Apple at Work

Sécurité des plateformes

La sécurité au cœur de la conception.

Apple prend très au sérieux la sécurité, tant du point de vue des utilisateurs et utilisatrices que de la protection des données d'entreprise. Nous intégrons des fonctionnalités de sécurité avancées à nos produits pour qu'ils soient sécurisés dès leur conception. Et ce, sans compromettre une formidable expérience d'utilisation, qui offre à tout un chacun la liberté de travailler comme il l'entend. Seul Apple est en mesure de fournir une approche aussi complète de la sécurité, car nous créons des produits intégrant le matériel, les logiciels et les services.

Sécurité du matériel
Pour être parfaitement sûr, le matériel doit reposer sur une structure sécurisée. C'est pourquoi les appareils Apple (exécutant iOS, iPadOS, macOS, tvOS ou watchOS) intègrent des capacités de sécurité au sein même des puces en silicium.

Il s'agit notamment de capacités exclusives du processeur central qui font tourner les fonctionnalités de sécurité système, ainsi qu'une autre puce dédiée aux fonctions de sécurité. Pour garantir un maximum de sécurité, le matériel prend en charge des fonctions limitées et bien dissociées dans le but de réduire la surface d'attaque. Les composants incluent une ROM de démarrage, qui forme une racine de confiance matérielle permettant un démarrage sécurisé, des moteurs AES dédiés pour un chiffrement et déchiffrement efficaces et sécurisés, ainsi qu'un coprocesseur Secure Enclave.

Le Secure Enclave est un système sur une puce (SoC) intégré à toutes les générations récentes d'iPhone, d'iPad, d'Apple Watch, d'Apple TV et de HomePod, ainsi qu'aux Mac avec puce Apple et Mac dotés de la puce Apple T2 Security. Le Secure Enclave suit le même principe de conception que le SoC, il contient une ROM de démarrage distincte et son propre moteur AES. Le Secure Enclave fournit également une structure permettant de générer et de stocker de manière sécurisée les clés nécessaires pour chiffrer les données au repos, tout en assurant la protection et la vérification des données biométriques destinées à Touch ID et Face ID.

Le chiffrement du dispositif de stockage doit être rapide et efficace, mais sans exposer les données (ou clés) utilisées pour établir les relations avec les clés cryptographiques. Le moteur matériel AES résout ce problème en effectuant un chiffrement et un déchiffrement rapides et intégrés à l'écriture ou à la lecture des fichiers. Un canal spécial du Secure Enclave fournit les clés de chiffrement nécessaires au moteur AES sans exposer ces informations au processeur d'application (ou processeur central) ou au système d'exploitation. Ainsi, les technologies Apple de Protection des données et FileVault protègent les fichiers des utilisateurs et utilisatrices sans exposer les clés de chiffrement de longue durée.

Apple a conçu le démarrage sécurisé pour veiller à ce que les niveaux inférieurs des logiciels ne soient pas altérés et que seuls les logiciels système fiables validés par Apple se lancent au démarrage. Le démarrage sécurisé commence par un code

immuable intitulé ROM de démarrage. Celui-ci est défini lors de la fabrication de la puce Apple et constitue la « racine de confiance matérielle ». Sur les ordinateurs Mac équipés de la puce T2, la confiance en un démarrage sécurisé de macOS commence avec la puce T2 elle-même. (La puce T2 et le Secure Enclave exécutent leur propre processus de démarrage sécurisé en utilisant une ROM de démarrage distincte, exactement comme pour le démarrage sécurisé des puces de série A et M1.)

Le Secure Enclave traite également les données d'empreinte et de visage issues des capteurs Touch ID et Face ID des appareils Apple. Cela garantit une authentification sûre tout en sécurisant les données biométriques des utilisateurs et utilisatrices. Cela permet aussi de bénéficier de la sécurité qu'offrent des codes et mots de passe plus longs et plus complexes avec, dans bien des situations, le confort d'une authentification rapide pour accéder à des sites ou effectuer des achats.

Les fonctionnalités de sécurité des appareils Apple sont rendues possibles par l'association de puces, de matériel, de logiciels et de services disponibles uniquement auprès d'Apple.

Sécurité du système

La sécurité du système s'appuie sur les capacités propres au matériel Apple et permet de contrôler l'accès aux ressources système des appareils Apple sans en compromettre la facilité d'utilisation. La sécurité du système englobe le processus de démarrage, les mises à jour logicielles et la protection des ressources système de l'ordinateur comme le processeur central, la mémoire, le disque, les logiciels et les données enregistrées.

Les versions les plus récentes des systèmes d'exploitation Apple sont les plus sécurisées. Le démarrage sécurisé est l'un des aspects les plus importants de la sécurité Apple. Il protège le système d'éventuelles infections de logiciels malveillants lors du démarrage. Le démarrage sécurisé commence au sein du matériel et établit une chaîne de confiance via les logiciels, chaque étape veillant à ce que la suivante fonctionne correctement avant de passer la main. Ce modèle de sécurité prend en charge non seulement le démarrage par défaut des appareils Apple, mais aussi les divers modes de récupération et la mise à jour en temps voulu des appareils Apple. Des sous-composants, comme la puce T2 et le Secure Enclave, effectuent également leur propre démarrage sécurisé pour s'assurer qu'ils n'utilisent que le code validé par Apple. Le système de mise à jour empêche même les appareils de revenir à une version antérieure du système d'exploitation afin de lutter contre les attaques utilisant ce procédé pour dérober les données de l'utilisateur ou de l'utilisatrice.

Les appareils Apple intègrent des protections au démarrage et à l'exécution, ce qui préserve leur intégrité pendant le fonctionnement. Les puces Apple intégrées aux iPhone, iPad, Apple Watch, Apple TV et HomePod, ainsi qu'à certains Mac, fournissent une architecture commune permettant de préserver l'intégrité du système d'exploitation. macOS propose également un vaste ensemble de fonctions de protection configurables prenant en charge son modèle informatique, ainsi que des capacités compatibles avec toutes les plateformes matérielles Mac.

Chiffrement et protection des données

Les appareils Apple sont dotés de fonctionnalités de chiffrement qui protègent les données utilisateur et permettent de les effacer à distance en cas de vol ou de perte de l'appareil.

La chaîne de démarrage sécurisé, la sécurité du système et les capacités de sécurité des apps contribuent à garantir que seuls du code et des apps de confiance peuvent être exécutés sur un appareil. Les appareils Apple disposent de fonctionnalités supplémentaires de chiffrement pour protéger les données utilisateur même si d'autres parties de l'infrastructure de sécurité ont été mises à mal : par exemple, si un appareil est perdu ou exécute du code non validé. Toutes ces fonctionnalités profitent aux utilisateurs et utilisatrices comme aux équipes d'administration informatique en protégeant à tout moment les informations personnelles et celles de l'entreprise, et en proposant des méthodes d'effacement à distance instantané et complet, en cas de vol ou de perte d'un appareil.

Les appareils iOS et iPadOS exploitent une méthode de chiffrement des fichiers intitulée Protection des données, tandis que les données des Mac dotés d'un processeur Intel sont protégées à l'aide d'une technologie de chiffrement des volumes nommée FileVault. Les Mac équipés de la puce Apple utilisent un modèle

hybride qui prend en charge la Protection des données, avec deux mises en garde : le niveau de protection le plus bas (classe D) n'est pas pris en charge, et le niveau par défaut (classe C) utilise une clé de volume qui agit exactement comme FileVault sur un Mac à processeur Intel. Dans les deux cas, les hiérarchies de gestion clés prennent leur source dans la puce dédiée du Secure Enclave sur les appareils qui en sont dotés. De même, les deux méthodes font appel à un moteur AES dédié qui permet un chiffrement pleine vitesse et veille à ce que les clés de chiffrement longue durée ne soient jamais transmises au noyau du système d'exploitation ni au processeur central, où elles pourraient être compromises. Un Mac doté d'un processeur Intel intégrant une puce T1 ou ne disposant pas de Secure Enclave n'utilise pas de puce dédiée pour protéger ses clés de chiffrement FileVault.

Outre la Protection des données et FileVault, les noyaux du système d'exploitation Apple utilisent d'autres mesures de protection et de sécurité pour empêcher tout accès aux données non autorisé. Le noyau impose des contrôles d'accès aux apps mises en bac à sable (ce qui restreint les données auxquelles une app a accès) et l'application d'un mécanisme appelé Data Vault (qui restreint l'accès aux données d'une app à partir de toutes les autres apps demandeuses, plutôt que de restreindre les appels qu'une app peut effectuer).

Sécurité des apps

Les apps constituent l'un des éléments cruciaux d'une architecture de sécurité. Si les apps offrent des avantages considérables en termes de productivité, elles sont également susceptibles d'avoir un impact négatif sur la sécurité du système, sa stabilité et les données des utilisateurs et utilisatrices si celles-ci ne sont pas correctement gérées.

C'est pourquoi Apple met en place des couches de protection pour s'assurer que les apps ne comportent aucun logiciel malveillant connu et n'ont pas été altérées. D'autres mesures de protection permettent de contrôler rigoureusement l'accès des apps aux données de l'utilisateur ou de l'utilisatrice. Ces contrôles de sécurité fournissent une plateforme stable et sécurisée pour les apps et permettent à des milliers de développeurs et développeuses de proposer des centaines de milliers d'apps pour iOS, iPadOS et macOS, sans que cela ait le moindre impact sur l'intégrité du système. Par ailleurs, les utilisateurs et utilisatrices peuvent accéder à ces apps sur leurs appareils sans avoir à se soucier des virus, des logiciels malveillants ou des attaques.

Toutes les apps pour iPhone, iPad et iPod touch s'obtiennent sur l'App Store et toutes s'exécutent au sein d'un environnement protégé de type bac à sable (ou « sandboxing »), pour offrir le maximum de contrôle.

Sur Mac, la plupart des apps s'obtiennent sur l'App Store, mais les utilisateurs et utilisatrices de Mac peuvent également télécharger et utiliser des apps provenant d'Internet. Pour sécuriser les téléchargements depuis Internet, macOS met en œuvre des mesures supplémentaires. Premièrement, par défaut sur macOS 10.15 et les versions ultérieures, toutes les apps pour Mac doivent être « notarisées » par Apple avant leur lancement. Cette condition permet de veiller à ce que ces apps soient exemptes de tout logiciel malveillant connu, sans exiger pour autant qu'elles soient fournies via l'App Store. De plus, macOS intègre une protection antivirus très efficace pour bloquer, et supprimer si nécessaire, les logiciels malveillants.

La mise en bac à sable, qui est une forme de contrôle supplémentaire sur les différentes plateformes, contribue à protéger les données utilisateur contre les tentatives d'accès non autorisé émanant des apps. Enfin, sous macOS, les données enregistrées sur le Bureau, dans les dossiers Documents et Téléchargements ainsi qu'à d'autres emplacements stratégiques sont protégées. Ainsi, que les tentatives d'accès proviennent d'apps elles-mêmes mises en bac à sable ou non, les utilisateurs et les utilisatrices gardent le contrôle sur les fichiers figurant à ces emplacements.

Sécurité des services

Apple a constitué un solide ensemble de services conçus pour permettre aux utilisateurs et utilisatrices de gagner encore en efficacité et en productivité à l'aide de leurs appareils. Ces services offrent de puissantes possibilités de stockage et de synchronisation sur le cloud, d'authentification, de paiement, de messagerie, de communication et autres, tout en protégeant la vie privée des utilisateurs et utilisatrices ainsi que la sécurité de leurs données.

Il s'agit notamment des services iCloud, Connexion avec Apple, Apple Pay, iMessage, Business Chat, FaceTime, Localiser et Continuité, qui peuvent nécessiter un identifiant Apple ou un identifiant Apple géré. Dans certains cas, il se peut qu'un identifiant Apple géré ne puisse pas être utilisé avec un service particulier, par exemple Apple Pay.

Remarque : tous les services et contenus Apple ne sont pas disponibles dans tous les pays ou zones géographiques.

Aperçu de la sécurité du réseau

En plus des protections intégrées qu'Apple utilise pour protéger les données enregistrées sur les appareils Apple, de nombreuses mesures permettent aux organisations de sécuriser les données en transit vers ou depuis un appareil. Toutes ces protections et mesures relèvent de la sécurité du réseau.

Les utilisateurs et les utilisatrices doivent être en mesure d'accéder aux réseaux de l'entreprise partout dans le monde, il est donc crucial de vérifier que leur accès est autorisé et de protéger les données transmises. Pour atteindre ce niveau de sécurité, iOS, iPadOS et macOS intègrent des technologies éprouvées et les normes les plus récentes pour les connexions aux réseaux Wi-Fi et cellulaires. C'est pourquoi nos systèmes d'exploitation utilisent – et mettent à la disposition des équipes de développement – des protocoles réseau standard pour authentifier, autoriser et chiffrer les communications.

Pour plus d'informations sur la sécurité avec les produits Apple :

apple.com/fr/business/it

apple.com/fr/macos/security

apple.com/fr/privacy/features

apple.com/security

Écosystème de partenaires

Les appareils Apple fonctionnent avec les outils et services de sécurité couramment utilisés dans les entreprises, ce qui garantit la conformité des appareils et des données qu'ils contiennent. Chaque plateforme prend en charge les protocoles standard pour le VPN (y compris les connexions VPN via le compte sous iOS et iPadOS 14) et le Wi-Fi sécurisé afin de protéger le trafic réseau et de se connecter en toute sécurité à l'infrastructure d'entreprise commune.

Le partenariat entre Apple et Cisco renforce la sécurité et la productivité par l'utilisation conjointe de leurs technologies respectives. Les réseaux Cisco renforcent la sécurité via Cisco Security Connector et accordent la priorité aux applications métier hébergées par des réseaux Cisco.