Sicurezza di macOS

Panoramica per i reparti IT

Apple ha progettato la piattaforma macOS con un approccio integrato per quanto riguarda hardware, software e servizi, che fornisce sicurezza fin dalle fondamenta e semplifica la configurazione, distribuzione e gestione dei dispositivi. macOS include le tecnologie di sicurezza chiave che servono ai professionisti IT per salvaguardare i dati aziendali e integrare i sistemi negli ambienti di rete protetti dell'azienda. Inoltre Apple ha collaborato con gli enti di certificazione per garantire la conformità con le più recenti specifiche in materia di sicurezza. Questa panoramica illustra brevemente alcune di queste funzioni.

Il documento tratta i seguenti argomenti.

- **Sicurezza del sistema:** il software sicuro e integrato che costituisce le fondamenta di macOS.
- **Crittografia e protezione dei dati:** l'architettura e il design di sistema che proteggono i dati dell'utente in caso di furto o smarrimento del dispositivo.
- **Sicurezza delle app:** i sistemi che proteggono il Mac dal malware e permettono alle app di funzionare in piena sicurezza senza compromettere l'integrità della piattaforma.
- **Autenticazione e firma digitale:** le funzioni incluse in macOS per la gestione delle credenziali e la compatibilità con le tecnologie standard di settore come le smart card e S/MIME.
- **Sicurezza della rete:** protocolli di rete standard di settore che consentono autenticazioni sicure e la crittografia dei dati in transito.
- **Controlli del dispositivo:** metodi che permettono la gestione dei dispositivi Apple, impediscono l'uso non autorizzato, e consentono la cancellazione a distanza se il dispositivo viene smarrito o rubato.

Per saperne di più sulla distribuzione e gestione di macOS, consulta la Guida di riferimento per la distribuzione di macOS su help.apple.com/deployment/macos.

Per informazioni sulle funzioni di sicurezza dei servizi Apple non citati in questo documento, consulta la guida "Sicurezza iOS" su www.apple.com/it/business/docs/iOS_Security_Guide.pdf.

Sicurezza del sistema

La sicurezza dei sistemi macOS è progettata in modo che il software e l'hardware siano sempre protetti, in tutti i componenti chiave di ogni Mac. Questa architettura è essenziale per la sicurezza di macOS e non interferisce mai con l'usabilità dei dispositivi.

UNIX

Il kernel di macOS (il cuore del sistema operativo) si basa sul sistema Berkeley Software Distribution (BSD) e il microkernel Mach. Il sistema BSD fornisce i servizi essenziali per il file system e le reti, uno schema per l'identificazione di utenti e gruppi e molte altre funzionalità di base. Impone inoltre le restrizioni di accesso a file e risorse di sistema a seconda dell'ID di utenti e gruppi.

Il microkernel Mach si occupa di gestione della memoria, controllo dei thread, astrazione dell'hardware e comunicazione tra processi. Le sue porte rappresentano attività e altre risorse, e per imporre l'accesso alle porte il Mach controlla quali attività possono inviarvi messaggi. I criteri di sicurezza BSD e i permessi di accesso Mach costituiscono le fondamenta della sicurezza di macOS e sono essenziali per la sicurezza a livello locale.

La sicurezza del kernel è di importanza fondamentale per la sicurezza dell'intero sistema operativo. La firma del codice protegge il kernel e le estensioni del kernel di terze parti, nonché altre librerie di sistema e gli eseguibili sviluppati da Apple.

Modello basato sul consenso degli utenti

Un aspetto importante della sicurezza Mac è il consenso o il rifiuto dei permessi (o diritti) di accesso. Un permesso si riferisce alla possibilità di eseguire un'operazione specifica, come accedere ai dati o eseguire un codice. I permessi sono assegnati a livello di cartelle, sottocartelle, file e app, oltre che per dati specifici contenuti nei file, determinate funzionalità delle app e funzioni amministrative. Le firme digitali identificano i diritti di accesso delle app e dei componenti di sistema

macOS controlla i permessi a livelli diversi, inclusi i componenti Mach e BSD del kernel. Per controllare i permessi per le app in rete, macOS utilizza i protocolli di rete.

Controlli degli accessi obbligatori

macOS utilizza inoltre i controlli degli accessi obbligatori: criteri che determinano le restrizioni di sicurezza create dallo sviluppatore e che non possono essere bypassati. Questo approccio è diverso dai controlli di accesso discrezionali, che permettono agli utenti di ignorare i criteri di sicurezza secondo le loro preferenze. I controlli degli accessi obbligatori non sono visibili agli utenti, ma costituiscono la tecnologia che rende possibili varie importanti funzioni, tra cui sandboxing, controlli censura, preferenze gestite, estensioni e la protezione dell'integrità di sistema.

Protezione integrità di sistema

OS X 10.11 e le versioni successive includono un livello di sicurezza detto "Protezione integrità di sistema", che limita i componenti alla modalità di sola lettura in determinate posizioni critiche del file system per impedire che vengano eseguiti o modificati da codice pericoloso. Si tratta di un'impostazione specifica del computer attiva di default dopo l'aggiornamento a OS X 10.11; disabilitandola si rimuove la protezione per tutte le partizioni sul dispositivo di archiviazione fisico. macOS applica questo criterio di sicurezza a ogni processo in esecuzione sul sistema, anche a quelli in sandboxing o con privilegi di amministratore.

Per saperne di più su queste aree del file system in sola lettura, leggi l'articolo del Supporto Apple "Informazioni sulla protezione dell'integrità di sistema nel Mac" su support.apple.com/HT204899.

Estensioni kernel

macOS prevede un meccanismo per le estensioni del kernel che consente il caricamento dinamico del codice nel kernel stesso senza bisogno di ricompilarlo o ricollegarlo. Queste estensioni del kernel (KEXT) offrono al tempo stesso modularità e caricamento dinamico, e sono quindi la scelta naturale per ogni servizio relativamente indipendente che deve poter accedere alle interfacce interne del kernel, come i driver dei dispositivi hardware o le app VPN.

Per migliorare la sicurezza dei computer Mac, a partire da macOS High Sierra per caricare le estensioni del kernel è necessario il consenso dell'utente. Questa procedura è nota come caricamento delle estensioni del kernel approvate dall'utente. Qualsiasi utente può approvare un'estensione del kernel, anche se non ha privilegi di amministratore.

Le estensioni del kernel non richiedono l'autorizzazione nei casi seguenti:

- Se sono state installate sul Mac prima dell'aggiornamento a macOS High Sierra.
- Se sostituiscono estensioni approvate in precedenza.
- Se il caricamento avviene senza consenso dell'utente perché è stato usato il comando `spctl` disponibile durante l'avvio dalla partizione macOS Recovery.
- Se il consenso al caricamento viene dato attraverso la configurazione MDM per la gestione dei dispositivi mobili. A partire da macOS High Sierra 10.13.2, puoi usare la soluzione MDM per specificare un elenco di estensioni del kernel che si caricheranno senza richiedere il consenso dell'utente. In questo caso il Mac con macOS High Sierra 10.13.2 deve essere registrato in MDM tramite il Device Enrollment Program (DEP) o la registrazione MDM approvata dall'utente.

Per saperne di più sulle estensioni del kernel, leggi l'articolo del Supporto Apple "Come prepararsi alle modifiche apportate alle estensioni del kernel in macOS High Sierra" su support.apple.com/HT208019.

Password del firmware

macOS consente l'uso di una password per impedire modifiche indesiderate alle impostazioni del firmware su un sistema specifico. La password del firmware viene usata per impedire:

- l'avvio da un volume di sistema non autorizzato;
- l'alterazione della procedura di avvio, per esempio l'avvio in modalità utente singolo;
- l'accesso non autorizzato a macOS Recovery;
- il Direct Memory Access (DMA) attraverso interfacce come Thunderbolt;
- la modalità disco di destinazione, che richiede il DMA.

N.B. Il chip T2 di Apple in iMac Pro impedisce agli utenti di ripristinare la password del firmware, anche se riescono ad accedere fisicamente al Mac. Sui Mac che non hanno il chip T2, sono necessarie ulteriori precauzioni per impedire agli utenti di accedere fisicamente ai componenti interni.

Internet Recovery

Quando non è possibile eseguire l'avvio dal sistema di recupero integrato, il computer Mac tenta automaticamente di eseguire l'avvio da macOS Recovery via internet. In questi casi, durante l'avvio compare un globo che gira invece del logo Apple. Internet Recovery permette all'utente di reinstallare la versione fornita inizialmente con il Mac oppure quella più recente.

Gli aggiornamenti di macOS sono distribuiti attraverso l'App Store ed eseguiti dall'installer di macOS, che utilizza le firme del codice per assicurare l'integrità e l'autenticità dell'installer e dei suoi pacchetti prima dell'installazione. Analogamente, il servizio Internet Recovery è la fonte autorevole per il sistema operativo in dotazione su un determinato Mac.

Per saperne di più su macOS Recovery, leggi l'articolo del Supporto Apple "Informazioni su macOS Recovery" su support.apple.com/HT201314.

Crittografia e protezione dei dati

Apple File System

Apple File System (APFS) è un nuovo e moderno file system per macOS, iOS, tvOS e watchOS. Ottimizzato per le unità di archiviazione Flash/SSD, offre tecniche crittografiche affidabili, metadati copy-on-write, condivisione dello spazio, clonazione di file e directory, istantanee, dimensionamento rapido delle directory, primitivi atomici a salvataggio sicuro, ed elementi fondamentali di sistema migliorati. Inoltre ha un esclusivo design copy-on-write che usa la coalescenza I/O per massimizzare le prestazioni e garantire al tempo stesso l'affidabilità dei dati.

APFS esegue l'allocazione di spazio su disco su richiesta. Se un singolo contenitore APFS ha più volumi, lo spazio libero disponibile è condiviso e può essere allocato a uno qualsiasi dei singoli volumi, in base alle esigenze. Ogni volume utilizza soltanto una parte del contenitore; di conseguenza, lo spazio disponibile corrisponde alle dimensioni totali del contenitore meno lo spazio usato da tutti i volumi nel contenitore.

Per macOS High Sierra, un contenitore APFS valido deve avere almeno tre volumi, i primi due dei quali sono nascosti all'utente.

- Volume di pre-avvio: contiene i dati necessari per l'avvio di ciascun volume di sistema nel contenitore.
- Volume di recupero: contiene il Disco di recupero.
- Volume di sistema: contiene macOS e la cartella dell'utente.

FileVault

Ogni Mac ha di serie la funzione FileVault che tramite crittografia XTS-AES-128 permette di proteggere tutti i dati archiviati sul computer. La protezione può essere applicata all'intero volume, sia per i dischi interni, sia per le unità rimovibili. Se l'utente inserisce il suo ID Apple e la password durante Impostazione Assistita, l'assistente suggerisce di abilitare FileVault e di archiviare la chiave di recupero in iCloud.

Una volta abilitato FileVault su Mac, l'utente deve fornire le credenziali corrette prima di continuare il processo di avvio e per accedere a modalità di avvio specifiche, come la modalità disco di destinazione. Se non vengono inserite le credenziali di login corrette o una chiave di recupero valida, il volume rimarrà interamente codificato e al sicuro da accessi non autorizzati, anche se l'unità fisica è stata rimossa e connessa a un altro sistema.

Per proteggere i dati in ambiente enterprise, il reparto IT deve definire e imporre i criteri per la configurazione di FileVault tramite MDM. Esistono varie opzioni per gestire i volumi codificati, tra cui chiavi di recupero istituzionali o personali (che volendo si possono archiviare in MDM per l'escrow), o una combinazione di entrambe. Come criterio MDM si può inoltre definire la rotazione delle chiavi.

Immagini disco codificate

In macOS le immagini disco codificate sono un contenitore sicuro che si può usare per archiviare o trasferire documenti riservati o altri file. Vengono create con Utility Disco, che si trova in /Applicazioni/Utility/. Le immagini disco si possono crittografare tramite crittografia AES a 128 bit o a 256 bit. Un'immagine disco attiva viene considerata come un volume locale connesso a un Mac, e gli utenti possono quindi copiare, spostare e aprire i file o le cartelle che contiene. Come con FileVault, i contenuti di un'immagine disco si possono codificare e decodificare in tempo reale. Così facendo, gli utenti hanno a disposizione un metodo per scambiarsi documenti, file e cartelle in modo sicuro: possono salvare l'immagine disco codificata su un supporto rimovibile, inviarla via email oppure archiviarla su un server remoto.

Certificazioni ISO 27001 e 27018

Apple ha ricevuto la certificazione ISO 27001 e ISO 27018 per il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), per l'infrastruttura, lo sviluppo e le attività che supportano i seguenti prodotti e servizi: Apple School Manager, iCloud, iMessage, FaceTime, ID Apple gestiti e iTunes U, secondo quanto previsto dallo Statement of Applicability v2.1 dell'11 luglio 2017. La conformità di Apple con lo standard ISO è stata certificata dalla British Standards Institution (BSI). I certificati di conformità ISO 27001 e ISO 27018 sono disponibili sul sito BSI:

www.bsigroup.com/it-IT/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/it-IT/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Convalida crittografica (FIPS 140-2)

I moduli crittografici di macOS sono stati ripetutamente convalidati per la conformità con gli standard statunitensi FIPS (Federal Information Processing Standard) 140-2 Livello 1 per ogni versione a partire da OS X 10.6. Come avviene per ogni versione importante, Apple sottopone al CMVP i moduli affinché vengano riconvalidati al momento del rilascio del sistema operativo Mac. Questo programma convalida l'integrità delle operazioni di crittografia nelle app di Apple e nelle app di altri sviluppatori che utilizzano correttamente i servizi crittografici di macOS. Tutti i certificati relativi alla convalida della conformità di Apple con lo standard FIPS 140-2 sono visibili sulla pagina del fornitore CMVP. Il programma CMVP conserva i moduli crittografici in due elenchi separati in base al loro stato attuale, consultabili su csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Certificazione Common Criteria (ISO 15408)

In passato Apple ha già ottenuto le certificazioni per macOS in base al programma Common Criteria e si sta riattivando per ottenere la valutazione di macOS High Sierra in base all'Operating System Protection Profile (PP_OSv4.1). Apple continua a valutare e richiedere le certificazioni relative alle versioni nuove e aggiornate dei Collaborative Protection Profile (cPP) oggi disponibili, e ha assunto un ruolo attivo all'interno dell'International Technical Community (ITC) per quanto riguarda lo sviluppo di cPP incentrati sulla valutazione di tecnologie chiave per la sicurezza mobile.

Certificazioni, programmi e linee guida sulla sicurezza

Apple ha collaborato con i governi di tutto il mondo per sviluppare linee guida volte a fornire istruzioni e consigli per il mantenere livelli più alti di sicurezza in caso di ambienti ad alto rischio, un processo noto anche come "hardening del dispositivo". Queste guide offrono informazioni ben definite e controllate su come configurare e usare le funzioni di serie in macOS per una protezione ottimale.

Per informazioni aggiornate su questi aspetti della sicurezza di macOS, leggi l'articolo del Supporto Apple "Linee guida, convalide e certificazioni di sicurezza del prodotto per macOS" su support.apple.com/HT201159.

Sicurezza delle app

macOS include di serie tecnologie per far sì che si possano installare solo app attendibili e per la protezione dal malware. Per garantire che le applicazioni non vengano alterate, macOS adotta inoltre un approccio a più livelli per la protezione runtime e la firma delle app.

Gatekeeper

Per controllare le fonti di provenienza delle app, macOS offre una funzione chiamata Gatekeeper, con la quale utenti e organizzazioni possono scegliere il livello di sicurezza che l'installazione deve rispettare.

Con l'impostazione Gatekeeper più sicura, gli utenti possono installare solo app firmate provenienti dall'App Store. L'impostazione di default consente di installare app dall'App Store e app contenenti un ID sviluppatore valido, che indica che sono state firmate da un certificato emesso da Apple e da allora non sono mai state modificate. Se necessario, Gatekeeper si può disabilitare completamente tramite un comando da Terminale.

In alcuni casi Gatekeeper applica anche la randomizzazione dei percorsi, per esempio quando le app vengono lanciate direttamente da un'immagine disco non firmata o dalla posizione in cui erano state scaricate e decompresse automaticamente. Questa tecnica fa sì che prima della loro apertura le app siano disponibili da una posizione di sola lettura non specificata del file system. Così facendo si impedisce alle app di accedere a codice o contenuti utilizzando i percorsi relativi, ma anche di aggiornarsi automaticamente se vengono lanciate da questa posizione di sola lettura. Se si usa il Finder per spostare un'app nella cartella Applicazioni, per esempio, la randomizzazione dei percorsi non viene più applicata.

Il principale vantaggio in termini di sicurezza che offre il modello di default è la protezione generale di tutto l'ecosistema. Se un autore malintenzionato riesce a impossessarsi della capacità di firmare con un ID sviluppatore, e la usa per distribuire malware, Apple è in grado di rispondere rapidamente revocando il certificato di firma, impedendo così il diffondersi del malware. Protezioni di questo tipo vanno a minare il modello economico della maggior parte delle campagne di malware su Mac e forniscono una sicurezza generale per tutti gli utenti.

Gli utenti possono bypassare temporaneamente queste impostazioni per installare qualsiasi app. Le aziende possono usare la loro soluzione MDM per definire e imporre le impostazioni di Gatekeeper, e per aggiungere certificati ai criteri di affidabilità di macOS per la valutazione della firma del codice.

XProtect

macOS include di serie una tecnologia per riconoscere il malware in base alla firma. Apple monitora costantemente i nuovi ceppi di infezione e aggiorna in automatico le firme XProtect, indipendentemente dagli aggiornamenti di sistema, per proteggere il Mac dai malware. XProtect rileva e blocca automaticamente l'installazione dei malware conosciuti.

Strumento per la rimozione dei malware

Se un malware riesce a farsi strada in un Mac, macOS include anche una tecnologia per rimediare alle infezioni. Oltre a monitorare l'attività di malware nell'ecosistema per poter revocare gli ID sviluppatore (laddove possibile) e rilasciare gli aggiornamenti XProtect, Apple aggiorna anche macOS per rimuovere le infezioni dai sistemi configurati per ricevere gli update automatici di sicurezza. Una volta ricevute le informazioni aggiornate, l'apposito strumento rimuove il malware dopo il successivo riavvio. Lo strumento di rimozione dei malware non riavvia in automatico il Mac.

Aggiornamenti di sicurezza automatici

Apple rilascia gli aggiornamenti per XProtect e per lo strumento di rimozione dei malware in automatico. Di default, macOS ricerca quotidianamente questi aggiornamenti. Per saperne di più, leggi l'articolo del Supporto Apple "Mac App Store: aggiornamenti di sicurezza automatici" su support.apple.com/HT204536.

Protezione runtime

I file, le risorse e il kernel di sistema vengono tenuti separati dallo spazio in cui sono attive le app dell'utente. Tutte le app dell'App Store sono in Sandbox per limitare l'accesso ai dati archiviati da altre app. Se un'app dell'App Store ha bisogno di accedere ai dati di un'altra app, può farlo solo utilizzando le API e i servizi forniti da macOS.

Firma obbligatoria del codice delle app

Tutte le app dell'App Store sono firmate da Apple per garantire che non siano state manomesse o alterate. Apple inoltre firma le app fornite con i dispositivi Apple. Molte app distribuite al di fuori dell'App Store sono firmate dallo sviluppatore usando un certificato ID sviluppatore emesso da Apple (unito a una chiave privata) per poter funzionare con le impostazioni di default di Gatekeeper.

Anche le app esterne all'App Store sono in genere firmate con un certificato ID sviluppatore emesso da Apple. In questo modo puoi controllare che l'app sia genuina e non sia stata manomessa. Anche le app sviluppate in-house andrebbero firmate con un ID sviluppatore emesso da Apple per convalidarne l'integrità.

I controlli degli accessi obbligatori (Mandatory Access Controls, MAC) richiedono la firma del codice per abilitare le autorizzazioni protette dal sistema. Per esempio, il codice delle app che richiedono l'accesso attraverso il firewall deve essere firmato con l'apposita autorizzazione MAC.

Autenticazione e firma digitale

Per conservare in modo pratico e sicuro le credenziali e le identità digitali degli utenti, macOS include il Portachiavi e altri strumenti che supportano l'autenticazione e tecnologie di firma digitale come le smart card e S/MIME.

Architettura di Portachiavi

macOS offre un archivio chiamato Portachiavi in cui si possono conservare in piena sicurezza i nomi utente e le password, incluse le identità digitali, le chiavi di codifica e le note protette. Per accedervi basta aprire l'app Accesso Portachiavi in/Applicazioni/Utility/. Con il Portachiavi gli utenti non dovranno più immettere manualmente le credenziali per ogni risorsa, né ricordarle a memoria. Di default viene creato un portachiavi per ogni utente Mac, ed è possibile crearne altri per esigenze specifiche.

Oltre ai portachiavi utente, macOS usa anche diversi portachiavi a livello di sistema per la gestione delle risorse di autenticazione non relative agli utenti, come le credenziali di rete e le identità dell'infrastruttura a chiave pubblica (PKI, Public Key Infrastructure). Uno di questi è il portachiavi Root di sistema, un archivio non modificabile di certificati root PKI di internet emessi da un'autorità di certificazione (CA), che facilita alcune comuni operazioni legate ai servizi bancari online e all'e-commerce. Analogamente puoi distribuire certificati emessi internamente da un'autorità di certificazione (CA) ai computer Mac gestiti, allo scopo di agevolare la convalida di servizi e siti internet interni.

Framework di autenticazione sicuro

I dati del Portachiavi si trovano in una partizione separata e sono protetti con liste di controllo degli accessi (ACL). Questo significa che le credenziali memorizzate dalle app di sviluppatori esterni non sono accessibili da app con identità diverse, a meno che l'utente non le autorizzi esplicitamente. Un tale livello di protezione permette di proteggere le credenziali di autenticazione memorizzate sui dispositivi Apple per tutt'una serie di app e servizi nella tua organizzazione.

Touch ID

I sistemi Mac con un sensore Touch ID si possono sbloccare usando la propria impronta digitale. La funzione Touch ID però non sostituisce la necessità di una password, che viene ancora richiesta per il login dopo lo spegnimento, il riavvio o il logout dal Mac. Dopo il login, gli utenti possono autenticarsi velocemente con Touch ID quando viene chiesta loro una password.

Possono inoltre usarlo per sbloccare le note protette da password nell'app Note, il pannello Password delle Preferenze di Safari e molti pannelli in Preferenze di Sistema. Per una maggiore sicurezza, gli utenti devono inserire una password invece di usare Touch ID per sbloccare il pannello Sicurezza e Privacy in Preferenze di Sistema. Se FileVault è attivo, gli utenti devono inserire la password anche per gestire le preferenze Utenti e Gruppi. Se più utenti usano lo stesso Mac, possono usare Touch ID per passare da un account all'altro.

Per saperne di più su Touch ID e le sue funzioni di sicurezza, leggi l'articolo del supporto Apple "Informazioni sulle tecnologie evolute di sicurezza con il Touch ID" su support.apple.com/HT204587.

Sblocco automatico con Apple Watch

Gli utenti che hanno un Apple Watch possono usarlo per sbloccare in automatico il loro Mac. Lo standard Bluetooth a basso consumo (Bluetooth Low Energy, BLE) e la tecnologia Wi-Fi peer-to-peer permettono a Apple Watch di sbloccare in piena sicurezza un Mac quando i dispositivi si trovano uno vicino all'altro. Questa funzione richiede un account iCloud per il quale è configurata l'autenticazione a due fattori.

Per i dettagli su questo protocollo e per saperne di più sulle funzioni di Continuity e Handoff, consulta la guida "Sicurezza iOS" su www.apple.com/it/business/docs/iOS_Security_Guide.pdf.

Smart card

A partire da Sierra, macOS include il supporto nativo per le schede PIV di verifica dell'identità personale. Queste schede sono molto diffuse all'interno di organizzazioni commerciali e governative, dove vengono usate per l'autenticazione a due fattori, la firma digitale e la codifica.

Le smart card contengono una o più identità digitali con una coppia di chiavi, una pubblica e una privata, e un certificato associato. Sbloccando la smart card con il PIN (Personal Identification Number), si ottiene l'accesso alle chiavi private usate per le operazioni di autenticazione, codifica e firma. Il certificato determina per quali scopi può essere usata una chiave, a quali attributi è associata, e se è stata convalidata (firmata) da una CA.

Le smart card si possono usare per l'autenticazione a due fattori. In questo caso i due fattori necessari per sbloccare la scheda sono "qualcosa che possiedi" (la scheda) e "qualcosa che conosci" (il PIN). A partire da Sierra, macOS include il supporto nativo per il login tramite finestra di autenticazione della smart card e l'autenticazione del certificato client sui siti web in Safari. Supporta inoltre l'autenticazione Kerberos tramite coppie di chiavi (PKINIT) per l'accesso con Single Sign-On ai servizi compatibili con Kerberos.

Per saperne di più sulla distribuzione di smart card con macOS, consulta la Guida di riferimento per la distribuzione di macOS su help.apple.com/deployment/macos.

Firma digitale e codifica

Nell'app Mail gli utenti possono inviare messaggi firmati e codificati digitalmente. Mail rileva automaticamente gli oggetti degli indirizzi email RFC 822 appropriati con distinzione di maiuscole/minuscole o i nomi alternativi degli oggetti sui certificati di firma digitale e codifica presenti sui token PIV allegati nelle smart card compatibili. Se un account email configurato corrisponde a un indirizzo email su un certificato di firma digitale o di codifica su un token PIV allegato, Mail visualizza automaticamente il pulsante per la firma digitale dell'email nella barra degli strumenti di un nuovo messaggio. Se Mail possiede il certificato di codifica email del destinatario o se può trovarlo nell'elenco indirizzi globale (GAL, Global Address List) di Microsoft Exchange, comparirà l'icona di un lucchetto aperto nella barra degli strumenti del nuovo messaggio. L'icona di un lucchetto chiuso indica che il messaggio verrà inviato codificato utilizzando la chiave pubblica del destinatario.

S/MIME per messaggio

macOS supporta lo standard S/MIME per singolo messaggio: gli utenti S/MIME possono scegliere se firmare e codificare di default tutti i messaggi, oppure se firmare e codificare singoli messaggi in modo selettivo.

Le identità usate con S/MIME si possono distribuire ai dispositivi Apple tramite un profilo di configurazione, una soluzione MDM, il protocollo SCEP (Simple Certificate Enrollment Protocol) o un'autorità di certificazione Microsoft Active Directory.

Sicurezza della rete

Oltre alle protezioni integrate usate da Apple per salvaguardare i dati archiviati sui computer Mac, esistono molte misure per la sicurezza di rete che le organizzazioni possono adottare per proteggere le informazioni in viaggio da e verso un Mac.

Gli utenti di dispositivi mobili devono poter accedere alle reti aziendali da qualsiasi parte nel mondo, perciò è importante assicurarsi che siano autorizzati e che i loro dati siano protetti durante la trasmissione. macOS utilizza protocolli di rete standard, e consente agli sviluppatori di accedervi, per garantire comunicazioni autenticate, autorizzate e codificate. Per raggiungere questi obiettivi in materia di sicurezza, macOS integra tecnologie consolidate e i più recenti standard per le connessioni dati su reti Wi-Fi.

TLS

macOS supporta i protocolli Transport Layer Security (TLS 1.0, TLS 1.1 e TLS 1.2) e DTLS. È compatibile con la crittografia AES-128 e AES-256 e preferisce suite di codifica con perfect forward secrecy. Varie app internet, tra cui Safari, Calendario e Mail, usano automaticamente questo protocollo per instaurare un canale di comunicazione codificata tra il dispositivo e i servizi di rete.

API di alto livello (come CFNetwork) semplificano l'adozione del protocollo TLS da parte degli sviluppatori nelle loro app, mentre API di basso livello (come SecureTransport) permettono un controllo dettagliato. CFNetwork non consente il protocollo SSLv3 e alle app che usano WebKit (come Safari) viene impedito di stabilire una connessione SSLv3.

A partire da macOS High Sierra e iOS 11, i certificati SHA-1 non sono più consentiti per le connessioni TLS a meno che non siano considerati attendibili dall'utente. Anche i certificati con chiavi RSA più brevi di 2048 bit non sono

consentiti. La suite di codifica simmetrica RC4 è stata deprecata in macOS Sierra e iOS 10. Di default, le suite di codifica RC4 non sono abilitate per i client e i server TLS implementati con le API SecureTransport, e non sono in grado di eseguire la connessione quando è disponibile solamente la suite di codifica RC4. Per una maggiore protezione, è necessario aggiornare i servizi o le app che richiedono la codifica RC4 affinché possano usare suite di codifica moderne e sicure.

App Transport Security

App Transport Security fornisce i requisiti di default per le connessioni, in modo che le app rispettino le best practice per le connessioni sicure quando usano le API NSURLConnection, CFURL o NSURLSession. Di default, App Transport Security limita la selezione della codifica includendo solamente suite che forniscono la forward secrecy, in particolare ECDHE_ECDSA_AES e ECDHE_RSA_AES in modalità GCM o CBC. Le app possono disabilitare il requisito di forward secrecy in base al dominio, e in tal caso RSA_AES viene aggiunta al set di codifiche disponibili.

I server devono supportare TLS 1.2 e forward secrecy, e i certificati devono essere validi e firmati tramite SHA-256 o superiore con chiave RSA da almeno 2048 bit o una chiave a curva ellittica da 256 bit.

Le connessioni di rete che non rispettano questi requisiti non funzioneranno, a meno che l'app non bypassi l'App Transport Security. Con un certificato non valido si avrà sempre un errore grave che impedisce la connessione. App Transport Security viene applicata in automatico alle app compilate per macOS 10.11 o successivo.

VPN

Di solito i servizi di rete sicuri come le connessioni VPN (Virtual Private Network) richiedono impostazioni e configurazioni minime per funzionare con macOS. I computer Mac funzionano con i server VPN compatibili con i seguenti protocolli e metodi di autenticazione:

- IKEv2/IPSec con autenticazione mediante segreto condiviso, certificati RSA, certificati ECDSA, EAP-MSCHAPv2 o EAP-TLS;
- SSL-VPN tramite l'apposita app client disponibile sull'App Store;
- Cisco IPSec con autenticazione utente tramite password, RSA SecurID o CRYPTOCard e autenticazione automatica mediante segreto condiviso e certificati;
- L2TP/IPSec con autenticazione utente tramite password MS-CHAPV2, RSA SecurID o CRYPTOCard, e autenticazione automatica mediante segreto condiviso.

Oltre alle soluzioni VPN di fornitori esterni, macOS supporta:

- **VPN su richiesta** per le reti che utilizzano l'autenticazione basata su certificato; per specificare quali domini richiedono una connessione VPN, i criteri IT usano un profilo di configurazione.
- **VPN per app** per gestire le connessioni VPN in modo molto più dettagliato. La soluzione MDM può specificare una connessione per ogni app gestita e per domini specifici in Safari, e garantire che sulla rete aziendale viaggino solo i dati protetti e non quelli personali.

Wi-Fi

macOS supporta i protocolli Wi-Fi standard di settore, tra cui WPA2 Enterprise, per fornire l'accesso autenticato alle reti wireless aziendali. WPA2 Enterprise utilizza la crittografia AES a 128 bit, dando agli utenti la massima sicurezza che i loro dati rimarranno protetti quando inviano e ricevono comunicazioni su una rete Wi-Fi. Grazie alla compatibilità con 802.1X, i computer Mac si possono integrare in un'ampia gamma di ambienti di autenticazione RADIUS. I metodi per l'autenticazione wireless 802.1X comprendono EAP-TLS, EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1 e LEAP.

L'autenticazione WPA/WPA2 Enterprise si può usare anche nella finestra di login di macOS, in modo che l'utente possa eseguire l'accesso per autenticarsi in rete.

Impostazione Assistita di macOS supporta l'autenticazione 802.1X con le credenziali (nome utente e password) tramite TTLS o PEAP.

Firewall

macOS include di serie un firewall per proteggere il Mac dagli accessi di rete e gli attacchi denial-of-service. Può essere configurato per:

- impedire tutte le connessioni in entrata, indipendentemente dall'app;
- consentire automaticamente al software integrato di ricevere le connessioni in entrata;
- consentire automaticamente al software attendibile scaricato di ricevere le connessioni in entrata;
- consentire o impedire l'accesso in base alle app specificate dall'utente;
- impedire al Mac di rispondere a richieste di sondaggi ICMP e portscan.

Single Sign-On

macOS supporta l'autenticazione alle reti aziendali mediante Kerberos, che viene usato dalle app per consentire agli utenti l'accesso ai servizi per i quali sono autorizzati. Kerberos si può usare anche per una serie di attività di rete, dalle sessioni sicure di Safari, all'autenticazione del file system di rete, alle app di sviluppatori esterni. È supportata anche l'autenticazione basata sui certificati (PKINIT), ma richiede che le app adottino un'API sviluppatore.

I token GSS-API SPNEGO e il protocollo HTTP Negotiate funzionano con i gateway di autenticazione Kerberos e i sistemi Windows Integrated Authentication compatibili i ticket Kerberos. Il supporto Kerberos si basa sul progetto open source Heimdal.

Sono supportati i seguenti tipi di crittografia:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Per configurare Kerberos, è necessario acquisire i ticket con Visore ticket, fare il login a un dominio Windows Active Directory, oppure usare lo strumento da riga di comando `kinit`.

Sicurezza di AirDrop

I computer Mac compatibili con AirDrop usano lo standard BLE e una tecnologia Wi-Fi peer-to-peer creata da Apple per inviare file e informazioni ai dispositivi nelle vicinanze, tra cui i dispositivi iOS compatibili con AirDrop con iOS 7 o successivo. Il segnale radio Wi-Fi viene usato per stabilire una comunicazione

diretta fra i dispositivi senza bisogno di una connessione internet né di un punto di accesso Wi-Fi. Il collegamento è crittografato tramite TLS.

Per saperne di più su AirDrop, la sicurezza di AirDrop e altri servizi Apple, leggi la sezione "Sicurezza della rete" della guida "Sicurezza iOS" suwww.apple.com/it/business/docs/iOS_Security_Guide.pdf.

Controlli del dispositivo

macOS supporta criteri e impostazioni di sicurezza flessibili, facili da imporre e da gestire. In questo modo le organizzazioni sono in grado di proteggere le proprie informazioni e garantire che i dipendenti rispettino i requisiti aziendali, anche se usano computer di loro proprietà, per esempio nell'ambito di un programma "bring your own device" (BYOD).

Le organizzazioni hanno a disposizione risorse come la protezione mediante password, i profili di configurazione e soluzioni MDM di fornitori esterni per gestire i dispositivi e tenere al sicuro i dati aziendali, anche quando i dipendenti vi accedono da un computer Mac personale.

Protezione mediante password

Sui computer Mac con Touch ID, la lunghezza minima del codice è di otto caratteri. È sempre consigliabile usare codici lunghi e complessi, perché sono più difficili da indovinare o attaccare.

Gli amministratori possono imporre codici complessi e altri criteri tramite la soluzione MDM o richiedendo agli utenti di installare manualmente i profili di configurazione. Per installare il payload "Requisiti codici" è necessaria una password di amministratore.

Per i dettagli su ogni criterio disponibile nelle impostazioni MDM, consulta help.apple.com/deployment/mdm/#/mdm4D6A472A.

Per i dettagli per gli sviluppatori su ogni criterio, consulta la pagina Configuration Profile Reference su developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef.

Imposizione delle configurazioni

Un profilo di configurazione è un file XML che consente a un amministratore di distribuire informazioni di configurazione ai computer Mac. Se l'utente rimuove un profilo di configurazione, tutte le impostazioni definite nel profilo saranno a loro volta rimosse. Gli amministratori possono imporre specifiche impostazioni associando dei criteri al collegamento Wi-Fi e all'accesso dei dati. Per esempio, un profilo di configurazione con le impostazioni per le email può anche specificare un criterio per la password del dispositivo: l'utente potrà accedere alla posta solo se la password rispetta i requisiti dell'amministratore.

Un profilo di configurazione di macOS contiene una serie di impostazioni, tra cui:

- Criteri per i codici
- Restrizioni sulle funzioni del dispositivo (per esempio per disabilitare la fotocamera)
- Impostazioni Wi-Fi o VPN
- Impostazioni di Mail o del server Exchange
- Impostazioni del servizio di directory LDAP
- Impostazioni del firewall
- Credenziali e chiavi
- Aggiornamenti software

Per un elenco aggiornato dei profili di configurazione, consulta la pagina di riferimento su help.apple.com/deployment/mdm/#/mdm5370d089.

I profili di configurazione si possono firmare e codificare per convalidarne l'origine, garantirne l'integrità e proteggerne i contenuti. Si possono inoltre vincolare a un Mac per impedirne completamente la rimozione o per consentirne la rimozione solo mediante password. I profili di configurazione che registrano un Mac in una soluzione MDM si possono rimuovere, ma così facendo si rimuovono anche le informazioni, i dati e le app della configurazione gestita.

Gli utenti possono installare i profili di configurazione scaricati da Safari, ricevuti con un messaggio di posta o inviati over-the-air tramite soluzione MDM. Quando l'utente configura un Mac nel DEP o in Apple School Manager, il computer scarica e installa automaticamente un profilo per la registrazione MDM.

Soluzione MDM

macOS supporta la gestione MDM, con cui le aziende possono configurare e gestire in sicurezza distribuzioni su larga scala di Mac, iPhone, iPad e Apple TV all'interno della propria organizzazione. Le funzioni MDM si basano sulle tecnologie già presenti nella piattaforma macOS, come i profili di configurazione, la registrazione over-the-air e il servizio di notifiche push di Apple (APNs), che viene usato per esempio per riattivare il dispositivo affinché possa comunicare direttamente con la soluzione MDM tramite una connessione sicura. Tramite il servizio APNs non vengono trasmesse informazioni riservate o proprietarie.

Con una soluzione MDM, i reparti IT possono registrare i computer Mac in un ambiente, configurare e aggiornare le impostazioni in wireless, monitorare il rispetto dei criteri aziendali e perfino cancellare o bloccare a distanza i computer Mac gestiti.

Registrazione dei dispositivi

La registrazione dei dispositivi, prevista da Apple School Manager e dagli Apple Deployment Program, offre un modo semplice e veloce per distribuire in un'azienda computer Mac acquistati direttamente da Apple o da un Rivenditore Autorizzato Apple che partecipa al programma.

Le organizzazioni possono registrare automaticamente i computer sul server MDM prima di consegnarli agli utenti, senza doverli toccare o preparare materialmente. Dopo la registrazione, gli amministratori accedono all'apposito sito web e collegano il programma alla loro soluzione MDM. I computer acquistati possono quindi essere assegnati automaticamente tramite la soluzione MDM. Una volta registrato il Mac, qualsiasi configurazione, restrizione o controllo specificato via MDM viene installato in automatico. Tutte le comunicazioni tra i computer e i server Apple sono codificate in transito con HTTPS (SSL).

Per rendere gli utenti operativi in pochi istanti, è possibile snellire ulteriormente la configurazione eliminando alcuni passaggi di Impostazione Assistita. Gli amministratori possono anche scegliere se consentire o meno all'utente di rimuovere il profilo MDM dal computer, e garantire che le restrizioni del dispositivo siano applicate fin dall'inizio. Una volta acceso il computer, il Mac si registra nella soluzione MDM dell'organizzazione e tutte le impostazioni di gestione, le app e i libri sono già installati. N.B. Il Device Enrollment Program non è disponibile in tutti i Paesi o territori.

Per ulteriori informazioni relative alle aziende, consulta la Guida per gli Apple Deployment Program su help.apple.com/deployment/business. Per ulteriori informazioni relative agli istituti didattici, consulta l'Aiuto di Apple School Manager su help.apple.com/schoolmanager.

Restrizioni

Gli amministratori possono abilitare le restrizioni (o in alcuni casi disabilitarle) per impedire agli utenti di accedere a determinate app, servizi o funzioni del dispositivo. Le restrizioni vengono inviate ai dispositivi tramite un apposito payload contenuto in un profilo di configurazione, e si possono applicare ai dispositivi macOS, iOS e tvOS.

Per un elenco aggiornato delle restrizioni a disposizione dei manager IT, visita help.apple.com/deployment/mdm/#/mdm2pHf95672

Cancellazione e blocco a distanza

I computer Mac possono essere cancellati a distanza da un amministratore o da un utente. La cancellazione a distanza immediata è disponibile soltanto se sul Mac è attivo FileVault. Quando viene inviato il comando da MDM o iCloud, il computer risponde con una conferma ed esegue la cancellazione. Nel caso del blocco a distanza, MDM richiede che al Mac venga applicato un codice a sei cifre, impedendo l'accesso se questo non viene inserito.

Privacy

Per Apple la privacy è un diritto fondamentale, perciò tutti i prodotti sono progettati in modo che le elaborazioni avvengano il più possibile sul dispositivo. Inoltre limitano la raccolta e l'uso dei dati personali, forniscono trasparenza e controllo sulle proprie informazioni, e si basano su solide fondamenta di sicurezza.

Apple offre di serie numerosi controlli e opzioni che permettono agli utenti macOS di decidere quali informazioni personali possono usare le app, in che modo e quando. Per saperne di più, vai su www.apple.com/it/privacy.