Apple at Work

Segurança da plataforma

Seguro por natureza.

A Apple preocupa-se com a segurança do utilizador e dos dados empresariais. Os nossos produtos foram concebidos para serem seguros, através da integração de medidas de proteção avançadas. A combinação destas medidas com uma experiência de utilizador fantástica proporciona aos utilizadores a máxima liberdade para trabalharem da forma que preferem. Só a Apple consegue proporcionar esta abordagem abrangente à segurança, uma vez que criamos produtos com hardware, software e serviços integrados.

Segurança do hardware
O software seguro requer uma base de segurança integrada no hardware. É por este motivo que os dispositivos Apple com o iOS, iPadOS, macOS, tvOS ou watchOS têm capacidades de segurança integradas no silício.

Isto inclui capacidades personalizadas da CPU que acionam funcionalidades de segurança do sistema e silício dedicado a funções de segurança. O componente mais essencial é o coprocessador Secure Enclave em dispositivos iOS, iPadOS, watchOS e tvOS modernos e em todos os computadores Mac com o processador Apple T2 Security. O Secure Enclave fornece a base da encriptação de dados inativos, do arranque seguro no macOS e da biometria.

Todos os dispositivos iPhone e iPad e computadores Mac modernos com um processador T2 incluem um sistema de hardware AES para acionar a encriptação de velocidade da linha à medida que os ficheiros são gravados ou lidos. Isto garante que a Proteção de dados e o FileVault protegem os ficheiros dos utilizadores sem exporem chaves de encriptação de longa duração à CPU ou ao sistema operativo.

O arranque seguro dos dispositivos Apple assegura que os níveis mais baixos de software não são alterados e que apenas o software aprovado do sistema operativo da Apple é carregado durante o arranque. Em dispositivos iOS e iPadOS, a segurança começa com um código imutável chamado Boot ROM, que é implementado durante o fabrico do processador e é conhecido como a raiz de confiança do hardware. Em computadores Mac com um processador T2, a confiança do arranque seguro começa com o próprio Secure Enclave.

O Secure Enclave permite que o Touch ID e o Face ID nos dispositivos Apple forneçam uma autenticação segura mantendo os dados biométricos do utilizador privados e protegidos. Desta forma, os utilizadores podem tirar

partido da segurança de códigos e palavras-passe mais longos e complexos e, em muitos casos, da conveniência da autenticação rápida.

As funcionalidades de segurança dos dispositivos Apple são possibilitadas pela combinação entre o design do silício, o hardware, o software e os serviços que só a Apple disponibiliza.

Segurança do sistema
Com base nas capacidades únicas do hardware da Apple, a segurança do sistema é concebida para maximizar a segurança dos sistemas operativos nos dispositivos Apple sem comprometer a facilidade de utilização. A segurança do sistema abrange o processo de arranque, as atualizações de software e o funcionamento contínuo do sistema operativo.

O arranque seguro começa pelo hardware e estabelece uma cadeia de confiança no software, onde cada passo assegura que o seguinte funciona corretamente antes de transferir o controlo. Este modelo de segurança suporta o arranque predefinido dos dispositivos Apple e os vários modos de recuperação e atualização de dispositivos iOS, iPadOS e macOS.

As versões mais recentes do iOS, iPadOS e macOS são as mais seguras. O mecanismo de atualização do software oferece atualizações atempadas dos dispositivos Apple e também fornece apenas software aprovado da Apple. O sistema de atualização pode até impedir ataques de retrogradação, para que os dispositivos não regressem a uma versão anterior do sistema operativo através de um método para roubar os dados do utilizador.

Por último, os dispositivos Apple incluem proteções de arranque e tempo de execução para manterem a sua integridade durante o funcionamento contínuo. Estas proteções variam significativamente entre os dispositivos iOS, iPadOS e macOS com base nos conjuntos de capacidades muito diferentes que suportam e os ataques que devem impedir.

Para atingirem este nível de proteção, o iOS e o iPadOS utilizam Proteção da integridade do kernel, Integridade do coprocessador do sistema, Códigos de autenticação de indicadores e Camada de proteção de páginas, enquanto o macOS utiliza segurança de Interface de firmware extensível unificado, Modo de gestão do sistema, proteções de Acesso direto à memória e segurança de firmware periférico.

Encriptação e proteção de dados
Os dispositivos Apple têm funcionalidades de encriptação que protegem os dados do utilizador e permitem a eliminação remota dos dados em caso de roubo ou perda do dispositivo.

As capacidades de cadeia de arranque seguro, segurança do sistema e segurança das apps ajudam a garantir que apenas apps e código aprovados são executados no dispositivo. Os dispositivos Apple têm funcionalidades de encriptação adicionais que protegem os dados do utilizador, mesmo quando outras partes da infraestrutura de segurança são comprometidas (por exemplo, em caso de perda do dispositivo ou execução de código não aprovado). Todas estas funcionalidades beneficiam os utilizadores e os administradores de TI, protegendo as informações pessoais e empresariais de forma contínua e fornecendo métodos de eliminação remota imediata e total dos dados em caso de roubo ou perda do dispositivo.

Os dispositivos iOS e iPadOS utilizam uma metodologia de encriptação de ficheiros chamada Proteção de dados, enquanto os dados nos computadores Mac são protegidos pela tecnologia de encriptação de volumes FileVault. Ambos os modelos integram as hierarquias de gestão principais no silício dedicado do Secure Enclave em dispositivos que incluem um SEP. Os dois modelos também tiram partido de um sistema AES dedicado para permitir a encriptação de velocidade da linha e para garantir que as chaves de

encriptação de longa duração nunca têm de ser fornecidas ao kernel do sistema operativo ou à CPU, onde podem ser comprometidas.

Segurança de apps

As apps estão entre os elementos mais críticos de uma arquitetura de segurança moderna. Embora as apps ofereçam benefícios de produtividade fantásticos aos utilizadores, também têm o potencial de afetar negativamente a segurança do sistema, a estabilidade e os dados dos utilizadores se não forem geridas corretamente. A Apple oferece várias camadas de proteção para garantir que as apps não têm malware conhecido e que não foram alteradas. As proteções adicionais gerem cuidadosamente o acesso das apps aos dados dos utilizadores.

Os controlos de segurança integrados fornecem uma plataforma segura e estável para as apps, o que permite que milhares de programadores distribuam centenas de milhares de apps para iOS, iPadOS e macOS sem afetarem a integridade do sistema. Além disso, os utilizadores podem aceder a estas apps nos dispositivos Apple com controlos que ajudam a proteger contra vírus, malware ou ataques não autorizados.

No iPhone, iPad e iPod touch, todas as apps são obtidas na App Store e colocadas em sandbox de forma a proporcionar controlos mais rigorosos. No Mac, muitas apps são obtidas na App Store, mas os utilizadores do Mac também descarregam e utilizam apps da internet. Para permitir o download seguro na internet, o macOS aplica várias camadas de controlos adicionais. Em primeiro lugar, por predefinição no macOS 10.15 ou posterior, a Apple tem de colocar todas as apps para Mac no sistema notarial antes da sua abertura. Este requisito assegura que as apps não têm malware conhecido sem exigir que as apps sejam fornecidas através da App Store. Adicionalmente, o macOS inclui uma proteção antivírus de referência no setor para bloquear e remover malware, se necessário.

A colocação em sandbox é um controlo adicional em todas as plataformas que ajuda a proteger os dados dos utilizadores do acesso não autorizado por parte das apps. Além disso, no macOS, os dados em áreas críticas são colocados em sandbox (o que assegura que os utilizadores controlam o acesso aos ficheiros na Secretária, pasta Documentos, pasta Descargas e outras áreas) e isolados de todas as apps, quer as apps que tentem obter acesso estejam em sandbox ou não.

Segurança dos serviços

A Apple criou um conjunto robusto de serviços que ajudam os utilizadores a obterem ainda mais utilidade e produtividade com os dispositivos. Estes serviços incluem ID Apple, iCloud, Iniciar sessão com a Apple, Apple Pay, iMessage, FaceTime, Siri e Encontrar. Estes serviços oferecem capacidades avançadas para sincronização e armazenamento na nuvem, autenticação, pagamento, mensagens, comunicações e muito mais, enquanto protegem a privacidade dos utilizadores e a segurança dos seus dados.

Ecossistema de parceiros

Os dispositivos Apple são compatíveis com serviços e ferramentas de segurança empresariais comuns, o que garante a conformidade dos dispositivos e dos dados que contêm. Cada plataforma é compatível com protocolos padrão para VPN e ligação Wi-Fi segura para proteger o tráfego de rede e estabelecer ligação de forma segura a infraestruturas empresariais comuns.

A parceria entre a Apple e a Cisco oferece mais segurança e produtividade. As redes da Cisco aumentam a segurança através do Cisco Security Connector e concedem prioridade às aplicações empresariais em redes da Cisco.

Saiba mais sobre a segurança com dispositivos Apple.

apple.com/pt/business/it

apple.com/macos/security

apple.com/privacy/features

apple.com/pt/security