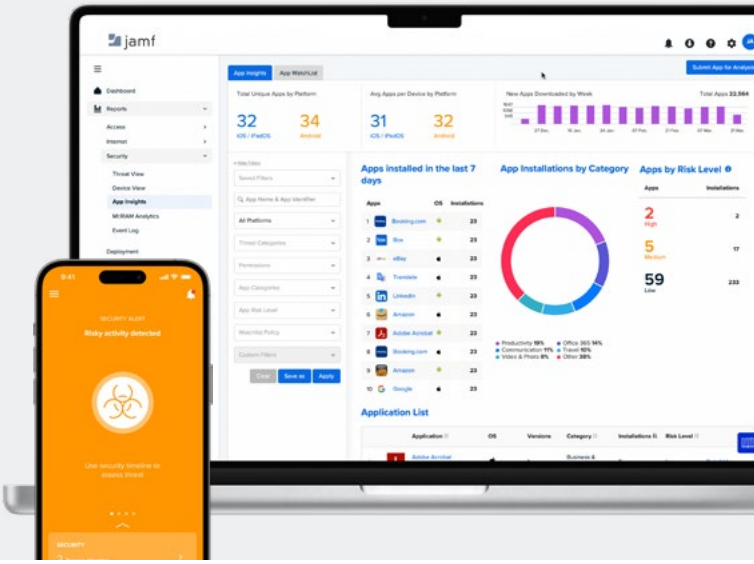
jamf

Bonnes pratiques :

Protéger l'entreprise contre les menaces



La sécurité revêt de nombreuses significations selon l'entreprise. Des risques critiques dans une organisation peuvent avoir moins d'importance dans une autre ou dans un autre secteur, non pas parce que la première attache davantage d'importance que la seconde à la sécurité, mais simplement parce qu'elles ne sont pas soumises aux mêmes obligations de conformité.

Au-delà des différences de classification et de hiérarchisation des facteurs de risque, les plans de cybersécurité de toutes les entreprises partagent un objectif commun : renforcer la posture de sécurité.

Pour y parvenir, il est essentiel d'enrichir votre plan de cybersécurité en ajoutant des stratégies éprouvées de défense contre les menaces. Chaque stratégie présentée dans ce document technique est une bonne pratique reconnue pour assurer la confidentialité, l'intégrité et la disponibilité des terminaux et des données sensibles. Mais au-delà de leur intérêt individuel, c'est lorsqu'elles sont combinées qu'elles offrent aux organisations le maximum d'avantages. Suivez notre guide pour :

- Développer une stratégie de défense en profondeur
- Étendre les couches de protection à l’ensemble de votre infrastructure
- Simplifier la gestion et la sécurité des terminaux Mac et mobiles
- Maintenir la conformité avec les règles de sécurité des données et de protection de la vie privée des utilisateurs
- Réduire la complexité en consolidant les workflows des équipes informatiques et de sécurité
- Accélérer la réponse aux incidents tout en augmentant la productivité des utilisateurs et le ROI

1. Chiffrement des données

Nous commençons notre tour d'horizon par le chiffrement. Souvent considérée comme la dernière ligne de défense, l'activation du chiffrement des volumes sur tous les types d'appareils reste essentielle. Elle apporte une couche de protection contre les accès non autorisés si les autres lignes de défense ne sont pas parvenues à arrêter les pirates. Les algorithmes de chiffrement peuvent être complexes, mais heureusement pour les administrateurs, le déploiement de cette mesure de sécurité reste très simple à gérer avec votre solution de gestion des appareils mobiles (MDM).

Les workflows administratifs comprennent des listes de contrôle des bonnes pratiques. Mettre en place un compte et un mot de passe administrateur sur tous les appareils gérés, encadrer les autorisations accordées aux utilisateurs pour déverrouiller les volumes chiffrés, conserver des registres précis des clés de récupération unique de chaque appareil… autant de tâches qui offrent une protection importante contre l'accès non autorisé aux données. Mais leur complexité et l'importance de l'effort manuel qu'elles demandent entraîne des lourdeurs administratives et introduisent des erreurs. Avec la diversité des systèmes d'exploitation (OS) pris en charge, multipliée par le nombre d'appareils, maintenir ces informations cruciales à jour devient un véritable défi.

Votre solution MDM simplifie le déploiement du chiffrement des données sur les appareils :

- Elle garantit une application homogène du chiffrement sur l'ensemble du parc d'appareils Apple en incluant macOS, iOS, iPadOS, watchOS, tvOS et visionOS.
- Elle assure la parité des mesures de sécurité entre les appareils appartenant à l'entreprise et les appareils BYOD tout en respectant la vie privée des utilisateurs.
- Elle automatise les workflows de chiffrement et applique une protection sans faille dès la fin du processus de configuration de l'appareil au moment de l'onboarding.
- Elle crée des comptes de niveau administrateur après une inscription réussie et utilise LAPS (solution de mot de passe d'administrateur local) pour Jamf Pro pour stocker les mots de passe aléatoires des comptes administrateurs locaux gérés, les renouveler et les afficher.
- Elle centralise la gestion des clés de récupération dans le dossier de chaque appareil pour sécuriser le stockage et faciliter l'accès en cas de besoin.

2 Application des correctifs et des mises à jour

L'un des moyens les plus efficaces pour les organisations de protéger leurs appareils, leurs utilisateurs et leurs données consiste à maintenir les appareils à jour en appliquant les mises à jour de sécurité et les correctifs des systèmes et des applications. Les menaces de type « zero-day » se multiplient et font de plus en plus de dégâts, mais nous nous concentrons dans cette section sur les vulnérabilités connues et les bugs pour lesquels les développeurs proposent des correctifs et des mises à jour. Nous insistons également sur l'importance de la régularité des mises à jour pour maintenir la posture de sécurité de vos appareils et de votre organisation.

Lorsque l'on parle de vulnérabilités connues, c'est le terme « connues » qui doit retenir votre attention : cela veut dire qu'il existe une mise à jour permettant d'atténuer le risque pour les données de l'organisation et sa conformité. Dans cette optique, la gestion des appareils mobiles (MDM) comprend un certain nombre de méthodes qui aident à protéger les appareils contre les menaces connues. Mais elle va plus loin : elle renforce les protections de sécurité natives de l'OS en exploitant les nouvelles fonctionnalités qui sont souvent incluses dans les dernières mises à jour. Tout cela profite aux organisations en maintenant la sécurité des données et en préservant la productivité des utilisateurs finaux.

Particulièrement flexibles, les solutions MDM s'assurent que les appareils restent à jour de plusieurs façons :

- La compatibilité immédiate avec les workflows de mises à jour et de mise à niveau de l'OS permet aux organisations d'établir librement leur calendrier de montée de version.
- Les applications gérées sont toujours à jour lorsqu'elles sont déployées à partir de l'App Store d'Apple. Pour les applications tierces, Jamf App Installers automatise le processus de mise à jour des plus de 700 applications du catalogue d'applications de Jamf.
- La solution MDM maintient la conformité réglementaire en appliquant les exigences de l'OS par le biais de règles.
- Elle s'intègre avec Jamf Connect pour mettre en place l'accès réseau Zero Trust (ZTNA) qui protège les ressources de tout accès par des appareils compromis, en déclenchant des workflows de correction automatisés.
- Elle gère et sécurise les terminaux à partir d'une solution holistique et centralisée qui offre aux équipes une visibilité indispensable sur l'état des appareils, ainsi que les outils nécessaires pour effectuer des mises à jour sur la base de données télémétriques en temps réel.

3 Authentification multifacteur (AMF)

Lorsque l'on aborde la gestion des identités et des accès (IAM) et les stratégies de défense en profondeur, l'AMF s'ajoute naturellement aux contrôles de sécurité visant à vérifier que les utilisateurs sont bien ceux qu'ils prétendent être au moment de l'authentification. La vérification des identifiants n'est qu'une moitié du modèle Zero Trust. La méthode établie consistant à s'appuyer uniquement sur les identifiants de l'utilisateur pour encadrer l'accès aux ressources sensibles a démontré ses lacunes : les mots de passe peuvent être faciles à deviner, et cette protection minime peut même être entièrement contournée par les pirates qui auront obtenu les identifiants par d'autres moyens, à commencer par le phishing.

Selon l'Agence américaine pour la cybersécurité et les infrastructures (CISA), « l'utilisation de l'AMF sur vos comptes réduit de 99 % les risques de piratage ». Cette statistique est confirmée par des organisations telles que Microsoft et Google : selon elles, l'AMF prévient 99,9 % des attaques sur vos comptes et bloquer environ 99,9 % des attaques automatisées par robot. Cela souligne à quel point l'AMF est essentielle à votre pile de sécurité, mais aussi à quel point elle est cruciale pour :

- Étendre le même niveau de sécurité à tous les terminaux : appareils d'entreprise et BYOD, utilisés en télétravail ou au bureau.
- Minimiser les menaces liées aux identifiants, notamment en empêchant l'accès non autorisé aux ressources protégées, même en cas de mot de passe compromis.
- Intégrer d'autres contrôles, fonctionnalités et services pour ajouter des couches supplémentaires de défense contre le paysage moderne des menaces.
- Réduire les risques liés à l'authentification en mettant en place des workflows sans mot de passe qui utilisent à la place au moins deux facteurs de vérification difficiles à contourner.
- Simplifier l'expérience de l'utilisateur lors de l'approvisionnement des appareils ou de l'accès aux ressources de l'entreprise en misant sur l'authentification unique (SSO) et la sécurité sans mot de passe, qui utilise simplement son appareil mobile.

4 Architecture Zero Trust

Lorsqu'on réfléchit au rôle essentiel que joue l'intégration de l'identité dans votre pile de sécurité, aucune discussion ne doit faire l'impasse sur l'accès réseau Zero Trust. Basé sur le principe de « confiance zéro », ce modèle applique une IAM de nouvelle génération pour réserver l'accès aux seuls utilisateurs de confiance munis d'appareils conformes. Dans tous les autres cas, l'accès est refusé par défaut.

Les menaces ont évolué avec le paysage informatique, qui a transformé les pratiques de travail en entreprise. Que l'on travaille au bureau ou à distance, sur un Mac ou un appareil mobile personnel ou d'entreprise, la productivité doit être préservée partout, à tout moment et sur n'importe quelle connexion réseau, en toute sécurité.

Tout comme les organisations doivent s'adapter aux environnements de travail hybrides, la sécurité doit évoluer pour que les appareils, les utilisateurs, les données et les connexions réseau sur lesquelles ils communiquent restent protégés malgré la multiplication des défis et des menaces. Rappelons en effet que le nombre de cyberattaques mondiales ciblant les appareils mobiles a augmenté de **147 %** entre décembre 2022 et 2023.

Le ZTNA contribue notamment à lutter contre les menaces qui ciblent les OS Mac et mobiles dans l'entreprise :

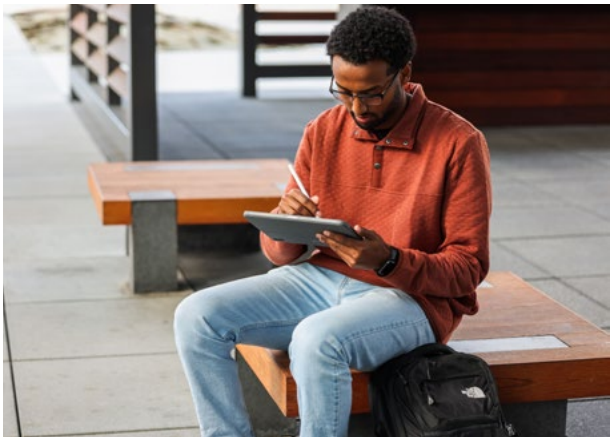
- Les appareils, les données et les ressources sont à la fois protégés et séparés. Chaque demande de ressource est refusée par défaut jusqu'à ce que l'intégrité de l'appareil ait été vérifiée. Cette approche sécurise les données en vérifiant que les identifiants n'ont pas été compromis et que l'appareil est bien conforme.

- L'infrastructure basée sur le cloud facilite l'intégration et l'extension homogène des mesures de défense à l'ensemble des parcs d'appareils mobiles et de postes de travail, sans avoir à gérer un équipement et des configurations complexes. La sécurité devient cohérente, quels que soient le système d'exploitation, le type d'appareil ou le modèle de propriété.

- Toutes les connexions réseau sont sécurisées à l'aide d'un micro-tunnelage qui isole chaque requête pour repousser les menaces basées sur le réseau, à commencer par les attaques de type Man-in-the-Middle. Cette technique applique le principe du moindre privilège, en accordant uniquement un accès chiffré aux ressources attribuées à l'utilisateur (contrairement aux solutions VPN traditionnelles qui fournissent un accès implicite à l'ensemble du réseau).

- Des règles d'accès contextuelles assurent la conformité aux règles de l'entreprise et aux réglementations ; elles accordent ou interdisent l'accès en fonction d'un certain nombre de critères, comme la présence de correctifs critiques sur l'OS et les applications.

- La protection constante garantit la sécurité des données de l'entreprise, tandis que le tunnelage partagé achemine intelligemment les données personnelles directement vers Internet. La protection privée des utilisateurs est respectée sans compromettre la sécurité, et inversement.



5 Évaluation des vulnérabilités

Au risque de donner l'impression d'exagérer son importance, l'évaluation des risques est absolument essentielle dans le domaine de l'informatique et de la sécurité de l'information. Tout d'abord, comment peut-on espérer assurer la sécurité de ce qu'on n'a pas encore découvert ? Partie intégrante d'un programme de gestion des vulnérabilités, le processus d'évaluation des risques et des vulnérabilités qui affectent votre organisation est une première étape cruciale pour la suite du processus. Elle informe et se nourrit de chaque processus et chaque workflow, dans chaque couche d'un plan complet de défense en profondeur.

Le processus de gestion des vulnérabilités se déroule en cinq étapes, mais nous allons nous concentrer sur les deux premières dans cette section :

1. Identification
2. Évaluation
3. Hiérarchisation
4. Résolution
5 Rapports

Nous avons expliqué l'importance de l'identification : on ne peut pas protéger ce que l'on ne connaît pas. Avec une solution MDM, ce processus commence par l'inventaire des appareils et de toutes les variables susceptibles d'avoir une incidence sur votre posture de sécurité. En voici quelques exemples classiques :

- Type d'appareil
- Version de l'OS
- Applications installées
- Configurations de durcissement
- Logiciel de sécurité des terminaux installé
- Modèle de propriété
- Utilisateurs affectés

L'étape suivante, l'évaluation, repose sur la capacité de votre solution de sécurité des terminaux à déterminer l'état de santé de chaque appareil en contact avec votre infrastructure. En combinant des analyses d'appareils, les données de connexion et l'inventaire transmis par votre solution MDM, les administrateurs peuvent comparer en temps réel l'état actuel des terminaux aux profils de référence afin d'identifier d'éventuelles lacunes de sécurité, par exemple :

- Les systèmes d'exploitation qui n'ont pas été mis à jour vers la dernière version
- Les applications installées qui présentent des vulnérabilités connues
- Les appareils dont les réglages de sécurité sont incomplets ou incorrects
- Les connexions réseau non sécurisées sur les appareils des utilisateurs distants

6. Détection et réponse des terminaux (EDR)

Une fois le risque identifié et évalué, il est temps de passer aux trois dernières étapes de la gestion des vulnérabilités. Il s'agit de convertir les données collectées et analysées en tâches concrètes pour atténuer les menaces avant qu'elles ne se propagent.

La troisième étape consiste donc à établir des priorités. Les administrateurs, éventuellement aidés de logiciels de sécurité des terminaux enrichis par intelligence artificielle (IA), trient les résultats en fonction des classifications de vulnérabilité et des facteurs de risque identifiés afin d'en déterminer l'impact sur l'entreprise.

À la quatrième étape, la résolution, les équipes du service informatique et de la sécurité déploient des workflows de correction pour corriger les vulnérabilités détectées au cours des étapes précédentes, en procédant par niveau de gravité décroissant.

Le dernier aspect du processus de gestion des vulnérabilités, mais qui est d'une importance capitale, est la création de rapports. Au cours de cette phase, les équipes :

- Documentent toutes leurs conclusions (elles décrivent ce qui s'est passé).
- Précisent les résultats positifs et négatifs (ce qui a fonctionné, ce qui a échoué).
- Fournissent du feedback pour éclairer les workflows actuels et futurs (notamment sur la cause profonde de l'échec d'une action ou les problèmes éventuellement rencontrés).
- Améliorent les processus en examinant les enseignements tirés de l'expérience (les points à garder en tête et à améliorer pour optimiser et faciliter les processus ou réduire le risque d'erreur).

Dans le cadre d'une stratégie de défense en profondeur, l'EDR soutient la performance des initiatives de cybersécurité en intégrant en toute sécurité un éventail de solutions pour :

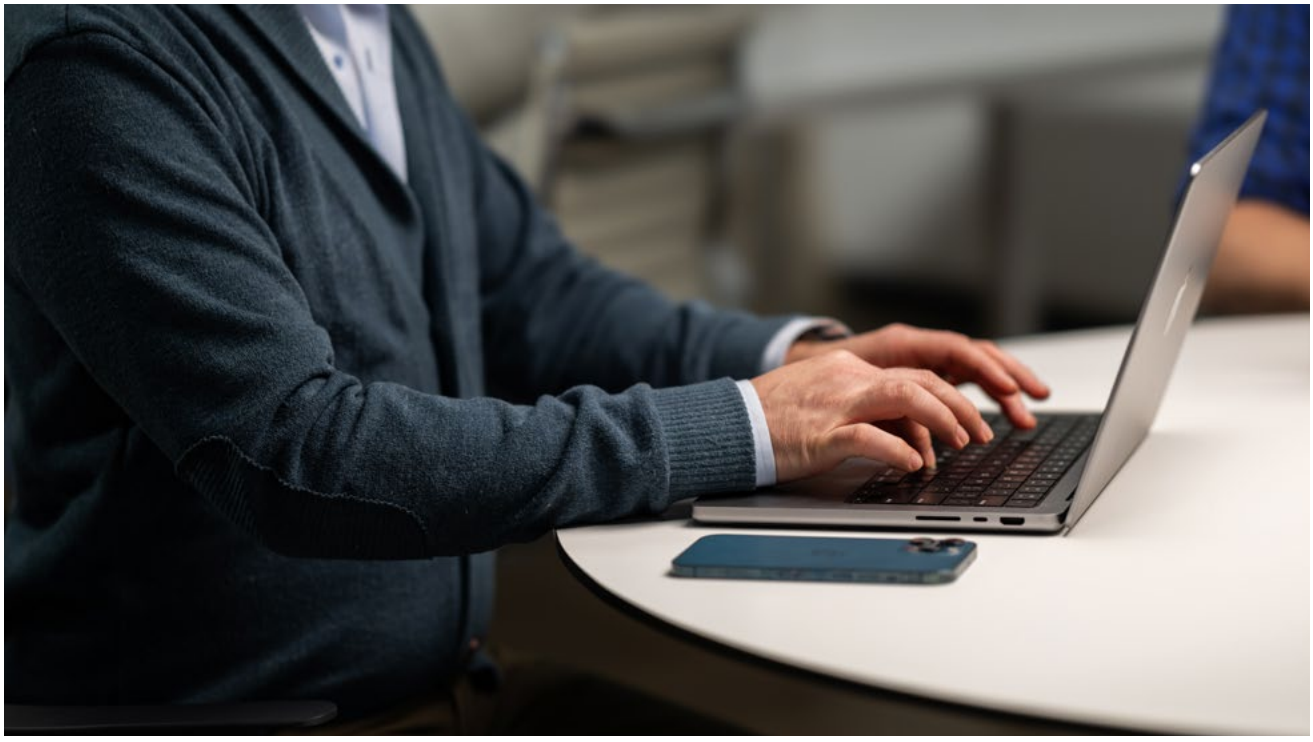
- Surveiller activement les terminaux afin de détecter les différents risques et alerter les équipes en cas de problèmes, comme la présence de logiciels malveillants ou un défaut de conformité.
- Analyser les données de télémétrie, manuellement ou avec l'aide de l'IA, pour identifier les menaces connues et inconnues.
- Automatiser la prévention des menaces ou mettre les appareils ciblés en quarantaine.
- Atténuer les menaces en assainissant les terminaux affectés et en déclenchant automatiquement des workflows de correction.
- Assurer une défense proactive contre les menaces, en s'appuyant sur le machine learning (ML) pour collecter et analyser rapidement les renseignements sur les menaces afin de soutenir la recherche des malveillances. Mais aussi réduire les délais d'intervention et guider les équipes dans le processus de réponse.

7. Renseignements sur les menaces enrichis par l'IA

Les solutions qui exploitent l'IA et le ML aident les équipes de toutes tailles, même sans spécialiste de l'informatique ou de la sécurité, à rassembler et analyser les données pour prendre des décisions informées plus rapidement que ne le permettent les processus manuels. Et ce gain de temps n'est que la partie émergée de l'iceberg si l'on pense au ROI de l'IA/ML et aux économies que ces technologies permettent de faire.

Selon IBM, « l'IA améliore ses connaissances pour “ comprendre” les menaces de cybersécurité et les cyberrisques en consommant des milliards de données ». Les avantages sont nombreux pour les organisations qui introduisent l'IA/ML dans leur plan de cybersécurité. Elles peuvent notamment :

- Collaborer avec les administrateurs pour obtenir les données utiles pour prendre des décisions éclairées au sujet des menaces, sur la base de renseignements personnalisés et adaptés à leur environnement.
- Surveiller, identifier, rechercher, vérifier et corriger les menaces inconnues 24 h/24, mais aussi développer des modèles de menaces reposant sur des données logiques et empiriques.
- Identifier et arrêter proactivement les menaces avant qu'elles ne s'aggravent, pour accroître le ROI de leur solution et éviter les dépenses liées aux conséquences des violations de données (et aux implications de conformité).
- Répondre plus rapidement aux incidents et accélérer les délais de résolution, en réduisant la fenêtre qui sépare la détection d'une menace de sa correction.
- Exploiter le ML et les workflows de sécurité automatisés pour libérer les équipes informatiques et de sécurité, qui auront alors la possibilité de développer de meilleures expériences technologiques pour aider leurs collègues à travailler mieux, pas plus.



8. Règles de conformité des appareils

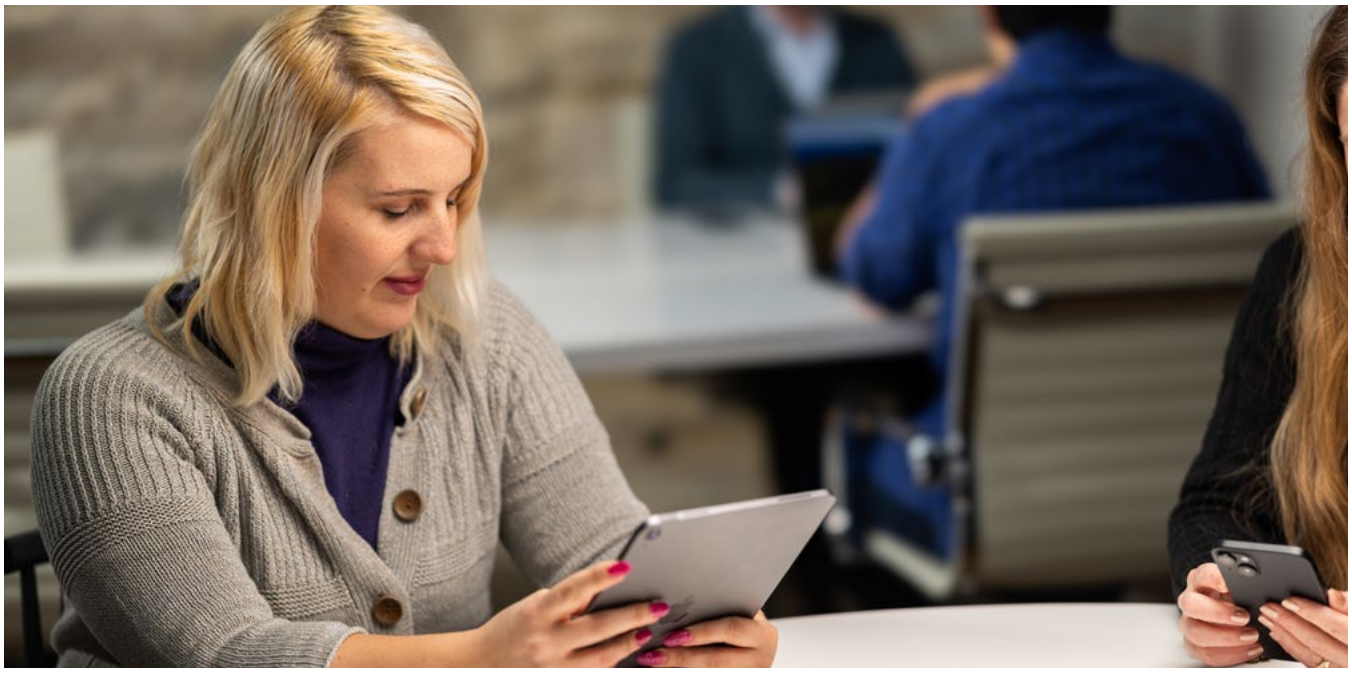
Un élément clé de la conformité consiste à configurer les appareils de manière à réduire la surface d'attaque du matériel et celle des logiciels qu'ils contiennent. Le concept de durcissement vise à « verrouiller » efficacement les terminaux en éliminant tout ce qui n'est pas indispensable aux utilisateurs pour accomplir les tâches qui leur incombent. Moins de code = moins de vecteurs de risque à exploiter.

Les cadres offrent aux organisations d'excellentes lignes directrices pour optimiser la sécurité des appareils, des données, des services, des processus et des workflows. Mais une fois les configurations définies, des facteurs externes – mises à jour, logiciels malveillants, nouvelles applications, comportement des utilisateurs, etc. – peuvent altérer les réglages et rendre les appareils non conformes.

La configuration des réglages n'est que la première moitié d'une stratégie de conformité. Il faut ensuite contrôler leur application, ce que permettent les règles définies dans votre solution de MDM, d'identité et de sécurité.

Les règles renforcent la posture de sécurité d'une organisation de plusieurs manières :

- Elles maintiennent les appareils en conformité avec les profils de référence et les exigences réglementaires du secteur.
- Elles veillent à ce que les appareils utilisent la version la plus récente de macOS et de leurs applications de productivité afin de prévenir les vulnérabilités connues.
- Elles demandent au fournisseur d'identité (IdP) et aux solutions de sécurité de vérifier les identifiants et l'intégrité des appareils chaque fois que les utilisateurs demandent l'accès à des ressources protégées, pour bloquer l'accès des comptes compromis et corriger les appareils qui ne répondent pas aux normes de sécurité de base.
- Elles garantissent une application homogène des normes de sécurité de l'organisation sur les appareils en BYOD en isolant les données et les applications sensibles dans un volume professionnel distinct au moment de l'inscription. Les données et les applications personnelles restent privées.
- Elles forcent le chiffrement de toutes les connexions filaires et sans fil lorsque des utilisateurs distants se connectent à des réseaux non fiables, afin de garantir la sécurité des données.



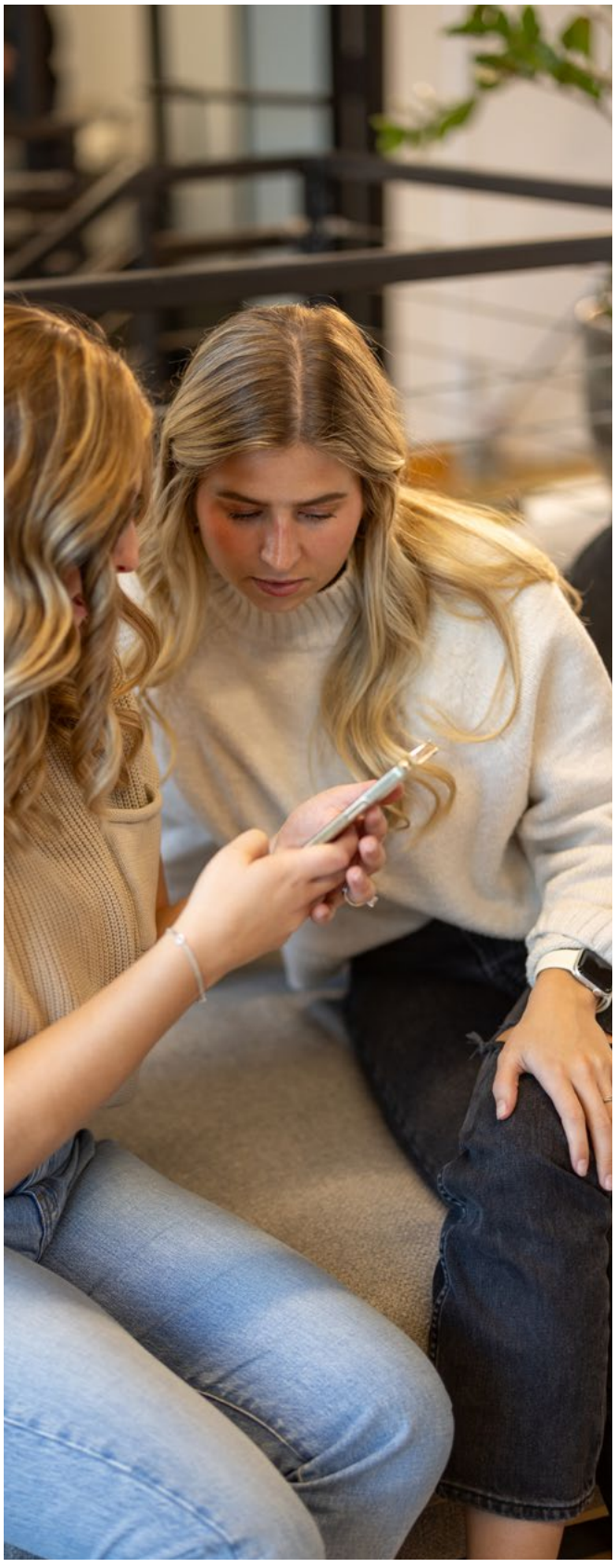
9. Formation et sensibilisation à la sécurité

Aucune stratégie globale de cybersécurité n'est complète sans un programme de sensibilisation à la sécurité pour les utilisateurs finaux.

Selon Forbes, « 93 % des organisations ont subi au moins deux violations liées à l'identité au cours de l'année écoulée. » Ce chiffre est à rapprocher des observations de Statista, qui a évalué le nombre de sites de phishing détectés dans le monde entier à 963 994 pour au 1er trimestre de 2024. Ces études renforcent notre conviction que les acteurs malveillants misent sur le manque de connaissances en sécurité des utilisateurs pour compromettre les identités afin d'étendre la portée d'une attaque.

L'objectif final de cybersécurité consiste à réduire le niveau de risque qui pèse sur votre entreprise pour le ramener au niveau de votre tolérance. Dans cette optique, la formation à la sécurité vient en appui de votre stratégie globale de sécurité pour :

- Tenir les utilisateurs informés des dernières menaces qui pèsent sur votre organisation.
- Faciliter l'identification des menaces courantes pour que les utilisateurs soient moins susceptibles de se laisser manipuler.
- Minimiser les erreurs en renforçant le maillon le plus faible de la chaîne de sécurité : l'homme.
- Autonomiser les utilisateurs pour qu'ils jouent leur rôle dans la protection des appareils et des données sensibles en limitant les fuites de données.
- Améliorer la conformité de manière globale en veillant à ce que les utilisateurs comprennent ce que l'on attend d'eux et en aidant les organisations à remplir les strictes obligations décrites dans leurs stratégies.



10. Plans de réponse aux incidents

Utilisées indépendamment les unes des autres, toutes ces bonnes pratiques donnent de bon résultats. Mais en combinant l'ensemble des contrôles, processus et workflows de sécurité, votre plan de sécurité devient une stratégie robuste et complète qui permet de neutraliser les menaces avant qu'elles ne puissent se concrétiser.

Mais que se passe-t-il si un appareil est compromis malgré tout ? Selon l'Institut national des normes et de la technologie (NIST), un plan solide de réponse aux incidents, intégré à votre stratégie de cybersécurité, est indispensable pour atténuer les menaces le plus rapidement possible.

Au niveau le plus simple, un plan de réponse aux incidents comporte quatre étapes :

1 Préparation

- Alignez les configurations matérielles et logicielles sur les références de sécurité afin de minimiser le risque de non-conformité (chiffrement des données).
- Intégrez des solutions MDM et de sécurité des terminaux pour simplifier l'évaluation des risques et uniformiser la gestion des vulnérabilités en vous appuyant sur un inventaire à jour (évaluation des vulnérabilités).

2 Détection et analyse

- Recueillez des données précises pour dresser un tableau complet de l'incident et de son déroulement (EDR).
- Réduisez le temps de collecte et d'analyse des données à quelques minutes (contre plusieurs jours ou semaines) en automatisant les tâches de sécurité répétitives grâce aux technologies de l'IA et du ML (renseignements sur les menaces enrichis par IA).

3 Confinement, élimination et rétablissement

- Minimisez les facteurs de risque et résolvez rapidement les incidents en orchestrant des workflows de correction grâce au partage sécurisé des données de télémétrie entre les solutions de MDM et de sécurité des terminaux (application des correctifs et des mises à jour).
- Exigez des facteurs d'authentification supplémentaires à titre de filet de sécurité numérique pour empêcher les acteurs malveillants de dérober des données en cas de compromission des identifiants (AMF).
- Assurez la sécurité et la productivité des utilisateurs sur n'importe quel appareil, qu'il soit personnel ou professionnel, et appliquez les mesures de sécurité de manière homogène à l'ensemble de votre infrastructure sur les appareils macOS, iOS/iPadOS, tvOS, watchOS, visionOS, Windows et iOS (architecture Zero Trust).

4 Activité post-incident

- Déployez des configurations de durcissement et gérez la conformité de façon simple et efficace à l'aide de workflows de gestion basés sur des règles (stratégies de conformité des appareils).
- Minimisez l'exposition aux menaces par des formations régulières de sensibilisation afin de donner aux utilisateurs les connaissances indispensables pour repérer les attaques courantes, à commencer par le phishing (formation et sensibilisation à la sécurité).

Conclusion

Vous savez bien qu'on n'attend pas de devoir récupérer des données après une catastrophe pour tester des plans de sauvegarde. C'est la même chose pour les plans de cybersécurité.

Votre PME utilise uniquement des appareils Apple ? Vous gérez un établissement scolaire qui a déployé des iPad individuels comme outil d'apprentissage sécurisé et respectueux de la vie privée ? Ou vous travaillez dans une grande entreprise du Fortune 500 comptant des milliers d'utilisateurs et d'appareils qui fonctionnent sous macOS/iOS, Windows et Android ? Dans tous les cas, il n'y a pas de meilleur moment pour prendre en charge les besoins de sécurité de votre organisation en misant sur une stratégie complète de défense en profondeur. Vous protégerez les utilisateurs et les données contre la multiplication des menaces sophistiquées et les pirates qui cherchent à voler les informations sensibles et confidentielles de votre organisation.

jamf

www.jamf.com/fr

Lancez-vous avec Jamf

ou contactez votre distributeur habituel pour commencer.