Überblick

iOS Sicherheit

Bei Apple nehmen wir Sicherheit sehr ernst, sowohl für die Benutzer als auch in Bezug auf den Schutz von Unternehmensdaten. Deshalb integrieren wir von Anfang an modernste Sicherheitslösungen in unsere Produkte, sodass sie von Grund auf sicher sind. Gleichzeitig achten wir darauf, ein tolles Benutzererlebnis zu gewährleisten, damit die Benutzer so arbeiten können, wie sie es möchten. Dieses umfassende Sicherheitskonzept kann nur Apple bieten, da wir Produkte mit integrierter Hardware, Software und Diensten entwickeln.

Von Grund auf sicher

iOS Geräte verfügen über fortschrittliche Features, um das gesamte System und alle auf der Plattform laufenden Apps zu schützen und sicherzustellen, dass geschäftliche und private Daten nahtlos verschlüsselt und verwaltet werden. Diese Features bieten von Anfang an eine umfassende Sicherheit.

Systemsicherheit. iOS ist so konzipiert, dass sowohl Software als auch Hardware über alle Kernkomponenten von jedem iOS Gerät hinweg sicher sind.

- Sobald das Gerät eingeschaltet wird, gewährleistet iOS einen sicheren Startvorgang. Eine weitere Systemverifizierung erfolgt durch die Geräteaktivierung.
- Alle Softwareupdates werden autorisiert, um sicherzustellen, dass nur von Apple bereitgestellte Software installiert wird.
- Umfangreiche Schutzmaßnahmen, darunter starke Coderichtlinien und innovative Features wie Touch ID und Face ID, sorgen dafür, dass nur autorisierte Benutzer Zugriff auf das Gerät haben.

Datensicherheit. iOS bietet stabile und leistungsstarke Methoden, um Daten jederzeit zu verwalten und zu schützen.

- iOS Geräte verfügen über einen dedizierten Hardwareprozessor und nutzen eine 256-Bit-AES-Verschlüsselung mit sofortiger Aktivierung.
- Für die Datensicherheit auf Dateiebene kommen starke Verschlüsselungscodes zum Einsatz, die vom Benutzercode abgeleitet werden.
- iOS nutzt bewährte Technologien, um nahtlose und sichere Verbindungen zu Unternehmensnetzwerken herzustellen und Daten während der Übertragung zu schützen.

App-Sicherheit. Ein vollständiges Sicherheitsmodell für iOS Apps schützt vor Malware und schädlichem Code und verhindert, dass unwissentlich in Daten oder die Privatsphäre eingegriffen werden kann.

- Apple prüft die Identität aller Entwickler, bevor diese an einem Apple Entwicklerprogramm teilnehmen dürfen.
- Die Apps im App Store werden von Apple überprüft, um sicherzustellen, dass sie keine wesentlichen Fehler aufweisen, nicht die Privatsphäre der Benutzer gefährden und nach klaren Richtlinien funktionieren.
- Interne Apps müssen signiert und mit einem Zertifikat von Apple aus dem Apple Developer Enterprise Program versehen werden.
- Mit Laufzeitschutz, Sandboxing und in iOS integrierten Berechtigungen können die Benutzer Apps laden, installieren und ausführen und sich sicher sein, dass sie nur autorisierten Zugriff auf Daten haben.

Freiheit zum Arbeiten

Dank umfassender integrierter Sicherheit bieten iOS Geräte den Mitarbeitern Freiheit bei der Arbeit. Die Benutzer können ihre Geräte personalisieren, sodass sie noch produktiver arbeiten können. Und iOS wahrt die Privatsphäre der Benutzer, während berufliche und private Daten nahtlos geschützt und voneinander getrennt werden.

Personalisierung. Mit iOS können Benutzer ihre Geräte mühelos über einen einfachen, optimierten Prozess einrichten. Dieser lässt sich mit dem Programm zur Geräteregistrierung (Device Enrolment Program, DEP) von Apple und Tools zur mobilen Geräteverwaltung (Mobile Device Management, MDM) noch weiter automatisieren.

- Mit dem Systemassistenten von iOS können die Benutzer ihre Geräte aktivieren, grundlegende Einstellungen konfigurieren und sofort loslegen.
- Benutzer können sich für ein personalisiertes Erlebnis mit ihrer eigenen Apple ID anmelden; Unternehmensdaten werden nicht in iCloud gesichert, private Daten dagegen schon. Zudem lassen sich so verlorene Geräte über „Mein iPhone suchen" aufspüren.

Trennung. iOS und MDM-Lösungen bieten intelligente Methoden, um Unternehmensdaten und -apps diskret zu verwalten und dabei berufliche und private Daten nahtlos voneinander zu trennen.

- Es besteht keine Notwendigkeit für Lösungen mit Containern oder zwei Arbeitsbereichen, die die Benutzer frustrieren und das Benutzererlebnis beeinträchtigen.
- Geschäftliche Accounts, Apps, Inhalte und Einstellungen, die über eine MDM-Lösung installiert wurden, werden von iOS als „verwaltet" betrachtet und können jederzeit von der IT entfernt werden, ohne dass private Daten davon betroffen sind.
- Netzwerkfeatures wie VPN pro App stellen sicher, dass Datenverkehr von Unternehmensapps über das Unternehmensnetzwerk läuft und privater Datenverkehr über das öffentliche Netzwerk.
- Features wie „In verwalteter Umgebung öffnen" können genutzt werden, um den Fluss von Unternehmensdaten zwischen Apps zu steuern und zu verhindern, dass Dokumente in den privaten Apps oder Cloud-Diensten des Benutzers gesichert werden. Dies gilt auch für Document-Provider-Erweiterungen.

Datenschutz. Die IT behält die Kontrolle über Unternehmensdaten, während persönliche Daten – wie Nachrichten, Standortdaten, Fotos und iCloud Daten – privat bleiben.

- Apple integriert umfangreiche Schutzmaßnahmen in Apps, Internet-Dienste und iOS, sodass sichere Datenschutzvorkehrungen die Unternehmensdaten zu jedem Zeitpunkt schützen.
- Entwickler können Tools wie Touch ID, APIs, 256-Bit-Verschlüsselung und App Transport Security nutzen, um sichere Apps zu entwickeln. Apple fordert von Entwicklern außerdem, dass sie erst um Erlaubnis bitten, bevor sie auf private Daten wie Kontakte zugreifen.

Weitere Ressourcen

- iOS Sicherheitsdokument: apple.com/business/docs/
- Face ID Sicherheitsdokument: apple.com/business/docs/
- Datenschutz-Webseite: apple.com/de/privacy/