jamf

Défense contre les menaces mobiles

une introduction

C’est incontestable : la plateforme Apple est, par défaut, l’une des plus sécurisées et robustes du marché. Mais cette plateforme est une cible en pleine expansion pour les pirates informatiques. C’est pourquoi les organisations doivent s’armer pour repousser les menaces actuelles et à venir.

Phishing, logiciels malveillants, applications vulnérables… De nombreuses attaques sont couramment utilisées pour exploiter les appareils et accéder aux ressources d’entreprise et aux données sensibles, notamment pour :

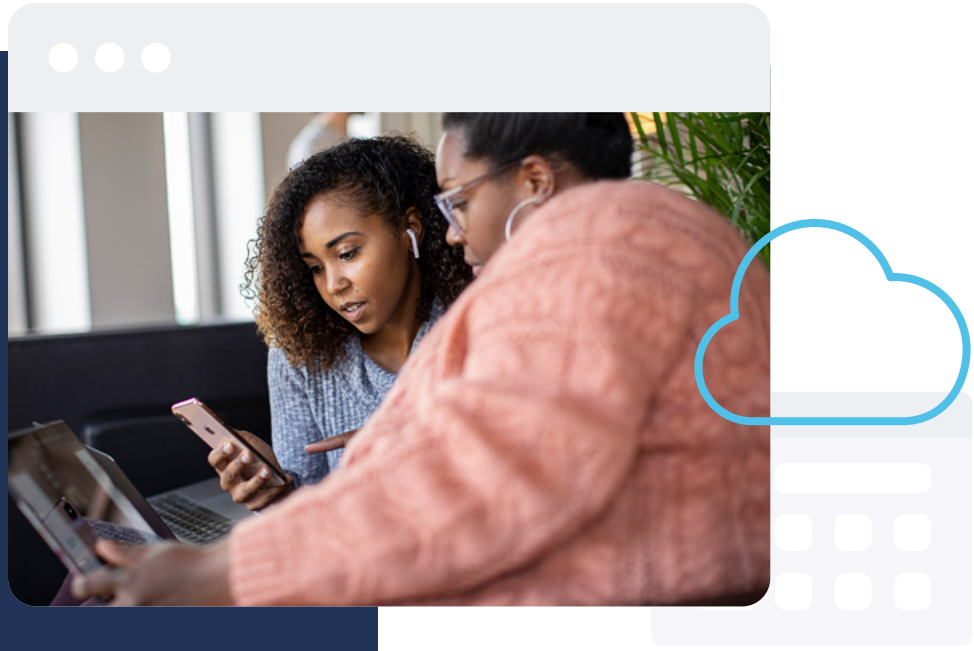
- Exfiltrer des informations confidentielles
- Obtenir l’accès aux services d’entreprise
- Collecter des données concernant la vie privée des utilisateurs
- Intercepter les communications réseau

Jamf sécurise vos terminaux mobiles grâce à la détection des menaces et à la prévention des vulnérabilités zero-day et les logiciels malveillants. Avec l’augmentation du nombre d’attaques ciblant des appareils mobiles, c’est un enjeu majeur pour les organisations, en particulier celles qui ont adopté des environnements à distance ou hybrides.

CE GUIDE ABORDE LA PROBLÉMATIQUE SOUS PLUSIEURS ANGLES :

1. Détection et prévention complètes des menaces
2. Protections fortes pour chaque cas d'utilisation
3. Capacités de signalement en temps réel
4. Contrôles des règles et accès conditionnel
5. Gestion unifiée des opérations

APPLE EST UNE CIBLE EN PLEINE EXPANSION POUR LES PIRATES...

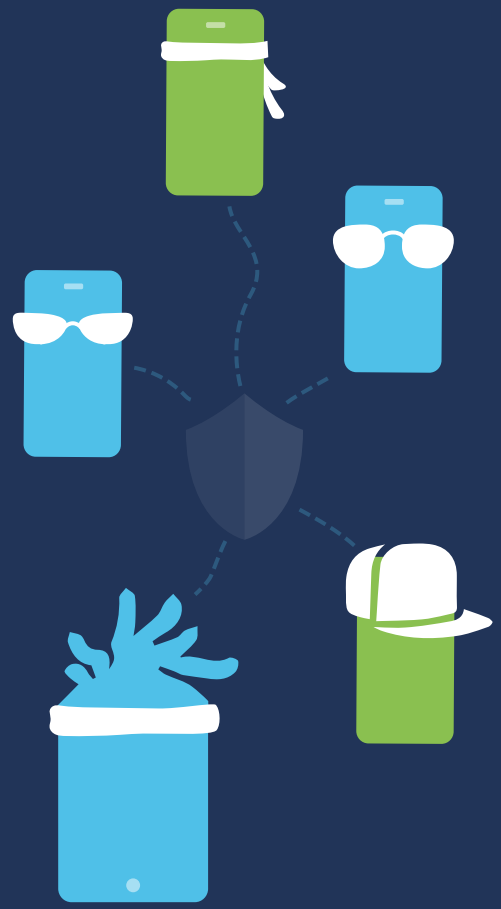


... ET ILS NE FONT PAS DE DISCRIMINATION.

C'est là qu'intervient **Jamf Protect**, la solution spécialement conçue pour protéger les appareils mobiles et vos utilisateurs contre les menaces. Légère, avec une faible empreinte réseau, elle exerce un impact minimal sur les performances de l'appareil et l'expérience de l'utilisateur final.

Les organisations qui déploient des appareils macOS auprès de leurs utilisateurs font confiance à Jamf Protect pour assurer la protection des terminaux. Elles protègent ainsi leur parc informatique des menaces de sécurité et des logiciels malveillants, tout en collectant des informations sur l'état des appareils. Et pour les appareils mobiles sous iOS, iPadOS ou Android ? Existe-t-il une solution de sécurité des terminaux capable de répondre à leurs besoins spécifiques, mais aussi de s'intégrer à **Jamf Pro** pour offrir une solution de gestion exhaustive ?

« PROTÉGEZ VOS ARRIÈRES »



Il est essentiel de « protéger ses arrières ». Protéger ses arrières, c'est protéger ses ressources sensibles. Dans ce guide, les ressources sensibles sont les appareils mobiles. C'est par leur intermédiaire que les pirates vont tenter d'accéder aux données sensibles.

D'après le Rapport sur la sécurité du Cloud 2021, **41 % des organisations** ont connu des incidents liés à des logiciels malveillants sur des appareils distants : c'est non seulement un chiffre saisissant, mais aussi une augmentation considérable par rapport à l'année précédente.
Lisez notre rapport Security 360 pour en savoir plus sur les tendances et les risques en matière de sécurité de cette année.

Pour ceux qui se demandent ce qui se cache derrière cette flambée des incidents, la réponse est à la fois simple et complexe. Suite à l'adoption massive du télétravail, le périmètre réseau a volé en éclats, et les utilisateurs utilisent des appareils mobiles pour rester productifs lorsqu'ils ne sont pas au bureau. Voilà pour l'explication simple. Mais pour les organisations, la tâche est complexe : elles doivent transformer leur infrastructure pour protéger les appareils et sécuriser les données, quel que soit le lieu de travail.

Pour minimiser la complexité, Jamf a choisi une approche basée sur le Cloud et combine des technologies de sécurité puissantes et avancées avec une flexibilité et une évolutivité extrêmes. Elle réunit des capacités de surveillance, de détection et de rapports pour donner aux équipes informatiques et de sécurité les moyens de surveiller l'état de santé de l'ensemble de leur flotte.

PROTECTION RÉSEAU

Le phishing n'est qu'une des nombreuses menaces auxquelles les entreprises modernes sont confrontées, mais il reste sans conteste la plus grande, car il cible le maillon faible de la chaîne de sécurité : l'utilisateur. Même si les utilisateurs sont formés et bien intentionnés, la marge d'erreur reste trop importante. Le taux de réussite des tentatives de compromission demeure assez élevé pour que les pirates continuent à cibler les utilisateurs.

Grâce à la protection intégrée au réseau, vous pouvez bloquer activement les menaces zero-day, sites web de phishing inclus, en temps réel. Les appareils restent protégés des effets de ces campagnes qui n'ont pas le temps de déclencher une attaque d'exploitation. En empêchant l'appareil d'accéder à ces domaines malveillants sur tous les types de connexion (filaire, Wi-Fi ou mobile), les organisations protègent leurs utilisateurs et leurs terminaux.

CAPACITÉS ÉTENDUES

Jamf Protect est conçu dès le départ dans une optique d'extension, grâce à un framework d'API. Jamf Protect s'intègre à plus de produits UEM (gestion unifiée des terminaux) et SIEM (gestion des informations et des événements de sécurité) que toute autre solution de sécurité. Les équipes informatiques et de sécurité peuvent ainsi maximiser leur arsenal actuel d'appliances, d'applications et de services de gestion et de sécurité, en profitant en plus d'informations sur les menaces, de workflows de correction et de possibilités d'automatisation.

Un excellent exemple d'intégration consiste à exploiter à la fois l'API de risque Jamf et les fonctionnalités de Jamf Protect pour mettre en place une communication inégalée. Les données sont ensuite échangées par les deux systèmes en temps réel, ce qui permet de créer des rapports personnalisés et de corriger toute anomalie dans l'intégrité des appareils mobiles de votre organisation.

VÉRIFICATION DES ACCÈS

Jamf Protect lutte sans cesse contre les innombrables attaques de cybersécurité qui envahissent le paysage mobile et ne montrent aucun signe de ralentissement.

Les attaques liées aux accès sont extrêmement efficaces et ce, pour une bonne raison : si un appareil est compromis et qu'il n'y a pas de signe visible de menace pour l'utilisateur (si l'appareil fonctionne toujours normalement, autrement dit), celui-ci a toujours accès aux ressources. L'appareil traitera la demande, l'accès sera accordé, et la ressource devient ainsi potentiellement vulnérable.

Jamf vous protège de ces attaques et élève votre posture de sécurité en autorisant uniquement les connexions sécurisées et les appareils fiables à accéder aux ressources de l'organisation. Comment ?

En surveillant continuellement les données de télémétrie et les informations contextuelles propres à chaque appareil afin de détecter des anomalies.

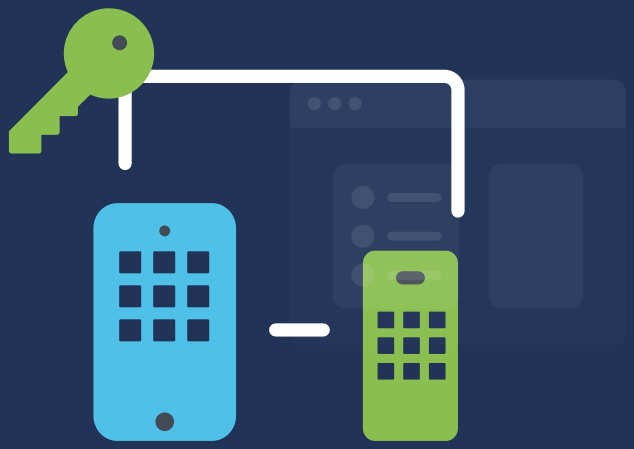
S'il s'avère que le terminal présente un risque élevé ou semble compromis, l'accès aux ressources est suspendu grâce à l'application de règles personnalisées.

MACHINE LEARNING AVANCÉ

Après cet aperçu de ce que Jamf peut faire pour protéger votre entreprise et votre flotte mobile, nous allons maintenant explorer plus en détail les fondements du logiciel. Vous aurez ainsi une vision plus précise de la manière dont il protège les appareils des menaces. Plutôt que ses fonctionnalités à proprement parler, nous allons voir les technologies de défense centrale qui les sous-tendent.

Permettez-moi de vous présenter MI:RIAM. Ce moteur d'intelligence artificielle avancé travaille en temps réel pour identifier le plus large éventail de menaces connues et de type zero-day. MI:RIAM collecte des informations provenant de 425 millions de capteurs dans le monde entier – c'est le plus grand ensemble de données sur les menaces. Ces données alimentent ses algorithmes, et des opérations sophistiquées de science des données délivrent des informations en temps réel sur les menaces et les risques en cours.

POUR TOUS LES APPAREILS



Votre flotte n'est composée que d'appareils iOS et iPadOS ? C'est parfait. Jamf Protect offre exactement les protections nécessaires pour assurer la sécurité de vos appareils Apple et de votre base d'utilisateurs face aux menaces actuelles et émergentes.

Vous avez également d'autres appareils dans votre parc mobile ? C'est parfait aussi ! Jamf sécurise les systèmes d'exploitation Android et Windows et en fait tout autant pour renforcer tous vos appareils mobiles. Jamf permet aux organisations de prendre en charge plusieurs modèles de propriété. La sécurité reste assurée, que les appareils appartiennent à l'entreprise ou aux employés dans le cadre d'un programme BYOD.

Les utilisateurs tiennent à savoir qu'ils sont protégés. Quant aux membres de votre équipe informatique ou de sécurité, ils veulent savoir comment s'exerce cette protection. Et les acteurs malveillants ? Eux doivent en savoir le moins possible pour maintenir la posture de sécurité de votre réseau et assurer la protection des données. Plusieurs types d'informations doivent être sécurisées à tout prix pour maintenir leur intégrité. De leur côté, les équipes informatiques et de sécurité doivent recevoir les données les plus récentes sur l'état des terminaux de l'entreprise.

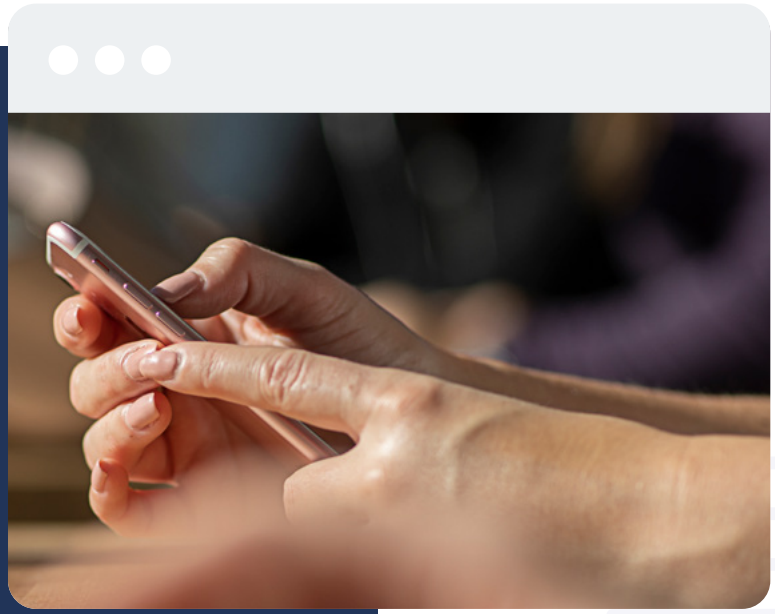
CONFIDENTIALITÉ DES UTILISATEURS

Les informations d'identification personnelle, renseignements médicaux personnels en tête, font partie des types de données les plus convoitées par les acteurs malveillants. C'est un cercle vicieux : plus ils collectent d'informations, plus ils ont d'outils pour lancer de nouvelles attaques.

Heureusement, Jamf protège la confidentialité en ligne en chiffrant les communications et en intégrant des fonctionnalités anti-phishing. Cela s'applique non seulement aux données personnelles de vos utilisateurs, mais aussi à celles qui doivent être traitées conformément à des réglementations de conformité. Les fonctions avancées de confidentialité et les contrôles empêchent l'accès d'utilisateurs ou d'appareils à risque aux ressources et aux données de l'entreprise.

INFORMATIONS EN TEMPS RÉEL

Les équipes informatiques et de sécurité peuvent obtenir des rapports détaillés sur la santé de leurs terminaux, en utilisant les modèle types fournis ou en les personnalisant pour répondre aux besoins spécifiques de l'organisation. Grâce à la personnalisation des rapports permise par Jamf Protect, les administrateurs disposent de données en temps réel dans la console. Ils peuvent également les exporter vers un SIEM partenaire via la fonctionnalité d'intégration pour les visualiser dans des tableaux de bord. Avec l'API, ils pourront intégrer Jamf Protect à une solution de gestion unifiée, comme Jamf Pro, pour échanger des données. Ces communications permettront d'automatiser la gestion des appareils et la correction des problèmes détectés sur les terminaux.



Il existe tellement de manières de protéger les données, les appareils et les utilisateurs, que nous ne pouvons même pas toutes les traiter dans cet e-book. La prochaine étape :

Profitez d’un essai gratuit pour en savoir plus. Vous pouvez également contacter avec votre revendeur habituel pour découvrir toutes les possibilités de Jamf.

jamf

Demander une version d'essai

Nous sommes impatients que vous commenciez.