JAMF software
Brief d'entreprise

Sécurité native Apple

Moins les niveaux sont nombreux, meilleure est la sécurité : la preuve

La sécurité des informations de l'entreprise est une lutte sans fin contre des menaces en perpétuelle évolution. Les attaques informatiques sont de plus en plus sophistiquées et leurs vecteurs changent sans cesse. Les cibles des menaces sont de plus en plus nombreuses, car de nouveaux appareils rejoignent les réseaux d'entreprise chaque jour. Une des solutions permettant de pallier ce problème de sécurité consiste à adopter la plateforme Apple et à tirer parti de l'infrastructure de sécurité native proposée par la société. Cette solution permet d'assurer la sécurité des appareils utilisés par la main-d'œuvre mobile d'aujourd'hui, sans dégrader son expérience utilisateur.

Les quatre piliers de la sécurité mobile

La sécurisation d'un ordinateur mobile, qu'il s'agisse d'un ordinateur portable, d'un smartphone ou d'une tablette, nécessite de porter une attention particulière à quatre domaines :

1. Données inactives : sécurisation des données stockées sur un appareil
2. Données en transit : sécurisation des données pendant leur passage sur le réseau jusqu'à l'appareil
3. Sécurité des applications : installation de logiciels de confiance provenant d'une source sûre
4. Application de correctifs : mise à jour des logiciels pour éviter les vulnérabilités

Par ailleurs, pour mettre en place une sécurité fiable dans l'ensemble d'une entreprise, trois fonctionnalités supplémentaires sont essentielles :

- Gestion des appareils : déploiement, distribution des applications et mise en œuvre des stratégies de sécurité
- Création de rapports : inventaire de tous les appareils et de leur configuration
- Audits et mesures correctives : audit de vérification de la conformité aux normes de sécurité et outils permettant de résoudre les problèmes le cas échéant

Chiffrement matériel

VPN

Écosystème de l'App Store

Utilitaires natifs d'application de correctifs logiciels

N'ajoutez pas de niveaux superflus

Plus un système est complexe, plus il est difficile de le sécuriser. Chaque niveau introduit de nouveaux points de défaillance, des vulnérabilités exploitables et des conflits potentiels. En informatique, la complexité prend la forme de niveaux logiciels supplémentaires. Le secteur de la sécurité informatique propose de nombreuses solutions adaptées aux quatre piliers de la sécurité, mais ces solutions se traduisent par une complexité accrue. Toutes choses étant égales par ailleurs, un système informatique doté de fonctions natives de sécurité est plus simple à gérer et plus sécurisé. Grâce à l'intégration de l'infrastructure de sécurité au système d'exploitation, les mises à jour sont simples et la complexité limitée.

La sécurité native Apple est inégalée

Apple est reconnue pour son leadership en matière de design et de fonctionnalité intuitive. Sa mise en œuvre d'une infrastructure de sécurité native pour iOS et OS X est moins connue. Au cours des dernières années, Apple a placé la barre très haut avec Mac, iPad et iPhone. Aujourd'hui, aucune autre plateforme de bureau ou mobile ne propose une telle combinaison de simplicité d'utilisation, contrôles de la confidentialité et sécurité informatique.

Comment Apple renforce les quatre piliers

Les systèmes OS X (Mac) et iOS (iPhone, iPad) incluent des fonctions natives de sécurité pour chacun des quatre piliers ci-dessus :

1. **Données inactives** : fonctionnalités de chiffrement matériel sur iPhone et iPad pour les données inactives activées par défaut. Pour Mac, le système de chiffrement du disque FileVault (fonctionnalité native d'OS X) protège les données avec un impact négligeable sur les performances et l'autonomie.
2. **Données en transit** : les appareils Apple peuvent se connecter à des VPN (Virtual Private Network) pour sécuriser les données en transit. Aucun logiciel supplémentaire n'est requis pour exploiter cette fonctionnalité de sécurité qui, une fois configurée, est transparente pour l'utilisateur.
3. **Sécurité des applications** : une des plus grandes contributions d'Apple à la sécurité informatique réside dans son App Store. Apple analyse tous les logiciels soumis sur l'App Store pour éliminer les programmes malveillants. Chaque paquet logiciel dispose d'une signature cryptographique pour éviter toute manipulation malveillante des fichiers.

OS X et iOS sont configurés pour rejeter tout logiciel non signé. Le service informatique peut signer ses propres paquets logiciels pour tirer parti de cette fonction de sécurité des applications.

4. **Application de correctifs** : depuis les débuts de l'informatique, aucun logiciel n'est exempt de défauts ou de bogues. Les pirates informatiques utilisent certains de ces défauts pour accéder à des informations ou les voler. En informatique, il est recommandé de mettre à jour tous les logiciels pour combler les vulnérabilités à mesure de leur découverte. Apple simplifie cette opération avec des utilitaires natifs d'application de correctifs logiciels intégrés au système d'exploitation. Le service informatique peut héberger un serveur Apple Software Update sur le réseau d'entreprise pour accélérer l'application des correctifs.

Sécurité native et gérée

Les fonctions de sécurité natives Apple sont conçues dans un esprit de simplicité, et une fois configurées, ne nécessitent que des interactions minimales de la part des utilisateurs. Ce fonctionnement est idéal pour les utilisateurs seuls et les petites entreprises. Pour les grandes entreprises, des outils de gestion à distance sont indispensables pour la configuration, le déploiement et la réalisation d'audits de sécurité des applications. Casper Suite de JAMF Software est conçue pour la plateforme Apple et s'intègre à toutes les fonctions de sécurité natives de la société. Cette suite est dotée d'outils de déploiement et de configuration, permet la réalisation d'un inventaire dynamique et intègre des fonctionnalités d'audit et d'application de correctifs.

Conclusion

La mise en place de bonnes pratiques de sécurité n'a pas à être complexe et lourde. Au cours des dix dernières années, Apple a bâti un écosystème riche d'appareils, de logiciels et de services qui offre la meilleure expérience utilisateur en matière d'informatique personnelle. Dans le même temps, les fonctions natives de sécurité incluses dans les systèmes d'exploitation Apple offrent une infrastructure de sécurité de niveau entreprise. Associé à un outil de gestion centré sur la plateforme Apple, l'écosystème Apple offre la meilleure expérience à l'utilisateur final comme au personnel chargé de la sécurité informatique.

Pour en savoir plus sur les fonctions de sécurité natives Apple et les outils de Casper Suite, rendez-vous sur
www.jamfsoftware.com/security

info@jamfsoftware.com | +31 20-240-2294 | www.jamfsoftware.com