Apple at Work

Sécurité des plateformes

Sécuritaires de nature.

Chez Apple, la sécurité est une priorité absolue qui concerne autant les utilisateurs que les données d'entreprise. Afin d'offrir des produits sécuritaires de nature, nous les concevons de A à Z avec des fonctionnalités de sécurité avancées, sans perdre de vue l'expérience utilisateur et la liberté de travailler à sa façon. Si seule Apple peut proposer cette stratégie globale en matière de sécurité, c'est parce que chaque produit est créé avec des composants matériels, des logiciels et des services intégrés.

Sécurité du matériel
La sécurité des logiciels doit d'abord reposer sur des fonctionnalités intégrées au matériel. C'est pourquoi les appareils Apple qui exécutent iOS, iPadOS, macOS, tvOS et watchOS comprennent des fonctionnalités de sécurité à même leurs composants.

Ces remparts incluent un processeur central avec capacités sur mesure assurant la protection du système et une puce dédiée à la sécurité. Le matériel axé sur la sécurité obéit à un principe : prendre en charge des fonctionnalités limitées et distinctes afin de réduire la surface d'attaque. Parmi ces composants, on trouve une mémoire morte d'amorçage, qui constitue une base matérielle sécurisée pour le démarrage, des moteurs AES dédiés qui permettent un chiffrement et un déchiffrement sûrs et efficaces, et un coprocesseur Secure Enclave.

Le Secure Enclave est un système sur une puce présent sur tous les récents modèles d'iPhone, iPad, Apple Watch, Apple TV et HomePod ainsi que sur les Mac à puce Apple et à puce T2 Security. Il suit les mêmes principes de conception que les autres systèmes sur une puce et contient sa propre mémoire morte d'amorçage et son propre moteur AES. Il fournit aussi la base sur laquelle s'appuient la création et le stockage sécurisés des clés pour le chiffrement des données au repos, et protège et évalue les données biométriques de Touch ID et Face ID.

Le chiffrement des supports de données doit être rapide et efficace. Il ne doit toutefois pas exposer les données (ou le matériel de chiffrement) qu'il utilise pour établir un contexte de chiffrement cryptographique. Le moteur AES physique règle ce problème en assurant un chiffrement et un déchiffrement rapides, au fil de l'écriture ou de la lecture des fichiers. Un canal spécial partant du Secure Enclave transmet le matériel de chiffrement nécessaire au moteur AES sans exposer l'information au processeur d'application (ou processeur central) ni au système d'exploitation général. Ainsi, FileVault et la technologie de protection des données d'Apple peuvent protéger les fichiers des utilisateurs sans révéler les clés de chiffrement longue durée.

Le démarrage sécurisé empêche la modification des couches logicielles inférieures, tout en veillant à ce que seuls les logiciels système vérifiés par Apple s'ouvrent quand l'utilisateur allume son appareil. Il prend sa source dans un code immuable appelé « mémoire morte d'amorçage », qui est défini pendant la fabrication du système sur une puce d'Apple et fait office de base matérielle sécurisée. Sur les ordinateurs Mac dotés de la puce T2, la fiabilité du démarrage sécurisé commence par la puce elle-même. (La puce T2 et le Secure Enclave exécutent également leurs propres processus de démarrage sécurisé à l'aide d'une mémoire morte d'amorçage distincte, un mécanisme identique à celui des puces M1 et de série A.)

Le Secure Enclave traite par ailleurs les données d'empreinte digitale et de reconnaissance faciale recueillies par les capteurs de Touch ID et Face ID. Cela garantit une authentification sécurisée, tout en assurant l'intégrité et la confidentialité des données biométriques. Les utilisateurs profitent ainsi de la sécurité accrue des codes et mots de passe longs et complexes, en plus de la commodité d'une authentification rapide.

Toutes ces fonctionnalités de sécurité sont le résultat de la conception de la puce, du matériel, des logiciels et des services offerts uniquement sur les appareils Apple.

Sécurité du système

Bien ancrées dans les composants matériels d'Apple, les fonctionnalités de sécurité contrôlent l'accès aux ressources système des appareils sans pour autant nuire à leur utilisation. La sécurité du système englobe le processus de démarrage, les mises à jour logicielles et la protection des ressources système comme le processeur central, la mémoire, le disque, les programmes et les données stockées.

Les plus récentes versions des systèmes d'exploitation Apple sont les plus sûres. Les fonctionnalités de sécurité reposent notamment sur le démarrage sécurisé, qui prévient les attaques de logiciels malveillants lorsque le système démarre. Le démarrage sécurisé commence au niveau matériel et initie une chaîne de confiance au niveau logiciel – une chaîne dans laquelle chaque maillon vérifie que le suivant fonctionne adéquatement avant de lui octroyer le contrôle. C'est ce modèle de sécurité qui sous-tend le démarrage par défaut des appareils Apple, mais aussi leurs différents modes de récupération et de mise à jour. Les sous-composants comme la puce T2 et le coprocesseur Secure Enclave procèdent également à leur propre démarrage sécurisé, de sorte que seul le code connu d'Apple s'exécute. Le système de mise à jour peut même prévenir les tentatives de retour à une version antérieure du système d'exploitation, qui visent à dérober les données de l'utilisateur.

Enfin, les appareils Apple intègrent des protections de démarrage et d'exécution assurant leur intégrité tout au long de leur utilisation. Les puces conçues par Apple sur iPhone, iPad, Apple Watch, Apple TV et HomePod, en plus de celle intégrée à Mac, fournissent une architecture commune qui empêche la corruption des systèmes d'exploitation. macOS comprend également un vaste éventail de protections configurables qui sous-tendent son modèle unique, ainsi que des fonctionnalités prises en charge sur tous les Mac.

Chiffrement et protection des données

Les appareils Apple intègrent des fonctions de chiffrement qui protègent les données des utilisateurs et permettent l'effacement à distance en cas de vol ou de perte.

La chaîne de démarrage sécurisée, la sécurité du système et les fonctionnalités de sécurité des apps contribuent à faire en sorte que seuls des apps et du code vérifiés s'exécutent. En outre, des fonctions de chiffrement additionnelles assurent la protection des données même lorsque certaines parties de l'infrastructure de sécurité ont été compromises (par exemple, si l'appareil a été perdu ou s'il exécute du code non vérifié). Et parce que les renseignements personnels et ceux de l'entreprise sont protégés et que les données d'un appareil perdu ou volé peuvent être entièrement effacées à distance en un instant, tout cela profite aux utilisateurs comme aux gestionnaires des TI.

Les appareils iOS et iPadOS utilisent une méthode de chiffrement des fichiers appelée « protection des données », tandis que les Mac à processeur Intel sont protégés par la technologie de chiffrement de disque FileVault. Les Mac dotés d'une puce Apple utilisent quant à eux un modèle hybride compatible avec la protection des données, à deux nuances près : 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 et se comporte exactement comme FileVault sur un Mac à processeur Intel. Dans tous les cas, les hiérarchies de gestion des clés sont ancrées dans la puce du Secure Enclave consacrée à cette fin, et un moteur AES dédié permet le chiffrement pleine vitesse et fait en sorte que des clés de chiffrement longue durée ne soient jamais transmises au noyau du système d'exploitation ou au processeur central, où elles pourraient être compromises. (Un Mac à processeur Intel équipé d'une puce T1 ou dépourvu de Secure Enclave n'utilise pas de puce dédiée pour protéger ses clés de chiffrement FileVault.)

Outre le recours à la protection des données et à FileVault pour empêcher tout accès non autorisé à l'information, les noyaux des systèmes d'exploitation renforcent la protection et la sécurité des appareils Apple. Les noyaux utilisent, d'une part, des contrôles d'accès pour mettre les apps en bac à sable (ce qui restreint les données auxquelles ces apps ont accès) et, d'autre part, un mécanisme appelé Data Vault (qui, au lieu de limiter les appels pouvant être passés par une app, restreint l'accès aux données d'une app par toutes les autres apps qui en font la demande).

Sécurité des apps

Les apps sont parmi les éléments les plus importants d'une architecture de sécurité. Bien qu'elles soient de formidables outils de productivité, si elles ne sont pas gérées adéquatement, elles peuvent potentiellement nuire à l'intégrité et à la stabilité du système et mettre les données des utilisateurs en péril.

Pour cette raison, Apple met en place des couches de protection pour vérifier que les apps ne comportent pas de programmes malveillants connus et qu'elles n'ont pas été altérées. Et d'autres mesures permettent de contrôler rigoureusement l'accès des apps aux données de l'utilisateur. Ces contrôles de sécurité offrent une plateforme stable et sûre pour les apps, ce qui permet aux équipes de développement de proposer des centaines de milliers d'apps pour iOS, iPadOS et macOS – le tout sans compromettre l'intégrité du système. Les utilisateurs ont ensuite accès à ces apps sur leurs appareils Apple sans craindre les virus, les logiciels malveillants et les autres types d'attaques.

Sur iPhone, iPad et iPod touch, toutes les apps proviennent de l'App Store (et sont placées en bac à sable) pour garantir un contrôle serré.

Sur Mac, de nombreuses apps sont obtenues via l'App Store, mais les utilisateurs peuvent également télécharger et installer des logiciels provenant d'Internet. Pour rendre ces téléchargements plus sûrs, macOS compte sur des contrôles supplémentaires. Tout d'abord, sous macOS 10.15 et les versions ultérieures, toutes les apps doivent être notarisées par Apple pour que leur exécution soit autorisée. Cette exigence vise à prévenir la présence de logiciels malveillants connus dans les apps lorsque celles-ci ne sont pas obtenues sur l'App Store. macOS inclut également une protection antivirus de pointe pour bloquer et, au besoin, supprimer tout logiciel malveillant.

La mise en bac à sable assure un contrôle complémentaire sur l'ensemble des plateformes en protégeant les données des utilisateurs de tout accès non autorisé par les apps. Et sous macOS, les données critiques sont elles aussi protégées. Ainsi, que les apps qui tentent d'y accéder soient elles-mêmes placées en bac à sable ou non, les utilisateurs demeurent maîtres de l'accès à leurs fichiers, notamment sur le Bureau et dans les dossiers Documents et Téléchargements.

Sécurité des services

Apple a mis en place une large gamme de services permettant aux utilisateurs d'en faire encore plus avec leurs appareils. Tous offrent de puissantes fonctionnalités – que ce soit pour le stockage et la synchronisation dans le nuage, l'authentification, les paiements, l'envoi de messages, les communications, le stockage des mots de passe et plus encore – tout en veillant à la confidentialité et à la sécurité des données des utilisateurs.

Ces services comprennent iCloud, Connexion avec Apple, Apple Pay, iMessage, FaceTime, Localiser, Continuité et le clavardage commercial, et peuvent nécessiter un identifiant Apple ou un identifiant Apple géré. Il est possible qu'un identifiant Apple géré ne puisse pas être utilisé pour certains services, par exemple Apple Pay.

Remarque : Certains contenus et services Apple pourraient ne pas être offerts dans tous les pays ou toutes les régions.

Aperçu de la sécurité du réseau

En plus des dispositifs qu'Apple intègre à ses appareils pour protéger l'information qui y est stockée, les entreprises disposent de nombreuses mesures pour assurer la sûreté des données qu'un appareil reçoit et envoie. Toutes ces protections appartiennent à la sécurité du réseau.

Les utilisateurs doivent pouvoir accéder aux réseaux d'entreprise où qu'ils soient dans le monde. Il est donc important de veiller à ce qu'ils y soient bel et bien autorisés et à ce que les données soient protégées durant leur transmission. Pour atteindre ces objectifs en matière de sécurité, iOS, iPadOS et macOS intègrent des technologies éprouvées et les plus récentes normes relatives à la connexion aux réseaux Wi-Fi et cellulaires. C'est pourquoi nos systèmes d'exploitation font appel à des protocoles réseau standards – et les mettent à la disposition des équipes de développement – pour l'authentification, l'autorisation et le chiffrement des communications.

Écosystème de partenaires

Les appareils Apple sont compatibles avec les outils et services de sécurité courants en entreprise, ce qui garantit la conformité des appareils et des données qui s'y trouvent. Chaque plateforme prend en charge les protocoles standards pour le VPN – y compris les connexions VPN par compte sous iOS 14 et iPadOS 14 – et la connexion Wi-Fi sécurisée de manière à protéger le trafic réseau et à permettre une connexion sûre à l'infrastructure de l'entreprise.

Le partenariat entre Apple et Cisco donne lieu à une sécurité et à une productivité accrues. Sur les réseaux de Cisco, la sécurité est renforcée par le biais de Cisco Security Connector, et les apps d'entreprise se voient accorder un accès prioritaire.

Apprenez-en plus sur la sécurité des appareils Apple.

apple.com/ca/fr/business/it

apple.com/ca/fr/macos/security

apple.com/ca/fr/privacy/features

support.apple.com/fr-ca/guide/security