jamf

Principales pratiques de sécurité pour la gestion des Mac

Introduction

L'évolution des opérations commerciales, les besoins croissants en sécurité et l'élargissement des choix offerts aux employés continuent de **stimuler l'adoption du Mac** dans les grandes entreprises (76 %). Selon une étude de Computerworld, « neuf professionnels de l'informatique sur dix vantent les avantages métier des Mac, des iPhone et des iPad sur le lieu de travail ». C'est une excellente nouvelle pour les employés comme pour les organisations ! En diversifiant l'éventail des technologies, on offre aux employés la possibilité d'être pleinement productifs et d'utiliser leur matériel et leurs logiciels de prédilection.

Pour les équipes informatiques et de sécurité, tout changement introduit des variables potentiellement source de risques sans un contrôle étroit Heureusement, il existe des stratégies pour atténuer les risques propres à macOS : les entreprises peuvent mettre en place des défenses en profondeur proactives, basées sur une solution complète de gestion des appareils mobiles, d'identité et d'accès et de sécurité des points de terminaison. Cette solution couvre l'ensemble de votre infrastructure pour protéger les appareils, les données et les utilisateurs contre l'évolution des menaces (nous y reviendrons à la section suivante).

L'intégration des solutions permet d'affiner les pratiques de sécurité plus granulaires et de maintenir la santé des points de terminaison à un niveau de référence. Les avantages sont multiples : la conformité renforcée soutient la productivité des employés tout en libérant le service informatique qui peut développer des workflows plus performants pour soutenir les opérations. Dans cet article, nous abordons plusieurs pratiques de sécurité essentielles :

- Gestion des correctifs et des mises à jour
- Détection des menaces et réponse aux incidents
- Protection et chiffrement des données
- Sécurité des réseaux et des applications

Le fondement de la gestion et de la sécurité des Mac

Avant d'aborder notre liste de pratiques de sécurité, prenons un instant pour expliquer l'importance de mettre en place une base solide pour vos processus et vos workflows de gestion des Mac. Même si elle est évolutive, une solution qui n'offre pas une prise en charge immédiate des correctifs les plus récents, par exemple, peut dégrader la sécurité des appareils et de l'organisation. Il arrive en effet que les développeurs tardent à assurer la compatibilité avec la dernière version de macOS ou n'offrent qu'une prise en charge limitée des fonctionnalités essentielles.

Gestion des appareils mobiles (MDM)

En **2024**, macOS se faisait remarquer en occupant la 9e place au classement des 50 produits les plus touchés par des CVE (vulnérabilités et expositions courantes), avec un total de 508 vulnérabilités. En mai 2025, macOS a atteint à la 2e place au classement des 10 produits les plus touchés, avec **243 CVE identifiées**, soit près de la moitié du total de 2024. Veuillez noter que ce classement et le nombre de CVE peuvent évoluer au fil de l'année.

Ces chiffres nous rappellent à quel point il est important que l'OS et les applications des appareils soient à jour. Des fonctionnalités modernes, et en particulier la gestion déclarative des appareils (DDM), permettent aux appareils d'appliquer les critères en toute autonomie et de signaler les changements en temps réel. Cette nouvelle approche allège la charge de la MDM, et améliore la vitesse et la fiabilité des mises à jour. Autre avantage, les équipes informatiques bénéficient d'une visibilité immédiate sur les principaux changements d'état.

L'intérêt de la MDM va d'ailleurs bien au-delà de la seule gestion des correctifs : elle simplifie les opérations, soutient l'efficacité de la prise de décision et orchestre bien d'autres aspects cruciaux de la gestion des Mac de manière centralisée. Les fonctions suivantes de la MDM expliquent son rôle crucial :

- Déploiement de configurations et de réglages sécurisés
- Installation d'applications gérées
- Mise en conformité basée sur des règles
- Tenue des inventaires d'actifs

Identité et accès

Protéger les données et veiller à ce que les employés aient accès aux ressources essentielles à leur travail : ces deux missions apparemment distinctes ont pourtant un point commun, la question des permissions. Selon le **Rapport 2024 de Verizon sur les enquêtes sur les violations de données**, « 68 % des violations impliquent un facteur humain ». Ce chiffre ne tient pas compte des menaces internes et décrit uniquement les incidents résultant d'une mauvaise configuration des permissions (principe du moindre privilège) et d'erreurs de l'utilisateur final quant à la gestion des identifiants.

Du point de vue de la sécurité, ce problème ne peut être résolu simplement en imposant une formation de sensibilisation à la sécurité sur la détection et le signalement des menaces. Il faut en effet aller plus loin et miser sur une solution qui va au-delà de l'utilisation d'identités cloud. On peut notamment mettre en œuvre :

- Des règles d'accès sensibles aux risques, pour bloquer les appareils et les comptes compromis
- Le tunnelage intelligent et segmenté, qui chiffre le trafic professionnel tout en préservant la confidentialité du trafic personnel
- L'authentification multifacteur (AMF), pour vérifier l'identité des personnes qui demandent des ressources.

La sécurité des points de terminaison

Toutes plateformes confondues, les **logiciels malveillants ciblant macOS** représentaient, en 2024, environ 11 % des détections mondiales. Bien que ce chiffre reste modeste, les équipes informatiques et de sécurité ne doivent pas prendre cette tendance à la légère. Ce chiffre a plus que doublé sur les deux dernières années, et avec l'émergence du malware en tant que service et des logiciels malveillants pilotés par l'IA, les Mac sont devenus des cibles de choix pour les pirates. On a en effet observé une **augmentation significative** des campagnes de type infostealer.

Si l'on ajoute à cela d'autres types de code malveillant, comme les APT ou les chevaux de Troie, qui cherchent à contourner les protections liées à la signature de code dans macOS, la prévention des logiciels malveillants s'impose comme une nécessité absolue pour défendre les appareils. Rappelons également l'existence d'autres contrôles indispensables pour maintenir la posture de sécurité des appareils et de l'organisation.
Par exemple :

- L'identification des menaces inconnues grâce à l'analyse comportementale
- Mise en quarantaine et suppression des applications suspectes et des menaces détectées
- Surveillance active, émission d'alertes et création de rapports basés sur les données de santé des appareils (télémétrie)
- Filtrage de l'accès aux contenus web risqués, tels que les URL de phishing zero-day.

Pratiques de sécurité clés pour la gestion des Mac

Il y a beaucoup de choses à couvrir dans cette section, et c'est pourquoi nous avons choisi le format de la check-list pour vous présenter les bonnes pratiques de sécurité. C'est la façon la plus simple de synthétiser les étapes pour les équipes informatiques et de sécurité. Ce format permet aux responsables informatiques d'avoir une vision claire et synthétique de l'ensemble des points, répartis en sept catégories reposant sur l'intégration des trois solutions fondamentales.

Inscription des appareils et provisionnement

- Déploiement sans intervention d'appareils sécurisés avec inscription dans la solution MDM
- Installation automatisée du système, avec provisionnement des applications gérées et des configurations.
- Appliquer les normes et les règles de sécurité de l'entreprise à tous les modèles de propriété (appareils d'entreprise et BYOD).

Protection et conformité des points de terminaison

- Renforcer les réglages de sécurité macOS (FileVault, Gatekeeper, XProtect)
- Adapter la prévention des menaces sur l'appareil et dans le réseau grâce à des analyses personnalisées
- Générer des conseils de sécurité pour configurer les points de terminaison au niveau de conformité souhaité afin d'établir des profils de référence personnalisés et alignés sur les cadres et les normes du secteur.

Gestion des identités et des accès (IAM)

- Mettre en place des contrôles d'accès basés sur le rôle (RBAC) pour appliquer le principe de moindre privilège.
- Minimiser les risques liés aux identifiants en implémentant la SSO et l'authentification sans mot de passe.
- Vérifier la santé des appareils et des identifiants avec l'architecture « zero trust »

Gestion des correctifs et des mises à jour

- Simplifier les mises à jour des systèmes d'exploitation et des applications pour atténuer automatiquement les vulnérabilités connues
- Surveiller les données de télémétrie et les partager en toute sécurité avec des solutions intégrées en temps réel
- Garantir la conformité grâce à des workflows de correction automatisés et basés sur des règles, qui se déclenchent en cas de non-conformité.

Détection des menaces et réponse aux incidents

- Utiliser le ML pour automatiser la collecte et l'analyse d'intelligence des menaces et pour fournir des conseils et des recommandations fondées sur des données.
- Résoudre rapidement les incidents grâce à des outils simples et efficaces de détection et de réponse sur les points de terminaison (EDR)
- Enrichir les enquêtes de recherche des menaces et automatiser la correction grâce à l'IA et à des workflows basés sur des règles

Protection et chiffrement des données

- Appliquer le chiffrement FileVault, et stocker et actualiser les clés de récupération dans les enregistrements des appareils, de façon sécurisée et automatisée.
- Généraliser l'accès réseau « zero trust » (ZTNA) à l'ensemble de votre infrastructure, en vérifiant l'intégrité des appareils et des identifiants avant d'accorder l'accès aux ressources professionnelles protégées.
- Stocker les données sur des volumes protégés et empêcher le partage ou la copie non autorisés vers des emplacements non approuvés, selon le principe de prévention des pertes de données (DLP).

Sécurité des réseaux et des applications

- Renforcer la sécurité sur les réseaux grâce au chiffrement permanent de toutes les connexions réseau et à la gestion des règles de pare-feu
- Gérer les autorisations des applications tierces et les références de sécurité de macOS
- Segmenter le trafic réseau, prévenir les attaques basées sur le réseau (« man-in-the-middle »), en acheminant chaque demande de ressources à travers son propre microtunnel.

Jamf, ça marche ! Des résultats concrets sur le terrain

Gagner en efficacité en réduisant les délais de provisionnement des appareils

« Nous gagnons plus d'une journée par ordinateur portable par rapport à un provisionnement manuel. »

– Product owner, Plateforme de signature électronique numérique et d'automatisation des documents.

Les entreprises qui adoptent le Mac à grande échelle enregistrent des **gains d'efficacité mesurables** et voient leur posture de sécurité s'améliorer.

Se libérer des tâches répétitives pour se consacrer à l'innovation

« Aujourd'hui, il nous faut seulement dix minutes par machine : c'est un gain de temps considérable. »

– Responsable informatique, Plateforme de gestion financière et de comptabilité

Démontrez l'impact des workflows automatisés de déploiement sans intervention en termes **de gain de temps et d'optimisation des ressources**.

Assurer la sécurité des données et la productivité des utilisateurs grâce à une approche complète de réduction des risques.

« Les fonctionnalités de détection des menaces en temps réel, de surveillance de la conformité et de centralisation des règles jouent un rôle décisif pour la protection de nos actifs et le respect des réglementations. »

– Responsable informatique, Bibliothèque publique numérique

Appuyez-vous sur la gestion des Mac pour **renforcer la sécurité** et le respect des règles, en maximisant l'impact de la détection des menaces en temps réel et de l'application centralisée des règles.

Garantir la conformité de l'organisation tout au long du cycle de vie des appareils

« Cette structure nous permet d'assurer activement notre conformité à des normes aussi strictes que SOC 2 Type II, ISO et HIPAA. C'est la preuve que Jamf sait à la fois renforcer la sécurité des organisations et les aider à respecter les réglementations sectorielles critiques. »

– Directeur informatique, Entreprise de santé numérique.

Renforcez activement le respect des critères de conformité et **implémentez des références de sécurité** fondées sur les normes et les cadres de votre secteur.

Conclusion

Avec la généralisation du Mac en entreprise, les organisations ont tout intérêt à miser sur une approche proactive et intégrée de la gestion et de la sécurité de leur parc. Le paysage des menaces évolue, les environnements de travail sont de plus en plus divers et complexes, et ce nouveau contexte appelle une stratégie de sécurité claire et ciblée, alignée sur les opérations, tout en restant suffisamment flexible pour répondre aux besoins de tous les acteurs, où qu'ils se trouvent.

Pour atteindre cet objectif, une solution « taille unique » ne suffit pas.

Il faut en effet une approche multicouche conçue nativement pour accompagner chaque étape du cycle de vie des Mac et de leurs applications. Cette approche a pour socle la gestion des appareils mobiles (MDM), la gestion des identités et des accès (IAM) et la sécurité des points de terminaison. Cette base permettra aux entreprises d'offrir à leurs employés de choisir leur appareil en toute confiance, sans avoir à arbitrer entre la sécurité et la protection de la vie privée des utilisateurs.

Pour résumer :

- **Les appareils sont conformes**
- **Les données sont sécurisées**
- **Les utilisateurs sont protégés**

Cet article a présenté les pratiques de sécurité essentielles pour maintenir l'intégrité des points de terminaison et assurer la conformité du parc aux réglementations. L'objectif est d'armer les équipes de sécurité des outils nécessaires pour réagir rapidement aux menaces, pour permettre aux équipes informatiques de se concentrer sur l'innovation et d'offrir une assistance optimale aux acteurs de l'entreprise. Cette approche donne également aux employés les moyens d'être les plus productifs possible en minimisant les interruptions.

En choisissant des solutions coordonnées et connectées, les entreprises peuvent compter sur un écosystème Mac sécurisé et évolutif qui fonctionne aux côtés des PC Windows dans un juste équilibre entre productivité, convivialité et protection. Ce fondement ouvre la voie à l'innovation et à la résilience, quel que soit le lieu de travail.

Principaux points à retenir

L'adoption du Mac en entreprise a augmenté de **76 %** grâce aux programmes de choix des employés et aux avantages de la plateforme en termes de productivité.

La sécurité des points de terminaison macOS revêt aujourd'hui une importance stratégique face à la multiplication des menaces, notamment les infostealers et les logiciels malveillants pilotés par IA.

90 % des professionnels de l'informatique reconnaissent les avantages métier de l'utilisation des appareils Apple au travail.

L'architecture « zero trust » et l'automatisation jouent un rôle crucial dans le maintien de la conformité, la détection des menaces et la réduction des temps de réponse.

L'intégration des solutions fondamentales permet de simplifier et d'automatiser la conformité en minimisant les interruptions pour les utilisateurs.

68 % des violations impliquent un facteur humain, faisant de la gestion des autorisations et des contrôles d'accès des priorités absolues.

Une approche complète doit inclure la MDM, la gestion des identités et des accès (IAM) et la sécurité des points de terminaison.

Les équipes informatiques et de sécurité doivent s'adapter aux variables introduites par les Mac et adopter des stratégies intégrées de défense en profondeur pour atténuer les risques.

Une stratégie de sécurité Mac exhaustive et intégrée accompagne et sécurise la croissance des entreprises tout en optimisant la productivité des utilisateurs.

Seule une stratégie de défense en profondeur peut atténuer les risques spécifiques à macOS en entreprise.

jamf

Essayez Jamf for Mac.

www.jamf.com/fr