LA SÉCURITÉ DES MAC

en entreprise

jamf

INTRODUCTION

Aujourd'hui et plus que jamais, offrir à ses employés une technologie de pointe est le fondement d'une entreprise prospère. Depuis l'apparition de la COVID-19, nous avons pu assister à une transformation numérique mondiale, transitionnant du travail au bureau avec son lot d'appareils et de réseaux au télétravail. Cette évolution a propulsé la sécurité au premier plan car les moyens modernes de protection du travail où que soient les employés sont primordiaux pour assurer le succès de l'organisation.

Mais comment les organisations évaluent-elles l'état actuel de leur sécurité pour savoir où elles se situent sur l'échelle ? Quels sont les facteurs qui entrent en comptent dans le choix du matériel et du logiciel pour non seulement maintenir la conformité de la sécurité, mais aussi pour protéger l'expérience utilisateur final ?

Pour améliorer la sécurité Mac dans l'entreprise, pour répondre à ces questions et bien plus encore, Jamf a chargé Vanson Bourne, une société tierce d'études de marché , d'effectuer une étude auprès de 1500 informaticiens et professionnels de l'InfoSec (la sécurité informatique) en Amérique du Nord et en Europe.

SYNTHÈSE

Les résultats révèlent que l'utilisation du Mac est en hausse, même parmi les organisations qui utilisent principalement des appareils non Mac. Les principaux facteurs incluent la préférence du service informatique et de l'InfoSec, la perception que le Mac est déjà plus sécurisé au départ que les appareils non Mac et la conviction que les Mac facilite le maintien de la sécurité totale par rapport aux autres types de matériel.

Mais aucun système d'exploitation ou aucun matériel n'est parfait. Peu importe le matériel, les organisations gèrent les futures dépenses pour la sécurité dans plusieurs domaines clés, telles que la prévention de la perte de données, les logiciels anti-virus, les outils de protection des terminaux et les outils de réponse.

Cette augmentation des dépenses pour la sécurité est le reflet de la pandémie de la COVID-19, qui a vu un grand nombre de travailleurs transitionner du travail au bureau au travail à distance. Il est donc impératif que les terminaux restent sécurisés quel que soit l'endroit où l'appareil est utilisé ou les ressources sont consultées.

Ce rapport évalue l'utilisation et les approches actuelles de l'appareil, les défis et l'avenir de la sécurité des terminaux pour donner une image complète de l'entreprise.

DONNÉES DÉMOGRAPHIQUES

Pour obtenir une vision globale, nous avons enquêté auprès des informaticiens et des professionnels de l'InfoSec dans des entreprises qui se trouvent en Amérique du Nord et en Europe, allant des PME aux GE. Sur les 1500 personnes interrogées, la moitié d'entre elles préfère les environnements Mac et l'autre moitié préfère les environnements non Mac.

PAR LA TAILLE DE L'ORGANISATION

Nombre d'employés	Répondants
100 à 199	150
200 à 499	252
500 à 999	**327**
1,000 à 2,999	358
3,000 à 4,999	261
5,000 ou plus	152

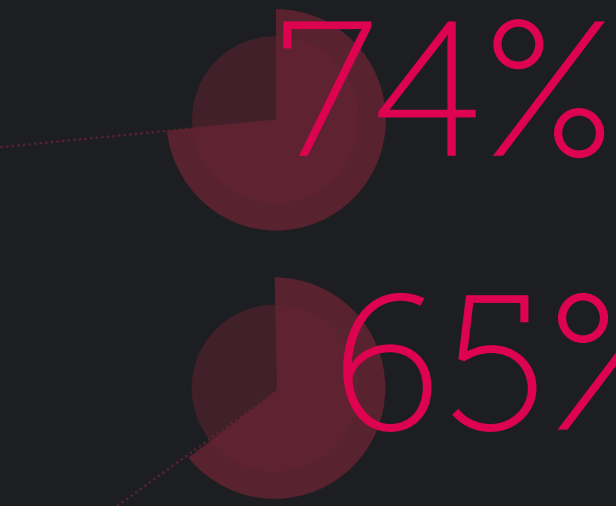
ENVIRONNEMENT

750 répondants avec une prédominance d'utilisateurs non-Mac

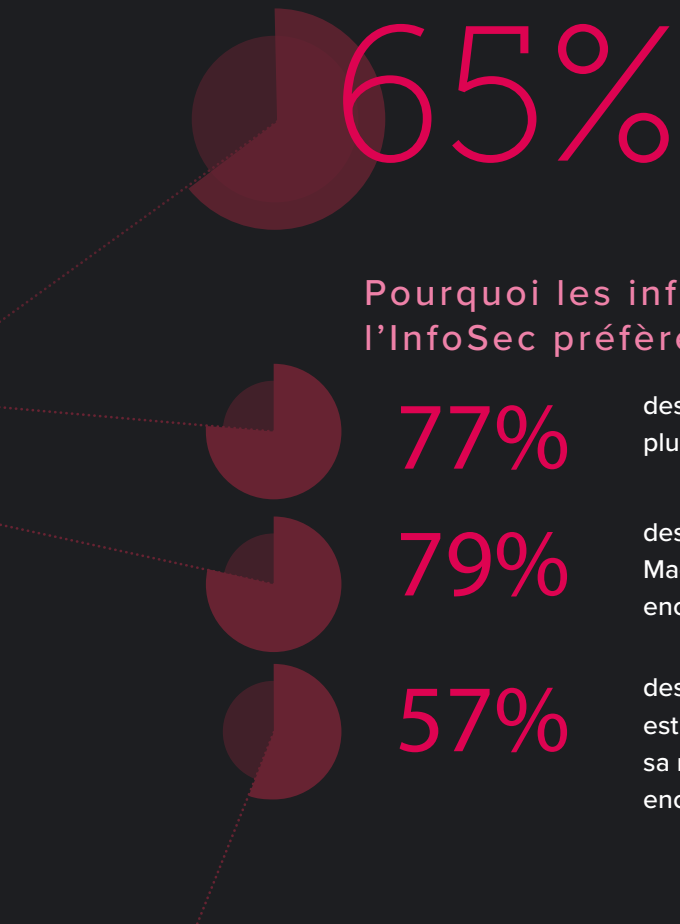
750 répondants ayant principalement des utilisateurs Mac

L'UTILISATION DES MAC EST EN HAUSSE

Il est évident que la majorité des informaticiens et des professionnels de l'InfoSec s'attendent à une augmentation du nombre d'appareils de Mac au cours des 12 prochains mois, quel que soit l'appareil que leurs organisations utilisent en ce moment.



74% des répondants ayant principalement un environnement Mac disent qu'ils augmenteront le nombre d'appareils dans leur organisation



65% des répondants dont l'environnement est principalement non Mac déclarent que leur organisation envisageront l'augmentation du nombre d'appareils Mac

Pourquoi les informaticiens et les professionnels de l'InfoSec préfèrent le Mac ?

77% des organisations Mac et non-Mac considèrent que le Mac est plus sûr dès son achat que les appareils non-Mac

79% des répondants dont l'environnement est principalement Mac disent que sa réputation en matière de sécurité les encourage à acheter des appareils Mac

57% des répondants dont l'environnement est principalement non Mac disent que sa réputation en matière de sécurité les encourage à acheter des appareils Mac

L'UTILISATION DES MAC EST EN HAUSSE

Les informaticiens et les professionnels de l'InfoSec se sont entendus pour dire que la surveillance et la visibilité des terminaux sont plus faciles sur Mac mais aussi que la maintenance de la sécurité des Mac est plus facile. De plus, grâce à l'ensemble des outils de sécurité actifs, 71 % des personnes interrogées dont l'organisation utilise des appareils Mac et des appareils non Mac affirment avoir une meilleure satisfaction de l'utilisateur final avec le Mac.

La réputation perçue et la satisfaction des utilisateurs finaux amènent 84% des répondants dont les organisations utilisent à la fois des appareils Mac et non Mac à dire qu'ils choisiraient Mac si tous les utilisateurs finaux de leur organisation devaient utiliser le même type d'appareil.

71% disent que Mac offre une meilleure satisfaction à l'utilisateur final

84% choisiraient Mac pour l'ensemble de leur personnel

LES DÉFIS DE LA MISE À JOUR DU SYSTÈME D'EXPLOITATION

Malgré la perception positive de la sécurité des Mac, les organisations ont toujours des défis et des préoccupations concernant la sécurité des systèmes d'exploitation (OS) et des appareils de leur flotte.

Les utilisateurs de Mac signalent qu'ils ont en moyenne moins de temps que leurs collègues non Mac pour déployer les correctifs de sécurité des OS. Mais malgré la différence de vitesse des mises à jour Mac, il s'écoule encore en moyenne quatre jours entre la publication d'un correctif et son déploiement.

En moyenne, les utilisateurs Mac déploient les correctifs de sécurité du système d'exploitation

30% **PLUS RAPIDEMENT** que les utilisateurs non Mac

4 jours **EN MOYENNE** pour le déploiement des correctifs de sécurité pour les utilisateurs Mac

Pour les principales versions d'OS, l'écart entre Mac et les autres est encore plus grand.

En moyenne, les utilisateurs Mac déploient les principales versions du système d'exploitation presque

2.5 fois **PLUS VITE** que les utilisateurs non Mac

5 jours **EN MOYENNE** pour le déploiement des principales versions du système d'exploitation pour les utilisateurs Mac

LES DÉFIS DE LA MISE À JOUR DU SYSTÈME D'EXPLOITATION

Le temps de déploiement du dernier grand système d'exploitation laisse les appareils ouverts aux failles. Les grandes organisations sont particulièrement vulnérables.

Pourquoi ?

5 PRINCIPALES RAISONS

- Test de la compatibilité
- Compatibilité avec l'outil de sécurité
- Compatibilité avec les applications internes
- Exigences de conformité
- Compatibilité avec les applications tierces

Les retards de la mise à jour du dernier système d'exploitation courant préoccupent les organisations car ils laissent les failles connues accessibles aux attaquants. Partout dans le monde, les entreprises sont confrontées à un large éventail de menaces qui pèsent sur les appareils d'utilisateur final et à la pression constante de se protéger des attaques de cybersécurité potentiellement nuisibles. En particulier dans l'environnement du télétravail, les organisations doivent se protéger des attaques communes sur leurs appareils, contre leurs utilisateurs et leurs données.

5 PRINCIPALES PRÉOCCUPATIONS CONCERNANT LA CYBERSÉCURITÉ

- Malware
- Perte des données
- Phishing/Spear Phishing
- Logiciel non autorisé
- Ransomware

LES DÉFIS SÉCURITAIRES

Lorsqu'il s'agit de contenir un éventuel incident sécuritaire, les plus grandes préoccupations, 37 % en moyenne en Amérique du Nord et en Europe, se révèlent être des faux positifs. Cela conduit à une perte de temps et de ressources consacrées à l'étude des menaces qui n'existent pas. Le temps passé à inspecter les faux positifs est du temps perdu pour identifier une menace réelle.

PRÈS DE LA MOITIÉ des équipes du service informatique et de l'InfoSec citent les menaces inconnues comme le plus grand défi consistant à contenir (47 %) et à remédier (45 %) à un éventuel incident sécuritaire, avec les autres principaux défis qui accompagnent la remédiation :

MANQUE

- de temps
- de personnel
- d'outils
- d'argent

Bien que le Mac soit considéré comme le meilleur appareil sécurisé du marché, l'attention portée aux cyberattaques et aux menaces augmentera avec l'adoption du Mac dans les entreprises. La précision et la bonne allocation des outils et des ressources sont essentielles pour lutter contre ce phénomène.

L'AVENIR DE LA SÉCURITÉ

Dans ce contexte, l'investissement dans les bons appareils et les outils de sécurité supplémentaires permet à l'organisation d'avoir un avenir plus sécurisé. C'est exactement ce que les organisations prévoient de faire. Elles investissent dans la sécurité.

96% des organisations prévoient une dépense plus importante pour la sécurité des terminaux en particulier :

1. Prévention de la perte des données (DLP)
2. Anti-virus/les nouvelles générations d'anti-virus (AV/NGAV)
3. Endpoint Detection and Response (EDR)
4. Security Information and Event Management (SIEM)
5. Cloud Access Security Brokers (CASB)

Grâce à cet investissement accru dans la sécurité, les équipes informatiques et de sécurité visent à renforcer leur parc et à améliorer la prévention, la détection, la réponse et la correction des incidents de sécurité. Et il est impératif qu'elles le fassent, car des employés dispersés ne font qu'accroître le stress des équipes informatiques et de sécurité de l'information, surtout si l'on considère que le nombre de travailleurs à distance a augmenté de 38 % en raison de la COVID-19.

CONCLUSION

La COVID-19 a stimulé le plus grand mouvement de la main-d'œuvre à domicile dans l'histoire. Avec la COVID-19 et l'augmentation du télétravail, l'expérience technologique est désormais un facteur majeur de l'expérience employé. Les organisations doivent offrir la meilleure expérience utilisateur final à leurs employés, tout en les gardant en sécurité.

Il est primordial de garantir la sécurité des terminaux et des appareils à mesure que les entreprises s'adaptent au travail à distance et à distribuer les ressources en conséquence pour mieux arrêter les menaces.

JAMF APPLE ENTERPRISE MANAGEMENT

Jamf est la seule solution Apple Enterprise Management qui automatise l'ensemble du cycle de vie des appareils Apple dans l'entreprise, notamment le déploiement, la gestion et la sécurité des appareils, le tout sans nuire à l'expérience utilisateur et sans obliger le service informatique à toucher l'appareil. Dans le portfolio de Jamf, Jamf Protect , une solution de protection des terminaux conçue exclusivement pour Mac, étend la sécurité du Mac et vous permet de détecter, prévenir, répondre aux menaces et remédier aux incidents de sécurité. Grâce à la prise en charge le jour même des versions du système d'exploitation Apple, les solutions Jamf ne vous obligeront jamais à retarder les mises à jour et à laisser les appareils à la merci des attaques.

C'est pourquoi les entreprises dépendant le plus de la sécurité, notamment les dix plus grandes banques américaines (selon bankrate.com) et vingt-quatre des vingt-cinq plus grandes marques (selon Forbes), font confiance à Jamf pour gérer leur environnement Apple.

Découvrez le potentiel offert par Jamf dans le cadre d'un essai gratuit.

VERSION D'ESSAI

Ou contactez votre revendeur Apple autorisé préféré pour une version test.