WithSecure Elements Endpoint Protection for Servers

Table des matières

Chapitre
1

Présentation

Sujets :

Ce guide fournit des informations d'ordre général sur le produit et explique comment l'utiliser.

Remarque : Pour obtenir des instructions d'installation et de déploiement, consultez le guide de l'administrateur de WithSecure Elements Endpoint Protection.

Doté d'outils ultrasophistiqués, WithSecure Elements Agent for Servers offre une protection sans faille aux serveurs Windows. Il est décliné dans une version Premium qui intègre des fonctionnalités de sécurité avancées, comme DataGuard et le contrôle des applications. Rapid Detection and Response peut être également activé en modifiant le type d'abonnement.

Le produit peut être installé sous les abonnements suivants :

- WithSecure Elements EPP for Servers
- WithSecure Elements EPP for Servers Premium
- WithSecure Elements EDR + EPP for Servers Premium

1.1 Configuration requise

Cette section contient des informations importantes sur WithSecure Elements Agent for Windows Servers.

Nous vous recommandons vivement de lire l'intégralité du document avant de commencer à utiliser le produit.

Navigateurs pris en charge

- Microsoft Edge
- Chrome, deux dernières versions majeures
- Firefox, deux dernières versions majeures

Systèmes d'exploitation pris en charge

Remarque : WithSecure ne couvre que les systèmes d'exploitation pris en charge par les fournisseurs. Si vous souhaitez profiter d'un support à long terme pour une plateforme que les fournisseurs ne prennent plus en charge, contactez votre représentant commercial.

WithSecure Elements Agent prend en charge les versions de système d'exploitation suivantes :

- Microsoft® Windows Server 2016, Standard
- Microsoft® Windows Server 2016, Essentials
- Microsoft® Windows Server 2016, Datacenter
- Microsoft® Windows Server 2016, Core
- Microsoft® Windows Server 2019, Standard
- Microsoft® Windows Server 2019, Datacenter
- Microsoft® Windows Server 2019, Core
- Microsoft® Windows Server 2022, Standard
- Microsoft® Windows Server 2022, Datacenter
- Microsoft® Windows Server 2022, Core
- Microsoft® Windows Server 2025, Standard
- Microsoft® Windows Server 2025, Datacenter
- Microsoft® Windows Server 2025, Core

Remarque : Windows Server 2016 Nano n'est pas pris en charge.

Toutes les éditions Microsoft Windows Server sont prises en charge, à l'exception de :

- Windows Server pour processeur Itanium
- Éditions Windows HPC pour le matériel spécifique
- Éditions Windows Storage
- Windows MultiPoint Server
- Windows Home Server

Remarque : Tous les systèmes d'exploitation doivent disposer du dernier Service Pack et TLS 1.2 doit être configuré et activé. Assurez-vous également que l'option **Désactiver la mise à jour automatique du certificat racine** dans la stratégie de groupe Microsoft est bien désactivée pour permettre l'établissement de connexions TLS. Les systèmes d'exploitation doivent prendre en charge les certificats Microsoft Azure Code Signing. Vous trouverez plus d'informations ici.

Remarque : Pour des raisons de performance et de sécurité, vous pouvez uniquement installer le produit sur une partition NTFS.

Remarque : Le client requiert .NET Framework 4.7.2 et l'installe automatiquement s'il est manquant.

Serveurs Terminal Server pris en charge

WithSecure Elements Agent prend en charge les plateformes de serveur de terminal suivantes :

- Microsoft Windows Terminal/Services RDP (sur les plateformes Windows Server mentionnées ci-dessus)
- Citrix® XenApp 5.0
- Citrix® XenApp 6.0

- Citrix® XenApp 6.5
- Citrix® XenApp 7.5 et 7.6

Configuration requise

- Processeur : Intel Pentium 4 2 GHz ou supérieur (doit prendre en charge SSE2).
- Mémoire : 1 Go sous les systèmes 32 bits/2 Go ou plus sous les systèmes 64 bits.
- Espace disque : 2 Go d'espace disque disponible.
- Affichage avec une résolution de 1 024 x 768 ou supérieure.
- Connexion Internet : une connexion Internet est requise pour valider votre abonnement, recevoir les mises à jour du produit et utiliser la détection cloud.
- Javascript doit être actif dans les paramètres du navigateur pour activer les pages de blocage.

Langues prises en charge

Les langues prises en charge sont l'anglais, le tchèque, le danois, le néerlandais, l'estonien, le finnois, le français, le français (canadien), l'allemand, le grec, le hongrois, l'italien, le japonais, le norvégien, le polonais, le portugais, le portugais (brésilien), le roumain, le russe, le slovène, Espagnol, espagnol (Amérique latine), suédois, turc, chinois traditionnel (Hong Kong), chinois traditionnel (Taïwan) et chinois simplifié (RPC).

Chapitre
2

Prise en main

Sujets :

- Modifier les paramètres du produit
- Comment voir l'action du produit

Cette section vous explique comment accéder aux outils/fonctionnalités du produit et modifier ses paramètres.

Remarque : Votre administrateur est susceptible d'avoir appliqué des paramètres de sécurité, ce qui signifie que vous ne pouvez peut-être pas modifier localement certaines fonctionnalités.

2.1 Modifier les paramètres du produit

Vous pouvez contrôler le comportement du produit en modifiant ses paramètres.

Notez que vous devez disposer des droits d'administration afin de pouvoir modifier les paramètres du produit. Il est possible d'accéder à certains d'entre eux depuis le menu contextuel de l'icône de barre d'état système.

Remarque : Votre administrateur est susceptible d'avoir appliqué des paramètres de sécurité, ce qui signifie que vous ne pouvez peut-être pas modifier localement certaines fonctionnalités.

Tâches associées

Exécution d'une analyse des programmes malveillants à la page 18
Vous pouvez analyser l'intégralité de votre ordinateur pour vous assurer de l'absence de fichiers dangereux ou d'applications indésirables.

Utiliser le contrôle d'accès DataGuard à la page 22
Le contrôle d'accès DataGuard protège les dossiers des ransomware (chantage au chiffrement) en empêchant les applications inconnues d'y accéder.

Modification des paramètres du pare-feu Windows à la page 41
Quand le pare-feu est activé, il limite l'accès vers et depuis votre ordinateur. Certaines applications doivent être autorisées à passer à travers le pare-feu pour fonctionner correctement.

Afficher les événements récents du produit à la page 11
Vous pouvez voir les actions prises par le produit et comment il a protégé votre ordinateur sur la page **Historique des événements**.

Désactivation de toutes les fonctionnalités de sécurité à la page 9
Pour libérer plus de ressources système, vous pouvez désactiver toutes les fonctionnalités de sécurité.

2.1.1 Accès rapide aux paramètres du produit

L'icône de barre d'état système permet d'accéder à de nombreux paramètres produit.

Pour ouvrir le menu contextuel de la barre d'état système, procédez comme suit :

Remarque : Si l'icône du produit est masquée, cliquez tout d'abord sur la flèche **Afficher les icônes masquées** située dans la barre des tâches.

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Le menu contextuel inclut les options suivantes :

Option	Description
Afficher l'état actuel	Affiche l'état de protection actuel de votre ordinateur.
Rechercher des mises à jour	Recherche et télécharge les dernières mises à jour.
Afficher les événements récents	Indique les actions effectuées par le produit pour protéger votre ordinateur.
Ouvrir les paramètres	Ouvre les paramètres du produit.
À propos	Affiche les informations de version du produit.

2.1.2 Désactivation de toutes les fonctionnalités de sécurité

Pour libérer plus de ressources système, vous pouvez désactiver toutes les fonctionnalités de sécurité.

Remarque : Votre administrateur est susceptible d'avoir défini une stratégie qui vous empêche de désactiver les fonctionnalités de sécurité.

Remarque : Votre ordinateur n'est pas intégralement protégé si vous désactivez les fonctionnalités de sécurité.

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ....
3. Sélectionnez **Désactiver toutes les fonctionnalités de sécurité**.

Elles seront automatiquement réactivées au prochain redémarrage de votre ordinateur. Vous avez également la possibilité de les activer manuellement depuis l'affichage principal du produit.

2.2 Comment voir l'action du produit

L'icône d'état de la protection indique que le produit fonctionne. Les statistiques de protection fournissent quant à eux des informations sur la façon dont il a protégé votre ordinateur.

2.2.1 Icônes d'état de la protection

L'icône d'état de la protection vous indique l'état global du produit et de ses fonctionnalités.

Les icônes d'état de la protection :

Icône de statut	Nom du statut	Description
	OK	Votre ordinateur est protégé. Les fonctionnalités sont activées et fonctionnent correctement.
	Expiré	Votre ordinateur n'est pas protégé. L'abonnement a expiré.
	Expiré et désactivé	Votre ordinateur n'est pas protégé. L'abonnement a expiré et le produit a été désactivé.

Icône de statut	Nom du statut	Description
	Désactivé; dysfonctionnement	La protection de votre ordinateur est incomplète ou inexistante. Le produit requiert une action immédiate. Par exemple, une fonctionnalité critique est désactivée/ne fonctionne pas correctement ou des mises à jour sont obsolètes.
	Désactivé	Votre ordinateur n'est pas entièrement protégé. Le produit requiert votre attention. Par exemple, une fonctionnalité de sécurité telle que la navigation basée sur la réputation est désactivée.
	Mise à jour	La protection est en train d'être configurée. Le produit est en cours de mise à jour.

Icônes d'état de la protection

Les icônes d'état de protection suivantes s'affichent dans la barre d'état système lorsque le produit requiert votre attention ou une action.

Icône de la barre d'état	Nom du statut	Description
	Attention	Votre ordinateur n'est pas entièrement protégé. Le produit requiert votre attention, par exemple, une ou plusieurs fonctionnalités de sécurité sont désactivées ou les mises à jour sont très anciennes.
	Avertissement	Votre ordinateur n'est pas protégé. Le produit nécessite une action immédiate, par exemple si l'abonnement a expiré ou si une fonctionnalité critique fonctionne mal.

2.2.2 Afficher les événements récents du produit

Vous pouvez voir les actions prises par le produit et comment il a protégé votre ordinateur sur la page **Historique des événements**.

Il affiche les divers événements associés aux produits installés, ainsi que les actions prises par ces derniers. Par exemple, vous pouvez voir les éléments dangereux qui ont été détectés puis nettoyés ou mis en quarantaine.

Procédez comme suit pour consulter l'historique complet des événements du produit :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ....
3. Sélectionnez **Événements récents**.
   La page **Historique des événements** s'ouvre.

L'historique des événements indique l'heure et la description de chaque événement. Selon le type de l'événement, vous pouvez cliquer dessus pour en savoir plus à son sujet. Par exemple, pour les fichiers dangereux, les informations suivantes sont disponibles :

- date et heure à laquelle le fichier dangereux a été détecté ;
- nom du programme malveillant et emplacement sur l'ordinateur ;
- action entreprise.

Chapitre
3

Protection de l'ordinateur contre le contenu dangereux

Sujets :

Le produit protège votre ordinateur contre les programmes susceptibles de l'endommager, de l'utiliser à des fins illégales ou de dérober vos informations personnelles.

Par défaut, la protection contre les programmes malveillants supprime tous les fichiers dangereux dès qu'elle les détecte de manière à ce qu'ils ne causent aucun dommage.

Le produit analyse automatiquement vos disques durs locaux, les supports amovibles (lecteurs portables ou DVD) et tout contenu téléchargé.

Le produit surveille également les modifications apportées à votre ordinateur qui sont susceptibles d'indiquer la présence de fichiers dangereux. Lorsque le produit décèle des modifications système dangereuses comme la modification de paramètres système ou des tentatives de changement de processus système importants, son composant DeepGuard arrête l'exécution de l'application car celle-ci peut présenter des risques.

Remarque : Votre administrateur peut appliquer des paramètres de sécurité, ce qui signifie que vous ne pourrez peut-être pas modifier localement certaines fonctionnalités.

3.1 Que fait du contenu dangereux

Les fichiers et applications dangereux peuvent tenter de porter atteinte à l'intégrité de vos données ou d'obtenir un accès non autorisé à votre ordinateur en vue de dérober vos informations personnelles.

3.1.1 Applications potentiellement indésirables et applications indésirables

Les applications potentiellement indésirables affichent des comportements ou des caractéristiques que vous êtes susceptible de considérer comme étant indésirables. De leur côté, les applications indésirables peuvent avoir une incidence plus néfaste sur votre appareil ou vos données.

Une application peut être identifiée comme potentiellement indésirable si elle peut :

- **affecter votre confidentialité ou votre productivité** - par exemple, en divulguant des renseignements personnels ou en effectuant des actions non autorisées ;
- **entraîner une surconsommation des ressources de votre appareil** - par exemple, en utilisant trop de mémoire ou de stockage ;
- **compromettre la sécurité de votre appareil ou des informations qui y sont stockées** - par exemple, en vous exposant à du contenu ou à des applications inattendus.

Si ces comportements et caractéristiques peuvent avoir un impact variable sur votre appareil ou vos données, ils ne sont néanmoins pas assez dangereux pour que les applications en question soient considérées comme des programmes malveillants.

Si une application présente des comportements ou des caractéristiques ayant un impact plus grave, celle-ci est perçue comme indésirable. De telles applications sont traitées avec une grande prudence par le produit.

Le produit gère une application différemment selon qu'il s'agit d'une application potentiellement indésirable ou indésirable :

- **Une application potentiellement indésirable** - Le produit bloquera automatiquement l'exécution de l'application. Si vous êtes certain de faire confiance à l'application, vous pouvez demander au produit WithSecure de l'exclure de l'analyse. Vous devez disposer des droits d'administrateur pour exclure un fichier bloqué de l'analyse.
- **Application indésirable** : le produit bloque automatiquement l'exécution de l'application.

Tâches associées

Activation de l'analyse en temps réel à la page 17
Activez l'analyse en temps réel pour supprimer les fichiers nuisibles avant qu'ils ne puissent causer des dégâts sur votre ordinateur.

Exécution d'une analyse des programmes malveillants à la page 18
Vous pouvez analyser l'intégralité de votre ordinateur pour vous assurer de l'absence de fichiers dangereux ou d'applications indésirables.

Utiliser le contrôle d'accès DataGuard à la page 22
Le contrôle d'accès DataGuard protège les dossiers des ransomware (chantage au chiffrement) en empêchant les applications inconnues d'y accéder.

3.1.2 Vers informatiques

Les vers sont des programmes malveillants capables de s'autorépliquer sur les appareils ou via les réseaux informatiques, et de réaliser des actions nuisibles à l'insu de l'utilisateur.

Les vers informatiques sont les seuls logiciels malveillants ayant la possibilité de s'autopropager sans action de l'utilisateur. Nombre d'entre eux sont conçus de sorte à tromper l'utilisateur. Ils peuvent prendre l'apparence d'images, de vidéos, d'applications ou de tout autre programme/fichier utiles. L'objectif consiste à gagner la confiance de l'utilisateur et de le pousser à installer le vers. D'autres vers sont en revanche entièrement furtifs, car ils exploitent les failles des appareils (ou des programmes qui y sont installés).

Une fois installé, le vers utilise les ressources physiques de l'appareil pour s'autorépliquer et se propager via le réseau. La diffusion d'une grande quantité de copies est susceptible d'altérer les performances de l'appareil. Et si de nombreux appareils sont infectés - qui envoient alors des copies du vers -, le réseau

lui-même peut être perturbé. Certains vers sont également capables d'endommager directement l'appareil touché (par exemple, en modifiant les fichiers qui y sont stockés, en installant d'autres applications nuisibles et en dérobant des données).

La plupart des vers se propagent uniquement sur un type de réseau spécifique. Toutefois, certains peuvent se propager sur deux types ou plus, bien qu'ils restent relativement rares. D'ordinaire, les vers essaient de se propager à travers l'un des réseaux suivants (même s'il en existe d'autres qui ciblent des canaux moins populaires) :

- Réseaux locaux
- Réseaux de messagerie
- Sites de réseaux sociaux
- Connexions Peer-to-peer (P2P)
- SMS ou MMS

Tâches associées

Activation de l'analyse en temps réel à la page 17
Activez l'analyse en temps réel pour supprimer les fichiers nuisibles avant qu'ils ne puissent causer des dégâts sur votre ordinateur.

Exécution d'une analyse des programmes malveillants à la page 18
Vous pouvez analyser l'intégralité de votre ordinateur pour vous assurer de l'absence de fichiers dangereux ou d'applications indésirables.

Utiliser le contrôle d'accès DataGuard à la page 22
Le contrôle d'accès DataGuard protège les dossiers des ransomware (chantage au chiffrement) en empêchant les applications inconnues d'y accéder.

3.1.3 Chevaux de Troie

Les chevaux de Troie sont des logiciels en apparence légitimes, mais qui contiennent une fonctionnalité malveillante. Leur rôle est d'introduire des parasites sur l'ordinateur à l'insu de l'utilisateur.

Les chevaux de Troie tirent leur nom d'une célèbre légende de la Grèce antique. Ils peuvent ressembler à des jeux, des économiseurs d'écran, des mises à jour d'application ou tout autre programme/fichier utile. Certains prennent l'apparence d'un logiciel existant, légitime et parfois même réputé, mais qui aura été modifié pour y dissimuler un parasite. L'utilisateur va télécharger et installer le programme, pensant avoir affaire à une version saine.

Une fois installés, ils peuvent également utiliser des leurres pour entretenir l'illusion de leur légitimité. Par exemple, un cheval de Troie ayant pris l'apparence d'un économiseur d'écran ou d'un fichier document affichera une image ou un document. Pendant que l'attention de l'utilisateur est accaparée par ces leurres, le cheval de Troie effectue silencieusement des actions non autorisées en arrière-plan.

En règle générale, les chevaux de Troie apportent des modifications nuisibles à l'appareil infecté (suppression/cryptage de fichiers, altération des paramètres des programmes, etc.) ou dérobent des données confidentielles qui y sont stockées. Ils peuvent être classés en fonction du type de leurs actions :

- **Trojan-downloader** (Cheval de Troie téléchargeur) : se connecte à un site distant pour télécharger et installer d'autres programmes
- **Trojan-dropper** (Cheval de Troie injecteur) : contient un ou plusieurs programmes supplémentaires qu'il installe
- **Trojan-pws** (Cheval de Troie dérobeur de mots de passe) : dérobe les mots de passe stockés sur les appareils ou saisis dans un navigateur Web
    - **Banking-trojan** (Cheval de Troie bancaire de type trojan-pws) : cible les données permettant d'accéder aux comptes bancaires en ligne (noms d'utilisateur et mots de passe)
- **Trojan-spy** (Cheval de Troie espion) : surveille l'activité sur les appareils et envoie des informations à un site distant

Tâches associées

Activation de l'analyse en temps réel à la page 17

Activez l'analyse en temps réel pour supprimer les fichiers nuisibles avant qu'ils ne puissent causer des dégâts sur votre ordinateur.

Exécution d'une analyse des programmes malveillants à la page 18
Vous pouvez analyser l'intégralité de votre ordinateur pour vous assurer de l'absence de fichiers dangereux ou d'applications indésirables.

Utiliser le contrôle d'accès DataGuard à la page 22
Le contrôle d'accès DataGuard protège les dossiers des ransomware (chantage au chiffrement) en empêchant les applications inconnues d'y accéder.

3.1.4 Portes dérobées

Les portes dérobées sont des fonctionnalités ou des programmes permettant de contourner les fonctions de sécurité d'un programme, d'un appareil, d'un portail ou d'un service.

À partir du moment où la conception/mise en œuvre d'une fonctionnalité dans un programme, un appareil, un portail ou un service pose un risque en matière de sécurité, cette dernière peut être considérée comme une porte dérobée. Par exemple, dans le cadre d'un portail en ligne, il peut s'agir d'un point d'accès administrateur secret avec mot de passe codé en dur.

Les portes dérobées exploitent généralement les défauts présents au sein du code d'un programme, d'un appareil, d'un portail ou d'un service. Il peut s'agir de bugs, de vulnérabilités ou de fonctionnalités non documentées.

La porte dérobée constitue un moyen utilisé par les pirates informatiques pour obtenir un accès non autorisé ou perpétrer des actions nuisibles leur permettant de contourner les fonctionnalités de sécurité, telles que les restrictions d'accès, l'authentification ou encore le chiffrement.

Tâches associées

Activation de l'analyse en temps réel à la page 17
Activez l'analyse en temps réel pour supprimer les fichiers nuisibles avant qu'ils ne puissent causer des dégâts sur votre ordinateur.

Exécution d'une analyse des programmes malveillants à la page 18
Vous pouvez analyser l'intégralité de votre ordinateur pour vous assurer de l'absence de fichiers dangereux ou d'applications indésirables.

Utiliser le contrôle d'accès DataGuard à la page 22
Le contrôle d'accès DataGuard protège les dossiers des ransomware (chantage au chiffrement) en empêchant les applications inconnues d'y accéder.

3.1.5 Exploits

Les exploits sont des éléments ou des méthodes permettant à un individu ou à un logiciel malveillant d'exploiter une faille de sécurité informatique dans un système d'exploitation ou un logiciel, que ce soit à distance ou à un niveau local.

Un exploit peut se présenter sous la forme d'un objet ou d'une méthode. Par exemple, un élément de programme spécial, une portion de code ou encore une chaîne de caractères constituent tous des objets. Une méthode représente quant à elle une séquence spécifique de commandes.

Un exploit est utilisé en vue d'exploiter une faille informatique ou une vulnérabilité dans un programme. En raison de l'unicité de chaque programme, les exploits sont minutieusement adaptés.

Les attaquants ont plusieurs moyens d'acheminer un exploit pour qu'il puisse infecter un ordinateur ou un appareil :

- **Intégration dans un programme piraté ou spécialement conçu** - Lorsque vous installez et lancez le programme, l'exploit est exécuté.
- **Intégration dans une pièce jointe** - Lorsque vous ouvrez la pièce jointe, l'exploit est exécuté.
- **Intégration dans un site Web piraté ou dangereux** - Lorsque vous consultez le site en question, l'exploit est exécuté.

Une fois exécuté, l'exploit altère le comportement du programme ciblé (par exemple, en le forçant à s'éteindre ou à modifier la mémoire/le stockage système de façon intempestive). Cela peut créer des

conditions favorables à la réalisation d'actions nuisibles, comme le vol de données ou l'obtention d'un accès non autorisé à des sections protégées du système d'exploitation.

Tâches associées

Activation de l'analyse en temps réel à la page 17
Activez l'analyse en temps réel pour supprimer les fichiers nuisibles avant qu'ils ne puissent causer des dégâts sur votre ordinateur.

Exécution d'une analyse des programmes malveillants à la page 18
Vous pouvez analyser l'intégralité de votre ordinateur pour vous assurer de l'absence de fichiers dangereux ou d'applications indésirables.

Utiliser le contrôle d'accès DataGuard à la page 22
Le contrôle d'accès DataGuard protège les dossiers des ransomware (chantage au chiffrement) en empêchant les applications inconnues d'y accéder.

3.1.6 Kits d'exploits

Les kits d'exploits sont des kits logiciels conçus pour identifier les vulnérabilités des systèmes des utilisateurs (ordinateurs ou appareils).

Comme son nom l'indique, un kit d'exploits contient une liste d'exploits capables de tirer profit d'une faille (vulnérabilité) au sein d'un programme, d'un ordinateur ou d'un appareil. Le kit est généralement intégré à un site dangereux ou piraté de sorte que tout ordinateur ou appareil y accédant soit exposé à ses effets.

Lorsqu'un nouvel ordinateur ou appareil se connecte au site piégé, le kit recherche les failles potentielles qui pourraient permettre l'introduction d'un exploit contenu dans la liste. S'il parvient à en trouver un, le kit le lance pour tirer parti de la vulnérabilité.

Une fois l'ordinateur/appareil infecté, le kit d'exploits peut y exécuter sa charge utile malveillante. D'ordinaire, un autre programme nuisible est installé et lancé sur l'ordinateur/appareil, permettant ainsi de réaliser divers types d'actions non autorisées.

Les kits d'exploits sont conçus pour être simples d'utilisation et offrir une grande modularité de manière à ce que leurs contrôleurs puissent gérer facilement les exploits et les charges utiles (ajout/suppression).

Tâches associées

Activation de l'analyse en temps réel à la page 17
Activez l'analyse en temps réel pour supprimer les fichiers nuisibles avant qu'ils ne puissent causer des dégâts sur votre ordinateur.

Exécution d'une analyse des programmes malveillants à la page 18
Vous pouvez analyser l'intégralité de votre ordinateur pour vous assurer de l'absence de fichiers dangereux ou d'applications indésirables.

Utiliser le contrôle d'accès DataGuard à la page 22
Le contrôle d'accès DataGuard protège les dossiers des ransomware (chantage au chiffrement) en empêchant les applications inconnues d'y accéder.

3.2 Comment analyser mon ordinateur ?

Lorsqu'elle est activée, la ***protection contre les programmes malveillants*** recherche automatiquement les éventuels fichiers dangereux au sein de votre ordinateur.

Nous vous conseillons de toujours laisser la ***protection contre les programmes malveillants*** activée. Vous pouvez également analyser vos fichiers manuellement et planifier des analyses quand vous voulez vous assurer qu'aucun fichier nuisible ne se trouve sur votre ordinateur ou quand vous souhaitez analyser des fichiers exclus des analyses en temps réel. Configurez une analyse planifiée si vous désirez analyser régulièrement l'ordinateur chaque jour ou chaque semaine.

3.2.1 Comment fonctionne l'analyse en temps réel

L'analyse en temps réel protège l'ordinateur en analysant tous les accès aux fichiers et en bloquant cet accès aux fichiers contenant des ***programmes malveillants***.

Lorsque votre ordinateur tente d'accéder à un fichier, l'analyse en temps réel analyse le fichier à la recherche d'éléments malveillants avant d'autoriser l'ordinateur à accéder au fichier.

Si l'analyse en temps réel détecte un contenu malveillant, ce dernier est placé en quarantaine avant qu'il ne puisse nuire.

Est-ce que l'analyse en temps réel affecte les performances de mon ordinateur ?

Normalement, vous ne remarquez pas le processus d'analyse car il ne prend que très peu de temps et de ressources système. La durée et les ressources système utilisées par l'analyse en temps réel dépend, par exemple, du contenu, de l'emplacement et du type de fichier.

L'analyse des fichiers sur disques amovibles tels que lecteurs CD, DVD et USB portables prend plus de temps.

Remarque : Les fichiers compressés, tels que les fichiers ***.zip***, ne sont pas analysés par l'analyse en temps réel.

L'analyse en temps réel peut ralentir votre ordinateur si :

- vous disposez d'un ordinateur qui ne respecte pas les conditions requises, ou
- vous accédez à de nombreux fichiers simultanément. Par exemple, quand vous ouvrez un répertoire qui contient de nombreux fichiers à analyser.

Activation de l'analyse en temps réel

Activez l'analyse en temps réel pour supprimer les fichiers nuisibles avant qu'ils ne puissent causer des dégâts sur votre ordinateur.

Pour s'assurer que l'analyse en temps réel est bien activée :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Protection contre les programmes malveillants** > **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier certains des paramètres.

4. Activez l'**analyse en temps réel**.

3.2.2 Analyser les fichiers manuellement

Vous pouvez analyser l'intégralité de votre ordinateur pour vous assurer de l'absence de fichiers dangereux ou d'applications indésirables.

L'analyse complète de l'ordinateur recherche les virus, logiciels espions et applications potentiellement indésirables sur tous les disques durs internes et externes. Elle recherche également d'éventuels éléments cachés derrière un rootkit. Cette analyse prend un certain temps. Vous pouvez également n'analyser que les composants de votre système où les applications dangereuses sont souvent détectées, afin de supprimer plus efficacement les applications indésirables et les éléments dangereux de votre ordinateur.

Analyse de fichiers et de dossiers

Si vous avez des doutes sur certains fichiers de votre ordinateur, vous pouvez limiter l'analyse à ces fichiers ou dossiers. Ces analyses sont beaucoup plus rapides qu'une analyse complète. Par exemple, lorsque vous connectez un disque dur externe ou une clé USB à votre ordinateur, vous pouvez l'analyser afin de vérifier qu'ils ne contiennent pas de fichiers dangereux.

Exécution d'une analyse des programmes malveillants

Vous pouvez analyser l'intégralité de votre ordinateur pour vous assurer de l'absence de fichiers dangereux ou d'applications indésirables.

Pour analyser votre ordinateur, procédez comme suit :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Pour optimiser la façon dont l'analyse manuelle contrôle votre ordinateur, sélectionnez et **Paramètres d'analyse** sur la page principale.
   a) Sélectionnez **Analyser uniquement les types de fichiers qui contiennent généralement du code malveillant (plus rapide)** si vous ne souhaitez pas analyser tous les fichiers.

      Les fichiers avec les extensions suivantes sont des exemples de types de fichiers connus : `com`, `doc`, `dot`, `exe`, `htm`, `ini`, `jar`, `pdf`, `scr`, `wma`, `xml` et `zip`.

   b) Sélectionnez **Analyser les fichiers compressés** pour analyser les fichiers contenus dans des archives compressées (par exemple, des fichiers Zip). Le fait de sélectionner cette option ralentit la vitesse de l'analyse. Pour analyser uniquement les archives (et non les fichiers à l'intérieur), laissez la case décochée.
3. Sur la page principale, sélectionnez .
4. Sélectionnez **Analyse anti-programmes malveillants** ou **Analyse complète de l'ordinateur**.
   - L'**Analyse anti-logiciels malveillants** commence par analyser la mémoire active de l'ordinateur, puis les emplacements où les logiciels malveillants sont couramment détectés, y compris les dossiers de documents. Elle peut détecter et supprimer plus rapidement les applications indésirables et les éléments nuisibles de l'ordinateur.
   - L'option **Analyse complète de l'ordinateur** recherche les virus, logiciels espions et applications potentiellement indésirables sur tous les disques durs internes et externes. Elle recherche également d'éventuels éléments dissimulés par un rootkit. Cette analyse est fastidieuse.

   L'analyse antivirus démarre.
5. Si l'analyse antivirus détecte des éléments dangereux, la liste de ceux-ci s'affiche.
6. Cliquez sur un élément détecté pour sélectionner l'action à effectuer sur le contenu dangereux.

Option	Description
Nettoyer	Nettoie les fichiers automatiquement. Les fichiers qui ne peuvent pas être nettoyés sont mis en quarantaine.
Quarantaine	Stocke les fichiers dans un endroit sûr, d'où ils ne peuvent pas se répandre ou endommager votre ordinateur.
Supprimer	Supprime définitivement les fichiers de votre ordinateur.
Ignorer	Ne fait rien pour l'instant et conserve les fichiers sur votre ordinateur.
Exclure	Autorise l'application à s'exécuter et l'exclut des analyses suivantes.

   Remarque : Certaines options ne sont pas disponibles pour tous les types de contenu dangereux.
7. Sélectionnez **Traiter tout** pour démarrer le nettoyage.
8. L'analyse anti-programmes malveillants affiche les résultats finaux et le nombre d'éléments dangereux nettoyés.

   Remarque : L'analyse anti-programmes malveillants peut nécessiter le redémarrage de l'ordinateur pour terminer le nettoyage. Le cas échéant, sélectionnez **Redémarrer** pour terminer le nettoyage des éléments dangereux et redémarrer l'ordinateur.

Vous pouvez consulter le rapport de la dernière analyse antivirus en sélectionnant **Ouvrir le rapport de la dernière analyse**.

Analyse dans l'Explorateur Windows

Vous pouvez analyser des disques, des dossiers et des fichiers à la recherche de virus et d'applications indésirables dans l'Explorateur Windows.

Si vous avez des doutes sur certains fichiers de votre ordinateur, vous pouvez limiter l'analyse à ces fichiers ou dossiers. Ces analyses sont beaucoup plus rapides qu'une analyse complète. Par exemple, lorsque vous connectez un disque dur externe ou une clé USB à votre ordinateur, vous pouvez l'analyser afin de vérifier qu'ils ne contiennent pas de fichiers dangereux.

Pour analyser un disque, un dossier ou un fichier :

1. Effectuez un clic droit sur le disque, le dossier ou le fichier que vous souhaitez analyser.
2. Dans le menu contextuel, sélectionnez **Recherche de programmes malveillants**.

   Remarque : Sous Windows 11, sélectionnez **Afficher plus d'options**, puis **Rechercher des programmes malveillants**.

   L'analyse antivirus démarre et contrôle le disque, le dossier ou le fichier que vous avez sélectionné.

Elle vous guide tout au long du processus de nettoyage en cas de détection de fichiers dangereux ou d'applications indésirables.

3.2.3 Planification d'analyses

Configurez votre ordinateur de sorte à rechercher et supprimer automatiquement les programmes malveillants ou autres applications nuisibles quand vous ne l'utilisez pas. Vous pouvez aussi programmer des analyses régulières pour vous assurer qu'il est parfaitement sûr.

Pour planifier une analyse :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez .
3. Sélectionnez **Paramètres d'analyse**.
4. Activez l'**analyse planifiée**.
5. Sous **Effectuer l'analyse**, sélectionnez la fréquence à laquelle vous souhaitez que votre ordinateur soit analysé automatiquement.

Option	Description
Tous les jours	Analysez votre ordinateur tous les jours.
Toutes les semaines	Analysez votre ordinateur certains jours de la semaine. Choisissez les jours dans la liste.
Toutes les quatre semaines	Analysez votre ordinateur le jour de votre choix toutes les quatre semaines. Sélectionnez le jour dans la liste. L'analyse démarre lors de la prochaine occurrence du jour sélectionné.

6. Sous **Heure de début**, sélectionnez l'heure à laquelle vous souhaitez que l'analyse planifiée soit exécutée.
7. Sélectionnez **Exécuter l'analyse en priorité basse** afin que l'analyse planifiée affecte moins les autres activités en cours sur l'ordinateur. Lorsqu'elle est exécutée en priorité basse, l'analyse prend plus de temps.
8. Sélectionnez **Analyser uniquement les types de fichiers qui contiennent généralement du code malveillant (plus rapide)** si vous ne souhaitez pas analyser tous les fichiers.

   Les fichiers avec les extensions suivantes sont des exemples de types de fichiers connus : `com`, `doc`, `dot`, `exe`, `htm`, `ini`, `jar`, `pdf`, `scr`, `wma`, `xml` et `zip`.

9. Sélectionnez **Analyser les fichiers compressés** pour analyser les fichiers contenus dans des archives compressées (par exemple, des fichiers Zip). Le fait de sélectionner cette option ralentit la vitesse de l'analyse. Pour analyser uniquement les archives (et non les fichiers à l'intérieur), laissez la case décochée.

Remarque : Les analyses planifiées sont interrompues lorsque le ***mode présentation*** est activé. À sa désactivation, elles s'exécutent de nouveau selon la planification établie.

3.3 Qu'est-ce que DeepGuard ?

DeepGuard offre une protection proactive et instantanée contre les menaces inconnues.

DeepGuard surveille les applications pour détecter et bloquer les modifications potentiellement dangereuses apportées au système en temps réel. Il s'assure que vous n'utilisiez que des applications sûres. Il contrôle la sécurité d'une application depuis le service approuvé du cloud. S'il est impossible de déterminer la sécurité d'une application, DeepGuard contrôle son comportement.

Conseil : Si vous souhaitez que WithSecure ajoute votre application à la liste des applications autorisées, demandez à ce qu'elle soit analysée ici. Nous vous informerons des résultats si vous nous avez fourni vos coordonnées.

DeepGuard bloque les nouveaux virus et les virus inconnus, les ***chevaux de Troie***, les ***vers***, les ***attaques*** et les autres applications dangereuses essayant de modifier votre ordinateur, et empêche toute application suspecte d'accéder à Internet.

DeepGuard détecte les modifications système potentiellement nuisibles suivantes :

- la modification de paramètres système (registre Windows),
- les tentatives de désactivation de programmes système importants, des programmes de sécurité comme ce produit par exemple, et
- les tentatives de modification de fichiers système importants.

Pour s'assurer que DeepGuard est bien activé :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Protection contre les programmes malveillants** > **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

4. Sélectionnez **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

5. Activez **DeepGuard**.

Lorsqu'il est activé, DeepGuard bloque automatiquement les applications qui tentent d'apporter des modifications potentiellement dangereuses au système.

Remarque : Toutes les règles DeepGuard sont visibles pour tous les utilisateurs. Elles peuvent inclure des noms de fichiers et de dossiers contenant des informations personnelles. Par conséquent, sachez que les autres utilisateurs d'un même ordinateur peuvent consulter les chemins d'accès et les noms de fichiers inclus dans les règles DeepGuard.

Tâches associées

Données de sécurité à la page 45
Le service envoie des requêtes sur des activités potentiellement malveillantes ou des appareils protégés à WithSecure ***Security Cloud***.

3.3.1 Autoriser les applications bloquées par DeepGuard

Vous pouvez contrôler le blocage ou l'autorisation des applications par DeepGuard.

Il arrive que DeepGuard bloque une application fiable, alors que vous voulez l'utiliser et que vous savez qu'elle n'est pas dangereuse. Vous êtes confronté à cette situation lorsqu'une application essaie d'apporter des changements potentiellement nuisibles au système. Vous avez aussi peut-être bloqué une application par mégarde via une fenêtre contextuelle DeepGuard.

Pour autoriser l'application bloquée par DeepGuard :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.

2. Sur la page principale, sélectionnez ⋯.
3. Sélectionnez **Quarantaine et exclusions**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

   La vue **Contrôle des fichiers et des applications** s'affiche.
4. Sélectionnez l'onglet **Bloqués**.
   Une liste des applications bloquées par DeepGuard apparaît.
5. Recherchez l'application que vous souhaitez autoriser et sélectionnez **Autoriser**.
6. Sélectionnez **Oui** pour confirmer que vous souhaitez autoriser l'application.

L'application sélectionnée est ajoutée à la liste **Exclus**, tandis que DeepGuard l'autorise de nouveau à apporter des modifications au système.

3.3.2 Utilisation de DataGuard

Il surveille un ensemble de dossiers en vue de détecter toute modification potentiellement dangereuse apportée par un ransomware ou un autre logiciel malveillant de même type.

Les ransomwares sont des programmes malveillants qui chiffrent les fichiers importants de votre ordinateur pour vous empêcher d'y accéder. Les pirates informatiques vous demandent alors une rançon pour les restaurer, bien que vous n'ayez aucune garantie que vos données personnelles vous soient restituées.

Lorsque DataGuard est activé, seules les applications fiables ont la possibilité d'accéder aux dossiers protégés. Le produit vous informe de toute tentative d'accès à un dossier protégé de la part d'une application suspecte. En revanche, si vous faites confiance à l'application en question, vous pouvez l'autoriser à y accéder. DataGuard permet également à DeepGuard d'utiliser sa liste de dossiers protégés en vue de renforcer toujours plus le niveau de protection.

Vous pouvez sélectionner les dossiers nécessitant une protection supplémentaire contre les logiciels destructeurs, à l'image des ransomwares.

Remarque : Vous devez activer DeepGuard pour pouvoir utiliser DataGuard (uniquement disponible dans la version Premium).

Pour gérer vos dossiers protégés :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Protection contre les programmes malveillants** > **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.
4. Activez **DataGuard**.
5. Sélectionnez **Afficher les dossiers protégés**.
6. Sélectionnez l'onglet **Protégés**.
   Les dossiers actuellement protégés sont présentés sous la forme d'une liste.
7. Ajoutez ou supprimez des dossiers au besoin.

   Pour ajouter un nouveau dossier protégé, procédez comme suit :

   a) Cliquez sur **Ajouter nouveau**.
   b) Sélectionnez le dossier que vous souhaitez protéger.
   c) Cliquez sur **Sélectionner un dossier**.

   Pour supprimer un dossier, procédez comme suit :

   a) Sélectionnez le dossier dans la liste.
   b) Cliquez sur **Supprimer**.

Conseil : Cliquez sur **Restaurer les paramètres par défaut** pour annuler les modifications apportées à la liste des dossiers protégés depuis l'installation du produit.

Tâches associées

Ajout et suppression de dossiers protégés à la page 22

Vous pouvez sélectionner les dossiers nécessitant une protection supplémentaire contre les logiciels destructeurs, à l'image des ransomwares.

3.3.3 Ajout et suppression de dossiers protégés

Vous pouvez sélectionner les dossiers nécessitant une protection supplémentaire contre les logiciels destructeurs, à l'image des ransomwares.

Par ailleurs, il bloque toute tentative d'accès non sécurisé à ces dossiers.

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ....
3. Sélectionnez **Quarantaine et exclusions**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

   La vue **Contrôle des fichiers et des applications** s'affiche.
4. Sélectionnez l'onglet **Protégés**.
   Les dossiers actuellement protégés sont présentés sous la forme d'une liste.
5. Ajoutez ou supprimez des dossiers au besoin.

   Pour ajouter un nouveau dossier protégé, procédez comme suit :

   a) Cliquez sur **Ajouter nouveau**.
   b) Sélectionnez le dossier que vous souhaitez protéger.
   c) Cliquez sur **Sélectionner un dossier**.

   Conseil : Comme vous devez autoriser séparément toutes les applications qui ont besoin d'accéder au dossier protégé, il est recommandé de ne pas ajouter de dossiers contenant les jeux ou les applications installées (par exemple, dossiers de bibliothèque Steam). Dans le cas contraire, ces applications risquent de ne plus fonctionner correctement.

   Pour supprimer un dossier, procédez comme suit :

   a) Sélectionnez le dossier dans la liste.
   b) Cliquez sur **Supprimer**.

Conseil : Cliquez sur **Restaurer les paramètres par défaut** pour annuler les modifications apportées à la liste des dossiers protégés depuis l'installation du produit.

3.4 Utiliser le contrôle d'accès DataGuard

Le contrôle d'accès DataGuard protège les dossiers des ransomware (chantage au chiffrement) en empêchant les applications inconnues d'y accéder.

Remarque : DataGuard est uniquement disponible dans la version Premium.

Pour activer le **contrôle d'accès DataGuard** :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Protection contre les programmes malveillants** > **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.
4. Activez **Contrôle d'accès DataGuard**.

3.4.1 Afficher les éléments mis en quarantaine

Vous pouvez afficher plus d'informations concernant les éléments en quarantaine.

La zone de quarantaine est un emplacement sûr où vous pouvez stocker les fichiers et les applications potentiellement dangereux ou indésirables afin de protéger votre ordinateur. Vous avez néanmoins la possibilité de les restaurer plus tard si jamais vous en avez besoin. En cas contraire, vous pouvez les supprimer. Notez que ces derniers seront alors supprimés de façon définitive.

Pour afficher des informations sur les éléments en quarantaine :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⋯.
3. Sélectionnez **Quarantaine et exclusions**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

   La vue **Contrôle des fichiers et des applications** s'affiche.
4. Sélectionnez l'onglet **En quarantaine**.
   Cette liste indique le nom, la date de détection et le type d'infection associés à chaque élément mis en quarantaine.
5. Double-cliquez sur un élément en quarantaine pour obtenir plus d'informations.
   Cela vous indique l'emplacement d'origine des éléments individuels mis en quarantaine.

3.4.2 Restaurer les éléments mis en quarantaine

Vous pouvez restaurer des éléments mis en quarantaine dont vous avez besoin.

Vous pouvez restaurer des applications ou des fichiers de la quarantaine si vous en avez besoin. Ne restaurez des éléments de la quarantaine que si vous êtes convaincu qu'ils ne représentent aucune menace. Les éléments restaurés retrouvent leur emplacement d'origine sur votre ordinateur.

Pour restaurer les éléments en quarantaine :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⋯.
3. Sélectionnez **Quarantaine et exclusions**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

   La vue **Contrôle des fichiers et des applications** s'affiche.
4. Sélectionnez l'onglet **En quarantaine**.
5. Sélectionnez l'élément en quarantaine que vous souhaitez restaurer.
6. Cliquez sur **Autoriser**.
7. Cliquez sur **Oui** pour confirmer que vous souhaitez restaurer l'élément en quarantaine.

L'élément sélectionné est automatiquement restauré à son emplacement d'origine. Selon le type d'infection, celui-ci peut être exclu des futures analyses.

Remarque : Pour afficher l'ensemble des fichiers et des applications actuellement exclus, sélectionnez l'onglet **Exclus** dans la vue **Contrôle des fichiers et des applications**.

3.4.3 Exclure des fichiers ou des dossiers de l'analyse

Lorsque vous excluez des fichiers ou des dossiers de l'analyse, ils ne sont pas inspectés à la recherche de contenu dangereux.

Pour exclure des fichiers ou des dossiers de l'analyse, procédez comme suit :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⋯.
3. Sélectionnez **Quarantaine et exclusions**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

   La vue **Contrôle des fichiers et des applications** s'affiche.
4. Sélectionnez l'onglet **Exclus**.
   Cette vue vous dresse la liste des fichiers et des dossiers exclus.
5. Sélectionnez **Ajouter nouveau**.
6. Sélectionnez le fichier ou le dossier que vous souhaitez exclure des analyses.
7. Sélectionnez **OK**.

Les fichiers ou dossiers sélectionnés sont exclus des analyses futures.

3.4.4 Afficher les applications exclues

Vous pouvez afficher les applications que vous avez exclues de l'analyse et les supprimer de la liste des exclusions, afin qu'elles soient prises en compte à l'avenir.

Si le produit détecte une application potentiellement indésirable dont vous ne mettez pas en doute la sécurité ou encore un logiciel espion que vous souhaitez conserver sur votre ordinateur afin d'utiliser une autre application, vous pouvez exclure cet élément de l'analyse ; le produit ne vous met alors plus en garde contre cet élément.

Remarque : Si l'application se comporte comme un virus ou une application dangereuse, il est impossible de l'exclure.

De plus, DeepGuard ne bloque pas certains jeux Steam. Par conséquent, vous n'avez pas besoin d'exclure les jeux Steam de l'analyse ou de désactiver DeepGuard pour les exécuter.

Pour afficher les applications exclues de l'analyse :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⋯.
3. Sélectionnez **Quarantaine et exclusions**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

   La vue **Contrôle des fichiers et des applications** s'affiche.
4. Sélectionnez l'onglet **Exclus**.
   Cette vue vous dresse la liste des fichiers et des dossiers exclus.
5. Si vous voulez à nouveau analyser une application exclue :
   a) Sélectionnez l'application que vous voulez à nouveau inclure dans l'analyse.
   b) Cliquez sur **Supprimer**.

De nouvelles applications s'affichent dans la liste d'exclusion dès lors que vous les avez exclues de l'analyse ; elles ne peuvent pas être ajoutées directement à la liste d'exclusion.

3.4.5 Ajout et suppression de dossiers protégés

Vous pouvez sélectionner les dossiers nécessitant une protection supplémentaire contre les logiciels destructeurs, à l'image des ransomwares.

Par ailleurs, il bloque toute tentative d'accès non sécurisé à ces dossiers.

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⋯.
3. Sélectionnez **Quarantaine et exclusions**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

   La vue **Contrôle des fichiers et des applications** s'affiche.
4. Sélectionnez l'onglet **Protégés**.
   Les dossiers actuellement protégés sont présentés sous la forme d'une liste.
5. Ajoutez ou supprimez des dossiers au besoin.

   Pour ajouter un nouveau dossier protégé, procédez comme suit :
   a) Cliquez sur **Ajouter nouveau**.
   b) Sélectionnez le dossier que vous souhaitez protéger.
   c) Cliquez sur **Sélectionner un dossier**.

   Conseil : Comme vous devez autoriser séparément toutes les applications qui ont besoin d'accéder au dossier protégé, il est recommandé de ne pas ajouter de dossiers contenant les jeux ou les applications installées (par exemple, dossiers de bibliothèque Steam). Dans le cas contraire, ces applications risquent de ne plus fonctionner correctement.

   Pour supprimer un dossier, procédez comme suit :
   a) Sélectionnez le dossier dans la liste.
   b) Cliquez sur **Supprimer**.

Conseil : Cliquez sur **Restaurer les paramètres par défaut** pour annuler les modifications apportées à la liste des dossiers protégés depuis l'installation du produit.

3.4.6 Affichage des coffres

Un coffre-fort est un dossier dans lequel seules les applications configurées pour ce coffre-fort peuvent écrire, créer ou renommer des fichiers et des sous-dossiers.

Pour afficher les dossiers configurés en tant que coffres :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ....
3. Sélectionnez **Quarantaine et exclusions**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

   La vue **Contrôle des fichiers et des applications** s'affiche.
4. Sélectionnez l'onglet **Coffres**.
   Cette liste vous montre les dossiers qui ont été définis comme coffres-forts.

3.5 Empêche les applications de télécharger les fichiers dangereux.

Vous pouvez empêcher les applications de votre ordinateur de télécharger des fichiers dangereux sur Internet.

Certains sites Web contiennent des logiciels d'attaque et d'autres fichiers malveillants pouvant endommager votre ordinateur. La protection réseau avancée vous permet d'empêcher toute application de télécharger des fichiers dangereux avant même qu'ils n'atteignent votre ordinateur.

Pour empêcher toutes les applications de télécharger des fichiers dangereux :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sélectionnez **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.
3. Sur la page principale, sélectionnez ⚙.
4. Sélectionnez **Protection contre les programmes malveillants** > **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.
5. Activez la **protection réseau avancée**.

Remarque : Le paramètre est activé lorsque vous désactivez le pare-feu.

3.6 Utiliser l'intégration d'AMSI pour identifier les attaques basées sur des scripts

L'interface d'analyse anti-programmes malveillants (AMSI) est un composant Windows permettant une inspection approfondie des services de script intégrés.

Remarque : L'intégration AMSI est uniquement disponible sous Windows Server 2016, 2019 et 2022.

Les programmes malveillants avancés exploitent des scripts déguisés ou chiffrés afin de contourner les méthodes d'analyse traditionnelles. Ils sont souvent chargés directement dans la mémoire et n'utilisent donc pas de fichiers sur l'appareil.

L'interface AMSI peut être utilisée par les applications et services Windows pour envoyer des demandes d'analyse au produit de sécurité installé sur l'ordinateur. Cela renforce la protection contre les logiciels dangereux qui incorporent des scripts ou des macros dans des composants Windows (comme PowerShell et Office 365) ou d'autres applications en vue d'échapper à toute détection.

Pour activer l'intégration d'AMSI dans le produit :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Protection contre les programmes malveillants** > **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

4. Activer **AMSI**.
   Le produit vous informe désormais lorsque AMSI détecte du contenu dangereux et enregistre ces détections dans l'historique d'événements.

Chapitre
4

Navigation sûre

Sujets :

- Blocage des sites Web dangereux
- Vérifier que les extensions de navigateur sont activées

La navigation basée sur la réputation vous permet de naviguer en toute sécurité sur Internet. Elle fournit des évaluations de sécurité pour les sites Web dans votre navigateur et bloque l'accès aux sites Web jugés dangereux.

4.1 Blocage des sites Web dangereux

Lorsqu'elle est activée, la navigation basée sur la réputation bloque l'accès aux sites Web dangereux.

Pour vous assurer que la navigation basée sur la réputation est bien activée :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Navigation sécurisée**.
4. Sélectionnez **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.
5. Activez **Navigation basée sur la réputation**.
6. Si votre navigateur est ouvert, redémarrez-le pour appliquer les paramètres modifiés.

Remarque : La navigation basée sur la réputation exige que l'extension de protection de la navigation soit activée dans votre navigateur.

4.1.1 Blocage des sites Web suspects et interdits

La navigation basée sur la réputation vous tient à l'écart des sites Web non fiables ou présentant du contenu interdit.

Vous pouvez parfois tomber sur un site Web dont le contenu est suspect, frauduleux ou interdit. Il peut s'agir, par exemple, d'un site Web de spam connu et contrefait abritant des programmes potentiellement indésirables ou à caractère illégal, quelle que soit votre localisation.

La navigation basée sur la réputation vous permet d'éviter d'accéder malencontreusement à ce type de sites Web.

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Navigation sécurisée**.
4. Sélectionnez **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.
5. Vérifiez que la **navigation basée sur la réputation** est bien activée.
6. Si vous souhaitez bloquer les sites Web considérés comme suspects en plus de ceux considérés comme dangereux, sélectionnez **Bloquer les sites Web suspects**.
7. Pour bloquer les sites Web présentant du contenu interdit, sélectionnez **Bloquer les sites Web interdits**.
8. Si votre navigateur est ouvert, redémarrez-le pour appliquer les paramètres modifiés.

Remarque : La navigation basée sur la réputation exige que l'extension de protection de la navigation soit activée dans votre navigateur.

4.1.2 Utilisation des icônes d'évaluation de la réputation

Lorsque vous utilisez Google, Bing, Yahoo! ou DuckDuckGo, la navigation basée sur la réputation affiche une icône d'évaluation de la sécurité des sites Web sur les pages des résultats de recherche.

Les icônes de couleur indiquent le niveau de sécurité du site ouvert. Le niveau de sécurité de chaque lien dans les résultats du moteur de recherche est également indiqué par les mêmes icônes.

	À notre connaissance, ce site est sûr. Nous n'avons rien trouvé de suspect.
	Ce site est suspect. Nous vous recommandons la plus grande prudence si vous décidez de le consulter. Évitez de télécharger des fichiers ou d'indiquer des informations personnelles.
	Le site est dangereux. Nous vous recommandons de ne pas le consulter. Sinon, un administrateur l'a bloqué et vous ne pouvez pas y accéder.

	Nous n'avons pas encore analysé ce site Web et ne disposons à l'heure actuelle d'aucune information le concernant.
	L'accès à ce site Web n'est jamais bloqué.

Conseil : Si vous estimez qu'un fichier ou qu'une URL a été détecté à tort, vous pouvez envoyer un échantillon à WithSecure Labs pour analyse à l'adresse https://www.withsecure.com/fr/support/contact-support/submit-a-sample. Vous pouvez envoyer plusieurs URL ou adresses IP en les combinant et en les soumettant sous la forme d'un fichier texte.

Pour afficher l'icône d'évaluation de la réputation sur la page des résultats de recherche :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez .
3. Sélectionnez **Navigation sécurisée**.
4. Sélectionnez **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.
5. Vérifiez que la **navigation basée sur la réputation** est bien activée.
6. Sélectionnez **Afficher la note de réputation des sites Web dans les résultats de recherche**.
7. Si votre navigateur est ouvert, redémarrez-le pour appliquer les paramètres modifiés.

Remarque : La navigation basée sur la réputation exige que l'extension de protection de la navigation soit activée dans votre navigateur.

4.1.3 Que faire si un site Web est bloqué ?

Une page de blocage de navigation basée sur la réputation s'affiche si vous tentez d'accéder à un site considéré comme nuisible.

Lorsqu'une page de blocage de navigation basée sur la réputation s'affiche :

1. Si vous souhaitez accéder au site Web, sélectionnez **Autoriser le site Web**.
   Le ***contrôle d'accès d'utilisateur Windows*** vous demande de confirmer cette action.
2. Si nécessaire, saisissez les informations de votre compte administrateur, puis confirmez la modification.

Si vous estimez qu'un site bloqué est fiable, sélectionnez **Signaler ce site Web**. Une nouvelle page s'affiche, dans laquelle vous pouvez renseigner les informations nécessaires pour envoyer un échantillon du site à des fins d'analyse. Si la page ne s'affiche pas, envoyez l'échantillon ici.

Remarque : Si la page de blocage ne s'affiche pas, assurez-vous que l'extension de la protection de la navigation est bien activée dans votre navigateur.

4.1.4 Exceptions de sites Web

La liste des exceptions de sites Web répertorie les sites autorisés ou bloqués.

Remarque : Si votre administrateur a explicitement bloqué un site Web ou si son contenu a été bloqué, l'accès à ce site est impossible, et ce même si vous l'ajoutez à la liste des **sites autorisés**.

Pour afficher et modifier les exceptions de sites Web, procédez comme suit :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez .
3. Sélectionnez **Navigation sécurisée** > **Modifier les paramètres**.
4. Sélectionnez **Afficher les exceptions de sites Web**.

   Si le site Web que vous souhaitez modifier figure déjà dans la liste Autorisé ou Refusé et que vous souhaitez le supprimer :

   a) Sélectionnez **Autorisé** ou **Refusé** en fonction de la liste que vous souhaitez modifier.
   b) Sélectionnez le site qui vous intéresse, cliquez sur le bouton droit de la souris, puis sur **Autoriser** ou **Refuser**.

Si le site Web ne figure dans aucune liste :

a) Sélectionnez **Autorisé** pour autoriser le site ou **Refusé** pour le bloquer.
b) Sélectionnez **Ajouter** pour ajouter un site Web à la liste.
c) Saisissez l'adresse du site Web que vous souhaitez ajouter, puis sélectionnez **OK**.
d) Dans la boîte de dialogue **Exceptions de sites Web**, sélectionnez **Fermer**.

5. Sélectionnez **OK** pour revenir à la page principale.

Pour modifier l'adresse d'un site Web autorisé ou bloqué, cliquez avec le bouton droit de la souris sur le site Web dans la liste, puis sélectionnez **Modifier**.

Pour supprimer un site Web autorisé ou bloqué de la liste, sélectionnez le site Web, puis cliquez sur **Supprimer**.

4.2 Vérifier que les extensions de navigateur sont activées

La navigation basée sur la réputation **nécessite** des extensions de navigateur pour pouvoir sécuriser vos activités en ligne (qu'il s'agisse de la navigation, d'opérations bancaires ou d'achats) et vous communiquer des informations pendant que vous surfez sur Internet.

Une fois installé sur votre ordinateur, le produit essaie d'installer automatiquement les extensions de navigateur. Lorsque vous ouvrez votre navigateur, il affiche une notification au sujet de la nouvelle extension installée. Il est alors possible que vous deviez l'activer.

Si l'extension de protection de la navigation WithSecure n'est pas disponible dans votre navigateur, vous devez la réinstaller manuellement.

Dans le cas où vous auriez manqué cette notification, la vue principale du produit vous indique si l'extension de navigateur n'a pas encore été configurée. Pour cela, sélectionnez simplement **Configurer**. Suivez ensuite les instructions à l'écran.

Cependant, si vous ne voyez pas la notification dans la vue principale du produit ou l'avez manquée, vous pouvez vérifier si l'extension de navigateur a été installée et activée de la manière suivante :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Modifier les paramètres** dans l'écran contextuel situé en bas à gauche.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

4. Sélectionnez **Oui** pour permettre à l'application d'apporter des modifications à votre appareil.
5. Sélectionnez **Navigation sécurisée**.
6. Selon votre navigateur, procédez comme suit :

   - Si vous utilisez **Firefox**, sous **Extensions de navigateur**, sélectionnez **Ouvrir les modules complémentaires Firefox**. L'extension sera ajoutée et activée pour Firefox.
   - Si vous utilisez **Chrome**, sous **Extensions de navigateur**, sélectionnez **Ouvrir le Chrome Web Store**. La page **Protection de la navigation par WithSecure** s'ouvre dans le Chrome Web Store. Si l'extension a déjà été installée sur Chrome, mais est actuellement désactivée, accédez à **Extensions** et activez-la. Si elle n'a pas encore été installée, sélectionnez **Ajouter à Chrome** > **Ajouter une extension**. L'extension est alors ajoutée et activée pour Chrome.
   - Si vous utilisez **Microsoft Edge**, sous **Extensions de navigateur**, sélectionnez **Ouvrir les modules complémentaires Edge**. La page **Protection de la navigation par WithSecure** s'ouvre dans les modules complémentaires Edge. Si l'extension a déjà été installée sur Microsoft Edge, mais est actuellement désactivée, sélectionnez **Activer** pour l'activer. Si elle n'a pas encore été installée, sélectionnez **Obtenir** > **Ajouter une extension**. L'extension est alors ajoutée et activée pour Microsoft Edge.

   Remarque : Il se peut que vous deviez réinstaller les extensions après la mise à niveau du produit ou l'installation d'un nouveau navigateur.

Pour vérifier que l'extension est bien activée, ouvrez la page de test suivante dans votre navigateur : https://unsafe.fstestdomain.com. Si la page de blocage du produit s'ouvre, cela signifie que l'extension

est en cours d'utilisation. En revanche, si la page ne s'affiche pas, vous devez activer l'extension manuellement.

Chapitre
5

Protection de vos données sensibles

Sujets :

Le ***contrôle de la connexion*** renforce la sécurité en empêchant les pirates informatiques de s'immiscer dans vos transactions confidentielles et en vous protégeant des activités nuisibles lors de vos opérations en ligne.

Le ***contrôle de la connexion*** détecte automatiquement les connexions sécurisées aux sites bancaires en ligne et bloque toute connexion ne renvoyant pas au site souhaité. Lorsque vous ouvrez un tel site, seules les connexions à des sites sécurisés et offrant une protection totale pour les transactions sont autorisées.

Si vous devez accéder à un site Web bloqué pour clore une transaction en cours, vous pouvez autoriser provisoirement l'accès à la page bloquée ou bien mettre fin à la session du ***contrôle de la connexion***.

Le ***contrôle de la connexion*** prend actuellement en charge les navigateurs suivants :

- Microsoft Edge (Chromium)
- Firefox
- Google Chrome

5.1 Activation du contrôle de la connexion

Lorsque le ***contrôle de la connexion*** est activé, vos connexions sécurisées profitent d'un niveau de protection accru.

Le ***contrôle de la connexion*** bloque les connexions non sécurisées. Par exemple, si vous accédez à un site bancaire ou que vous effectuez des paiements en ligne, le ***contrôle de la connexion*** active et bloque toutes les connexions qui ne sont pas nécessaires au bon fonctionnement des services bancaires en ligne. De cette façon, ces dernières ne peuvent pas interférer avec vos opérations confidentielles.

Pour activer le ***contrôle de la connexion***, procédez comme suit :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Navigation sécurisée** > **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

4. Activez le **contrôle de la connexion**.
5. Pour configurer les paramètres de ***contrôle de la connexion*** :

   - Désactivez **Déconnecter les applications non approuvées** si vous ne souhaitez pas que le ***contrôle de la connexion*** interrompe vos connexions déjà ouvertes. Si vous laissez ce paramètre activé, le ***contrôle de la connexion*** interrompt vos connexions Internet actuelles.
   - Désactivez le paramètre **Déconnecter les outils de scripts et en ligne de commande** si vous avez besoin d'utiliser un outil externe qui est bloqué par le ***contrôle de la connexion***.

     Remarque : Nous vous recommandons de ne pas désélectionner ce paramètre, à moins que cela ne soit absolument nécessaire. En effet, certaines attaques impliquant des programmes malveillants utilisent des composants Windows intégrés (comme PowerShell) en vue d'accéder à vos informations personnelles et identifiants bancaires.

   - Choisissez la façon dont vous souhaitez que le ***contrôle de la connexion*** gère les données qui ont été copiées dans votre Presse-papiers. Par défaut, le ***contrôle de la connexion*** les efface toutes afin de protéger votre confidentialité lorsque la session se termine.

     Désactivez ce paramètre si vous ne souhaitez pas que le ***contrôle de la connexion*** efface le contenu de votre Presse-papiers.

   - Par défaut, l'accès à distance à votre appareil est bloqué pendant votre session bancaire. Les transactions bancaires sont toujours privées et confidentielles. Vous ne devez jamais vous connecter à votre banque en ligne si quelqu'un a accès à distance à votre appareil.

     Important : Ne désactivez pas le paramètre **Bloquer l'accès à distance pendant la session bancaire** à la demande de quiconque, à moins que vous ne connaissiez à la fois la personne qui réclame l'accès et l'objet exact de la demande.

5.2 Utilisation du contrôle de la connexion

Lorsqu'il est activé, le ***contrôle de la connexion*** détecte automatiquement tout accès à un site bancaire en ligne.

Lorsque vous ouvrez un tel site dans votre navigateur, l'indicateur ***Contrôle de la connexion*** s'affiche en haut de votre écran. Toutes les autres connexions sont bloquées lorsque la protection bancaire est activée.

Conseil : Si vous ne souhaitez pas que vos autres connexions actives soient interrompues lors de l'activation du ***contrôle de la connexion***, sélectionnez l'indicateur **Contrôle de la connexion** et l'icône ⚙ située en haut à droite de la notification associée pour modifier les paramètres.

Pour fermer la session du ***contrôle de la connexion*** et restaurer vos autres connexions, procédez comme suit :

1. Sélectionnez l'indicateur **Contrôle de la connexion** situé en haut de votre écran.

2. Sélectionnez **Terminer** dans la notification.

Chapitre
6

Utilisation du filtre des résultats de recherche

Sujets :

Le filtre des résultats de recherche masque le contenu réservé aux adultes en s'assurant que Google, Yahoo, Bing et YouTube utilisent le niveau "strict" de SafeSearch.

Bien que cela ne puisse pas empêcher tout contenu inapproprié et explicite d'apparaître dans vos résultats de recherche, cela vous aide à éviter la plupart de ces contenus.

6.1 Activer le filtre des résultats de recherche

Vous pouvez activer le filtre des résultats de recherche pour ne pas afficher les contenus explicites.

Pour activer le filtre des résultats de recherche :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Contrôle du contenu Web**.
4. Activez le **filtre des résultats de recherche**.

Lorsque le filtre des résultats de recherche est activé, il remplace les paramètres des modes de sécurité de SafeSearch pour les sites Web visités par les personnes connectées à un compte utilisateur Windows.

Chapitre
7

Consulter les tâches automatisées

Votre administrateur peut configurer des tâches planifiées de manière à analyser automatiquement votre ordinateur, rechercher les mises à jour manquantes et installer les mises à jour de sécurité.

Pour en savoir plus sur les tâches exécutées automatiquement sur votre ordinateur :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez .
3. Sélectionnez **Tâches automatisées**.

Cette page indique la description et la planification associées à chacune des tâches, la dernière fois où elles ont été exécutées et leur prochaine exécution programmée.

Le tableau suivant vous montre quelques exemples de planification pour les tâches :

Planification	Description
@daily	La tâche s'effectue à une heure aléatoire chaque jour.
@weekdays	La tâche s'effectue à une heure aléatoire chaque jour de la semaine.
@weekly	La tâche s'effectue à une heure aléatoire un jour spécifique de chaque semaine.
@monthly	La tâche s'effectue à une heure aléatoire un jour spécifique de chaque mois.

Planification	Description
12 ? * 5	La tâche s'effectue selon l'expression CRON spécifiée, soit dans le cas présent une heure aléatoire comprise entre 12:00 et 13:00 chaque samedi. Une expression CRON est une chaîne composée de quatre champs séparés par des espaces selon la forme générale suivante : <hours> <days of the month> <months> <days of the week> Chaque champ contient généralement une valeur numérique ou un caractère spécial qui peut indiquer une valeur aléatoire, par exemple.

Chapitre
8

Qu'est-ce qu'un pare-feu ?

Sujets :

- Modification des paramètres du pare-feu Windows
- Utiliser les pare-feux personnels

Le ***pare-feu*** empêche les intrus et les applications nuisibles de pénétrer dans votre ordinateur via Internet.

Le pare-feu n'autorise que des connexions Internet sécurisées depuis votre ordinateur et bloque les intrusions depuis le Web.

8.1 Modification des paramètres du pare-feu Windows

Quand le pare-feu est activé, il limite l'accès vers et depuis votre ordinateur. Certaines applications doivent être autorisées à passer à travers le pare-feu pour fonctionner correctement.

Le produit utilise le pare-feu Windows pour protéger votre ordinateur.

Pour modifier les paramètres du pare-feu Windows :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Dans la vue principale, sélectionnez **Virus et menaces**.
3. Sélectionnez **Paramètres du Pare-feu Windows**.

Pour en savoir plus sur le pare-feu Windows, consultez la documentation Microsoft Windows.

8.2 Utiliser les pare-feux personnels

Le produit conçu pour fonctionner avec le pare-feu Windows. Les autres pare-feux personnels nécessitent une configuration supplémentaire pour fonctionner avec le produit.

Le produit utilise le pare-feu Windows pour les fonctions pare-feu de base comme le contrôle du trafic réseau entrant et la séparation de votre réseau interne de l'Internet public. En outre, DeepGuard contrôle les applications installées et empêche toute application suspecte d'accéder à Internet sans votre autorisation.

Si vous remplacez le pare-feu Windows par un pare-feu personnel, veillez à ce qu'il autorise le trafic réseau entrant et sortant pour tous les processus WithSecure et veillez à autoriser l'ensemble de ces derniers lorsque le pare-feu vous y invite.

Conseil : Si votre pare-feu dispose d'un mode de filtrage manuel, autorisez tous les processus WithSecure.

Chapitre
9

Comment utiliser les mises à jour

Sujets :

Les mises à jour protègent votre ordinateur contre les dernières menaces.

Le produit récupère automatiquement les dernières mises à jour pour votre ordinateur lorsque vous êtes connecté à Internet. Il détecte le trafic réseau et ne vient nullement déranger votre utilisation d'Internet, même si votre connexion est lente.

9.1 Afficher les dernières mises à jour

Affichez la date et l'heure de la dernière mise à jour.

Si vous avez activé les mises à jour automatiques, le produit reçoit automatiquement les dernières mises à jour dès que vous êtes connecté à Internet.

Pour consulter les détails des dernières mises à jour pour les produits installés :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez .
3. Sélectionnez **Mises à jour**.
4. Le détail des dernières mises à jour est disponible sous **Connexion**.
5. Pour rechercher manuellement les dernières mises à jour, sélectionnez **Rechercher maintenant**. Le produit installe automatiquement les dernières mises à jour disponibles.

   Remarque : Votre connexion Internet doit être active pour que vous puissiez rechercher les dernières mises à jour.

9.2 Modifier les paramètres de connexion

Instructions pour modifier le mode de connexion à Internet de votre ordinateur et définir comment vous souhaitez gérer les mises à jour lorsque vous utilisez des réseaux mobiles.

Votre fournisseur d'accès Internet peut vous proposer ou demander d'utiliser un proxy. Un proxy agit en tant qu'intermédiaire entre votre ordinateur et Internet. Il intercepte toutes les demandes afin de vérifier s'il peut les traiter en utilisant son cache. Il sert également à améliorer les performances, filtrer les demandes et assurer votre anonymat sur Internet pour garantir votre sécurité.

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez .
3. Sélectionnez **Mises à jour** > **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

4. Sous **Configuration du proxy manuel**, choisissez si votre ordinateur utilise ou non un serveur proxy pour se connecter à Internet.
   - Sélectionnez **Ne pas utiliser** si votre ordinateur est directement connecté à Internet.
   - Sélectionnez **Utiliser les paramètres du navigateur** pour utiliser les mêmes paramètres de proxy HTTP que ceux configurés dans votre navigateur Web.
   - Sélectionnez **Adresse personnalisée**, puis ajoutez l'adresse du proxy et le **numéro de port** pour configurer manuellement les paramètres de votre proxy HTTP.

Chapitre
10

Confidentialité

Sujets :

- Données de sécurité
- Amélioration du produit

Cette section explique ce qu'est Security Cloud et comment vous pouvez nous aider à améliorer le produit en envoyant des données anonymes.

10.1 Données de sécurité

Le service envoie des requêtes sur des activités potentiellement malveillantes ou des appareils protégés à WithSecure ***Security Cloud***.

Basé dans le cloud, WithSecure Security Cloud est un système d'analyse des cybermenaces exploité par WithSecure. Nous collectons le minimum de données nécessaires pour vous fournir les services de sécurité que vous avez souscrits et offrir une protection de haute qualité à tous nos utilisateurs.

WithSecure Security Cloud nous permet de conserver une vue d'ensemble actuelle du contexte mondial des cybermenaces et de protéger nos clients contre les nouvelles menaces dès leur découverte.

Security Cloud ne collecte que des données pouvant contenir des informations sur des fichiers ou des sites Web bloqués par WithSecure pour des raisons de sécurité. Les données de sécurité ne sont pas utilisées à des fins de marketing personnalisé.

Fourniture de données

En tant que contributeur, vous autorisez Security Cloud à conserver des données de sécurité qui nous aident à renforcer votre protection contre les nouvelles menaces. Ces informations sont conservées pendant une durée limitée à l'issue de laquelle elles sont supprimées.

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Accédez à la page des **paramètres de confidentialité**.
4. Sélectionnez **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.
5. Sous **Security Cloud**, sélectionnez **Autoriser une analyse plus approfondie**.

10.2 Amélioration du produit

Vous pouvez nous aider à améliorer le produit en nous envoyant des données d'utilisation.

Pour ce faire, procédez comme suit :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Accédez à la page des **paramètres de confidentialité**.
4. Sélectionnez **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.
5. Sous **Amélioration du produit**, sélectionnez **Envoyer des données d'utilisation anonymes**.

Remarque : Vous pouvez lire notre déclaration de confidentialité ici.

Chapitre
11

Assistance technique

Sujets :

- Où puis-je trouver les informations de version du produit ?
- Utilisation de l'outil d'assistance
- Débogage des problèmes de produit
- Arnaques par téléphone, et que faire si vous pensez en être victime

Vous pouvez trouver ici des informations qui vous aideront à résoudre vos problèmes techniques.

Si vous avez une question au sujet du produit ou un problème avec celui-ci, consultez la Communauté WithSecure et voyez si vous pouvez y trouver une réponse avant de contacter notre service client.

11.1 Où puis-je trouver les informations de version du produit ?

Notre équipe d'assistance peut vous demander la version de votre produit, si vous avez besoin de nous contacter.

Pour afficher les informations de version actuelles, procédez comme suit :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Assistance**.
4. Accédez à **Informations de version** pour en savoir plus sur le produit installé.

11.2 Utilisation de l'outil d'assistance

Avant de contacter le support, exécutez l'outil d'assistance pour collecter des informations de base sur le matériel, le système d'exploitation, la configuration réseau et les logiciels installés.

Si vous rencontrez des difficultés techniques avec votre produit de sécurité, vous pouvez créer un fichier WSDIAG et le transmettre à notre assistance technique. Le fichier contient des informations qui peuvent être utiles en cas de panne ou pour résoudre des problèmes propres à votre ordinateur.

Vous pouvez créer le fichier à l'aide de l'outil de support. L'outil rassemble des informations sur votre système et sa configuration. Les informations incluent les détails du produit, les journaux du système d'exploitation et les paramètres système. Notez qu'une partie des informations peut être confidentielle. Les informations recueillies sont stockées dans un fichier qui est enregistré sur le bureau de votre ordinateur.

Pour exécuter l'outil d'assistance, procédez comme suit :

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Assistance**.
4. Sélectionnez **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.
5. Sélectionnez **Exécuter l'outil d'assistance**.
6. Sélectionnez **Exécuter les diagnostics** dans la fenêtre **Outil d'assistance**.
   L'outil d'assistance démarre et affiche la progression de la collecte de données.

Lorsque la collecte est terminée, l'outil enregistre les données dans une archive sur votre bureau. Vous pouvez ensuite envoyer les données collectées (fichier de diagnostic) ici : https://www.withsecure.com/fr/support/contact-support/email-support.

Conseil : Si vous ne pouvez pas accéder à l'outil d'assistance via le produit lui-même, accédez à la page Web Outils d'assistance et sous **Outil d'assistance (WSDIAG) pour Windows**, sélectionnez **Télécharger** et enregistrez le fichier `wsdiag_standalone.exe`, par exemple dans votre dossier Téléchargements. Double-cliquez sur le fichier pour exécuter l'outil.

11.3 Débogage des problèmes de produit

La journalisation de débogage aide notre support client à analyser et à résoudre les problèmes, le cas échéant, dans le produit.

Vous pouvez donner temporairement à notre service client une autorisation spécifique pour analyser les problèmes du produit. Notez que les informations collectées par la journalisation de débogage peuvent être considérées comme sensibles.

WebView2 est une technologie utilisée pour intégrer du contenu Web dans des applications natives. Par exemple, notre page de connexion au compte utilise la technologie WebView2.

Si vous rencontrez des difficultés avec les vues Web intégrées, le débogueur de la console WebView2 peut aider notre support client à analyser les problèmes de vue Web pour vous.

Pour autoriser temporairement notre assistance à déboguer les problèmes liés au produit :

Remarque : Activez la **Journalisation du débogage** uniquement lorsque notre agent du service client vous le demande.

1. Ouvrez WithSecure Elements Agent à partir du menu **Démarrer** de Windows.
2. Sur la page principale, sélectionnez ⚙.
3. Sélectionnez **Modifier les paramètres**.

   Remarque : Vous devez disposer des droits d'administrateur pour modifier les paramètres.

4. Sous **Outils**, sélectionnez l'interrupteur à bascule pour activer la **Journalisation du débogage**. Une fois la journalisation de débogage activée, l'option **Débogueur de console WebView2** devient visible.
5. Si vous voulez activer le **Débogueur de console WebView2**, sélectionnez le commutateur à bascule. Une fois que vous entrez dans une vue Web intégrée, la fenêtre de la console s'ouvre.
6. Dès que notre service client a terminé l'analyse du problème, désactivez la **Journalisation du débogage** en sélectionnant l'interrupteur à bascule.

11.4 Arnaques par téléphone, et que faire si vous pensez en être victime

Les escroqueries par téléphone sont malheureusement en augmentation avec des escrocs utilisant l'ingénierie sociale pour cibler leurs victimes.

Cette rubrique a pour but de vous aider à identifier ces appels et, dans le pire des cas, si vous avez été ciblé, de vous donner des informations sur la marche à suivre.

Que sont les arnaques par téléphone ?

Ces appels téléphoniques peuvent être totalement imprévus ou émaner d'une publicité ou d'un lien qui ouvre une fenêtre contextuelle sur votre ordinateur. Celle-ci vous invite à contacter rapidement le numéro d'assistance technique indiqué ; elle peut s'afficher soudainement et il est difficile de s'en débarrasser.

Comment reconnaître une arnaque par téléphone ?

Ces types d'appels suivent généralement un certain schéma : les arnaqueurs prétendent que votre ordinateur a un problème, vous expliquent qu'il s'agit d'un virus (ce qui est faux), et vous manipulent afin de vous facturer un service qui n'existe pas non plus. Ils vous prennent au dépourvu et se servent de vos émotions. Voici le scénario de base :

- Les escrocs par téléphones prétendent provenir d'une entreprise bien connue, telle que Microsoft, votre banque ou même votre opérateur réseau. Comme ils utilisent un nom réputé, vous êtes plus en confiance. Ils semblent également bien informés et utilisent des termes techniques, ce qui les rend légitimes et crédibles.
- C'est quand le risque semble réel et que vous vous inquiétez des virus que vous donnez aux escrocs l'accès à votre ordinateur. Ils vous convainquent de les laisser installer une application qui leur donne accès à votre ordinateur à l'aide d'outils d'accès à distance.
- Une fois que les escrocs ont accès à votre ordinateur, ils font semblant d'éliminer un virus, et peuvent également vous demander vos informations d'identification. Une fois qu'ils ont « corrigé » le problème, ils vous demandent de vous connecter à votre banque en ligne ou de remplir un formulaire avec vos informations de carte bancaire. Les escrocs vous facturent le faux service, pour un montant bien supérieur à ce que vous pensiez. En réalité, il est difficile de savoir combien ils vous facturent réellement.

Que faire si vous pensez avoir été victime d'une arnaque

Si vous pensez être victime d'une arnaque et reconnaissez le scénario décrit ci-dessus, procédez comme suit :

- Agissez sans attendre.

- Contactez immédiatement votre société de carte bancaire ou votre banque, signalez l'arnaque et faites opposition sur toutes vos cartes bancaires ou de crédit. Si vous réagissez rapidement, l'établissement pourra peut-être même bloquer la transaction et vous restituer les sommes prélevées.
- Signalez l'arnaque aux autorités compétentes.
- Changez tous vos mots de passe sur chaque site Web ou service qui, selon vous, peut avoir été affecté.
- Désinstallez tout logiciel tiers inconnu.
- Exécutez une analyse complète sur votre ordinateur : ouvrez votre produit de sécurité, puis sélectionnez **Virus et menaces** > **Analyse complète de l'ordinateur**.

À retenir concernant les appels téléphoniques non sollicités

- Si vous recevez ce type d'appel, commencez par vous demander si vous l'avez sollicité.

  Remarque : Normalement, le support client vous appelle si vous l'avez déjà contacté et créé un ticket de support.

- Les sessions à distance sont une pratique d'assistance technique courante pour vous aider à résoudre des problèmes.

  A faire : N'autorisez les sessions à distance qu'avec des personnes ou des entreprises que vous connaissez et en qui vous avez confiance. N'autorisez les sessions à distance que si vous avez préalablement contacté votre fournisseur de services et que vous disposez d'un dossier d'assistance valide avec lui. De plus, conservez vos données d'accès à distance comme vous le feriez pour tout autre mot de passe.

- Ne donnez jamais accès à votre appareil à des inconnus. Donner à des escrocs un accès à distance équivaut effectivement à leur donner des droits d'administrateur sur votre ordinateur. Même si celui-ci dispose d'un logiciel antivirus, il ne pourra pas vous protéger, car les escrocs prennent le contrôle de votre ordinateur.
- Microsoft a informé ses utilisateurs qu'elle n'incluait jamais de numéro de téléphone dans les messages d'erreur ou d'avertissement de ses logiciels.
- Ne donnez jamais de vous-même vos informations d'identification ou de carte bancaire.
- Mettez immédiatement fin à l'appel.
- Ces types d'appels sont illégaux ; en cas de doute, signalez-les aux autorités compétentes en matière de lutte contre la fraude.

Comment le produit de sécurité peut-il vous aider ?

Une fois le produit de sécurité installé, votre ordinateur est protégé contre les virus, les chevaux de Troie et les ransomwares. Les fonctionnalités de protection de la navigation, de protection bancaire et de l'outil d'accès à distance ajoutent également une autre couche de sécurité et garantissent que vous pouvez naviguer et effectuer vos opérations bancaires en ligne en toute sécurité.

Si vous avez été ciblé et que vous avez déjà installé un produit de sécurité, vous pouvez immédiatement exécuter une analyse complète de l'ordinateur pour aider à détecter toutes les applications qui ont pu être installées par les escrocs ; celles-ci sont appelées applications potentiellement indésirables (PUA). Cependant, le produit n'est pas en mesure de vous protéger contre ces types d'arnaques téléphoniques.

Faites preuve de vigilance et prenez soin de vous.