Apple at Work

Sicurezza della piattaforma

Sicuri fin dalle fondamenta.

Per Apple, proteggere gli utenti e i dati aziendali è una priorità. Abbiamo integrato funzioni di sicurezza evolute nei nostri prodotti per renderli sicuri fin dalle fondamenta. E lo abbiamo fatto offrendo allo stesso tempo una straordinaria esperienza utente, per dare a ogni singola persona la libertà di lavorare come preferisce. Solo Apple è in grado di offrire questo approccio globale alla sicurezza, perché creiamo prodotti con hardware, software e servizi integrati.

Sicurezza hardware
Un software sicuro necessita di un hardware sicuro, per questo nei dispositivi iOS, iPadOS, macOS, tvOS e watchOS la sicurezza è integrata già a livello di processore, con funzioni ad hoc della CPU e un chip dedicato. Il componente più importante è il coprocessore Secure Enclave, presente nei più recenti dispositivi iOS, iPadOS, watchOS e tvOS e in tutti i Mac con chip Apple T2 Security. Il Secure Enclave è la base portante delle funzioni di archiviazione criptata, dell'avvio protetto in macOS e dell'utilizzo dei dati biometrici.

Tutti i più recenti iPhone, iPad e i Mac con chip T2 includono un motore AES hardware dedicato che permette di criptare i dati ad alta velocità in fase di lettura e scrittura. In questo modo, le funzioni Data Protection e FileVault possono proteggere i file degli utenti senza rivelare chiavi di codifica a lungo termine alla CPU o al sistema operativo.

L'avvio protetto dei dispositivi Apple impedisce la manomissione dei livelli più bassi del software e garantisce che all'avvio del sistema si carichino solo programmi autorizzati da Apple. Sui dispositivi iOS e iPadOS, la sicurezza comincia da un codice immutabile chiamato Boot ROM, creato durante la fabbricazione del chip e riconosciuto come "root of trust" (RoT) dell'hardware. Sui Mac con chip T2, la catena di affidabilità per l'avvio protetto ha inizio dal Secure Enclave.

Il Secure Enclave permette di utilizzare l'autenticazione sicura con Touch ID e Face ID sui dispositivi Apple mantenendo riservati i dati biometrici degli utenti, che in questo modo possono approfittare della sicurezza offerta da codici e password di maggiore lunghezza e complessità, ma con la comodità di potersi autenticare in un istante.

Le funzioni di sicurezza dei dispositivi Apple sono rese possibili dall'esclusiva combinazione di chip, hardware, software e servizi che solo Apple è in grado di offrire.

Sicurezza del sistema

La sicurezza del sistema fa leva sulle caratteristiche uniche dell'hardware Apple per massimizzare la sicurezza dei sistemi operativi sui nostri dispositivi senza comprometterne la facilità d'uso, e comprende la procedura di avvio, gli aggiornamenti software e il funzionamento continuo del sistema operativo.

L'avvio protetto comincia dall'hardware ed è il primo anello di una catena di affidabilità in cui ogni passaggio verifica che quello successivo funzioni correttamente prima di cedere il controllo. Questo modello di sicurezza si applica non solo alla normale procedura di avvio dei dispositivi Apple, ma anche alle varie modalità di recupero e aggiornamento di iOS, iPadOS e macOS.

Le versioni più recenti di iOS, iPadOS e macOS sono le più sicure. Il meccanismo di aggiornamento software fornisce update tempestivi, e in più garantisce che venga inviato solo software approvato da Apple. Il sistema di aggiornamento può perfino proteggere i dispositivi dagli attacchi downgrade, impedendo l'installazione di una versione OS precedente con l'obiettivo di rubare i dati dell'utente.

Infine, i dispositivi Apple integrano protezioni per l'avvio e il runtime che ne preservano l'integrità durante il normale utilizzo. Queste protezioni variano in modo significativo fra i dispositivi iOS, iPadOS e macOS, in considerazione delle diverse funzioni supportate e, quindi, degli attacchi che devono impedire.

Per ottenere questo livello di protezione, iOS e iPadOS utilizzano meccanismi Kernel Integrity Protection, System Coprocessor Integrity, Pointer Authentication Code e Page Protection Layer, mentre macOS usa la sicurezza Unified Extensible Firmware Interface, la modalità System Management Mode, protezioni Direct Memory Access e funzioni di sicurezza del firmware periferico.

Crittografia e protezione dei dati

I dispositivi Apple integrano funzioni per la crittografia che proteggono i dati dell'utente e consentono l'inizializzazione a distanza se il dispositivo viene smarrito o rubato.

L'avvio protetto, la sicurezza a livello di sistema e le funzioni di sicurezza delle app contribuiscono a garantire che solo il codice e le app attendibili possano essere eseguiti su un dispositivo. I dispositivi Apple hanno ulteriori funzioni di crittografia che proteggono i dati dell'utente anche nel caso in cui altre parti dell'infrastruttura di sicurezza vengano compromesse, per esempio se un dispositivo viene smarrito o esegue un codice non approvato. Tutte queste funzioni vanno a vantaggio sia degli utenti, sia degli amministratori IT, perché tengono costantemente al sicuro le informazioni personali e aziendali e forniscono metodi per inizializzare a distanza il dispositivo in caso di furto o perdita.

Per la crittografia dei file, i dispositivi iOS e iPadOS utilizzano un metodo chiamato Data Protection, mentre la sicurezza dei dati su Mac è garantita da una tecnologia di codifica del volume chiamata FileVault. Sui dispositivi con processore SEP, le gerarchie di gestione delle chiavi di entrambi i metodi si basano sul chip dedicato del Secure Enclave. Inoltre, entrambi usano un motore AES dedicato per la crittografia ad alta velocità dei file e per garantire che le chiavi di codifica a lungo termine non vengano mai rivelate al sistema operativo del kernel o alla CPU, dove potrebbero subire manomissioni.

Sicurezza delle app

Le app sono tra gli elementi più importanti di un'architettura di sicurezza moderna. Pur offrendo incredibili vantaggi a livello di produttività, se non gestite correttamente possono avere un impatto negativo sulla sicurezza e la stabilità del sistema, oltre che sui dati dell'utente. Apple offre più livelli di protezione per garantire che le app siano prive di malware e non siano state manomesse. Ulteriori misure di sicurezza gestiscono l'accesso ai dati dell'utente monitorando scrupolosamente il processo.

I controlli di sicurezza integrati creano una piattaforma stabile e sicura per le app, permettendo a migliaia di sviluppatori di fornire centinaia di migliaia di app per iOS, iPadOS e macOS senza compromettere l'integrità del sistema. E gli utenti possono accedere a queste app sui dispositivi Apple con la certezza di poter contare su controlli che contribuiscono a respingere virus, malware e attacchi.

Su iPhone, iPad e iPod touch, tutte le app provengono dall'App Store e tutte sono sottoposte a sandboxing per garantire il massimo controllo. Sul Mac, molte app provengono dall'App Store ma gli utenti possono anche usare anche app scaricate da internet: per garantire la sicurezza anche in questo secondo caso, macOS mette in campo alcuni controlli aggiuntivi. Innanzitutto, a partire da macOS 10.15 tutte le app per Mac devono essere autenticate da Apple prima del lancio. In questo modo si ha la certezza che le app non contengano malware, anche se non provengono dall'App Store. macOS include inoltre una protezione antivirus standard di settore per bloccare e, se necessario, rimuovere il malware.

Come misura aggiuntiva su tutte le piattaforme, il sandboxing contribuisce a impedire che app non autorizzate abbiano accesso ai dati dell'utente. E in macOS, il sandboxing si applica anche ai dati stessi nelle aree critiche del sistema operativo: in questo modo gli utenti mantengono il pieno controllo sulle app che possono accedere ai file nelle cartelle Scrivania, Documenti e Download, e in altre sezioni, indipendentemente dal fatto che vengano o meno eseguite in ambiente sandboxed.

Sicurezza dei servizi

Per aiutare gli utenti a ottenere il massimo dai loro dispositivi, Apple ha creato una serie di servizi fra cui ID Apple, iCloud, Accedi con Apple, Apple Pay, iMessage, FaceTime, Siri e Dov'è. Questi servizi offrono potenti funzioni per l'archiviazione e la sincronizzazione cloud, l'autenticazione, i pagamenti, la messaggistica, le comunicazioni e non solo, il tutto proteggendo la privacy degli utenti e la sicurezza dei loro dati.

Ecosistema di partner

I dispositivi Apple sono compatibili con gli strumenti e i servizi di sicurezza aziendali più diffusi, per garantire la conformità dei dispositivi e dei dati che contengono. Ogni piattaforma supporta i protocolli standard per VPN e connessioni Wi-Fi protette, così da tutelare il traffico di rete e garantire il collegamento sicuro alle infrastrutture aziendali più utilizzate.

La partnership di Apple con Cisco migliora la sicurezza e la produttività grazie all'utilizzo congiunto delle rispettive tecnologie. Le reti Cisco offrono una maggiore sicurezza tramite Cisco Security Connector e danno la priorità alle app aziendali sulle reti Cisco.

Scopri di più sulla sicurezza dei dispositivi Apple.

apple.com/it/business/it

apple.com/it/macos/security

apple.com/it/privacy/features

apple.com/it/security