de l'accès conditionnel, notifications aux utilisateurs ou toute autre forme ciblée de correction et de réponses. Avec Jamf Pro et Jamf Connect, les attaques contre un utilisateur ou un appareil peuvent entraîner la suspension des autorisations, la modification des accès et toute une série de mesures correctives axées sur l'identité.

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

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.

En utilisant Jamf Protect avec Jamf Pro et en s'appuyant sur Jamf Connect, les administrateurs veillent à ce que seuls les employés de confiance accèdent aux applications d'entreprise, à l'aide d'appareils fiables et conformes. Si un appareil est infecté, il peut être rapidement corrigé et remis en service avec Jamf Pro.

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.

Gérez et sécurisez Apple pour des avantages sans précédent.

Avec les bons outils, les équipes informatiques et de sécurité peuvent déployer en toute confiance une initiative Mac complète et ont les moyens de vérifier et authentifier les identités et les accès. Quant aux utilisateurs, ils ont accès aux ressources dont ils ont besoin, sans aucun compromis sur les critères de sécurité et de confidentialité.

Profitez dès aujourd'hui des solutions d'entreprise Jamf et bénéficiez de la visibilité et des outils de remédiation dont votre organisation moderne a besoin.

Lancez-vous

Vous pouvez également contacter votre revendeur pour essayer Jamf gratuitement.

jamf

www.jamf.com/fr/