Sécurité de macOS

Présentation pour les services informatiques

Apple a opté pour une approche intégrée de la plateforme macOS dès sa conception. Le matériel, les logiciels et les services offrent ainsi des fonctionnalités de sécurité natives, ce qui rend les Mac plus simples à configurer, déployer et gérer. macOS délivre des technologies de sécurité essentielles exploitées par les services informatiques pour protéger les données des entreprises, et s'intègre parfaitement aux environnements réseau sécurisés pré-existants. En outre, Apple collabore avec des organismes de normalisation pour assurer la conformité de ses produits avec les dernières certifications de sécurité. Cette présentation va vous expliquer ces fonctionnalités dans les grandes lignes.

Ce document s'articule autour des thèmes suivants :

- **Sécurité du système :** le logiciel intégré et sécurisé à la base de macOS.
- **Chiffrement et protection des données :** l'architecture et la conception protégeant les données des utilisateurs en cas de perte ou de vol de l'appareil.
- **Sécurité des apps :** le système qui protège le Mac des logiciels malveillants et garantit que les apps s'exécutent en toute sécurité, sans compromettre l'intégrité de la plateforme.
- **Authentification et signature numérique :** les équipements intégrés à macOS pour la gestion des identifiants et la prise en charge des technologies standard de l'industrie, comme les cartes à puce et S/MIME.
- **Sécurité des réseaux :** les protocoles réseau standard qui assurent une authentification sécurisée et un chiffrement des données en transit.
- **Contrôle des appareils :** les méthodes permettant de gérer les appareils Apple, d'empêcher les utilisations non autorisées et d'effacer les données à distance en cas de perte ou de vol de l'appareil.

Pour plus d'informations sur le déploiement et la gestion de macOS, veuillez consulter Référence pour le déploiement macOS : help.apple.com/deployment/macos.

Pour plus d'informations sur les fonctionnalités de sécurité des services Apple qui ne sont pas présentées dans ce document, veuillez consulter le Guide Sécurité iOS : www.apple.com/fr/business/docs/iOS_Security_Guide.pdf.

Sécurité du système

Le système macOS est conçu pour que les logiciels et le matériel soient sécurisés sur tous les principaux composants de chaque Mac. Cette architecture est au cœur de la sécurité de macOS et ne nuit jamais à l'utilisabilité de l'appareil.

UNIX

Le cœur du système d'exploitation de macOS, le noyau, est basé sur BSD (Berkeley Software Distribution) et le micro-noyau Mach. BSD fournit le système de fichiers et les services réseau de base, un schéma d'identification pour les groupes et les utilisateurs, et bien d'autres fonctions essentielles. BSD applique également des restrictions d'accès aux fichiers et aux ressources système selon les identifiants des utilisateurs et des groupes.

Mach fournit la gestion de la mémoire, le contrôle de thread, l'abstraction matérielle et la communication inter-processus. Les ports Mach représentent les tâches et les autres ressources. Mach autorise l'accès aux ports après avoir contrôlé les tâches qui peuvent communiquer avec eux. Les règles de sécurité BSD et les autorisations d'accès Mach constituent un fondement essentiel de la sécurité sous macOS et jouent un rôle primordial dans l'application de la sécurité au niveau local.

La sécurité du noyau joue un rôle crucial dans la sécurité de l'ensemble du système d'exploitation. La signature de code protège le noyau et les extensions de noyau tierces, ainsi que les autres bibliothèques système et exécutables développés par Apple.

Modèles d'autorisation de l'utilisateur

Un aspect important de la sécurité du Mac passe par l'octroi ou le refus d'autorisations d'accès (parfois appelées droits d'accès). Les autorisations permettent d'effectuer des opérations spécifiques, comme accéder à des données ou exécuter du code. Elles sont accordées au niveau des dossiers, des sous-dossiers, des fichiers et des apps. Elles concernent également des données spécifiques au sein de fichiers, des fonctionnalités dans des apps et des fonctions d'administration. Les signatures numériques identifient les droits d'accès aux apps et aux composants du système.

macOS contrôle les autorisations à de nombreux niveaux, y compris au niveau des composants Mach et BSD du noyau. Pour contrôler les autorisations des apps en réseau, macOS utilise des protocoles réseau.

Contrôles d'accès obligatoires

macOS utilise également les contrôles d'accès obligatoires, des règles définissant les restrictions de sécurité créées par les développeurs, et qui ne peuvent pas être contournées. Cette approche est différente de celle des contrôles d'accès facultatifs. En effet, ces derniers autorisent les utilisateurs à déroger aux règles de sécurité selon leurs préférences. Les contrôles d'accès obligatoires ne sont pas visibles pour les utilisateurs. Ils permettent néanmoins le fonctionnement de plusieurs fonctionnalités importantes, dont la mise en bac à sable, les contrôles parentaux, les préférences gérées, les extensions et la Protection de l'intégrité du système.

Protection de l'intégrité du système

OS X 10.11 et les versions ultérieures intègrent une protection au niveau du système appelée Protection de l'intégrité du système. Son rôle est de restreindre l'accès aux composants en lecture seule dans certains emplacements critiques du système de fichiers, afin d'empêcher tout code malveillant de les exécuter ou de les modifier. La Protection de l'intégrité du système est un réglage spécifique à l'ordinateur qui est activé par défaut lors de la mise à niveau vers OS X 10.11. La désactiver supprime la protection pour toutes les partitions de l'appareil de stockage physique. macOS applique cette règle de sécurité à tous les processus actifs au sein du système, qu'ils soient exécutés en bac à sable ou avec des privilèges administrateur.

Pour plus d'informations sur les emplacements du système de fichiers en lecture seule, veuillez consulter l'article de l'Assistance Apple « À propos de la fonctionnalité Protection de l'intégrité du système sur votre Mac » : support.apple.com/HT204899.

Extensions de noyau

macOS dispose d'un mécanisme d'extension de noyau permettant le chargement dynamique du code au sein du noyau sans besoin de recompiler ou de rétablir la liaison. Ces extensions de noyau (KEXTs) offrant à la fois le chargement modulaire et dynamique, elles constituent un choix naturel pour les services autonomes devant accéder aux interfaces internes du noyau, comme les pilotes de périphériques matériels ou les apps VPN par exemple.

Pour améliorer la sécurité du Mac, le chargement des extensions du noyau installées pendant ou après l'installation de macOS High Sierra nécessite l'accord de l'utilisateur. C'est ce qu'on appelle le chargement des extensions de noyau approuvées par l'utilisateur. Tous les utilisateurs peuvent approuver une extension de noyau, même s'ils ne bénéficient pas de privilèges administrateur.

Les extensions de noyau peuvent se passer d'autorisation dans les cas suivants :

- Elles ont été installées sur le Mac avant la mise à niveau vers macOS High Sierra.
- Elles remplacent des extensions déjà approuvées auparavant.
- Elles sont autorisées à se charger sans accord de l'utilisateur en ayant recours à la commande `spctl` disponible lors du démarrage à partir de la fonctionnalité de récupération de macOS.
- Elles sont autorisées à se charger via la configuration de la gestion des appareils mobiles (Mobile Device Management, MDM). À partir de macOS High Sierra 10.13.2, vous pouvez utiliser la MDM pour spécifier une liste d'extensions de noyau qui pourront être chargées sans l'accord de l'utilisateur. Pour utiliser cette option, l'utilisateur devra disposer d'un Mac équipé de macOS High Sierra 10.13.2 inscrit à la MDM via le Programme d'inscription des appareils (Device Enrollment Program, DEP) ou via l'inscription à la MDM approuvée par l'utilisateur.

Pour plus d'informations sur les extensions de noyau, consultez l'article de l'Assistance Apple « Préparation aux modifications apportées aux extensions de noyau dans macOS High Sierra » : support.apple.com/HT208019.

Mot de passe du programme interne

macOS prend en charge l'utilisation d'un mot de passe pour empêcher les modifications indésirables des réglages du programme interne sur un système spécifique. Ce mot de passe de programme interne proscrit les situations suivantes :

- Démarrage à partir d'un volume système non autorisé
- Altération du processus de démarrage, par exemple démarrer en mode utilisateur unique
- Accès non autorisé à la fonctionnalité de récupération de macOS
- Accès direct à la mémoire via des interfaces telles que Thunderbolt
- Mode disque cible, qui nécessite l'accès direct à la mémoire

Remarque : la puce T2 d'Apple de l'iMac Pro empêche les utilisateurs de réinitialiser le mot de passe du programme interne, même s'ils accèdent physiquement au Mac. Les Mac n'étant pas dotés d'une puce T2 doivent faire l'objet de précautions supplémentaires pour empêcher l'accès physique des utilisateurs aux systèmes internes du Mac.

Récupération par Internet

Les Mac essayent automatiquement de démarrer à partir de la fonctionnalité de récupération de macOS par Internet lorsqu'ils ne parviennent pas à démarrer à partir du système de récupération intégré. Dans ce cas de figure, le logo Apple qui s'affiche normalement au démarrage est remplacé par un globe en rotation. La récupération par Internet permet aux utilisateurs de réinstaller la version de macOS la plus récente, ou bien la version d'origine livrée avec leur Mac.

Les mises à jour de macOS sont distribuées via l'App Store et exécutées par le programme d'installation de macOS, qui utilise des signatures de code pour assurer l'intégrité et l'authenticité du programme d'installation et de ses paquets avant l'installation. De la même manière, le service de récupération par Internet est la source faisant autorité sur le système d'exploitation d'origine d'un Mac spécifique.

Pour plus d'informations sur la fonctionnalité de récupération de macOS, consultez l'article de l'Assistance Apple « À propos de la fonctionnalité de récupération de macOS » : support.apple.com/HT201314.

Chiffrement et protection des données

Système de fichiers Apple

Le système de fichiers Apple (APFS) est un nouveau système de fichiers moderne conçu pour macOS, iOS, tvOS et watchOS. Optimisé pour le stockage Flash/SSD, il offre les caractéristiques suivantes : chiffrement avancé, copie sur écriture des métadonnées, partage des espaces, clonage de fichiers et de répertoires, instantanés, redimensionnement rapide de répertoires, opérations atomiques primitives de sauvegarde sécurisée, bases de système de fichiers améliorées et fonction de copie sur écriture unique exploitant une E/S coalescente pour fournir des performances maximales tout en garantissant la fiabilité des données.

APFS attribue de l'espace disque sur demande. Lorsqu'un conteneur APFS contient plusieurs volumes, son espace libre est partagé et peut être attribué à chacun des volumes individuels, selon leurs besoins respectifs. Puisque chaque volume utilise une partie seulement du conteneur, l'espace disponible est donc égal à la taille totale du conteneur, moins l'espace utilisé dans tous les volumes du conteneur.

Pour macOS High Sierra, un conteneur APFS valide doit comporter au moins trois volumes, les deux premiers n'étant pas visibles par l'utilisateur :

- Volume de prédémarrage : contient les données nécessaires au démarrage de chacun des volumes système du conteneur.
- Volume de secours : contient le disque de récupération.
- Volume système : contient macOS et le dossier Utilisateur.

FileVault

Tous les Mac sont dotés d'une fonctionnalité de chiffrement intégrée qui assure la sécurité des données au repos. Il s'agit de FireVault. FireVault utilise le chiffrement de données XTS-AES-128 pour sécuriser les données des Mac au repos. Il est possible d'étendre ce chiffrement à la protection complète des volumes des appareils de stockage internes et amovibles. Si un utilisateur saisit un identifiant Apple et un mot de passe pendant la phase de l'Assistant réglages, celui-ci suggère d'activer FireVault et de stocker la clé de secours dans iCloud.

Lorsqu'un utilisateur active FireVault sur un Mac, il est invité à fournir des identifiants valides avant de poursuivre le processus de démarrage et de pouvoir accéder à des modes de démarrage spécialisés, comme le mode disque cible. Sans les identifiants de connexion valides ou une clé de secours, l'ensemble du volume reste chiffré et protégé contre les accès non autorisés même si le périphérique de stockage physique est retiré et connecté à un autre ordinateur.

Pour protéger les données au sein de l'environnement d'une entreprise, les services informatiques doivent définir et appliquer les règles de configuration de FireVault par le biais de la MDM. Les organisations disposent de plusieurs options de gestion des volumes chiffrés, notamment les clés de secours institutionnelles, les clés de secours personnelles (qui peuvent éventuellement être stockées sous séquestre avec la MDM), ou bien une combinaison des deux. Il est également possible de définir une règle de rotation des clés dans la MDM.

Images disque chiffrées

Sous macOS, les images disque chiffrées ont une fonction de conteneurs sécurisés dans lesquels les utilisateurs peuvent stocker ou transférer des documents et d'autres fichiers sensibles. Les images disque chiffrées sont créées par l'Utilitaire de disque, situé dans /Applications/Utilitaires/. Les images disque peuvent être chiffrées à l'aide d'un chiffrement AES 128 bits ou 256 bits. Une image disque montée étant traitée comme un volume local connecté à un Mac, les utilisateurs peuvent copier, déplacer et ouvrir les fichiers et les dossiers qui y sont stockés. De la même manière que pour FileVault, les contenus d'une image disque sont chiffrés et déchiffrés en temps réel. Les images disque chiffrées permettent aux utilisateurs d'échanger des documents, des fichiers et des dossiers en toute sécurité. Pour ce faire, il leur suffit de sauvegarder une image disque chiffrée sur un support amovible, de l'envoyer en pièce jointe d'un e-mail ou de la stocker sur un serveur distant.

Certifications ISO 27001 et 27018

Apple a obtenu les certifications ISO 27001 et ISO 27018 pour le système de gestion de la sécurité de l'information (ISMS) concernant l'infrastructure, le développement et l'exploitation mis en œuvre dans les produits et services suivants : Apple School Manager, iCloud, iMessage, FaceTime, les identifiants Apple gérés et iTunes U, conformément à la Déclaration d'applicabilité v 2.1 du 11 juillet 2017. La conformité d'Apple aux normes ISO a été certifiée par BSI (British Standards Institution). Rendez-vous sur le site de BSI pour consulter les certificats de conformité ISO 27001 et ISO 27018.

www.bsigroup.com/fr-FR/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/fr-FR/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Validation cryptographique (FIPS 140-2)

Les modules cryptographiques de macOS ont été certifiés à plusieurs reprises conformes aux Federal Information Processing Standards (FIPS) 140-2 niveau 1 pour chaque version depuis OS X 10.6. Comme pour toute version majeure, Apple soumet les modules finaux au CMVP pour confirmer la validation lors de la diffusion publique du système d'exploitation Mac. Ce programme valide l'intégrité des opérations cryptographiques des apps Apple et des apps tierces exploitant les services cryptographiques et les algorithmes approuvés de macOS. Tous les certificats de validation de conformité FIPS 140-2 Apple sont accessibles sur la page répertoriant les fournisseurs adhérant au programme CMVP. Le CMVP sépare les statuts de validation des modules cryptographiques en deux listes distinctes basées sur leur statut actuel : csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Certification Critères Communs (ISO 15408)

Les certifications précédemment obtenues pour macOS ont été délivrées par le programme de certification Critères Communs. Apple prend maintenant part à un processus d'évaluation de macOS High Sierra par rapport au profil de protection du système d'exploitation (PP_OSv4.1). Apple continue à évaluer et à prendre part à des certifications pour les nouvelles versions et les versions mises à jour des profils de protection collaboratifs (cPP) disponibles actuellement. Apple a joué un rôle majeur au sein de la communauté technique internationale (iTC), où elle a développé des cPP axés sur l'évaluation de technologies de sécurité mobile essentielles.

Certifications, programmes et procédures de sécurité

Apple a collaboré avec des autorités dans le monde entier afin de développer des guides comportant des instructions et des conseils pour préserver un niveau élevé de sécurité des environnements, aussi appelé « durcissement des appareils » pour les environnements à risque élevé. Ces guides proposent des informations précises et validées sur la configuration et l'utilisation des fonctionnalités intégrées à macOS pour améliorer la sécurité.

Pour connaître les dernières informations relatives aux certifications, validations et procédures de sécurité pour macOS, consultez l'article de l'Assistance Apple « Sécurité des produits : certifications, validations et procédures applicables pour macOS » : support.apple.com/HT201159.

Sécurité des apps

Les technologies intégrées à macOS défendent les appareils en cas d'attaque de logiciels malveillants et garantissent que seules des apps de confiance peuvent être installées. Pour empêcher les manœuvres frauduleuses sur les apps de confiance, macOS intègre également une approche à plusieurs niveaux pour les protéger au moment de l'exécution et exige une signature.

Gatekeeper

La fonctionnalité Gatekeeper intégrée à macOS contrôle les sources à partir desquelles l'installation d'apps est autorisée. Gatekeeper permet aux utilisateurs et aux organisations de définir le niveau de sécurité requis pour l'installation des apps.

Avec le réglage Gatekeeper le plus sécurisé, les utilisateurs peuvent uniquement installer des apps signées à partir de l'App Store. Un réglage par défaut permet aux utilisateurs d'installer des apps à partir de l'App Store et des apps ayant une signature d'identifiant de développeur valide. Cette signature indique que les apps ont été signées par un certificat émis par Apple et qu'elles n'ont pas été modifiées depuis. Si nécessaire, Gatekeeper peut être totalement désactivé par le biais d'une commande du terminal.

En outre, Gatekeeper est capable de générer des chemins aléatoires dans certaines situations, notamment lorsque des apps sont ouvertes directement depuis une image disque non signée, ou bien depuis l'emplacement où elles ont été téléchargées et automatiquement désarchivées. Avec la génération aléatoire de chemins, l'utilisateur accède aux apps depuis un emplacement en lecture seule non spécifié dans le système de fichiers avant le lancement. L'ouverture depuis un emplacement en lecture seule les empêche d'accéder au code ou aux contenus par le biais de chemins relatifs, ainsi que de se mettre à jour. Utiliser le Finder pour déplacer une app, par exemple dans le dossier Applications, désactivera la fonction de génération aléatoire de chemin pour cette app.

Le modèle de protection par défaut offre un avantage majeur du point de vue de la sécurité : la protection est étendue à l'intégralité du système. Dans l'éventualité où l'auteur d'un logiciel malveillant parviendrait à voler ou à obtenir la capacité de signature d'un identifiant de développeur valide et à l'utiliser pour diffuser son logiciel malveillant, Apple serait en mesure de révoquer son certificat de signature sans délai, et ainsi mettre un terme à la propagation du logiciel malveillant. Ce type de protection nuit au modèle économique de la plupart des campagnes de diffusion de logiciels malveillants sur Mac et fait bénéficier les utilisateurs d'une protection complète.

Il est possible de contourner ces réglages temporairement pour installer une app. Les organisations peuvent utiliser leur solution MDM pour définir et appliquer des réglages Gatekeeper, mais aussi pour ajouter des certificats aux règles de confiance de macOS relatives à l'évaluation de la signature de code.

XProtect

macOS intègre une technologie permettant la détection de logiciels malveillants basée sur les signatures. Apple surveille les nouvelles infections et souches virales pour mettre automatiquement à jour les signatures XProtect et assurer la protection des systèmes Mac face aux logiciels malveillants, indépendamment des mises à jour du système. XProtect détecte automatiquement les tentatives d'installation de logiciels malveillants avérés et les bloque.

Outil de suppression de logiciels malveillants

Dans l'éventualité où un logiciel malveillant parviendrait à s'installer sur un Mac, macOS intègre aussi les technologies visant à l'en déloger. Apple surveille l'activité des logiciels malveillants au sein de l'écosystème pour être en mesure de révoquer les identifiants de développeurs (le cas échéant) et de publier des mises à jour de XProtect. Apple publie également des mises à jour de macOS pour permettre aux systèmes d'exploitation de supprimer les logiciels malveillants des systèmes attaqués qui ont été configurés pour recevoir des mises à jour de sécurité automatiques. L'outil de suppression de logiciels malveillants reçoit les données récentes, et supprime le logiciel incriminé au prochain redémarrage. Il n'est pas en mesure d'effectuer un redémarrage automatique du Mac.

Mises à jour de sécurité automatiques

Apple publie automatiquement les mises à jour de XProtect et de l'outil de suppression des logiciels malveillants. Par défaut, macOS recherche quotidiennement les nouvelles mises à jour. Pour plus d'informations sur les mises à jour de sécurité automatiques, consultez l'article de l'Assistance Apple « Mac App Store : mises à jour de sécurité automatiques » : support.apple.com/HT204536.

Protection à l'exécution

Les fichiers système, les ressources et le noyau sont protégés et isolés de l'espace utilisateur dédié aux apps. Les apps de l'App Store sont exécutées dans un bac à sable pour restreindre l'accès aux données stockées par d'autres apps. Si une app de l'App Store doit accéder aux données d'une autre app, elle ne peut le faire qu'en utilisant les API et les services fournis par macOS.

Signature de code de l'app obligatoire

Toutes les apps de l'App Store sont signées par Apple afin de s'assurer qu'elles n'ont pas été piratées ou altérées. Apple signe toutes les apps fournies avec les appareils Apple. Beaucoup d'apps provenant de services autres que l'App Store sont signées par leurs développeurs, qui utilisent un certificat d'identifiant de développeur émis par Apple (associé à une clé privée) pour témoigner de leur conformité aux critères par défaut de Gatekeeper.

Les apps ne provenant pas de l'App Store sont normalement signées avec un certificat de développeur émis par Apple. Cela vous permet de valider que l'app est authentique et n'a pas été détournée. Les apps développées en interne doivent également être signées à l'aide d'un identifiant de développeur émis par Apple, pour que vous puissiez valider leur intégrité.

Les contrôles d'accès obligatoires requièrent une signature de code avant de pouvoir activer certains droits protégés par le système. Par exemple, les apps demandant un accès au travers du coupe-feu devront être dotées d'une signature de code présentant les autorisations de contrôles d'accès obligatoires adéquates.

Authentification et signature numérique

Pour stocker les identifiants et les identités numériques des utilisateurs de manière simple et sécurisée, macOS a recours au Trousseau et à d'autres outils permettant l'authentification et la prise en charge d'autres technologies de signature numérique, comme les cartes à puce et S/MIME.

Architecture du Trousseau

Le Trousseau est un référentiel macOS qui assure le stockage sécurisé des noms et mots de passe des utilisateurs, y compris les identités numériques, les clés de chiffrement et les notes sécurisées. Il est accessible via l'app Trousseaux d'accès, située dans /Applications/Utilitaires/. Avec un trousseau, il n'est plus nécessaire de saisir des identifiants pour chaque ressource, ni même de s'en souvenir. Un trousseau initial par défaut est créé pour chaque utilisateur Mac, mais les utilisateurs peuvent créer d'autres trousseaux à des fins spécifiques.

En plus des trousseaux utilisateur, macOS comporte également des trousseaux au niveau du système qui gèrent les moyens d'authentification non spécifiques de l'utilisateur, comme les identifiants de connexion au réseau et les identités d'infrastructure à clés publiques (PKI). L'un de ces trousseaux, le trousseau Racines du système, est une banque immuable de certificats racine Internet PKI émis par une autorité de certification (AC) qui facilite les tâches courantes comme la banque en ligne et le commerce électronique. De la même manière, vous pouvez déployer des certificats provisionnés en interne, délivrés par une AC, sur des ordinateurs Mac gérés afin de faciliter la validation de sites et services internes.

Structure d'authentification sécurisée

Les données du Trousseau sont segmentées et protégées par des listes de contrôle d'accès, de façon à ce que des apps avec des identités différentes ne puissent accéder aux identifiants stockés par des apps tierces, sauf approbation explicite de l'utilisateur. Cette protection vous permet de sécuriser les informations d'authentification sur les appareils Apple pour un large éventail d'apps et de services au sein de votre entreprise.

Touch ID

Les systèmes Mac équipés d'un capteur Touch ID peuvent être déverrouillés avec une empreinte digitale. Touch ID ne remplace pas entièrement le mot de passe, qui est toujours exigé pour se connecter après un démarrage, un redémarrage ou la déconnexion d'un Mac. Après la connexion initiale, les utilisateurs peuvent s'authentifier rapidement avec Touch ID à chaque demande de mot de passe.

Ils peuvent également utiliser Touch ID pour déverrouiller des notes protégées par mot de passe dans l'app Notes, le volet Mots de passe des préférences Safari et plusieurs volets de Préférences Système. Pour des raisons de sécurité, l'accès au volet Sécurité et confidentialité de Préférences Système nécessite la saisie d'un mot de passe. Si FireVault est activé, les utilisateurs devront également saisir un mot de passe pour gérer les préférences Utilisateurs et groupes. Si plusieurs personnes utilisent le même Mac, elles peuvent utiliser Touch ID pour passer d'un compte à l'autre.

Pour plus d'informations sur Touch ID et sa sécurité, consultez l'article de l'Assistance Apple « À propos de la technologie de sécurité avancée Touch ID » : support.apple.com/HT204587.

Déverrouillage automatique avec l'Apple Watch

Les utilisateurs possédant une Apple Watch peuvent s'en servir pour déverrouiller automatiquement leur Mac. L'Apple Watch exploite la technologie Bluetooth Low Energy (BLE) et le Wi-Fi pair-à-pair pour déverrouiller un Mac de manière sécurisée, après vérification que les deux appareils sont placés côte à côte. Cette méthode requiert un compte iCloud sur lequel l'identification à deux facteurs est configurée.

Pour en savoir plus sur le protocole et obtenir plus d'informations sur les fonctionnalités Continuité et Handoff, consultez le Guide Sécurité iOS : www.apple.com/fr/business/docs/iOS_Security_Guide.pdf.

Cartes à puce

macOS Sierra et les versions ultérieures intègrent la prise en charge native des cartes de vérification de l'identité personnelle (PIV). Ces cartes sont couramment employées pour appliquer l'identification à deux facteurs, la signature numérique et le chiffrement dans les organisations commerciales et publiques.

Les cartes à puce comportent une ou deux identités numériques associées à une paire de clés (une privée et une publique) et à un certificat. Déverrouiller une carte à puce avec un numéro d'identification personnel (PIN) donne accès aux clés privées utilisées dans les opérations d'authentification, de chiffrement et de signature. Le certificat détermine le rôle que peut avoir une clé, les attributs qui lui sont associés, et vérifie qu'elle a été validée (signée) par une AC.

Les cartes à puce peuvent être utilisées dans le cadre de l'identification à deux facteurs. Les deux facteurs nécessaires au déverrouillage d'une carte sont « un élément que vous possédez » et « un élément que vous connaissez » (le code PIN). macOS Sierra et les versions ultérieures intègrent la prise en charge native de l'authentification par connexion de la carte à puce et de l'authentification aux sites web dans Safari par certificat client. Il assure également l'authentification Kerberos à l'aide de paires de clés (PKINIT) pour l'authentification unique sur les services pris en charge par Kerberos.

Pour plus d'informations sur le déploiement des cartes à puce de macOS, veuillez consulter le document Référence pour le déploiement macOS : help.apple.com/deployment/macos.

Signature numérique et chiffrement

Les utilisateurs peuvent utiliser l'app Mail pour envoyer des messages signés numériquement et chiffrés. Mail récupère automatiquement les noms d'objet ou les noms d'objet alternatifs des adresses e-mail sensibles à la casse conformes à la norme RFC 822 à partir des certificats de signature numérique et de chiffrement associés aux jetons PIV joints des cartes à puce compatibles. Si un compte d'e-mail configuré correspond à une adresse e-mail figurant sur un certificat de signature numérique ou de chiffrement associé à un jeton PIV, Mail affiche automatiquement le bouton de signature dans la barre d'outils d'un nouveau message. Si Mail dispose du certificat de chiffrement d'e-mail du destinataire ou le récupère dans la Liste d'adresses globale de Microsoft Exchange, une icône de cadenas déverrouillé s'affiche dans la barre d'outils du nouveau message. L'affichage d'une icône de cadenas verrouillé signifie que le message envoyé sera chiffré avec la clé publique du destinataire.

S/MIME par message

macOS prend en charge les certificats S/MIME par message. Cela veut dire que les utilisateurs peuvent choisir de toujours signer et chiffrer les messages par défaut ou bien de signer et chiffrer des messages individuels.

Il est possible d'envoyer les identités utilisées avec S/MIME à des appareils Apple par le biais d'un profil de configuration, d'une solution MDM, d'un protocole SCEP (Simple Certificate Enrollment Protocol) ou d'une AC Microsoft Active Directory.

Sécurité des réseaux

En plus des protections intégrées qu'Apple utilise pour protéger les données enregistrées sur les Mac, de nombreuses mesures de sécurité réseau permettent aux organisations de sécuriser les données en transit vers ou depuis un Mac.

Les utilisateurs mobiles 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. macOS exploite des protocoles réseau standard pour authentifier, autoriser et chiffrer toutes

les communications, et offre aussi aux développeurs l'accès à ces protocoles. Pour atteindre ces objectifs de sécurité, macOS intègre des technologies éprouvées et les normes les plus récentes en matière de connexions de données à un réseau Wi-Fi.

TLS

macOS prend en charge les protocoles Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2) et DTLS. Il exploite les algorithmes AES-128 et AES-256, et favorise les suites de chiffrement dotées de la confidentialité persistante (PFS, Perfect Forward Secrecy). Safari, Calendrier, Mail et d'autres apps Internet utilisent automatiquement ce protocole pour activer un canal de communication chiffré entre l'appareil et les services réseau.

Les API de haut niveau, comme CFNetwork, permettent aux développeurs d'intégrer plus facilement le protocole TLS à leurs apps, tandis que les API de bas niveau, comme secureTransport, offrent un contrôle plus précis. CFNetwork ne permet pas d'utiliser SSLv3, et les apps exploitant WebKit, comme Safari, ne sont pas en mesure de créer des connexions SSLv3.

À compter de macOS High Sierra et iOS 11, les certificats SHA-1 ne sont plus autorisés à établir des connexions TLS, sauf si elles sont approuvées par l'utilisateur. Les certificats comportant des clés RSA de moins de 2 048 bits sont également proscrits. La suite de chiffrement symétrique RC4 a été dépréciée sous macOS Sierra et iOS 10. Par défaut, les suites de chiffrement RC4 sont désactivées pour les clients et serveurs TLS déployés avec des API SecureTransport, et ceux-ci ne sont pas en mesure de se connecter lorsque seule la suite de chiffrement RC4 est disponible. Pour plus de sécurité, les services et les apps nécessitant RC4 doivent être mis à niveau vers l'utilisation de suites de chiffrement plus modernes et plus sécurisées.

App Transport Security

App Transport Security fournit des exigences de connexion par défaut. Les apps sont donc contraintes d'adhérer aux meilleures pratiques en matière de connexion sécurisée lorsqu'elles utilisent les API NSURLConnection, CFURL ou NSURLSession. Par défaut, App Transport Security limite le choix des chiffrements pour uniquement intégrer des suites dotées de la confidentialité persistante, notamment ECDHE_ECDSA_AES et ECDHE_RSA_AES en mode GCM ou CBC. Les apps peuvent désactiver la confidentialité persistante par domaine, auquel cas RSA_AES sera ajouté à la liste des chiffrements disponibles.

Les serveurs doivent prendre en charge TLS 1.2 et la confidentialité persistante, et les certificats doivent être validés et signés avec SHA-256 ou un hachage supérieur, avec au minimum une clé RSA 2048 bits ou une clé de courbe elliptique 256 bits.

Les connexions réseau ne répondant pas à ces critères échoueront, sauf si l'app annule App Transport Security. Les certificats invalides entraînent systématiquement un échec total de connexion. App Transport Security est automatiquement appliqué aux apps compilées pour macOS 10.11 ou version ultérieure.

VPN

Les services réseau sécurisés tels que les réseaux privés virtuels (VPN) demandent généralement une installation et une configuration minimales pour être utilisés avec macOS. Les Mac fonctionnent avec les serveurs VPN qui prennent en charge les protocoles et les méthodes d'authentification suivants :

- IKEv2/IPSec avec authentification par secret partagé, certificats RSA, certificats ECDSA, EAP-MSCHAPv2 ou EAP-TLS
- SSL-VPN à l'aide d'une app client correspondante disponible sur l'App Store

- Cisco IPSec avec authentification des utilisateurs par mot de passe, RSA SecurID ou CRYPTOCard et authentification des machines par secret partagé et par certificat
- L2TP/IPSec avec authentification des utilisateurs via les protocoles MS-CHAPv2 Password, RSA SecurID ou CRYPTOCard et authentification des machines par secret partagé

En plus des solutions VPN tierces, macOS prend en charge les fonctions suivantes :

- **VPN à la demande** pour les réseaux utilisant l'authentification par certificat. Les règles informatiques identifient les domaines nécessitant une connexion VPN à l'aide d'un profil de configuration de VPN.
- **VPN via l'app** pour gérer les connexions VPN à un degré de granularité bien plus élevé. La MDM peut spécifier une connexion pour chaque app gérée et pour des domaines particuliers dans Safari. Cela garantit que les données sécurisées transitent toujours vers et depuis le réseau de l'entreprise, contrairement aux données personnelles des utilisateurs.

Wi-Fi

macOS prend en charge les protocoles Wi-Fi standard, notamment WPA2 Enterprise, pour fournir un accès authentifié aux réseaux sans fil des entreprises. WPA2 Enterprise utilise le chiffrement AES 128 bits, pour garantir aux utilisateurs un niveau optimal de protection lors de l'envoi et de la réception de données par le biais d'une connexion réseau Wi-Fi. Avec la prise en charge de la norme 802.1X, le Mac peut s'intégrer à une grande diversité d'environnements d'authentification RADIUS. Les méthodes d'authentification sur les réseaux sans fil avec la norme 802.1X comprennent EAP-TLS, EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1 et LEAP.

L'authentification WPA/WPA2 Enterprise peut aussi être utilisée dans la fenêtre de connexion de macOS de sorte que l'utilisateur puisse se connecter pour s'authentifier sur le réseau.

L'Assistant réglages de macOS prend en charge l'authentification 802.1X avec nom d'utilisateur et mot de passe en utilisant le protocole TTLS ou PEAP.

Coupe-feu

macOS intègre un coupe-feu pour protéger le Mac en cas d'accès non autorisé au réseau et d'attaques par déni de service. Il prend en charge les configurations suivantes :

- Bloquer toutes les connexions entrantes, quelles que soient les apps
- Autoriser automatiquement les logiciels intégrés à recevoir des connexions entrantes
- Autoriser automatiquement les logiciels signés et téléchargés à recevoir des connexions entrantes
- Ajouter ou refuser un accès selon les apps spécifiques de l'utilisateur
- Empêcher le Mac de répondre aux interrogations ICMP et aux requêtes de balayage des ports

Authentification unique

macOS prend en charge l'authentification sur les réseaux d'entreprise via Kerberos. Les apps peuvent utiliser Kerberos pour authentifier les utilisateurs auprès de services auxquels ils sont autorisés à accéder. Kerberos peut être utilisé pour d'autres activités réseau, comme les sessions Safari sécurisées et l'authentification du système de fichiers réseau (NFS) pour les apps tierces. L'authentification par certificat (PKINIT) est prise en charge, mais il est toutefois nécessaire que l'app adopte un API de développeur.

Les jetons GSS-API SPNEGO et le protocole HTTP Negotiate utilisent des passerelles d'authentification basées sur Kerberos et des systèmes d'authentification intégrés à Windows prenant en charge les tickets Kerberos. La prise en charge de Kerberos est basée sur le projet open source Heimdal.

Les types de chiffrement suivants sont pris en charge :

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Pour configurer Kerberos, procurez-vous des tickets auprès du Visualiseur de ticket, connectez-vous à un domaine Windows Active Directory ou utilisez l'outil de ligne de commande `kinit`.

Sécurité AirDrop

Les Mac prenant en charge AirDrop utilisent la technologie BLE et le Wi-Fi pair-à-pair conçu par Apple pour envoyer des fichiers et des informations aux appareils à proximité, notamment aux appareils iOS compatibles AirDrop équipés d'iOS 7 ou d'une version ultérieure. La radio Wi-Fi permet la communication directe entre les appareils sans connexion Internet ni point d'accès Wi-Fi. Cette connexion est chiffrée avec TLS.

Pour plus d'informations sur AirDrop, la sécurité AirDrop et d'autres services Apple, consultez la rubrique « Sécurité du réseau » du Guide Sécurité iOS : www.apple.com/fr/business/docs/iOS_Security_Guide.pdf.

Contrôle des appareils

macOS est compatible avec des configurations et des règles de sécurité flexibles simples à mettre en œuvre et à gérer. Les organisations peuvent ainsi protéger les informations sensibles et vérifier que les employés respectent les exigences de l'entreprise, y compris dans les situations où ils utilisent des ordinateurs personnels, notamment dans le cadre d'un programme d'utilisation d'appareils personnels (BYOD).

Les organisations peuvent avoir recours à la protection par mot de passe, aux profils de configuration et aux solutions MDM tierces pour gérer les parcs d'appareils et garantir la sécurité des données de l'entreprise, y compris lorsque les employés accèdent à ces données depuis leurs ordinateurs personnels.

Protection par mot de passe

Les Mac avec Touch ID exigent un code d'accès de huit caractères minimum. Il est recommandé d'utiliser des codes d'accès longs et complexes, qui seront plus difficiles à deviner ou à attaquer.

Les administrateurs peuvent appliquer des règles de mot de passe complexes via la MDM ou en demandant aux utilisateurs d'installer des profils de configuration manuellement. L'installation d'une entité de règle de mot de passe macOS nécessite un mot de passe administrateur.

Pour plus d'informations sur les règles disponibles dans les réglages MDM, consultez l'article suivant : help.apple.com/deployment/mdm/#/mdm4D6A472A.

Pour plus d'informations sur ces règles du point de vue du développeur, consultez le guide de référence des profils de configuration : developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef.

Application de la configuration

Un profil de configuration est un fichier XML qui permet à un administrateur de distribuer des informations de configuration à des ordinateurs Mac. Si l'utilisateur supprime un profil de configuration, tous les réglages définis par le profil seront également supprimés. Les administrateurs peuvent appliquer des réglages en associant des règles à l'accès au Wi-Fi et aux données. Par exemple, un profil de configuration qui contient une configuration de messagerie peut également indiquer une règle de mot de passe pour l'appareil. Un utilisateur ne pourra pas accéder à ses e-mails si le mot de passe ne respecte pas les conditions mises en place par l'administrateur.

Il est possible de définir plusieurs réglages au sein d'un profil de configuration macOS :

- Règles de code de verrouillage
- Restrictions des fonctionnalités de l'appareil (par exemple, l'appareil photo)
- Réglages Wi-Fi ou VPN
- Réglages du serveur Mail ou Exchange
- Réglages du service d'annuaire LDAP
- Réglages du coupe-feu
- Identifiants et clés
- Mises à jour logicielles

Pour connaître la liste des profils actuels, consultez le guide de référence des profils de configuration : help.apple.com/deployment/mdm/#/mdm5370d089.

Les profils de configuration peuvent être signés et chiffrés pour valider leur origine, garantir leur intégrité et protéger leurs contenus. Les profils de configuration peuvent également être verrouillés sur un Mac pour empêcher complètement leur suppression, ou pour l'autoriser uniquement avec un mot de passe. Les profils de configuration dont le rôle est d'inscrire un Mac auprès d'une solution MDM peuvent être supprimés. Toutefois, les informations de configuration, les données et les apps gérées seront également supprimées.

Les utilisateurs peuvent installer des profils de configuration téléchargés depuis Safari, envoyés dans un e-mail ou envoyés à distance via une solution MDM. Lorsqu'un utilisateur configure un Mac dans le cadre du Programme d'inscription des appareils (Device Enrolment Program, DEP) ou dans Apple School Manager, l'ordinateur télécharge et installe automatiquement un profil destiné à l'inscription à la MDM.

Gestion des appareils mobiles (MDM)

Avec macOS, les entreprises peuvent utiliser la MDM pour configurer et gérer les déploiements évolutifs de Mac, d'iPhone, d'iPad et d'Apple TV dans leur organisation de manière sécurisée. Les capacités MDM reposent sur des technologies macOS existantes comme les profils de configuration, l'inscription à distance et le service de notification push d'Apple (APN). Le service APN peut par exemple faire sortir l'appareil de veille pour qu'il communique directement avec la solution MDM par le biais d'une connexion sécurisée. Le service APN ne transmet aucune information de nature confidentielle ou propriétaire.

Avec la MDM, les services informatiques peuvent inscrire des Mac dans un environnement d'entreprise, configurer et mettre à jour des réglages à distance, contrôler la conformité aux règles de l'entreprise, et même effacer ou verrouiller à distance les Mac gérés.

Inscription des appareils

L'inscription des appareils est l'une des fonctionnalités d'Apple School Manager et des programmes de déploiement Apple. Elle permet d'effectuer le déploiement rapide et rationalisé des Mac qu'une entreprise a achetés auprès d'Apple ou d'un Revendeur Agréé Apple participant.

Les organisations peuvent inscrire automatiquement les ordinateurs à la solution MDM sans avoir à intervenir physiquement ou à préparer les ordinateurs avant que les utilisateurs n'en prennent possession. Une fois l'inscription effectuée, les administrateurs doivent se connecter au site web du programme pour y associer leur solution MDM. La solution MDM attribue alors automatiquement les ordinateurs de l'entreprise. Une fois qu'un Mac a été inscrit, toutes les configurations, restrictions ou commandes spécifiées via une solution MDM sont automatiquement installées. Toutes les données en transit entre les ordinateurs et les serveurs Apple sont chiffrées avec le protocole HTTPS (SSL).

Il est possible de simplifier davantage le processus d'installation en passant certaines étapes de l'Assistant réglages, pour que les utilisateurs soient plus rapidement opérationnels. Les administrateurs peuvent également donner aux utilisateurs la possibilité ou non de supprimer le profil MDM de l'ordinateur, et vérifier que les restrictions de l'appareil sont bien mises en œuvre dès le début. Une fois l'ordinateur sorti de l'emballage et activé, il s'inscrit à la solution MDM de l'organisation, et l'ensemble des réglages de gestion, les apps et les livres sont installés. Remarque : l'inscription des appareils n'est pas disponible dans tous les pays et toutes les zones géographiques.

Pour plus d'informations sur les offres destinées aux entreprises, consultez l'Aide Programmes de déploiement Apple : help.apple.com/deployment/business. Pour plus d'informations sur les offres destinées au secteur de l'éducation, consultez l'Aide Apple School Manager : help.apple.com/schoolmanager.

Restrictions

Les administrateurs activent ou, dans certains cas, désactivent les restrictions pour empêcher les utilisateurs d'accéder à des apps, des services ou des fonctions spécifiques de l'appareil. Les restrictions sont envoyées aux appareils par le biais d'une entité Restrictions comprise dans un profil de configuration. Les restrictions peuvent être appliquées à des appareils macOS, iOS et tvOS.

La liste des restrictions actuellement disponibles pour les responsables informatiques est disponible ici : help.apple.com/deployment/mdm/#/mdm2pHf95672

Effacement et verrouillage à distance

Les Mac peuvent uniquement être effacés à distance par un administrateur ou un utilisateur. L'effacement à distance instantané n'est disponible que si FireVault est activé. Lorsque la MDM ou iCloud envoie une commande d'effacement à distance, l'ordinateur envoie une confirmation et procède à l'effacement. Lors d'un verrouillage à distance, la MDM requiert la saisie d'un code d'accès à six chiffres pour accéder au Mac. Sans ce code, aucun utilisateur ne peut accéder à l'appareil.

Confidentialité

Apple estime que la confidentialité est un droit fondamental de chacun. C'est la raison pour laquelle les produits Apple sont conçus de sorte à favoriser le traitement sur l'appareil, limiter la collecte et l'utilisation des données, donner aux utilisateurs un maximum de contrôle sur leurs informations et les gérer en toute transparence, et exploitent une structure hautement sécurisée.

Apple propose un grand nombre de commandes et d'options permettant aux utilisateurs macOS de choisir quand et comment les apps peuvent utiliser leurs informations, et de connaître les informations auxquelles elles ont accès. Pour plus d'informations, consultez www.apple.com/fr/privacy.