jamf

Une expérience exceptionnelle pour les utilisateurs finaux d’appareils Apple dans une entreprise axée sur le PC

Introduction

Expérience et productivité vont de pair.

En accordant aux processus informatiques le soin que donne Apple à l'expérience utilisateur, les entreprises réduisent les frictions et maximisent à la fois la productivité et le rendement de l'investissement (ROI).

Deuxième volume de la série Pourquoi Jamf, ce guide s'adresse aux responsables informatiques et aux administrateurs de tous niveaux. Ils y trouveront toutes les informations dont ils ont besoin pour veiller à ce que leurs investissements en matière d'identité, de sécurité, d'automatisation et d'observabilité soient mis au service de la productivité des employés, en surmontant les difficultés et les obstacles les plus courants.

Synthèse

Quand le provisionnement des appareils, la gestion des accès, les mises à jour logicielles et la défense contre les menaces reposent sur des processus manuels, la productivité en souffre. Ce guide explique comment l'intégration de la gestion des appareils, des identités et de la sécurité simplifie les opérations informatiques tout en améliorant l'expérience utilisateur. Grâce au déploiement sans intervention, aux contrôles d'accès basés sur le rôle et à la gestion automatisée du cycle de vie des applications, Jamf fluidifie l'intégration, sécurise les appareils et maintient leur conformité. Avec Self Service+, les employés installent des applications approuvées et trouvent des solutions aux problèmes courants en toute autonomie, ce qui a le double avantage de réduire le nombre de tickets d'assistance et de faciliter le respect des règles. Le résultat : un workflow évolutif qui renforce la sécurité, simplifie la gestion et soutient la productivité des employés dès le premier jour.

Les problèmes de productivité, et la réponse de Jamf

Facilitez l'accueil des nouveaux employés en proposant des appareils « prêts à l'emploi » et fonctionnels dès leur sortie de l'emballage.

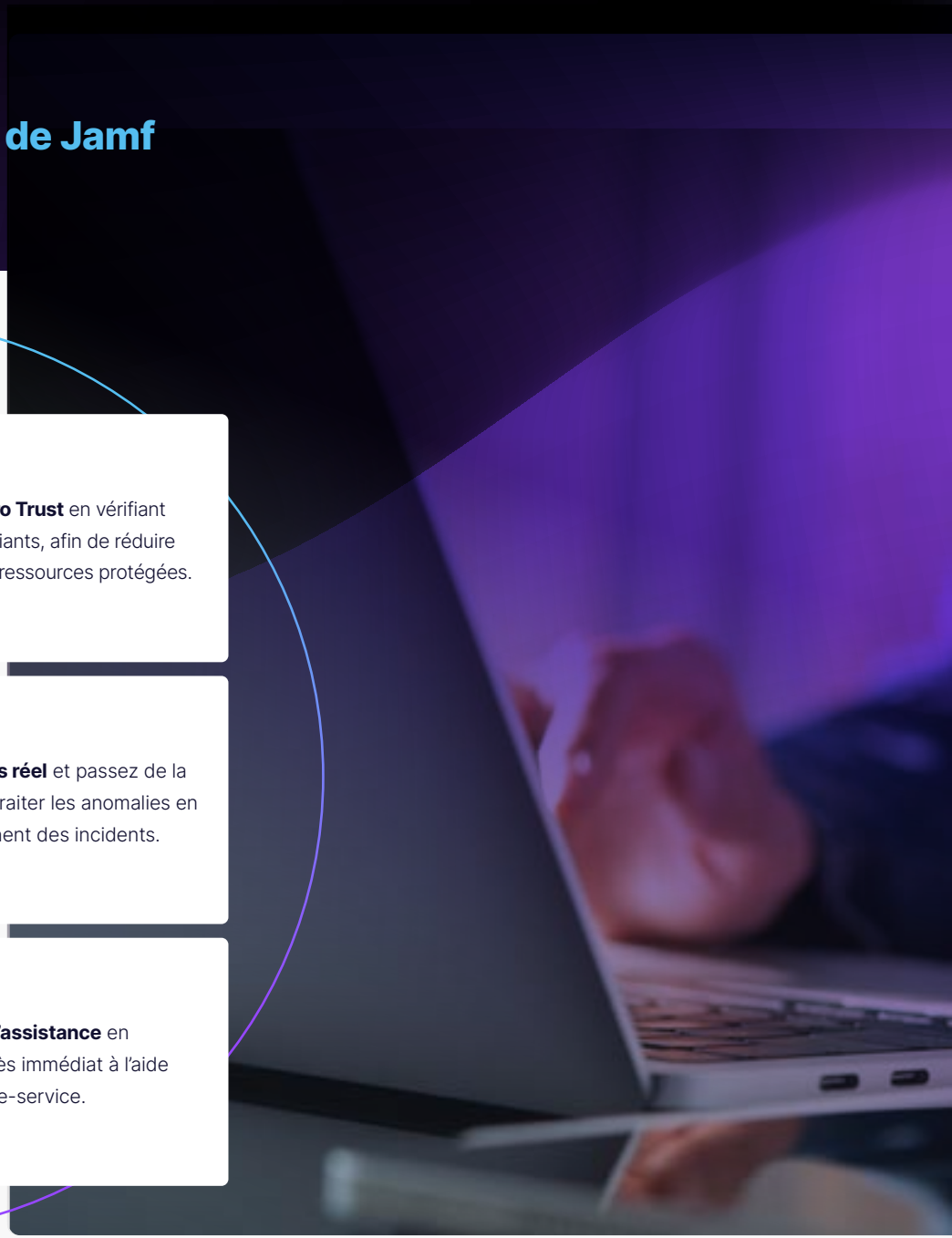
Mettez en œuvre le principe **Zero Trust** en vérifiant l'état des appareils et des identifiants, afin de réduire les risques d'exposition pour les ressources protégées.

Appliquez des configurations de référence sécurisées et des optimisations propres à chaque rôle dès la première connexion.

Obtenez une **visibilité en temps réel** et passez de la réactivité à la proactivité, pour traiter les anomalies en amont avant qu'elles ne deviennent des incidents.

Tenez automatiquement les logiciels à jour pour minimiser les temps d'arrêt et maximiser la conformité.

Allégez la charge du service d'assistance en donnant aux utilisateurs un accès immédiat à l'aide dont ils ont besoin grâce au libre-service.



Une intégration simple et fluide pour être productif dès le premier jour

Pour le service informatique, le processus de provisionnement manuel classique se déroule généralement comme ceci :

1. **Acheter le matériel.**
2. **Déballer les appareils.**
3. **Rassembler les appareils pour les préparer.**
4. **Suivre les écrans de configuration initiale.**
5. **Installer :**
   - Les mises à jour de l'OS
   - Les applications
   - La sécurité des points de terminaison
6. **Configurer :**
   - Les paramètres matériels
   - Les paramètres logiciels
   - Les profils de référence sécurisés
7. **Vérifier que les points de terminaison sont surveillés.**
8. **Attribuer chaque appareil à son utilisateur final.**
9. **Vérifier que l'utilisateur final peut s'authentifier.**
10. **Vérifier que l'utilisateur final a accès aux outils nécessaires.**

En théorie, ces dix étapes peuvent sembler relativement simples lorsqu'il s'agit de préparer l'appareil d'un nouvel employé. Mais en pratique, une organisation qui gère plus de 1 000 appareils sera nécessairement réticente à l'idée de suivre ce processus, même pour une dizaine d'appareils, en raison de l'impact que cela représente en termes de temps, de productivité et de budget.

Et selon les besoins de l'entreprise, les étapes 5 et 6 peuvent à elles seules prendre plusieurs heures par appareil. Autrement dit, une tâche consistant simplement à appliquer les correctifs du système d'exploitation et des logiciels, à installer une suite de productivité à configurer des réglages de conformité peut facilement occuper une demi-journée de travail – surtout si l'on pense à tous les redémarrages.

Quelle solution pour éviter d'impacter les ressources ?

Une stratégie d'intégration qui unifie la gestion, l'identité et la sécurité pour automatiser le provisionnement en fonction du rôle de l'utilisateur final, avec un déploiement sans intervention. Non seulement cela réduit à quelques minutes seulement le temps qu'un nouvel employé doit attendre pour que son matériel soit utilisable, mais cela diminue considérablement le délai avant lequel il peut se mettre au travail.

Le résultat :

- **Une intégration rapide**, sans attendre l'assistance du service informatique.
- Les employés ne sont pas obligés de récupérer leur appareil au bureau.
- Les erreurs humaines et la fatigue liée aux tâches répétitives sont éliminées.
- Les employés sont productifs et actifs dès leur premier jour.
- Des workflows efficaces font gagner du temps et de l'argent aux entreprises.

Pourquoi Jamf ?

Jamf propose un workflow à la fois souple et puissant qui évite au service informatique de perdre du temps à résoudre les tickets d'assistance liés à l'intégration. En rassemblant les tâches d'installation courantes dans un modèle de déploiement automatisé, le service informatique met en place des workflows plus efficaces et conviviaux pour les utilisateurs finaux. Ceux-ci vont en effet inscrire eux-mêmes leur appareil et accéder aux logiciels, aux outils et aux configurations dont ils ont besoin, sans attendre et en toute sécurité, grâce à Self Service.

Des règles d'accès qui protègent les données sans ralentir les utilisateurs

Les listes de contrôle d'accès (ACL) constituent la pierre angulaire de la sécurité des données ; ce sont elles qui déterminent si un compte d'utilisateur doit ou non être autorisé à accéder à une ressource protégée. Il est d'usage de prendre en compte le nombre d'appareils pour déterminer les effectifs d'assistance informatique. Mais lorsqu'il s'agit d'identité, c'est le nombre d'utilisateurs pris en charge qui sert à élaborer une stratégie de sécurité des données.

Dans une configuration manuelle, le chiffre clé est le nombre d'autorisations nécessaires, multiplié par le nombre total d'utilisateurs finaux. L'expansion des effectifs s'accompagne mécaniquement d'une augmentation du nombre d'autorisations à traiter manuellement. Cela produit un impact immédiat sur les performances, qui entraîne des retards considérables et accroît les risques d'erreur humaine, notamment en raison de la fatigue induite par les processus répétitifs. D'autre part, comme cette pratique impose à l'équipe informatique de traiter manuellement chaque changement, tout ce qui déclenche une modification (promotion d'employé, évolution de la tolérance au risque, etc.) implique une intervention sur le compte concerné et, souvent, sur l'appareil associé. On comprend que cette méthode ne soit pas viable à grande échelle.

Quelle est la solution optimale et évolutive ?

L'intégration de la gestion des accès aux identités (IAM) avec la gestion des appareils et la sécurité des points de terminaison permet de répondre aux besoins des entreprises avec une grande souplesse. Elle allège également les efforts manuels liés aux changements en proposant un modèle de sécurité centralisé. Celui-ci s'appuie sur le contrôle d'accès basé sur le rôle (RBAC) pour déterminer l'accès des utilisateurs aux ressources en fonction de leur rôle plutôt que de leur identité ou de leur appareil.

Le résultat :

- **L'attribution des autorisations** est simplifiée ; elle se fait sur la base du rôle de l'utilisateur et des groupes auxquels il appartient, à partir d'un référentiel central.
- Le principe du moindre privilège est appliqué, **afin de limiter les accès** à ce qui est nécessaire, sans plus.
- Les droits d'accès s'appliquent lors de l'**authentification de l'utilisateur**, puis le suivent au fil des changements d'appareil et de rôle.
- **Les efforts d'administration sont réduits**, même à grande échelle, car chaque changement n'est traité qu'une seule fois par le service informatique.
- Les contrôles d'audit sont **simplifiés** grâce à la centralisation de la visibilité et de la journalisation de conformité.

Pourquoi Jamf ?

Grâce à la prise en charge native des fournisseurs d'identité cloud (IdP), les contrôles de sécurité centralisés qui régissent les identifiants des utilisateurs et les points de terminaison s'appliquent également à votre instance Jamf. Jamf s'appuie sur l'intégration de l'identité pour offrir une expérience utilisateur parfaitement fluide. De plus, la plateforme applique les stratégies IAM aux appareils Mac et mobiles qui accèdent aux ressources de l'entreprise, aux côtés des PC Windows. Le résultat : un paradigme d'identité véritablement unifié, à la fois personnalisable et évolutif.

Gérer le cycle de vie des applications sans le chaos

Les solutions logicielles professionnelles constituent l'un des facteurs les plus importants de l'expérience utilisateur. Mais il faut concilier :

- **Les besoins de l'entreprise,**
- **La diversité des systèmes d'exploitation,**
- **Les préférences de l'utilisateur,**
- **Les différents types d'appareils.**

Autrement dit, la voie de la conformité est semée d'embûches. Quant à la prise en charge des applications natives, du code interne et des logiciels hébergés dans le cloud, elle multiplie encore les obstacles.

Quand il faut gérer les correctifs pour plusieurs systèmes d'exploitation différents, en comptant les mises à jour de sécurité et d'applications, une tâche de quelques minutes peut aisément devenir un projet de plusieurs heures ou plusieurs jours quand l'ampleur du parc dépasse les capacités de l'équipe informatique.

Même avec un faible nombre d'appareils par membre de l'équipe, ces procédures de mise à jour manuelles empêchent les utilisateurs finaux de travailler et exposent les organisations à divers types de risques :

- **Vulnérabilités non corrigées** liées à des retards dans les mises à jour
- **Logiciels défectueux** en raison de mises à jour incomplètes
- **Posture de sécurité affaiblie** par les incohérences dans l'application des correctifs
- **Utilisation d'applications** non contrôlées ou non approuvées (shadow IT)
- **Intégrité** des applications compromise ou **installations** d'applications non sécurisées

Quelle solution harmonise la gestion du cycle de vie des applications ?

Avec une stratégie qui centralise le déploiement des applications, tout en intégrant la visibilité des terminaux, l'application des règles de conformité et l'automatisation des mises à jour logicielles, les appareils restent à jour sans effort pour les utilisateurs. Les vulnérabilités connues susceptibles de compromettre les données de l'entreprise sont systématiquement atténuées dans l'ensemble de l'infrastructure, quels que soient le système d'exploitation et le type d'appareil.

Le résultat :

Les informations d'inventaire sont **mises à jour en temps réel**, ce qui permet de savoir quelles applications et quelles versions sont installées sur les appareils gérés.

Les applications **proviennent de développeurs légitimes** ; leur authenticité et leur intégrité sont vérifiées par des signatures numériques.

Les logiciels sont installés de façon native et **mis à jour automatiquement**, pour alléger la charge de l'équipe informatique et simplifier le cycle de vie des applications gérées.

La **conformité** est assurée par des règles qui veillent à ce que les applications gérées soient disponibles et configurées de la même manière sur tous les appareils pris en charge.

Les pistes d'audit sont **simplifiées**. Grâce à la journalisation unifiée, la conformité est démontrée et les preuves sont faciles à partager avec les auditeurs.

Pourquoi Jamf ?

Pour être performante, une stratégie de gestion des correctifs doit être sûre, efficace, évolutive et cohérente. Avec les programmes d'installation des apps de Jamf, tous ces avantages sont respectés et associés à une automatisation, afin de maintenir la conformité et d'appliquer les configurations sécurisées aux points de terminaison lors du déploiement de logiciels tiers. Cette approche s'ajoute à des règles puissantes et flexibles, qui s'appuient sur des critères de référence pour maintenir les systèmes d'exploitation à jour. Cette combinaison renforce la posture des appareils afin de l'aligner sur la sécurité globale de l'entreprise.

Arrêter les menaces avant qu'elles n'atteignent l'utilisateur

Rien de pire pour la productivité qu'une menace qui bloque l'accès aux données, ralentit la connectivité internet ou compromet l'intégrité des données de l'entreprise – quand ce n'est pas les trois à la fois.

Les trois sections précédentes traitent du déploiement des appareils, des droits d'accès et de la gestion du cycle de vie des applications. Dans cette section, nous nous intéressons à la défense contre les menaces et à la prévention, essentielles pour maintenir la productivité des employés face aux malveillances modernes. Les menaces sophistiquées, en particulier, ciblent aussi bien les appareils mobiles, les plateformes et les services cloud pour cibler les utilisateurs d'entreprise, qu'ils travaillent au bureau ou à distance.

Il est crucial d'apporter une réponse efficace aux incidents pour éviter que les menaces ne se transforment en catastrophes. Malheureusement, lorsqu'un point d'accès vulnérable est compromis, l'utilisateur final en subit déjà les conséquences. Quant à la correction, elle va, elle aussi, apporter son lot de perturbation et prolonger les délais de rétablissement. **Le résultat :**

- Une **perte** de **productivité**,
- Qui entraîne des **temps d'arrêt** prolongés,
- **Aggrave l'impact** sur toutes les équipes,
- **Nuit** aux opérations de l'entreprise,
- Ce qui entraîne une **perte de revenus**,
- **Érode** la confiance des clients,
- Et accroît les **coûts de** remédiation.

Quelle solution permet au service informatique de garder une longueur d'avance sur les menaces ?

Pour arrêter efficacement une menace, il faut d'abord être en mesure de l'identifier. Qu'il s'agisse d'une application non conforme ou d'un paramètre désactivé par un utilisateur, la clé de la prévention des risques pour les données de l'entreprise consiste à neutraliser la vulnérabilité.

Il faut :

- **Une surveillance active** des données de télémétrie contextualisées et de l'intégrité des terminaux.
- Une vision approfondie des matrices de risques des points d'accès **afin d'évaluer la gravité des menaces et de les hiérarchiser**
- **De la visibilité sur les appareils** qui accèdent aux ressources sécurisées, qu'il s'agisse d'appareils gérés ou non.
- **L'intégration des** solutions pour créer une stratégie unifiée de gestion des appareils, des identités et de la sécurité des points de terminaison.
- **Des technologies d'apprentissage automatique** (ML) pour renforcer l'identification et la résolution des menaces inconnues et les exploiter à grande échelle.

Pourquoi Jamf ?

Jamf valide la conformité des points de terminaison grâce à plusieurs couches de protection. La supervision en temps réel permet de contrôler l'état de santé de l'appareil. Les détections sont enregistrées et signalées au service informatique pour prévenir l'exposition des ressources de l'entreprise. Ces données sont utilisées pour remédier au risque en mettant automatiquement l'appareil en conformité. Le problème est résolu en coulisses pour l'utilisateur final, sans intervention du service informatique.

Zéro temps d'arrêt : préserver la productivité des employés et la fluidité des revenus

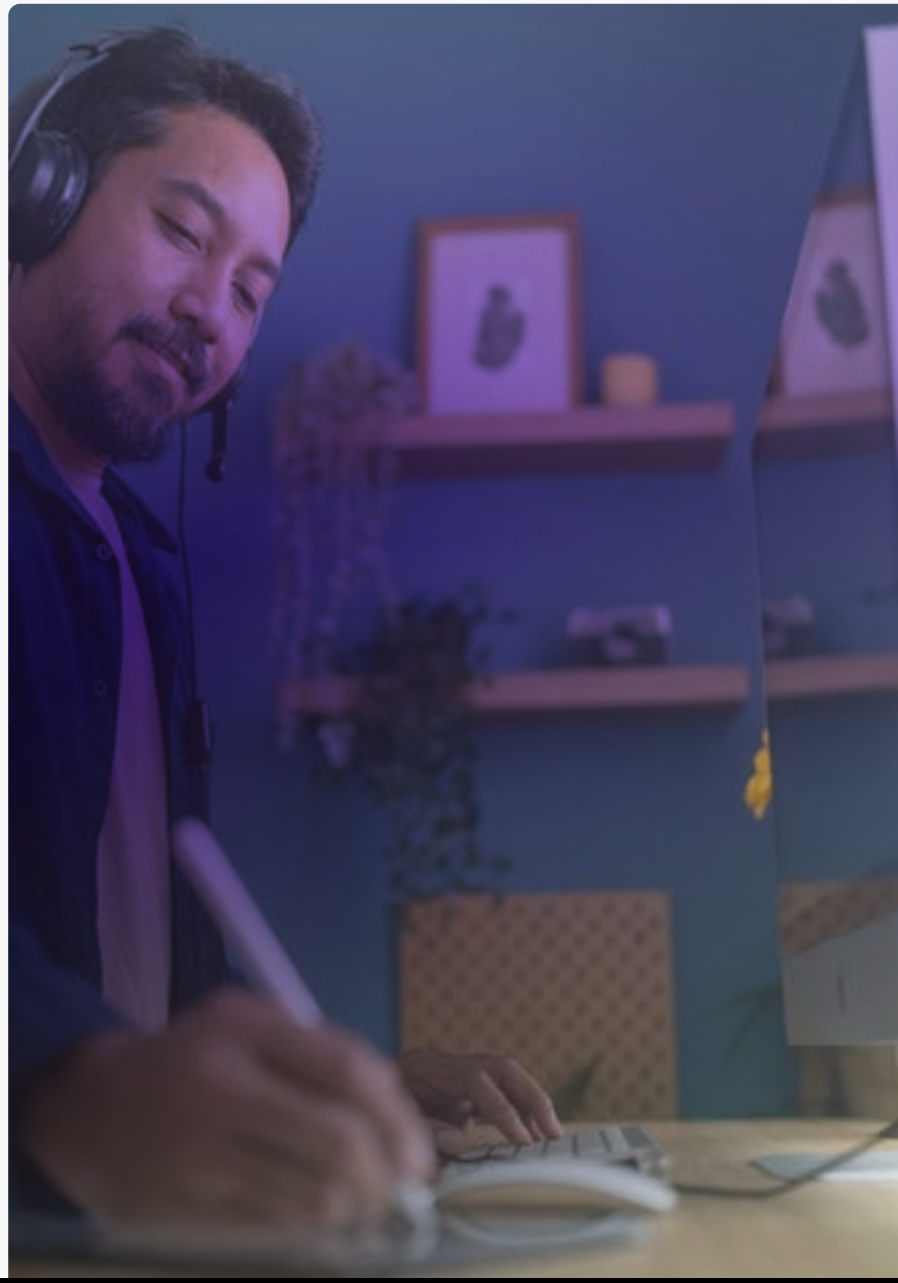
Les entreprises ont des environnements complexes :

- **Prise en charge multi-plateforme**
- **Appareils de bureau et mobiles**
- **Technologies cloud et hybrides**
- **Équipes dispersées**
- **Multiplicité des modèles de propriété**

Tous ces facteurs sont autant de défis pour les stratégies de gestion globales. Qu'il s'agisse de préserver la productivité des équipes hybrides, d'intégrer étroitement les solutions de différents fournisseurs ou d'étendre la sécurité à l'ensemble de l'infrastructure, le service informatique des entreprises doit surmonter de nombreuses complexités pour soutenir le développement des activités de l'entreprise.

Les entreprises modernes qui exercent leurs activités sur la scène mondiale ont souvent des systèmes tentaculaires. Leurs différents efforts stratégiques composent une vaste initiative de transformation numérique.

L'époque où un pare-feu, un antivirus, un domaine sur site et une connexion VPN suffisaient à sécuriser le trafic dans l'enceinte du réseau est révolue. Aujourd'hui, chaque domaine exige des solutions dynamiques et flexibles pour gérer et sécuriser efficacement les appareils et tous les systèmes d'exploitation, partout dans le monde, tout en offrant aux utilisateurs un accès pratique et sûr aux ressources, doublé de protections et de garanties de confidentialité.



Quelle solution permet de sécuriser dynamiquement les ressources protégées sur l'ensemble des plateformes ?

Les solutions existantes sont souvent lacunaires et créent des risques de violation des données. Les entreprises d'aujourd'hui ont besoin de technologies flexibles, basées sur des architectures Zero Trust pour tirer parti de l'IAM, de la gestion des appareils et de la sécurité des points de terminaison ; le but étant d'offrir une solution complète qui va au-delà de l'atténuation des menaces pour assurer la conformité.

Il faut donc :

- Passer d'un modèle de confiance implicite à un modèle où **l'accès est refusé par défaut** ; autrement dit, ne jamais faire confiance, toujours vérifier.
- **Valider explicitement les identifiants** et **l'état de l'appareil** à chaque fois demande d'accès.
- Ajouter une couche de **connaissance contextuelle** pour lutter contre les menaces sophistiquées grâce à l'analyse comportementale.
- Mettre en œuvre des **défenses au sein du réseau** qui isolent le trafic au sein de microtunnels uniques, pour empêcher l'espionnage et les mouvements latéraux.
- **Accélérer** la réponse aux incidents et automatiser les workflows de remédiation pour réduire les temps d'arrêt.

Pourquoi Jamf ?

Avec l'accès réseau « zero trust » (ZTNA) de Jamf, la protection contre les menaces modernes s'étend à tous les types d'appareils pris en charge. Toutes les plateformes bénéficient de la même protection, et les stratégies de sécurité sont appliquées de façon homogène à l'ensemble du parc, quelles que soient la localisation et la connectivité réseau des appareils. En incorporant plusieurs couches de défenses dès la conception, les utilisateurs finaux bénéficient d'un accès natif aux ressources de l'entreprise. Quant aux équipes informatiques, elles peuvent compter sur un meilleur alignement entre les opérations commerciales et les exigences de conformité.

Minimiser les tickets d'assistance pour maximiser la productivité des utilisateurs

L'une des principales missions du service informatique est de répondre aux besoins des utilisateurs. Dans la plupart des organisations, le nombre d'employés dépasse largement celui des professionnels de l'informatique. C'est pourquoi la capacité du service informatique à trier et résoudre les problèmes avec rapidité et efficacité est fortement influencée par des facteurs tels que :

- **Le débit moyen des tickets**
- **L'efficacité des workflows**
- **La taille de l'équipe**
- **La culture d'entreprise**
- **Les compétences de ses membres**

La moindre défaillance est exacerbée par un désalignement de ces aspects. Il en découle une baisse de l'efficacité des opérations commerciales et des problèmes de conformité aux objectifs de l'entreprise.

Ces effets s'inscrivent sur le long terme, mais les personnes concernées ressentent des effets plus immédiats ; elles sont souvent ralenties dans leur travail par :

- Des logiciels **non installés**
- **Des paramètres** mal configurés
- **Des autorisations** incorrectes
- Des messages **d'erreur** système
- Des incompatibilités **matérielles**

Quelle solution transforme l'informatique en moteur de productivité ?

La sagesse nous dit que ce n'est pas en augmentant les droits d'accès des utilisateurs qu'on améliore leur expérience. En essayant de « résoudre » un problème, il arrive que l'équipe informatique ouvre la porte à un risque plus grave et augmente la probabilité d'atteinte aux données et d'incidents de sécurité.

En revanche, elle peut mettre en place un référentiel centralisé permettant aux utilisateurs de résoudre eux-mêmes leurs problèmes non techniques et d'obtenir sans attendre les solutions dont ils ont besoin. Cette approche libère les équipes et leur permet de consacrer leurs compétences à l'amélioration des workflows, pour doper la productivité des utilisateurs et soutenir les objectifs de l'entreprise.

Le principe :

- Les **parties prenantes sont incluses dans la solution** au lieu d'être perçues comme une source de problèmes.
- Les utilisateurs finaux peuvent **installer des applications approuvées** et **configurer des paramètres validés** sans compromettre les schémas d'autorisation.
- Les **mises à jour des applications** sont automatisées à l'aide d'une boutique conviviale qui permet de les appliquer en un clic.
- La boutique de l'entreprise est reliée aux **IdP basés sur le cloud** pour faciliter davantage le processus pour les utilisateurs.
- On met à disposition une **boutique native** en phase avec l'expérience des utilisateurs, et complétée par des notifications en cas de mise à jour disponible.

Pourquoi Jamf ?

Self-Service+ pour Mac, iPhone et iPad est une boutique d'entreprise native d'Apple et personnalisable. Applications, outils, scripts, ressources, imprimantes et mises à jour sont accessibles d'un simple clic, sans aucune autorisation administrative supplémentaire. Grâce à l'intégration avec l'IdP, le service informatique peut approuver temporairement les demandes sans dégrader la conformité à long terme ; une piste d'audit complète est toujours conservée.

Conclusion

Les organisations productives éliminent les frictions des opérations informatiques et de l'expérience des employés. En unifiant la gestion des appareils, la gestion des identités et la sécurité des points de terminaison, les entreprises peuvent automatiser l'intégration, appliquer des contrôles d'accès cohérents, maintenir l'intégrité des applications et prévenir les menaces avant qu'elles ne perturbent le travail. Jamf offre ces capacités par le biais de workflows conçus pour s'adapter à des parcs d'appareils diversifiés et pour préserver la productivité et la sécurité des utilisateurs. Avec le déploiement sans intervention, des protections proactives et un Self Service qui permet aux employés de résoudre eux-mêmes les problèmes courants, l'équipe informatique réduit les lourdeurs opérationnelles tout en renforçant la conformité et la résilience de l'entreprise. Le résultat : un environnement sécurisé et simplifié, dans lequel les employés peuvent fournir un travail utile dès le premier jour.

Points clés à retenir

- **Accélérez l'intégration dans les grands parcs d'appareils :** le déploiement sans intervention permet de fournir des appareils prêts à l'emploi sans avoir à procéder à un provisionnement manuel fastidieux.
- **Élargissez les accès sans ralentir les utilisateurs** : l'accès basé sur le rôle aligne automatiquement les autorisations sur l'identité au fil de la croissance de l'entreprise.
- **Préservez la santé des applications sur des milliers de points de terminaison :** l'automatisation des correctifs et des mises à jour assure la sécurité des logiciels sans perturber la productivité.
- **Arrêtez les menaces avant qu'elles n'interrompent les opérations** : la surveillance continue et l'application de la conformité réduisent les temps d'arrêt dans les équipes distribuées.
- **Autonomisez les utilisateurs tout en allégeant la charge de travail du service informatique** : le Self Service leur permet d'installer des applications approuvées et de résoudre des problèmes courants sans créer de nouveaux tickets.
- **Offrez une expérience cohérente sur toutes les plateformes, partout dans le monde** : les workflows unifiés préservent la sécurité et la productivité des appareils, que les employés travaillent au bureau ou à distance.

Vous voulez voir tout cela en action ?

Découvrez Jamf dès aujourd'hui.