jamf

Mac et iOS sans compromis

dans les entreprises orientées PC

Introduction

Lorsque les appareils Apple font leur entrée dans une entreprise qui utilise essentiellement Windows, c'est l'efficacité, et non la taille de l'équipe, qui détermine la charge de travail du service informatique.

Ce guide constitue la première partie de la série *Pourquoi Jamf*. Destiné aux responsables informatiques et aux administrateurs de tous niveaux, il contient toutes les informations nécessaires pour faire en sorte que les investissements en matière d'identité, de sécurité, d'automatisation et d'observabilité offrent des résultats conformes et réduisent la part de travail manuel. L'objectif est de créer une expérience Apple cohérente sans alourdir la charge opérationnelle.

Synthèse

Pour les entreprises centrées sur Windows qui adoptent de plus en plus d'appareils Apple, l'efficacité opérationnelle est déterminante. Cet e-book explique comment intégrer Apple sans augmenter les effectifs, le coût de possession, ni la complexité, en ciblant précisément les problèmes qui nuisent aux processus et aux workflows. Le résultat ? Des déploiements plus rapides, une meilleure visibilité et une expérience Apple cohérente et sécurisée, qui évolue avec l'entreprise.

Problèmes d'intégration résolus par Jamf

Décloisonnez les données et éliminez les ralentissements dans les workflows en **intégrant l'identité**, la **sécurité** et les **solutions informatiques en place** au sein d'une stratégie holistique.

Automatisez l'ensemble du cycle de vie des appareils Apple grâce aux **intégrations de l'écosystème**, de l'approvisionnement à la mise hors service sécurisée, en passant par l'application des correctifs.

Accélérez la **réponse aux incidents** grâce à l'évaluation constante de données télémétriques riches qui permettent l'application systématique des postures de référence.

Optimisez la productivité des employés avec des workflows d'intégration sans intervention axés sur la simplicité.

Mettez en place des politiques d'accès complètes et unifiées grâce à une architecture **« zero trust »** intégrant les **fournisseurs d'identité** (IdP) de toutes les plateformes.

Une intégration étroite avec votre infrastructure existante

Lorsque les processus de gestion des appareils ne sont pas connectés aux outils de sécurité et d'identité en place, c'est tout l'environnement qui en souffre : données en silos, workflows inefficaces et défauts de conformité deviennent la norme.

On pense souvent que les appareils Apple ne sont pas compatibles avec les réseaux traditionnels centrés sur Windows. Cette croyance a plusieurs dizaines d'années déjà, mais elle se heurte à la réalité des technologies modernes des entreprises : la prise en charge multiplateforme n'est pas seulement nécessaire pour assurer la continuité de l'activité à l'échelle mondiale, elle est désormais une évidence incontournable. C'est d'autant plus important que les organisations s'appuient de plus en plus sur des architectures, des applications et des services basés sur le cloud pour produire de la valeur. Les équipes d'aujourd'hui utilisent un large éventail d'appareils, de plateformes et de versions, et les organisations doivent assurer un support homogène de tous leurs effectifs distribués.

Parallèlement à la prise en charge multiplateforme, l'intégration approfondie joue un rôle essentiel pour assurer la compatibilité entre votre pile technologique et les appareils Apple de plus en plus nombreux.

Pour l'intégration des appareils Apple est-elle plus simple avec Jamf ?

La réponse : une **interface de programmation d'application de plateforme** (Platform API).

Pour garantir une communication fluide entre les points de terminaison Apple et votre pile technologique, il faut lier les solutions aux flux de travail de gestion, d'identité et de sécurité à l'aide de liaisons sécurisées et basées sur des normes.

Quelles sont les implications pour la conformité des entreprises face au paysage moderne des menaces ? Des solutions plus simples et une complexité réduite.

L'intégration d'Apple à votre environnement permet d'atteindre plusieurs objectifs sur l'ensemble des plateformes :

L'automatisation assure la cohérence des workflows et la parité de la couverture

La **sécurité centrée sur l'identité** offre une protection unifiée contre les menaces

Vous maintenez la conformité à l'aide de **solutions que vous possédez déjà**

Vous optimisez les temps de réponse en décloisonnant les équipes informatiques

Pourquoi Jamf ?

La place de marché Jamf propose plus de 300 intégrations conçues pour faciliter l'adoption d'Apple dans votre entreprise, et ce nombre augmente sans cesse.

Réduisez les interruptions pour vos employés en simplifiant le déploiement des appareils

Chaque heure passée à attendre qu'un appareil soit prêt est une heure de productivité perdue ; dans les environnements PC, cette attente est en moyenne de 2 à 4 heures par appareil.

Dans une initiative d'intégration d'appareils Apple dans un environnement essentiellement composé de PC, la phase la plus critique, juste après la planification, est celle du déploiement. Les employés attendent que leur nouvel appareil soit provisionné par le service informatique. Cette attente dépend des réglages à appliquer, du nombre d'applications à installer et des configurations spécifiques à mettre en place en fonction du rôle de chacun, et le délai qui sépare la réception de l'appareil du moment où il est utilisable est un temps d'arrêt pour la productivité.

Et si je vous disais que ces délais peuvent être réduits à environ 15 minutes par ordinateur Apple (et à peine 5 à 7 minutes pour un iPad ou un iPhone) ?

Le secret de cette rapidité ? Le « provisionnement sans intervention ». En connectant Apple Business Manager (ABM) à une solution de gestion dédiée à Apple, les équipes informatiques peuvent profiter d'un cadre d'automatisation inégalé dans les environnements Windows. ABM peut être envisagé comme l'équivalent Apple de Windows Autopilot. Toutefois, dans la mesure où Apple contrôle à la fois le matériel et le service d'inscription, l'intégration est bien plus poussée. Le service informatique intègre ABM à Jamf et établit l'état final des appareils dans la console de gestion : applications, configurations, règles de sécurité et paramètres d'identité. Ensuite, à chaque fois que l'entreprise achète des appareils auprès d'Apple, ABM synchronise les détails de ces acquisitions avec Jamf et les ajoute à un groupe de préinscription.

Pour l'équipe informatique, le travail est quasiment terminé.

Les appareils appartenant à l'entreprise sont directement expédiés à leurs utilisateurs, au bureau ou à leur domicile. Il ne leur reste plus qu'à déballer et allumer leur nouvelle machine ! L'appareil s'inscrit automatiquement dans Jamf et le workflow de préinscription s'exécute pour provisionner l'appareil en toute simplicité. Grâce à l'automatisation du déploiement sans intervention, l'utilisateur final n'a pas besoin de faire quoi que ce soit, pas même de soumettre un ticket au service d'assistance.

Pourquoi Jamf ?

Avec les blueprints de Jamf et la gestion déclarative des appareils, les appareils appliquent proactivement les règles ce qui réduit la configuration à environ 15 minutes pour les Mac et à moins de 7 minutes pour les appareils mobiles. L'attestation d'appareil géré apporte une preuve de conformité ancrée dans le matériel : le service informatique a la confirmation qu'un appareil est authentique avant qu'il n'accède aux ressources de l'entreprise.

Apple intègre l'attestation, l'identité et la gestion au sein d'un cadre unifié allant du processeur au logiciel.

La **gestion déclarative des appareils (DDM)** permet aux appareils d'appliquer des réglages de manière asynchrone et de signaler leur état au service de gestion des appareils, sans avoir à interroger constamment l'assistance Apple. Grâce à cela, les appareils se configurent plus rapidement et restent conformes même sans connexion à Internet.

L'attestation d'appareil géré apporte des preuves solides concernant les attributs de l'appareil lors de l'évaluation de sa fiabilité ; les déclarations cryptographiques basées sur Secure Enclave et les serveurs d'attestation d'Apple démontrent l'authenticité de l'appareil avant qu'il n'entre en contact avec les ressources de l'entreprise.

Avec la Platform SSO les utilisateurs n'ont plus besoin de mot de passe : ils utilisent Touch ID avec des identifiants résistants au phishing basés sur des clés liées au matériel dans Secure Enclave. Avec cette méthode, ils s'authentifient une seule fois lors de la connexion et obtiennent ensuite un accès immédiat aux applications de l'entreprise, sans avoir à jongler avec les mots de passe.

Automatisez les tâches et les processus informatiques dans toute l'entreprise

Selon Forrester, le coût typique d'une réinitialisation de mot de passe est de 70 dollars ; **une entreprise moyenne y consacre plus d'un million de dollars par an.**

L'automatisation est un vaste concept qui peut recouvrir de nombreuses notions. Il est essentiel de comprendre la relation entre automatisation et temps. Bien sûr, l'automatisation des tâches fait gagner du temps aux équipes informatiques, mais il faut aussi du temps pour acquérir les compétences nécessaires pour développer cette automatisation.

On comprend alors pourquoi le volume d'appareils, de technologies et de solutions utilisés dans l'entreprise fait perdre autant de temps aux équipes informatiques. Le bénéfice de l'automatisation va au-delà de l'efficacité ; elle libère les équipes pour qu'elles se consacrent à des tâches stratégiques plutôt qu'à des urgences de routine. Ses avantages sont multiples :

Une application cohérente des règles

Les règles s'appliquent uniformément aux Mac, aux iPhone et aux iPad : aucun appareil ne passe entre les mailles du filet.

Réduction de l'erreur humaine

Les workflows normalisés éliminent les risques liés aux processus manuels.

Évoluer sans augmenter les effectifs

Répondez à l'augmentation des besoins en gestion et en sécurité au fil du développement de l'entreprise.

Le bon cadre d'automatisation prend en charge les tâches répétitives : déploiement des appareils, application des règles, mise à jour des logiciels et réinitialisation des mots de passe. Mais Apple va encore plus loin. Avec la gestion déclarative des appareils, les appareils n'attendent pas les instructions du serveur : ils appliquent spontanément les règles et signalent les changements d'état en temps réel. Ce cadre fait baisser le nombre de tickets d'assistance, accélère la mise en conformité et allège la part de travail manuel lorsque votre parc Apple s'agrandit.

Pourquoi Jamf ?

Les workflows d'automatisation intelligents de Jamf éliminent les configurations manuelles grâce à la gestion basée sur des règles, aux groupes intelligents et aux processus pilotés par API. Cette approche garantit un déploiement cohérent et sans erreur, et surveille la conformité à grande échelle.

Renforcez les politiques d'accès avec l'approche « zero trust »

Le paysage des menaces évolue constamment. Les acteurs malveillants utilisent désormais des technologies de pointe, IA en tête, pour imaginer des attaques toujours plus sophistiquées, optimiser les charges utiles et échapper à toute détection.

Ne vous y trompez pas : toutes les plateformes sont visées, et aucun système d'exploitation n'est invulnérable. Il est donc primordial de tenir les terminaux à jour et de mettre en œuvre une stratégie de défense en profondeur, véritable pierre angulaire d'une gestion moderne des appareils. La clé consiste à traiter chaque appareil, chaque utilisateur et chaque demande comme suspects jusqu'à preuve du contraire. Zero Trust n'est pas un produit, c'est un cadre. Et l'architecture d'Apple est conçue spécialement pour ce cadre.

L'attestation d'appareil géré démontre de façon cryptographique l'authenticité d'un appareil avant qu'il n'entre en contact avec les ressources de l'entreprise. La Platform SSO lie l'identité de l'utilisateur à des clés matérielles hébergées dans Secure Enclave, ce qui complique considérablement le vol d'identifiants. La gestion déclarative des appareils veille à ce que les appareils appliquent les règles de sécurité en toute autonomie, même lorsqu'ils sont hors ligne. Tous ces éléments créent une base où la confiance est le fruit d'un contrôle constant et non un parti pris.

Les entreprises gagnent en agilité et accélèrent la réponse aux incidents **en unifiant la gestion, l'identité et la sécurité sur l'ensemble du parc d'appareils grâce aux étapes suivantes :**

Pourquoi Jamf ?

Secure Enclave et l'attestation d'appareil géré d'Apple vérifient l'identité des appareils au niveau matériel. De son côté, Jamf applique des contrôles réseau « zero trust » avec des règles d'accès basées sur le risque, la vérification de la conformité des appareils et l'intégration de l'accès conditionnel, qui protège les données sensibles au niveau du point de terminaison.

Mise en œuvre de l'Accès réseau « zero trust » (ZTNA)

- Appliquez des règles d'accès contextuelles qui valident l'état de l'appareil et l'intégrité des identifiants à chaque demande.
- Isolez les sessions à l'aide de microtunnels pour réduire les attaques courantes sur l'appareil et sur le réseau.
- Étendez la protection à macOS, iOS, iPadOS, Android et Windows.

Application de profils de référence et de critères de conformité

- **Déployez automatiquement des configurations de sécurité de référence** alignées sur les réglementations ou des exigences de conformité personnalisées.
- **Contrôlez la posture des appareils** et de l'entreprise à l'aide de critères de conformité.
- **Utilisation de l'IA/ML pour rechercher les menaces, répondre aux incidents et faciliter l'assistance informatique**
- Détectez proactivement les menaces connues et renforcez vos capacités d'**identification et de neutralisation précoces des menaces inconnues**
- **Réduisez les temps de réponse et accélérez la remédiation** en comblant les lacunes de sécurité.
- Utilisez l'**assistant IA de Jamf** pour aider les équipes à explorer l'environnement, à valider les recommandations de configuration et à mettre au point des remédiations plus rapidement.

Optimisation de la visibilité et amélioration de la réponse tout au long du cycle de vie de l'appareil

La plupart des conversations de sécurité portent sur les menaces actives. Pourtant, certains risques majeurs (avec les coûts qu'ils impliquent) se cachent dans les angles morts : les inventaires obsolètes, les licences logicielles inutilisées et les appareils qui quittent l'organisation sans que les données aient été correctement effacées.

Les équipes informatiques et de sécurité tendent à se focaliser intensément sur les problèmes posés par les pirates, au point que certains aspects de la visibilité des appareils passent parfois au second plan.

La visibilité ne consiste pas seulement à savoir ce qui se trouve sur votre réseau. Elle implique de savoir ce qui est installé, quelles licences possède l'entreprise, ce qui est conforme et ce qui doit être mis hors service. Les données contextuelles relatives aux points de terminaison (inventaires à jour, logiciels installés, etc.) dressent un tableau complet de leur santé tout au long de leur cycle de vie. Grâce à la gestion déclarative des appareils, les appareils Apple signalent spontanément leurs changements d'état, qu'ils concernent la version du système d'exploitation, le niveau de sécurité, les applications installées ou autre. Et tout cela, sans attendre que le service informatique les interroge. De cette façon, l'inventaire est toujours parfaitement à jour.

Voyons en quoi le manque de visibilité nuit aux organisations :

Licences de logiciels inutilisées

En raison de l'absence de suivi précis des licences logicielles, 50 % d'entre elles sont inutilisées, ce qui représente environ **45 millions de dollars par mois** de dépenses inutiles.

Mise hors service des appareils

D'après les études, 10 à 20 % des violations de données survenues ces dernières années sont imputables aux déchets électroniques et à des protocoles d'élimination incorrects. Ils représentent un véritable angle mort pour les entreprises qui se focalisent sur les points de terminaison activement utilisés.

Lacunes de conformité

Sans une gestion correcte, les entreprises qui renouvellent et redistribuent leurs appareils risquent de voir leurs données tomber entre de mauvaises mains (pensez aux initiés malveillants). Ce peut être le cas, par exemple, si l'ancien ordinateur portable d'un cadre des ressources humaines est remis à un nouveau commercial. Il se pourrait que l'appareil contienne encore des informations personnellement identifiables accessibles au nouvel utilisateur. Selon les réglementations qui régissent votre secteur, cela peut être contraire aux lois sur la confidentialité, RGPD en tête.

L'approche d'Apple en matière de gestion rend cette situation plus facile à contrôler. Les appareils déclarent spontanément leur état et les règles s'appliquent automatiquement. Et quand vient le moment d'effacer un appareil pour le redéployer, l'intégration entre Apple Business Manager et votre solution de gestion garantit que l'appareil s'inscrit à nouveau automatiquement, sans intervention manuelle ni aucune faille de sécurité.

Pourquoi Jamf ?

Avec Jamf, le service informatique peut s'assurer que les Mac équipés d'une puce Apple fonctionnent en mode Full Security avant leur mise hors service. De cette façon, les données chiffrées FileVault restent protégées même en cas de perte ou d'élimination non contrôlée de l'appareil. Sachant que 10 à 20 % des violations de données sont liées aux déchets électroniques, la visibilité matérielle sur l'état du Secure Boot vient combler une lacune dont la plupart des entreprises ne prennent conscience que lorsqu'il est trop tard.

Des workflows spécialisés aux résultats tangibles

Le véritable indicateur de performance de la gestion des appareils n'est pas à chercher du côté de l'administration informatique, mais des employés et des clients qui remarquent une amélioration dans leurs tâches quotidiennes. Ces exemples concrets montrent à quel point les appareils peuvent améliorer l'efficacité des workflows :

Santé

Lorsqu'un patient quitte l'hôpital et que le statut de son dossier médical change en conséquence, son iPad de chevet efface automatiquement toutes ses données et se réinitialise pour le patient suivant, sans qu'aucun membre du personnel n'ait à intervenir sur l'appareil. Les soignants utilisent des iPhones partagés sur lesquels les applications activées changent en fonction du rôle et des identifiants.

Aviation

Le sac de vol électronique sur iPad des pilotes remplace les listes de contrôle, les cartes et les manuels volumineux. Les mécaniciens, les agents d'embarquement et les personnels navigants reçoivent automatiquement les bonnes applications, quel que soit l'appareil qu'ils prennent en main.

Commerce de détail

Des iPads verrouillés en mode App individuelle servent de kiosques en libre-service. Pas de dépannage ni de contenu inapproprié, et il n'est même pas nécessaire de réinitialiser le système en fin de journée. Le personnel de vente navigue en toute simplicité entre le système de caisse, l'inventaire et les informations client ; les appareils partagés sont automatiquement configurés en fonction de la personne qui se connecte.

Fabrication

Bien souvent, les ouvriers de production n'ont pas d'identifiants réseau ni d'expérience en matière de technologie mobile. Des casiers de chargement sécurisés assurent l'assistance de niveau zéro. Si un iPad ne fonctionne pas, il suffit de le brancher pour qu'il se réinitialise automatiquement et se configure en toute autonomie. L'employé peut simplement prendre un autre iPad et se remettre au travail sans faire de signalement à l'assistance ni intervenir sur l'appareil.

Services financiers

Les experts en sinistres, les agents de crédit et les conseillers de terrain ont besoin d'accéder instantanément à des données sensibles sur des appareils partagés, bien souvent dans des lieux imprévisibles, tout en répondant à de strictes exigences de conformité. Il suffit à un expert de prendre un iPad dans un rack et de saisir une fois ses identifiants pour obtenir un accès immédiat aux applications de gestion des sinistres, aux outils photo et aux dossiers des clients. Une fois le travail terminé, il retire ses identifiants en quelques secondes ; l'appareil est alors prêt pour l'utilisateur suivant, avec une piste d'audit complète pour garantir la conformité des opérations.

Conclusion

L'intégration d'Apple dans les entreprises centrées sur Windows n'implique ni refonte à grande échelle ni alourdissement de la charge opérationnelle. Il invite au contraire à adopter des workflows efficaces, automatisés et normalisés. En unifiant la gestion du cycle de vie des appareils, de l'identité et de la sécurité sur une base native Apple intégrée aux outils existants, les équipes informatiques font franchir un nouveau cap de maturité à leurs opérations. Les avantages de cette approche sont pluriels : plus proactive, elle réduit les efforts manuels et renforce la cohérence. Les organisations peuvent moderniser leurs opérations à leur propre rythme tout en maintenant une disponibilité multiplateforme et en assurant la conformité et le contrôle de l'ensemble du parc de bureau et mobile.

Principaux points à retenir

- L'intégration d'Apple est un défi d'efficacité, pas un problème d'effectifs.
- Avec le déploiement sans intervention, les heures de configuration sont réduites à quelques minutes pour minimiser les temps d'arrêt.
- L'unification de la gestion, des identités et de la sécurité décloisonne les opérations.
- L'automatisation permet de systématiser l'application des règles à grande échelle tout en réduisant les erreurs humaines.
- L'accès réseau « zero trust » renforce la sécurité sans ajouter de complexité.
- La visibilité du cycle de vie préserve le temps de fonctionnement, facilite la conformité et permet de maîtriser les dépenses en logiciels.
- La gestion déclarative des appareils assure la conformité des appareils, même hors ligne.

Vous voulez voir tout cela à l'œuvre ?

Découvrez Jamf dès aujourd'hui