Apple at Work

Sécurité des plateformes

Les produits Apple sont conçus pour être parfaitement sûrs.

Apple prend très au sérieux la sécurité, tant du point de vue de l'utilisateur 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 utilisateur, 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 personnalisées du processeur central qui font tourner les fonctionnalités de sécurité système ainsi que la puce dédiée aux fonctions de sécurité. Le composant le plus stratégique est le coprocesseur Secure Enclave équipant les appareils iOS, iPadOS, watchOS et tvOS récents ainsi que tous les ordinateurs dotés de la puce Apple T2 Security. La Secure Enclave est la structure sur laquelle reposent le chiffrement des données au repos, le démarrage sécurisé dans macOS et les données biométriques.

Tous les iPhone et iPad récents ainsi que les ordinateurs Mac avec puce T2 sont dotés d'un moteur matériel AES dédié permettant d'effectuer un chiffrement ultrarapide à l'écriture ou à la lecture des fichiers. Cela garantit que la Protection des données et FileVault protègent les fichiers des utilisateurs sans exposer les clés de chiffrement durables au processeur central ou au système d'exploitation.

Le démarrage sécurisé des appareils Apple veille 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. Sur les appareils iOS et iPadOS, la sécurité commence par un code immuable intitulé ROM de démarrage. Celle-ci est définie lors de la fabrication de la puce et connue en tant que « racine matérielle de confiance ». Sur les ordinateurs Mac équipés d'une puce T2, la confiance en un démarrage sécurisé débute avec la Secure Enclave elle-même.

La Secure Enclave permet aux fonctionnalités Touch ID et Face ID des appareils Apple de garantir une authentification sûre tout en sécurisant les données

biométriques des utilisateurs. Ceux-ci bénéficient donc 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 très rapide.

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

S'appuyant sur les capacités propres au matériel Apple, la sécurité du système est conçue pour optimiser la sécurité des systèmes d'exploitation 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 le fonctionnement continu du système d'exploitation.

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 des appareils iOS, iPadOS et macOS.

Les versions les plus récentes d'iOS, d'iPadOS et de macOS sont les plus sûres. Non seulement le mécanisme de mise à jour logicielle livre les nouvelles versions aux appareils Apple en temps voulu, mais il ne fournit que les logiciels fiables d'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.

Enfin, les appareils Apple intègrent des protections au démarrage et à l'exécution, ce qui préserve leur intégrité pendant le fonctionnement. Ces protections varient de façon significative entre les appareils iOS, iPadOS et macOS, en fonction des capacités très différentes qui sont les leurs et des attaques auxquelles ils doivent faire face.

Pour parvenir à ce niveau de protection, iOS et iPadOS utilisent des systèmes de protection de l'intégrité du noyau et de l'intégrité du coprocesseur, des codes d'authentification de pointeurs (PAC) et une couche de protection des pages (PPL), tandis que macOS utilise l'Interface micrologicielle extensible unifiée (UEFI), le mode de gestion du système (SMM), les protections de l'accès direct à la mémoire (DMA) et la sécurité des micrologiciels des périphériques.

Chiffrement et protection des données

Les appareils Apple sont dotés de fonctionnalités de chiffrement pour protéger les données des utilisateurs et permettre l'effacement à distance en cas de vol ou de perte.

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 de l'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 à la fois aux utilisateurs et aux administrateurs informatiques 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 utilisent une méthode de chiffrement des fichiers intitulée Protection des données, tandis que les données des ordinateurs Mac sont protégées à l'aide d'une technologie de chiffrement des volumes nommée FileVault. Pour ces deux types d'appareils, les principales hiérarchies de gestion trouvent leurs fondations dans le composant en silicium dédié de la Secure Enclave sur les appareils qui intègrent un SEP (processeur Secure Enclave). Les deux types d'appareils exploitent également un moteur AES dédié permettant un chiffrement très rapide et veillant à ce qu'il ne soit jamais nécessaire de fournir les clés de chiffrement durables au noyau du système d'exploitation ou au processeur central, où celles-ci pourraient être mises à mal.

Sécurité des apps

Les apps constituent l'un des éléments cruciaux d'une architecture de sécurité moderne. Si les apps offrent aux utilisateurs 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 si celles-ci ne sont pas correctement gérées. 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. Des protections complémentaires s'appliquent pour l'accès aux données des utilisateurs quelles qu'elles soient à partir des apps et arbitrent attentivement ce processus.

Les commandes de sécurité intégrées constituent une plateforme stable et sécurisée pour les apps et permettent à des milliers de développeurs 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. Quant aux utilisateurs, ils peuvent accéder à ces apps depuis leurs appareils Apple grâce aux commandes en place qui les aident à se prémunir des virus, des logiciels malveillants et des attaques non autorisées.

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, pour offrir le maximum de contrôle. Sur Mac, la plupart des apps s'obtiennent sur l'App Store, mais les utilisateurs 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. Par ailleurs, macOS intègre une protection antivirus standard pour bloquer et, le cas échéant, éliminer tout logiciel malveillant.

La mise en bac à sable (« sandboxing »), qui est une forme de contrôle supplémentaire sur les différentes plateformes, contribue à protéger les données des utilisateurs contre les tentatives d'accès non autorisé émanant des apps. Et sous macOS, les données enregistrées sur le Bureau, dans les dossiers Documents et Téléchargements ainsi qu'à d'autres emplacements stratégiques sont elles-mêmes mises en bac à sable. Ainsi, que les tentatives d'accès proviennent d'apps elles-mêmes mises en bac à sable ou non, les utilisateurs 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 de gagner encore en efficacité et en productivité à l'aide de leurs appareils. Il s'agit notamment des services suivants : identifiant Apple, iCloud, Connexion avec Apple, Apple Pay, iMessage, FaceTime, Siri et Localiser. 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 ainsi que la sécurité de leurs données.

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 des protocoles standard pour le VPN 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.

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

apple.com/chfr/business/it

apple.com/fr/macos/security

apple.com/chfr/privacy/features/

apple.com/chfr/security