Apple at Work

Seguridad de la plataforma

Dispositivos diseñados para ser seguros.

En Apple, la seguridad es primordial, tanto para el usuario como para proteger datos empresariales. Desde el principio, hemos incorporado medidas de seguridad avanzadas en nuestros productos, lo cual hace que el diseño sea seguro. Hemos hecho esto de una forma que, a la vez, ofrece a los usuarios una experiencia única, ya que tienen la libertad de trabajar como quieran. Solo Apple puede ofrecer este enfoque integral en cuanto a la seguridad, ya que creamos productos con hardware, software y servicios integrados.

Seguridad del hardware
Para que el software sea seguro, es necesario contar con una base de seguridad incorporada en el hardware. Es por eso que los dispositivos Apple, que funcionan con iOS, iPadOS, macOS, tvOS o watchOS, tienen capacidades de seguridad desarrolladas en silicio.

Entre estas, se incluyen capacidades personalizadas de la CPU, que impulsan funcionalidades de seguridad del sistema, así como silicio adicional destinado a las funciones de seguridad. El hardware centrado en la seguridad admite funciones limitadas y sutilmente definidas para minimizar la superficie de ataque. Entre dichos componentes, se incluyen una ROM de arranque, que forma una raíz de confianza para el hardware a fin de que el arranque sea seguro; motores AES pensados para que los procesos de encriptación y desencriptación sean eficaces y seguros; y un Secure Enclave.

Secure Enclave es un sistema en chip (SoC) que se incluye en todos los dispositivos iPhone, iPad, Apple Watch, Apple TV y HomePod de generaciones recientes, además de en las Mac con Apple Silicon y en las que tienen el chip Apple T2 Security. Secure Enclave sigue el mismo principio de diseño que el SoC (es decir, contiene su propia ROM de arranque sutil y su propio motor AES). Secure Enclave también ofrece la base para crear y almacenar de forma segura las claves necesarias para encriptar los datos almacenados. Además, protege y evalúa los datos biométricos que se usan con Touch ID y Face ID.

El proceso de encriptación del almacenamiento debe ser rápido y eficaz. Al mismo tiempo, no puede exponer los datos (o los materiales de codificación) que se usan para establecer relaciones de codificación criptográfica. El motor AES del hardware resuelve este problema, ya que encripta y desencripta en línea rápidamente a medida que los archivos se escriben o se leen. Secure Enclave tiene un canal especial que proporciona los materiales de codificación que necesita el motor AES sin exponer esta información al procesador de apps (o CPU) o al sistema operativo general. De ese modo, la tecnología de FileVault y la protección de datos de Apple protegen los archivos de los usuarios sin exponer claves de encriptación duraderas.

Apple diseñó un arranque seguro para proteger los niveles más bajos de software contra la manipulación y para permitir que solo el software del sistema operativo confiable de Apple se cargue al inicio. El arranque seguro se inicia en un código inmutable, denominado "ROM de arranque", que se establece durante la fabricación del SoC de Apple y se conoce como la raíz de confianza del hardware. En computadoras Mac con un chip T2, la confianza en el arranque seguro de macOS comienza con el T2. (Tanto el chip T2 como Secure Enclave ejecutan sus propios procesos de arranque seguro a través de sus propias ROM de arranque. Esta es una analogía exacta sobre cómo los chips de la serie A y M1 arrancan de forma segura).

Secure Enclave también procesa los datos de las huellas digitales y los rostros de los sensores de Touch ID y Face ID en dispositivos Apple. Esto hace que la autenticación sea segura y que, a la vez, se mantenga la privacidad y la seguridad de los datos biométricos del usuario. También permite a los usuarios beneficiarse de la seguridad que brindan las contraseñas y los códigos más largos y complejos y, en muchas situaciones, la conveniencia que ofrece la autenticación con Swift para obtener acceso o realizar compras.

Estas funcionalidades de seguridad de los dispositivos Apple son posibles gracias a la combinación del diseño de silicio, el hardware, el software y los servicios exclusivos de Apple.

Seguridad del sistema

En función de las capacidades únicas del hardware de Apple, la seguridad del sistema es responsable de controlar el acceso a los recursos del sistema en los dispositivos Apple sin comprometer la usabilidad. La seguridad del sistema abarca el proceso de arranque; las actualizaciones de software; y la protección de los recursos del sistema informático, como la CPU, la memoria, el disco, los programas de software y los datos almacenados.

Las versiones más recientes de los sistemas operativos de Apple son las más seguras. Una parte importante de la seguridad de Apple es el arranque seguro, que protege el sistema contra infecciones de malware en el momento del arranque. El arranque seguro comienza en el hardware y crea una cadena de confianza a través del software, donde cada paso asegura que el siguiente se ejecute correctamente antes de delegar el control. Este modelo de seguridad es compatible no solo con el arranque predeterminado de los dispositivos Apple, sino también con los distintos modos de recuperación y actualizaciones oportunas en los dispositivos Apple. Algunos componentes secundarios, como el chip T2 y Secure Enclave, también ejecutan su propio arranque para asegurarse de arrancar código de Apple en buen estado. El sistema de actualización puede incluso prevenir ataques de desactualización, de modo que los dispositivos no se puedan revertir a una versión anterior del sistema operativo (que un atacante sabe cómo comprometer) como método para robar datos del usuario.

Los dispositivos Apple también incluyen medidas de protección de arranque y de tiempo de ejecución para mantener su integridad durante el funcionamiento continuo. El silicio diseñado por Apple en los dispositivos iPhone, Apple Watch, Apple TV, HomePod y Mac con Apple Silicon tiene una arquitectura común para proteger la integridad del sistema operativo. En macOS, también se incluye una serie expandida y configurable de capacidades de protección para abarcar los distintos modelos de computación, así como capacidades compatibles en todas las plataformas de hardware de Mac.

Encriptación y protección de datos
Los dispositivos Apple tienen funcionalidades de encriptación para proteger los datos del usuario y permitir el borrado remoto ante el robo o la pérdida del dispositivo.

La cadena de arranque segura, la seguridad del sistema y las capacidades de seguridad de las apps ayudan a verificar que solo el código y las apps confiables se ejecuten en un dispositivo. Los dispositivos Apple tienen funcionalidades de encriptación adicionales para resguardar los datos del usuario, incluso cuando otras partes de la infraestructura de seguridad se ven comprometidas (por ejemplo, si un dispositivo se pierde o ejecuta código que no es de confianza). Todas estas funcionalidades benefician a los usuarios y a los administradores de TI, ya que protegen la información personal y empresarial, y proporcionan métodos de borrado instantáneo y remoto ante el robo o la pérdida del dispositivo.

Los dispositivos iOS y iPadOS usan una metodología de encriptación de archivos llamada Protección de datos, mientras que los datos de las computadoras Mac con procesadores Intel están protegidos con una tecnología de encriptación de volumen llamada FileVault. Las Mac con Apple Silicon usan un modelo híbrido compatible con Protección de datos, con dos advertencias: el nivel de protección más bajo (Clase D) no es compatible, y el nivel predeterminado (Clase C) usa una clave de volumen y actúa como FileVault en una Mac con procesador Intel. En todos los casos, las jerarquías de administración de claves están arraigadas en el silicio dedicado de Secure Enclave. Asimismo, un motor AES dedicado es compatible con la encriptación de velocidad de línea y ayuda a garantizar que las claves de encriptación duraderas no estén expuestas al sistema operativo del kernel o la CPU (donde podrían verse comprometidas). (Una Mac con procesador Intel y un chip T1 o que no tiene Secure Enclave no usa silicio dedicado para proteger sus claves de encriptación de FileVault).

Además de usar Protección de datos y FileVault para evitar el acceso no autorizado a los datos, los kernels del sistema operativo de Apple refuerzan la protección y la seguridad. El kernel usa controles de acceso a las apps de la zona protegida (que restringe a qué datos puede acceder una app) y un mecanismo llamado Data Vault (que restringe el acceso a los datos de una app de todas las demás apps solicitantes en lugar de restringir las llamadas que una app puede realizar).

Seguridad de las apps
Las apps se encuentran entre los elementos más importantes de la arquitectura de seguridad. Aunque las apps les brindan increíbles beneficios de productividad a los usuarios, también pueden llegar a tener un impacto negativo sobre la seguridad, la estabilidad y los datos del usuario del sistema si no se gestionan de forma correcta.

Por este motivo, Apple proporciona capas de protección para garantizar que las apps estén libres de malware conocido y que no se hayan manipulado. Las medidas de protección adicionales hacen que el acceso que tienen las apps a los datos del usuario se medie con cuidado. Estos controles de seguridad brindan una plataforma segura y estable para las apps, lo cual les permite a los miles de desarrolladores enviar cientos de miles de apps para iOS, iPadOS y macOS (todo ello sin afectar la integridad del sistema). Además, los usuarios pueden acceder a estas apps en los dispositivos Apple sin temor a los virus, el malware o los ataques no autorizados.

En el iPhone, iPad o iPod touch, todas las apps se obtienen de App Store (y todas las apps están en una zona protegida) para proporcionar los controles más estrictos.

En la Mac, muchas apps se obtienen de App Store, pero los usuarios de Mac también descargan y usan apps de Internet. Para que la descarga de Internet sea segura, macOS usa controles adicionales. Primero, de forma predeterminada en macOS 10.15 o posteriores, Apple debe certificar todas las apps de Mac antes de la publicación. Este requisito es útil para asegurarse de que las apps no tengan malware conocido sin requerir que las apps deban estar disponibles a través de App Store. Además, macOS incluye protección antivirus de última generación para bloquear (y, si es necesario, eliminar) el malware.

Como control adicional en las plataformas, la zona protegida ayuda a proteger los datos del usuario contra los accesos no autorizados de las apps. Además, en macOS, los datos que se encuentran en áreas importantes están protegidos en sí mismos, lo cual ayuda a garantizar que los usuarios no pierdan el control del acceso desde todas las apps a los archivos que están en el escritorio, en las carpetas de documentos y de descargas, y en otras áreas, ya sea que las apps que intentan acceder estén en una zona protegida o no.

Seguridad de los servicios

Apple creó un sólido conjunto de servicios para ayudar a los usuarios a obtener aún más utilidad y productividad de sus dispositivos. Estos servicios brindan capacidades potentes para el almacenamiento en la nube, la sincronización, el almacenamiento de contraseñas, la autenticación, los pagos, los servicios de mensajería, las comunicaciones, etc., a la vez que se protegen la privacidad y la seguridad de los datos del usuario.

Entre estos servicios, se incluyen iCloud, Iniciar Sesión con Apple, Apple Pay, iMessage, Business Chat, FaceTime, Encontrar y Continuidad. También es posible que estos servicios requieran que el usuario cuente con un Apple ID o un Apple ID administrado. En algunos casos, los Apple ID administrados no se pueden usar con servicios específicos, como Apple Pay.

Nota: No todos los servicios y el contenido de Apple están disponibles en todos los países o regiones.

Descripción general de la seguridad de la red

Además de las medidas de seguridad integradas que usa Apple para proteger los datos almacenados en los dispositivos Apple, hay muchas medidas que las organizaciones pueden tomar para mantener la información segura mientras circula hacia y desde un dispositivo. Todas estas medidas se clasifican dentro de la seguridad de la red.

Los usuarios necesitan acceso a redes empresariales de cualquier parte del mundo, por lo que es importante asegurarse de que estén autorizados y de que sus datos estén protegidos durante la transmisión. Para cumplir con estos objetivos de seguridad, iOS, iPadOS y macOS integran tecnologías probadas y los últimos estándares relacionados con las conexiones de redes celulares y Wi-Fi. Por eso, nuestros sistemas operativos usan protocolos de redes estándares para las comunicaciones autenticadas, autorizadas y encriptadas, y les brindan acceso a los desarrolladores a los mismos protocolos.

Ecosistema de socios

Los dispositivos Apple funcionan con herramientas y servicios comunes de seguridad empresarial, lo que garantiza el cumplimiento de los dispositivos y los datos que residen en ellos. Cada plataforma es compatible con protocolos estándares de VPN (incluidas las conexiones de VPN por cuenta en iOS y iPadOS 14) y Wi-Fi seguro para proteger el tráfico de la red. Además, cada plataforma se conecta de forma segura a las infraestructuras empresariales comunes.

La asociación de Apple con Cisco brinda mayor seguridad y productividad cuando se combinan. Las redes de Cisco brindan una seguridad mejorada a través del conector de seguridad de Cisco y otorgan prioridad a las apps empresariales en las redes de Cisco.

Obtén más información sobre la seguridad con los dispositivos Apple.

apple.com/business/it

apple.com/macos/security

apple.com/privacy/features

apple.com/security