Aperçus

Voici quelques articles qui explorent comment la gestion des appareils mobiles (MDM) peut aider votre entreprise :

Qu'est-ce que le mode kiosque ? Un guide pour verrouiller les appareils Android et Apple en entreprise

Le mode kiosque transforme les téléphones et tablettes standards en outils professionnels dédiés. Cerberus Enterprise aide les organisations à verrouiller les appareils sur une seule application ou sur un petit ensemble d'applications approuvées pour des cas d'utilisation tels que les points de vente (POS), l'enregistrement des clients ou la navigation de flotte, tout en facilitant la sécurisation, le support et la gestion à grande échelle de ces appareils spécialisés.

Comment choisir la bonne solution MDM : une liste de contrôle en 7 points pour les petites entreprises

Choisir une solution MDM tardivement dans le processus d'achat est plus facile lorsque la comparaison reste pratique. Cette liste de contrôle aide les petites entreprises à évaluer les fournisseurs selon les sept critères qui comptent généralement le plus lors des déploiements réels : la sécurité, le support Android et Apple, la facilité d'utilisation pour les équipes restreintes, l'évolutivité, les limites de confidentialité, le coût total de possession et la capacité de support au quotidien.

Créer une classe numérique sûre et concentrée : un guide sur le MDM pour les écoles K-12

Les appareils gérés par l'école fonctionnent mieux lorsqu'ils restent centrés sur l'apprentissage. Cerberus Enterprise aide les organisations de niveau K-12 à maintenir la concentration des appareils des élèves grâce aux applications gérées, aux restrictions de type kiosque, à la configuration standardisée des appareils partagés ou prêtés, ainsi qu'aux actions de récupération à distance qui réduisent les pertes, l'usage détourné et les interruptions en classe.

Équiper vos techniciens de terrain : comment le MDM booste l'efficacité et la sécurité sur site

Les techniciens de terrain dépendent des appareils mobiles pour leurs horaires, notes d'intervention, références techniques, historique client et mises à jour de tâches lors de leurs interventions sur site. Cerberus Enterprise aide à maintenir ces appareils opérationnels grâce aux applications gérées, des modèles d'appareils standardisés, des commandes de support à distance et une visibilité basée sur la localisation qui peut améliorer la coordination des interventions tout en renforçant la sécurité sur le terrain.

Au-delà de la carte : utiliser le MDM pour une gestion de flotte et une sécurité des conducteurs plus intelligentes

Les opérations de flotte reposent sur les appareils mobiles pour la navigation, l'envoi d'ordres de mission, la messagerie, le journalisation et l'exécution sur le terrain. Cerberus Enterprise aide à maintenir ces appareils concentrés sur les flux de travail approuvés grâce aux applications gérées, aux contrôles de type kiosque et appareils dédiés, aux politiques de communication sécurisées, au dépannage à distance et à une supervision basée sur la localisation qui peut réduire les temps d'arrêt et favoriser des opérations de conduite plus sûres.

Comment les géorepérages, le suivi en direct et les cartes de localisation améliorent les opérations en entreprise

Les fonctionnalités de géolocalisation dans Cerberus Enterprise aident les organisations à passer d'une simple visibilité des appareils à un contrôle opérationnel plus concret. Les rapports de localisation périodiques, le suivi en direct, les transitions de géorepérage et les cartes interactives peuvent soutenir la logistique, le service sur le terrain, la santé, le commerce de détail, la construction et d'autres équipes distribuées qui ont besoin d'une meilleure visibilité sur l'endroit où le travail s'effectue et sur les moments où les appareils entrent ou sortent de zones importantes.

Comment le multi-tenant aide les MSP à développer leurs services MDM et à créer de nouvelles sources de revenus

Le multi-tenant permet aux MSP, aux revendeurs et aux organisations multi-sociétés de gérer plusieurs entreprises à partir d'un seul compte Cerberus Enterprise tout en maintenant chaque environnement séparé. Ce modèle réduit les frictions opérationnelles, améliore l'évolutivité des services et prend en charge l'accès délégué via des sous-comptes et une administration explicite contrôlée par le client. Il crée également des opportunités commerciales plus solides pour les prestataires qui souhaitent combiner l'octroi de licences logicielles avec l'enrôlement, le support, la conformité et les services de mobilité gérée.

Améliorer l'opérativité de l'entreprise grâce aux solutions MDM

La gestion des appareils mobiles (MDM) centralise le contrôle des appareils de l'entreprise, simplifiant ainsi l'enrôlement, la configuration et la maintenance. Le provisionnement automatisé et les opérations groupées réduisent le travail informatique manuel et garantissent des politiques cohérentes sur tous les appareils. Les fonctionnalités de sécurité, telles que le chiffrement, la surveillance de la conformité et l'effacement à distance, protègent les données de l'entreprise. Dans l'ensemble, le MDM améliore la productivité tout en réduisant les coûts de support et la complexité opérationnelle.

Sécurité avancée dans la gestion Android Enterprise

Android Enterprise utilise un profil professionnel pour isoler les applications et les données de l'entreprise du contenu personnel sur le même appareil. Cette conteneurisation crée des environnements chiffrés distincts, gérés indépendamment par les administrateurs informatiques. Les politiques de sécurité peuvent contrôler le partage des données professionnelles sans affecter les applications personnelles. L'architecture protège les données de l'entreprise même si des applications personnelles sont compromises.

MDM pour iPhone Apple et enrôlement automatisé

Le cadre MDM d'Apple permet une gestion centralisée des iPhones dans les environnements d'entreprise. Combiné à Apple Business Manager, les appareils peuvent s'enrôler et se configurer automatiquement lors de leur première activation. Les administrateurs peuvent déployer et configurer silencieusement les applications d'entreprise, appliquer des paramètres de sécurité et surveiller la conformité. Cette automatisation garantit une configuration cohérente des appareils et réduit les erreurs de paramétrage.

Comprendre la gestion des appareils mobiles (MDM)

La gestion des appareils mobiles (MDM) fournit une plateforme centralisée pour surveiller, sécuriser et contrôler les appareils mobiles accédant aux systèmes de l'entreprise. Les capacités de base incluent l'application de politiques de sécurité, la gestion des applications et le verrouillage ou l'effacement à distance des appareils perdus. Le MDM aide à protéger les données de l'entreprise tout en maintenant la conformité des appareils. Il permet aux organisations de toutes

tailles de gérer en toute sécurité une main-d'œuvre mobile croissante.

Modèles de déploiement des appareils en entreprise

Les organisations peuvent adopter plusieurs modèles de propriété d'appareils tels que le BYOD, le CYOD, le COPE, le COBO et le COSU. Chaque modèle équilibre différemment les coûts, la flexibilité de l'utilisateur et le contrôle de la sécurité. Le BYOD privilégie le confort de l'utilisateur, tandis que le COBO et le COSU maximisent le contrôle et la sécurité de l'entreprise. Le choix du bon modèle dépend des exigences réglementaires, des besoins de la main-d'œuvre et de la capacité de gestion informatique.

MDM vs EMM vs UEM

Le MDM se concentre sur la gestion et la sécurisation des appareils mobiles via l'application de politiques, le contrôle de la configuration et la gestion à distance. L'EMM élargit ce périmètre pour inclure la gestion des applications et du contenu, tandis que l'UEM tente de gérer tous les points de terminaison, y compris les ordinateurs portables et de bureau. Pour de nombreuses PME, des suites EMM ou UEM complètes ajoutent une complexité inutile. En pratique, des capacités MDM robustes répondent souvent à la plupart des besoins de gestion mobile.

Le MDM sur les téléphones personnels et la vie privée des employés

Les systèmes MDM modernes utilisent la conteneurisation pour séparer les données professionnelles et personnelles sur les appareils appartenant aux employés. Les employeurs

peuvent uniquement gérer et surveiller l'environnement de travail, y compris les applications d'entreprise et les informations de conformité des appareils. Les données personnelles telles que les photos, les messages et l'historique de navigation restent inaccessibles à l'entreprise. Cette séparation technique permet des programmes BYOD sécurisés tout en préservant la vie privée des employés.

ROI du MDM et valeur commerciale

Le MDM doit être évalué comme un investissement stratégique plutôt que comme une simple dépense de sécurité. Il génère des retours financiers grâce à la réduction des pertes d'appareils, à la diminution des coûts de support informatique et à l'amélioration de l'efficacité opérationnelle. La gestion automatisée augmente également la productivité des employés et réduit les temps d'arrêt. De plus, une sécurité renforcée réduit le risque et l'impact financier des violations de données.

Gestion des appareils conforme à la loi HIPAA

Les organisations de santé doivent protéger les données électroniques des patients conformément aux exigences de sécurité de la loi HIPAA. Le MDM aide à appliquer le chiffrement, les contrôles d'authentification, la transmission sécurisée des données et les journaux d'audit détaillés. Il permet également l'effacement à distance et l'application centralisée des politiques pour les appareils accédant aux systèmes médicaux. Ces contrôles réduisent les risques de non-conformité tout en permettant des flux de travail mobiles dans les environnements de santé.

Le MDM pour les opérations et la sécurité dans le commerce de détail

Les organisations de vente au détail s'appuient sur les appareils mobiles pour les systèmes de point de vente (POS), la gestion des stocks et les opérations en magasin. Le MDM garantit que ces appareils restent sécurisés, à jour et conformes aux normes telles que PCI-DSS. Une gestion centralisée réduit les temps d'arrêt et simplifie le déploiement des appareils sur plusieurs sites. Le résultat est une efficacité opérationnelle accrue et un risque réduit d'incidents de sécurité liés aux paiements.

Revision #6
Created 2026-06-24 08:07:43 UTC by Admin
Updated 2026-06-24 09:42:09 UTC by Admin