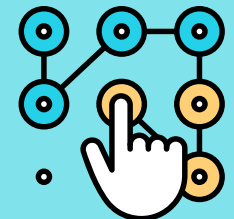
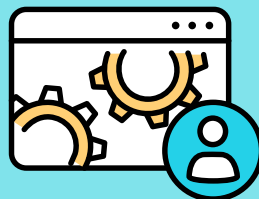


# La protection des terminaux sur Mac

une introduction



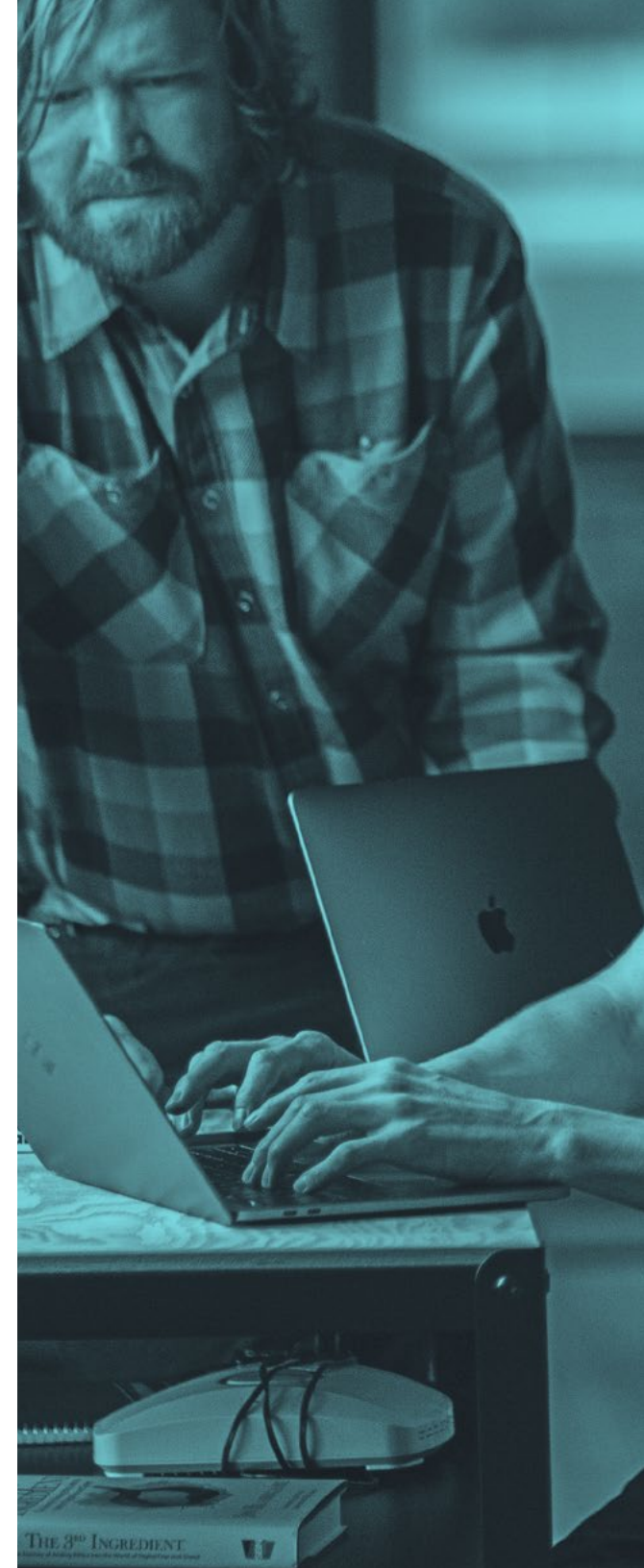
Sans aucun doute, le Mac est l'appareil le plus sûr sur le marché dans sa configuration de base, et ce depuis plusieurs décennies. Quand les organisations réfléchissent à la composition de leur flotte, elles ne peuvent pas oublier les solutions de sécurité qui sont essentielles pour protéger les données, les appareils et les utilisateurs.

La complaisance peut conduire à des violations préjudiciables et au coût élevé. Avec une solution de protection des terminaux faite pour Mac, les équipes informatiques et de sécurité peuvent non seulement se protéger contre les

menaces connues, mais aussi continuer de s'adapter et anticiper les besoins futurs de leur organisation en terme de sécurité.

Que vous soyez une grande société travaillant avec une flotte Apple ou une petite entreprise gérant une poignée de Mac, Jamf vous offre une protection des terminaux au-delà de ce qu'Apple fournit avec ses fonctionnalités natives.

Dans cet e-book, nous expliquons ce que la protection des terminaux Mac implique et pourquoi une protection conçue pour plusieurs systèmes d'exploitation est insuffisante.



---

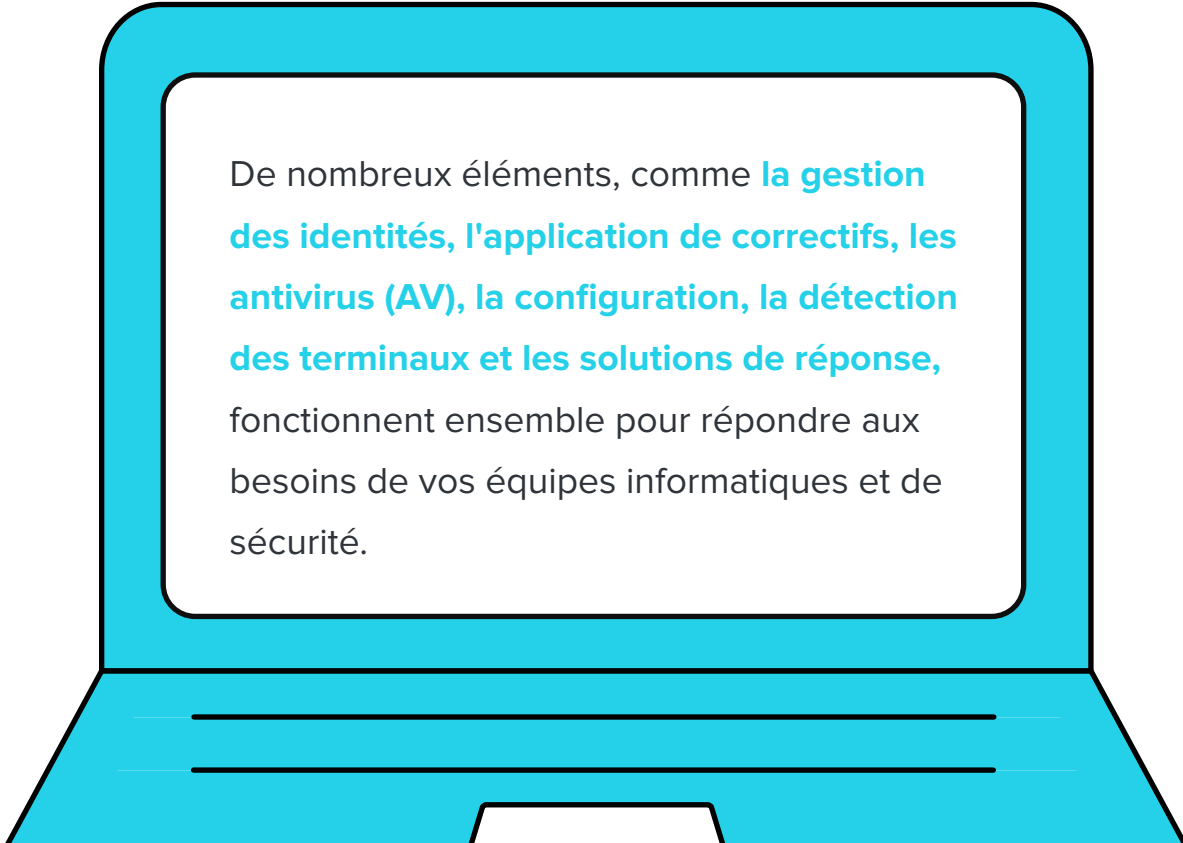
# Protection des terminaux sur Mac

Étendez la sécurité native d'Apple et soyez prêts pour l'inconnu

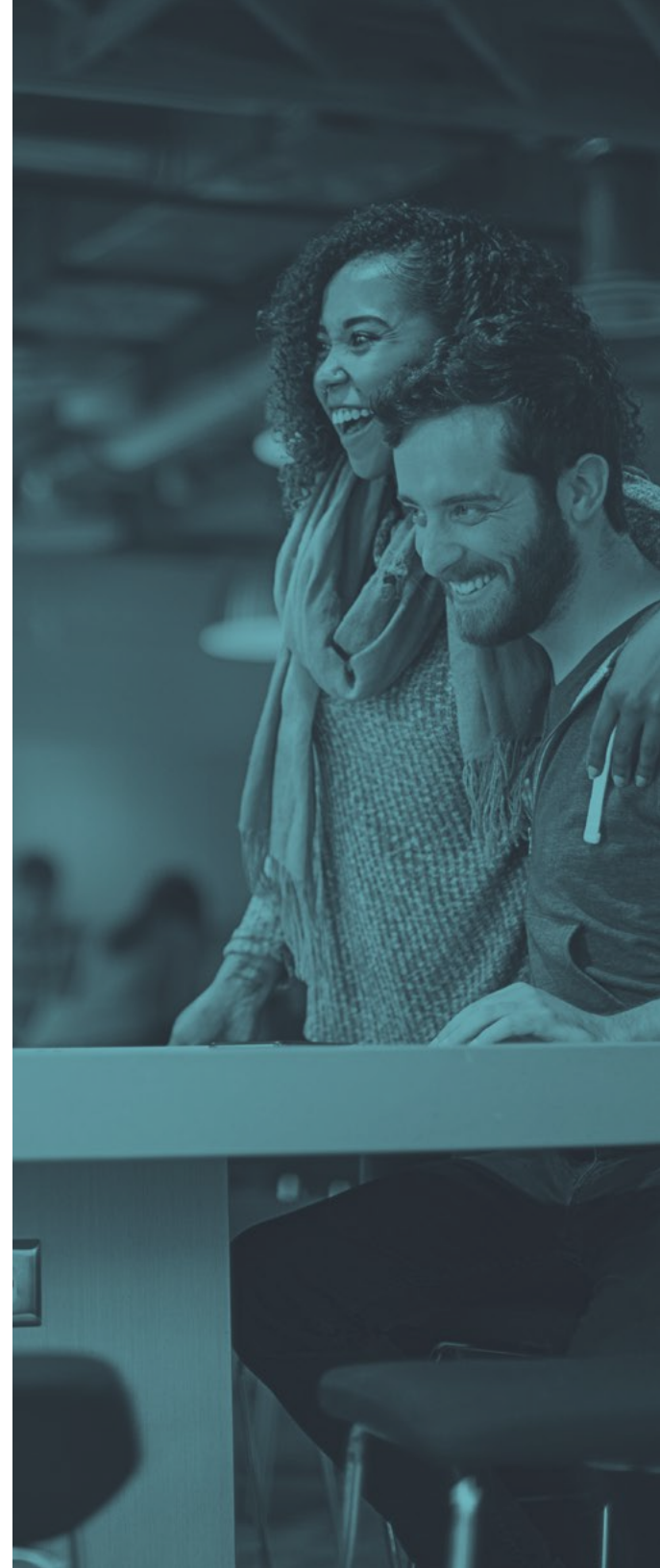


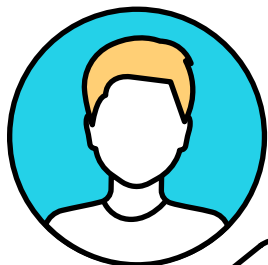
Alors que Mac est de plus en plus choisi par les grandes sociétés, les petites entreprises, les écoles et les organismes de santé, il est devenu crucial de veiller à ce que les appareils et les données soient utilisés à des fins légitimes par les utilisateurs autorisés.

**C'est là que la protection des terminaux Mac entre en jeu.**



De nombreux éléments, comme **la gestion des identités, l'application de correctifs, les antivirus (AV), la configuration, la détection des terminaux et les solutions de réponse**, fonctionnent ensemble pour répondre aux besoins de vos équipes informatiques et de sécurité.





## GESTION DES IDENTITÉS

Les mesures de sécurité mises en œuvre par la gestion des identités affectent à la fois les utilisateurs finaux et les équipes informatiques tout au long du cycle de vie des employés, qu'ils travaillent sur place ou à distance. Les applications VPN et SaaS et la connexion des employés aux ressources de l'entreprise représentent autant d'occasions de renforcer votre protection des terminaux.

Les employés sont de plus en plus mobile et travaillent de partout sur différents appareils. Les organisations doivent donc être en mesure de gérer et de sécuriser les appareils et les informations de l'entreprise sans les difficultés qui accompagnent la liaison à une instance Active Directory locale. Jamf Connect prend en charge les utilisateurs dès le moment où ils déballent leur Mac et l'allument. Ils peuvent accéder aux applications, ressources et données de l'entreprise avec un ensemble unique d'informations d'identification cloud.

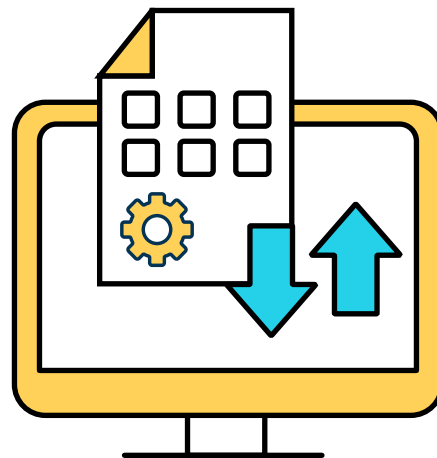
Avec Jamf Connect, les organisations peuvent surveiller l'identité et l'accès, et bénéficier d'une hiérarchisation cohérente de la sécurité des appareils et des données. Le tout avec un impact minimal sur l'expérience de l'utilisateur final



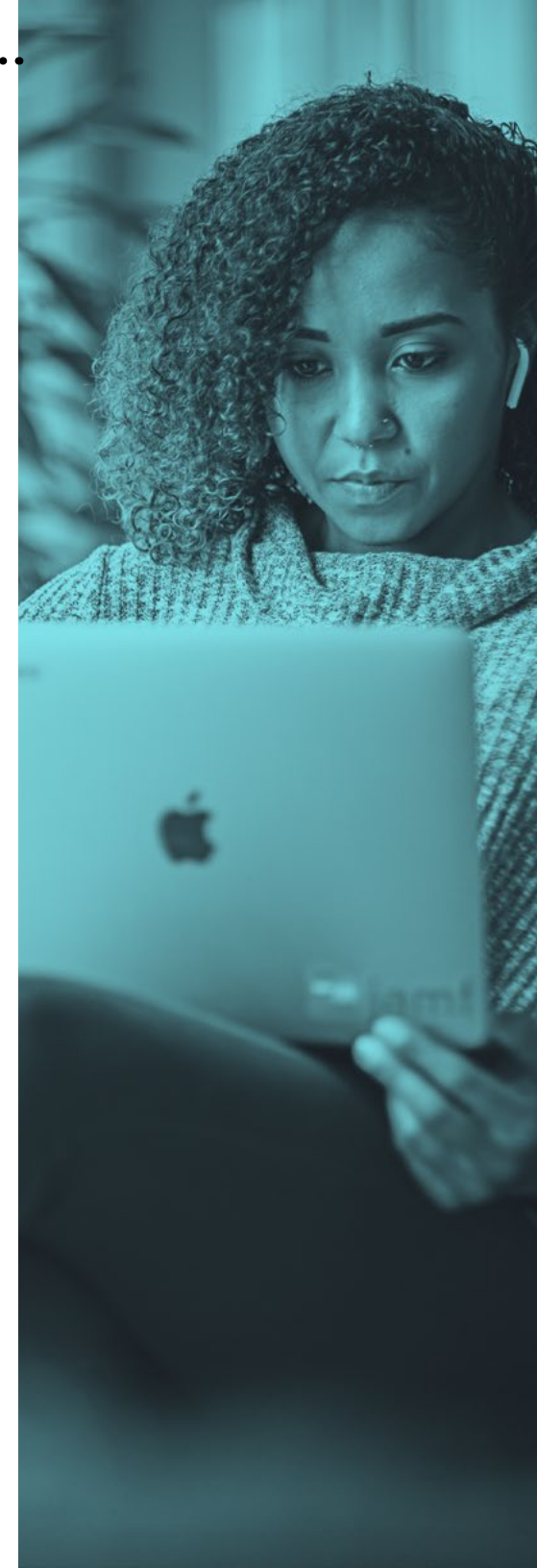
## APPLICATION DES CORRECTIFS



L'application des correctifs de sécurité doit être effectuée fréquemment et facilement pour éviter toutes les vulnérabilités connues. Avec Jamf, le service informatique gagne un temps critique en simplifiant le travail nécessaire au maintien et à la mise à jour des applications sur macOS. Il gagne également en visibilité pour la conformité et la compatibilité tout en maintenant une expérience utilisateur transparente. Les dernières versions de macOS peuvent aussi être utilisées dès leur publication, pour éviter les lacunes de sécurité en raison de retards de mise à niveau.



Les outils de sécurité et de gestion ne doivent pas vous forcer à reporter les mises à jour et mises à niveau du système d'exploitation. Avec Jamf, la solution ne se met en travers de votre route: au contraire, elle vous permet d'adopter les nouvelles versions de macOS le jour de leur sortie, sans délai. Vous avez le plein contrôle du calendrier de mise à niveau de vos appareils.



## ANTIVIRUS (AV)

Le besoin d'AV sur Mac peut sembler nouveau, mais c'est la nouvelle réalité qui l'exige. Mac et macOS sont de plus en plus ciblés à mesure que leur empreinte s'étend dans l'entreprise.

Un AV est une exigence incontournable pour la sécurité des appareils professionnels. Apple inclut un mécanisme d'AV de base sur macOS avec XProtect, Gatekeeper et MRT. Cependant, ces outils sont mis à jour de façon sporadique et les organisations manquent de visibilité sur leurs actions. Jamf Protect ajoute des fonctionnalités AV sophistiquées pour prévenir et mettre en quarantaine les logiciels malveillants sur Mac. Cela va bien au-delà de ce que les solutions axées sur Windows sont en mesure de fournir sur macOS.

Les organisations ne devraient pas attendre que des logiciels malveillants, publicitaires ou autres indésirables surgissent. Elles doivent implémenter un AV qui identifie et atténue efficacement les attaques spécifiques à Mac sans gaspiller de ressources précieuses à chercher des menaces propres à Windows. Des capacités AV efficaces et complètes sur Mac sont essentielles pour la sécurité et l'expérience de l'appareil. Dans le même temps, toute solution AV qui interfère avec la capacité de votre utilisateur final à être productif ne fera que l'agacer. Jamf Protect est conçu pour protéger macOS contre les logiciels malveillants, sans changer l'expérience que les utilisateurs finaux attendent de Mac.



Un AV pour Mac n'est plus un supplément facultatif, c'est un indispensable. Non seulement avez-vous besoin d'un AV, mais ce dernier doit être conçu spécifiquement pour Mac, sans les limitations propres aux AV imaginé pour plusieurs systèmes.

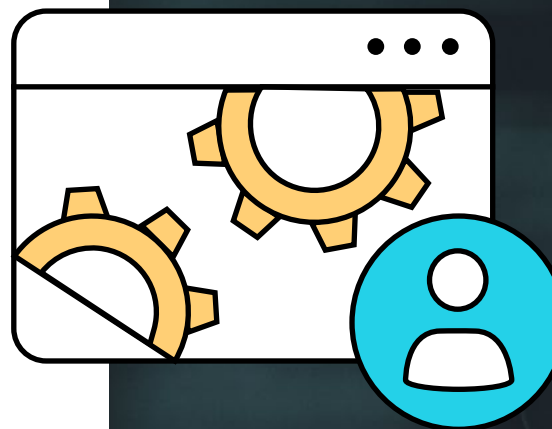
## CONFIGURATION

La posture de sécurité de Mac dans sa configuration de base est excellente, et même la meilleure parmi la concurrence. Mais nous pouvons faire encore mieux pour sécuriser vos appareils et vos données, et ce facilement. Alors si le renforcement de votre sécurité est facile, pourquoi ne pas s'y atteler ?

Il existe un nombre important de connaissances et de scripts au sein de la communauté de la sécurité pour cela. Avec Jamf, il est facile de les implémenter, de les exécuter, et de surveiller tous les utilisateurs qui tentent de dériver de ces normes. Jamf élimine les obstacles qui vous empêchaient peut-être de mettre en place une ligne de sécurité de base sur vos appareils.

L'utilisation de FileVault, l'activation d'exigences en matière de pare-feu et de mot de passe, et la configuration d'économiseur d'écran et de verrouillage entrent en jeu pour établir vos critères et étalons de sécurité.

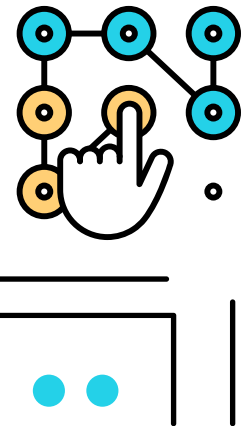
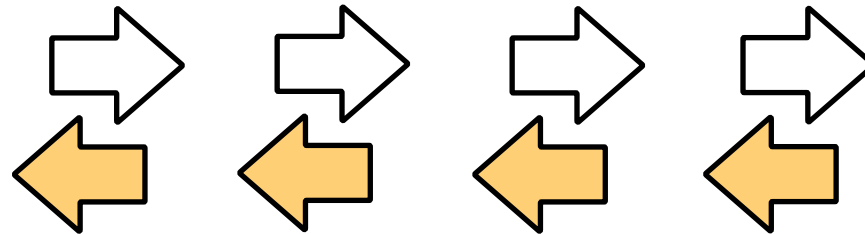
Vous ne savez pas par où commencer ? Le Center for Information Security fournit des benchmarks du secteur, et Jamf est une entreprise certifiée CIS. En travaillant avec Jamf, vous êtes donc déjà sur la bonne voie : nous avons des ressources pour vous aider. Découvrez-en davantage sur les benchmarks de sécurité CIS et Jamf avec notre [liste de contrôle de sécurité pour macOS](#).





## DÉTECTION ET RÉPONSE AXÉES SUR MAC

Les outils de détection et de réponse pour terminaux (EDR) existent pour Mac depuis un certain temps, mais la plupart ne sont pas conçus pour détecter efficacement les attaques qui ciblent spécifiquement Mac. Ils tentent plutôt de reproduire les modèles pour appareils Windows sur Mac. Jamf Protect se focalisant uniquement sur Mac et macOS : cela minimise les faux positifs tout en maximisant les taux de détection.

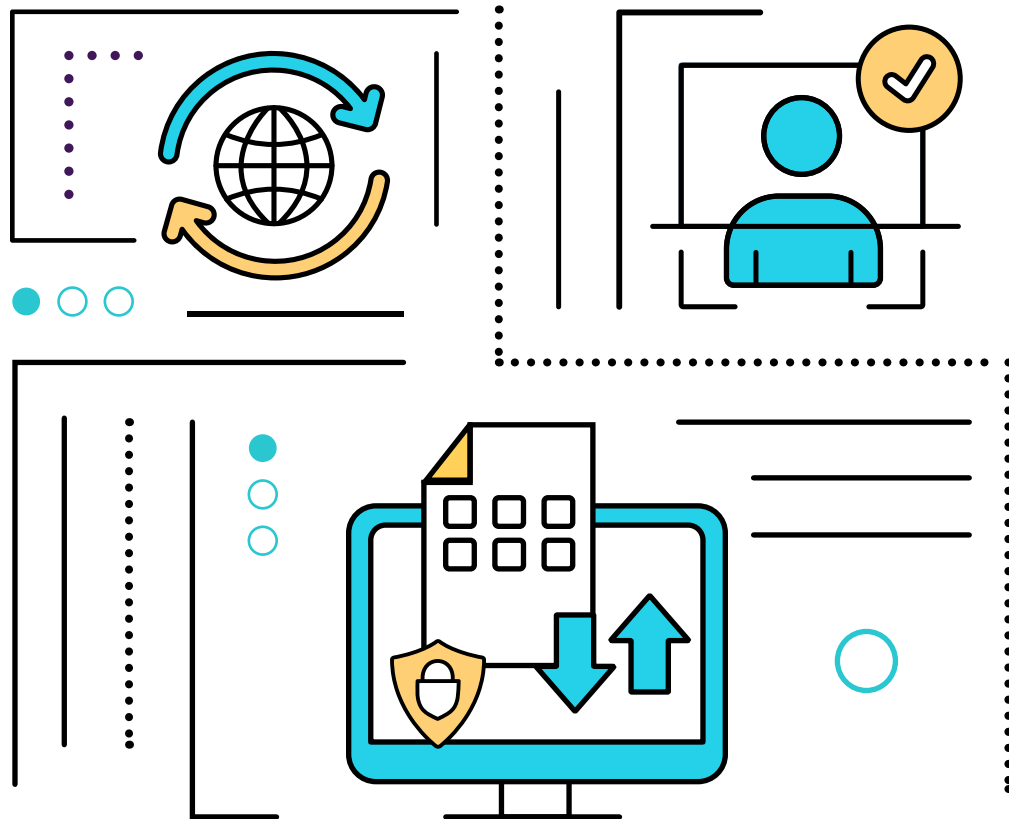


En associant Jamf Protect et Jamf Pro, vous obtenez des capacités correctives minimalement intrusives qui vont bien au-delà des capacités moyennes des EDR. Avec Jamf, les équipes informatiques et de sécurité peuvent mettre en place un plan d'intervention transparent en cas d'incident, pour permettre à vos employés de mieux travailler ensemble.



## GESTIONNAIRE DE CYCLE DE VIE D'APPLICATION

Intégrez Jamf Pro à Apple Business Manager pour attribuer et gérer les licences des applications et logiciels de votre organisation. Jamf Pro peut également vous aider avec l'application des correctifs, les mises à jour logicielles et la visibilité de l'état de votre flotte de Mac.



# La protection des terminaux sur Mac

La protection avec Jamf Protect assure la conformité des terminaux, répond aux besoins en terme d'antivirus en protégeant macOS des logiciels malveillants, contrôle et sécurise les applications Mac au sein de l'organisation, et détecte et corrige les menaces spécifiques à Mac avec un impact minimal sur l'expérience des utilisateurs.

Et associé à Jamf Pro, Jamf Protect offre des capacités complètes d'automatisation, d'enquête et de correction pour atténuer les risques de sécurité des terminaux, mineurs comme majeurs.

**Demandez un essai gratuit** ou contactez votre revendeur Apple préféré lorsque vous vous sentirez d'attaque à renforcer votre sécurité avec une solution Mac.

Apprenez-en davantage sur les **capacités de protection des terminaux** de Jamf pour Mac.