Apple at Work

Segurança da plataforma

Projetado para ser seguro.

Na Apple, nos importamos profundamente com a segurança do usuário e com a proteção de dados corporativos. Integramos segurança avançada aos nossos produtos desde a concepção deles, tornando-os seguros desde o desenvolvimento. Isso é feito de modo a equilibrar com uma excelente experiência para o usuário, oferecendo aos usuários a liberdade de trabalharem como preferirem. Somente a Apple pode fornecer essa abordagem completa de segurança, pois criamos produtos com hardware, software e serviços integrados.

Segurança de hardware
O software seguro requer uma base de segurança incorporada ao hardware. É por isso que os dispositivos Apple com iOS, iPadOS, macOS, tvOS ou watchOS têm recursos de segurança projetados em silício.

Esses dispositivos contêm recursos personalizados da CPU que alimentam os recursos de segurança do sistema e silício dedicado a funções de segurança. Para minimizar a superfície de ataque, o hardware centrado em segurança aceita funções limitadas. Tais componentes incluem um ROM de inicialização, o que gera uma fonte de confiança de hardware para uma inicialização segura, mecanismos AES dedicados para criptografia e descriptografia segura e eficiente, bem como o Secure Enclave.

O Secure Enclave é um sistema em um chip (SoC) incluído em todos os dispositivos iPhone, iPad, Apple Watch, Apple TV e HomePod das gerações mais recentes e no Mac com Apple Silicon assim como os computadores com o chip Apple T2 Security. O Secure Enclave segue o mesmo princípio de fabricação que o SoC, com sua própria ROM de Inicialização dedicada e mecanismo AES. O Secure Enclave também contém a base para a geração e o armazenamento das chaves necessárias para criptografar dados em repouso e protege e avalia os dados biométricos para Touch ID e Face ID.

A criptografia do armazenamento deve ser rápida e eficiente. Ao mesmo tempo, ela não deve expor os dados (ou material de chavemento) utilizados para estabelecer relações de chaveamento criptográficas. O mecanismo de hardware AES resolve este problema ao executar uma rápida criptografia e descriptografia

integrada à medida que os arquivos são criados ou lidos. Um canal especial do Secure Enclave oferece o material de chaveamento necessário ao mecanismo AES sem expor essas informações ao processador do aplicativo (ou CPU) ou sistema operacional em geral. Isso garante que as tecnologias de Proteção de Dados da Apple e o FileVault protejam os arquivos dos usuários sem expor as chaves criptografadas de longa duração.

A Apple desenvolveu a inicialização segura para proteger os níveis mais baixos de software contra violação e permitir que somente softwares confiáveis do sistema operacional da Apple fossem carregados durante a inicialização. A inicialização segura começa no código imutável chamado ROM de inicialização, que é estabelecido durante a fabricação do SoC da Apple e é conhecido como a fonte de confiança de hardware. Em computadores Mac com chip T2, a confiança da inicialização segura do macOS inicia com o T2. (Tanto o chip T2 quanto o Secure Enclave também executam seus próprios processos de inicialização segura com seus próprios ROM de inicialização separados. Esse processo é análogo a como os chips A-series e M1 inicializam de maneira segura.)

O Secure Enclave também processa informações das digitais e do rosto a partir dos sensores do Touch ID e Face ID nos dispositivos Apple. Isso proporciona uma autenticação segura enquanto mantém os dados de identificação biométrica do usuário confidenciais e protegidos. Também permite que os usuários se beneficiem da segurança de senhas e códigos mais longos e complexos com a conveniência da autenticação swift para acessos ou compras em muitas situações.

Esses recursos de segurança da Apple foram concretizados pela combinação do chip, hardware, software e dos serviços disponíveis exclusivos da Apple.

Segurança do sistema

A partir de recursos exclusivos do hardware da Apple, a segurança do sistema é responsável por controlar o acesso a recursos do sistema em dispositivos Apple sem comprometer a usabilidade. A segurança do sistema abrange o processo de inicialização, as atualizações de software e a proteção de recursos do sistema do computador, como CPU, memória, disco, programas de software e dados armazenados.

As versões mais recentes dos sistemas operacionais da Apple são as mais seguras. Uma parte importante da segurança da Apple é a inicialização segura, o que protege o sistema de infecção por malware no momento da inicialização. A inicialização segura começa no hardware e cria uma rede de segurança por meio do software na qual cada etapa garante que a próxima está funcionando adequadamente antes de passar o controle. Esse modelo de segurança é compatível com não apenas a inicialização padrão dos dispositivos Apple, mas também os vários modos de recuperação e atualizações oportunas em dispositivos Apple. Os subcomponentes como o chip T2 e o Secure Enclave também fazem sua própria inicialização segura para ajudar a garantir que eles inicializem somente códigos em boas condições da Apple. O sistema de atualizações pode evitar até mesmo ataques de downgrade para que os dispositivos não possam ser convertidos a uma versão anterior do sistema operacional (que um invasor saiba como comprometer) como um método de roubar dados do usuário.

Os dispositivos Apple também contêm proteções de inicialização e tempo de execução para que possam manter a integridade em uma operação em andamento.

O chip desenvolvido pela Apple para iPhone, iPad, Apple Watch, Apple TV e HomePod bem como o Mac com Apple Silicon oferecem uma estrutura em comum para a proteção da integridade do sistema operacional. O macOS também contém um conjunto de recursos de proteção expandido e configurável para oferecer suporte ao seu modelo computacional diferente, assim como os recursos compatíveis em todas as plataformas de hardware Mac.

Criptografia e proteção de dados
Os dispositivos Apple contam com recursos de criptografia para proteger os dados do usuário e ativar a limpeza remota em caso de roubo ou perda.

A cadeia de inicialização segura, a segurança do sistema e os recursos de segurança dos apps ajudam a confirmar que somente códigos e apps confiáveis sejam executados em um dispositivo. Os dispositivos Apple têm outros recursos de criptografia que protegem os dados dos usuários, até mesmo quando outras partes da infraestrutura de segurança tiverem sido comprometidas (por exemplo, se um dispositivo for perdido ou estiver executando código não confiável). Todos esses recursos beneficiam tanto os usuários quanto os administradores de TI, pois protegem informações pessoais e corporativas e oferecem os métodos para que o dispositivo seja apagado remotamente de maneira imediata e completa em caso de perda ou roubo.

Os dispositivos iOS e iPadOS usam uma metodologia de criptografia de arquivos chamada Proteção de Dados, enquanto os dados em computadores Mac com processador Intel são protegidos por uma tecnologia de criptografia de volume chamada FileVault. Um Mac com Apple Silicon utiliza um modelo híbrido compatível com a Proteção de Dados de acordo com as seguintes condições: o nível mais baixo de proteção (Nível D) não é compatível, e o nível padrão (Nível C) usa uma chave de volume e funciona como o FileVault em um computador Mac com processador Intel. Em todos os casos, as hierarquias de gerenciamento de chave estão localizadas no chip dedicado do Secure Enclave e um mecanismo AES dedicado é compatível com criptografia de velocidade de linha e ajuda a garantir que chaves criptografadas de longa duração não sejam expostas ao kernel do sistema operacional ou CPU (onde elas poderão ser comprometidas). (Um computador Mac com processador Intel com um chip T1 ou sem o Secure Enclave não utiliza o chip dedicado para proteger as chaves criptografadas do FileVault.)

Além da Proteção de Dados e do FileVault para evitar acessos não autorizados aos dados, os kernels do sistema operacional da Apple garantem proteção e segurança. O kernel utiliza os controles de acesso à área restrita de apps (que restrigem quais dados um app pode acessar) e um mecanismo chamado Data Vault (que restringe o acesso aos dados de um app de todos os apps solicitantes em vez de restringir as chamadas que um app pode fazer).

Segurança de apps
Os apps são os elementos mais críticos de uma arquitetura de segurança. Embora os apps proporcionem benefícios incríveis para a produtividade dos usuários, eles também têm o potencial de afetar negativamente a segurança do sistema, a estabilidade e os dados do usuário se não forem processados de maneira correta.

Em função disso, a Apple fornece camadas de proteção para garantir que os apps não tenham malware conhecido nem adulterações. Proteções adicionais garantem que o acesso dos apps aos dados dos usuário seja intermediado cuidadosamente. Esses controles de segurança oferecem uma plataforma estável e segura para apps, permitindo que milhares de desenvolvedores entreguem centenas de milhares de apps no iOS, iPadOS e macOS sem afetar a integridade do sistema. E os usuários podem acessar esses apps nos dispositivos Apple sem medo de vírus, malware ou ataques não autorizados.

No iPhone, iPad e iPod touch, todos os apps são obtidos pela App Store—e todos os apps ficam em área restrita—para oferecer os controles mais rígidos.

No Mac, muitos apps são obtidos na App Store, mas os usuários de Mac também podem baixar e usar apps na internet. Para uma maior compatibilidade com downloads da internet, o macOS contém controles adicionais em camadas. Primeiro, por padrão no macOS 10.15 ou posterior, todos os apps de Mac precisam ser autenticados pela Apple para serem lançados. Esse requisito ajuda a garantir que esses apps estejam livres de malware conhecido sem exigir que os apps sejam disponibilizados por meio da App Store. Além disso, o macOS oferece proteção antivírus de última geração para bloquear e, se necessário, remover malware.

As áreas restritas, como um controle adicional entre as plataformas, ajudam a evitar que os apps acessem dados dos usuários de modo não autorizado. No macOS, os dados em áreas críticas estão protegidos, o que ajuda a garantir que os usuários mantenham o controle de acesso a arquivos na Mesa, Documentos, Download e outras áreas de todos os apps, independentemente de as tentativas de acesso ocorrerem por parte deles em área restrita ou não.

Serviços de segurança
A Apple desenvolveu um amplo conjunto de recursos para ajudar os usuários a aproveitarem ao máximo a funcionalidade e produtividade de seus dispositivos. Esses serviços oferecem sofisticados recursos de armazenamento em nuvem, sincronização, armazenamento de senhas, autenticação, pagamento, mensagens, comunicações e muito mais; protegendo sempre a privacidade e a segurança dos dados dos usuários.

Esses serviços incluem o iCloud, Iniciar Sessão com a Apple, Apple Pay, iMessage, Business Chat, FaceTime, Buscar e Continuidade e podem exigir um ID Apple ou um ID Apple gerenciado. Em alguns casos, não será possível usar um ID Apple gerenciado com um serviço específico como o Apple Pay.

Nota: nem todos os serviços e conteúdos da Apple estão disponíveis em todos os países ou regiões.

Visão geral sobre a segurança de rede

Além das medidas de segurança integradas que a Apple usa para proteger dados armazenados em dispositivos Apple, existem muitas medidas que as empresas podem adotar para manter as informações seguras conforme elas são transmitidas de e para um dispositivo. Todas essas medidas de segurança fazem parte da segurança de rede.

Os usuários devem conseguir acessar as redes corporativas de qualquer lugar do mundo, portanto é importante garantir que tenham autorização para isso e que os dados deles sejam protegidos durante a transmissão. Para atender a estes objetivos de segurança, o iOS, iPadOS e macOS fazem parte de tecnologias comprovadas e dos mais recentes padrões para conexões Wi-Fi e de rede celular. É por esse motivo que nossos sistemas operacionais usam e fornecem acesso a desenvolvedores para protocolos de rede padrão a comunicações autenticadas, autorizadas e criptografadas.

Ecossistema de parceiros

Os dispositivos Apple funcionam com serviços e ferramentas de segurança corporativa em comum, garantindo a conformidade dos dispositivos e dos dados contidos neles. As plataformas são compatíveis com os protocolos padrão para VPN, incluindo as conexões de VPN por conta no iOS e iPadOS 14 e Wi-Fi seguro para proteger o tráfego de rede, além de estabelecer uma conexão com segurança à infraestrutura comum da empresa.

Quando usadas em conjunto, a parceria da Apple com a Cisco proporciona segurança e produtividade aprimoradas. As redes da Cisco oferecem segurança aprimorada por meio do Cisco Security Connector e concedem prioridade aos aplicativos empresariais nas redes da Cisco.

Saiba mais sobre a segurança em dispositivos Apple.

apple.com/business/it

apple.com/macos/security

apple.com/privacy/features

apple.com/security