jamf

La protection contre les menaces sur mobile

Une introduction

C’est incontestable, Apple a créé l’une des plateformes sécurisées prêtes à l’emploi les plus robustes du marché. Cependant, cette plateforme est une cible en pleine expansion pour les pirates informatiques. C’est pourquoi les organisations doivent disposer des armes leur permettant de repousser les menaces actuelles et à venir.

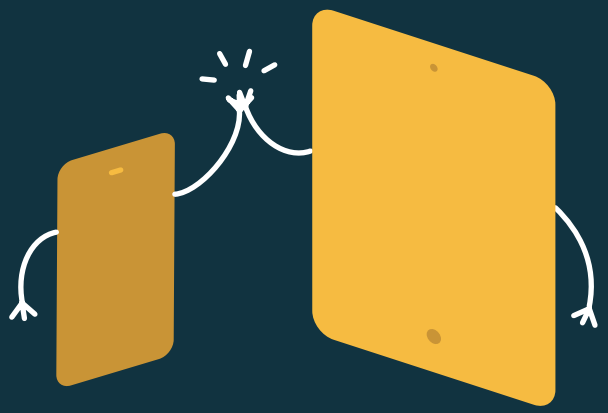
Les campagnes d’attaques courantes telles que le phishing, les logiciels malveillants et les applications vulnérables sont utilisées pour exploiter les appareils et accéder aux ressources d’entreprise et aux données sensibles, notamment pour :

- 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 Threat Defense protège vos terminaux mobiles contre les attaques grâce à la détection des menaces et à la prévention du phishing de type zero-day et des logiciels malveillants. Il s’agit là de l’une des principales problématiques des organisations, en particulier de celles qui ont adopté des environnements à distance ou hybrides, étant donné l’augmentation du nombre d’attaques ciblant des appareils mobiles.

DANS CE GUIDE, NOUS ALLONS ABORDER LES SUJETS SUIVANTS :

- Détection et prévention complètes des menaces
- Protections fortes pour tous les cas d’utilisation
- Capacités de rapports en temps réel
- Contrôles des règles et accès conditionnel
- Gestion unifiée des opérations



APPLE EST UNE CIBLE EN PLEINE EXPANSION POUR LES PIRATES, QUI NE FONT AUCUNE DISCRIMINATION.

Les organisations qui déploient des appareils macOS auprès de leurs utilisateurs font confiance à Jamf Protect pour assurer la protection des terminaux afin de préserver leur parc informatique des menaces de sécurité, de bloquer les logiciels malveillants et de fournir des informations sur l'état des appareils. Mais qu'en est-il des appareils mobiles, tels que ceux basés sur iOS et iPadOS ? Quelle sécurité des terminaux est disponible pour les appareils mobiles ? Existe-t-il un système de sécurité qui répond à leurs besoins spécifiques et qui s'intègre également à Jamf Pro pour offrir une solution de gestion exhaustive ?

Oui, c'est **Jamf Threat Defense**, la solution spécialement conçue pour protéger les appareils mobiles Apple et vos utilisateurs des menaces, tout en conservant une empreinte réduite avec un impact minime sur les performances des appareils et sur l'expérience de l'utilisateur final.

« PROTÉGER SES 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 à distance : c'est non seulement un chiffre saisissant, mais aussi une augmentation considérable par rapport à l'année précédente.

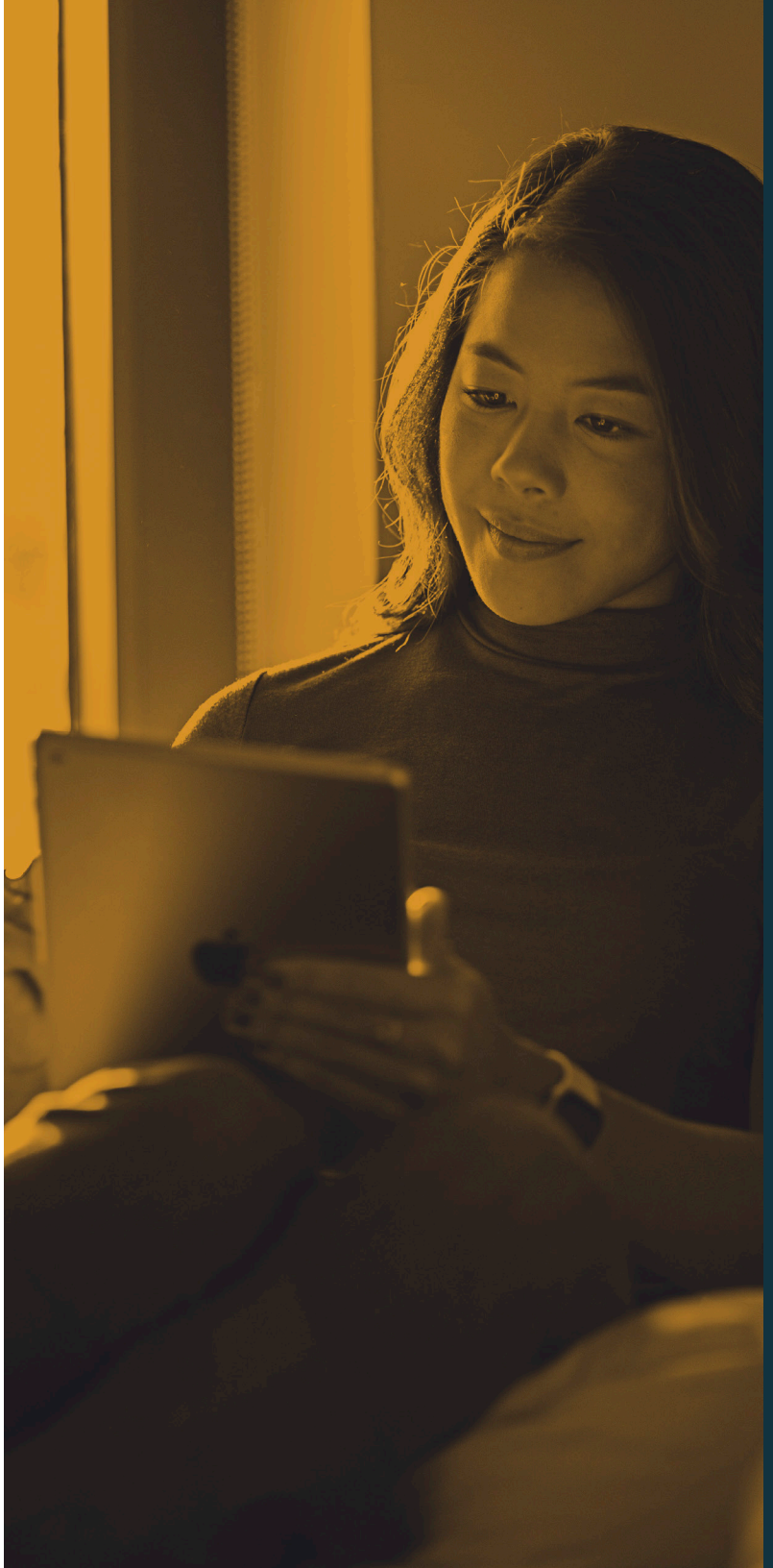
Pour ceux qui s'interrogent sur ce qui se cache derrière cette flambée des incidents, la réponse est à la fois simple et complexe. Suite à la transition vers des environnements de travail à distance ou hybrides, le périmètre réseau a volé en éclats, et les utilisateurs ont recours à des appareils mobiles pour rester productifs en télétravaillant. C'est la partie simple. La partie complexe, c'est la façon dont les organisations ont transformé leur infrastructure pour assurer la protection des appareils et la sécurité des données.

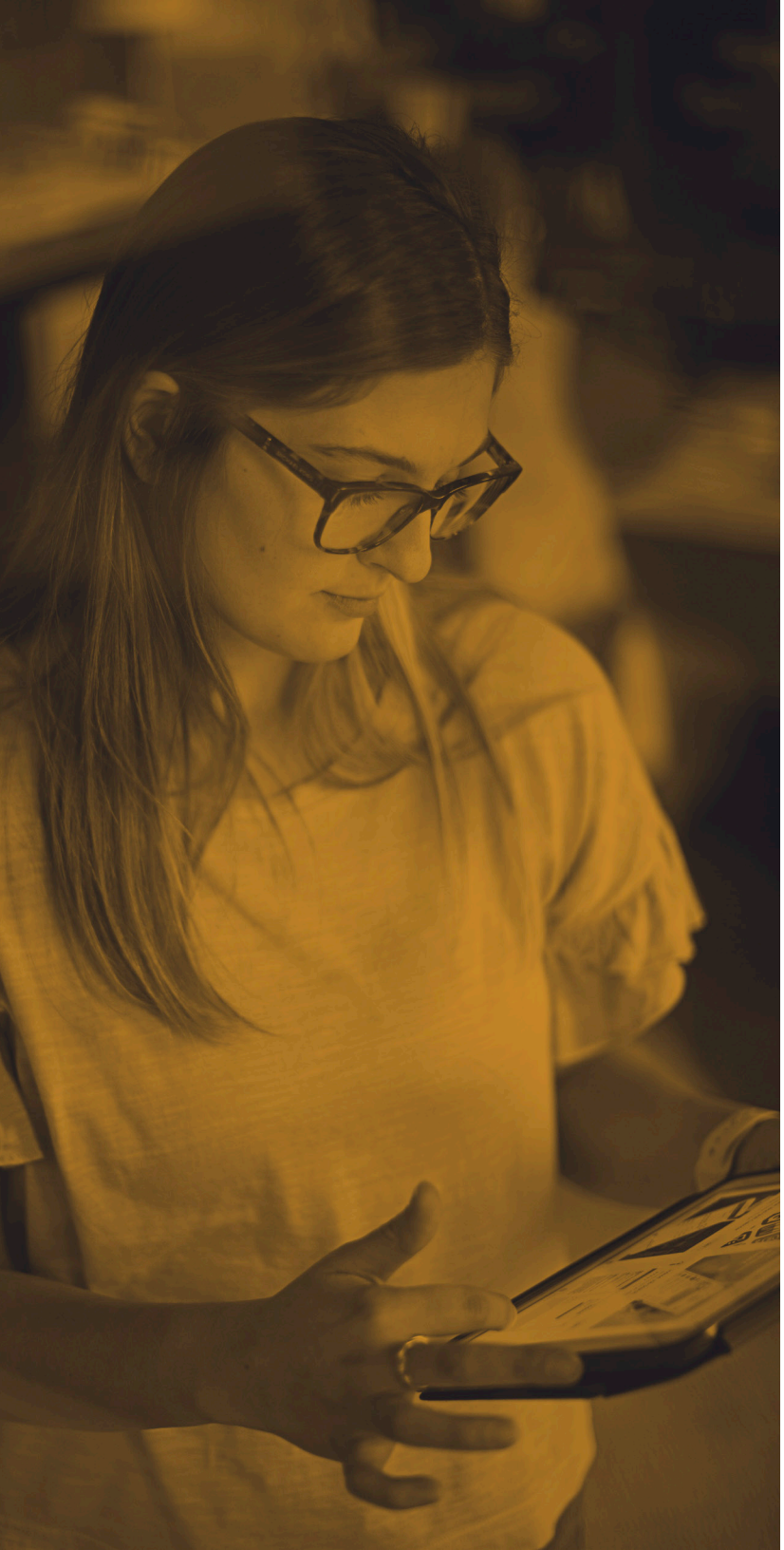
Minimisant la complexité, Jamf Threat Defense est une approche basée sur le Cloud, qui combine des technologies de sécurité puissantes et avancées avec une flexibilité et une évolutivité extrêmes. La solution inclut des capacités de surveillance, de détection et de rapports, qui permettent aux équipes informatiques et de sécurité de surveiller l'état de santé de l'ensemble de leur parc informatique.

PROTECTION RÉSEAU

Le phishing n’est que l’une des 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, ce qui implique que les risques de compromission des systèmes sont élevés, et que les pirates continueront donc à cibler les utilisateurs.

En fournissant une protection sur le réseau, Jamf Threat Defense bloque activement les menaces zero-day telles que les sites de phishing en temps réel. Ainsi, les appareils sont protégés des effets de ces campagnes avant que toute attaque soit déclenchée, car ils ne peuvent pas accéder aux domaines malveillants, quel que soit le type de communication : filaire, Wi-Fi ou cellulaire.





CAPACITÉS ÉTENDUES

L'extension des fonctionnalités est conçue par défaut dans Jamf Threat Defense grâce à l'intégration avec un framework d'API de fournisseur. Jamf Threat Defense peut se targuer d'offrir plus de partenariats de gestion unifiée des terminaux (UEM) et d'information et de gestion des événements sécuritaires (SIEM) que les autres solutions de sécurité. Les équipes informatiques et de sécurité peuvent ainsi maximiser l'investissement existant dans les équipements, applications et services de sécurité et de gestion des appareils, afin de profiter d'informations sur les menaces, de workflows de correction et de l'automatisation.

Un exemple parfait d'intégration est l'utilisation conjointe de l'API de Jamf avec les fonctionnalités de Jamf Threat Defense, pour permettre une communication sans précédent entre les deux plateformes logicielles. Ainsi, les données sont partagées entre les systèmes en temps réel, ce qui permet d'obtenir des rapports d'état personnalisés et d'apporter des corrections sur les terminaux iOS de votre organisation.

ACCÈS ADAPTÉ

L'une des principales raisons expliquant l'efficacité des attaques liées aux accès est que, si un appareil est compromis et qu'il n'y a pas d'indicateur visible de la menace pour l'utilisateur (c'est-à-dire, si l'appareil fonctionne toujours normalement), celui-ci aura toujours accès aux ressources. L'appareil traitera la demande et l'accès sera accordé, ce qui risque de compromettre également la ressource.

Jamf Threat Defense contre 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 saisies contextuelles propres à chaque appareil afin de détecter des anomalies. Si le terminal présente un risque élevé ou semble compromis, l'accès aux ressources sera interdit, grâce à l'application de règles personnalisées.

Après avoir découvert comment Jamf Threat Defense peut protéger votre entreprise et votre parc d'appareils mobiles, nous allons maintenant explorer plus en détail les fondements du logiciel pour vous donner une vision plus précise de la manière dont il opère pour protéger les appareils des menaces. Nous n'allons pas aborder les fonctionnalités à proprement parler, mais plutôt certaines des technologies de défense centrale intégrées à la base des fonctionnalités mentionnées auparavant.

Jamf Threat Defense s'efforce de contrer les nombreuses attaques de cybersécurité qui envahissent le paysage de la sécurité sur mobile et dont la progression ne montre aucun signe de ralentissement.

MACHINE LEARNING AVANCÉ

Laissez-nous vous présenter : MI:RIAM. Ce n'est pas le successeur de Siri, mais un moteur d'intelligence avancé qui travaille en temps réel pour identifier le plus large éventail de menaces connues et de menaces de type zero-day. En utilisant le plus grand ensemble de données sur les menaces, MI:RIAM collecte des informations provenant de 425 millions de capteurs dans le monde entier afin d'alimenter ses algorithmes, en utilisant des sciences de données avancées pour fournir des informations en temps réel sur les menaces et les risques en cours.

POUR TOUS LES APPAREILS

Votre parc informatique ne comporte que des appareils iOS et iPadOS ? C'est parfait. Jamf Threat Defense a exactement le type de protections nécessaires pour assurer la sécurité de vos appareils Apple et de votre base d'utilisateurs face aux menaces actuelles et émergentes.

Vous avez d'autres types d'OS dans votre parc d'appareils mobiles ? C'est très bien aussi ! Jamf Threat Defense prend en charge les systèmes d'exploitation des appareils hors Apple, et permet là aussi de protéger vos appareils mobiles contre les menaces, d'assurer la sécurité de vos données et de maintenir la productivité des utilisateurs. Et enfin, de nombreux modèles de propriété sont compatibles, que les appareils soient détenus par la société ou que l'organisation propose un programme du type BYOD (Bring Your Own Device), CYOD, COPE ou COBO, afin d'offrir une flexibilité maximale sans transiger sur la sécurité.

PROTÉGEZ VOS DONNÉES

En tant qu'utilisateur, vous voulez savoir que vous êtes protégé. En tant que membre du service informatique, vous voulez savoir comment vos utilisateurs sont protégés. Mais vous avez aussi besoin que les acteurs malveillants en sachent 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 l'intégrité du système. Les équipes informatiques et de sécurité doivent être informées de l'état des terminaux de leur entreprise et savoir quelles stratégies de correction sont déployées pour assurer une sécurité maximale.

CONFIDENTIALITÉ DE L'UTILISATEUR

Les informations d'identification personnelle, dont les renseignements médicaux personnels, font partie des types de données les plus convoitées par les acteurs malveillants. C'est un cercle vicieux : plus ils collectent d'informations et plus ils sont à même de poursuivre leurs attaques. Heureusement, Jamf Threat Defense protège la confidentialité en ligne grâce à des communications chiffrées et à des fonctionnalités anti-phishing. Cela s'applique non seulement aux données personnelles de vos utilisateurs, mais aussi aux informations sensibles qui doivent être traitées conformément à des réglementations de conformité. Les fonctionnalités avancées de confidentialité et de contrôle des règles appliquent l'accès conditionnel zero trust et interdisent l'accès aux utilisateurs ou appareils à risque.

INFORMATIONS EN TEMPS RÉEL

Les équipes informatiques et de sécurité peuvent obtenir des rapports détaillés sur la santé de leurs terminaux à l'aide des fonctionnalités de rapports par défaut incluses, ou les personnaliser pour répondre aux besoins spécifiques de l'organisation. La personnalisation des fonctionnalités de rapports de Jamf Threat Defense permet aux administrateurs de disposer de données en temps réel dans la console, ou de les exporter vers un partenaire SIEM via la fonctionnalité d'intégration, pour les visualiser dans des tableaux de bord. Ils peuvent également choisir d'utiliser l'API pour s'associer à une solution de gestion unifiée, comme Jamf Pro, pour transmettre les données entre les logiciels, afin de permettre une gestion automatisée des appareils et une correction des problèmes détectés sur les terminaux.

Il existe énormément de possibilités pour protéger les données, les appareils et les utilisateurs, tellement que nous ne pouvons même pas toutes les traiter dans cet e-book. Voici donc votre prochaine étape :

Demandez une version d'essai

Découvrez par vous-même une version gratuite de Jamf.
Vous pouvez également contacter votre revendeur Apple habituel pour découvrir tout ce qui est possible avec Jamf.

Quel que soit votre choix, nous sommes ravis que vous puissiez découvrir Jamf.