Présentation

Sécurité d’iOS

Apple prend la sécurité très au sérieux, aussi bien du point de vue des données des utilisateurs que des données d’entreprise. Nous intégrons des fonctionnalités de sécurité avancées à nos produits pour qu’ils soient sécurisés dès leur conception. Et ce, sans compromettre une formidable expérience utilisateur, qui offre à tout un chacun la liberté de travailler comme il l’entend. Seule Apple est en mesure de fournir une approche aussi complète de la sécurité, car nous créons des produits intégrant le matériel, les logiciels et les services.

La sécurité dès la conception

Les appareils iOS incluent des fonctionnalités avancées qui visent à protéger tout le système, à sécuriser toutes les apps s'exécutant sur la plateforme, et à garantir une gestion et un chiffrement transparents des données personnelles et de l'entreprise. Ces fonctionnalités assurent une sécurité complète de l'appareil, dès sa sortie de l'emballage.

Sécurité du système. iOS est conçu pour que les logiciels et le matériel soient sécurisés sur tous les principaux composants de chaque appareil iOS.

- iOS assure un processus de démarrage sécurisé dès que l'appareil est allumé. Le système bénéficie d'une vérification complémentaire via l'activation de l'appareil.
- Toutes les mises à jour logicielles requièrent une autorisation pour limiter les installations aux logiciels fournis par Apple.
- Des protections système étendues sont disponibles, y compris des règles de code d'accès renforcées et des fonctionnalités innovantes comme Touch ID et Face ID, pour que seuls les utilisateurs autorisés puissent accéder à l'appareil.

Sécurité des données. iOS offre des méthodes solides et puissantes pour assurer la gestion et la protection permanentes des données.

- Les appareils iOS sont fournis avec un processeur matériel dédié et le chiffrement AES-256 est activé d'emblée.
- La protection des données au niveau des fichiers utilise des clés de chiffrement puissantes dérivées du code unique de l'utilisateur.
- iOS utilise des technologies éprouvées pour se connecter aux réseaux d'entreprise naturellement et en toute sécurité, ce qui protège les données pendant leur transmission.

Sécurité des apps. Un modèle de sécurité complet protège les apps iOS des logiciels et des codes malveillants. Il veille à ce que les données et la confidentialité ne soient pas compromises à l'insu de l'utilisateur.

- Apple vérifie l'identité de tous les développeurs qui participent aux programmes pour développeurs d'Apple.
- Apple valide les apps de l'App Store pour s'assurer qu'elles ne comportent pas de bugs importants, ne compromettent pas la vie privée des utilisateurs et fonctionnent conformément à des directives claires.
- Les apps internes doivent être signées et fournies avec un certificat Apple via l'Apple Developer Enterprise Program.
- Avec la protection à l'exécution, la mise en bac à sable et les autorisations intégrées à iOS, les utilisateurs peuvent télécharger, installer et exécuter des apps en sachant que leur mode d'accès aux données est réglementé.

Liberté de travailler

Chaque appareil iOS intègre des fonctionnalités de sécurité complètes, qui donnent plus de liberté aux employés dans l'accomplissement de leurs tâches. Les utilisateurs peuvent personnaliser leurs appareils pour être encore plus productifs. iOS respecte la vie privée des utilisateurs, tout en protégeant et en séparant les données professionnelles et personnelles.

Personnalisation. Afin de simplifier l'installation pour les utilisateurs, iOS offre un processus rationalisé pouvant être automatisé par le biais du Programme d'inscription des appareils (Device Enrollment Program, DEP) d'Apple et des outils de gestion des appareils mobiles (Mobile Device Management, MDM).

- Avec l'Assistant réglages d'iOS, les utilisateurs peuvent activer leurs appareils, configurer les réglages de base et commencer à travailler immédiatement.
- Les utilisateurs peuvent se connecter avec leur identifiant Apple pour personnaliser leur expérience, et utiliser Localiser mon iPhone pour retrouver un appareil égaré. Ils peuvent enregistrer leurs données personnelles sur iCloud, mais pas les données de l'entreprise.

Séparation. iOS et les solutions MDM offrent des moyens intelligents de gérer de façon discrète les données et apps de l'entreprise, tout en séparant de façon transparente les données professionnelles et personnelles.

- Nul besoin de conteneurs ou de doubles espaces de travail qui frustrent les utilisateurs et portent atteinte à leur expérience.
- Tout compte, app, contenu et réglage d'entreprise installé via une solution MDM est considéré comme « géré » par iOS et peut être supprimé à tout moment par le service informatique, sans affecter les données personnelles.
- Grâce à des fonctionnalités réseau comme la connexion VPN via l'app, le trafic des apps d'entreprise passe par le réseau de l'entreprise, tandis que le trafic personnel passe par le réseau public.
- Des fonctionnalités comme la gestion des autorisations d'ouverture permettent de contrôler le flux des données d'entreprise entre les apps et d'empêcher l'enregistrement de documents dans les apps ou services dans le nuage personnels de l'utilisateur. Cela s'applique également aux extensions des fournisseurs de documents.

Confidentialité. Les données de l'entreprise restent sous le contrôle du service informatique, et les données personnelles (comme les messages, données de localisation, photos et données iCloud) restent privées.

- Apple intègre des dispositifs de sécurité étendus aux apps, aux services Internet et à iOS pour que des mesures de confidentialité fortes protègent en permanence les informations de l'entreprise.
- Les développeurs peuvent utiliser des outils comme les API Touch ID, le chiffrement 256 bits et App Transport Security pour concevoir des apps plus sécurisées. Apple oblige également les développeurs à demander l'autorisation d'accéder à des données personnelles, telles que les contacts.

Ressources complémentaires

- Document Sécurité iOS : apple.com/business/docs/
- Sécurité de Face ID : apple.com/business/docs/
- Page web sur la confidentialité : apple.com/fr/privacy/

© 2018 Apple Inc. Tous droits réservés. Apple, le logo Apple, iPhone et Touch ID sont des marques d'Apple Inc., déposées aux États-Unis et dans d'autres pays. App Store, iBooks Store, iCloud et iTunes Store sont des marques de service d'Apple Inc., déposées aux États-Unis et dans d'autres pays. IOS est une marque commerciale ou déposée de Cisco aux États-Unis et dans d'autres pays, utilisée sous licence. Les autres noms de produits et de sociétés mentionnés dans ce document appartiennent à leurs propriétaires respectifs. Les caractéristiques des produits sont susceptibles d'être modifiées sans préavis. Les informations contenues dans ce document sont fournies à titre indicatif uniquement ; Apple n'assume aucune responsabilité quant à leur utilisation.
Septembre 2017