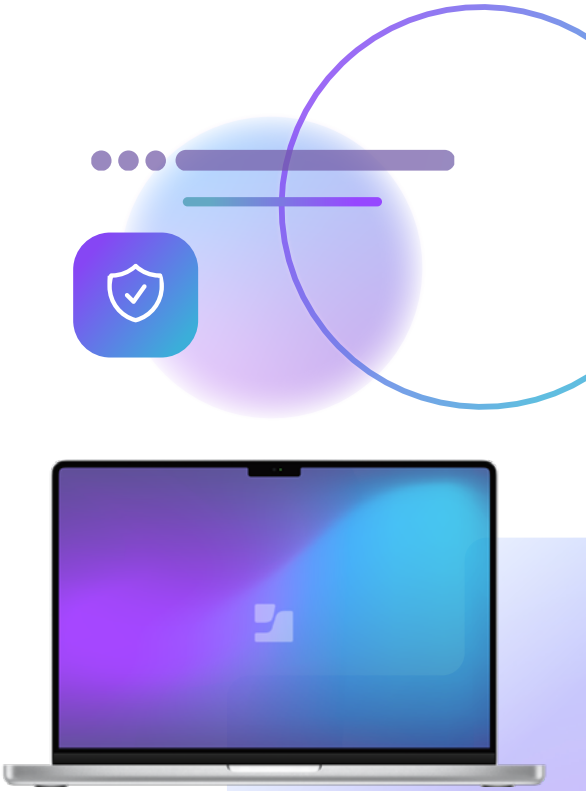
Check-list : identifier les lacunes de sécurité

Un guide rapide à destination des administrateurs informatiques et des équipes de sécurité qui gèrent un parc Mac

Le Mac est déjà très populaire auprès des ingénieurs, des spécialistes du marketing, des cadres, des équipes de création et de bien d'autres professionnels encore. Et il continue de gagner du terrain : au deuxième trimestre 2025, il affichait une croissance de 21,4 % sur 12 mois, soit plus que tout autre constructeur.

Ce n'est pas une surprise. C'est une réalité : les **employés aiment travailler sur un Mac**. Aujourd'hui, de plus en plus d'employés utilisent leur appareil de prédilection pour travailler, ce qui améliore aussi bien leur satisfaction professionnelle que leur productivité. Mais quelles sont les implications pour les professionnels du service informatique et de la sécurité ?



Les Mac et les PC Windows sont différents. Leurs systèmes d'exploitation, leurs stratégies matérielles, leurs architectures et leurs philosophies de conception ne sont pas les mêmes. Pour cette raison, ils requièrent des approches différentes en matière de sécurité. Les administrateurs qui ont essentiellement travaillé avec Windows risquent de remarquer des lacunes dans leur stratégie, surtout si leur parc d'appareils est vaste. Tant le matériel que les logiciels du Mac sont fabriqués par Apple. Les administrateurs ont donc besoin d'outils qui s'appuient sur l'écosystème Apple et le comprennent.

Dans cet article, nous passons brièvement en revue les stratégies de sécurité propres au Mac pour vous aider à repérer les angles morts. Nous aborderons le provisionnement, la gestion des identités et des accès, la protection des terminaux, et la conformité, avec des check-lists spécialement pensées pour les professionnels de l'informatique et de la sécurité.

Vous voulez approfondir le sujet ? Lisez notre livre blanc :

Défense en profondeur : combler les lacunes de sécurité par l'intégration et la superposition de solutions

Check-lists des lacunes de sécurité pour les administrateurs informatiques

Déploiement sans intervention et provisionnement des appareils

Pensez à :

- Utiliser Apple Business Manager avec votre plateforme de gestion des appareils mobiles (MDM)
- Utiliser l'inscription automatisée des appareils pour définir les entités et les restrictions
- Imposer une version minimale de l'OS avant que Mac ne passe par l'Assistant réglages

Authentification des utilisateurs et intégration des fournisseurs d'identité

Pensez à :

- Intégrer l'authentification unique de plateforme avec votre fournisseur d'identité (IdP) et votre MDM
- Choisir une solution MDM qui prend en charge la configuration de l'authentification unique extensible.
- Exiger l'authentification pour les opérations privilégiées après la connexion initiale

Déploiement des mises à jour de l'OS Apple

Pensez à :

- Déployer les mises à jour automatiques et les mises à niveau logicielles annuelles ; la cadence est différente de celle des appareils Windows
- Tester vos solutions de gestion et de sécurité avec la dernière version de macOS (important : tests bêta pour les versions majeures).
- Déployer les Rapid Security Responses sans affecter la productivité des utilisateurs

32 % des organisations utilisent au moins un appareil présentant des vulnérabilités critiques (et qu'il est possible de corriger).

Rapport 360

Check-lists des lacunes de sécurité pour les équipes de sécurité

Alignement sur les cadres de conformité

Pensez à :

- Automatiser le durcissement des appareils en intégrant le **Projet de conformité de macOS en matière de sécurité** (mSCP).
- Implémenter les critères et les références **CIS niveau 1 et niveau 2** ou **NIST 800-171**
- Mettre en œuvre, maintenir et automatiser des réglages de gestion afin d'appliquer des contrôles de sécurité spécifiques à l'ensemble du parc Mac.

Sécurité des terminaux intégrée pour les menaces propres aux Mac

Pensez à :

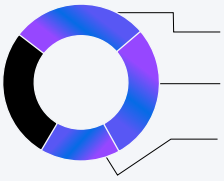
- Installer des outils dédiés au blocage des menaces connues et zero-day qui ciblent particulièrement les Mac
- Mettre en œuvre une protection terminaux en temps réel exploitant les fonctionnalités intégrées de macOS comme XProtect, Gatekeeper et Notarization.
- Rechercher la présence de logiciels malveillants propres à Mac en vous appuyant sur les dernières recherches d'experts.

Streaming des données télémétriques de macOS vers les SIEM/SOAR existants.

Pensez à :

- Choisir des outils qui utilisent l'API de sécurité des points de terminaison pour fournir directement les données télémétriques
- Aligner la télémétrie de macOS sur vos modèles de données SIEM existants
- Installer des outils qui contextualisent la télémétrie pour la rendre immédiatement utilisable
- Analyser en temps réel les événements de sécurité de macOS, comme le contournement de Gatekeeper ou le signalement de logiciels malveillants par XProtect

Principaux logiciels malveillants sous Mac :

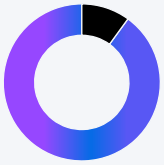


Infostealers **28,36 %**

Logiciels publicitaires **28,13 %**

Chevaux de Troie **16,61 %**

Rapport 360



Plus de **90 % des cyberattaques** ont le phishing comme point de départ.

Rapport 360

Installation et suivi des applications

Pensez à :

- Installer des outils pour maintenir à jour les logiciels macOS tiers dans votre environnement
- Produire des rapports sur les versions des applications Mac et leur utilisation
- Contrôler les canaux de distribution des applications par le biais de comptes gérés et de certificats de développeur.

Accès des utilisateurs et des appareils aux ressources de l'entreprise

Pensez à :

- Exploiter les technologies Apple telles que Network Relay pour mettre en place un accès réseau « zero trust »
- Utiliser l'attestation des appareils basée sur le matériel via Secure Enclave pour appliquer les règles d'accès conditionnel
- Développer des modèles « zero trust » propres à la plateforme macOS

Cette check-list vous guidera dans la mise en place d'une stratégie de défense en profondeur.

jamf

www.jamf.com/fr

Envie d'aller plus loin ?
Lisez notre livre blanc.