Apple at Work

Seguridad de la plataforma

Diseñado para ser seguro.

En Apple damos muchísima importancia a la seguridad del usuario y los datos corporativos. Nuestros productos están diseñados para ser seguros gracias a prestaciones avanzadas en todos los niveles. Y todo sin interferir en la experiencia del usuario y dándole libertad absoluta para trabajar como quiera. Solo Apple puede ofrecer este nivel de seguridad, ya que el hardware, el software y los servicios de todos nuestros productos están perfectamente integrados.

Seguridad del hardware
Sin un hardware seguro, no hay software seguro que valga. Por eso los dispositivos Apple (con iOS, iPadOS, macOS, tvOS y watchOS) integran funcionalidades de seguridad en el propio chip.

Esto incluye características personalizadas de la CPU que hacen posibles las prestaciones de seguridad del sistema y el chip. La seguridad del hardware se basa en el principio de ofrecer funciones limitadas y definidas de forma individual para reducir al máximo la superficie de ataque. Entre sus componentes hay una ROM de arranque que proporciona una raíz de confianza de hardware para ofrecer un arranque seguro, motores AES dedicados para cifrar y descifrar los datos de la forma más segura y eficiente, y el Secure Enclave.

El Secure Enclave es un sistema en chip (SoC) que está incluido en todos los iPhone, iPad, Apple Watch, Apple TV y HomePod recientes, así como en los Mac con chips de fabricación propia y el chip T2 Security de Apple. El Secure Enclave sigue el mismo principio de diseño que el sistema en chip, por lo que incluye una ROM de arranque y un motor AES. Además, cuenta con tecnologías básicas que permiten generar y almacenar de forma segura las claves necesarias para cifrar los datos en reposo, así como proteger y evaluar los datos biométricos de Touch ID y Face ID.

El cifrado de los datos almacenados debe hacerse de forma rápida y eficiente sin exponer el material que utiliza para establecer relaciones entre las claves criptográficas. Para ello, el motor de hardware AES cifra y descifra los archivos a medida que se leen o escriben. Un canal especial del Secure Enclave proporciona

los materiales necesarios al motor AES sin compartir esta información con el procesador de aplicaciones (es decir, la CPU) ni el sistema operativo. De esta forma, la tecnología de protección de datos de Apple y FileVault protegen los archivos del usuario sin revelar las claves de cifrado de larga duración.

Apple ha diseñado el arranque seguro para proteger el software de bajo nivel frente a manipulaciones y cargar únicamente software de sistema operativo de Apple. El arranque seguro comienza con la ROM de arranque, un código inmutable que se crea durante la fabricación del chip y que se conoce como «raíz de confianza» del hardware. En los ordenadores Mac con el chip T2, esta tecnología de arranque seguro comienza en el propio chip. (Tanto el chip T2 como el Secure Enclave ejecutan los procesos de arranque seguro en sus propias ROM de arranque, al igual que los chips de la serie A y el chip M1.)

El Secure Enclave también procesa los datos faciales y de las huellas dactilares que se obtienen mediante los sensores Face ID y Touch ID de los dispositivos Apple, lo que permite autenticarse de forma segura y mantener la privacidad de los datos biométricos. Además, los usuarios pueden compatibilizar el uso de contraseñas y códigos más largos y complejos con la comodidad de autenticarse rápidamente para comprar o iniciar sesión en muchas situaciones.

Las prestaciones de seguridad de los dispositivos Apple son posibles gracias a una combinación de chips, hardware, software y servicios que solo están disponibles en Apple.

Seguridad del sistema

La seguridad del sistema, basada en las funcionalidades únicas del hardware de Apple, se encarga de controlar el acceso a los recursos del sistema en nuestros dispositivos sin renunciar a la facilidad de uso. La seguridad del sistema engloba el proceso de arranque, las actualizaciones de software y la protección de recursos del sistema como la CPU, la memoria, el disco, los programas y los datos almacenados.

Las últimas versiones de los sistemas operativos de Apple son las más seguras. Una parte fundamental de la seguridad de Apple es el arranque seguro, que protege el sistema del software malicioso desde que se enciende el dispositivo. El arranque seguro comienza con el hardware y crea una cadena de confianza a través del software, donde cada paso verifica que el siguiente funciona correctamente antes de ceder el control. Este modelo de seguridad no solo funciona con el arranque por omisión de los dispositivos Apple, sino también en los distintos modos de recuperación y actualización de dispositivos Apple. Algunos subcomponentes, como el chip T2 y el Secure Enclave, también realizan su propio arranque seguro para ejecutar únicamente código de confianza procedente de Apple. El sistema de actualización previene incluso ataques en los que los dispositivos retroceden a una versión anterior del sistema operativo (y, por tanto, más vulnerable) como método para sustraer los datos del usuario.

Los dispositivos Apple incluyen medidas de protección para el arranque y la ejecución de forma que conservan su integridad mientras están en uso. Los chips diseñados por Apple para el iPhone, iPad, Apple Watch, Apple TV y HomePod, así como los chips fabricados por Apple para el Mac, tienen una arquitectura común que protege la integridad del sistema operativo. macOS también incluye un conjunto de prestaciones de seguridad ampliadas y configurables que están

hechas a la medida de su modelo computacional, además de funcionalidades admitidas en todas las plataformas de hardware del Mac.

Cifrado y protección de los datos
Los dispositivos Apple incluyen prestaciones de cifrado para proteger los datos del usuario y permitir el borrado remoto en caso de robo o pérdida.

La cadena de arranque seguro, la seguridad del sistema y las prestaciones de seguridad de las apps se ocupan de que solo se ejecuten en el dispositivo el código y las apps de confianza. Los dispositivos Apple cuentan con prestaciones de cifrado adicionales para proteger los datos del usuario, incluso cuando otras partes de la infraestructura de seguridad están en peligro (por ejemplo, si el dispositivo se pierde o ejecuta código que no es de confianza). Todas estas prestaciones benefician tanto a los usuarios como a los administradores de TI, ya que protegen la información personal y corporativa y proporcionan métodos para borrar el dispositivo a distancia y de forma inmediata en caso de robo o pérdida.

Los dispositivos iOS y iPadOS usan la protección de datos como método de cifrado de archivos, mientras que la información de los ordenadores Mac se protege mediante la tecnología FileVault de cifrado de volúmenes. Los ordenadores Mac con chips de Apple emplean un modelo híbrido que es compatible con la protección de datos con dos matices: el nivel de protección más bajo (clase D) no está admitido y el nivel predeterminado (clase C) utiliza una clave de volumen, por lo que desempeña el mismo papel que FileVault en los Mac con procesadores de Intel. En cualquier caso, las jerarquías de la gestión de claves están integradas en el chip independiente del Secure Enclave y hay un motor AES dedicado que permite el cifrado inmediato e impide que las claves de cifrado de larga duración queden expuestas al sistema operativo del kernel y a la CPU, lo cual podría suponer un riesgo. (Los Mac con procesadores de Intel y el chip T1 no tienen un chip dedicado que protege las claves de cifrado de FileVault, y lo mismo se puede decir de los equipos sin el Secure Enclave.)

La seguridad de los kernels de los sistemas operativos de Apple se combina con la protección de datos y FileVault para impedir el acceso no autorizado a los datos. El kernel utiliza controles de acceso a las apps aisladas (lo que restringe los datos a los que pueden acceder) y un mecanismo llamado FileVault que limita el acceso a los datos de una app a aquellas que lo solicitan en vez de las llamadas que puede hacer una app.

Seguridad de las apps
Las apps son una parte fundamental de una arquitectura de seguridad. Aunque las apps ofrecen a los usuarios muchas ventajas relacionadas con la productividad, también pueden afectar negativamente a la seguridad del sistema, la estabilidad y los datos del usuario si no se gestionan de forma adecuada.

Por esa razón, Apple ofrece capas de protección para garantizar que las apps no contengan ningún software dañino conocido y que no hayan sido manipuladas. Se aplican medidas de seguridad adicionales para el acceso a los datos del usuario desde las apps y se supervisa el proceso cuidadosamente. Estos controles de seguridad integrados crean una plataforma estable y segura que permite a miles de desarrolladores ofrecer cientos de miles de apps para iOS, iPadOS y macOS que no

afectan a la integridad del sistema. Los usuarios pueden acceder a estas apps en sus dispositivos Apple sin temor a virus, software malicioso o ataques.

En el iPhone, el iPad y el iPod touch, todas las apps se descargan del App Store y los procesos están aislados (sandboxing).

En el Mac, muchas apps se descargan del App Store, aunque los usuarios también pueden descargar y usar apps de internet. macOS dispone de controles adicionales para permitir la descarga segura de internet. Para empezar, en macOS 10.15 y las versiones posteriores, todas las apps para Mac tienen que estar certificadas por Apple para poder abrirse. Este requisito garantiza que las apps no contengan software dañino aunque no provengan del App Store. Por si fuera poco, macOS incluye protección antivirus de última generación que bloquea el software malicioso y lo elimina si es necesario.

Como medida adicional, todas las plataformas hacen uso de los procesos aislados (sandboxing) para que las apps sin autorización no puedan acceder a los datos del usuario. Y como en macOS los datos de determinadas áreas también van por separado, los usuarios tienen siempre el control del acceso a los archivos del escritorio, documentos, descargas y otras secciones desde todas las apps, con independencia de si están aisladas o no.

Seguridad de los servicios
Apple ha creado un gran conjunto de servicios para que los usuarios puedan ser aún más productivos con sus dispositivos. Estos servicios ofrecen grandes posibilidades de almacenamiento en la nube, sincronización, guardado de contraseñas, autenticación, pagos, mensajería, comunicación y mucho más, al√tiempo que protegen la privacidad del usuario y los datos.

Entre ellos están iCloud, Iniciar Sesión con Apple, Apple Pay, iMessage, Chat para Clientes, FaceTime, Buscar y Continuidad, que pueden requerir un ID de Apple o un ID de Apple Gestionado. Algunos servicios no permiten utilizar ID de Apple Gestionados, como es el caso de Apple Pay.

Nota: No todos los servicios y contenidos de Apple están disponibles en todos los países y regiones.

Seguridad de la red
Además de las tecnologías de defensa integradas que Apple utiliza para proteger los datos almacenados en sus dispositivos, las empresas disponen de muchas otras medidas de seguridad que sirven para mantener a salvo la información mientras viaja de un dispositivo a otro. Todas estas medidas forman parte de la seguridad de la red.

Los usuarios necesitan acceder a las redes corporativas desde cualquier lugar del mundo, así que es importante asegurarse de que cuentan con autorización y sus datos están protegidos durante su transmisión. Para ello, iOS, iPadOS y macOS integran tecnologías de eficacia probada y los estándares más recientes de conexión a redes wifi y de datos móviles. Ese es el motivo por el que nuestros sistemas operativos utilizan y ponen en manos de los desarrolladores protocolos de red estándar para las comunicaciones autenticadas, autorizadas y cifradas.

Consulta más información sobre la seguridad con los dispositivos Apple.

apple.com/es/business/it

apple.com/es/macos/security

apple.com/es/privacy/features

apple.com/security

Ecosistema de socios

Los dispositivos Apple son compatibles con las herramientas y servicios más utilizados en las empresas, por lo que el cumplimiento y la seguridad de los datos están garantizados. Todas las plataformas admiten protocolos estándar de VPN (lo que incluye conexiones VPN por cuenta en iOS y iPadOS 14) y redes wifi seguras para proteger el tráfico de red y conectarse a la infraestructura común de la empresa.

La colaboración de Apple con Cisco mejora la seguridad y la productividad cuando se usan ambas tecnologías juntas. Las redes de Cisco ofrecen un mayor seguridad a través de Cisco Security Connector y dan prioridad a las apps empresariales que están en las redes de Cisco.