Informations

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

Qu'est-ce que le mode Kiosque ? Un guide pour verrouiller les appareils Android et Apple pour les entreprises

Le mode Kiosque transforme les téléphones et tablettes classiques en outils professionnels spécialisés. Cerberus Enterprise aide les organisations à verrouiller les appareils sur une seule application ou un ensemble restreint d’applications approuvées pour des cas d'utilisation tels que les terminaux de paiement pour la vente au détail, l'enregistrement des visiteurs et la navigation pour les flottes, tout en facilitant la sécurisation, le support et la gestion de ces appareils spécialisés à grande échelle.

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

Choisir une solution MDM tard dans le processus d’achat est plus facile lorsque la comparaison reste pragmatique. Cette liste de contrôle aide les petites entreprises à évaluer les fournisseurs selon les sept critères qui importent 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 capacité de support au quotidien.

Créer une salle de classe numérique sûre et axée : un guide de la GRC pour les écoles de la maternelle à la 12e année

Les appareils gérés par l'école fonctionnent le mieux lorsqu'ils restent concentrés sur l'apprentissage. Cerberus Enterprise aide les organisations de la maternelle à la 12e année à maintenir les appareils des élèves concentrés grâce à des applications gérées, des restrictions de type borne, des configurations standardisées pour les 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 sur le terrain : comment le MDM améliore l'efficacité et la sécurité sur site

Les techniciens sur le terrain dépendent des appareils mobiles pour les horaires, les notes de service, les références techniques, l'historique des clients et les mises à jour des tâches lorsqu'ils travaillent sur site. Cerberus Enterprise les aide à maintenir ces appareils prêts grâce aux applications gérées, aux modèles d'appareils standardisés, aux commandes de support à distance et à une visibilité basée sur la géolocalisation qui peut améliorer la coordination de la planification tout en renforçant la sécurité sur le terrain.

Au-delà de la Carte : Utilisez la GRC pour une Gestion de Flotte Plus Intelligente et une Sécurité des

Conducteurs Accrue

Les opérations de flotte s'appuient sur les appareils mobiles pour la navigation, la transmission, la messagerie, la journalisation et l'exécution sur le terrain. Cerberus Enterprise aide à maintenir ces appareils concentrés sur les flux de travail approuvés grâce à des applications gérées, des contrôles de mode kiosque et d'appareils dédiés, des politiques de communication sécurisées, un dépannage à distance et une supervision basée sur la géolocalisation qui peut réduire les temps d'arrêt et soutenir des opérations de conduite plus sûres.

Comment les clôtures géographiques, le suivi en direct et les cartes de localisation améliorent les opérations de l'entreprise

Les fonctionnalités basées sur la localisation dans Cerberus Enterprise aident les organisations à passer d'une simple visibilité des appareils à un contrôle opérationnel plus pratique. Les rapports de localisation périodiques, le suivi en direct, les transitions de clôtures géographiques et les cartes interactives peuvent soutenir la logistique, le service en milieu, la santé, le commerce de détail, la construction et autres équipes réparties qui ont besoin de mieux comprendre où se déroulent les travaux et quand les appareils entrent ou sortent de zones importantes.

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

La multi-tenancy permet aux MSP, revendeurs et organisations multi-sociétés de gérer plusieurs entreprises depuis un seul compte Cerberus Enterprise tout en gardant chaque environnement séparé. Ce modèle réduit les frictions opérationnelles, améliore la scalabilité des services et prend en charge l'accès délégué via des sous-comptes et une administration contrôlée explicitement par les clients. Il crée également des opportunités commerciales plus fortes pour les fournisseurs qui souhaitent combiner la licence logicielle avec l'intégration, le support, la conformité et les services de mobilité gérée.

Améliorez l'efficacité de votre entreprise avec les solutions MDM :

La gestion centralisée des appareils mobiles simplifie l'inscription, la configuration et la maintenance. La provisionnement automatisé et les opérations groupées réduisent le travail manuel de l'équipe informatique et garantissent une application uniforme des politiques 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. Globalement, la gestion des appareils mobiles 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 d’entreprise du contenu personnel sur le même appareil. Cette conteneurisation crée des environnements cryptés distincts, gérés indépendamment par les administrateurs informatiques. Les politiques de sécurité peuvent contrôler le partage des données d’entreprise sans affecter les applications personnelles. L’architecture protège les données professionnelles même si les applications personnelles sont compromises.

Apple iPhone MDM et inscription automatisée

Le framework MDM d'Apple permet la gestion centralisée des iPhones dans les environnements professionnels. Combiné 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 des applications d'entreprise, appliquer des paramètres de sécurité et surveiller la conformité. Cette automatisation garantit une configuration d'appareils cohérente et réduit les erreurs de configuration.

Comprendre la gestion des appareils mobiles

La gestion des appareils mobiles offre une plateforme centralisée pour surveiller, sécuriser et contrôler les appareils mobiles accédant aux systèmes d'entreprise. Les principales fonctionnalités comprennent l'application de politiques de sécurité, la gestion des applications et le verrouillage ou l'effacement à distance des appareils perdus. La GMD aide à protéger les données de l'entreprise tout en maintenant la conformité des appareils. Elle permet aux entreprises de toutes tailles de gérer en toute sécurité une main-d'œuvre mobile en constante augmentation.

Modèles de déploiement des appareils 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 de l'utilisateur et le contrôle de la sécurité. Le BYOD privilégie la commodité de l'utilisateur, tandis que le COBO et le COSU maximisent le contrôle et la sécurité de l'entreprise. Le choix du modèle approprié dépend des exigences réglementaires, des besoins de la main-d'œuvre et de la capacité de gestion informatique.

MDM contre EMM contre UEM

MDM se concentre sur la gestion et la sécurisation des appareils mobiles grâce à l'application de politiques, le contrôle de configuration et la gestion à distance. EMM étend cette portée pour inclure la gestion des applications et du contenu, tandis que UEM tente de gérer tous les terminaux, 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 en matière 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 d'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.

Retour sur investissement Cerberus et valeur commerciale

Il faut considérer la GRC comme un investissement stratégique, et non comme une simple dépense de sécurité. Elle génère des retours financiers grâce à la réduction des pertes de dispositifs, 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. De plus, une sécurité renforcée réduit le risque et l’impact financier des violations de données.

Gestion des appareils conforme à HIPAA

Les établissements de santé doivent protéger les données électroniques des patients conformément aux exigences de sécurité de HIPAA. La GMD aide à faire respecter le cryptage, les contrôles d'authentification, la transmission sécurisée des données et les journaux d'audit détaillés. Elle 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 non-conformité tout en permettant les flux de travail mobiles dans les environnements de santé.

MDM pour les opérations et la sécurité de détail

Les entreprises de retail s'appuient sur les appareils mobiles pour les systèmes de point de vente, la gestion des stocks et les opérations en magasin. Cerberus assure la sécurité, la mise à jour et la conformité de ces appareils aux 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 efficacité opérationnelle accrue et un risque réduit d'incidents de sécurité liés aux paiements.

Revision #13
Created 2026-03-12 17:05:16 UTC by Admin
Updated 2026-06-23 17:14:26 UTC by Admin