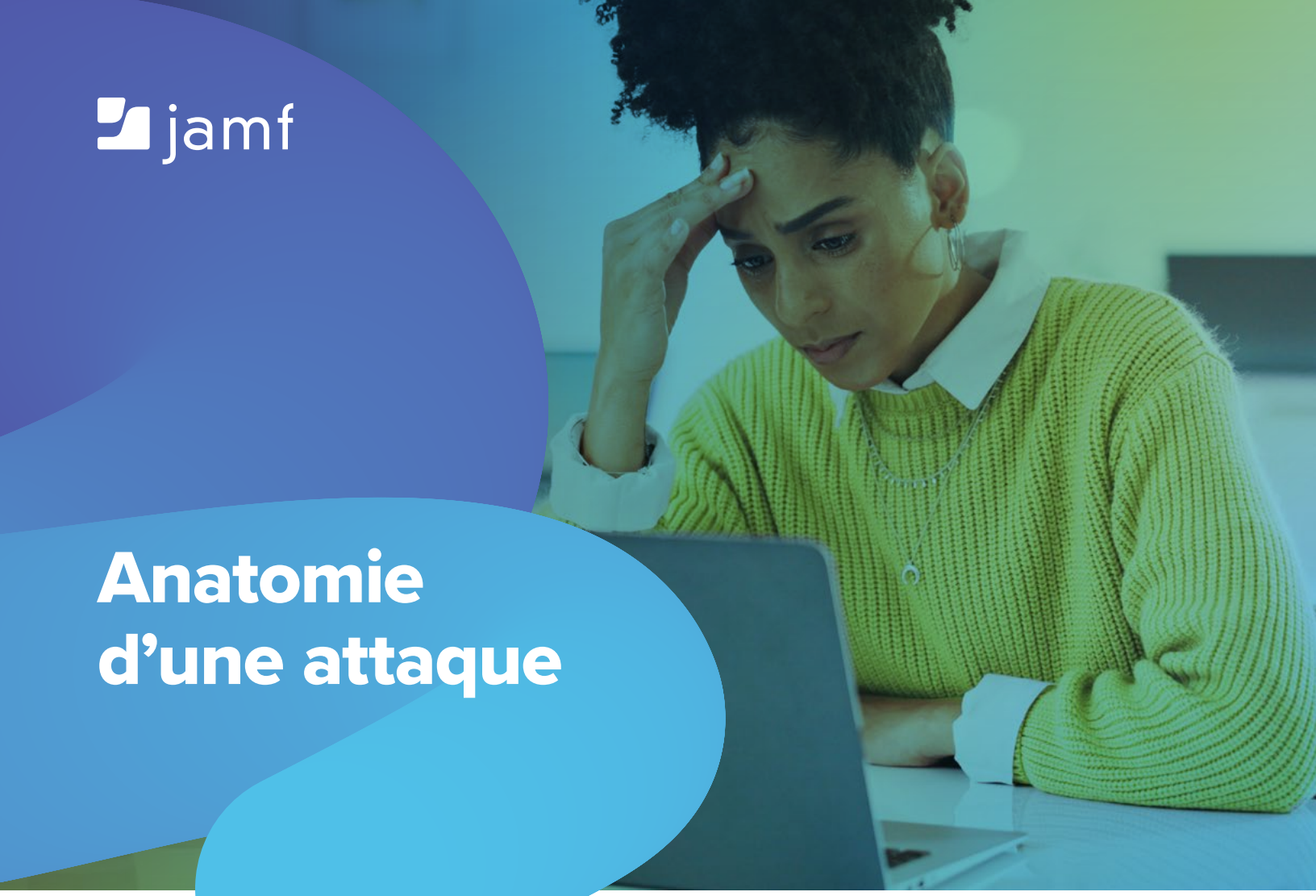


Anatomie d’une attaque

Dans le monde connecté d’aujourd’hui, les professionnels de la cybersécurité doivent constamment lutter contre les acteurs malveillants. Il leur suffit d’une vulnérabilité ou d’un jeu d’identifiants compromis pour infiltrer les réseaux de l’organisation. Pour vous, c’est tout l’inverse : tout doit être parfait à chaque fois, sans quoi vous risquez qu’un appareil non conforme ou des identifiants n’ouvrent la porte à une violation de données.

Comme le disait Thomas Jefferson, « le savoir, c’est le pouvoir ». Les pirates cherchent à connaître les failles des défenses d’une organisation, tandis que les professionnels de la cybersécurité veulent comprendre la nature des cyberattaques qui les visent.

Pour cela, il faut examiner chaque phase de la chaîne de cyberattaque pour en détailler l’anatomie. C’est comme cela que vous pourrez réduire les risques et renforcer les protections.

Dans cet article technique, nous allons :

- Décomposer la « cyber kill chain »
- Illustrer le fonctionnement d’une attaque
- Opposer des protections stratégiques aux enchaînements de l’attaque
- Rappeler l’importance de combler les failles de sécurité

Produire une vision claire de l'attaque

Les attaques varient parce que les pirates choisissent leurs techniques en fonction des cibles sélectionnées et des vulnérabilités qu'elles présentent. Si certains aspects sont similaires, l'individualité des attaques, combinée aux nombreuses variables qui influent sur la sécurité d'un terminal, fait de la cybersécurité un mélange d'art et de science.

Mais en dépit de cette variété, une certitude demeure : une attaque présente une succession d'étapes articulées en **cyber kill chain**, pour reprendre les termes de Lockheed Martin qui l'a théorisée. L'analyse de chaque phase permet aux professionnels de la cybersécurité d'identifier dans leur armure les failles que les pirates chercheront à cibler et exploiter.

> **« Voilà mes projets, Et voilà mes plans »**
>
> **– Tearsfor Fears**

Avant d'apprendre à lire la feuille de route d'un pirate, voyons les sept phases de la cyber kill chain :

1. **Reconnaissance :** recherche et identification de cibles en ligne et hors ligne.
2. **Armement :** les résultats de la recherche servent à mettre au point et/ou à acquérir les outils qui seront utilisés.
3. **Livraison :** des outils malveillants sont activement utilisés contre les cibles pour obtenir un accès.
4. **Exploitation :** une fois l'accès obtenu, les pirates cherchent à l'étendre en exploitant les vulnérabilités et les failles de sécurité.
5. **Installation :** le déploiement de code malveillant jette les bases de la réussite de la campagne.
6. **Commandement et contrôle :** un moyen de communication avec les dispositifs compromis est établi avant la phase finale de l'attaque.
7. **Passage à l'action :** une fois les préparatifs terminés, les pirates mettent en œuvre les outils pour atteindre leurs objectifs : collecte d'informations confidentielles, exfiltration de données, exécution d'un ransomware, etc.

C’est l’heure du spectacle !

Examinons de plus près chaque phase de la cyber kill chain. Dans cette section, nous prendrons pour exemple un logiciel malveillant « en tant que service » appelé **Atomic Stealer** (AMOS) et connu pour cibler macOS. Il nous servira à illustrer l’anatomie d’une attaque et son déroulement dans le monde réel.

1 Reconnaissance

Dans la phase de collecte de renseignements, les pirates se consacrent entièrement à faire des recherches sur leur cible pour mieux connaître son infrastructure, la topographie de son réseau et ses fournisseurs de services, en amont et en aval. La moindre information les aide à créer un profil de l’organisation ciblée. Il est important de noter que cette phase peut comprendre des activités de reconnaissance passive et active.

Reconnaissance active

Ces activités peuvent être détectées par les organisations : les outils invasifs laissent des empreintes numériques, comme un nombre excessif de tentatives de connexion infructueuses ou de prises d’empreintes numériques sur le réseau.

Reconnaissance passive

Essentiellement open source, cette activité vise à recueillir des informations de façon anonyme, sans prévenir la cible. En voici quelques exemples :

- Utilisation des réseaux sociaux pour cibler les victimes travaillant dans des secteurs de grande valeur comme la cryptographie
- Utilisation des réseaux sociaux pour identifier les personnes qui occupent des postes stratégiques au sein de l’organisation cible
- Recensement des partenaires et des fournisseurs pour identifier les services utilisés par la cible
- Utilisation de l’ingénierie sociale pour inciter des employés à divulguer des informations sensibles et utiles pour accroître les chances de réussite de l’attaque

2 Armement

Une fois la reconnaissance terminée, les pirates trient les informations recueillies et personnalisent les outils qui seront utilisés au cours des premières étapes de l’attaque. Dans notre exemple, ils ont accompli plusieurs opérations pour mettre en œuvre Atomic Stealer. Ils ont développé le logiciel malveillant et signé le DMG de manière ad hoc. Ils ont été jusqu’à fournir des instructions d’installation spécifiques pour indiquer aux utilisateurs comment contourner les avertissements Gatekeeper d’Apple. Ils ont créé un site web malveillant imitant celui du navigateur Arc et redirigé les visiteurs vers ce site pour qu’ils téléchargent la version compromise du logiciel.

REMARQUE : Au cours des phases 1 et 2, les solutions de sécurité ne sont pas particulièrement efficaces pour arrêter cyber kill chain, car rien n’est confirmé avant la phase 3. Nous ne sommes pas dans Minority Report : aux stades 1 et 2, il n’y a pas d’attaques. Tout est encore à l’état d’idées d’hypothèses dans la tête d’un acteur malveillant. C’est à partir de la troisième phase que la cybercriminalité commence. Il faut attendre qu’il passe à l’action pour l’arrêter.

3 Livraison

Au cours de cette phase, les pirates mettent leurs recherches et leurs tactiques en application.

ÉTAPE 1. Mise en ligne du site web contrefait

ÉTAPE 2. Diffusion du site via des publicités sponsorisées qui le présentent comme le site légitime du navigateur Arc

ÉTAPE 3. L’utilisateur télécharge et exécute le logiciel qui infecte son terminal avec le logiciel malveillant Atomic Stealer

Les publicités sponsorisées ont un rayon d'action très vaste et se positionnent en tête des recherches des utilisateurs. Cette campagne peut donc infecter des dizaines de terminaux en un temps relativement court. Cette attaque ne se lance pas automatiquement lorsqu'on visite le site web, et cette technique permet d'échapper à la détection. Comme l'indique Jamf Threat Labs, les attaques utilisant des variantes d'Atomic Stealer prolifèrent rapidement quand les pirates utilisent le phishing par e-mail, par SMS et via les réseaux sociaux pour atteindre un plus grand nombre de victimes.

Des solutions comme **Jamf Pro** et **Jamf Protect** fonctionnent en tandem pour protéger les utilisateurs contre ce type de menaces. Jamf Pro utilise des filtres de contenu pour bloquer les URL de phishing, même si les utilisateurs cliquent sur le lien malveillant. La sécurité des terminaux surveille activement l'état des appareils et alerte les administrateurs en cas de changement de l'état de conformité. Les profils d'inscription à la gestion des appareils sécurisent les données en stockant les données professionnelles sur un volume séparé et chiffré, isolé des données personnelles. Si des données d'entreprise sont compromises, les administrateurs peuvent déclencher automatiquement des workflows de correction et même effacer les données sensibles de l'appareil pour empêcher toute divulgation.

4 Exploitation

La méthode de livraison de la charge utile peut varier mais, comme l'indiquent les recherches approfondies de Jamf Threat Labs, *« l'objectif et la logique restent les mêmes en fin de compte. »* Autrement dit, il s'agit de compromettre les identifiants de l'utilisateur et d'exfiltrer les données sensibles.

C'est précisément la fonction d'Atomic Stealer : voler les données de l'utilisateur après l'avoir incité à saisir ses identifiants, en dissimulant un appel AppleScript basé sur la commande « osascript » native de macOS derrière un processus de mise à jour automatique.

Certes, les actions effectuées en arrière-plan par ce logiciel malveillant sont largement documentées par **Jamf Threat Labs** (et vous les retrouverez plus loin dans la section Passage à l'action). Mais de nombreuses variantes et évolutions de ce code malveillant sont régulièrement détectées, et elles permettent aux pirates d'effectuer un certain nombre d'opérations à l'insu de l'utilisateur. Ils peuvent notamment l'espionner en contournant le **cadre de transparence, de consentement et de contrôle d'Apple.**

Même si les pirates parviennent à compromettre les identifiants d'un utilisateur au cours de la campagne de phishing, Jamf Trusted Access va s'efforcer d'arrêter les phases suivantes de la cyber kill chain. Pour ce faire, la solution collecte des données télémétriques riches en temps réel et informe les administrateurs en cas de changement dans l'état de santé de l'appareil. Elle va également déclencher des workflows de correction automatiques, par exemple en déployant des mises à jour pour corriger les vulnérabilités et mettre un terme à la phase d'exploitation.

Quant aux identifiants compromis, **Jamf Connect** gère les identités et les accès, ce qui permet de désactiver les comptes touchés jusqu'à ce que l'incident soit circonscrit. Pour accélérer **la réponse à l'incident et le rétablissement,** l'intégration avec Jamf Protect permet de mettre en place l'**accès réseau zero-trust** (ZTNA). Cette approche minimise automatiquement les risques en détectant l'utilisation d'identifiants compromis pour accéder à d'autres applications et services. Cette méthode isole les menaces sur les services touchés et empêche les mouvements latéraux au sein de votre infrastructure. Surtout, elle permet aux utilisateurs de continuer d'utiliser les services non touchés. Enfin, des vérifications matérielles et logicielles sont effectuées à chaque demande. Cette couche de protection supplémentaire empêche que des appareils ou des identifiants compromis accèdent aux ressources de l'entreprise, en attendant que des workflows automatiques les remettent en conformité.

5 Installation

Les pirates continuent de déployer du code malveillant pour acquérir une persistance. Ils conservent ainsi leur accès aux systèmes compromis tout en cherchant à se propager par déplacement latéral dans le réseau. Ils vont ainsi pouvoir compromettre d'autres dispositifs en exploitant des outils personnalisés et natifs, comme des utilitaires de ligne de commande et des portes dérobées. L'objectif d'Atomic Stealer est simplement de voler toutes les informations de l'utilisateur en une seule fois sans laisser de traces, et n'agit donc que peu à ce stade. Mais dans d'autres types d'attaques, cette phase permet généralement de préparer ou mener des opérations furtives.

Il est essentiel de se défendre contre cette phase **en s'appuyant sur la visibilité et la sécurité**. C'est en détectant, en prévenant et en corrigeant les menaces connues qu'on pourra garantir la conformité. La surveillance active de l'état des appareils alerte les administrateurs en cas de changement dans la posture de sécurité d'un appareil. Une fois triées, ces alertes permettent d'initier des workflows de réponse aux incidents. Jamf Protect empêche l'exécution de logiciels malveillants connus, notamment en les mettant en quarantaine et en les supprimant avant qu'ils ne s'exécutent. Dans le cas des menaces inconnues, les journaux des appareils sont transmis à une solution SIEM tierce afin d'aider les **équipes de recherche des menaces** à détecter et à supprimer celles qui se cachent dans les systèmes pour collecter des données.

6. Commande et contrôle (C2)

L'objectif d'Atomic Stealer est avant tout de voler vos identifiants puis de les utiliser pour dérober vos données. Mais pour d'autres pirates, la course ne s'arrête pas là. Le Trousseau Apple est un dépôt d'identifiants central et sécurisé, qui peut donner aux attaquants les clés d'un éventail de fonctions, logiciels et services. C'est donc une cible tentante pour quiconque veut :

- Obtenir un large accès à de vastes ressources de données
- Étendre une attaque par des mouvements latéraux
- Gagner de l'argent en vendant les données et/ou en escroquant les victimes

En clair : plus les données sont nombreuses, plus le potentiel de gain est important.

Il faut impérativement empêcher toute communication avec des appareils compromis. Le ZTNA surveille les terminaux et bloque les connexions aux services malveillants tels que les serveurs C2 pour empêcher les attaquants de communiquer avec les appareils compromis. Le ZTNA exerce également une surveillance continue de la santé des appareils et des informations d'identification pour détecter les défauts de conformité. Sur cette base, il peut empêcher l'accès d'appareils et d'identifiants non conformes ou compromis aux ressources protégées. Grâce à l'intégration de Jamf Pro, il peut aussi exécuter automatiquement des workflows pour corriger les appareils vulnérables et compromis.

7. Passage à l'action

Au cours de cette phase finale, les attaquants mettent leur projet à exécution, quel qu'il soit :

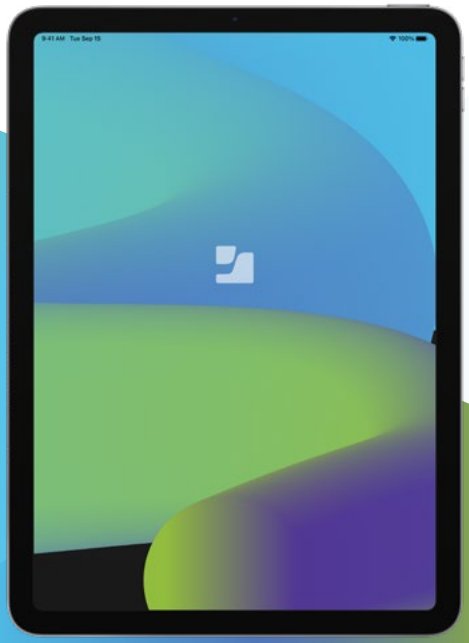
- **Espionnage**
- Exfiltration de données
- Extorsion
- Attaques contre la chaîne d'approvisionnement
- Cyberterrorisme

Voire une combinaison de plusieurs objectifs. Cette phase est difficile à quantifier : de même que chaque organisation a des besoins uniques, les actions d'un pirate dépendent de ses objectifs propres. Dans le cas d'Atomic Stealer, la commande osascript mentionnée précédemment imite l'apparence et les interactions d'une alerte système légitime, mais elle utilise les identifiants de l'utilisateur pour collecter des données confidentielles dans le trousseau d'Apple :

- Noms d'utilisateur et mots de passe
- Cookies de session du navigateur
- Données sensibles de l'utilisateur
- Coordonnées de carte de paiement
- Portefeuilles de cryptomonnaie
- Métadonnées du système

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

– Chris Triolo, HP



Comblez les failles de votre armure

Des protections inadéquates, souvent conçues pour les systèmes d'exploitation des ordinateurs de bureau, présentent des lacunes néfastes pour les appareils mobiles. Ceux-ci deviennent alors une porte pour les pirates qui veulent infiltrer les réseaux d'une entreprise.

Les appareils mobiles sont loin d'être le seul risque de violation de données. Néanmoins, les menaces continuent de les cibler en raison de leur ubiquité sur le lieu de travail et de l'utilisation croissante d'appareils personnels pour accéder aux données professionnelles. Une **étude de Jamf Threat Labs** a chiffré ce risque : « 40 % des utilisateurs mobiles utilisent un appareil qui présente des vulnérabilités connues. » Grâce aux failles non corrigées des appareils vulnérables, les acteurs malveillants peuvent :

- Exécuter du code malveillant sur les appareils
- Contourner les protections de sécurité internes
- Accéder à des données d'entreprises sans autorisation
- Obtenir des données personnelles sans autorisation
- Espionner les utilisateurs à leur insu
- Pivoter à partir de l'appareil infecté pour compromettre les réseaux
- Exfiltrer des données personnelles et professionnelles, ainsi que des informations confidentielles

Apple est connu pour allier forme et fonction, pour marier style et pertinence. Cette philosophie s'applique à une caractéristique cruciale de la conception : la sécurité et la protection de la vie privée. Les systèmes d'exploitation macOS et iOS intègrent nativement plusieurs protections qui protègent les appareils, les utilisateurs et leurs données contre une myriade de menaces, tant au niveau matériel que logiciel.

Les pirates font évoluer leurs techniques. Ils imaginent de nouvelles menaces et créent des variantes de logiciels malveillants émergents, comme la famille des Infostealers. Les protections de sécurité qui reposent uniquement sur la détection de signatures statiques ne permettent plus de se défendre contre les menaces sophistiquées. Certaines d'entre elles, comme Atomic Stealer, affichent « des chaînes de développement complètement différentes, qui n'ont rien à voir avec une version principale suivie de mises à jour, » selon Dark Reading. On comprend alors pourquoi les **menaces sophistiquées échappent aux protections intégrées** et mettent en danger les appareils, les utilisateurs et les données.

Intégrer de manière holistique **la gestion, l'identité et la sécurité en une seule solution.** Les faire collaborer dans le réseau et sur l'appareil pour bloquer complètement le trafic malveillant. Enfin, prévenir l'exfiltration des données d'entreprise pour les mettre à l'abri des pirates. Le ZTNA pilote ce workflow en empêchant l'accès aux services protégés de l'entreprise, en détectant automatiquement les identifiants compromis et en les désactivant pour minimiser les risques. Les données télémétriques sont partagées à grande échelle en toute sécurité pour permettre l'automatisation de workflows d'atténuation des risques jusqu'à ce que les vulnérabilités soient corrigées. L'accès aux ressources demandées n'est autorisé qu'une fois le terminal certifié conforme.

Avec un plan de sécurité basé sur un **cadre de défense en profondeur** mature, les organisations ont toutes les cartes en main pour réduire les risques, prévenir les attaques connues et répondre rapidement aux incidents. Les workflows de correction automatisés rétablissent la conformité des terminaux.

En intégrant et en superposant les solutions, les entreprises opposent aux menaces sophistiquées des protections complètes et multicouches qui « capturent et atténuent » les risques. Ces couches de protection s'appliquent à l'ensemble de l'entreprise et constituent une base de défense pour tous les types d'appareils et de systèmes d'exploitation qui ont besoin d'accéder aux ressources et aux données de l'entreprise.

Selon un récent rapport **Frost Radar : Sécurité des terminaux 2023**, le cabinet Frost & Sullivan a souligné que Jamf était un leader de la sécurité des terminaux en raison des capacités de défense en profondeur de nos solutions :

- Détection en temps réel des applications et des scripts malveillants, et recommandation d'actions aux utilisateurs.
- Gestion cohérente des vulnérabilités, prévention des menaces et contrôle des règles.
- Rapports de sécurité sur toutes les plateformes Mac et mobiles, dont macOS, iOS/iPadOS et Android. Une protection supplémentaire contre les menaces web qui couvre toutes ces plateformes, mais aussi Windows et les Chromebooks.
- Un cadre de configuration et d'audit élargi pour aider ses clients à respecter des normes de conformité complexes.
- Des données télémétriques enrichies sur les terminaux, exportables dans des outils tiers de collecte et d'analyse des journaux.
- Une application cohérente des règles et protège aussi bien les appareils d'entreprise que les appareils personnels.
- Jamf Trusted Access est la seule solution spécifiquement conçue pour les appareils Apple qui combine la gestion des appareils, la gestion des identités et des accès, et la sécurité des terminaux.

Conclusion

Tant que des pirates cibleront les appareils, les utilisateurs et les données, il faudra mettre en place des contrôles de sécurité pour minimiser les risques et empêcher de graves violations de données.

Pour être pérenne, un plan de sécurité doit être itératif et inclure plusieurs éléments clés :

- Ayez une connaissance des risques et des niveaux de tolérance.
- Mettez en œuvre des couches de contrôle, d'atténuation des risques et de prévention des menaces.
- Intégrez les solutions de gestion des appareils, des identités et des accès, et de sécurité des points finaux pour qu'elles fonctionnent en coordination.
- Faites converger les équipes informatiques et de sécurité, pour éliminer les silos, favoriser la communication et accélérer la réponse aux incidents.
- Misez sur des workflows d'automatisation pour remédier rapidement aux menaces tout en minimisant les erreurs commises par l'utilisateur.
- Alignez les besoins et les exigences de l'entreprise sur des normes et des cadres afin de renforcer les contrôles de sécurité et maintenir la conformité.
- Mettez en place une équipe d'intervention d'urgence pour accélérer la réponse aux incidents. S'il n'est pas possible de mettre en place une équipe dédiée, pensez à nouer un partenariat avec une équipe de professionnels de confiance, comme Jamf Threat Labs, pour appuyer la recherche des menaces inconnues.

Associez-vous à **Jamf, un leader de la gestion et de la sécurité des appareils Apple**. Appuyez-vous sur une **expertise spécialisée** en matière de sécurité, comme celle du Jamf Threat Labs, pour combler les lacunes de votre sécurité. Votre partenaire vous aider à mettre en place des workflows automatisés pour renforcer votre posture de sécurité contre les menaces sophistiquées et protéger vos données sensibles en sécurisant chaque appareil. Quel que soit le type d'appareil ou de système d'exploitation, sa localisation ou son type de connexion réseau, **Jamf aide votre entreprise à réussir avec Apple au travail**.