Guide Enjeux & Perspectives

Insight

Gestion et Sécurité des périphériques en entreprise avec Apple, Insight et Jamf

Pour faciliter l'adoption des appareils Apple en entreprise, les trois partenaires proposent une offre commune afin de configurer, déployer, gérer et sécuriser une flotte de Mac, d'iPad ou d'iPhone.

En généralisant le télétravail, la crise sanitaire aura bousculé les habitudes de travail donnant un nouvel essor à la mobilité. Smartphone, tablette ou ordinateur portable, les collaborateurs doivent pouvoir collaborer n'importe où, et n'importe quand.

Avec des terminaux qui ne sont plus protégés derrière le pare-feu de l'entreprise, cette mobilité augmente, toutefois, la surface d'exposition aux risques.

Les organisations doivent s'outiller en conséquence afin de gérer et sécuriser leurs flottes de terminaux mobiles. C'est tout le sens du partenariat tripartite entre Apple, Insight et l'éditeur de solutions de MDM (Mobile Device Management) Jamf.

Découvrons en 5 points la puissance de cette collaboration qui entend proposer une offre simple, agile, sur mesure et un accompagnement expert à valeur ajoutée, afin de répondre aux nouveaux besoins et enjeux compétitifs des organisations.

1/ Apple gagne du terrain en entreprise

Depuis le début de la pandémie, Apple accroît sa présence dans la sphère professionnelle. Entre 2019 et 2020, le taux de pénétration en entreprise des appareils sous macOS est passé de 17 à 23 % aux Etats-Unis selon IDC. Les iPhone représentent 49 % de la base installée de smartphones au sein des entreprises américaines et l'iPad est la tablette numéro un pour le «business». La tendance se confirme en 2021. Toujours d'après IDC, les ventes de Mac ont bondi de 111 % au premier trimestre.

« *Avant, le monde Apple s'adressait surtout aux créatifs,* observe **Vincent Bonnin**, Channel Sales Engineer chez Jamf. *Cette époque est révolue. Apple est en train de prendre toute sa place dans un univers jusqu'alors très «Windows only» avec des terminaux qui s'adaptent aux besoins de tous les professionnels. En milieu hospitalier, les infirmières sont dotées d'iPad, les médecins de MacBook. En magasin, l'iPad sert de caisse enregistreuse.* »

En unissant leurs forces, Apple, Insight et Jamf proposent aux entreprises une offre globale, du déploiement des terminaux préconfigurés à leur administration en passant par l'accompagnement au changement des utilisateurs.

Pour **Régis Dolnet**, Senior Manager Consulting Services chez Insight, doter les collaborateurs de matériels de la firme à la pomme agit comme un levier d'attractivité et de rétention des talents. « *Apple a un côté « premium » qui valorise les collaborateurs. En faisant ce choix, une entreprise véhicule aussi une image positive à l'extérieur.* »

2/ La puissance d'un partenariat tripartite

En unissant leurs forces, Apple, Insight et Jamf proposent aux entreprises une offre globale, du déploiement des terminaux préconfigurés à leur administration en passant par l'accompagnement au changement des utilisateurs. Cette offre à 360° repose notamment sur les solutions et l'expérience de Jamf. Spécialiste de l'Apple Entreprise Management depuis près de 20 ans, l'éditeur distribue l'outil de MDM Jamf Pro (anciennement The Casper Suite).

Cette solution automatise la configuration des appareils et applique à distance la politique de sécurité de l'entreprise en gérant l'accès aux applications, en contrôlant la manière dont les données sont utilisées et partagées ou en forçant les mises à jour. Jamf propose également Jamf Connect, un outil de gestion d'authentification qui s'interface aux gestionnaires d'identités du marché comme Okta ou Azure AD. Dernier née, Jamf Protect est une solution de sécurité développée pour macOS qui détecte les menaces spécifiques aux Mac et garantit la bonne conformité des terminaux.

3/ Un accompagnement sur mesure

De son côté, Insight assure l'adoption, le déploiement et l'accompagnement de bout en bout, de l'intégration en volume d'appareils Apple jusqu'à leur sortie du parc. « *Le déploiement se fait depuis le numéro de série de l'appareil qui appelle le mode de configuration prédéfini,* explique **Aurélien Bonnin**, Senior Manager Consulting Services chez Insight. *Quand le collaborateur démarre pour la première fois la machine, il se connecte à son compte entreprise. Quelques minutes plus tard, il dispose de sa version entreprise avec les droits d'accès associés.* »

Une fois les terminaux déployés, la solution de MDM permettra de les gérer, de les sécuriser et de les mettre à jour à distance.

Deux ateliers sont menés par les experts d'Insight. Un atelier de vulgarisation présente la solution de MDM et ses fonctionnalités. Lors du second atelier dédié à l'architecture et au design, il s'agira de la configurer paramètre par paramètre. Objectif : définir des profils type d'utilisateurs (personae), des cas d'usage et les droits associés. Après une phase de test, la solution passe en pilote dans un environnement réel de production avant le déploiement généralisé.

Mais, ce n'est pas tout. **Aurélien Bonnin** insiste sur l'importance de l'accompagnement au changement, géré par Insight. « *Les utilisateurs vont découvrir de nouvelles fonctionnalités mais aussi un certain nombre de restrictions. Il convient de procéder étape par étape et de mettre en avant les bénéfices de ce changement. Depuis un magasin d'applications privatif, une entreprise pourra, par exemple, proposer des nouveaux services.* » Il conseille également de mener une communication ciblée auprès des utilisateurs par mail ou l'intranet. L'administrateur bénéficiera, lui, d'une formation technique.

Ainsi, Insight a accompagné Apax Partners, KPMG ou encore Paris Dauphine dans la mise en œuvre des solutions nécessaires pour gérer leur flotte respective de terminaux.

Autre cas de figure : la gestion d'un parc d'appareils à destination du grand public. Aéroports de Paris (ADP) met ainsi à disposition des voyageurs des tablettes afin de les inciter à s'abonner à son programme fidélité et d'en profiter immédiatement dans l'espace commercial.

L'accompagnement et les services d'Insight permettent ainsi aux entreprises d'avancer, d'innover, de développer leur potentiel et se transformer pour le futur.

4/ Une sécurité renforcée

Les matériels Apple ont la réputation d'être davantage sécurisés que leurs équivalents des mondes Windows et Android. Une réputation qui n'est pas surfaite. Ils bénéficient nativement du concept de sandboxing restreignant l'accès d'une application aux ressources système. Le système d'exploitation macOS intègre, lui, un framework de sécurité composé de GateKeeper, MRT (Malware Removal Tool), et XProtect.

L'accompagnement et les services d'Insight permettent ainsi aux entreprises d'avancer, d'innover, de développer leur potentiel et se transformer pour le futur.

« *Cette protection individuelle n'est toutefois pas suffisante en entreprise,* estime **Vincent Bonnin**. *Il convient d'aller plus loin en mettant en place des moyens de détection et de remédiation contre les menaces avancées de type malware ou ransomware. Les entreprises concentrent à tort leur attention sur la sécurisation des PC. Moins bien protégés, les appareils Apple peuvent faire office de vecteur d'attaque pour s'introduire dans le système d'information.* » En avril et mai 2021, Jamf a détecté deux failles majeures, dont une « zero day », et l'éditeur a, aussi, récemment racheté Wandera, un spécialiste de l'accès réseau zero trust (ZTNA). Tout est mis en place et pensé pour une sécurité renforcée au service des clients.

Au-delà de cette protection, un administrateur peut généraliser la rotation automatique des mots de passe et la double authentification. En s'appuyant sur le couple identifiant + mot de passe, le collaborateur s'authentifie par un procédé biométrique comme l'empreinte digitale (Touch ID) ou la reconnaissance faciale (Face ID).

En cas de perte ou de vol, un administrateur pourra supprimer à distance toutes les données de l'appareil ou bien n'effacer que les données d'entreprise. Le concept de containerisation, opérant un sas étanche entre sphère personnelle et sphère professionnelle, permet aussi, dans le cadre d'une politique de BYOD (Bring Your Own Device), d'autoriser les terminaux personnels en entreprise tout en les sécurisant.

En s'appuyant sur le couple identifiant + mot de passe, le collaborateur s'authentifie par un procédé biométrique comme l'empreinte digitale (Touch ID) ou la reconnaissance faciale (Face ID).

D'autres formes de restrictions peuvent intervenir pour protéger les données sensibles comme désactiver les fonctions « enregistrer sous », « copier-coller » ou empêcher les captures d'écran. Si un utilisateur tente de modifier un iPhone ou un iPad (jailbreak) pour contourner la politique de sécurité, le MDM sonne l'alerte et coupe automatiquement l'accès aux données et aux applications.

5 / Une expérience collaborateur enrichie

Pour **Vincent Bonnin**, « *un équilibre doit être trouvé entre les prérequis de sécurité et l'expérience utilisateur qui doit être impactée le moins possible. Il s'agit de conserver dans un cadre professionnel, ce qui fait le succès d'Apple. A savoir des machines véloces, puissantes et agréables.* » A chaque entreprise de placer le curseur au bon endroit en fonction de son profil et de son secteur d'activité. Certaines organisations adopteront un contrôle léger, quand d'autres verrouilleront les appareils avec un accès limité aux préférences.

« *A l'inverse, il existe des parades pour fluidifier l'échange d'informations et améliorer l'expérience collaborateur, comme la mise en place d'une authentification unique (SSO, Single Sign-On)* », avance **Régis Dolnet**. Une solution de MDM permet aussi de proposer une expérience utilisateur similaire au sein de parcs hybrides composés à la fois de PC et de Mac.

Ainsi, les équipes Insight guident et accompagnent l'entreprise pour un mode de travail plus agile, une expérience utilisateur totale, enrichie, performante et dynamique.

Insight, partenaire de votre transformation

Insight accompagne au plus près les entreprises dans leurs changements digitaux et apporte des réponses à la complexité des projets IT. S'appuyant sur des experts en organisation, transformation numérique, déploiement de solutions technologiques, services et produits, accompagnement au changement, Insight met toute la diversité de ses ressources humaines au service de l'efficacité et du business des organisations.

Pour en savoir plus, veuillez contacter votre chargé de compte Insight.

+33 (0)1 30 67 25 00 | info.fr@insight.com
fr.insight.com/solve/connected-workforce

Insight jamf