Manuel de l'utilisateur

HP Sure Sense

Première édition : juin 2019

Référence du document : L63508-051

Sommaire

1 Mise en route

HP Sure Sense utilise des modèles d'apprentissage en profondeur pour détecter les fichiers malveillants et empêcher les attaques de logiciels malveillants, les attaques « jour zéro », les rançongiciels et les menaces persistantes avancées (APT) de nuire à votre ordinateur.

HP Sure Sense utilise les composants suivants :

- **Modèle prédictif :** Un modèle prédictif léger d'apprentissage en profondeur. Il détecte de manière autonome les cyber-menaces et permet une protection contre les menaces APT et « jour zéro ».
- **Services Cloud de réputation de fichier :** Une base de données basée sur le Cloud contenant des informations sur les fichiers connus qui ajoutent une deuxième couche de classification. Lorsque cette option est activée, le hachage pour les fichiers PE (Portable Executable) est envoyé aux services de réputation de fichier dans le Cloud.
- **Réseau de distribution de contenu :** Un système qui distribue les dernières mises à jour de logiciels et de modèles prédictifs pour HP Sure Sense.

Onglets du menu principal

Le menu principal comprend les onglets suivants :

- **Statut** : Affiche l'état de la protection, le résumé des menaces et d'autres informations.
- **Journal des alertes** : Affiche un tableau qui répertorie les événements de sécurité et les journaux. Il contient des informations sur la sécurité, les mises à jour et la gestion. Sur cette page, vous pouvez afficher des informations supplémentaires sur les alertes de sécurité et prendre d'autres mesures.
- **Mise en quarantaine** : Affiche un tableau qui répertorie tous les fichiers en quarantaine. Chaque entrée est basée sur une valeur de hachage unique. Les entrées comprennent des informations relatives aux fichiers et à l'emplacement d'origine du fichier. Vous pouvez restaurer les fichiers mis en quarantaine à partir de la colonne **Action**.
- **Paramètres** : Vous permet de configurer si les notifications s'affichent, de définir les langues de la console et de gérer d'autres préférences. Pour afficher ou modifier les **Paramètres avancés** : Sélectionnez **Modifier**, puis entrez les informations d'authentification de l'administrateur.

Analyse complète

L'analyse complète examine tous les fichiers existants sur les lecteurs locaux de l'ordinateur. Tous les fichiers identifiés comme malveillants sont bloqués et mis en quarantaine.

Protection contre les menaces évoluées

Lorsque l'option Protection contre les menaces évoluées est activée, elle surveille le comportement de tous les procédés en cours d'exécution pour les logiciels malveillants. Si un processus est identifié comme rançongiciel, le processus est arrêté.

2 Processus de sécurité

Protection contre les logiciels malveillants

Tous les fichiers ajoutés aux lecteurs locaux de l'ordinateur sont automatiquement scannés et analysés. Lorsqu'un fichier est identifié comme malveillant, les actions suivantes se produisent :

- Le fichier est bloqué et mis en quarantaine. Le processus de quarantaine copie le fichier dans le dossier de quarantaine, supprime le fichier de son emplacement d'origine et ajoute le fichier à la table de quarantaine.
- Un événement est ajouté à la page du **Journal des alertes**. Une notification s'affiche pour indiquer que la menace est empêchée. Si vous cliquez sur la notification, la page de **Quarantaine** s'ouvre avec l'entrée appropriée en surbrillance.

REMARQUE : Les fichiers malveillants sur des périphériques de stockage externes sont bloqués et empêchés de s'exécuter, mais ne sont pas mis en quarantaine.

Restauration et suppression de fichiers en quarantaine

Les fichiers déplacés vers le dossier en quarantaine peuvent être restaurés ou supprimés selon les besoins. Les fichiers restaurés sont déplacés vers leur emplacement d'origine et autorisés à s'exécuter. La suppression d'un fichier mis en quarantaine supprime l'entrée de la table de quarantaine et supprime le fichier du dossier de quarantaine. Il ne modifie pas la classification du fichier, et toute nouvelle copie du fichier est bloquée et mise en quarantaine.

Pour supprimer ou restaurer des fichiers en quarantaine :

1. Ouvrez la page **Quarantaine**.
2. Sélectionnez le fichier que vous souhaitez supprimer. Sélectionnez l'icône **Action**.
3. Sélectionnez parmi les options pour **Restaurer le fichier**, **Supprimer le fichier** ou afficher les **Détails de fichier**.

IMPORTANT : Avant de restaurer un fichier en quarantaine, assurez-vous que le fichier n'est pas un logiciel malveillant.

Pour supprimer tous les fichiers à la fois :

▲ Sur la page de **Quarantaine**, sélectionnez l'icône de poubelle située à droite de la zone de recherche.

Ajout et suppression de fichiers de confiance

Les fichiers de confiance sont des fichiers qui ont été bloqués puis restaurés et autorisés à être exécutés par l'utilisateur. Vous pouvez ajouter des fichiers de confiance dans la liste de fichiers de confiance à partir de la page de **Quarantaine** ou de la page du **Journal des alertes**. Vous pouvez ajouter des processus à la liste des fichiers de confiance uniquement à partir de la page du **Journal d'alerte**.

Les fichiers ajoutés à la liste des fichiers de confiance sont restaurés dans leurs dossiers d'origine et supprimés du dossier de quarantaine. Les processus ajoutés à la liste des fichiers de confiance sont autorisés à s'exécuter et ne sont plus surveillés pour un comportement de rançongiciel. Les fichiers et processus ajoutés à la liste de fichiers de confiance ne sont pas analysés.

Pour ajouter un fichier de confiance ou un processus :

1. Ouvrez la page du **Journal des alertes**.
2. Sélectionnez l'icône Actions dans l'entrée du fichier ou du processus que vous souhaitez ajouter.
3. Pour ajouter un fichier, sélectionnez **Restaurer un fichier**.

   Pour ajouter un processus, sélectionnez **Ajouter aux fichiers de confiance**.

IMPORTANT : Avant d'ajouter un fichier ou un processus à la liste de fichiers de confiance, vérifiez qu'il ne s'agit pas de logiciels malveillants.

Pour supprimer un fichier de confiance ou un processus dans la liste de fichiers de confiance :

1. Dans la page **Paramètres**, sélectionnez **Modifier les fichiers de confiance**.
2. Sélectionnez le fichier ou le processus que vous souhaitez supprimer, puis sélectionnez l'icône **Actions**.
3. Pour supprimer un fichier, sélectionnez **Fichier de quarantaine**.

   Pour supprimer un processus, sélectionnez **Supprimer de la liste**.

Exclusions

Les dossiers et processus peuvent être exclus de l'analyse à l'aide de l'option **Exclusions**.

IMPORTANT : Avant d'ajouter un dossier à la liste d'exclusion, HP recommande ce qui suit :

- Ajoutez uniquement des dossiers en lecture seule pour minimiser la possibilité pour des dossiers de confiance d'être victimes d'attaques.
- N'ajoutez pas de dossiers temporaires. Les logiciels malveillants ont tendance à écrire des modules sur des dossiers temporaires. Cet avis est également pertinent pour les dossiers système tels que `Windows` ou `system32`.
- Si une solution spécifique continue à retourner des faux positifs, consultez le fournisseur de la solution pour obtenir des recommandations.

Pour accéder à la liste d'exclusions :

1. Ouvrez la page **Paramètres**, puis faites défiler vers le bas pour accéder aux **Paramètres avancés**.
2. Sélectionnez **Modifier les exclusions**.

A Désinstallation de HP Sure Sense

Si HP Sure Sense est actuellement installé et qu'une nouvelle installation est nécessaire, vous devez d'abord retirer la version actuelle. La méthode pour désinstaller est fonction de la façon dont HP Sure Sense a été installé.

Si HP Sure Sense a été installé manuellement à l'aide de l'assistant d'installation :

▲ Exécutez le programme d'installation, puis sélectionnez **Désinstaller**.

Si HP Sure Sense a été préinstallé sur votre périphérique :

1. Dans **Paramètres Windows**, allez à **Applications et fonctionnalités**.
2. Désinstallez le programme d'installation HP Sure Sense.