Apple at Work

Sicurezza della piattaforma

Sicuri dalle fondamenta.

Per Apple, la sicurezza è una priorità: sia quella dell'utente che quella dei dati aziendali. Abbiamo integrato nei nostri prodotti funzioni di protezione evolute che li rendono sicuri fin dalle fondamenta. E lo abbiamo fatto in modo che restassero sempre facili e piacevoli da usare, per lasciare a ogni utente la libertà di lavorare come preferisce. Solo Apple può offrire un approccio alla sicurezza così completo, perché hardware, software e servizi sono pensati fin dall'inizio per agire insieme, come una vera squadra.

Sicurezza dell'hardware
Perché un software sia davvero sicuro, deve esserlo anche l'hardware su cui gira. Ecco perché i dispositivi Apple con iOS, iPadOS, macOS, tvOS o watchOS sono progettati attorno alla sicurezza dell'utente già a partire dal chip.

Questo è possibile grazie a speciali tecnologie della CPU che formano le basi per la protezione a livello di sistema, oltre a un ulteriore chip specificamente dedicato alle funzioni di sicurezza. L'hardware progettato per la sicurezza supporta un numero limitato di funzioni ben definite con lo scopo di ridurre al minimo la superficie di attacco. I componenti includono una boot ROM che costituisce la root of trust hardware per l'avvio protetto, motori AES dedicati per gestire le operazioni di codifica e decodifica in modo sicuro ed efficiente, e un Secure Enclave.

Il Secure Enclave è un system on a chip (SoC) incluso in tutte le generazioni recenti di iPhone, iPad, Apple Watch, Apple TV e HomePod, e nei Mac con chip Apple o con chip Apple T2 Security. Il Secure Enclave segue il principio di progettazione dei SoC, quindi contiene una boot ROM e un motore AES dedicati. Inoltre fornisce le fondamenta che permettono di generare e archiviare in modo sicuro le chiavi necessarie per la crittografia dei dati a riposo, e protegge e valuta i dati biometrici per Touch ID e Face ID.

La crittografia dell'archiviazione deve essere veloce ed efficiente. Allo stesso tempo, non può esporre i dati che utilizza per stabilire le relazioni delle chiavi crittografiche. Il motore hardware AES risolve questo problema eseguendo rapidamente la codifica e la decodifica in-line mentre i file vengono scritti o letti. Dal Secure Enclave, un canale speciale trasmette al motore AES le informazioni necessarie senza renderle visibili alla CPU o al sistema operativo. In questo modo le tecnologie Apple Data Protection e FileVault possono proteggere i file dell'utente senza rivelare chiavi di codifica a lungo termine.

Apple ha progettato la funzione di avvio protetto per impedire la manomissione dei livelli più bassi del software e garantire che quando si avvia il sistema operativo si carichino solo programmi autorizzati da Apple. L'avvio protetto parte dal codice immutabile della boot ROM, che viene generato durante la fabbricazione del SoC Apple e rappresenta la root of trust hardware. Sui modelli di Mac con Apple T2 Security, la catena di fiducia per l'avvio sicuro di macOS ha inizio dal chip T2. Sia il chip T2 che il Secure Enclave eseguono i processi di avvio sicuro utilizzando una propria boot ROM, esattamente come i chip serie A e M1.

In più, il Secure Enclave elabora i dati dell'impronta digitale e del volto che vengono acquisiti dai sensori Touch ID e Face ID sui dispositivi Apple. Ciò consente di offrire un'autenticazione sicura tutelando la riservatezza dei dati biometrici. Permette inoltre di usare password e codici più lunghi e complessi con la comodità, in molte situazioni, di un'autenticazione rapida per l'accesso o per completare un acquisto.

Queste funzioni di sicurezza dei dispositivi sono rese possibili dalla combinazione di chip, hardware, software e servizi che solo Apple può offrire.

Sicurezza del sistema
Basata sulle esclusive funzioni di sicurezza dell'hardware Apple, la sicurezza a livello di sistema controlla l'accesso alle risorse di sistema sui dispositivi senza compromettere l'usabilità, dal processo di avvio, fino alla gestione degli aggiornamenti software e alla protezione di risorse come CPU, memoria, disco, programmi e dati archiviati.

Le versioni più recenti dei sistemi operativi Apple offrono il livello più alto di sicurezza. Su questo piano ha un ruolo importante l'avvio sicuro, che protegge il sistema dai malware quando si accende il dispositivo. L'avvio sicuro parte dall'hardware e costruisce una catena di fiducia attraverso il software: prima di cedere il controllo, ogni anello della catena verifica che quello successivo funzioni correttamente. Questo modello di sicurezza supporta non solo il normale processo di avvio dei dispositivi Apple, ma anche le varie modalità per il ripristino e l'aggiornamento. Anche sottocomponenti come il chip T2 e il Secure Enclave eseguono un proprio processo di avvio sicuro per garantire che venga caricato solo il codice autorizzato da Apple. Il sistema di aggiornamento può perfino impedire gli attacchi di downgrade, perché non consente di riportare i dispositivi a una versione precedente del sistema operativo che i malintenzionati potrebbero saper compromettere per impadronirsi dei dati personali.

I dispositivi Apple includono anche protezioni di avvio e runtime che ne garantiscono l'integrità durante l'uso quotidiano. I chip progettati da Apple su iPhone, iPad, Apple Watch, Apple TV e HomePod, e i Mac con chip Apple, forniscono un'architettura comune per tutelare l'integrità del sistema operativo. Inoltre, macOS include un set più ampio e configurabile di protezioni per il suo particolare modello di calcolo, oltre a funzioni supportate da tutte le piattaforme hardware Mac.

Crittografia e protezione dei dati
I dispositivi Apple hanno funzioni di crittografia per proteggere i dati dell'utente e si possono inizializzare a distanza in caso di perdita o furto.

La catena di avvio sicuro e le funzioni di sicurezza a livello di sistema e di app garantiscono che il dispositivo esegua solo codice e app attendibili. Ulteriori funzioni di crittografia sui dispositivi Apple proteggono i dati dell'utente anche nel caso in cui altre parti dell'infrastruttura di sicurezza vengano compromesse, per esempio se un dispositivo viene perso o esegue codice non approvato. Tutte queste funzioni vanno a vantaggio sia dell'utente, sia degli amministratori IT,

perché salvaguardano le informazioni personali e aziendali, e in più forniscono opzioni per cancellare a distanza e all'istante i contenuti di un dispositivo che è stato perso o rubato.

I dispositivi iOS e iPadOS usano un metodo di codifica dei file chiamato Data Protection, mentre i dati sui Mac con processore Intel sono protetti da FileVault, una tecnologia di codifica dei volumi. I Mac con chip Apple utilizzano un modello ibrido e compatibile con la funzione Data Protection, con due riserve: il livello di protezione più basso (classe D) non è supportato, e il livello predefinito (classe C) utilizza una chiave di volume e funziona proprio come FileVault sui Mac con processore Intel. In tutti i casi, le gerarchie di gestione delle chiavi sono radicate nel chip dedicato del Secure Enclave, mentre un motore AES dedicato esegue la codifica alla velocità di linea e garantisce che le chiavi di codifica a lungo termine non vengano mostrate al sistema operativo del kernel o alla CPU (dove potrebbero subire manomissioni). I Mac con processore Intel e chip T1, o sprovvisti di Secure Enclave, non utilizzano un chip dedicato per proteggere le chiavi di codifica di FileVault.

Oltre che dalle funzioni Data Protection e FileVault, che impediscono di accedere ai dati senza autorizzazione, la sicurezza viene garantita anche dalle tecnologie presenti nei kernel dei sistemi operativi Apple. Il kernel utilizza il controllo degli accessi per il sandboxing delle app (che limita i dati a cui l'app può accedere) e un meccanismo detto Data Vault che limita l'accesso ai dati di un'app da parte di tutte le altre app che lo richiedono, anziché limitare le richieste di accesso che ogni singola app può effettuare.

Sicurezza delle app

Le app sono fra gli elementi più critici dell'architettura di sicurezza. Offrono enormi vantaggi per la produttività, ma se non gestite correttamente possono anche compromettere la sicurezza e la stabilità del sistema e mettere a rischio i dati dell'utente.

Per questo, i livelli di protezione sui dispositivi Apple garantiscono che le app non contengano malware conosciuti e non siano state manomesse. Ulteriori meccanismi impongono che l'accesso ai dati dell'utente da parte delle app venga gestito con la massima attenzione. Questi controlli di sicurezza 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 tutte queste app possono essere utilizzate sui dispositivi Apple senza temere virus, malware o attacchi.

Su iPhone, iPad e iPod touch, tutte le app si scaricano dall'App Store e tutte sono sandboxed, per garantire il massimo controllo.

Su Mac, molte app provengono dall'App Store, ma è anche possibile scaricarle da internet. macOS dispone quindi di controlli aggiuntivi per garantire download sicuri. Per prima cosa, a partire da macOS 10.15 tutte le app per Mac devono essere autenticate da Apple per potersi avviare. Questo requisito permette di assicurare che le app non contengano malware conosciuti anche quando non sono distribuite tramite l'App Store. Inoltre, macOS include un sistema di protezione antivirus all'avanguardia per bloccare i malware e se necessario rimuoverli.

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 ogni utente mantiene il pieno controllo

sull'accesso ai file nelle cartelle Scrivania, Documenti, Download e non solo, anche quando le app che tentano di utilizzarli non sono sandboxed.

Sicurezza dei servizi
Apple ha sviluppato un set di servizi che aiutano a trarre il massimo vantaggio dai dispositivi. Offrono funzioni per archiviare file sul cloud, sincronizzare contenuti, memorizzare password, autenticarsi, pagare acquisti, inviare messaggi, comunicare e fare tante altre cose, e sono tutti progettati in modo da proteggere la privacy e i dati personali.

I servizi includono iCloud, Accedi con Apple, Apple Pay, iMessage, Business Chat, FaceTime, Dov'è e Continuity, e potrebbero richiedere un ID Apple o un ID Apple gestito. In alcuni casi non è possibile utilizzare un ID Apple gestito con un particolare servizio, come Apple Pay.

N.B. Non tutti i servizi e i contenuti Apple sono disponibili in tutti i Paesi o territori.

Panoramica sulla sicurezza di rete
I meccanismi di protezione integrati da Apple tengono al sicuro le informazioni archiviate sui dispositivi, ma le aziende hanno a disposizione molti sistemi per salvaguardare i dati anche mentre vengono trasmessi da un dispositivo all'altro. In questo caso si parla di sicurezza della rete.

Ogni utente deve poter accedere alle reti aziendali da qualsiasi parte del mondo, quindi è importante assicurarsi che abbia l'autorizzazione necessaria e che i suoi dati siano protetti in fase di trasmissione. Per raggiungere questi obiettivi di sicurezza, iOS, iPadOS e macOS integrano tecnologie collaudate e i più recenti standard per le connessioni su rete Wi-Fi e rete dati cellulare. Ecco perché i nostri sistemi operativi utilizzano protocolli di rete standard per comunicazioni autenticate, autorizzate e criptate, protocolli a cui ha accesso anche chi sviluppa app per le nostre piattaforme.

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/security

Ecosistema di partner
I dispositivi Apple sono compatibili con i principali strumenti e servizi di sicurezza usati nelle aziende, così da garantire la conformità dei dispositivi stessi e dei dati che contengono. Ogni piattaforma supporta i protocolli standard per le VPN (incluse le connessioni VPN per account in iOS e iPadOS 14) e il Wi-Fi sicuro per proteggere il traffico di rete, e si collega in sicurezza all'infrastruttura aziendale.

La partnership di Apple con Cisco permette di creare un ambiente ancora più sicuro grazie all'uso congiunto delle rispettive tecnologie. Le reti Cisco offrono una maggiore sicurezza tramite Cisco Security Connector e danno la priorità alle app aziendali.