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. Seule Apple peut proposer cette stratégie globale en matière de sécurité, puisque nous créons nous-mêmes chacun de nos produits 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. Celles-ci incluent un processeur central avec des capacités sur mesure assurant la protection du système et une puce dédiée aux fonctionnalités de sécurité.

L'élément le plus important, toutefois, est le coprocesseur Secure Enclave, que l'on retrouve dans les appareils iOS, iPadOS, watchOS et tvOS récents et sur tous les ordinateurs Mac dotés de la puce T2 Security d'Apple. Le Secure Enclave fournit la base sur laquelle s'appuient le chiffrement des données au repos, le démarrage sécurisé dans macOS et la protection des données biométriques.

Tous les modèles récents d'iPhone, d'iPad et de Mac avec puce T2 incluent un moteur AES matériel dédié qui permet un chiffrement pleine vitesse au moment où les fichiers sont écrits ou lus. Ainsi, les fichiers des utilisateurs bénéficient de la protection des données et de FileVault, sans que les clés de chiffrement longue durée soient exposées au processeur central ou au système d'exploitation.

Le démarrage sécurisé des appareils Apple empêche la modification des couches logicielles inférieures, tout en veillant à ce que seuls les logiciels système vérifiés par Apple s'ouvrent au démarrage. Sur les appareils iOS et iPadOS, la sécurité prend sa source dans un code immuable appelé « mémoire morte d'amorçage », défini pendant la fabrication de la puce et faisant office de base matérielle sécurisée. Sur les ordinateurs Mac dotés de la puce T2, la fiabilité du démarrage sécurisé commence par le Secure Enclave lui-même.

Le Secure Enclave permet l'authentification sécurisée par Touch ID et Face ID sur les appareils Apple, 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.

Les fonctionnalités de sécurité des appareils Apple sont le résultat de la conception de la puce, du matériel, du logiciel et des services offerts uniquement par Apple.

Sécurité du système

Bien ancrées dans les composants matériels d'Apple, les fonctionnalités de sécurité optimisent la protection du système d'exploitation des appareils sans pour autant nuire à leur utilisation. La sécurité du système comprend le processus de démarrage, les mises à jour logicielles et les opérations continues du système d'exploitation.

Le démarrage sécurisé commence au niveau matériel et initie une chaîne de confiance au niveau logiciel – une chaîne dans laquelle chaque étape vérifie que la suivante 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 les différents modes de récupération et de mise à jour sous iOS, iPadOS et macOS.

Les plus récentes versions d'iOS, d'iPadOS et de macOS sont les plus sécuritaires. En plus d'assurer la mise à jour des appareils Apple en temps opportun, le mécanisme de mise à jour logicielle autorise uniquement l'installation de programmes vérifiés par Apple. Il peut même prévenir les mises à niveau inférieur et ainsi empêcher les tentatives de retour à une version antérieure du système d'exploitation comme manière de dérober les données de l'utilisateur.

Enfin, les appareils Apple intègrent des protections de démarrage et d'exécution qui assurent le maintien de leur intégrité durant leur utilisation continue. Ces protections varient beaucoup entre les appareils iOS, iPadOS et macOS, selon les différents ensembles de fonctionnalités qu'ils prennent en charge et les attaques contre lesquelles ils doivent par conséquent se prémunir.

Pour atteindre un tel niveau de sécurité, iOS et iPadOS font appel à la protection de l'intégrité du noyau, à l'intégrité du coprocesseur système, à des codes d'authentification des pointeurs (PAC) et à la fonction de couche de protection de page (PPL). macOS, quant à lui, tire profit de la sécurité de l'interface micrologicielle extensible unifiée (UEFI), d'un mode de gestion système (SMM), de protections d'accès direct à la mémoire (DMA) et de la sécurité micrologicielle périphérique.

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 en tout temps 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 administrateurs des TI.

Les appareils iOS et iPadOS utilisent une méthode de chiffrement appelée « protection des données », tandis que les ordinateurs Mac sont protégés par la technologie de chiffrement de disque FileVault. 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 fait en sorte que les clés de chiffrement longue durée n'ont jamais à être transmises au noyau du système d'exploitation ou au processeur central, où elles pourraient être compromises.

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

Les contrôles de sécurité intégrés offrent une plateforme stable et sûre pour les apps, ce qui permet aux développeurs 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 des appareils Apple dotés de fonctionnalités qui les protègent aussi contre 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 apps provenant d'Internet. Pour sécuriser ces téléchargements, 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 standard 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 mises en bac à sable. 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 un vaste éventail de services permettant aux utilisateurs d'en faire encore plus avec leurs appareils. Ces services comprennent l'identifiant Apple, iCloud, Connexion avec Apple, Apple Pay, iMessage, FaceTime, Siri et Localiser. 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 et plus encore – tout en veillant à la confidentialité et à la sécurité des données des usagers.

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 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

apple.com/ca/fr/macos/what-is