INTRODUCTION À LA SÉCURITÉ DE LA SANTÉ

Les établissements de santé sont, comme de nombreuses organisations dans le monde, tributaires de la technologie pour améliorer leurs pratiques. Au fil de leur apparition, les avancées déterminent – du moins en partie – la continuité des activités. Et elles transforment bien souvent les méthodes de travail, de stockage et de gestion, quand ce n'est pas les trois à la fois.

Ce n'est un secret pour personne : si le monde entier a été secoué par le Covid-19 et ses variants, la santé continue d'en subir les effets. Ceux-ci peuvent être directs, comme le nombre de patients à soigner, et indirects, liés à des impératifs connexes mais extérieurs :

- Assurer la gestion continue des données et des enregistrements confidentiels des patients, des utilisateurs et des terminaux, tout en restant conforme aux exigences réglementaires.
- Mettre en œuvre des changements au cœur des opérations, en introduisant la télésanté par exemple, tout en assurant la sécurité des patients et des soignants.
- Maintenir la sécurité des données dans tous les business models et se protéger contre les menaces et les attaques informatiques en hausse

« TROIS, LE NOMBRE MAGIQUE »

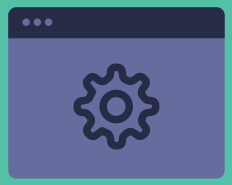
Les pratiques modernes de sécurité s'appuient sur de nombreux composants. Cet e-book n'a pas pour but de recenser l'intégralité des matériels et logiciels existants. Il cherche plutôt à comprendre les besoins uniques du secteur de la santé et s'efforce de mettre en avant les outils et processus qui y répondent le mieux.

Commençons par adopter une vue de haut niveau de la sécurité dans le secteur santé, pour voir les grandes catégories de composants, d'outils et de bonnes pratiques :

MATÉRIEL	LOGICIEL	CONFORMITÉ

Mais il ne suffit pas de choisir une solution dans chaque catégorie pour assurer la sécurité d'un établissement de santé. Si c'était aussi simple, les problèmes de sécurité n'existeraient pas. Ces catégories représentent plutôt l'angle d'attaque des solutions face à certains problèmes, et certains sont mieux adaptés que d'autres.

Par exemple, Jamf Protect surveille les incidents liés aux logiciels malveillants sur votre Mac. Cet outil les détecte, les prévient et les corrige, puis produit des rapports. Ce type de menaces cible principalement les logiciels et nécessitent donc une approche logicielle. La protection des terminaux entre donc dans la catégorie des logiciels.



Matériel

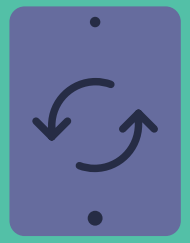
Les menaces et les attaques qui visent directement vos appareils Apple entrent dans la catégorie du matériel. On y classe également les pratiques de sécurité qui visent à corriger les vulnérabilités susceptibles de donner un accès physique aux appareils : chiffrement intégral du disque pour protéger les données au repos, activation de mots de passe pour empêcher l'accès non autorisé au menu de démarrage de macOS, ou déverrouillage de votre appareil iOS.

Logiciel

Pour savoir ce qui entre dans la catégorie des logiciels, pensez aux menaces et aux attaques qui visent principalement le système d'exploitation ou qui y opèrent.

Quelques grandes familles :

- Protection des terminaux
- Mise en place d'un VPN (réseau privé virtuel) ou d'un ZTNA (accès réseau Zero-Trust)
- Cycle de vie des applications et gestion des correctifs



Conformité

La conformité est sans doute la catégorie la plus importante de cette trinité. C'est aussi celle qui suscite le plus de préoccupations chez tous les acteurs. La conformité ne fait pas de distinction entre matériel et logiciel. Les acteurs de la catégorie « conformité » sont principalement concernés par le contrôle, l'obtention et le maintien de la conformité avec les **réglementations qui régissent les pratiques de santé**. Aux États-Unis il s'agit essentiellement de la **loi HIPAA de 1996, qui encadre la gestion électronique de l'assurance maladie**, et de la **loi HITECH de 2009 sur les technologies des informations de santé**.

Il existe une multitude de façons d'appuyer la **gestion de la conformité**, mais voici quelques points de départ fiables et valables pour tout type d'équipe :

- Les solutions de gestion des informations et des événements de sécurité (SIEM) centralisent la gestion des journaux
- Les outils de surveillance de sécurité supervisent activement l'état des appareils par rapport à des cadres de sécurité communs

Bonne pratique :

Les organisations ont tout intérêt à utiliser des cadres de gestion de la sécurité pour procéder au renforcement des terminaux et appliquer les bonnes pratiques de l'industrie. Citons notamment la **série SP 800-53 du National Institute of Standards and Technology (NIST)**, ou les **critères du Center for Internet Security (CIS)**.

« NOTRE VÉRITABLE ENNEMI N'A PAS ENCORE MONTRÉ SON VISAGE. »

– Michael Corleone

À l'instar du personnage incarné par Al Pacino dans Le Parrain III, qui doit faire face à plusieurs ennemis connus et inconnus, la sécurité informatique est confrontée à une horde apparemment sans fin d'acteurs malveillants.

Si les attaquants eux-mêmes peuvent être « sans visage », les moyens qu'ils emploient pour attaquer et compromettre les terminaux sont, eux, bien connus. Forts de ces informations, les administrateurs informatiques et les équipes de sécurité œuvrant dans le secteur de la santé peuvent protéger leurs appareils de plusieurs façons :

Renforcement des réglages des appareils

Gestion des dispositifs

Mise en œuvre de la protection des terminaux

Application des derniers correctifs sur les appareils

Surveillance des appareils en temps réel

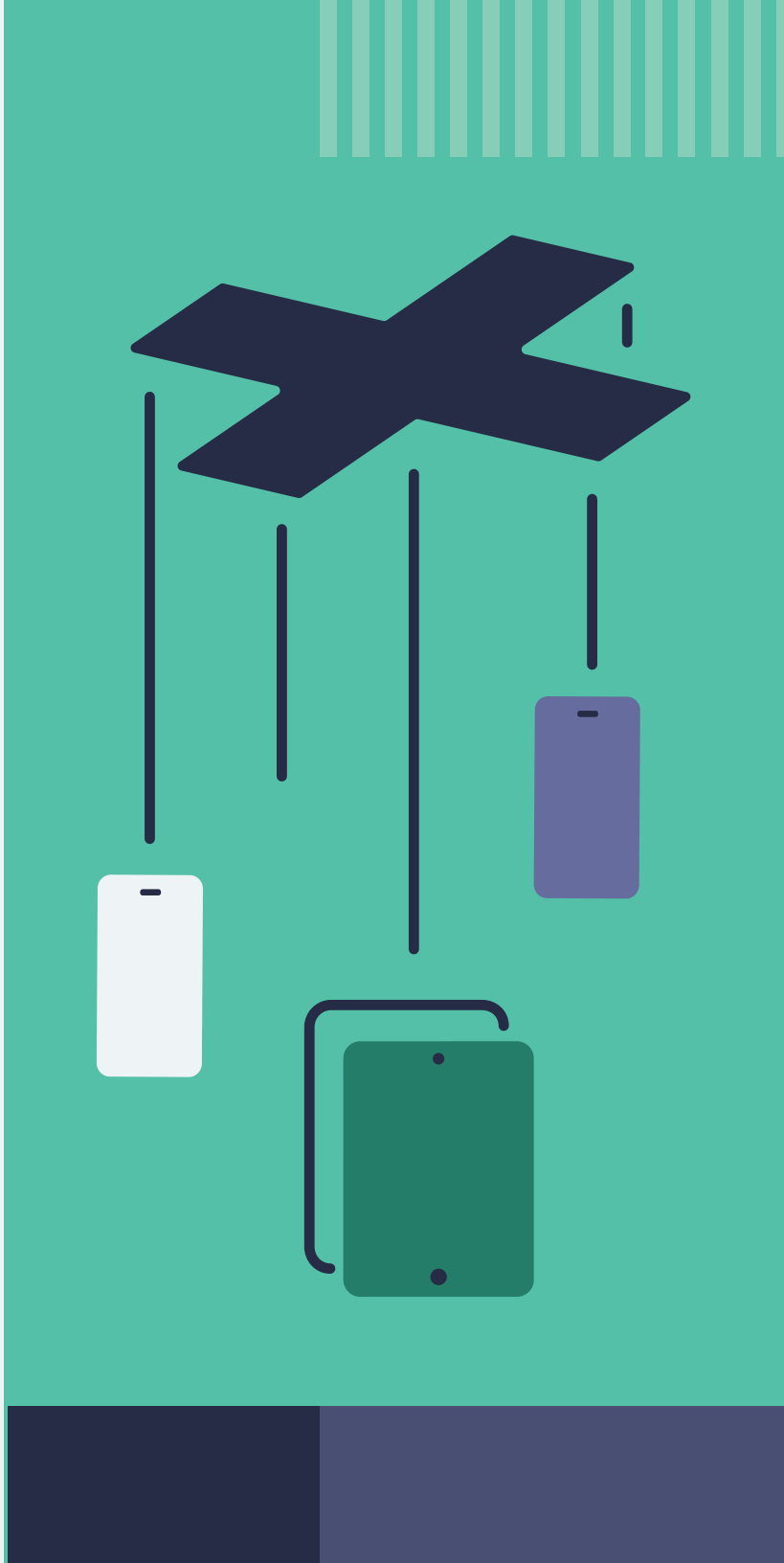
Triage des problèmes détectés

Atténuation des risques

ET

Maintien de la conformité des appareils

L'objectif : protéger toutes les parties prenantes contre la compromission d'appareils, la perte et le vol de données et les failles de sécurité. Autrement dit, tous les incidents qui pourraient avoir un impact négatif sur les performances, l'expérience de l'utilisateur final et le niveau de soins apporté aux patients.



Parmi les menaces potentielles, certaines concernent particulièrement les établissements de santé :

- Les attaques de logiciels malveillants – rançongiciels et dénis de service (DoS) surtout – peuvent paralyser les systèmes. Les soignants sont alors dans l'impossibilité d'utiliser les équipements pour administrer des soins critiques, voire vitaux.

- Les appareils dont le système ou les applications ne sont pas à jour exposent les organisations à des vulnérabilités connues et exploitables. Ils ouvrent ainsi la porte aux violations de données, aux fuites et au vol d'informations personnellement identifiables (IPI) ou de dossiers confidentiels réglementés.

- Les soignants attendent un minimum de convivialité des technologies qu'ils utilisent. Que ce soit parce qu'il manque une fonctionnalité ou qu'une application n'est pas à jour, un appareil qui ne fonctionne pas correctement fait perdre du temps. Et cela a des conséquences tangibles. De même, l'appareil configuré pour l'employé des RH n'aura que peu d'utilité pour le médecin qui fait ses visites, et inversement.

- Les réglementations gouvernementales encadrent la collecte, le stockage, la gestion, le partage et l'élimination des données confidentielles et médicales. Toute fuite de données peut donner lieu à une supervision réglementaire entraînant des sanctions civiles et pénales. Et l'on ne parle pas des risques de perte de patientèle ou de fermeture d'établissement causés par la dégradation de la réputation.

« LA PLUS GRANDE VICTOIRE EST CELLE QUI NE NÉCESSITE AUCUNE BATAILLE. » – Sun Tzu

Les problématiques liées à la sécurité du secteur de la santé sont aussi nombreuses que les approches pour les gérer. Elles ne se limitent à un mode de déploiement unique. Les acteurs malveillants emploient des méthodes variées pour contourner les défenses d'une organisation et compromettre leur cible.

La bonne nouvelle ? La sécurité des soins de santé ne suit pas non plus un modèle de déploiement unique. En réalité, la stratégie de « défense en profondeur » s'avère la meilleure pour faire face à la multiplicité des menaces. Elle consiste à superposer plusieurs protections défensives dans un effort concerté pour déjouer les attaques. Les organisations peuvent ainsi identifier les failles de sécurité et déployer des workflows de correction pour les combler et minimiser les risques.

Protection des terminaux

Pour beaucoup, la protection contre les logiciels malveillants doit rester la priorité de tout plan de sécurité visant à protéger les appareils, les utilisateurs et les données. Ce raisonnement n'est pas totalement infondé, compte tenu des capacités des logiciels de **protection des terminaux**, comme **Jamf Protect**. Ceux-ci parviennent en effet à prévenir les menaces connues et émergentes sur l'ensemble de votre flotte d'appareils macOS. Mais en réalité, cet aspect n'est qu'une variable dans la posture de sécurité globale de votre organisation.

La protection des appareils contre les logiciels malveillants joue un rôle essentiel : elle réduit les risques, sécurise les données et diminue les temps d'arrêt pour vos utilisateurs finaux. Dans ce domaine, le choix est large et les options sont nombreuses, mais certaines fonctionnalités intéresseront particulièrement les établissements de santé :

- Surveillance active des menaces en temps réel
- Détection des menaces connues et potentielles reposant sur les signatures et l'analyse
- Prévention des logiciels malveillants connus pour éliminer les menaces
- Correction des menaces et des logiciels malveillants identifiés
- Système d'alertes informant l'utilisateur final des menaces détectées et rectifiées
- Rapports en temps réel offrant aux administrateurs Mac plusieurs niveaux de compréhension, du résumé de haut niveau aux détails granulaires
- Faible empreinte des agents installés sur les terminaux : moins de ressources consommées = performances préservées

D'autres capacités, sans être indispensables, facilitent la vie des équipes informatiques et de sécurité, tout en les aidant à répondre aux problèmes rencontrés, à les trier et à les corriger :

1. Intégration avec d'autres produits. Par exemple, la protection des terminaux peut transmettre ses informations sur l'état des appareils à votre solution MDM. Cette intégration **permet d'exploiter des workflows SOAR (orchestration, automatisation et réponse de sécurité) : ceux-ci corrigent automatiquement les problèmes détectés**, en supprimant les logiciels malveillants et en effectuant des tâches de nettoyage, notamment.

2. Les environnements hautement réglementés ont tout intérêt à **s'aligner sur les cadres de sécurité**. Leurs directives pour la configuration des appareils et le suivi des indicateurs clés sont approuvées par le secteur et fondées sur les bonnes pratiques, et permettent d'atteindre le plus haut niveau de sécurité possible.

Gestion des appareils

Misez sur une suite de gestion des appareils mobiles (MDM) : c'est la clé d'une gestion efficace, efficiente et proactive de votre flotte d'appareils macOS et iOS. Naturellement, rien n'empêche le service informatique d'utiliser l'outil de configuration natif d'Apple, Apple Configurator 2, pour configurer chaque appareil manuellement. Mais en réalité, cette application n'a été conçue que pour gérer une poignée d'appareils à la fois. Au-delà, par exemple lors du déploiement et de la gestion de centaines ou de milliers d'appareils, la gestion des appareils via un logiciel de MDM – comme **Jamf Pro** ou **Jamf Now** – s'impose.

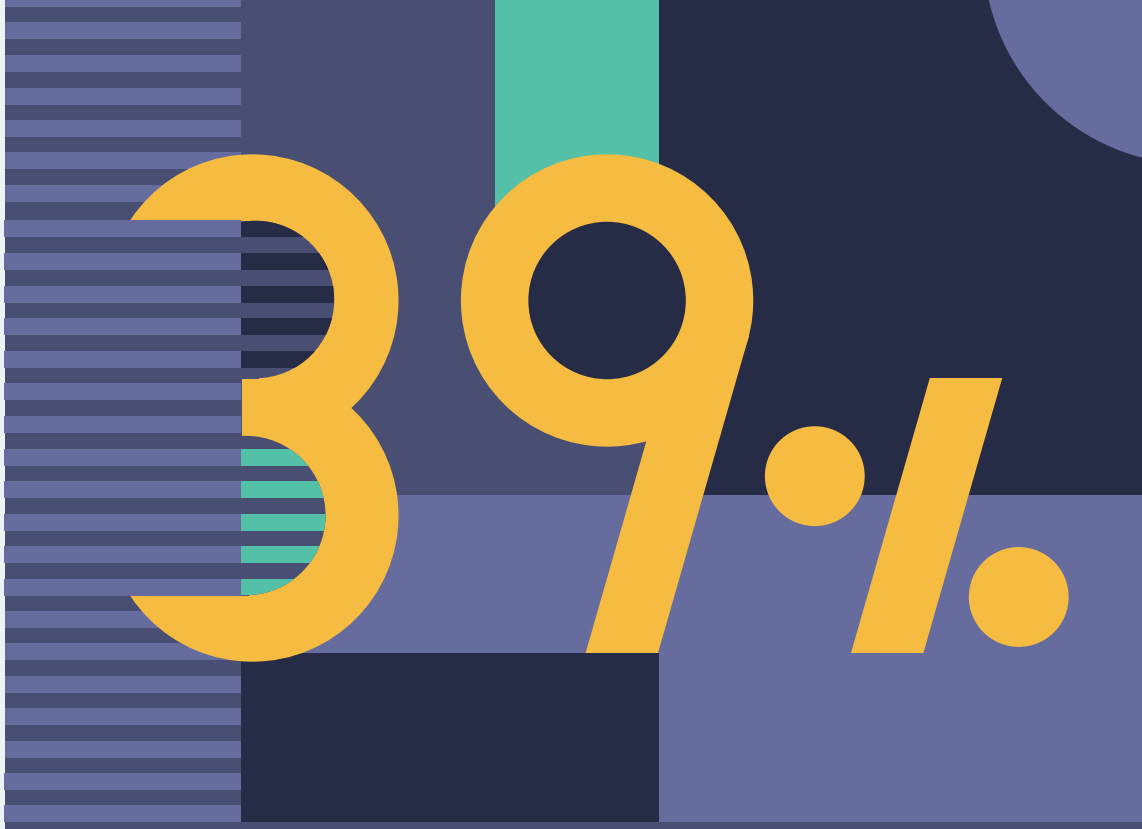
Jamf Pro s'aligne sur les cadres de gestion, de sécurité et de confidentialité d'Apple. Il permet ainsi à l'informatique de gérer des flottes entières à partir d'un tableau de bord unique et convivial. Grâce à ses fonctionnalités avancées combinées à des workflows puissants, les appareils restent configurés et alignés sur les politiques de l'entreprise, sans sacrifier l'expérience Apple des utilisateurs finaux.

La gestion des appareils renforce la sécurité globale en permettant aux organisations de :

- Simplifier l'onboarding/offboarding en rationalisant l'inscription des appareils.
- Normaliser des configurations types répondant aux besoins communs à certains services, types d'utilisateurs ou groupes. Les médecins, par exemple, vont utiliser les mêmes apps pour documenter leurs consultations et accéder aux périphériques de leur service (imprimantes, scanners, etc.).
- Développer des règles reflétant les stratégies organisationnelles comme les politiques d'utilisation acceptable (AUP).
- Déployer des logiciels et des mises à jour sur les appareils et mettre à la disposition des utilisateurs un Self Service contenant des apps préautorisées. Tout cela se fait sans utiliser les identifiants Apple ni se soucier des coûts d'abonnement et d'achat individuels.
- Gérer leur inventaire matériel et logiciel, ainsi que l'état de santé de la flotte Apple.
- Mettre en œuvre des processus modernes de gestion des identités pour suivre l'affectation des appareils, avec une visibilité sur les numéros de série, les informations de garantie et l'entretien.
- Suivre et localiser les appareils égarés en temps réel et minimiser les risques de perte des données grâce aux commandes de verrouillage et d'effacement à distance.

Gestion du cycle de vie des apps et des correctifs

Comment votre organisation gère-t-elle les cycles de mise à jour des systèmes d'exploitation et des applications ? Est-ce que vous testez les mises à jour dans un environnement isolé pour vérifier leur compatibilité avant de les déployer sur des systèmes de production ? Et quels contrôles avez-vous mis en place pour vérifier que les appareils de votre flotte ont bien reçu tous les correctifs nécessaires ? Si la réponse à l'une de ces questions est « ? », votre organisation fait sans doute partie des 39 %.



Mais quels 39 %, demandez-vous ? C'est une excellente question !

Ce chiffre désigne le pourcentage des organisations qui, selon les conclusions de **Security 360, Rapport annuel sur les tendances** de Jamf, « **ont laissé des appareils souffrant de vulnérabilités connues fonctionner dans un environnement de production, sans limiter leurs privilèges ni leur accès aux données.** »

Cette situation est problématique. En effet, un nombre important de **vulnérabilités et d'expositions communes** (CVE) s'appuient sur des failles non corrigées pour attaquer et compromettre les terminaux. La liste CVE des failles de cybersécurité divulguées est tenue à jour par la **MITRE Corporation**. Elle bénéficie en outre du parrainage du ministère américain de la sécurité intérieure (DHS) et de l'**Agence pour la cybersécurité et la sécurité des infrastructures** (CISA). Elle compte plus de 160 000 enregistrements CVE uniques dont la gravité varie.

Là encore, il est essentiel de disposer d'une solution MDM qui sache gérer les versions des logiciels installés sur votre flotte d'appareils et le cycle de vie des apps. Elle doit permettre au service informatique de :

- Déterminer quels appareils nécessitent des mises à jour du système d'exploitation, des applications et des périphériques.
- Identifier les correctifs nécessaires en s'appuyant sur une liste actualisée des versions des correctifs.
- Désactiver les apps et les services qui présentent une menace parce qu'ils ne sont pas corrigés ou ne sont plus pris en charge par le développeur.
- Utiliser les « groupes intelligents » de Jamf en conjonction avec les « règles » pour fournir efficacement des mises à jour aux appareils – et seulement à ceux qui en ont besoin.

Renforcement des appareils

La sécurisation des appareils n'a rien d'une tâche triviale. La configuration des appareils dépend de votre environnement, de vos besoins organisationnels et des exigences réglementaires. Selon ces critères, ainsi que le nombre et les types d'appareils concernés, le processus initial peut prendre de quelques minutes à plusieurs heures par appareil. En général, plus la flotte est importante, plus les besoins et les exigences de conformité varient entre les types d'utilisateurs et départements. Il faudra donc d'autant plus de temps à l'informatique pour renforcer les appareils. C'est assez logique : il faut beaucoup moins de temps pour sécuriser les cent appareils d'un même service que pour configurer cinquante appareils répartis sur cinq services différents, dont la moitié est hors site.

Cela souligne l'importance de se procurer les outils adaptés à la tâche. Dans ce cas, le durcissement consiste à « verrouiller » les fonctionnalités superflues ou qui nécessitent une configuration spécifique pour respecter les règles de l'organisation. Il s'agit également de limiter la surface d'attaque des appareils afin de **réduire le nombre de vecteurs d'entrée pour les acteurs malveillants**.

Dans leur grande majorité, ces fonctionnalités sont configurables à l'aide de la solution MDM utilisée pour la gestion de votre flotte. La clé d'un support optimal de macOS et iOS ? Une solution qui offre une **prise en charge le jour même** des dernières versions des systèmes d'exploitation Apple, et donc des cadres Apple de gestion des appareils, de sécurité et de confidentialité. Vous bénéficiez ainsi d'une compatibilité totale de ces aspects clés :

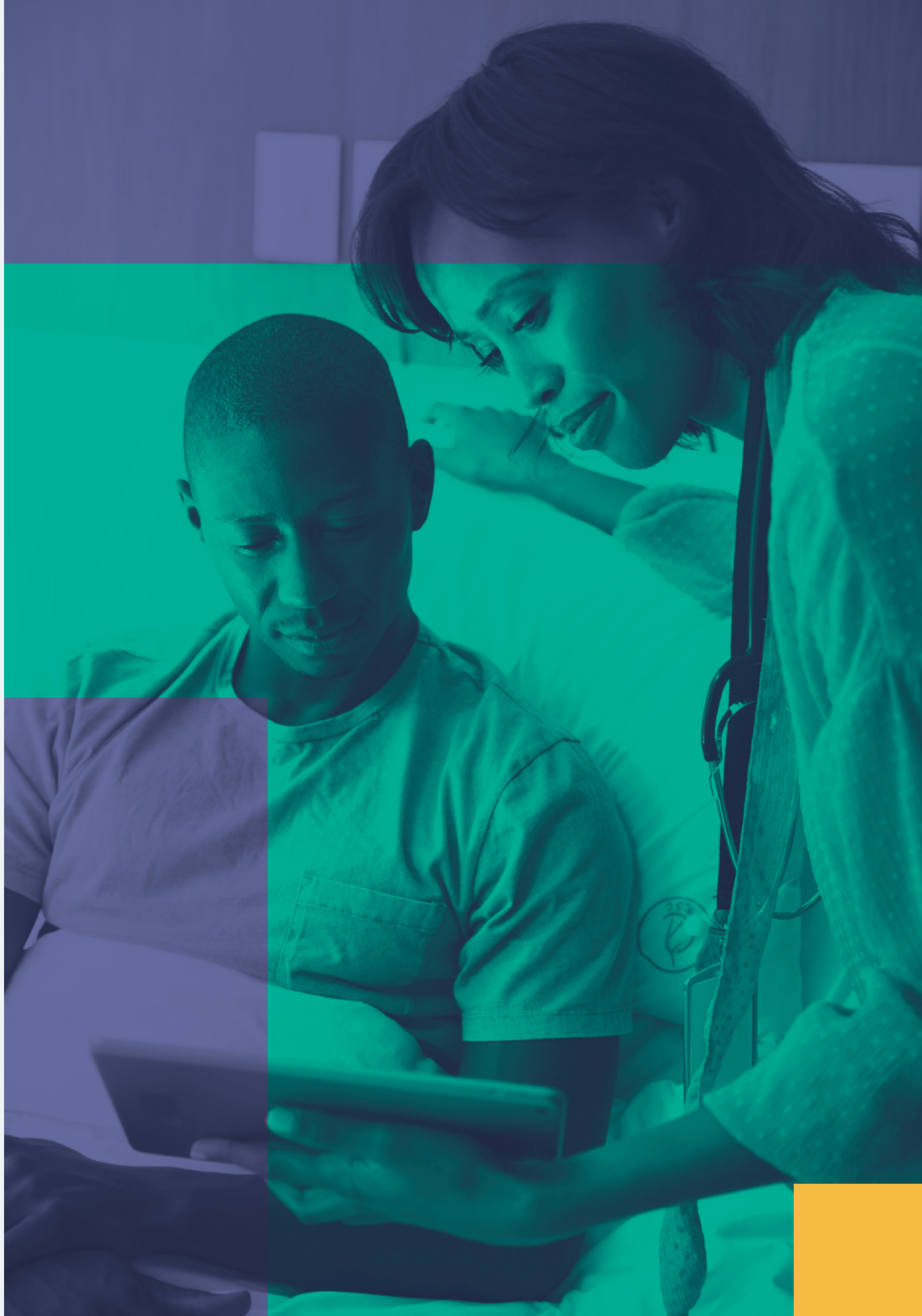
- Commandes utilisées pour gérer les appareils
- Réglages configurables pour sécuriser davantage les appareils
- Adhésion de toutes les apps aux contrôles de confidentialité des utilisateurs

Prenons l'exemple de l'activation du chiffrement du disque complet de FileVault. Elle est indispensable pour protéger les données au repos contre les utilisateurs non autorisés. En cas de perte ou de vol d'un appareil, les données privées stockées sur l'appareil sont illisibles pour quiconque ne possède pas la clé de déchiffrement. Sans une prise en charge appropriée, un utilisateur disposant d'un compte valide peut se retrouver dans l'impossibilité de déverrouiller le contenu du disque, parce que son compte n'aura pas été ajouté au groupe de sécurité de FileVault sur cet appareil. Lorsque votre **solution MDM administre correctement FileVault**, elle ajoute l'utilisateur au groupe approprié pour qu'il ait accès aux données sécurisées. Et en cas d'urgence, une clé de récupération est automatiquement générée et stockée avec l'enregistrement de l'appareil dans la MDM.

Accès sécurisé et communication

Nous avons abordé l'importance de la protection des terminaux, de la gestion des appareils, de leur renforcement et des mises à jour. Voyons maintenant la sécurisation des connectivités réseau avec des **solutions conçues pour l'informatique moderne**. Elle joue en effet un rôle crucial dans la sécurité des données, le maintien de leur intégrité et leur protection contre les menaces – toujours sans affecter les utilisateurs finaux.

Il y a cinq à dix ans, le VPN était la principale méthode de sécurisation des communications – et c'était une approche tout à fait raisonnable. Le VPN était – et reste pour certains – la norme de facto pour le chiffrement des connectivités réseaux, en particulier pour la connexion à distance aux ressources organisationnelles. Mais dans les environnements modernes de travail à distance et hybride, comme la télésanté, le modèle de sécurité du VPN est dépassé. Surtout, il n'offre pas **la flexibilité et les protections supplémentaires en matière de sécurité et d'accès** du ZTNA.



Selon la définition de **Gartner**, l'accès réseau Zero-Trust (ou ZTNA, pour Zero Trust Network Access) est un produit ou un service qui crée **une frontière logique reposant sur l'identité et le contexte, autour d'une application ou d'un ensemble d'applications**. En un mot, le modèle de sécurité crée des microtunnels au niveau de chaque application. Pour les personnes impliquées, les avantages sont les mêmes :

- Seuls les utilisateurs autorisés peuvent se connecter aux applications de santé.
- Les règles sont uniformément appliquées à l'ensemble des ressources et des clouds.
- Les microtunnels appliquent le principe du moindre privilège et empêchent les déplacements latéraux.
- Mise en œuvre de l'authentification unique (SSO), unifiée sur tous les appareils.

Le VPN a du bon, mais au prix de quelques problèmes de sécurité considérables : il accorde aux utilisateurs authentifiés l'accès à toutes les ressources – et pas seulement à celles dont ils ont spécifiquement besoin. Un autre problème important, dont la gestion échappe totalement à l'informatique : les utilisateurs doivent faire le choix de se connecter via un VPN pour que les protections s'activent. C'est ce qui ressort d'**une enquête menée par security.org**, qui posait notamment la question suivante : « Utilisez-vous un VPN ? ». 43 % des utilisateurs ont répondu : « Je sais ce que c'est, mais je n'en utilise pas ».

En coulisse, le **ZTNA s'assure que l'utilisateur est authentifié et autorisé et contrôle la fiabilité de l'appareil avant d'accorder l'accès aux données**.

Création des identités

La **gestion des identités des utilisateurs et l'octroi des accès** aux ressources de l'entreprise jouent un rôle décisif dans la sécurité de tout type d'environnement. Lorsque la sécurité et la conformité des soins de santé est en jeu, il faut faire preuve de la plus grande rigueur. Les soignants remplissent une mission critique, et les exigences réglementaires dictent les règles, l'accès et l'utilisation des données : les délais d'actions sont réduits, la marge d'erreur encore plus.

Dans ce contexte, pourquoi compter sur des opérations manuelles ou ponctuelles pour gérer les comptes d'utilisateurs, et prendre le risque d'une erreur humaine ? Vous ne devriez pas ; cette approche n'est ni efficace ni fiable. Dans les environnements dynamiques qui évoluent constamment, les organisations ont tout intérêt à standardiser l'approvisionnement des comptes et des accès pour automatiser les workflows. Avec des normes et des workflows appropriés pour l'approvisionnement des identités, les utilisateurs finaux bénéficient d'un accès sécurisé aux ressources utiles à tout moment, quels que soient leur appareil et leur emplacement.

En s'appuyant à la fois sur les fournisseurs d'identité Cloud (IdP) et sur la technologie d'authentification unique (SSO), le service informatique peut créer des workflows types automatisés pour :

- Normaliser l'onboarding des nouveaux employés
- Normaliser les déploiements matériels
- Accorder l'accès aux ressources, applications et services
- Mettre en place et appliquer des règles pour encadrer les mots de passe
- Synchroniser les mots de passe sur tous les types d'appareils
- Intégrer le ZTNA pour limiter l'accès aux ressources compromises sans empêcher l'accès aux services non affectés

Déploiement du matériel

Le déploiement de nouveaux appareils, ordinateurs portables Macbook Pro ou appareils mobiles comme l'iPad ou l'iPhone, semble simple à première vue : il suffit d'acheter, de configurer et de déployer les appareils. Mais ce processus est souvent semé d'embûches. En raison des problèmes d'acquisition ou de coordination logistique, c'est généralement au niveau de l'approvisionnement que l'on rencontre les obstacles qui retardent le plus la remise des appareils aux utilisateurs.

Mais ce n'est pas une fatalité. En effet, Apple s'est particulièrement attaché à ce que ses appareils puissent être déployés sans aucun contact physique ou presque, grâce au déploiement Zero-Touch. Pour le service informatique, le déploiement des appareils est aussi simple que rapide avec le modèle Zero-Touch :

- ☑ Création d'un compte Apple Business Manager/School Manager
- ☑ Association du compte Apple Business Manager/School Manager à la solution MDM.
- ☑ Configuration des réglages du profil d'enrôlement PreStage.

C'est tout !

Quand votre organisation achète de nouveaux appareils auprès d'Apple (ou de ses revendeurs autorisés), leurs enregistrements sont ajoutés à votre compte ASM/ABM. Une fois l'enrôlement effectué auprès d'Apple, votre MDM se charge du reste.

Une solution IdP, comme Jamf Connect, **peut automatiser davantage le processus d'approvisionnement en tirant parti de l'authentification SSO basée sur le cloud.** Grâce à cette méthode, l'utilisateur final peut recevoir directement son nouvel appareil d'Apple – un gain de temps considérable pour le service informatique. Il s'épargne en effet toute la configuration manuelle. Quant aux utilisateurs, ils sont parfaitement autonomes. Il leur suffit de déballer leur nouvel appareil, de l'allumer et de terminer le processus d'enrôlement. Pendant que les utilisateurs suivent le processus d'inscription simplifié, des workflows sécurisés et personnalisés s'exécutent en arrière-plan. Ils installent les apps essentielles, ouvrent l'accès aux services, sécurisent le terminal et ajoutent les configurations indispensables, en un minimum de temps.

Rapports de conformité

Dans le secteur de la santé, la pression de la conformité et des rapports obligatoires s'exerce sur les données : les dossiers médicaux, les données de confidentialité des patients, et toute information permettant d'identifier un patient ou des détails de son historique de santé. La collecte, la gestion, le partage, le stockage et l'élimination de ces données sont soumis aux réglementations découlant de la loi HIPAA.

Les organismes de santé sont tenus de se conformer à ces directives. Par contre, c'est à eux de déterminer leur approche et la façon dont ils vont mettre en œuvre et gérer les mesures de protection nécessaires. Ils doivent avoir l'assurance que les informations PII/PHI sont protégées et le restent. En cas de faille, ils sont tenus de prendre des mesures et de remédier au problème, par exemple en remettant l'application, le service ou l'appareil incriminé en conformité dans les meilleurs délais.

Pour évaluer un logiciel de rapports de conformité, vous voulez qu'il puisse **renforcer la sécurité tout en allégeant les efforts liés aux audits de conformité**. Pour cela, gardez en tête les critères suivants :

- Les journaux de chaque terminal doivent être collectés et transmis en temps réel à un emplacement central. Là, ils pourront être examinés par les équipes informatiques et de sécurité.
- Des filtres d'événements intégrés examinent les journaux, détectent les problèmes et les trient en fonction de leur gravité.
- Le niveau de détail des journaux d'audit peut être configuré dans des modèles adaptés à différents types d'appareils et exigences de conformité.
- Le déploiement et la configuration des logiciels de conformité sur les terminaux peut se faire selon de multiples méthodes, selon les besoins organisationnels.
- Des préférences de détection personnalisables adaptent la collecte aux exigences réglementaires.
- Alignement sur des cadres de conformité fiables : NIST SP 800-53r4, NIST SP 800-171 et la Certification du modèle de maturité de la cybersécurité (CMMC) pour la gestion des informations non classifiées contrôlées (CUI) dans les systèmes et organismes non fédéraux.
- Intégration avec des solutions logicielles pour centraliser en continu la collecte des journaux (SIEM) ; création de règles pour mettre les appareils en conformité (MDM) ; exécution de workflows de correction pour atténuer les risques liés aux logiciels malveillants et aux applications indésirables (protection des terminaux).

« LA MEILLEURE FAÇON DE PRÉDIRE L'AVENIR EST DE LE CRÉER. »

– Abraham Lincoln

L'avenir est aux progrès technologiques qui permettent l'accès à distance aux soins de santé et à la télésanté. Dans le monde entier, des soignants exploitent déjà les avantages de la télésanté. Au-delà des consultations entièrement à distance, des modèles hybrides comprenant aussi des visites en personne émergent. S'ils offrent de nombreuses possibilités, ils soulèvent aussi des problèmes de sécurité.

C'est normal : utilisé sur le terrain, un appareil comme Macbook Pro ou un iPad est plus susceptible d'être perdu ou volé. Mais il peut aussi être victime d'une fuite de données due à une app mal développée, ou d'une attaque d'exfiltration de type « Man-in-the-Middle » (MitM) en se connectant à un point d'accès Wi-Fi non fiable.

Les acteurs malveillants ne disparaîtront pas. Il n'existe pas de solution miracle pour les empêcher de tenter d'exploiter des vulnérabilités ou d'obtenir des renseignements médicaux personnels. L'objectif n'est pas de vous effrayer, mais plutôt de vous informer d'une menace bien réelle et omniprésente : en ligne, hors ligne, à la cafétéria de l'hôpital, au domicile des patients ou dans les transports. Pour un organisme de santé, la question n'est pas de savoir « **si** » une faille de sécurité se produira, mais « **quand** ».

Et pour la victime, cette variable est inconnue. Mais le tableau n'est pas aussi sombre qu'il n'y paraît...

- ☑ Formez régulièrement vos employés à l'**identification des tentatives d'hameçonnage** et au signalement des problèmes de sécurité.
- ☑ Travaillez avec des partenaires de confiance pour exploiter les **solutions et services les plus sûrs.**
- ☑ Aligner vos règles internes sur les exigences réglementaires et les cadres standards de gestion des appareils, de sécurité et de respect de la vie privée.
- ☑ Minimisez les risques, atténuez les menaces et corrigez les problèmes.
- ☑ Tenez-vous informé
- ☑ Réduisez les surfaces d'attaque.
- ☑ Étudiez des processus d'évaluation des risques et une stratégie de défense approfondie sur plusieurs fronts.
- ☑ Maintenez la conformité des appareils
- ☑ Protégez les utilisateurs, les appareils et les données sensibles.
- ☑ Apprenez aux utilisateurs finaux à repérer les menaces d'aujourd'hui... et de demain.

« ...DEMAIN APPARTIENT À CEUX QUI S'Y PRÉPARENT AUJOURD'HUI. »

– Malcolm X

Face à l'expansion des services de santé et aux menaces connues et inconnues qui visent le secteur, les paroles de Malcom X et d'Abraham Lincoln sont une source d'inspiration pour les organismes de santé. En prenant aujourd'hui des décisions judicieuses qui façonneront et créeront l'avenir de leur organisation, ils se donnent les moyens de répondre aux besoins de sécurité modernes d'aujourd'hui.

Jamf est prêt à vous aider à répondre à vos besoins en matière de sécurité. Découvrez-le en faisant un essai gratuit.

Demander une version d'essai

Ou contactez votre revendeur Apple habituel pour essayer Jamf gratuitement.