SOPHOS

Cybersecurity made simple.

Sophos Endpoint pour Mac

Aide

Table des matières

1 Sophos Endpoint

Remarque
Il se peut que toutes les fonctions ne soient pas décrites dans ce manuel. Ceci dépend de votre licence.

Sophos Endpoint est configuré et administré de manière centralisée à partir de Sophos Central Admin.

Les tâches qui peuvent être effectuées sur le Mac sont les suivantes :

- Vérifier l'État (page 2) du Mac.
- Contrôler un fichier (page 8) ou Contrôler le Mac (page 8) à la recherche de menaces.
- Retrouvez plus de renseignements sur les Événements (page 3) du Mac tels que les menaces détectées.
- Nettoyage d'une menace (page 8).
- Modifier les paramètres de sécurité (page 8). Par exemple, vous pouvez désactiver des fonctions afin de résoudre des problèmes.
- Mettre à jour (page 9).
- Résoudre les problèmes (page 9).

Remarque
Vous devez utiliser la **Connexion administrateur** et saisir le mot de passe de la protection antialtération pour nettoyer les menaces ou modifier les paramètres.

2 État

Remarque
Il se peut que toutes les fonctions ne soient pas décrites dans cette section. Ceci dépend de votre licence.

La page **État** vous permet de :

- Voir l'état de sécurité de l'ordinateur.
- Contrôler la présence de menaces sur le Mac.
- Voir les fonctions installées et leur état de sécurité.

Remarque
Le lien **À propos** vous permet de mettre à jour vos définitions de virus ou de réparer le produit.

État de sécurité

Une icône dans la partie supérieure de la page affiche l'état.

 Verte. Il n'y a aucune alerte ou uniquement des alertes de faible priorité.

 Rouge. Il y a des alertes de priorité élevée.

 Jaune. Il y a des alertes de priorité moyenne.

 Gris. L'état est inconnu.

En dessous, toutes les fonctions installées sont affichées avec leur état de sécurité individuel.

Contrôler le Mac

Cliquez sur **Contrôler** pour contrôler la présence de menaces dans tous les fichiers du Mac.

Remarque
Si une menace est détectée, l'option **Contrôler** n'est pas disponible. Vous pouvez cliquer sur **Afficher les détails** pour obtenir plus d'informations sur la menace.

Lorsque le contrôle est terminé, vous êtes informé des résultats du contrôle. Si des menaces sont détectées, vous pouvez cliquer sur **Afficher les détails** ou sur **Événements** pour obtenir plus d'informations.

3 Événements

Remarque
Il se peut que toutes les fonctions ne soient pas décrites dans cette section. Ceci dépend de votre licence.

La page **Événements** affiche les événements sur le Mac comme, par exemple, les menaces détectées.

Vous pouvez filtrer les événements, par exemple, pour afficher uniquement ceux qui nécessitent une intervention ou pour rechercher des types d'événements spécifiques.

Liste des événements

La liste des événements affiche :

- La gravité. Une icône indique si l'événement est de priorité élevée, moyenne ou s'il est pour information.
- La source. Une icône indique la fonction Sophos qui a signalé l'événement.
- La date et l'heure de l'événement.
- Une description de l'événement.
- Un lien qui vous permet d'agir (le cas échéant). Cette information apparaît uniquement si vous êtes connecté en tant qu'administrateur.

Pour afficher les détails d'un événement, cliquez sur son entrée dans la liste.

Les actions que vous effectuez sont les mêmes que celles qui sont disponibles dans la console Sophos Central Admin. Retrouvez la liste sur la page **Alertes** de l'Aide de Sophos Central.

Malwares et PUA

Malware est un terme générique utilisé pour désigner un logiciel malveillant. Il désigne les virus, les vers, les chevaux de Troie et les spywares.

Les applications potentiellement indésirables (PUA) sont des programmes qui ne sont pas malveillants (composeurs, outils d'administration à distance et outils de piratage) mais dont l'utilisation sur des réseaux d'entreprise est généralement considérés comme inappropriée.

Menaces Web

Les Menaces Web désignent les sites Web malveillants et les téléchargements dangereux.

Certains sites Web sont également considérés comme inappropriés, par exemple, les sites Web pour adultes ou les réseaux sociaux. Vous pouvez les bloquer.

Éléments contrôlés

Cette catégorie inclut :

- Les applications qui ne représentent pas une menace à la sécurité mais dont vous considérez l'utilisation inappropriée sur votre lieu de travail.
- Les périphériques et les supports multimédia amovibles.
- Les téléchargements dangereux ou les sites Web dont l'utilisation est inappropriée sur votre lieu de travail.
- Les fichiers contenant des informations sensibles (renseignements personnels ou informations financières) que vous ne souhaitez pas divulguer.

Trafic malveillant

Le Trafic malveillant désigne le trafic entre les ordinateurs qui pourrait indiquer une tentative éventuelle de prise de contrôle du Mac (une attaque de « commande et de contrôle »).

Ransomware

Un ransomware est un logiciel malveillant (ou crypto-virus) qui vous empêche d'accéder à vos fichiers tant que vous ne payez pas une rançon.

4 Détections

Vous pouvez contrôler le Mac à la recherche de menaces et voir les menaces que Sophos a détecté et contre lesquelles vous êtes protégés.

Contrôler l’ordinateur

Cliquez sur **Contrôler** pour contrôler la présence de menaces dans tous les fichiers du Mac.

Lorsque le contrôle est terminé, vous êtes informé des résultats du contrôle. Si des menaces sont détectées, vous pouvez aller sur la page **Événements** pour voir plus de renseignements.

Historique des malwares et PUA

Affiche l’historique des malwares et PUA détectés. Cliquez sur la flèche pour afficher les détails sur la page **Événements**.

Historique de détection

Indique le nombre de menaces d’un type spécifique qui ont été détectées. Cliquez sur un type pour voir les informations sur les menaces détectées de ce type sur la page **Événements**.

Réinitialiser le récapitulatif

Cliquez sur **Réinitialiser le récapitulatif** pour mettre l’historique affiché dans la page **Détections** à zéro.

5 Paramètres

Remarque
Il se peut que toutes les fonctions ne soient pas décrites dans cette section. Ceci dépend de votre licence.

La page **Paramètres** est uniquement disponible si vous utilisez **Connexion admin** et que vous saisissez le mot de passe de la protection antialtération (disponible auprès de votre administrateur Sophos Central).

Vous pouvez modifier temporairement les paramètres de sécurité sur ce Mac.

Ceci pourrait vous être utile pour résoudre les problèmes. Par exemple, vous avez la possibilité de désactiver une fonction pour voir si ceci entraîne des problèmes sur le Mac.

Comment modifier les paramètres ?

Activez l'option **Remplacer la stratégie Sophos Central pendant une durée maximale de 4 heures pour résoudre les problèmes**.

Vous pouvez à présent modifier cette page. Les modifications remplacent temporairement la stratégie que vous (ou un autre administrateur) avez appliquée à partir de la console Sophos Central Admin.

Après quatre heures, les paramètres de la stratégie appliquée de manière centralisée sont rétablis.

Remarque
Vous pouvez rétablir ces paramètres plus tôt si vous le désirez. Vous ne pouvez pas le faire pour des fonctions individuelles. Vous devez désactiver l'option **Remplacer la stratégie Sophos Central pendant une durée maximale de 4 heures pour résoudre les problèmes**, qui s'applique à toutes les fonctions.

Contrôle en temps réel

Le contrôle en temps réel procède au contrôle des éléments au moment où l'utilisateur tente d'y accéder. L'accès est accordé si le fichier est sain. Vous pouvez sélectionner :

- **Fichiers**. Le contrôle est effectué sur les fichiers locaux et (si cette option est sélectionnée dans la stratégie) sur les partages réseau.
- **Internet**. Le contrôle est effectué sur les ressources Internet. Le contrôle peut être effectué sur les téléchargements en cours, l'accès aux sites Web malveillants est bloqué et les sites Web de réputation douteuse sont détectés.

Contrôles des utilisateurs

- **Contrôle des périphériques**. Cette fonction vous permet de contrôler l'accès aux périphériques et autres supports amovibles.

- **Contrôle d’applications**. Cette fonction vous permet de détecter et de bloquer les applications qui ne représentent pas une menace à la sécurité mais dont vous considérez l’utilisation inappropriée sur votre lieu de travail.
- **Contrôle du Web**. Cette fonction vous permet d’assurer la protection contre les téléchargements dangereux, de contrôler les sites Web visités par les utilisateurs et d’empêcher la perte de données.

Protection à l’exécution (runtime)

La protection à l’exécution assure la protection contre les menaces en détectant le comportement ou le trafic suspect ou malveillant sur les Macs. Vous pouvez sélectionner :

- **Détection du trafic malveillant**. Cette option permet de détecter le trafic entre un Mac et un serveur qui pourrait indiquer une tentative éventuelle de prise de contrôle du Mac.
- **Détection de ransomware (CryptoGuard)**. Cette option permet d’assurer la protection contre les malwares empêchant l’accès aux fichiers et demandant le paiement d’une somme d’argent pour les rendre accessibles.

6 Comment faire pour...

6.1 Contrôler un fichier

Pour contrôler les fichiers individuellement :

Dans le Finder, cliquez avec le bouton droit de la souris sur le fichier et sélectionnez **Contrôler avec Sophos Endpoint**.

Une boîte de dialogue **Contrôle des éléments du Finder** apparaît afin que vous puissiez voir la progression du contrôle et les résultats.

6.2 Contrôler le Mac

Pour contrôler tous les fichiers sur le Mac :

1. Rendez-vous sur la page **État** ou sur la page **Détections**.
2. Cliquez sur **Contrôler**.
   Lorsque le contrôle est terminé, vous êtes informé des résultats du contrôle.
3. Si des menaces sont détectées, vous pouvez aller sur la page **Événements** pour voir plus de renseignements.

6.3 Nettoyage d'une menace

Pour éliminer une menace détectée :

1. Cliquez sur **Connexion administrateur** et saisissez le mot de passe de la protection antialtération (disponible auprès de l'administrateur de Sophos Central).
   Le lien **Paramètres** de la barre de menus est maintenant actif.
2. Sur la page **Événements**, vous pouvez voir toutes les informations sur la menace qui a été détectée.
3. Recherchez un lien actif près des informations sur la menace.

Les actions que vous effectuez sont les mêmes que celles qui sont disponibles dans la console Sophos Central Admin. Retrouvez la liste sur la page **Alertes** de l'Aide de Sophos Central.

6.4 Modifier les paramètres de sécurité

Pour modifier les paramètres de sécurité :

1. Cliquez sur **Connexion administrateur** et saisissez le mot de passe de la protection antialtération (disponible auprès de l'administrateur de Sophos Central).
   Le lien **Paramètres** de la barre de menus est maintenant actif.
2. Allez sur la page **Paramètres**.
3. Activez l'option **Remplacer la stratégie Sophos Central pendant une durée maximale de 4 heures pour résoudre les problèmes**.
4. Utilisez les curseurs affichés sur la page pour désactiver les fonctions de sécurité.

Après quatre heures, les paramètres de la stratégie appliquée de manière centralisée sont rétablis.

Remarque
Vous pouvez rétablir ces paramètres plus tôt si vous le désirez. Vous ne pouvez pas le faire pour des fonctions individuelles. Vous devez désactiver l'option **Remplacer la stratégie Sophos Central pendant une durée maximale de 4 heures pour résoudre les problèmes**, qui s'applique à toutes les fonctions.

6.5 Mettre à jour

Pour procéder à la mise à jour :

1. Cliquez sur **À propos**.
2. Cliquez sur **Mettre à jour**.

6.6 Résoudre les problèmes

Pour résoudre les problèmes :

1. Cliquez sur **À propos**.
2. Cliquez sur **Diagnostic** pour collecter des données sur le problème.

Vous pouvez également cliquer sur **Forum Sophos Community** pour obtenir plus d'informations.

6.7 Chiffrer le Mac

La fonction de chiffrement d'appareils chiffre le disque dur de votre Mac à l'aide de la technologie FileVault 2. Lorsque votre administrateur active la fonction **Chiffrement d'appareils**, la boîte de dialogue **Sophos Device Encryption** apparaît.

1. Dans la boîte de dialogue **Sophos Device Encryption**, saisissez votre mot de passe de connexion et cliquez sur **Chiffrer**.
   Le chiffrement d'appareils est activé. Autrement, cliquez sur **Reporter** pour démarrer le processus ultérieurement.
2. Votre clé de secours est automatiquement stockée dans Sophos Central.

Lorsque le disque système est chiffré, les volumes de données internes sont automatiquement chiffrés. Les disques chiffrés sont automatiquement déverrouillés au démarrage du Mac. Les volumes de données amovibles tels que les lecteurs USB ne sont pas chiffrés.

6.8 Accéder au Mac en cas d'oubli du mot de passe

Si vous ne pouvez pas vous connecter à votre Mac en raison de l'oubli de votre mot de passe, vous allez avoir besoin d'une clé de récupération.

Si vous utilisez **Sophos Device Encryption**, la clé de récupération se trouve dans Sophos Central. Pour récupérer votre clé de secours, procédez de l'une des manières suivantes :

- Connectez-vous au Portail libre-service de Sophos et suivez les instructions de l'Aide de Sophos Central.
- Demandez à votre administrateur de récupérer la clé de secours conformément aux instructions de la section Utilisation de la récupération FileVault (page 10). Utilisez cette méthode si vous ne pouvez pas utiliser le Portail libre-service.

6.8.1 Utilisation de la récupération FileVault

Pour demander à un administrateur de vous obtenir une clé de récupération, procédez comme suit.

1. Redémarrez votre Mac et attendez que la boîte de dialogue **ID de la clé de récupération** s'affiche. L'**ID de la clé de récupération** s'affiche uniquement pendant un court moment. Pour l'afficher de nouveau, veuillez redémarrer votre Mac.
2. Contactez votre administrateur et communiquez-lui l'**ID de la clé de récupération**.
   Votre administrateur doit trouver la clé de récupération de votre Mac dans Sophos Central et vous la communiquer.
3. Cliquez sur le point d'interrogation dans le champ **Mot de passe**.
   Un message apparaît.
4. Cliquez sur la flèche à côté du message pour passer dans le champ de la clé de récupération.
5. Saisissez la clé de secours.
6. Suivez les instructions à l'écran pour créer un nouveau mot de passe.
   Si votre compte d'utilisateur a été importé à partir d'Active Directory, cliquez sur **Annuler** dans la boîte de dialogue **Réinitialisation du mot de passe** et demandez à votre administrateur de réinitialiser le mot de passe.
7. Cliquez sur **Créer un nouveau jeu de clés** si invité à le faire.

Vous pouvez de nouveau accéder à votre Mac.

7 Pourquoi le transfert de mon fichier est-il bloqué ?

Vous pourriez voir apparaître un message vous indiquant qu'un transfert de fichier (par exemple, la copie, le déplacement ou l'envoi par email de fichiers) a été bloqué.

Une telle situation se produit lorsque votre entreprise a défini une stratégie lui assurant qu'il est impossible d'envoyer des informations sensibles par inadvertance à des utilisateurs qui ne sont pas censés les recevoir.

Il existe deux types de messages :

Transfert bloqué

Si vous recevez un message « Transfert de fichiers bloqué », vous ne pouvez pas transférer les fichiers. Votre administrateur aura peut être complété ce message par quelques conseils.

Transfert autorisé

Si vous recevez un message « Demande de transfert de fichiers bloquée », vous ne pouvez pas transférer les fichiers. Votre administrateur aura peut être complété ce message par quelques conseils. Cliquez sur **Autoriser** si vous êtes sûr que l'opération sera effectuée en toute sécurité.

8 Aide supplémentaire

Vous pouvez obtenir le support technique comme suit :

- Rendez-vous sur le forum Sophos Community en anglais sur community.sophos.com et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support Sophos sur www.sophos.com/fr-fr/support.aspx.

9 Mentions légales