Aide du client Symantec™ Endpoint Protection pour Mac - French - France

December 2020

Comment Symantec Endpoint Protection protège votre Mac

Symantec Endpoint Protection combine plusieurs couches de protection pour sécuriser votre ordinateur contre les attaques de virus et de spyware ainsi que les tentatives d'intrusion.

Le type de protection décrit chaque couche de protection.

Table 1: Types de protection

Protection	Description
Protection contre les virus et les spywares	Symantec Endpoint Protection intègre des analyses antivirus planifiées, des analyses à la demande et Auto-Protect, qui s'exécute en arrière-plan pour surveiller les virus. Lorsqu'un virus est trouvé, Symantec Endpoint Protection l'élimine. Fonctionnement de la protection contre les virus et les spywares sur votre Mac
Protection contre les menaces réseau	Symantec Endpoint Protection intercepte des données à la couche réseau. Elle utilise des signatures pour analyser des paquets ou des flux de paquets. Elle analyse chaque paquet individuellement en recherchant les configurations qui correspondent aux attaques réseau ou aux attaques de navigateur. La protection contre les menaces réseau inclut ce qui suit : • Une fonction de prévention d'intrusion, qui détecte les attaques sur les composants du système d'exploitation et la couche d'application. Lorsque Symantec Endpoint Protection détecte une menace sur le réseau, cette menace est bloquée. • Un pare-feu, qui autorise ou bloque le trafic réseau en fonction des stratégies et des règles de pare-feu. (A partir de la version 14.2.) Fonctionnement de la protection contre les menaces réseau sur votre Mac
Contrôle des périphériques	Les administrateurs instance de Symantec Endpoint Protection Manager configurent une politique de contrôle des périphériques. Des périphériques peuvent être bloqués ou débloqués avec cette politique par nom de périphérique, fournisseur de périphérique, modèle de périphérique ou numéro de série. Sur un client géré, vous pouvez consulter les paramètres de Device Control dans l'onglet **Advanced** (Avancé). Device Control n'est pas disponible pour des clients non gérés. Contrôle des périphériques sur le client Symantec Endpoint Protection pour Mac
Détection et intervention de terminal client	Les administrateurs instance de Symantec Endpoint Protection Manager configurent une stratégie Activity Recorder (Enregistreur d'activité) qui fournit les moyens de détecter et d'exposer une activité réseau suspecte.

Le client télécharge automatiquement les définitions de virus, les définitions d'IPS et les mises à jour de produit sur votre ordinateur.

Mise à jour des définitions de virus, des définitions de prévention d'intrusion et du logiciel client

Fonctionnement de la protection contre les virus et les spywares sur votre Mac

Symantec Endpoint Protection utilise des définitions de virus pour détecter les virus connus pendant des analyses planifiées et des analyses manuelles. Auto-Protect utilise des définitions de virus pour analyser constamment l'activité d'ordinateur.

Symantec Endpoint Protection vous informe lorsqu'il détecte un virus ou un autre risque de sécurité. Un virus ou un autre risque de sécurité est détecté lorsqu'un des événements suivants survient :

- Auto-Protect trouve un virus pendant qu'il surveille votre ordinateur.
- Auto-Protect trouve un virus à partir d'une analyse que vous avez planifiée ou démarrée manuellement.

Avec les paramètres par défaut, Symantec Endpoint Protection tente automatiquement de réparer le virus qu'il a trouvé. S'il ne peut pas réparer le fichier, le client met sans risque le fichier en quarantaine de sorte qu'il ne puisse pas nuire à votre ordinateur. Généralement, le client réalise ces réparations sans aucune action de votre part. Lorsque votre ordinateur détecte un virus, vous pouvez choisir d'en informer Symantec.

Dans certaines circonstances, le client vous invite à choisir entre réparer, supprimer ou restaurer le fichier infecté qu'il a détecté. Vos réponses déterminent ce que le client fera avec le fichier infecté.

Réponse aux messages sur les infections et les détections de risques

Activation ou désactivation de l'envoi d'informations de sécurité à Symantec

Fonctionnement de la protection contre les menaces réseau sur votre Mac

La protection contre les menaces réseau inclut les technologies de protection suivantes :

- Prévention d'intrusion
- Pare-feu

Prévention d'intrusion

La prévention d'intrusion détecte et bloque automatiquement les attaques réseau. La prévention d'intrusion est une couche de défense interne qui protège les ordinateurs client. La prévention d'intrusion est parfois appelée le système de prévention d'intrusion (IPS).

La prévention d'intrusion intercepte des données à la couche réseau. Elle utilise des signatures pour analyser des paquets ou des flux de paquets. Elle analyse chaque paquet individuellement en recherchant les configurations qui correspondent aux attaques réseau ou aux attaques de navigateur. La prévention d'intrusion détecte les attaques sur les composants du système d'exploitation et la couche d'application.

La prévention d'intrusion utilise des signatures pour identifier des attaques sur les ordinateurs client. Pour les attaques connues, la prévention d'intrusion rejette automatiquement les paquets qui correspondent aux signatures.

Pare-feu

Le pare-feu surveille le trafic réseau et bloque tout trafic potentiellement dangereux pour protéger votre Mac. Le pare-feu Symantec Endpoint Protection n'est pas disponible sur les clients non gérés.

Le pare-feu Symantec Endpoint Protection surveille le trafic au niveau de la couche Transport et Internet. Le pare-feu intégré au client Mac surveille le trafic au niveau de la couche d'application supérieure, après avoir été surveillé par le pare-feu Symantec Endpoint Protection. Vous pouvez donc activer les deux pare-feu en même temps pour qu'ils s'exécutent en parallèle.

Le pare-feu utilise les types de règles suivants pour autoriser ou bloquer le trafic réseau :

- Règles par défaut
- Règles personnalisées
- Règles intégrées
- Règles de protection

Ces règles incluent la détection des analyses de port, détection des dénis de service, la protection contre l'usurpation d'adresse MAC, Smart DHCP et Smart DNS. Les paramètres du pare-feu sont entièrement contrôlés par l'administrateur instance de Symantec Endpoint Protection Manager. Vous pouvez activer ou désactiver le pare-feu uniquement si l'administrateur autorise le contrôle client pour l'utilisateur sur le client Mac.

La fonction de protection pare-feu a été ajoutée dans la version 14.2.

Gestion de la prévention d'intrusion

Gestion de la protection pare-feu pour le client Mac

Compatibilité du système d'exploitation avec Symantec Endpoint Protection pour Mac

Symantec Endpoint Protection pour Mac prend en charge les versions suivantes du système d'exploitation :

- macOS 12
- macOS 11 (processeur Intel et puce M1)
- macOS 10.15 à 10.15.7

Pour plus d'informations sur la prise en charge des versions antérieures du système d'exploitation Mac, reportez-vous à l'article Mac compatibility with the Endpoint Protection client (Compatibilité Mac avec le client Endpoint Protection).

Autorisation des extensions système pour Symantec Endpoint Protection pour macOS 10.15 ou version ultérieure

Notes de mise à jour, nouveaux correctifs et configuration système requise pour toutes les versions d'Endpoint Protection

Installation du client Symantec Endpoint Protection pour Mac

Vous pouvez directement installer un client Symantec Endpoint Protection sur un ordinateur Mac si vous ne pouvez pas ou ne voulez pas utiliser l'installation à distance en mode Push. Les étapes sont semblables, qu'il s'agisse d'un client autonome ou géré.

Vous ne pouvez installer un client géré que via un package créé par instance de Symantec Endpoint Protection Manager. Vous pouvez convertir un client autonome en client géré à tout moment en important les paramètres de communication client-serveur sur le client Mac.

NOTE

Pour préparer le client Symantec Endpoint Protection pour Mac en vue de son utilisation avec un logiciel tiers de déploiement à distance, voir :

Exporting and Deploying a Symantec Endpoint Protection client via Apple Remote Desktop or Casper (Exportation et déploiement d'un client Symantec Endpoint Protection via Apple Remote Desktop ou Casper)

Table 2: Méthodes d'installation du client pour Mac

Si vous avez téléchargé le fichier d'installation.	1. Extrayez le contenu dans un dossier sur un ordinateur Mac, puis ouvrez le dossier. 2. Ouvrez `SEP_MAC`. 3. Copiez le fichier `Symantec Endpoint Protection.dmg` sur le bureau de l'ordinateur Mac. 4. Cliquez deux fois sur `Symantec Endpoint Protection.dmg` pour monter le fichier en tant que disque virtuel. Installez ensuite le client Symantec Endpoint Protection pour Mac.
Si vous avez téléchargé un package d'installation client .zip à partir du portail Broadcom Support Portal. Pour plus d'informations, voir : Portail Broadcom Support Portal	1. Copiez le fichier sur le bureau de l'ordinateur Mac. Le fichier peut être nommé `Symantec Endpoint Protection.zip` ou `Symantec_Endpoint_Protection_version_Mac_Client.zip`, où version est la version du produit. 2. Cliquer avec le bouton droit sur **Ouvrir avec > Utilitaire d'archive** pour extraire le contenu du fichier. 3. Ouvrez le dossier résultant. Installez ensuite le client Symantec Endpoint Protection for Mac.

L'image ou le dossier de disque virtuel en résultant contient le programme d'installation de l'application et un dossier appelé Ressources supplémentaires. Les deux éléments doivent être situés dans le même emplacement pour une installation réussie. Si vous copiez le programme d'installation sur un autre emplacement, vous devez également copier Ressources supplémentaires.

Pour installer le client Symantec Endpoint Protection pour Mac :

1. Double-cliquez sur `Installer Symantec Endpoint Protection`.
2. Pour commencer l'installation, cliquez sur **Installer**.
3. Pour installer un outil d'aide nécessaire à l'installation du client Symantec Endpoint Protection, entrez le nom d'utilisateur et le mot de passe d'administration de votre Mac, puis cliquez sur **Installer un utilitaire**.
4. Une fois l'installation terminée, cliquez sur **Continuer** pour terminer la configuration de votre client Symantec Endpoint Protection.
5. Pour configurer votre client Symantec Endpoint Protection, procédez comme suit :

Autorisez l'extension système Symantec Endpoint Protection.	Dans la boîte de dialogue **Security & Privacy** (Sécurité et confidentialité), sous l'onglet **General** (Général), au niveau du message **System software from application "Symantec Endpoint Protection" was blocked from loading** (le logiciel système de l'application "Symantec Endpoint Protection" n'a pas pu être chargé), cliquez sur **Allow** (Autoriser). Si nécessaire, cliquez sur l'icône en forme de verrou pour effectuer les modifications. Vous devez autoriser l'extension système pour que Symantec Endpoint Protection soit entièrement fonctionnel. Voir : Autorisation des extensions système pour Symantec Endpoint Protection pour macOS 10.15 ou version ultérieure
Autorisez l'accès complet au disque.	Dans la boîte de dialogue **Security & Privacy** (Sécurité et confidentialité), dans l'onglet **Privacy** (confidentialité), assurez-vous que l'**Symantec System Extension** (Extension système Symantec) est autorisée à accéder aux données et aux paramètres d'administration de tous les utilisateurs de votre unité Mac. Si nécessaire, cliquez sur l'icône en forme de verrou pour effectuer les modifications.
Autorisez la modification du profil réseau.	Lorsque le message **Symantec Endpoint Protection would like to filter network content** (Symantec Endpoint Protection souhaite filtrer le contenu du réseau) s'affiche, cliquez sur **Allow** (Autoriser).

6. Cliquez sur **Complete** (Terminer).

Autorisation des extensions système pour Symantec Endpoint Protection pour macOS 10.15 ou version ultérieure

La demande d'autorisation des extensions système est une nouvelle fonction de sécurité de macOS 10.15.Vous devez autoriser l'extension système pour que Symantec Endpoint Protection soit entièrement fonctionnel.

Pour autoriser l'extension système pour Symantec Endpoint Protection, pendant la configuration de votre client Symantec Endpoint Protection, dans la boîte de dialogue **Security & Privacy** (Sécurité et confidentialité), sous l'onglet **General** (Général), au niveau du message **System software from application "Symantec Endpoint Protection" was blocked from loading** (le logiciel système de l'application "Symantec Endpoint Protection" n'a pas pu être chargé), cliquez sur **Allow** (Autoriser).

Pour plus d'informations, consultez l'article :

Installation du client Symantec Endpoint Protection pour Mac

Mise à niveau de l'invite pour le client Symantec Endpoint Protection pour Mac

Les administrateurs instance de Symantec Endpoint Protection Manager peuvent assigner un package d'installation client pour mettre à niveau automatiquement les ordinateurs clients gérés, avec des paramètres pour l'installation du client.

Si vous êtes connecté au Mac, une invite s'affichera pour vous demander de redémarrer afin de terminer l'installation. Selon les paramètres d'installation du client, vous pourrez peut-être retarder le redémarrage.

Si vous n'êtes pas connecté sur le Mac, l'installation le redémarre automatiquement.

Prise en main du client Symantec Endpoint Protection

Lorsque vous ouvrez le client Symantec Endpoint Protection, le message que **You are Protected** (Votre ordinateur est protégé) s'affiche en haut de la page, sauf en cas de présence d'un problème devant être résolu. Cliquez sur **Fix** (Résoudre) pour résoudre les problèmes.

Le client Symantec Endpoint Protection affiche les principales tâches que vous pouvez effectuer.

Table 3: Pages du client Symantec Endpoint Protection

Option	Description
Sécurité	Affiche l'état de protection de votre ordinateur.
Analyses	Vous permet d'analyser votre ordinateur. Vous pouvez choisir d'exécuter une analyse rapide ou une analyse complète. Vous pouvez également déposer un fichier ou un dossier à analyser. Exécution d'une analyse manuelle
LiveUpdate	Exécute LiveUpdate pour mettre à jour les définitions et les fichiers de produits pour Symantec Endpoint Protection. Mise à jour de contenu immédiate sur Symantec Endpoint Protection
Avancé	Donne plus d'options détaillées pour la protection antivirus et antispywares, la protection contre les menaces réseau et LiveUpdate.

Gestion de la protection de votre Mac avec Symantec Endpoint Protection

Les paramètres par défaut dans Symantec Endpoint Protection protègent votre Mac d'un grand nombre de malwares. Le client prend en charge automatiquement le malware ou vous permet de choisir comment prendre en charge le malware.

Selon les paramètres mis à disposition par votre administrateur, vous pouvez effectuer l'une des tâches suivantes pour participer au suivi de la protection de votre ordinateur.

NOTE
Il est possible que votre administrateur ne vous ait pas accordé la permission de contrôler ces tâches.

Table 4: Protection de votre ordinateur

Etapes	Description
Etape 1 : vérifiez que la protection contre les virus et les spywares et que la protection contre les menaces réseau sont activées.	La page **Security** (Sécurité) apparaît et indique une coche verte et le message **You are Protected** (Votre ordinateur est protégé), si vos protections sont activées. Activation et désactivation de la protection contre les virus et les spywares Activation ou désactivation de la protection contre les menaces réseau
Etape 2 : assurez-vous que le logiciel et les définitions sont à jour.	La page **Security** (Sécurité) affiche la date à laquelle les définitions ont été mises à jour pour la dernière fois pour la protection contre les virus et les spywares et pour la protection contre les menaces réseau. Sous **LiveUpdate**, l'heure de la dernière mise à jour de produit apparaît. Pour afficher le numéro de version du logiciel, cliquez sur **Aide > Info**.
Etape 3 : mettez à jour le logiciel ou les définitions si nécessaire.	Dans le client Symantec Endpoint Protection, cliquez sur **LiveUpdate** pour mettre à jour imédiatement le logiciel et les définitions. Mise à jour des définitions de virus, des définitions de prévention d'intrusion et du logiciel client
Etape 4 : exécutez une analyse.	Vous pouvez planifier des analyses pour qu'elles s'exécutent à intervalles réguliers, ou vous pouvez exécuter une analyse immédiate. Configuration des analyses planifiées Exécution d'une analyse manuelle

Gestion de vos paramètres de protection contre les virus et les spywares

Renouvellement de la licence de votre produit

Un message vous indiquant que la licence de Symantec Endpoint Protection a expiré peut s'afficher sous l'icône du client Symantec Endpoint Protection dans la barre de menu. Le client Symantec Endpoint Protection utilise une licence pour mettre à jour les éléments suivants :

- Logiciel client
- Fichiers de définition de protection pour les analyses antivirus et antispyware et pour la prévention d'intrusion

Le client peut utiliser une licence d'évaluation ou une licence payante. Si l'une ou l'autre des licences a expiré, le client ne met à jour ni les définitions ni le logiciel client.

Pour tout type de licence, vous devez contacter votre administrateur afin de mettre à jour ou renouveler la licence.

Réponse aux messages sur les infections et les détections de risques

Activation ou désactivation de Device Control sur le client Symantec Endpoint Protection pour Mac

Les administrateurs instance de Symantec Endpoint Protection Manager peuvent configurer des clients gérés avec une politique Device Control. Des périphériques peuvent être bloqués ou débloqués avec cette politique par nom de périphérique, fournisseur de périphérique, modèle de périphérique ou numéro de série.

Vous pouvez afficher les activités de Device Control dans la page **Advanced** (Avancé) en cliquant sur **Activity > Security History** (Activité > Historique de sécurité).

Les paramètres du client Symantec Endpoint Protection pour **Device Control** vous permettent d'activer ou désactiver Device Control. Si Device Control est activé, vous pouvez également activer ou désactiver des notifications quand des périphériques sont bloqués ou débloqués.

Pour modifier les paramètres, vous devez vous authentifier avec les informations d'authentification de l'administrateur Mac. Si ces paramètres sont grisés, alors l'administrateur les a verrouillés pour vous empêcher d'activer ou de désactiver cette fonction.

Vous ne pouvez pas ajouter ou modifier de périphériques à bloquer ou débloquer par le biais de l'interface client Symantec Endpoint Protection.

NOTE
La politique Device Control de instance de Symantec Endpoint Protection Manager contrôle les paramètres de contrôle des périphériques. A la prochaine pulsation, toutes les modifications que vous apportez à ces paramètres retournent à ce que la politique dicte.

Device Control n'est pas disponible pour des clients non gérés.

A propos de Protection Web et de l'accès au cloud pour le client Mac

Protection Web et de l'accès au cloud automatise la redirection du trafic Web vers Symantec Web Security Service et sécurise le trafic Web sur chaque ordinateur qui utilise Symantec Endpoint Protection.

L'administrateur contrôle les paramètres utilisés par Protection Web et de l'accès au cloud, notamment l'URL de configuration de proxy et le certificat racine Symantec Web Security Service facultatif. Seul l'administrateur instance de Symantec Endpoint Protection Manager peut configurer ces paramètres, qui n'apparaissent pas dans l'interface utilisateur du client Symantec Endpoint Protection. Vous pouvez afficher l'URL du fichier de configuration de proxy sur le Mac sous **Préférences Système > Réseau**, puis **Proxys**. Le certificat Cloud Services s'affiche dans **Keychain Access**.

Les navigateurs Web Safari, Chrome et Firefox versions 65 et ultérieures prennent en charge Protection Web et de l'accès au cloud. Les versions Symantec Endpoint Protection antérieures à la version 14.2 RU1 prennent uniquement en charge Safari et Chrome.

NOTE
La méthode de tunnel ne s'exécute pas sur les clients Mac.

Désinstallation du client Symantec Endpoint Protection pour Mac

Désinstallez le client Symantec Endpoint Protection pour Mac via l'icône client sur la barre de menu. La désinstallation du client Symantec Endpoint Protection pour Mac requiert les informations d'authentification de l'utilisateur administrateur.

NOTE
Après la désinstallation du client Symantec Endpoint Protection, vous êtes invité à redémarrer l'ordinateur client pour terminer la désinstallation. Assurez-vous d'enregistrer tout travail en cours ou de fermer les applications ouvertes avant de commencer.

Pour désinstaller le client Symantec Endpoint Protection pour Mac

1. Sur l'ordinateur client Mac, ouvrez le client Symantec Endpoint Protection, puis cliquez sur **Symantec Endpoint Protection > Désinstaller Symantec Endpoint Protection**.
2. Cliquez à nouveau sur **Désinstaller** pour commencer la désinstallation.
3. Pour installer un outil d'aide nécessaire à la désinstallation du client Symantec Endpoint Protection, entrez le nom d'utilisateur et le mot de passe d'administration de votre Mac, puis cliquez sur **Installer un utilitaire**.
4. Dans la boîte de dialogue **Symantec Endpoint Protection tente de modifier une extension système**, entrez le nom d'utilisateur et le mot de passe d'administration de votre Mac, puis cliquez sur **OK**.

   Il se peut également que vous soyez invité à saisir un mot de passe pour désinstaller le client. Ce mot de passe peut être différent du mot de passe administrateur de votre Mac.
5. Une fois la désinstallation terminée, cliquez sur **Redémarrer**.

Si la désinstallation échoue, vous devrez utiliser une autre méthode. Voir :

Désinstallation de Symantec Endpoint Protection

Mise à jour des définitions de virus, des définitions de prévention d'intrusion et du logiciel client

Les produits Symantec nécessitent des informations à jour pour protéger l'ordinateur des nouvelles menaces découvertes. Symantec intègre ces informations à Symantec Endpoint Protection par l'intermédiaire de LiveUpdate. LiveUpdate récupère les mises à jour de produits et de définition pour votre ordinateur en utilisant votre connexion Internet.

Les mises à jour de définition sont les fichiers qui maintiennent les produits Symantec à jour avec la dernière technologie de protection contre les menaces. LiveUpdate récupère les nouveaux fichiers de définition de virus ou de signatures de la prévention d'intrusion sur un site Internet de Symantec, puis remplace les anciens fichiers de définitions.

Les mises à jour de produit sont des améliorations sur le client installé. Les mises à jour de produit sont généralement créées pour étendre la compatibilité du système d'exploitation ou du matériel, pour corriger les problèmes de performances ou pour corriger des erreurs de produit. Les mises à jour de produit sont publiées en fonction des besoins. Le client reçoit des mises à jour de produit directement d'un serveur LiveUpdate. Les mises à jour de produits et de définitions sont appelées des mises à jour de contenu.

Table 5: Manières d'effectuer des mises à jour de contenu sur votre ordinateur

Tâche	Description
Mise à jour immédiate de contenu	Vous pouvez exécuter LiveUpdate immédiatement. Mise à jour de contenu immédiate sur Symantec Endpoint Protection
Mise à jour de contenu sur planification	Par défaut, LiveUpdate s'exécute automatiquement à intervalles planifiés. Mise à jour de contenu planifiée sur Symantec Endpoint Protection

Gestion de la protection de votre Mac avec Symantec Endpoint Protection

Mise à jour de contenu immédiate sur Symantec Endpoint Protection

Vous pouvez mettre à jour les fichiers de définition et de produit immédiatement à l'aide de LiveUpdate. Vous devez exécuter LiveUpdate manuellement pour les raisons suivantes :

- Le logiciel client a été installé récemment.
- La dernière analyse a été exécutée il y a longtemps.
- Vous suspectez la présence d'un virus ou d'un autre problème de malware.

Pour mettre immédiatemment à jour le contenu de Symantec Endpoint Protection :

Lancez LiveUpdate de l'une des manières suivantes :

- Cliquez avec le bouton droit de la souris sur l'icône Symantec Endpoint Protection dans la barre de menus, puis cliquez sur **LiveUpdate**.
- Ouvrez le client Symantec Endpoint Protection, puis cliquez sur **LiveUpdate**.

LiveUpdate se connecte au serveur LiveUpdate configuré, recherche les mises à jour disponibles, puis les télécharge et les installe automatiquement. Une barre d'état indique la progression du téléchargement.

Mise à jour de contenu planifiée sur Symantec Endpoint Protection

Mise à jour des définitions de virus, des définitions de prévention d'intrusion et du logiciel client

Mise à jour de contenu planifiée sur Symantec Endpoint Protection

Planifications sur les clients Mac gérés

Par défaut, les clients Mac gérés reçoivent une planification de instance de Symantec Endpoint Protection Manager qui exécute LiveUpdate toutes les quatre heures. L'administrateur instance de Symantec Endpoint Protection Manager contrôle la planification. Les clients gérés ne peuvent pas supprimer, modifier ou afficher la planification créée par l'administrateur ou créer une nouvelle planification.

Planifications sur les clients Mac non gérés

Vous pouvez créer une planification de sorte que LiveUpdate s'exécute automatiquement à intervalles planifiés. Il peut être nécessaire de planifier l'exécution de LiveUpdate lorsque vous n'utilisez pas votre ordinateur.

Pour planifier la mise à jour du contenu de Symantec Endpoint Protection :

1. Dans le client Symantec Endpoint Protection, sur la page **Avancé**, cliquez sur **Protéger mon Mac**, puis sur l'icône de paramètres **Analyse LiveUpdate planifiée**.

   Votre planification actuelle apparaît.

2. Sélectionnez un intervalle depuis le menu déroulant Planification LiveUpdate.

   L'actualisation a lieu toutes les **4** heures. Vous pouvez également choisir une exécution **quotidienne** ou **hebdomadaire**, en choisissant une heure ou une date et une heure.

3. Cliquez sur **Appliquer les modifications**.

Mise à jour de contenu immédiate sur Symantec Endpoint Protection

Mise à jour des définitions de virus, des définitions de prévention d'intrusion et du logiciel client

A propos de la connexion au serveur de gestion via un serveur proxy

Il peut vous être demandé d'autoriser Symantec Endpoint Protection à utiliser vos paramètres d'identification pour se connecter au serveur de gestion via un serveur proxy. Vous recevez un message vous demandant si vous autorisez le processus `symdaemon` à accéder à vos informations d'identification.

Vous devez cliquer sur **Toujours autoriser** dans le message. Si vous ne le faites pas, vous recevez le même message chaque fois que le client communique avec le serveur LiveUpdate. Si vous cliquez sur **Refuser**, votre client ne pourra pas recevoir les mises à jour du logiciel ou des définitions.

Mise à jour des définitions de virus, des définitions de prévention d'intrusion et du logiciel client

Gestion de vos paramètres de protection contre les virus et les spywares

Par défaut, Symantec Endpoint Protection protège votre ordinateur contre les virus et les risques de sécurité, y compris les menaces réseau, dès que vous le lancez. La protection antivirus et antispywares intègre Auto-Protect, qui recherche les virus dans les programmes actifs. Il surveille également l'ordinateur pour toute activité pouvant indiquer la présence d'un virus ou d'un risque de sécurité. L'interception d'Auto-Protect empêche les virus d'infecter votre ordinateur et vous devez garder Auto-Protect activé.

Pour des clients gérés, l'ampleur du contrôle que vous avez sur ces paramètres dépend de la façon dont l'administrateur a configuré le client. En outre, toutes les modifications que vous apportez à ces paramètres peuvent revenir à ce que la politique dicte à la prochaine pulsation.

La section Gestion de la protection contre les virus et les spywares décrit les tâches que vous accomplissez pour gérer la protection antivirus et antispywares sur votre Mac.

Table 6: Gestion de la protection contre les virus et les spywares

Etapes	Description
Etape 1 : activer ou désactiver la protection contre les virus et les spywares	Vous pouvez facilement activer et désactiver la protection contre les virus et les spywares. Symantec recommande de laisser cette protection activée par défaut. Activation et désactivation de la protection contre les virus et les spywares
Etape 2 : personnaliser les paramètres Auto-Protect	Auto-Protect est une partie importante de la protection antivirus et antispywares. Vous pouvez configurer ces options depuis la page **Advanced** (Avancé). Configuration des paramètres Auto-Protect et des paramètres de zone d'analyse
Etape 3 : rechercher les virus sur votre ordinateur	Vous pouvez configurer des analyses antivirus planifiées ou immédiates. Configuration des analyses planifiées Suspension, mise en sommeil et arrêt des analyses Exécution d'une analyse manuelle
Etape 4 : répondre quand Symantec Endpoint Protection détecte un virus	Lorsque Symantec Endpoint Protection analyse votre ordinateur, il peut : • Vous avertir des actions que vous pouvez effectuer. • Vous informer des actions de protection qu'il a exécutées pour vous. Réponse aux messages sur les infections et les détections de risques

Activation et désactivation de la protection contre les virus et les spywares

Par défaut, la protection antivirus et antispywares est activée, en même temps qu'Auto-Protect.

Vous pouvez mieux contrôler Auto-Protect en définissant des options spécifiques.

Si la protection contre les virus et les spywares est désactivée, un « x » rouge apparaît sur la page **Status** (Statut) avec le message **Virus and Spyware Protection is disabled** (La protection contre les virus et les spywares et désactivée). Si la protection a été désactivée, réactivez-la rapidement.

NOTE
Les analyses planifiées se poursuivent, que la protection contre les virus et les spywares soit activée ou non. Votre administrateur peut limiter l'accès à certaines fonctionnalités de Symantec Endpoint Protection. Vous pouvez ne pas être autorisé à désactiver ces paramètres, planifier des analyses ou personnaliser les options

de protection.La saisie de votre mot de passe administrateur Mac peut être nécessaire pour modifier des paramètres.

Pour activer et désactiver la protection contre les virus et les spywares

1. Pour activer la protection antivirus et antispywares, dans le client Symantec Endpoint Protection, sur la page **Advanced** (Avancé), cliquez sur **Protect My Mac** (Protéger mon Mac), puis sur activez l'option **Automatic Scans** (Analyses automatiques).
2. Pour désactiver la protection antivirus et antispywares, dans le client Symantec Endpoint Protection, sur la page **Advanced** (Avancé), cliquez sur **Protect My Mac** (Protéger mon Mac), puis sur désactivez l'option **Automatic Scans** (Analyses automatiques).

Configuration des paramètres Auto-Protect et des paramètres de zone d'analyse

Gestion de vos paramètres de protection contre les virus et les spywares

Réponse aux messages sur les infections et les détections de risques

Configuration des paramètres Auto-Protect et des paramètres de zone d'analyse.

Sur les clients gérés, si votre administrateur vous le permet, vous pouvez personnaliser la manière dont Auto-Protect recherche les virus et répare les fichiers infectés.

Les paramètres Auto-Protect apparaissent en tant qu'options sous **Protect My Mac** (Protéger mon Mac). Vous devez activer l'option **Automatic Scans** (Analyses automatiques) pour activer Auto-Protect.

La zone **Scan Zone Settings** (Paramètres de zone d'analyse) permet d'indiquer les fichiers à prendre en compte dans une analyse ou à exclure d'une analyse.

Pour configurer les paramètres Auto-Protect :

1. Dans le client Symantec Endpoint Protection, sur la page **Advanced** (Avancé), cliquez sur **Protect My Mac** (Protéger mon Mac), puis sur l'icône de paramètres **Automatic Scans** (Analyses automatiques).
2. Vous pouvez modifier les options suivantes :

Mise en quarantaine automatique	Vous pouvez choisir d'envoyer tous les fichiers ne pouvant pas être réparés en quarantaine.
Réparation automatique	Auto-Protect peut réparer automatiquement tous les fichiers infectés détectés.
Analyser	Vous pouvez choisir **Data Disks** (Disques de données) et **All other disks** (Tous les autres disques).
Analyser les fichiers compressés	Pour choisir d'inclure les fichiers compressés dans une analyse Auto-Protect. L'analyse comprend le fichier compressé et les fichiers qu'il contient.

WARNING
Si vous ne sélectionnez pas l'option **Auto Repair** (Réparation automatique), aucun fichier infecté n'est mis en quarantaine, même si vous sélectionnez l'option **Auto Quarantine** (Quarantaine automatique).Le logiciel vous demande si vous souhaitez réparer un fichier infecté. Si vous ne réparez pas le fichier, il reste dans l'ordinateur. Si vous sélectionnez l'option **Réparation automatique** et que vous ne sélectionnez pas l'option **Quarantaine automatique**, tous les fichiers infectés sont supprimés.

3. Cliquez sur **Done** (Terminé).

Pour configurer les paramètres de zone d'analyse :

1. Dans le client Symantec Endpoint Protection, sur la page **Advanced** (Avancé), cliquez sur **Protect My Mac** (Protéger mon Mac), puis sur l'icône de paramètres **Scan Zone Settings** (Paramètres de la zone d'analyse).
2. Vous pouvez modifier les options suivantes :

Analyse générale	Tous les fichiers et processus de votre ordinateur sont analysés lorsque vous y accédez.
Analyser uniquement	Seuls les fichiers ou dossiers que vous indiquez sont pris en compte dans l'analyse.
Ne pas analyser	Tous les fichiers sont analysés, à l'exception des fichiers ou dossiers que vous excluez expressément de l'analyse.
Utiliser défaut	Ce choix analyse tous les emplacements.

3. Cliquez sur **OK**.

Fonctionnement de la protection contre les virus et les spywares sur votre Mac

Activation et désactivation de la protection contre les virus et les spywares

Gestion des fichiers mis en quarantaine

Configuration des analyses planifiées

Symantec Endpoint Protection exécute automatiquement une analyse par défaut si vous avez un client géré. Si votre administrateur vous y autorise, vous pouvez configurer des analyses planifiées supplémentaires.

Sur un client non géré, vous devez effectuer vos propres analyses.Symantec vous recommande d'effectuer une analyse manuelle complète dès que possible, puis de configurer une analyse planifiée régulière. Vous pouvez mettre toutes les analyses sur pause ou les retarder, y compris les analyses planifiées et les analyses manuelles.

Sur un client géré, les analyses par défaut s'exécutent tous les jours à 20h00, et Auto Repair est désactivé.

> **NOTE**
> Symantec recommande de ne pas exécuter d'analyse planifiée plus d'une fois par jour. En effet, l'augmentation de la fréquence des analyses ou la configuration de plusieurs analyses planifiées peuvent entraîner des problèmes de performances.

Exécution d'une analyse manuelle

Pour configurer les analyses planifiées :

1. Dans le client Symantec Endpoint Protection, sur la page **Advanced** (Avancé), cliquez **sur Protect My Mac** (Protéger mon Mac), puis sur l'icône de paramètres **Scheduled Scans** (Analyses planifiées).
2. Dans la boîte de dialogue, cliquez sur **Add scheduled scans** (Ajouter des analyses planifiées) ou sur une analyse planifiée en cours puis sur **Edit** (Modifier) pour régler les paramètres correspondants.
3. L'onglet **Scan Items** (Eléments à analyser) permet de définir les options suivantes :

Lecteurs	Vous pouvez choisir d'analyser ou non les disques durs (**Hard drives**)et les lecteurs amovibles (**Removable drives**).
Dossiers	Vous pouvez choisir d'analyser vos fichiers **Dossier d'origine (Utilisateur actif)**, **Applications** et **Bibliothèque**. Si aucun utilisateur n'est connecté au moment de l'analyse planifiée d'un dossier de base, l'analyse ne s'exécute pas.

Options d'analyse	Sélectionnez parmi les options suivantes : • **Analyse des fichiers compressés** • **Réparation automatique** • **Mise en quarantaine automatique** • **Activer l'analyse en période d'inactivité**

4. L'onglet **Planification d'analyse** permet de définir les options suivantes :

Planification d'analyse	Vous pouvez configurer l'exécution d'une analyse à un intervalle spécifique en heures, de façon quotidienne, hebdomadaire ou mensuelle. L'option **Run at a specific interval** (Exécuter à un intervalle spécifique) est sélectionnée par défaut lorsque vous planifiez une nouvelle analyse.
Exécuter chaque	Disponible quand l'option **Run at specific interval** (Exécuter à un intervalle spécifique) est sélectionné pour **Scan Schedule** (Planification d'analyse).
Heure de démarrage	Disponible quand vous sélectionnez **Daily** (Quotidienne), **Weekly** (Hebdomadaire) ou **Monthly** (Mensuelle) pour la planification de l'analyse. Vous pouvez sélectionner l'heure à laquelle l'analyse démarre. Nous vous conseillons de choisir une heure à laquelle vous n'êtes pas normalement au bureau, car les analyses peuvent ralentir les performances de votre ordinateur.
Activé	Disponible quand vous sélectionnez **Weekly** (Hebdomadaire) ou **Monthly** (Mensuelle) pour la planification de l'analyse. Vous pouvez sélectionner le jour de la semaine ou du mois à laquelle l'analyse démarre. Nous vous conseillons de choisir une heure à laquelle vous n'êtes pas normalement au bureau, car les analyses peuvent ralentir les performances de votre ordinateur.

5. Dans l'onglet **Tuning** (Réglage), vous pouvez ajuster le mode d'optimisation des performances de l'analyse.
6. Cliquez sur **OK**.
7. Cliquez sur **Done** (Terminé).

Suspension, mise en sommeil et arrêt des analyses

Gestion de la protection de votre Mac avec Symantec Endpoint Protection

Réponse aux messages sur les infections et les détections de risques

Activation ou désactivation de l'envoi d'informations de sécurité à Symantec

Exécution d'une analyse manuelle

Vous pouvez être amené à analyser des fichiers manuellement. Vous pouvez par exemple avoir besoin d'analyser les fichiers qui ont été enregistrés sur votre ordinateur avant l'installation de Symantec Endpoint Protection. Ou vous pouvez décider que certains fichiers exclus d'une analyse planifiée nécessitent une analyse.

> **NOTE**
> Vous pouvez mettre toutes les analyses sur pause ou les retarder, y compris les analyses planifiées et les analyses manuelles.

Pour exécuter une analyse manuelle :

Dans le client Symantec Endpoint Protection, sur la page **Scans** (Analyses), effectuez l'une des opérations suivantes :

- Pour lancer une analyse rapide, cliquez sur **Quick Scan** (Analyse rapide), puis sur **Start a Quick Scan** (Lancer une analyse rapide).
- Pour lancer une analyse complète, cliquez sur **Full Scan** (Analyse complète), puis sur **Start a Full Scan** (Lancer une analyse complète).
- Pour analyser un fichier ou un dossier, cliquez sur **File Scan** (Analyse de fichier), puis sur **Select a file** (Sélectionner un fichier).Le Finder s'ouvre et vous pouvez choisir d'afficher les fichiers masqués (**Show Hidden Files**) et

d'analyser les fichiers compressés (**Scan Compressed Files**). Vous pouvez également choisir d'activer la réparation automatique (**Auto Repair**) et la quarantaine automatique (**Auto Quarantine**).

Suspension, mise en sommeil et arrêt des analyses

Configuration des analyses planifiées

Activation ou désactivation de l'envoi d'informations de sécurité à Symantec

Suspension, mise en sommeil et arrêt des analyses

La fonctionnalité de suspension vous permet d'arrêter une analyse et de la reprendre à un autre moment choisi. Vous pouvez également arrêter et annuler une analyse à tout instant. Les droits administrateur ne sont pas nécessaires pour utiliser ces fonctionnalités.

Quand une analyse reprend, elle démarre à l'endroit où elle s'est arrêtée.

> **NOTE**
> Si vous tentez de suspendre une analyse pendant que le client analyse un fichier compressé, le client peut mettre plusieurs minutes à réagir à la demande de suspension de l'analyse.

Si le report est activé, vous pouvez également reporter une analyse, mais seulement avant que l'analyse commence. Vous ne pouvez pas reporter une analyse en cours.

Pour suspendre ou arrêter une analyse planifiée en cours :

1. Dans la boîte de dialogue de progression de l'analyse, cliquez sur **Pause** (Suspendre).
2. Dans la boîte de dialogue de progression de l'analyse, cliquez sur **Resume** (Reprendre) pour poursuivre l'analyse ou cliquez sur **Stop** (Arrêter) pour arrêter l'analyse. Vous pouvez également cliquer sur **Done** (Terminé) pour fermer la fenêtre.

Pour suspendre ou arrêter une analyse manuelle :

1. Dans la boîte de dialogue de progression de l'analyse, cliquez sur **Pause** (Suspendre) pour suspendre l'analyse.
2. Cliquez sur **Cancel** (Annuler) pour arrêter une analyse manuelle ou cliquez sur **Resume** (Reprendre) pour poursuivre l'analyse.

Pour mettre en sommeil une analyse qui est sur le point de démarrer :

1. Dans la fenêtre qui apparaît, cliquez sur le menu déroulant pour sélectionner une valeur de mise en sommeil. Vous pouvez définir le report sur 15 minutes minimum ou sur une journée maximum.
2. Cliquez sur **OK** pour mettre en sommeil l'analyse.

   Vous n'avez rien à faire, l'analyse s'exécutera comme prévu.

Configuration des analyses planifiées

Exécution d'une analyse manuelle

Réponse aux messages sur les infections et les détections de risques

Vous pouvez vérifier si votre ordinateur est infecté et effectuer quelques tâches supplémentaires pour renforcer la sécurité et obtenir de meilleures performances.

Votre administrateur peut gérer votre client ou vous pouvez exécuter un client non géré. Les tâches de protection que vous pouvez effectuer dépendent du niveau de contrôle que votre administrateur exerce sur le client.

Si Symantec Endpoint Protection détecte un virus ou un risque de sécurité, vous pouvez être invité à réagir au risque. Selon les réglages effectués par votre administrateur, vous pouvez être informé de l'action automatiquement entreprise par le client.

Table 7: Réponse aux message sur les infections

Contenu du message	Action requise
Le fichier infecté a été réparé	Aucun(e)
Vous demande d'autoriser la réparation du fichier infecté.	Autorisez la réparation. Cette option varie en fonction de vos préférences Auto-Protect. Gestion de vos paramètres de protection contre les virus et les spywares Si l'option activant la réparation automatique des fichiers infectés n'est pas cochée, vous devez réparer le fichier manuellement. Réparation des fichiers infectés
Impossible de réparer le fichier infecté	Gérez l'infection dans la quarantaine. Gestion des fichiers mis en quarantaine

Fonctionnement de la protection contre les virus et les spywares sur votre Mac

Réparation des fichiers infectés

Si un fichier infecté n'est pas automatiquement réparé ou placé en quarantaine, vous pouvez le réparer à partir de la liste des résultats de l'analyse. Vous pouvez réparer manuellement des fichiers se trouvant sur le disque dur de votre ordinateur ou sur des supports amovibles.

Pour réparer des fichiers infectés :

1. Dans la liste des résultats d'analyse, sélectionnez le fichier à réparer, puis cliquez sur **Réparer**.

   Vous pouvez également cliquer sur le bouton droit de la souris depuis le Mac **Finder** ou depuis le menu **Rechercher**.
2. Répétez ces opérations aussi souvent que nécessaire.
3. Effectuez une autre analyse pour repérer d'autres fichiers éventuellement infectés.
4. Vérifiez les fichiers réparés pour vous assurer qu'ils fonctionnent correctement.

Gestion de vos paramètres de protection contre les virus et les spywares

Gestion des fichiers mis en quarantaine

Gestion des fichiers mis en quarantaine

Par défaut, si le client détecte un virus dans un fichier, il tente de supprimer le virus. S'il ne parvient pas à supprimer le virus, le fichier est placé en quarantaine sur votre ordinateur. Si Symantec Endpoint Protection détecte un risque de sécurité dans un fichier, il commence par placer le fichier en quarantaine. Il répare ensuite les éventuels effets secondaires du risque.

Quand vous mettez à jour vos définitions de virus, le client contrôle automatiquement la quarantaine. Vous pouvez réanalyser les éléments en quarantaine. Les dernières définitions peuvent peut-être permettre de nettoyer ou de réparer les fichiers mis en quarantaine.

Pour gérer les fichiers mis en quarantaine :

1. Dans le client Symantec Endpoint Protection, sur la page **Advanced** (Avancé), cliquez sur **Activity > Security History > Quarantine** (Activité > Historique de sécurité > Quarantaine).
2. Sélectionnez le fichier à gérer, puis sélectionnez l'option appropriée :

Réparer	Sélectionnez cette option pour tenter de réparer un fichier mis en quarantaine. Assurez-vous que vos définitions de virus sont plus récentes que la date de mise en quarantaine du fichier.
Supprimer	Sélectionnez cette option pour supprimer de la quarantaine les fichiers dont vous n'avez plus besoin.
Restaurer	Si vous êtes sûr que le fichier ne contient pas de virus, vous pouvez le restaurer à son emplacement d'origine sur votre ordinateur. Cette option n'analyse pas le fichier, ni ne tente de le réparer.

Réponse aux messages sur les infections et les détections de risques

Activation ou désactivation de l'envoi d'informations de sécurité à Symantec

Symantec Endpoint Protection peut envoyer à Symantec des informations pseudonymes sur les menaces détectées. Symantec utilise ces informations pour protéger vos ordinateurs client des nouvelles menaces ciblées et en mutation. Toutes les données que vous soumettez améliorent la capacité de Symantec à réagir face aux menaces et à personnaliser la protection de votre ordinateur.

Les données que collecte la télémétrie de Symantec peuvent inclure des éléments pseudonymes qui ne sont pas directement identifiables. Symantec n'a pas besoin d'utiliser les données de télémétrie pour identifier des utilisateurs individuels et ne cherche d'ailleurs pas à le faire.

Par défaut, votre ordinateur client envoie les informations relatives aux détections à Symantec. Vous pouvez désactiver les envois, bien que Symantec vous recommande de laisser ce paramètre activé.

Cette option envoie uniquement des informations sur les détections de virus.

NOTE
Symantec recommande de laisser cette option activée.

Pour activer ou désactiver l'envoi d'informations de sécurité pseudonymes à Symantec :

Dans le client Symantec Endpoint Protection, sur la page **Advanced** (Avancé), cliquez sur **Product Settings** (Paramètres du produit), puis activez ou désactivez l'option **Security Info Submission** (Soumission des informations de sécurité).

Configuration des analyses planifiées

Exécution d'une analyse manuelle

Gestion de la prévention d'intrusion

Les paramètres par défaut de la prévention d'intrusion protègent votre client Mac. Cependant, si vous souhaitez gérer votre propre protection, vous pouvez gérer la prévention d'intrusion comme partie intégrante de la protection contre les menaces réseau.

Table 8: Gestion de la prévention d'intrusion

Etapes	Description
Etape 1 : En savoir plus sur la prévention d'intrusion	Découvrez comment la prévention d'intrusion détecte et bloque les attaques réseau. Fonctionnement de la protection contre les menaces réseau sur votre Mac
Etape 2 : Télécharger les signatures IPS les plus récentes	Par défaut, les dernières signatures sont téléchargées sur le client. Cependant, vous pouvez télécharger les signatures immédiatement. Mise à jour de contenu immédiate sur Symantec Endpoint Protection
Etape 3 : Activer ou désactiver la prévention d'intrusion	Vous pouvez avoir besoin de désactiver la prévention d'intrusion à des fins de dépannage ou si les ordinateurs clients détectent un trop grand nombre de faux positifs. En règle générale, vous ne devez pas désactiver la prévention d'intrusion. Activation ou désactivation de la protection contre les menaces réseau
Etape 4 : Activer les notifications de la prévention d'intrusion	Vous pouvez configurer des notifications pour qu'elles apparaissent quand Symantec Endpoint Protection détecte une attaque. Activation ou désactivation des notifications de la protection contre les menaces réseau

Gestion de la protection pare-feu pour le client Mac

Le pare-feu Symantec Endpoint Protection pour Mac fournit une protection pare-feu qui s'intègre complètement à Symantec Endpoint Protection, qui inclut des événements, des politiques et des commandes. Le pare-feu Symantec Endpoint Protection est uniquement disponible sur les clients gérés.

NOTE
Le pare-feu Symantec Endpoint Protection pour Mac ne s'intègre pas au pare-feu intégré du système d'exploitation. Au lieu de cela, il s'exécute en parallèle. Le pare-feu du système d'exploitation examine la couche d'application, alors que le pare-feu Symantec Endpoint Protection examine les niveaux inférieurs (adresse IP et transport).Le pare-feu Symantec Endpoint Protection pour Mac n'offre pas de règles de blocage pair à pair, même si vous pouvez les créer en partie à l'aide des règles de pare-feu personnalisées.

Table 9: Gestion de la protection par pare-feu

Etapes	Description
Etape 1 : en savoir plus sur la protection pare-feu.	Découvrez comment la protection pare-feu surveille le trafic et protège contre les vecteurs d'attaque courants. Fonctionnement de la protection contre les menaces réseau sur votre Mac
Etape 2 : activation ou désactivation du pare-feu	Vous devrez peut-être désactiver le pare-feu pour résoudre des problèmes, par exemple, si le trafic que vous pensiez autorisé est bloqué. En règle générale, vous ne devez pas désactiver le pare-feu. Activation ou désactivation de la protection contre les menaces réseau

Activation ou désactivation de la protection contre les menaces réseau

En règle générale, lorsque vous désactivez les composants de la protection contre les menaces réseau sur votre ordinateur, celui-ci est moins sécurisé. Cependant, vous pouvez vouloir désactiver la prévention d'intrusion pour empêcher les faux positifs ou désactiver le pare-feu afin de résoudre les problèmes de trafic bloqué. La prévention d'intrusion et le pare-feu font partie de la protection contre les menaces réseau.

Pour des clients gérés, l'ampleur du contrôle que vous avez sur ces paramètres dépend de la façon dont l'administrateur a configuré le client. En outre, toutes les modifications que vous apportez à ces paramètres peuvent revenir à ce que la politique dicte à la prochaine pulsation.

Le pare-feu n'est pas disponible pour les clients non gérés.

Pour activer ou désactiver la protection contre les menaces réseau :

1. Dans le client Symantec Endpoint Protection, sur la page **Advanced** (Avancé), cliquez sur **Network Threat Protection** (Protection contre les menaces réseau).
2. Pour activer ou désactiver la prévention d'intrusion, sélectionnez ou désélectionnez l'option **Intrusion Prevention** (Prévention d'intrusion).
3. Pour activer ou désactiver le pare-feu, sélectionnez ou désélectionnez l'option **Firewall** (Pare-feu).
4. Pour activer ou désactiver les notifications pour la prévention d'intrusion et le pare-feu, cliquez sur l'icône de paramètres de **Vulnerability Protection** (Protection contre les vulnérabilités), puis dans la boîte de dialogue, sélectionnez ou désélectionnez l'option **Display Vulnerability Protection Notifications** (Afficher les notifications de protection contre les vulnérabilités).
5. Cliquez sur **Done** (Terminé).

Si vous désactivez ces composants, vous devez les activer à nouveau dès que possible pour vous assurer que votre ordinateur dispose de la meilleure protection.

Gestion de la prévention d'intrusion

Gestion de la protection pare-feu pour le client Mac


Symantec
A Division of Broadcom