Analyses

Voici quelques articles qui expliquent comment le MDM peut aider votre entreprise :

Qu'est-ce que le mode kiosque ?

Guide pour sécuriser les appareils Android et Apple en entreprise

Le mode kiosque transforme les téléphones et tablettes standard en outils professionnels ciblés. Cerberus Enterprise aide les organisations à verrouiller les appareils sur une seule application ou un petit ensemble d'applications approuvées pour des cas d'usage tels que les points de vente, l'accueil des visiteurs et la navigation de flotte, tout en rendant ces appareils spécialisés plus faciles à sécuriser, à prendre en charge et à gérer à grande échelle.

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

Choisir un MDM tard dans le processus d'achat est plus simple lorsque la comparaison reste concrète. Cette liste de contrôle aide les petites entreprises à évaluer les fournisseurs selon les sept critères qui comptent généralement le plus dans les déploiements réels : sécurité, prise en charge d'Android et d'Apple, facilité d'utilisation pour les équipes réduites, évolutivité, limites de confidentialité, coût total de possession et facilité de support au quotidien.

Créer une classe numérique sûre et ciblée : guide du MDM pour les établissements scolaires

Les appareils gérés par l'établissement fonctionnent mieux lorsqu'ils restent centrés sur l'apprentissage. Cerberus Enterprise aide les établissements scolaires à garder les appareils des élèves ciblés grâce à des applications gérées, des restrictions de type kiosque, des configurations standardisées d'appareils partagés ou prêtés et des actions de récupération à distance qui réduisent les pertes, les dérives et les perturbations en classe.

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

Les techniciens de terrain dépendent des appareils mobiles pour les plannings, les notes d'intervention, les références techniques, l'historique client et les mises à jour des tâches lorsqu'ils travaillent sur site. Cerberus Enterprise aide à maintenir ces appareils prêts grâce à des applications gérées, des modèles d'appareils standardisés, des commandes d'assistance à distance et une visibilité géolocalisée 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

plus intelligente et la sécurité des conducteurs

Les opérations de flotte reposent sur des appareils mobiles pour la navigation, la répartition des missions, la messagerie, la journalisation et l'exécution sur le terrain. Cerberus Enterprise aide à maintenir ces appareils ciblés sur les flux de travail approuvés grâce à des applications gérées, des contrôles de type kiosque et d'appareil dédié, des stratégies de communication sécurisée, un dépannage à distance et une supervision géolocalisée qui peuvent 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 de l'entreprise

Les fonctionnalités de géolocalisation de Cerberus Enterprise aident les organisations à passer d'une simple visibilité des appareils à un contrôle opérationnel plus concret. La communication périodique de la position, le suivi en direct, les transitions de géorepérage et les cartes interactives peuvent accompagner la logistique, les services de terrain, la santé, le commerce de détail, la construction et d'autres équipes réparties qui ont besoin d'une meilleure visibilité sur le lieu où le travail se déroule et sur le moment où les appareils entrent dans des zones importantes ou en sortent.

Comment le multi-tenant aide les MSP à faire évoluer 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 de meilleures opportunités commerciales pour les fournisseurs qui souhaitent associer les licences logicielles à l'intégration, au support, à la conformité et aux services de mobilité gérés.

Améliorer l'efficacité opérationnelle de l'entreprise grâce aux solutions MDM

La gestion des appareils mobiles centralise le contrôle des appareils de l'entreprise, ce qui simplifie l'inscription, la configuration et la maintenance. Le provisionnement automatisé et les opérations groupées réduisent le travail informatique manuel et garantissent des stratégies cohérentes sur tous les appareils. Des fonctionnalités de sécurité telles que le chiffrement, la surveillance de la conformité et l'effacement à distance protègent les données de l'entreprise. Globalement, 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 un même appareil. Cette conteneurisation crée des environnements chiffrés distincts gérés indépendamment par les administrateurs informatiques. Les stratégies de sécurité peuvent contrôler le partage des données de l'entreprise sans affecter les applications personnelles. L'architecture protège les données de l'entreprise même si des applications personnelles sont compromises.

MDM pour Apple iPhone et inscription automatisée

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

Comprendre la gestion des appareils mobiles

La gestion des appareils mobiles fournit une plateforme centralisée pour surveiller, sécuriser et contrôler les appareils mobiles accédant aux systèmes de l'entreprise. Ses capacités principales incluent l'application de stratégies 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 toute taille de gérer

en toute sécurité des effectifs mobiles croissants.

Modèles de déploiement des appareils en entreprise

Les organisations peuvent adopter plusieurs modèles de propriété des appareils, tels que BYOD, CYOD, COPE, COBO et COSU. Chaque modèle équilibre différemment le coût, la flexibilité pour l'utilisateur et le contrôle de sécurité. Le BYOD privilégie la commodité pour 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 des effectifs et de la capacité de gestion informatique.

MDM, EMM et UEM

Le MDM se concentre sur la gestion et la sécurisation des appareils mobiles par l'application de stratégies, le contrôle de la configuration et la gestion à distance. L'EMM étend ce périmètre à la gestion des applications et du contenu, tandis que l'UEM cherche à gérer tous les points de terminaison, y compris les ordinateurs portables et de bureau. Pour de nombreuses PME, les 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.

MDM sur les téléphones personnels et confidentialité des employés

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

peuvent gérer et surveiller que l'environnement professionnel, y compris les applications de l'entreprise et les informations de conformité de l'appareil. 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 confidentialité 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 baisse 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. En outre, une sécurité renforcée réduit le risque et l'impact financier des violations de données.

Gestion des appareils conforme à la HIPAA

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

MDM pour les opérations et la sécurité du commerce de détail

Les organisations du commerce de détail dépendent des appareils mobiles pour les systèmes de point de vente, la gestion des stocks et les opérations en magasin. Le MDM garantit que ces appareils restent sécurisés, à jour et conformes à des normes telles que PCI-DSS. La gestion centralisée réduit les temps d'arrêt et simplifie le déploiement des appareils sur plusieurs sites. Le résultat est une meilleure efficacité opérationnelle et un risque réduit d'incidents de sécurité liés

aux paiements.

Revision #6
Created 2026-11-10 15:15:20 UTC by Admin
Updated 2026-11-12 09:55:01 UTC by Admin