Introduction à la sécurité des appareils Apple

POUR DÉBUTANTES

jamf

Il suffit d'une cyberattaque bien orchestrée ou d'un logiciel malveillant téléchargé par accident pour mettre un coup d'arrêt brutal à votre productivité. Les pirates ne cessent de se perfectionner, et les entreprises doivent se concentrer sur la sécurité pour protéger les données de leurs clients, de leurs employés ou de leurs étudiants.

Les problèmes de sécurité d'Apple, comme tous les problèmes de sécurité informatique, sont bien réels et constituent une menace importante pour les ressources de l'organisation et la sécurité des parties prenantes.

Apple fabrique des systèmes d'exploitation incroyablement sûrs ; il ne fait aucun doute que les mesures de sécurité et de confidentialité intégrées à son matériel et à ses logiciels ont joué un rôle important dans sa popularité et son adoption massive dans les entreprises, les établissements d'enseignement et d'autres organisations du secteur. Et comme Apple reste la plateforme de choix pour le matériel personnel comme professionnel, elle est devenue une cible plus intéressante pour les attaquants. Les administrateurs doivent donc réagir rapidement aux incidents de sécurité dès qu'ils surviennent, sans attendre qu'ils ne dégénèrent en problèmes graves. Les administrateurs Mac et les équipes de sécurité (ainsi que les acteurs qu'ils soutiennent) ont même tout intérêt à opter pour la prévention. Comment ? En s'appuyant sur des solutions spécialement pensées pour Apple afin de se protéger efficacement contre les menaces qui visent spécifiquement cette marque.

Ce guide s'adresse aux administrateurs et aux gestionnaires qui veulent aborder sérieusement la question de la sécurité de leurs appareils Apple d'entreprise. Il offre aux nouveaux venus des informations de base mais les vétérans de la gestion Apple y trouveront certainement quelques rappels utiles.

Introduction à la sécurité Apple

Plusieurs facteurs concourent à la sécurité du matériel et des données de votre organisation :

1. **Sécurité native Apple :** exploiter les systèmes de sécurité déjà intégrés à macOS, iOS, iPadOS et tvOS.
2. **Appareils enrôlés :** inscrire et déployer des appareils avec une gestion et une visibilité sécurisées et centralisées.
3. **Sécurité des appareils :** protéger vos appareils physiques et mettre vos utilisateurs à l'abri des menaces
4. **Chiffrement des données :** sécuriser les données au repos et en transit, sur l'appareil comme sur le réseau, en permanence.
5. **Contrôle de la conformité :** surveiller les appareils pour déterminer leur état de santé et leur appliquer des standards de référence.
6. **Sécurité des applications et correctifs :** appliquer en temps voulu les correctifs des systèmes d'exploitation, des applications et des logiciels.

1

PREMIER BLOC :

la sécurité native Apple

Les appareils Apple sont les machines prêtes à l'emploi les plus sûres du marché, et les solutions de gestion et de sécurité spécialisées étendent leurs capacités.

Les fonctionnalités de sécurité déjà intégrées à macOS (le système d'exploitation pour Mac), iOS (l'OS de l'iPad et de l'iPhone) et tvOS (l'OS de l'Apple TV) sont nombreuses et s'accompagnent de plusieurs avantages :

- **Les systèmes d'exploitation Apple reposent sur UNIX, une base informatique riche issue d'une plateforme mature et bien étudiée, avec des racines de développement profondes pour une stabilité à toute épreuve.**
- **Un cadre de sécurité solide pour les OS :**
  - Notarisation
  - Gatekeeper
  - XProtect
  - Malware Removal Tool (MRT)
  - Transparence, consentement et contrôle (TCC)
  - Rapid Security Responses
  - Mode de verrouillage
- **Sécurité assurée par le verrouillage et le suivi des appareils perdus avec le service Find My.**
- **Possibilité de mettre en œuvre et de configurer des contrôles de sécurité à l'aide des options de configuration transmises par la gestion des appareils mobiles (MDM)**
  - Les appareils Apple intègrent des modes d'inscription sécurisés, comme l'inscription automatisée des appareils et l'inscription à l'initiative de l'utilisateur, pour les appareils de l'entreprise comme ceux des employés. L'écosystème est ainsi compatible avec tous les modèles de propriété (BYOD, CYOD et COPE) et fonctionne sans URL d'inscription ni invitation par e-mail, toujours sources de risque.
  - L'intégration transparente avec Apple Business Manager ou Apple School Manager facilite la gestion centralisée de l'ensemble du matériel de l'organisation. Elle permet notamment de superviser les appareils à distance et d'utiliser la MDM pour effectuer en toute sécurité des opérations de gestion – déploiement d'applications, approvisionnement sécurisé des appareils et workflows sans contact.

Une solution MDM spécialisée peut aligner ces configurations de sécurité existantes sur les besoins de votre organisation et les critères de l'industrie, puis les déployer et les appliquer à l'ensemble de votre flotte Apple, quelle que soit sa taille. Il n'est pas plus difficile de préparer un Mac que d'en préparer mille, et toutes les opérations sont efficaces et sécurisées. En facilitant l'exécution des tâches administratives sur des groupes d'appareils sélectionnés, la MDM vous offre également davantage de contrôles de sécurité. Vous pouvez aussi réduire les tâches répétitives, par exemple en verrouillant et en effaçant à distance les appareils perdus ou à retirer de l'inventaire de votre site. Pour en savoir plus, consultez notre e-book Introduction à la gestion de appareils Apple.

Les fonctionnalités de sécurité en détail

Fonctionnalités de sécurité natives de macOS, iOS, iPadOS et tvOS

macOS	iOS et iPadOS	tvOS
Mises à jour de logiciels	Mises à jour de logiciels	Mises à jour de logiciels
Protection de l'intégrité du système (SIP)	Système sécurisé	App Store
Gatekeeper	App Store	Réglages et mots de passe AirPlay
App Store	Identification biométrique	Restrictions d'application
Chiffrement FileVault	Chiffrement matériel	Économiseur d'écran
Supervision	Supervision	Supervision
XProtect et Malware Removal Tool (MRT)	Essai des applications en sandbox	
Find My	Find My	
Réglages de confidentialité	Réglages de confidentialité	
Notarisation et mise en quarantaine des dossiers	Secure Enclave et identification biométrique	
API de sécurité des terminaux	Notarisation	
Essai des applications en sandbox		
Secure Enclave et identification biométrique		

2

DEUXIÈME BLOC :

inscrire et déployer les appareils en toute sécurité

La clé du succès repose sur des fondations solides. De ces fondations découle la viabilité de l'édifice et les principes généraux qui régissent la gestion et la sécurité du cycle de vie du matériel et des applications.

Pour approvisionner les appareils et déployer votre flotte de manière sécurisée, rationnelle et efficace, la meilleure option est l'inscription automatique des appareils, qui fait partie des services gratuits proposés par Apple via Apple Business Manager et Apple School Manager.

Quand vous utilisez cette méthode, vous informez Apple de tous les appareils que votre organisation possède ou utilise via d'autres modèles de propriété (que nous verrons plus bas), et vous les affectez à la solution MDM de votre organisation pour les gérer. Ensuite, lorsqu'un appareil inscrit dans ce programme s'allume :

- Il s'inscrit automatiquement dans votre solution MDM
- Il active la supervision, essentielle pour autoriser des contrôles de sécurité plus stricts
- Il autorise les administrateurs à appliquer des profils de configuration et à durcir les réglages
- Le système s'assure que les réglages de sécurité et les charges utiles stratégiques sont déployés avant que l'utilisateur ne puisse commencer à utiliser l'appareil.
- La gestion et le déploiement des mises à jour de l'OS et des correctifs de sécurité sont normalisés
- Les workflows d'approvisionnement des appareils sont considérablement allégés grâce à la centralisation de l'achat, de la configuration et du déploiement des applications, ce qui garantit également qu'elles proviennent de sources vérifiées et fiables.
- Les utilisateurs sont autonomisés : ils peuvent réaliser certaines tâches de maintenance sur leurs appareils sans l'aide de l'informatique.
- La gestion peut se faire à distance quel que soit l'appareil, sa localisation et le réseau auquel il est connecté

Modèles de propriété des appareils

Automatiser la gestion et la sécurité de votre flotte d'appareils devient absolument essentiel quand le nombre d'appareils augmente et que les équipes se décentralisent. L'adoption croissante de la plateforme Apple et des appareils mobiles dans l'espace de travail, tous secteurs confondus, a considérablement diversifié les usages et les profils d'utilisateur.

Certaines organisations ont adopté les produits Apple par le biais de programmes de choix des employés, qui leur qui attribuent un appareil d'entreprise macOS, iOS ou iPadOS. D'autres ont ouvert la porte à Apple en autorisant les employés à utiliser leurs appareils personnels pour accéder aux ressources de l'entreprise. En leur offrant la possibilité de travailler plus confortablement en utilisant le matériel et les logiciels qu'ils connaissent le mieux, les organisations autonomisent leurs employés. Autre avantage de poids, elles réduisent leurs dépenses en matériel, en particulier lorsque les utilisateurs disposent déjà d'un équipement fonctionnel qu'ils maîtrisent et apprécient.

La question n'est donc plus « Comment fournir des appareils aux utilisateurs ? » mais « Comment sécuriser les ressources de l'entreprise ? »

C'est là qu'intervient la MDM de votre organisation qui, en prenant en charge différents modèles de propriété flexibles, permet plusieurs approches :

Usage professionnel des appareils personnels (BYOD)

Il s'agit sans doute du modèle le plus courant. Il autorise les utilisateurs à utiliser leur appareil personnel pour accéder aux ressources de l'entreprise. Les utilisateurs sont invités à inscrire manuellement leurs appareils dans la MDM de l'entreprise avant d'accéder aux ressources professionnelles, ce qui a un double avantage. D'une part, les employés sont assurés d'obtenir les outils nécessaires pour accéder aux données et aux services utiles à leur travail. D'autre part, l'entreprise sait que les appareils sont équipés des logiciels et des paramètres de sécurité nécessaires pour protéger les données professionnelles en cours d'utilisation, au repos et en transit.

Choisissez votre appareil (CYOD)

Dans cette variante du BYOD, l'organisation détient les appareils utilisés dans le cadre du travail – ou de l'apprentissage s'il s'agit d'un établissement scolaire. Avec un programme de choix des employés, les utilisateurs peuvent choisir l'appareil Apple qui répond le mieux à leurs besoins. Chaque appareil est inscrit, assigné à un utilisateur et géré par la MDM de l'organisation. Les applications, les profils de configuration, les réglages des appareils et les logiciels de sécurité sont appliqués conformément aux normes de sécurité de l'organisation et en tenant compte des besoins professionnels de l'utilisateur.

Détenu par l'entreprise, activé par l'utilisateur (COPE)

Le modèle COPE est une tendance croissante dans les grandes organisations, en particulier celles qui pleinement adopté le télétravail ou les pratiques hybrides. Quand elles choisissent cette approche, les organisations achètent et possèdent l'équipement, puis l'inscrivent et le gèrent entièrement dans la solution MDM. Comme dans le cas du CYOD, les outils professionnels sont installés et gérés en fonction de l'appareil et de la posture de sécurité de l'entreprise. Mais comme dans le BYOD, l'organisation autorise et encourage même les utilisateurs à faire également un usage personnel de leur appareil. Les données de l'entreprise restent au sein d'applications gérées, protégées par des profils de configuration. Cette approche peut poser la question de l'accès de l'entreprise aux données personnelles et privées présentes sur l'appareil. Il est donc essentiel de prendre ce facteur en compte en équilibrant gestion et confidentialité par le biais de règles d'utilisation acceptables (PUA) et de gestion des données.

Des méthodes d'inscription flexibles

Pour simplifier la gestion de plusieurs modèles de propriété au sein d'un même environnement MDM, Apple a mis au point deux méthodes d'inscription différentes. Utilisables conjointement, elles permettent de gérer et renforcer la sécurité de l'organisation sans compromettre la vie privée de l'utilisateur.

Inscription automatisée des appareils

C'est la méthode la plus courante, privilégiée par la plupart des organisations qui possèdent l'équipement utilisé par les employés. Elle garantit la validité de chaque étape de la chaîne d'inscription, de l'approvisionnement auprès d'Apple (ou d'un tiers agréé) à la phase d'inscription lorsque l'appareil est mis sous tension, en passant par la configuration préalable dans la MDM. Chaque étape fait l'objet d'une procédure automatisée pour une gestion continue, des usines d'Apple à l'administrateur. La supervision est automatiquement activée sur les appareils inscrits : l'organisation dispose alors d'une base fiable qui donne au service informatique un contrôle total sur l'appareil tout au long de son cycle de vie. La supervision est la racine de la confiance, et elle est indispensable pour effectuer certaines tâches de gestion sur les appareils gérés.

Inscription par l'utilisateur

Plus récente, cette méthode d'inscription est plus adaptée aux appareils qui appartiennent à des particuliers dans le cadre d'un modèle BYOD. Cette fois, l'inscription repose sur l'utilisateur ou le propriétaire de l'appareil, qui doit inscrire manuellement son appareil via l'application Réglages et s'authentifier à l'aide de ses identifiants d'entreprise. Une fois le processus d'inscription terminé, la MDM de l'organisation assure une communication bidirectionnelle sécurisée entre elle et l'appareil de l'utilisateur.

Une fois inscrits, ces appareils personnels peuvent être gérés par la MDM. Les administrateurs sont autorisés à installer des applications gérées, à déployer des profils de configuration et à modifier certains paramètres. L'organisation peut ainsi définir des exigences propres aux appareils mais aussi appliquer des opérations de gestion ou des critères à l'utilisateur lui-même plutôt qu'à l'appareil. Apple a prévu des limitations pour permettre aux organisations de sécuriser l'accès à leurs données, leur interaction avec les apps, leur stockage sur l'appareil et leur transmission sur les réseaux, sans pour autant affecter les applications et les données personnelles de l'utilisateur. Les organisations peuvent personnaliser la visibilité des appareils gérés en associant un identifiant Apple personnel aux données personnelles et un identifiant Apple géré à celles de l'entreprise.

3

TROISIÈME BLOC :

sécuriser les appareils

Protéger les appareils, les données et les utilisateurs contre les menaces

« Les pirates informatiques n'ont besoin de réussir qu'une seule fois ; nous devons réussir à chaque fois. »

– Chris Triolo, HP

Si l'on se penche sur les violations de données les plus vastes, les plus complexes et même les plus meurtrières de l'histoire récente, on peut voir émerger un fil rouge. L'attaque Stuxnet, par exemple, a désactivé le programme d'enrichissement nucléaire de l'Iran en infectant l'ordinateur portable d'un entrepreneur qui mettait à jour l'équipement SCADA. LinkedIn a été la cible d'un développeur qui a exploité son API pour récupérer les informations personnelles de 700 millions d'utilisateurs avant de les vendre en ligne. Aadhaar est une gigantesque base de données qui abrite les identifiants, les informations personnelles et les données financières de plus de 1,1 milliard de citoyens indiens. Son contenu a été dérobé et vendu par des acteurs malveillants qui sont parvenus à accéder à la base de données en passant par un site non protégé. Dans ces cas comme dans bien d'autres, les attaques ont été rendues possibles par la compromission d'un seul appareil.

C'est en effet le moyen le plus courant de contourner le cadre de sécurité d'une organisation pour accéder à des données sensibles – et mettre ainsi en péril la sécurité de l'utilisateur final. Quel que soit le secteur d'activité de votre organisation, qu'elle fournisse des données et des ressources à des travailleurs intellectuels, des étudiants, des enseignants, des soignants, des employés à distance, des vendeurs ou des grands voyageurs, ses appareils peuvent se trouver n'importe où dans le monde et se connecter via des réseaux non sécurisés. Et cette dispersion augmente de manière exponentielle l'exposition aux risques des équipements et du réseau de l'entreprise.

Appareils perdus ou volés

La perte ou le vol d'un iPhone, d'un iPad ou d'un Mac n'est pas seulement une perte financière : c'est aussi un risque de sécurité considérable dont les retombées potentielles peuvent être difficiles à estimer. Les quelques exemples suivants nous rappellent à quel point il est essentiel de réduire les risques liés à la perte et au vol d'appareils.

SCÉNARIOS DU MONDE RÉEL

Un employé en télétravail prépare des documents juridiques pour une affaire civile en cours. Il s'est installé dans un café près de chez lui pour travailler. Le temps d'aller chercher un deuxième café, il laisse son Mac d'entreprise sans surveillance. À ce moment précis, un voleur s'approche et dérobe l'ordinateur portable. L'appareil n'est pas verrouillé : l'attaquant a un accès illimité aux informations sensibles et potentiellement confidentielles de l'entreprise. Les conséquences pourraient être très lourdes pour les affaires judiciaires en cours et la réputation de l'entreprise.

Un deuxième exemple : un élève utilise son iPhone personnel pour accéder à des ressources scolaires via le portail éducatif de son école. Il égare son appareil entre deux cours. Un autre élève trouve le téléphone et accède aux comptes de l'étudiant et à des informations sensibles – son adresse, son numéro de téléphone ou son numéro d'élève. Un utilisateur non autorisé peut utiliser ces informations pour usurper l'identité de la victime pour en tirer des avantages ou commettre des délits. Il pourrait aussi infecter l'appareil avec des logiciels malveillants avant de le rendre à son utilisateur légitime, afin de l'espionner et de le surveiller à distance.

Soyons clairs : on ne peut pas éviter les pertes et les vols. Tout le monde peut être victime d'un accident ou d'un moment d'inattention. Il est donc essentiel d'anticiper la situation et de planifier en conséquence, en mettant en place les stratégies d'atténuation appropriées afin de minimiser les risques avant qu'un appareil ne soit perdu ou volé.

Pour assurer pleinement la sécurité des utilisateurs et des données, pensez également que certains appareils doivent être protégés contre l'utilisation abusive, la découverte accidentelle des données d'une autre personne ou la consultation de contenus risqués ou inappropriés. C'est notamment le cas des appareils destinés aux étudiants et aux patients, et ceux qui sont utilisés par plusieurs utilisateurs.

En fonction des besoins spécifiques de votre organisation, l'application de réglages sécurisé et de configurations conformes aux exigences de l'organisation peut être une entreprise considérable. Surtout quand le nombre d'appareils augmente.

Lorsque vous appliquez manuellement des restrictions et des réglages de sécurité sur les appareils, vous devez :

Gestion

- Activer l'utilisation d'un mot de passe sur tous les appareils
- Activer l'option Find My Mac dans les Préférences système > iCloud.
- Dépendre de la capacité de chaque utilisateur à se connecter à iCloud ou mémoriser son mot de passe (condition préalable à l'activation de FindMy).
- En cas de perte ou de vol d'un appareil, signaler l'incident à Apple et activer l'effacement
- Effectuer le suivi de l'inventaire du parc à l'aide des numéros de série ou des étiquettes d'actifs
- Activer le contrôle parental sur les appareils pour bloquer les contenus inappropriés et les sites web malveillants (sur le navigateur Safari)
- Assurer la maintenance des Mac en appliquant toutes les mises à jour du système et des applications pour minimiser les vulnérabilités
- Configurer et durcir les réglages des appareils afin de minimiser les erreurs de configuration qui pourraient laisser des données exposées.
- Déployer les applications prises en charge et les tenir à jour.
- Installer et configurer une solution de sécurité des terminaux afin de surveiller les appareils, d'identifier les menaces et d'y remédier.

iPhone et iPad

- Activer l'utilisation d'un mot de passe sur tous les appareils
- Activer l'option Find My Mac dans les Préférences système > iCloud.
- Dépendre de la capacité de chaque utilisateur à se connecter à iCloud ou mémoriser son mot de passe
- Effectuer le suivi de l'inventaire de la flotte à l'aide des numéros de série ou des étiquettes d'actifs
- En cas de perte ou de vol d'un appareil, signaler l'incident à Apple et activer l'effacement
- Créer un compte unique et activer le contrôle parental sur chaque appareil.
- Assurer la maintenance des appareils iOS en appliquant toutes les mises à jour du système et des applications pour minimiser les vulnérabilités
- Configurer et durcir les réglages des appareils afin de minimiser les erreurs de configuration qui pourraient laisser des données exposées.
- Déployer les applications gérées et les tenir à jour.
- Installer une solution de sécurité des terminaux afin de surveiller les appareils, d'identifier les menaces et d'y remédier.

Apple TV

- Exiger des mots de passe sur toutes les Apple TV
- Configurer des restrictions :
  - Dans le menu principal, allez dans Réglages > Général > Restrictions
  - Sélectionnez Restrictions pour l'activer
  - Si on vous le demande, composez un code à quatre chiffres
  - Saisissez à nouveau les quatre chiffres pour confirmer, puis sélectionner OK
  - Mémorisez le code d'accès
  - Répétez l'opération pour toutes les Apple TV

Pour limiter AirPlay sur les Apple TV :

- Dans le menu principal, allez dans Réglages > AirPlay
- Activez ou désactivez AirPlay

Choisissez parmi :

- Tous
- Toute personne se trouvant sur le même réseau
- Répétez l'opération pour toutes les Apple TV

Et maintenant, voyons comment on réalise ces tâches de gestion et de sécurisation avec une solution MDM de pointe comme Jamf Pro :

Mac, iPhone, iPad et Apple TV

- Définissez toutes les limitations et fonctionnalités de sécurité dès la première utilisation, ou les activer automatiquement grâce à la supervision et aux règles et profils de configuration
- Verrouillez ou effacez à distance tout appareil perdu ou mal utilisé, quelle que soit sa localisation physique, et qu'il dispose ou non d'un compte iCloud signé (aucun identifiant Apple requis).
- Permettez à plusieurs utilisateurs de partager des appareils en toute sécurité en les réinitialisant entre deux utilisations, et en associant les autorisations et les réglages à l'utilisateur plutôt qu'à l'appareil
- Assignez des identifiants Apple gérés aux appareils pour les tâches professionnelles tout en autorisant l'utilisateur à accéder à ses propres applications, données et réglages stockés dans iCloud avec son identifiant Apple personnel.
- Tenez l'inventaire de tous les appareils en ayant la possibilité de les regrouper par catégorie – et pas seulement par numéro de série ou étiquette d'actif – afin de recueillir de nombreuses données utiles : utilisateurs affectés, version du système d'exploitation, applications installées, etc.
- Réalisez des tâches de gestion en envoyant des commandes à un appareil spécifique ou à un groupe, par exemple pour déployer des mises à jour de sécurité, passer à une nouvelle version de l'OS ou effacer les codes secrets oubliés sur les appareils verrouillés.
- Mettez en place un contrôle parental et bloquez l'accès aux applications inappropriées ou à risque, en appliquant des restrictions granulaires de façon globale ou selon des critères définis.
- Déployez des applications gérées pour permettre aux utilisateurs de rester productifs à la maison, au bureau, à l'école ou ailleurs. Approuvez des applications et mettez-les à disposition des utilisateurs dans le catalogue Self Service pour les autonomiser.
- Intégrez des solutions de sécurité des terminaux à votre MDM pour que vos appareils soient constamment surveillés et protégés contre les menaces de sécurité. En partageant des données de télémétrie riches avec la MDM, vous pourrez mettre en place des règles de gestion et automatiser la réponse aux incidents.
- Centralisez tous les aspects des tâches de gestion des appareils pour protéger les utilisateurs et les données contre les cybermenaces sans compromettre le respect de la vie privée.

Cette approche n'a pas seulement l'avantage de rationaliser le travail des administrateurs et du personnel informatiques, elle facilite également la tâche des utilisateurs finaux. Elle préserve l'expérience Apple qu'ils apprécient tout en respectant les exigences de l'entreprise, les obligations de sécurité et de conformité industrielle et la confidentialité des utilisateurs.

4

QUATRIÈME BLOC :

chiffrement des données

Données au repos et en transit : spécificités et approches de sécurité.

Les écoles doivent protéger les informations relatives aux élèves, les établissements de santé abritent les antécédents médicaux des patients et les entreprises sont soucieuses de protéger leur propriété intellectuelle. Dans toutes ces situations, le chiffrement n'est plus une option : c'est une bonne pratique impérative pour toute organisation qui souhaite conserver des données sensibles, confidentielles, stratégiques ou protégées pour une raison ou une autre.

À tout moment, les données d'un appareil peuvent se trouver dans trois états :

Données au repos :
les données sont stockées localement (généralement) sur un appareil qui n'est pas en cours d'utilisation.

Données en transit :
les données sont transférées (reçues ou transmises) sur un canal de communication comme un réseau câblé ou sans fil.

Données en cours d'utilisation :
ni conservées dans la mémoire permanente, ni transmises sur les réseaux, ces données sont utilisées par des applications ou d'autres processus.

Chaque état présente des risques inhérents. Par conséquent, une solution adaptée à un état risque de ne pas offrir une couverture adaptée à un autre, voire ne pas fonctionner du tout. Certes, c'est un facteur de complexité supplémentaire pour votre stratégie de sécurité. Mais ne vous inquiétez pas : les solutions efficaces reposent toutes sur la fonction fondamentale du chiffrement.

SCÉNARIOS DU MONDE RÉEL

Un nouvel employé du service des RH de votre organisation reçoit son nouveau Mac et s'empresse d'effectuer le processus de configuration pour commencer à travailler. Parmi ses nouvelles tâches, il doit créer une arborescence des contacts d'urgence **à l'aide d'un tableur**. Doivent y figurer le nom de chaque employé, sa fonction, l'adresse e-mail de l'entreprise, son adresse personnelle et le numéro de son contact d'urgence, en précisant s'il s'agit d'un contact principal ou secondaire. Ces informations contiennent notamment les coordonnées personnelles des membres des équipes de gestion et de direction. Elles doivent être **sauvegardées localement** sur l'ordinateur et un double doit être mis à la disposition des personnes autorisées qui y **accèderont en toute sécurité sur un référentiel cloud**.

Dans le scénario ci-dessus, les parties en gras indiquent un exemple spécifique de chaque état des données. Premièrement, quand les données sont manipulées « à l'aide d'un tableur », elles sont « en cours d'utilisation » et doivent être sécurisées pendant leur séjour dans l'application. Il faut donc contrôler et vérifier l'intégrité du logiciel pour s'assurer qu'un acteur ou un logiciel malveillant n'a pas compromis sa sécurité interne. Deuxièmement, les données « sauvegardées localement » sont des données au repos. Dans ce contexte, il est essentiel d'activer le chiffrement pour empêcher leur consultation par des personnes non autorisées. Troisièmement, quand des personnes autorisées y « accèderont en toute sécurité sur un référentiel cloud », les données seront en transit – elles circuleront via une connexion réseau. Cette connexion doit être chiffrées de bout en bout pour que seules les deux extrémités puissent déchiffrer les messages. Les données seront ainsi protégées contre toute réception non autorisée ou écoute clandestine.

Ce troisième peut évoquer les services VPN traditionnels, mais toute la différence réside dans la formulation « personnes autorisées ». En effet, l'accès réseau zero-trust (ZTNA) n'assure pas seulement le chiffrement des données en mouvement : il s'intègre également à votre fournisseur d'identité (IdP) pour que seuls les utilisateurs et les appareils correctement authentifiés et autorisés reçoivent l'accès aux ressources demandées, abritées derrière de couches supplémentaires de protection, selon le principe de moindre privilège. De plus, contrairement aux services VPN traditionnels qui donnent souvent accès à l'ensemble du réseau une fois l'authentification effectuée, les connexions sécurisées du ZTNA établissent des micro-tunnels isolés vers chaque application ou service. La sécurité est renforcée à trois titres : par le principe du moindre privilège, par des contrôles d'état qui vérifient que les appareils répondent à des exigences minimales, et par l'authentification systématique de l'utilisateur à chaque demande d'accès.

Comment chiffrer les trois états des données

Données au repos

Chiffrement du volume ou de l'appareil au complet

Le chiffrement des données stockées sur un appareil mobile ou dans un volume de votre ordinateur est une bonne pratique à plusieurs titres. Combinaison de mesures proactives et réactives, l'activation du chiffrement, très simple, offre une sécurité et une sûreté maximales aux données stockées de manière permanente. Le chiffrement utilise des algorithmes si puissants qu'il faudrait des centaines, voire des milliers d'années de travail continu avec des machines de pointe pour en venir à bout. Quand on pense à l'effort relativement minime que requiert sa mise en place, il ne faut pas hésiter une seconde à inclure ce contrôle de sécurité à votre stratégie de défense en profondeur. C'est le dernier rempart entre un acteur malveillant et des données confidentielles.

Voyons comment le chiffrement intégral des appareils ou des volumes peut atténuer efficacement les risques liés à des incidents de sécurité :

Perte ou vol d'un appareil

Le risque de perte est particulièrement élevé pour les appareils mobiles comme les iPhone, les iPad et les MacBook. Plus la mobilité est grande, plus la probabilité de perte ou de vol est grande. Une fois qu'un appareil n'est plus entre vos mains, des malfaiteurs ont toute latitude pour tenter d'obtenir les données qui y sont stockées.

Bien sûr, un code ou un mot de passe complexe devrait protéger votre appareil. Mais selon l'appareil, un acteur malveillant peut toujours avoir accès à tout ou partie des données qu'il contient – sauf si elles sont chiffrées. Le simple fait d'activer le chiffrement brouille les données au point de les rendre illisibles à moins de détenir la clé de déchiffrement. Et ce, même si l'appareil est réinitialisé ou que son disque dur SSD est connecté à un autre appareil en tant que disque externe par un moyen ou un autre. Les données chiffrées restent chiffrées jusqu'à ce que la clé de déchiffrement ou de récupération soit utilisée pour les déchiffrer. Dans tous les autres cas, les données sont illisibles et, par conséquent, inutiles.

Accès physique

La perte et le vol d'un appareil ne sont pas les seuls scénarios permettant un accès physique non autorisé. Pensez aux appareils partagés sur le lieu de travail, à l'ordinateur installé à votre bureau ou à tout appareil informatique laissé sans surveillance. Quand vous mettez fin à votre session, que vous éteignez votre machine ou que vous la verrouillez avant de vous en éloigner, les données qu'elle contient sont et restent chiffrées. Il faut une clé de déchiffrement ou de récupération pour décrypter et lire les données sécurisées.

Conformité réglementaire

Selon le secteur auquel appartient votre organisation, vous pouvez être soumis à des réglementations qui imposent des exigences minimales en matière de protection et de traitement des données, et encadrent les rôles autorisés à travailler avec des types de données protégées. Certains secteurs font l'objet de réglementations plus strictes que d'autres ; c'est notamment le cas du secteur financier et de la santé. D'autres se concentrent uniquement sur certains aspects de la sécurité des données, comme dans le secteur de l'éducation où les réglementations visent à protéger le bien-être des étudiants et leurs IPI.

Comme indiqué précédemment, les réglementations découlent de lois dont la violation peut avoir des conséquences désastreuses pour l'organisation ou l'institution. Et bien souvent, le chiffrement des données fait partie des contrôles de sécurité requis dans différents états de données, notamment au repos et en transit, afin de minimiser le risque d'interception, d'exfiltration ou d'exposition d'informations réglementées.

Chiffrement des données et appareils Apple

- Le système macOS dispose déjà d'une fonction intégrée de chiffrement des volumes avec FileVault. Il n'est pas nécessaire d'installer un logiciel supplémentaire pour chiffrer un dossier, un disque ou un volume sur un Mac.
- Les Mac plus récents, comme ceux équipés de la puce Apple Silicon, s'appuient sur la Secure Enclave. Ce composant matériel dédié gère la création et le stockage des clés de chiffrement et effectue les calculs algorithmiques.
- Les Mac basés sur la technologie Intel utilisent un composant matériel dédié similaire, appelé puce de sécurité T2, pour exécuter des fonctionnalités semblables à la Secure Enclave.
- FileVault est certifié FIPS 140-2. Cela signifie que le système de chiffrement d'Apple répond aux normes extrêmement strictes de l'administration fédérale américaine.
- FileVault s'active manuellement ou à distance : l'utilisateur peut sélectionner l'option sur son appareil, mais le service informatique peut également automatiser son application sur des centaines, voire des milliers d'appareils, avec une simple règle dans Jamf Pro.
- Les utilisateurs chiffrent et déchiffrent les volumes simplement en s'authentifiant auprès de macOS ou en saisissant leur code d'accès sur les appareils iOS et iPadOS. Sur les appareils compatibles, les technologies TouchID ou FaceID d'Apple permettent d'ajouter une couche de sécurité biométrique reposant sur l'empreinte digitale ou la reconnaissance faciale de l'utilisateur.

Pour activer manuellement FileVault sur macOS :

- Rendez-vous dans Paramètres système > Confidentialité et sécurité > FileVault
- Sélectionnez le bouton « Activer... » pour activer le chiffrement du volume.
- Répétez l'opération pour tous les appareils

Si vous devez activer FileVault sur tous les appareils de votre entreprise, utilisez votre solution MDM pour automatiser, déployer et appliquer le chiffrement. Vous pouvez déployer un profil de configuration ou une règle qui activera FileVault. Le service informatique peut obtenir les clés de récupération s'il faut déchiffrer le volume par la suite.

- Créez un profil de configuration tout simplement en sélectionnant des options au sein de Jamf Pro.
- Déployez-le sur une sélection d'appareil ou sur tous les appareils basés sur macOS.
- **Et non, il n'y a pas de troisième étape.**

Avec Jamf Pro, vous pouvez également configurer la redirection des clés de récupération, même si l'activation de FileVault est confiée aux utilisateurs. La clé sera sauvegardée dans la solution de gestion des appareils du service informatique, qui pourra la retrouver facilement en cas de besoin.

Qu'en est-il sur l'iPad et l'iPhone ?

Sur les appareils iOS et iPadOS, le chiffrement est encore plus simple. Les appareils iOS disposent d'un chiffrement intégré qui s'active dès que l'utilisateur définit son code secret. L'opération peut être réalisée de façon individuelle ou imposée par Jamf Pro, qui peut aussi définir des critères de force du code (longueur minimale, complexité, etc.).

Données en transit

Chiffrement des connexions réseau de bout en bout

Les bonnes pratiques conventionnelles dictaient l'utilisation d'un VPN pour protéger les données lors de leur circulation entre un appareil et un autre service. Cette méthode est vieille de plusieurs décennies maintenant. Elle a été développée à l'époque pour jeter un pont sécurisé entre deux réseaux disjoints en passant par un réseau non fiable, comme l'Internet.

Ce contrôle de sécurité est toujours utilisé par de nombreux particuliers et entreprises. Mais les changements survenus dans le paysage informatique au cours des dernières années, notamment l'adoption d'Apple en entreprise, la croissance explosive des appareils mobiles à usage personnel et professionnel et la généralisation du télétravail, ont révélé les limites de la technologie VPN. Celle-ci ne suffit plus à protéger efficacement les appareils, les utilisateurs et les données dans le contexte des menaces modernes.

Tous ces changements combinés ont révolutionné nos façons de travailler – et de nous divertir – sur les ordinateurs et les appareils mobiles. Dans ce contexte, pourquoi votre stratégie de sécurité devrait-elle reposer des processus obsolètes pour assurer la sécurité des données en transit ?

L'alternative tient en un mot : ZTNA, ou accès réseau zero-trust. Cette solution a été développée pour répondre à un besoin très concret : connecter une grande variété d'appareils et d'utilisateurs locaux et distants, alors que l'accès aux données via des réseaux non fiables et le recours à des services cloud étendent l'infrastructure et érodent le périmètre du réseau de l'organisation. Le tout dans un contexte de multiplication et de sophistication croissante des menaces de sécurité, qui sont de plus en plus nombreuses à cibler macOS et les appareils mobiles.

En clair : la sécurisation des connexions au réseau ne concerne plus seulement une poignée d'employés en déplacement ou quelques cas ponctuels de travail à distance.

Elle ne s'arrête pas non plus au chiffrement des communications entre deux points : elle exige des protections de sécurité granulaires afin de protéger les acteurs, d'empêcher les accès non autorisés aux ressources de l'entreprise et de minimiser l'introduction de menaces. Le ZTNA y parvient en combinant plusieurs moyens :

- Il s'intègre à l'IdP cloud pour élargir le champ d'application des comptes utilisateur gérés : les permissions définies de façon centralisée suivent l'utilisateur partout.
- Des contrôles fréquents s'assurent que les terminaux répondent aux exigences minimales : application des correctifs, intégrité des dispositifs de sécurité (pas d'appareil jailbreaké ou rooté), présence et configuration adéquate de la sécurité des terminaux.
- Si un contrôle révèle une anomalie ou qu'un appareil est considéré comme compromis, l'intégration du ZTNA à une solution MDM de pointe, comme Jamf Pro, permet de réaliser des opérations de gestion basées sur des règles. Les données de télémétrie sont transmises en toute sécurité pour suspendre l'accès de l'appareil et exécuter des workflows de correction qui vont rétablir la conformité du terminal, et vérifier que tout problème détecté a été résolu.
- Il renonce au principe de confiance implicite appliqué par les VPN traditionnels. Son mantra : « ne jamais faire confiance, vérifier systématiquement » à chaque fois que l'on demande l'accès à une ressource de l'entreprise. Ce n'est qu'après une vérification réussie que l'accès à la ressource demandée est accordé.

CHIFFREMENT DES DONNÉES

Étapes de protection des données en transit

Une connectivité réseau sécurisée à un serveur VPN

Pour connecter un VPN manuellement :

iOS et iPadOS

- Rendez-vous dans Paramètres système > VPN
- Sélectionnez « Ajouter une configuration VPN »
- Saisissez l'adresse du serveur VPN sur l'appareil
- Sélectionnez-le dans vos options réseau
- Répétez l'opération pour chaque appareil

macOS

- Rendez-vous dans Paramètres système > VPN et filtres
- Sélectionnez « Ajouter une configuration VPN »
- Saisissez l'adresse du serveur VPN sur l'appareil
- Sélectionnez-le dans vos options réseau
- Répétez l'opération pour chaque appareil

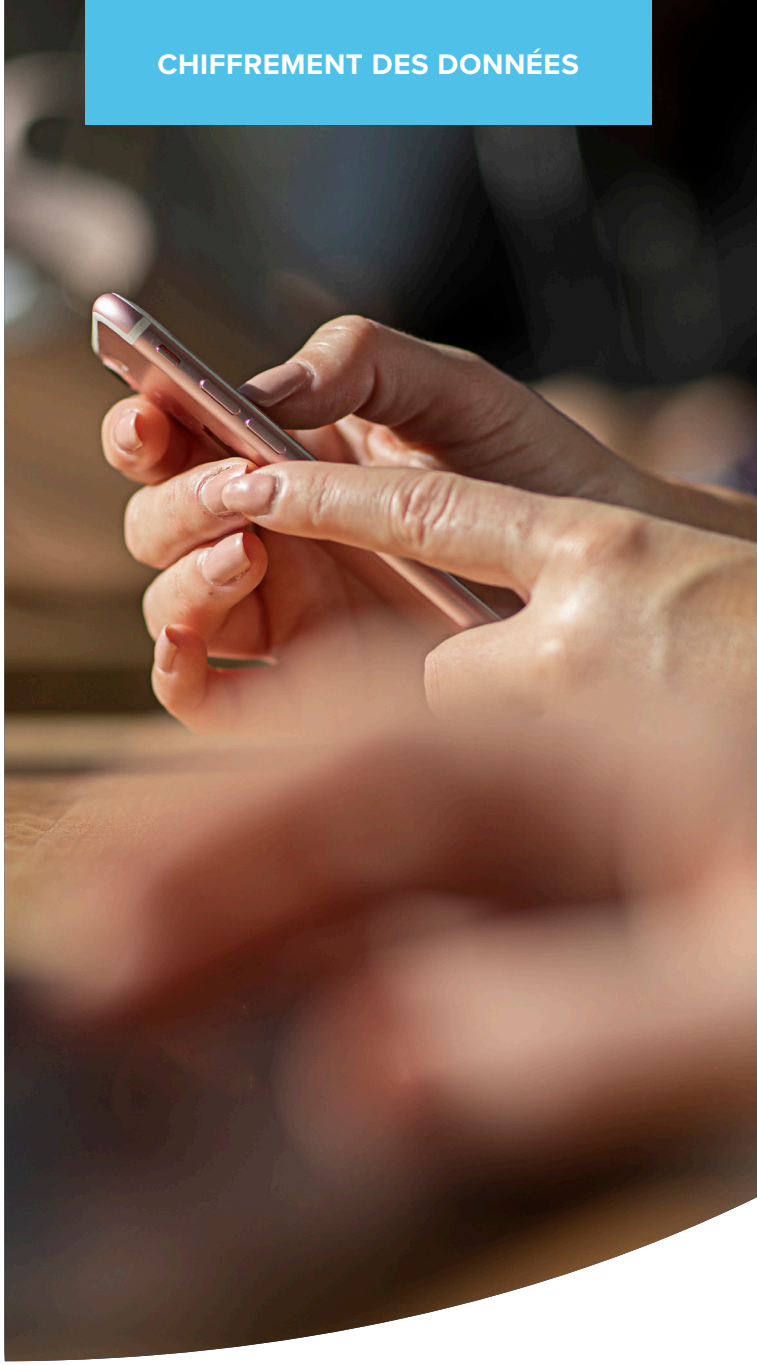
Pour connecter plusieurs appareils à un VPN :

Après avoir mis en place un fournisseur de VPN

- Créez un profil de configuration dans une MDM comme Jamf pour iOS et/ou macOS
- Déployez les configurations à autant d'appareils que vous le souhaitez
- Vous avez deviné : il n'y a pas d'étape trois

« Comment être sûr que le chiffrement est continu ? »

Héberger votre MDM dans le cloud est gage de sécurité et de cohérence dans le chiffrement. Avec un produit réputé tel que Jamf Cloud, vous avez l'assurance que votre serveur est sécurisé, que vos données sont protégées et que les mises à jour et les correctifs sont appliqués dès leur publication.



Les avantages du ZTNA sur le VPN traditionnel :

- Alors que le VPN repose sur un modèle de confiance implicite, le ZTNA procure une sécurité renforcée avec une approche explicite zero-trust qui vérifie les utilisateurs et les appareils avant de leur accorder l'accès aux ressources demandées.
- Le split-tunneling sécurise le trafic business tandis que le trafic personnel est acheminé directement vers Internet, et non vers un réseau central. Les avantages de cette approche sont multiples : réduction de la charge, économie de bande passante, amélioration des performances et une confidentialité garantie pour les utilisateurs finaux.
- Grâce à la protection permanente, les ressources sont protégées, même si le service est désactivé. En effet, il s'activera automatiquement en cas de demande d'accès.
- Profitez des avantages d'une empreinte minimale et d'un hébergement cloud : pas de contrat d'assistance coûteux, de configurations complexes ou de matériel à gérer.
- Le ZTNA couvre également macOS, iOS, iPadOS, Android et Windows, ce qui réduit le TCO et allège la charge administrative des équipes informatiques qui prennent en charge un environnement hétérogène.

Dans cette section, nous avons abordé les bases du chiffrement des données, les solutions natives des appareils Apple et les étapes permettant d'activer ce contrôle de sécurité sur macOS, iOS et iPadOS. Nous avons vu la supériorité du ZTNA sur le VPN traditionnel : cette technologie moderne sécurise les connexions réseau distantes en continu, ajoute des couches de sécurité supplémentaires – vérification des utilisateurs et des appareils – avant l'accès et garantit la protection des au repos et en mouvement. Mais qu'en est-il lorsque les données sont utilisées ou traitées par des applications ?

Les données ne sont plus dans aucun des deux états précédents et ne sont protégées par aucun contrôle de sécurité spécifique. La solution réside plutôt dans l'association de workflows de gestion et de sécurité continus.

CHIFFREMENT DES DONNÉES

Quand les applications accèdent aux données et les manipulent, les données passent de la mémoire (RAM) à l'application puis y retournent avant d'être définitivement enregistrées dans l'espace de stockage de l'appareil. Les applications élaborées par des développeurs connus et fiables contiennent des mécanismes de sécurité qui garantissent leur sécurité interne. Il y a de nombreuses raisons à cela ; surtout, il faut s'assurer que les données traitées au sein d'une application ne soient pas partagées avec d'autres programmes, services ou processus s'exécutant sur l'appareil. Cette mesure vise à préserver l'intégrité des données, mais aussi celle des applications.

Toutefois, la vigilance est de mise : des applications peuvent avoir été compromises par l'exploitation d'une vulnérabilité ou subi des modifications non autorisées de leur sécurité interne. Certaines applications malveillantes aux fonctions apparemment légitimement exécutent en parallèle des tâches clandestines et mettent en péril la sécurité des données pendant leur utilisation.

Dans ce contexte, quelle est la meilleure solution ? Notre réponse : une palette de bonnes pratiques, une stratégie de défense en profondeur, et des processus et workflows qui s'appuient sur Jamf Pro pour sécuriser au maximum les données en cours d'utilisation :

- Appliquer en continu une règle de gestion des correctifs et se procurer des applications auprès de sources légitimes, comme l'App Store d'Apple, les sites web de développeurs ou un fournisseur de gestion de confiance – les App Installers de Jamf, par exemple.
- Déployer des applications gérées via votre solution MDM préférée et mettre en place une gestion basée sur des règles pour les tenir à jour.
- Vérifier les réglages des appareils en installant des profils de configuration afin de réduire au minimum les menaces liées aux erreurs de configuration.
- Durcir les réglages des appareils pour limiter les comportements à risque susceptibles d'introduire des menaces, comme le jailbreaking d'iOS ou d'iPadOS, ou le chargement latéral d'applications à partir de sources non autorisées ou non sécurisées.
- Mettre en œuvre un programme de formation continue des utilisateurs afin de les tenir informés des menaces courantes et des risques que comportent certaines pratiques comme le Shadow IT.
- Élaborer une règle d'utilisation acceptable (PUA) à faire signer par tous les acteurs pour les sensibiliser aux comportements attendus et aux conséquences en cas d'infraction.

5

CINQUIÈME BLOC :

surveillance de la conformité

Vous devez connaître l'état des protocoles et des contrôles en place sur tous les appareils.

Même le meilleur système de sécurité a toujours un point faible. Pour une couverture optimale, les administrateurs doivent maintenir le parc de leur entreprise sous une étroite supervision. En effet, chaque appareil doit être mis à jour, bénéficier des derniers correctifs et correctement configuré.

« La conscience de l'ignorance est le début de la sagesse. »
— Socrate

La collecte de données télémétriques riches, qui donnent un aperçu des réglages de sécurité, des paramètres et de l'état de santé de chaque appareil, apporte de précieux renseignements au service informatique. Mieux armé pour protéger les appareils, les utilisateurs et les données, il peut également corriger et remettre en conformité les terminaux problématiques avant que la menace n'ait des conséquences plus lourdes, comme une violation de données.

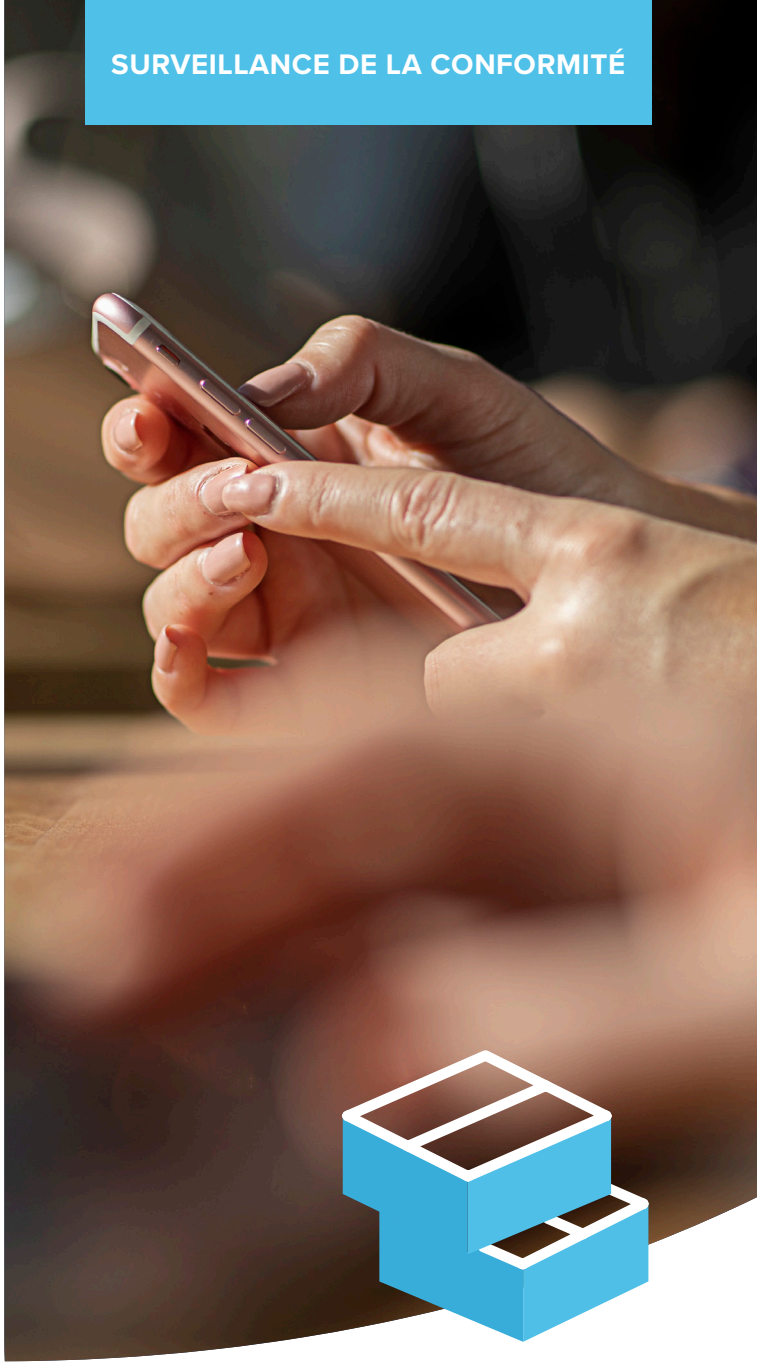
Comme pour la plupart des blocs présentés dans cet e-book, il existe plusieurs approches pour contrôler la conformité des terminaux : certaines sont manuelles, d'autres sont automatisées. L'efficacité du contrôle de la conformité est soumise à l'influence de différents facteurs : la base de connaissances, les solutions de gestion des appareils et de sécurité utilisées et les considérations budgétaires, pour ne citer que les plus importants.

Pour gérer manuellement l'inventaire et la conformité, il faut :

- Veiller à ce que tous les appareils de votre organisation soient protégés en procédant à des contrôles permanents
- Suivre physiquement chaque appareil
- Mettre à jour les applications de chaque appareil individuellement
- Vérifier que les réglages de sécurité, comme le chiffrement, sont configurés de manière cohérente sur chaque appareil
- Contrôler et confirmer que personne n'a introduit de risques (logiciels malveillants ou applications suspectes)
- Appliquer les mises à jour du système d'exploitation et de sécurité dès qu'elles sont disponibles afin de corriger les vulnérabilités connues et les bugs logiciels.
- Déployer le personnel adéquat pour trier les problèmes détectés, mettre en quarantaine les appareils compromis et effectuer les tâches de correction afin de rétablir la conformité des terminaux concernés

Cette méthode exige une vigilance constante et d'importants créneaux horaires pour mener à bien toutes les tâches de gestion. Elle repose également sur une grande implication des acteurs et des équipes de gestion, qui doivent coopérer efficacement. Soulignons également que cette méthode est essentiellement réactive : quand la vitesse compte, en cas d'incident par exemple, les délais de réaction risquent d'être prolongés, et il sera généralement impossible d'intervenir avant que le problème ne soit installé.

SURVEILLANCE DE LA CONFORMITÉ



Enfin, avec la multiplication et la diversification des appareils à prendre en charge, le temps nécessaire aux équipes informatiques et de sécurité pour répondre manuellement aux problèmes augmente de façon exponentielle. Les acteurs malveillants ont donc d'autant plus de temps pour mettre en œuvre leur chaîne d'attaque contre les organisations, ce qui augmente le risque de violation de données.

Surveiller l'inventaire avec Jamf, c'est :

- Obtenir des informations actualisées en temps réel sur tous les appareils simultanément.
- Déployer des mises à jour et des configurations de sécurité pour tout appareil qui n'est pas sécurisé correctement
- Tous en chœur : **il n'y a pas d'étape trois**

L'inventaire des appareils permet aux administrateurs de prendre le pouls de chaque appareil Apple de leur flotte. Informés de l'état actuel des appareils, les administrateurs savent quelles mises à jour envoyer et où, et quelles fonctionnalités de sécurité configurer. La création de groupes intelligents, basés sur des critères dynamiques, leur permet d'appliquer les mises à jour de façon sélective ou globale. Jamf Pro permet de cibler l'ensemble des appareils ou de les sélectionner selon des critères personnalisables – autorisations granulaires, types d'appareils, etc. – et ses puissants outils facilitent considérablement l'exécution des tâches liées à la conformité spécifiques. Pour en savoir plus, lisez notre e-book Introduction à la gestion d'inventaire.

Quand vous gérez la conformité avec Jamf, vous :

- Auditez les terminaux sur la base des critères du CIS (Center for Internet Security)
- Transférez toutes vos données de conformité vers le cloud pour une gestion centralisée
- Accédez aux journaux unifiés macOS et à la télémétrie complète des terminaux pour identifier les menaces rapidement et efficacement
- Assurez la conformité à l'aide de règles qui automatisent les tâches de correction et préservent la conformité des terminaux
- Surveillez les vulnérabilités et les expositions communes (CVE) pour comprendre les menaces présentes dans votre environnement.
- Prévenez les menaces de sécurité à l'aide d'analyses exhaustives alignées sur le cadre MITRE ATT&CK.
- Partagez en toute sécurité des données de télémétrie entre les solutions de gestion (Jamf Pro) et de sécurité (Jamf Protect) via l'API. Vous pouvez ainsi développer des workflows avancés pour minimiser les temps de réponse aux incidents et les résoudre sans délai

Il ne suffit pas de sécuriser vos appareils ; de nombreuses réglementations exigent que les organisations puissent prouver que les appareils sont continuellement sûrs et conformes. Elles doivent donc fournir des documents pour corroborer les niveaux de conformité à différents moments. En effet, si vous ne pouvez pas fournir la preuve qu'un appareil était conforme à un instant donné, c'est qu'il ne l'était pas à toutes fins utiles.

Mais les outils de rapport de Jamf fournissent aux organisations les données de télémétrie de chaque terminal, triées selon des critères clés comme les niveaux de correctifs, les vulnérabilités détectées et les horodatages. Toutes les opérations effectuées au cours du cycle de vie de l'appareil sont consignées. De plus, des intégrations permettent de partager ces données de télémétrie avec des outils internes et tiers pour les exploiter, par exemple, dans des tableaux de bord centralisés et des visualisations. Elles peuvent enfin être exportées dans d'autres formats, pour produire des rapports de conformité à destination d'audits réglementaires

6

SIXIÈME BLOC :

sécurité et gestion des applications

Les rapports de correctifs, les règles et les App Installers maintiennent les applications à jour et renforcent la sécurité.

Sécurité des applications

Savoir que les vulnérabilités identifiées sont corrigées est essentiel à la posture de sécurité des appareils. Mais savez-vous d'où viennent vos applications ? Avez-vous la certitude qu'elles ne contiennent pas de logiciels malveillants ? Ces questions sont cruciales pour votre organisation : si vous ne pouvez pas faire confiance à vos sources d'applications, vous mettez en danger la sécurité de vos appareils, la vie privée des utilisateurs finaux et la confidentialité des données sensibles.

Apple fait de la sécurité et de la confidentialité une priorité absolue. L'entreprise veille à ce que vous puissiez télécharger et utiliser des applications en toute sécurité.

Les points clés de la gestion et de la sécurité des applications :

1 **Les apps sont exécutées dans une sandbox :** chaque application fonctionne dans un espace qui lui est propre et ne peut pas interagir avec d'autres applications. Avant d'autoriser les apps à lire ou écrire des données partagées par d'autres, il faut obtenir l'approbation explicite d'un utilisateur authentifié.

2 **Approvisionnement centralisé et sécurisé :** les applications de l'App Store d'Apple sont vérifiées afin d'atténuer les risques de sécurité. Cette vérification se fait en deux volets : la notarisation d'une part, et un référentiel sécurisé d'autre part. Basé sur le cloud et géré par Apple, il héberge les applications qui ont passé des évaluations de sécurité rigoureuses. Ce référentiel permet également aux développeurs de mettre la dernière version de leurs applications à disposition des utilisateurs, éliminant ainsi les risques liés au téléchargement de logiciels illégitimes à partir de sources hasardeuses.

3 **La notarisation garantit l'intégrité de la technologie :** pour un maximum de fiabilité, les logiciels sont signés par l'identifiant unique du développeur, ce qui garantit qu'ils ont été vérifiés par Apple et ne contiennent aucun composant malveillant ni aucune anomalie d'authenticité. Lorsqu'une application est notariée, vous pouvez être sûr qu'elle n'a pas été falsifiée ou compromise.

4 **Gatekeeper bloque l'exécution des applications suspectes :** avant qu'une application macOS ne soit autorisée à s'exécuter la première fois (et après chaque mise à jour par la suite), Gatekeeper contrôle la validité des tickets de notarisation attribués. Si le ticket est valide, l'application est autorisée à fonctionner sans problème. Mais si ce n'est pas le cas, l'exécution de l'app est bloquée, et l'utilisateur est informé qu'elle a pu être modifiée par une partie non autorisée et que l'intégrité de sa sécurité interne n'est pas garantie.

5 **Limitation de l'utilisation des applications :** sur les appareils iOS, le seul moyen sûr d'obtenir des applications est de passer par l'App Store. Cela dit, le jailbreaking des appareils iOS et iPadOS ouvre l'accès à des app stores tiers qui sont souvent utilisés pour distribuer des applications piratées ou modifiées. On y trouve gratuitement des applications commerciales auxquelles des acteurs malveillants ont ajouté du code pour voler des données ou espionner les utilisateurs. Avec une MDM comme Jamf Pro, les administrateurs peuvent configurer des alertes qui signalent les appareils jailbreakés ; ils peuvent ensuite lancer des workflows de correction pour remédier au problème de sécurité.

Sur macOS, les utilisateurs (ou les administrateurs disposant d'une MDM) peuvent choisir entre deux options Gatekeeper :

- App Store Mac
- App Store Mac et développeurs identifiés

En limitant les utilisateurs de macOS à l'App Store Mac, les administrateurs contrôlent la sécurité des applications à l'échelle de l'appareil et minimisent le risque d'introduire des menaces provenant d'applications suspectes ou compromises. Mais si vous avez besoin d'applications qui ne sont disponibles que sur le site web du développeur, la deuxième option autorise les applications de l'App Store et celles qui proviennent de développeurs identifiés et contrôlés par Apple, dont les paquets de logiciels sont signés par un identifiant pour davantage de sécurité.

Bonnes pratiques

Pour macOS, autorisez le Mac App Store et les développeurs identifiés, en particulier si vous créez vos propres applications ou si vous repackagez des applications pour les déployer. Demandez également un identifiant développeur à Apple et signez les applications développées en interne par l'organisation afin que Gatekeeper leur fasse confiance. Enfin, si vous utilisez Jamf Pro comme solution MDM, vous pouvez déployer le catalogue d'applications Self Service sur tous les appareils. Le service informatique peut ainsi pré-approuver des applications, des paramètres, des configurations et bien plus encore, puis permettre aux utilisateurs d'installer les outils et les services dont ils ont besoin, quand ils en ont besoin. Et tout cela, sans ticket d'assistance, sans modification des permissions et sans identifiant Apple.

Réglages manuels des options de Gatekeeper :

- Rendez-vous dans Paramètres système > Confidentialité et sécurité > Sécurité
- Sélectionnez l'une des deux options disponibles
- Répétez l'opération pour tous les appareils de votre organisation.

Réglages des options Gatekeeper avec Jamf Pro :

- Créez et déployez un profil de configuration avec vos réglages Gatekeeper sur tous vos appareils.
- **C'est tout !**

Correctifs et mises à jour des applications

Mises à jour de l'OS, contrôle des versions grâce aux commandes MDM, Rapid Security Response, etc.

Les organisations doivent mettre en œuvre une stratégie de gestion des correctifs afin de tester et intégrer les corrections de bugs le plus rapidement possible. Elles assureront ainsi la protection de leur matériel, de leurs données et de leurs utilisateurs. Indispensables, les tests sont pourtant souvent négligés lorsqu'il s'agit de déployer des correctifs, en particulier lorsqu'ils comblent des vulnérabilités de sécurité urgentes. En réalisant ces deux opérations le plus tôt possible, le service informatique réduit l'impact de la propagation des menaces de sécurité tout en limitant au maximum l'introduction de problèmes plus importants, les correctifs pouvant parfois affecter par inadvertance des fonctionnalités critiques.

Pour tous les aspects abordés dans cet e-book, la durée des tâches administratives du service informatique est directement corrélée au nombre d'appareils gérés. C'est également le cas avec la gestion des correctifs, à une variable près : le nombre de correctifs à déployer, qui peut faire augmenter de manière exponentielle les tâches administratives nécessaires sur chaque appareil.

Voyons de quelles options disposent les administrateurs pour gérer les correctifs manuellement et à l'aide d'une MDM :

Options de gestion manuelle des correctifs :

- Former les utilisateurs à effectuer eux-mêmes les mises à jour dès qu'ils reçoivent des notifications sur leurs appareils.
- Collecter tous les appareils lorsqu'un nouveau correctif est déployé et le déployer manuellement.
- Corriger les appareils auxquels il manque des correctifs dans le cadre de vos processus de contrôle continu de conformité.

Options de gestion des correctifs via la MDM (Jamf Pro) :

- Jamf reçoit automatiquement les notifications de mises à jour et de correctifs, et fournit les outils permettant de les déployer sur tous les appareils de votre organisation, au moment où vous le décidez.
- Le catalogue d'applications Self Service de Jamf autonomise les utilisateurs : il les informe quand une mise à jour est disponible et leur permet de la réaliser eux-mêmes.
- Évitez de dépendre des utilisateurs finaux et allégez la charge de l'équipe informatique en automatisant la distribution des correctifs. Envoyez les correctifs sous forme de règles l'ensemble de flotte ou à une sélection d'appareils grâce aux groupes intelligents dynamiques.

Pour en savoir plus sur le cycle de vie des applications et les possibilités d'automatisation et de déploiement, consultez notre livre blanc.

Moderniser votre sécurité

Vous l'avez certainement compris, il n'existe pas d'approche générique de la sécurité. Une stratégie globale comporte plusieurs couches qui protègent vos appareils, vos utilisateurs et vos données de manière holistique, tout en offrant des protections granulaires qui forment un filet de sécurité numérique. C'est ce que l'on appelle la défense en profondeur : si une couche ne parvient pas à contrer une menace, la couche supérieure ou inférieure le fera.

Vous connaissez déjà sans doute l'approche de la sécurité par couches, même si vous ne vous en doutez pas. Prenons un exemple très familier : votre maison.

Il existe tout un éventail de protections anciennes et nouvelles pour la sécurité domestique, et vous avez sans aucun doute mis en place plusieurs d'entre elles pour protéger vos proches et vos biens :

- Serrures à pêne dormant sur les portes
- Système d'alarme domestique
- Vidéosurveillance
- Gardiens de sécurité
- Détecteurs de fumée et de monoxyde de carbone
- Extincteur à incendie
- Assurance habitation

En théorie, chacune des solutions ci-dessus peut assurer la sécurité du domicile. Mais seule, elle ne fournit qu'un aspect de la sécurité globale nécessaire. Cependant, lorsque vous les combinez, ces pièces s'emboîtent comme un puzzle pour former le tableau complet et cibler l'ensemble des problèmes. La cybersécurité, comme la gestion et la sécurité de votre flotte d'appareils Apple, repose sur des principes similaires. Il est donc fondamental d'autonomiser et d'informer les utilisateurs pour qu'ils appliquent les bonnes pratiques de sécurité afin de minimiser les risques et d'atténuer les menaces.

L'une des couches de la sécurité des terminaux consiste à signaler les risques qui pèsent sur les appareils. Certains utilisateurs savent détecter les attaques de phishing et éviteront de cliquer sur un lien malveillant ; d'autres, un peu trop confiants, peuvent suivre des instructions suspectes et introduire un risque pour l'appareil, l'utilisateur et les données. Mais comment peut-il savoir s'il a cliqué sur un lien malveillant ou compromis son appareil ou ses identifiants ?

Il y a une app pour ça ! Jamf Trust offre une protection contre les risques initiés par l'utilisateur, comme dans l'exemple d'attaque de phishing ci-dessus. Jamf envoie des notifications Apple Push lorsqu'une menace est détectée sur l'appareil, par exemple si le lien a installé un logiciel malveillant qui enregistre les frappes sur l'appareil.

La solution a déterminé l'existence d'une menace et en a informé l'utilisateur (ainsi que l'administrateur). Elle a aidé l'utilisateur à prendre conscience du danger et à se méfier de ce genre d'incidents. Quant au service informatique, il a pu répondre à l'incident et le corriger rapidement, en utilisant à la fois Jamf Pro et Jamf Protect pour mettre l'appareil en quarantaine, nettoyer l'infection, corriger toutes les vulnérabilités présentes et rétablir sa configuration de référence. Enfin, mettez cette expérience à profit pour orienter les prochaines formations de sensibilisation à la sécurité.

La sécurité des appareils et des données est un sujet extrêmement sérieux.

Les organisations peuvent choisir de devancer les attaques et les vols de données en mettant en place les protections de sécurité les plus solides possibles offerts par Apple. Et avec Jamf, ces opérations seront bien plus faciles, rapides et efficaces que les protocoles manuels.

En matière de cybersécurité, personne n'aime les surprises. Autant que possible, il faut éviter d'avoir à faire face à une attaque. Découvrez les meilleures options de sécurité pour votre organisation en essayant gratuitement les solutions Jamf, ou contactez un représentant Jamf dès aujourd'hui pour discuter d'une solution complète et personnalisée de gestion et de sécurité Apple pour votre entreprise.

Vous avez essayé le reste… Maintenant, choisissez le meilleur !

Essayez Jamf

Ou contactez votre revendeur Apple habituel pour un essai gratuit.