iOS-säkerhet – översikt

Vi på Apple tar säkerheten på största allvar, både för användaren och för skyddet av företagsdata. Vi bygger in avancerade säkerhetsfunktioner i våra produkter för att skydda dem. Och vi har gjort det på ett sätt som inte stör den enastående användarupplevelsen eller människors frihet att arbeta som de vill. Endast Apple kan leverera denna omfattande säkerhet, eftersom vi skapar produkter där hårdvara, mjukvara och tjänster är integrerade med varandra.

Utformad med säkerheten i åtanke

iOS-enheter är försedda med avancerade funktioner som skyddar hela systemet och alla appar som körs på plattformen samt ser till att såväl företagsdata som privata data krypteras och hanteras på ett smidigt sätt. Dessa funktioner ger omfattande säkerhet redan från början.

Systemsäkerhet. iOS har utformats så att både mjukvara och hårdvara skyddas i alla kärnkomponenter på alla iOS-enheter.

- iOS garanterar säker uppstart från det ögonblick en enhet slås på. Systemet genomgår ytterligare verifiering via enhetsaktiveringen.
- iOS gör det enkelt för IT-avdelningen att hantera uppdateringar av systemmjukvara som åtgärdar säkerhetsbrister. Alla mjukvaruuppdateringar auktoriseras för att säkerställa att enbart mjukvara levererad av Apple installeras.
- Det finns omfattande skydd i form av bland annat policyer för starka lösenkoder samt innovativa funktioner som Touch ID och Face ID, så att endast auktoriserade användare ska få åtkomst till enheten.

Datasäkerhet. iOS innehåller stabil och kraftfull funktionalitet för att ständigt hålla data hanterade och skyddade.

- iOS-enheter levereras med en särskild hårdvaruprocessor och använder sig av AES-256-kryptering redan från start.
- Dataskydd på filnivå använder starka krypteringsnycklar baserade på användarens unika lösenkod.
- iOS använder beprövad teknik för att smidigt och säkert ansluta till företagsnätverk och data skyddas under överföringen.

Appsäkerhet. En komplett säkerhetsmodell för iOS-appar skyddar mot skadeprogram, skadlig kod och oron för att användarens data eller personliga integritet inte är skyddad mot dolda attacker.

- Apple kontrollerar identiteten hos alla utvecklare innan de kan gå med i Apples utvecklarprogram.
- Apparna i App Store granskas av Apple för att säkerställa att de inte innehåller allvarliga buggar, inte kränker användarens integritet samt att de fungerar enligt tydliga riktlinjer.
- Interna appar måste vara signerade och utgivna med ett certifikat utfärdat av Apple via Apple Developer Enterprise Program.
- Med iOS inbyggda skydd under körning, sandlådefunktionen samt rättigheter kan användarna ladda ned, installera och köra appar i vetskapen att dessa enbart kan komma åt data på sätt som är auktoriserade.

Friheten att arbeta

Den omfattande inbyggda säkerheten gör att medarbetare med iOS-enheter kan arbeta på sätt som passar dem. Användarna kan anpassa sina enheter och på så sätt bli ännu mer produktiva. iOS skyddar dessutom användarnas integritet samtidigt som det på ett smidigt sätt skyddar och skiljer på arbetsrelaterad och privat information.

Anpassning. iOS gör det enkelt för användare att ställa in sina egna enheter med en enkel och smidig process, som kan automatiseras ytterligare med Apples program för enhetsregistrering (DEP) och en MDM-lösning.

- Inställningsassistenten hjälper medarbetarna att aktivera sina enheter, göra grundläggande inställningar och börja arbeta på direkten.
- Användare kan logga in med sina egna Apple-ID:n och få en personlig upplevelse. Företagsdata säkerhetskopieras inte till iCloud, men det gör privata data. Användare kan hitta försvunna enheter med funktionen Hitta min iPhone.

Separation. iOS och MDM-lösningar möjliggör smarta sätt att hantera företagets appar och data i bakgrunden medan jobbdata och personliga data hålls separata på ett smidigt sätt.

- På så sätt elimineras behovet av behållare och dubbla arbetsytor som annars irriterar användarna och försämrar användarupplevelsen.
- Företagets konton, appar, inställningar, innehåll och kontakter som installeras via en MDM-lösning betraktas som ”hanterade” av iOS och kan när som helst tas bort av IT-personalen utan att några personliga data påverkas.
- Nätverksfunktioner som VPN per app säkerställer att trafik från företagsappar går via företagets nätverk och att personlig trafik går via det offentliga nätverket.
- Funktioner som Hanterad öppning kan användas för att styra flödet av företagsdata mellan appar samt förhindra att dokument sparas i användarens personliga appar eller molntjänster. Även dokumentapptillägg omfattas.

Integritet. Företagets data kontrolleras av IT-avdelningen medan användarens personliga data, som meddelanden, platsdata, bilder och iCloud-data, förblir privata.

- Apple bygger in starkt skydd i appar, internettjänster och iOS, så att företagsinformationen alltid skyddas av effektiva dataskydd.
- Utvecklare kan skapa säkra appar genom att använda sig av verktyg som API:er för Touch ID, 256-bitarskryptering och App Transport Security (ATS). Apple kräver dessutom att utvecklare ber om lov innan de använder personlig information, såsom kontakter.

Ytterligare resurser: iOS-säkerhet | Handledningen Face ID Security | Webbsidan om personlig integritet