

 jamf

La gestion des règles et de la conformité

pour les débutants

Plus que jamais, les entreprises doivent aider leurs employés à travailler à distance ou dans un environnement hybride, et cela nécessite plus qu'une gestion des appareils de base. Les appareils mobiles d'entreprise permettent de travailler partout et à tout moment, mais cette flexibilité pose le risque d'une trop grande utilisation personnelle des appareils professionnels, même si vous avez autorisé cette utilisation sur les forfaits cellulaires de l'entreprise.

Jamf Data Policy aide les organisations à autoriser et à gérer le télétravail en assurant la productivité des utilisateurs, où qu'ils soient et quels que soient les appareils qu'ils utilisent, dans des environnements hybrides et à distance.

Grâce à ces technologies, les organisations peuvent :

- Mettre en place des règles personnalisables pour assurer la conformité
- Configurer des plafonds de données et des alertes de dépassement
- Filtrer les contenus inappropriés
- Élargir les règles à toutes les communications réseau
- Surveiller et éliminer le Shadow IT
- Gérer l'utilisation en temps réel



Découvrez tout ce que vous devez savoir pour établir une politique d'utilisation acceptable et gérer vos données et appareils de manière à répondre aux besoins de votre entreprise et de vos utilisateurs finaux.

La gestion des appareils est souvent considérée comme une tâche très scientifique. Une tâche reposant sur toutes sortes de données pour arriver à un niveau de gestion optimal, permettant de garantir que les appareils, les utilisateurs et les données seront protégés et le resteront. Bien que nous ne contestons pas cet aspect scientifique, il faut aussi un peu de « magie » pour être un bon administrateur informatique. Une magie qui mélange l'expérience et une compréhension approfondie des besoins uniques de chaque réseau. Après tout, malgré les standards et les bonnes pratiques, chaque réseau est un îlot indépendant, fonctionnant selon les règles spécifiques de son organisation.

« La magie, ça n'existe pas ! » — Oncle Vernon

Lorsque tous vos appareils fonctionnent de manière optimale, cela vous semble magique ?

Les données sont sécurisées, et les applications et ressources d'entreprise sont accessibles, tout en étant protégées. Les utilisateurs sont heureux, ils peuvent utiliser des appareils sécurisés pour accomplir leurs tâches professionnelles et personnelles, sans que des pratiques de gestion compliquées les empêchent d'être productifs ou d'apprécier leurs temps de pause. Et lorsque des problèmes sont détectés, ils sont automatiquement corrigés sans que l'équipe informatique ait à lever le petit doigt ou que l'utilisateur final le remarque.

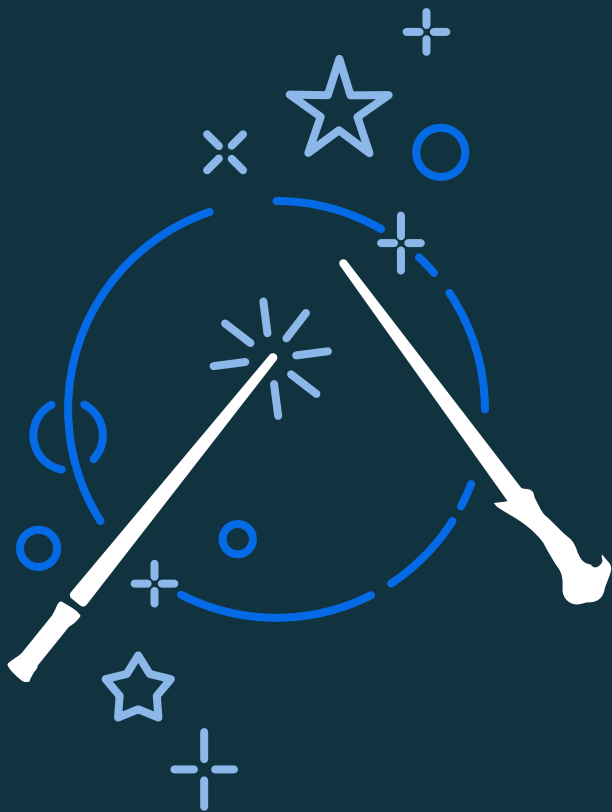


C'est ce type de magie que les administrateurs d'appareils mobiles utilisant Jamf Data Policy exercent. Au-delà de la gestion de base, Jamf Data Policy permet aux organisations d'assurer leurs pratiques professionnelles dans des environnements de travail à distance et hybrides. Quel que soit le type d'appareil, qu'il s'agisse d'un appareil personnel dans le cadre d'un programme BYOD (Bring your own device) ou d'un appareil d'entreprise pour lequel une utilisation personnelle est autorisée, il est essentiel de disposer d'une politique d'utilisation acceptable, ainsi que de moyens pour la gérer et la faire appliquer.

Voici quelques conseils pour commencer à créer ou à évaluer votre politique d'utilisation acceptable. Déterminez comment votre organisation peut :

- Permettre aux administrateurs de surveiller la consommation des données grâce à des analyses en temps réel et à des rapports granulaires
- Faire appliquer des politiques d'utilisation acceptable
- Éliminer le Shadow IT
- Filtrer le contenu
- Mettre en place des règles de protection personnalisées pour répondre aux besoins de vos utilisateurs et de votre organisation
- Prendre en charge votre réseau de manière globale, quel que soit le type d'appareil ou de propriété



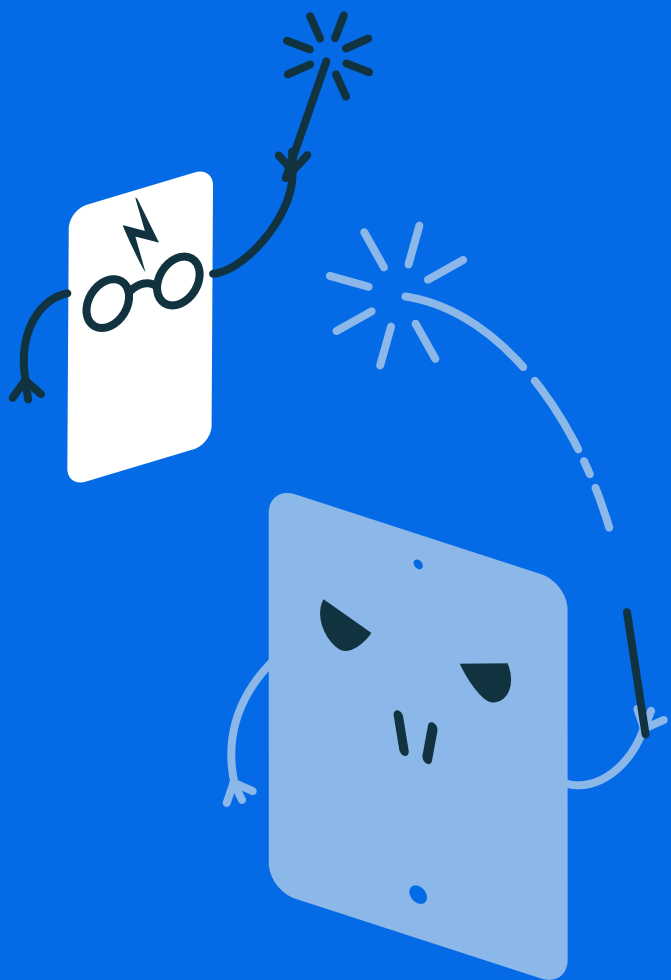


HARRY POTTER CONTRE VOLDEMORT

Avant d'explorer toutes les fonctionnalités de Jamf Data Policy, découvrons certaines des raisons pour lesquelles il est nécessaire d'aider votre organisation à gérer le parc d'appareils mobiles sur son réseau. Et comment mieux décrire le cas d'utilisation qu'en invoquant le plus grand des magiciens modernes, Harry... Potter, bien sûr !

Dans la série de livres écrits par J.K. Rowling, les magiciens ont un point commun avec les administrateurs informatiques : ils doivent faire un choix. En l'occurrence, choisir le camp de Voldemort ou celui d'Harry. Laissez-nous vous expliquer tout ça.

Si vous choisissez la méthode de Voldemort, votre organisation maintient l'ordre d'une main de fer. Elle force les utilisateurs à s'adapter à vos règles en dépit de leurs besoins ou des potentielles conséquences fâcheuses.



Mais si vous choisissez le camp d'Harry, votre organisation favorise l'équité et la justice, en acceptant les compromis et en valorisant la coopération pour résoudre les problèmes globaux.

« **Bientôt nous aurons tous à choisir entre le bien... et la facilité.** »

– Albus Dumbledore

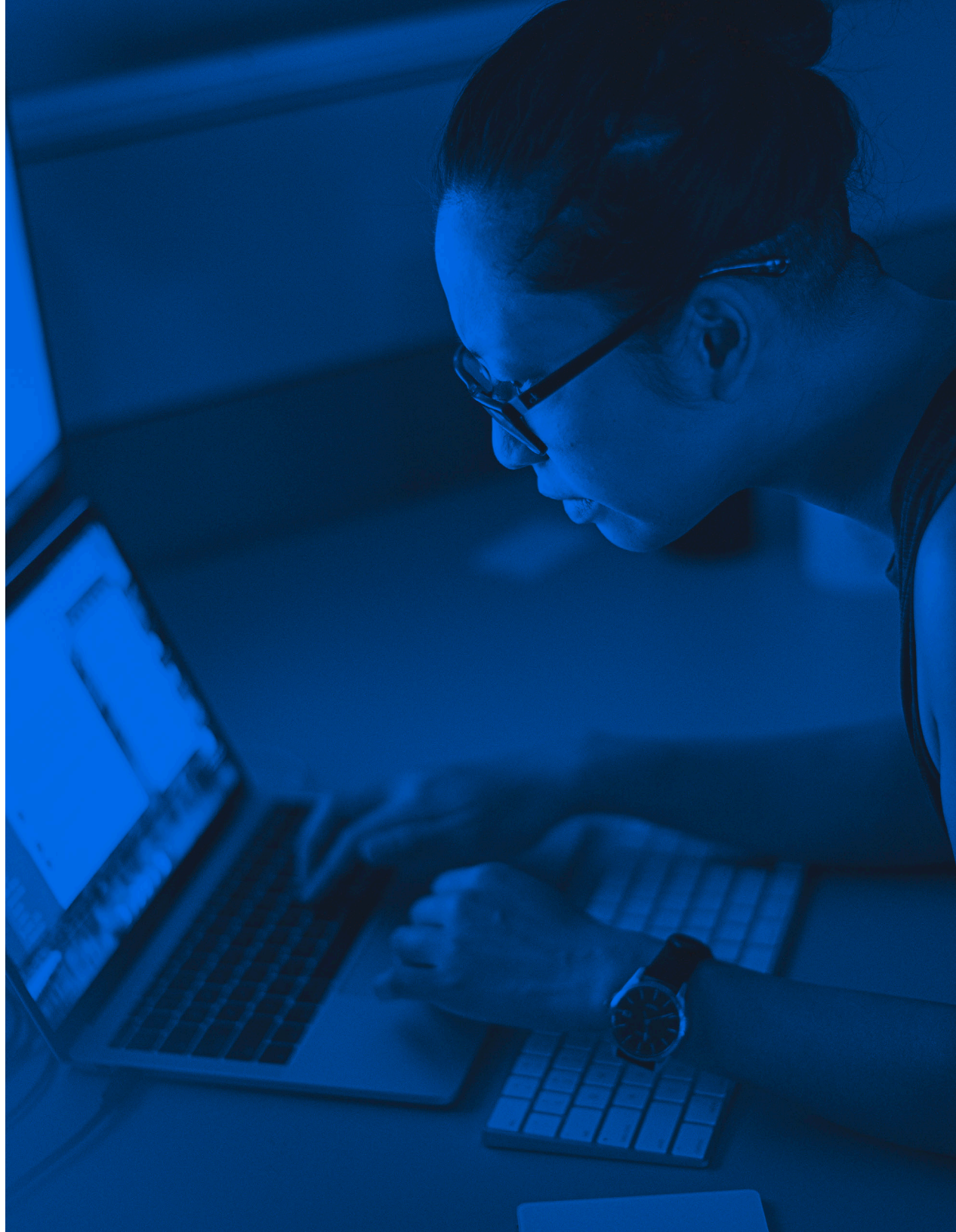
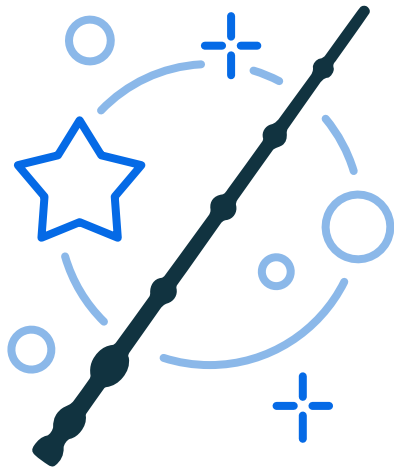
Bien qu'il soit facile pour l'équipe informatique de choisir la voie de Voldemort au nom de la sécurité et de la protection des utilisateurs, la réalité est que, souvent, la deuxième voie offre plus d'options pour assurer la sécurité des données et des utilisateurs. En effet, tous les acteurs travaillent ensemble pour atteindre l'objectif commun et n'ont pas à lutter contre des contrôles excessifs ou restrictifs, qui réduisent la productivité et frustrent les utilisateurs sans pour autant assurer une protection satisfaisante.

Comme nous l'avons déjà dit, chaque réseau est unique et respecte un ensemble différent de règles, de lois et de réglementations. Ainsi, en matière de règles et de gestion des données, il n'existe pas de solution adaptée à tous. Gérer les appareils selon la méthode de Voldemort ne fera qu'enfermer l'équipe informatique dans une approche limitée, supprimant la flexibilité nécessaire pour surveiller, détecter et corriger les éventuels problèmes rencontrés dans le monde dynamique de l'informatique. Vous n'êtes pas d'accord ?

LA BAGUETTE DE SUREAU

Comme Harry Potter, les administrateurs informatiques ne sont que des êtres humains. Des hommes et des femmes ordinaires, avec des compétences certes fantastiques, mais qui doivent être canalisées pour exprimer leur plein potentiel. Harry avait la Baguette de bureau. Vous avez Jamf Data Policy.

Nous allons explorer plus spécifiquement deux fonctionnalités qui offrent aux organisations les défenses nécessaires pour gérer leurs appareils mobiles de A à Z, de manière cohérente et efficace.



CONTRÔLE DES RÈGLES EN TEMPS RÉEL

Voici comment configurer des règles pour limiter l'accès aux contenus inappropriés et aux applications qui ne sont pas considérées comme essentielles pour l'entreprise : définir des règles de plafonnement de la consommation de données et les appliquer lorsque les seuils sont atteints ; définir les sites Web, services et applications accessibles ; offrir une visibilité sur la consommation grâce à des contrôles basés sur les catégories ; ou encore personnaliser les vérifications pour déclencher l'application automatique des règles.

D'après Jamf, plus de 50 % de la consommation de données en entreprise n'est pas directement liée aux objectifs stratégiques. Ce niveau sans précédent de visibilité sur l'utilisation de données permet aux organisations de redéfinir leurs règles d'utilisation acceptable. Elles peuvent gérer précisément les pools de données et l'utilisation du trafic réseau afin que les appareils mobiles soient utilisés comme des outils professionnels, et non comme des objets de divertissement.



« Le temps ne ralentit pas lorsque quelque chose de désagréable nous attend. »

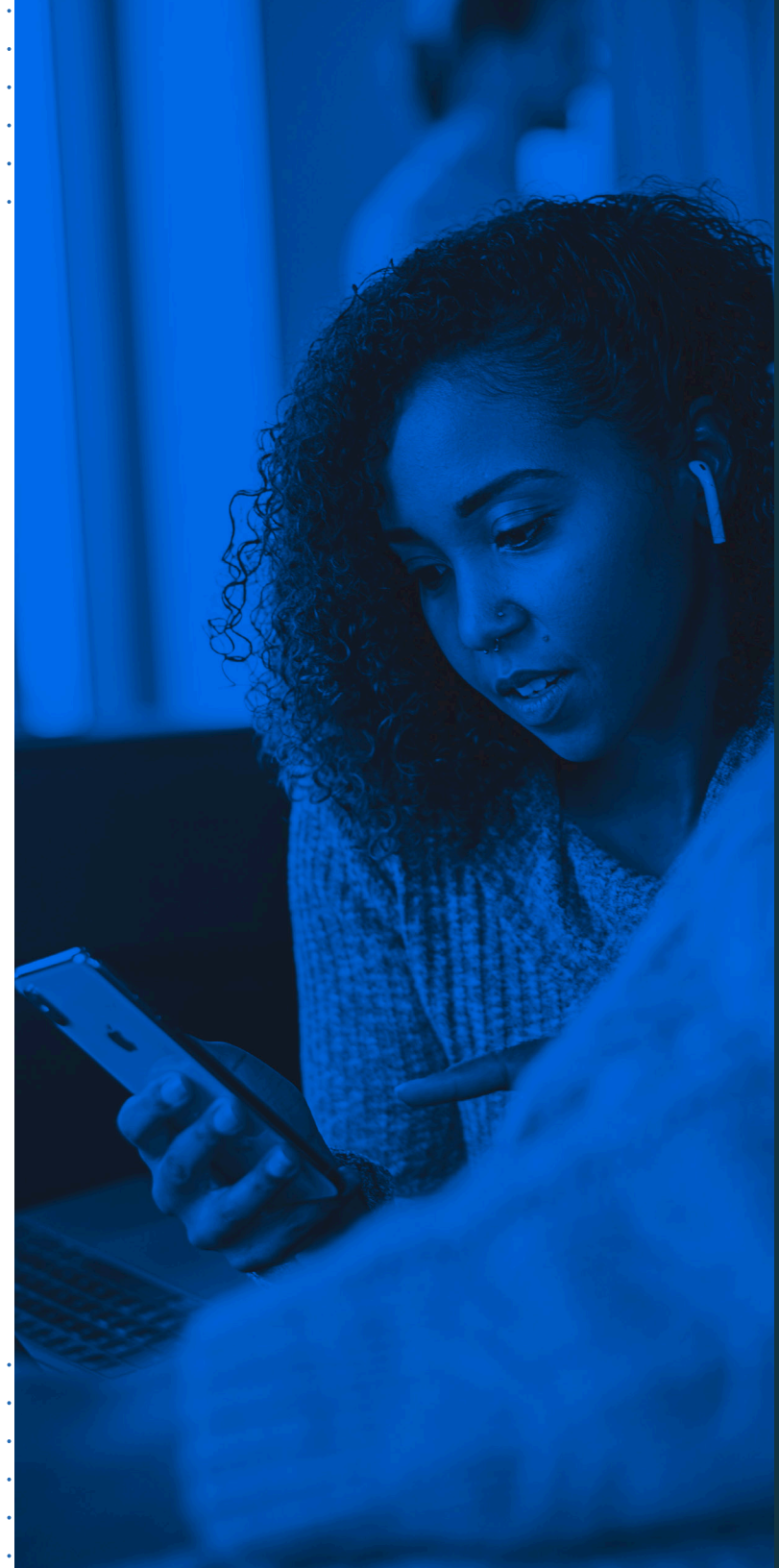
– Harry Potter et la Coupe du feu

TOUS LES APPAREILS MOBILES, TOUS LES MODÈLES DE PROPRIÉTÉ

BYOD. CYOD. COPE. Tous ces acronymes barbares se rapportent à des programmes de gestion des appareils mobiles en entreprise qui indiquent des degrés de prise en charge variés. Et comme si la difficulté de choisir un modèle de propriété ne suffisait pas, il faut en plus s'y retrouver parmi tous les types d'appareils mobiles, fournisseurs et opérateurs différents.

Avec Jamf Data Policy, tout est beaucoup plus simple.

Le seul choix que doit faire votre organisation est celui des appareils les plus adaptés à ses besoins. Quel que soit le type d'appareil, le modèle de propriété ou le système d'exploitation, Jamf prend en charge toutes les options. Le service informatique peut ainsi se concentrer sur la gestion des appareils mobiles avec une attention particulière pour les règles de sécurité et de conformité, sans se soucier d'avoir à gérer plusieurs systèmes hétérogènes (ce qui revient souvent à essayer de faire rentrer un rond dans un carré).



LA CAPE D'INVISIBILITÉ

Pour l'équipe informatique, une cape d'invisibilité pourrait s'avérer bien pratique lorsque de nombreuses demandes de support arrivent toutes en même temps. Imaginez pouvoir vous concentrer sur les problèmes à résoudre plutôt que d'avoir à traiter les vagues successives d'e-mails, de messages, d'appels et de « petites questions ».

Si cela vous fait envie, Jamf Data Policy offre plusieurs autres fonctionnalités qui pourraient vous aider à juguler le flux de requêtes en standardisant l'utilisation des ressources, en faisant respecter la conformité et en définissant les attentes des utilisateurs.

ENTIÈREMENT PERSONNALISABLE

Chaque réseau est unique, tout comme chaque organisation gère son infrastructure à sa façon et définit ses propres exigences stratégiques. Cela dépend principalement de la tolérance au risque de chaque organisation. De la même manière que les entreprises modifient leur posture de sécurité pour répondre aux risques, Jamf Data Policy permet une personnalisation complète des règles et de la façon dont elles sont mises en œuvre.

De la personnalisation des catégories de filtrage de contenu à la définition de listes d'autorisation et de blocage sur mesure, les règles peuvent être appliquées de manière globale (à l'organisation dans son ensemble) ou au cas par cas, à un seul utilisateur ou à un groupe. Tous les choix sont possibles, pour répondre aux besoins de votre organisation. Et surtout, vous seul décidez du meilleur choix pour votre entreprise.





FILTRAGE DE CONTENU

Jamf a découvert que les applications et services de jeu ou réservés aux adultes sont nettement plus susceptibles d'utiliser des connexions non chiffrées, qui peuvent exposer les organisations à des risques de fuites de données ou de non-conformité avec les organismes réglementaires. Au-delà des catégories mentionnées ci-dessus, l'accès à des contenus contenant des armes, des discours de haine ou d'autres éléments dangereux peut entraîner des conséquences civiles ou pénales graves pour les utilisateurs ou l'organisation.

Sans parler des menaces de sécurité associées au contenu Web, telles que les sites Web de phishing et autres logiciels malveillants malheureusement courants sur Internet. Le filtrage de contenu ne consiste pas uniquement à bloquer les ressources malveillantes ou inappropriées. Utilisé de manière proactive, il permet d'autoriser uniquement les données approuvées, en veillant à ce que les sites Web, services et applications acceptables soient accessibles.

De plus, il est essentiel de réduire l'exposition aux litiges et actions en justice, en gérant et en maintenant une utilisation conforme des données, et en surveillant et en bloquant l'accès aux services non autorisés. Ces services, tels que le Shadow IT, peuvent affaiblir la posture de sécurité de vos appareils et de votre réseau en divulguant par inadvertance des données sensibles de l'entreprise.

LA PIERRE PHILOSOPHALE

Cette section ne va pas malheureusement pas révéler les secrets de l'élixir de longue vie ni de la transformation du plomb en or, mais elle sera presque aussi intéressante. Nous allons présenter deux autres fonctionnalités de Jamf Data Policy qui, à leur manière, sont un peu magiques. Elles collectent des informations en temps réel, ce qui permet à l'équipe informatique de transformer ces données en mesures concrètes à prendre pour mieux s'adapter à votre parc d'appareils et mieux le gérer.

Mieux encore, ces fonctionnalités permettent d'adapter les protections au réseau. Même si de nouvelles sessions sont lancées ou des connexions existantes sont fermées, vos appareils et vos utilisateurs resteront protégés, et la conformité sera assurée sur tous les types de connexion réseau.

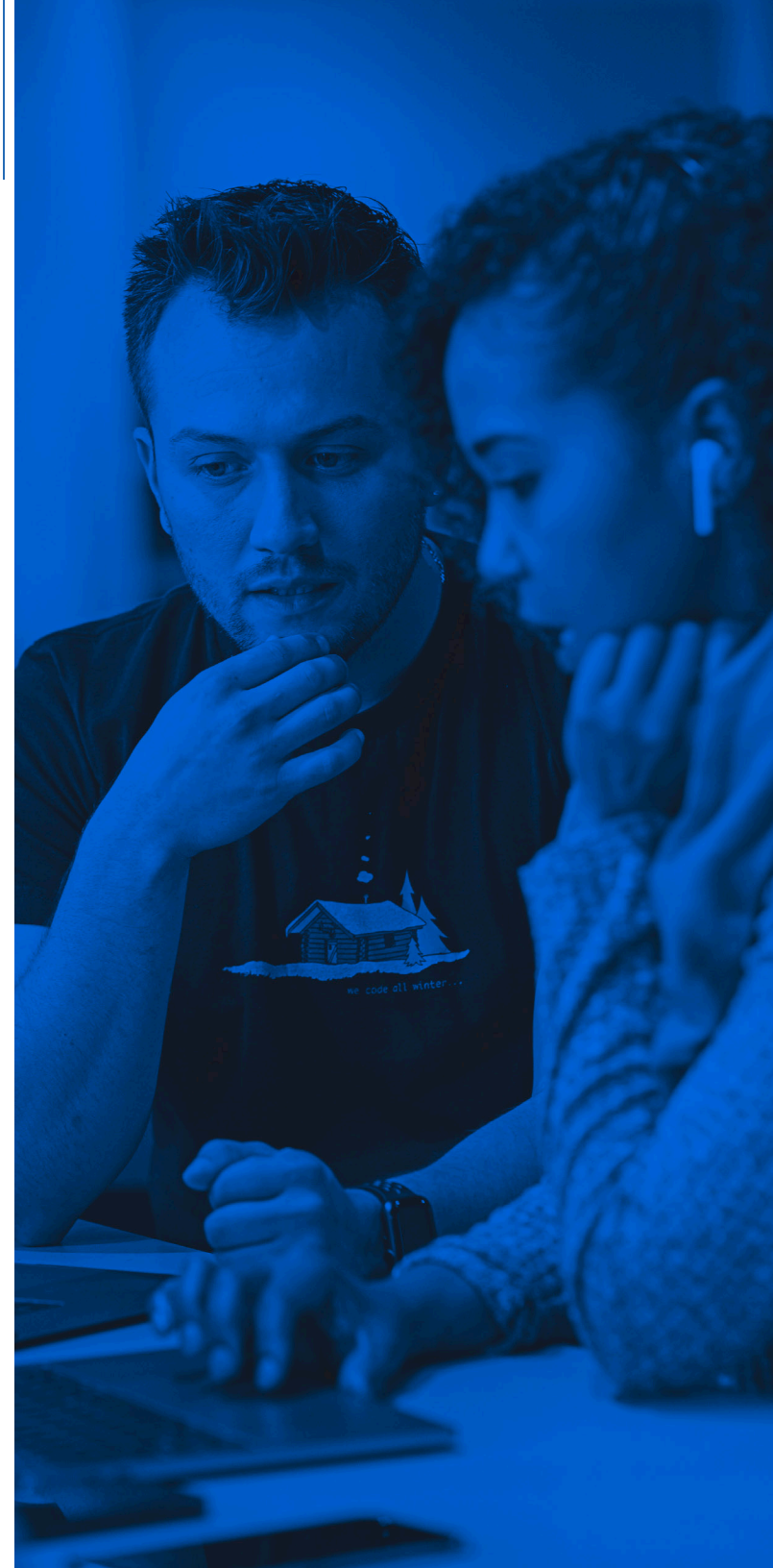


S'ADAPTE AU RÉSEAU

Comme nous l'avons déjà dit, il n'existe pas de solution unique. Les connexions réseau sur votre appareil mobile sont une parfaite illustration de ce principe. Par exemple, lorsque les utilisateurs doivent utiliser des connexions cellulaires dont l'utilisation est décomptée, ils ont plus conscience des limites de consommation, en raison des frais supplémentaires applicables pour l'itinérance ou des frais de dépassement. Cependant, s'ils peuvent se connecter à un hotspot Wi-Fi public, il est fort probable que la bande passante ne soit plus un souci.

Jamf Data Policy clarifie la gestion de ces zones d'ombre en permettant aux administrateurs de créer et de faire appliquer des règles pour différents types de connexion réseau et leurs variables spécifiques.

Imaginons que votre organisation applique le modèle COPE (corporate-owned, personally enabled) et fournisse des appareils mobiles aux employés pour leur usage personnel et professionnel, mais que le forfait de données cellulaires fasse partie d'un pool de données partagé par tous les utilisateurs. Votre organisation devra limiter la bande passante utilisée en connexion cellulaire afin que tous les utilisateurs disposent d'assez de données, sans mettre en place de gestion de la bande passante sur les connexions Wi-Fi. Jamf Data Policy permet de définir exactement ce genre de règles : limiter la bande passante en connexion cellulaire, mais pas en Wi-Fi. De plus, les règles sont assez intelligentes pour détecter quelle connexion est utilisée et s'ajuster automatiquement sans ordre supplémentaire du service informatique, et sans nuire à l'expérience de l'utilisateur final.



INFORMATIONS EN TEMPS RÉEL

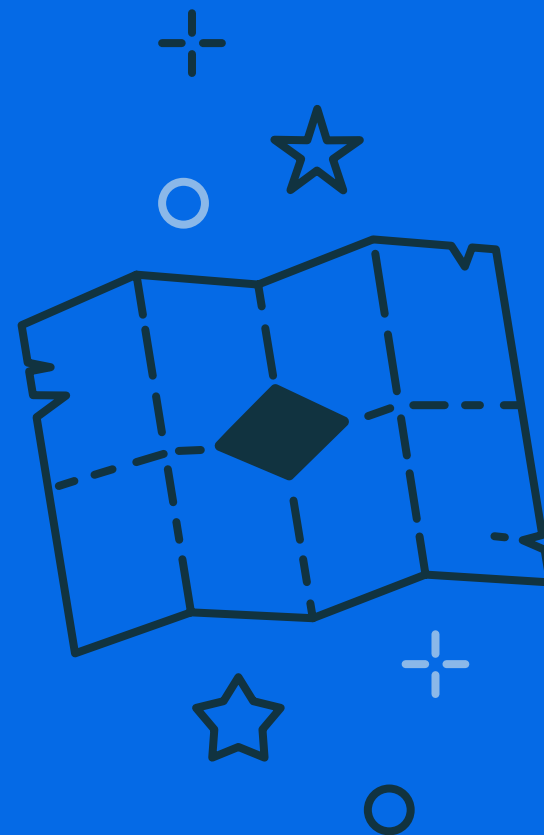
« Je jure solennellement que mes intentions sont mauvaises. »

— *Harry Potter*

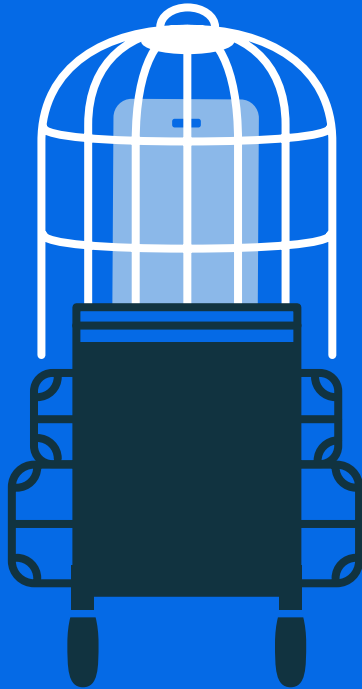
Demandez à n'importe quel administrateur s'il préfère savoir qu'une erreur est sur le point de se produire (approche proactive) ou si une erreur s'est déjà produite (approche réactive). La réponse sera probablement toujours la même : mieux vaut être informé à l'avance.

Tout le monde préfère être informé avant que quelque chose de fâcheux n'arrive, si ce n'est pour l'empêcher, au moins pour résoudre le problème aussi rapidement que possible.

Bonne nouvelle ! C'est possible avec les informations en temps réel de Jamf Data Policy. Des rapports précis informent le service informatique de la manière dont les appareils utilisent leurs données, et sur quelles connexions. Les administrateurs peuvent modifier de manière proactive les règles qui devraient être plus (ou moins) restrictives, apporter des changements aux pools de données existants, configurer le filtrage de contenu pour activer ou désactiver l'accès à certains services ou à certaines applications, ou simplement surveiller de plus près la posture de sécurité d'un appareil.



9³/₄



DÉPART SUR LE QUAI 9³/₄

L'enrôlement de votre parc de mobiles et des appareils personnels de vos utilisateurs dans Jamf Pro est un excellent point de départ pour la gestion des appareils. Mais, dans les environnements de travail modernes centrés sur le travail à distance ou hybride, la gestion des appareils physiques nécessite un outil plus spécialisé.

Cet outil, c'est Jamf Data Policy :

- Gérez l'envoi et la réception des données sur l'appareil lui-même grâce à des règles intelligentes adaptées au réseau
- Respectez la conformité réglementaire sur toutes les connexions réseau
- Filtrez le contenu avec soixante-dix modèles conçus intelligemment pour empêcher les appareils de se connecter aux sites Web, apps et services vulnérables, compromis et malveillants, en plus des contenus non approuvés

Enfin, Jamf Data Policy simplifie le travail du service informatique en éliminant le Shadow IT et en appliquant des politiques d'utilisation acceptable pour tous les appareils, quel que soit le niveau de propriété, afin de sécuriser non seulement les données mais également les appareils et les utilisateurs, sans nuire à l'expérience.

Demandez une version d'essai

Commencez dès aujourd'hui avec un essai gratuit ou contactez votre revendeur Apple habituel.

