Apple at Work

Seguridad de la plataforma

Diseñados para ser seguros.

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
Un software seguro necesita basarse un hardware seguro, 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. El componente más esencial es el coprocesador Secure Enclave, incluido en los últimos dispositivos iOS, iPadOS, watchOS y tvOS, además de todos los ordenadores Mac con el chip T2 Security de Apple. El Secure Enclave es la base para cifrar los datos en reposo, arrancar macOS de forma segura y usar los datos biométricos.

Todos los iPhone y iPad más modernos, así como los ordenadores Mac con el chip T2, incluyen un motor de hardware AES independiente que permite el cifrado inmediato al leer o escribir archivos. De esta forma, la tecnología de protección de datos y FileVault protegen los archivos del usuario sin revelar las claves de cifrado de larga duración a la CPU ni al sistema operativo.

El arranque seguro de los dispositivos vela por los niveles de software más bajos para que solo se cargue el software de confianza del sistema operativo. En los dispositivos iOS y iPadOS, la seguridad comienza con un código inmutable llamado Boot ROM que se crea durante la fabricación del chip y que se conoce como «raíz de confianza» del hardware. En los ordenadores Mac con chip T2, esta tecnología de arranque seguro comienza con el propio Secure Enclave.

Detrás de Touch ID y Face ID está el Secure Enclave, que permite a los usuarios autenticarse de forma segura en sus dispositivos Apple sin exponer sus datos biométricos. De este modo, disfrutan de códigos y contraseñas más largos y complejos, además de un acceso cómodo y rápido en muchos casos.

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
Basándose en las funcionalidades únicas del hardware, la seguridad del sistema está diseñada para maximizar la seguridad de los sistemas operativos de Apple sin renunciar a la facilidad de uso. La seguridad del sistema engloba el proceso de arranque, las actualizaciones de software y el funcionamiento continuo del sistema operativo.

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 iOS, iPadOS y macOS.

Las versiones más recientes de iOS, iPadOS y macOS son las más seguras. El mecanismo de actualización de software pone al día los dispositivos Apple únicamente con software de confianza. El sistema de actualización previene incluso ataques en los que los dispositivos retroceden a una versión anterior del sistema operativo como método para sustraer los datos del usuario.

Por último, los dispositivos Apple incluyen medidas de protección para el arranque y la ejecución de forma que conservan su integridad mientras están en uso. Estas medidas de protección varían mucho entre dispositivos iOS, iPadOS y macOS, en función de las distintas funcionalidades que admitan y los ataques que deban afrontar.

Para conseguir este nivel de protección, iOS y iPadOS usan sistemas de integridad del kernel y del coprocesador, códigos de autenticación de puntero y una capa de protección de página. Por su parte, macOS usa el sistema de seguridad Unified Extensible Firmware Interface (UEFI), el modo de gestión del sistema (SMM), protecciones de acceso directo a memoria (DMA) y seguridad del firmware del dispositivo.

Cifrado y protección de 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 ayudan a que solo el código y las apps de confianza se ejecuten en el dispositivo. 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 en todo momento 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 un método de cifrado de archivos llamado «protección de datos», mientras que la información de los ordenadores Mac se protege mediante la tecnología FileVault de cifrado de volumen. La jerarquía de gestión clave de estos dos métodos se basa en el Secure Enclave independiente que incluyen los dispositivos con procesador SEP. Además, ambos modelos utilizan el motor AES, lo que permite un cifrado muy rápido y garantiza que las claves de cifrado de larga duración no se revelen nunca al sistema operativo de kernel ni la CPU, donde podrían correr peligro.

Seguridad de las apps

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

Gracias a los controles de seguridad integrados, se crea una plataforma estable y segura que permite a miles de desarrollares ofrecer cientos de miles de apps para iOS, iPadOS y macOS que no afectan a la integridad del sistema. Y los usuarios pueden acceder a estas apps desde sus dispositivos Apple con controles que los protegen frente a virus, software dañino y 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. Además, macOS incluye una protección antivirus estándar en el sector para bloquear y eliminar el software dañino llegado el caso.

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 en macOS, los datos de determinadas áreas también se aíslan. De este modo, los usuarios tienen siempre el control de acceso a los archivos del escritorio, documentos, descargas y otras secciones desde todas las apps, con independencia de que estén 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 son el ID de Apple, iCloud, Iniciar Sesión con Apple, Apple Pay, iMessage, FaceTime, Siri y Buscar, entre otros. Estos servicios ofrecen grandes posibilidades de almacenamiento en la nube y sincronización, autenticación, pagos, mensajería, comunicación y mucho más, al tiempo que protegen la privacidad del usuario y los datos.

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. Cada plataforma admite protocolos estándar para la VPN y la conexión wifi que protegen el tráfico de red y se conectan de forma segura a los sistemas corporativos más habituales.

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 del Cisco Security Connector y dan prioridad a las apps empresariales que están en las redes de Cisco.

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/es/security