ESET Cyber Security

Guide de l'utilisateur

Cliquez ici pour consulter la version de l'aide en ligne de ce document

Digital Security
Progress. Protected.

ESET Cyber Security a été développé par ESET, spol. s r.o.

Pour plus d’informations, consultez le site https://www.eset.com.

Assistance technique : https://support.eset.com

RÉV. 12/04/2024

ESET Cyber Security

ESET Cyber Security représente une nouvelle approche de sécurité informatique véritablement intégrée. La version la plus récente du moteur d'analyse ESET LiveGrid® utilise la vitesse et la précision pour assurer la sécurité de votre ordinateur.Le résultat est un système intelligent constamment en alerte, défendant votre ordinateur contre les attaques et les logiciels malveillants.

ESET Cyber Security est une solution complète de sécurité qui résulte de notre engagement à long terme d'offrir à la fois une protection maximale et un impact minimal sur le système. Les technologies avancées de ESET Cyber Security, basées sur l'intelligence artificielle, permettent une élimination proactive des infiltrations de virus, vers, chevaux de Troie, spyware, logiciels publicitaires, rootkits et autres attaques basées sur Internet sans handicaper les performances du système.

Nouveautés de la version 7

ESET Cyber Security version 7 contient les mises à jour et les améliorations suivantes :

- **Haute performance et plus grande stabilité** : architecture plus légère, chaque composant étant plus isolé. Ne démarre que lorsque c'est nécessaire et empêche l'application entière de se bloquer en cas de défaillance. De meilleures optimisations permettent une analyse plus rapide et plus efficace.

- **Compatibilité avec l'architecture ARM** : offre une prise en charge native des processeurs Apple basés sur l'architecture ARM. Les versions précédentes utilisaient Rosetta 2 pour la prise en charge de l'architecture ARM.

- **Nouveau design de l'interface utilisateur graphique** : comprend la prise en charge du mode sombre.

- **Programme d'installation multilingue** : comprend toutes les langues dans un seul fichier d'installation.

- **Mises à jour automatiques** : recherche des mises à jour, télécharge automatiquement de nouvelles versions et vous avertit à propos de chaque mise à jour.

- **Préférences de l'application** : cette section a été repensée et améliorée.

Pour plus d'informations sur les nouvelles fonctionnalités d'ESET Cyber Security, consultez cet article de la base de connaissances ESET.

Migration des paramètres

Depuis la version 7.2 et les versions ultérieures, les paramètres d'ESET Cyber Security version 6 sont automatiquement migrés vers la nouvelle version pendant la mise à niveau.

Après la migration, ESET Cyber Security affiche une notification sur l'écran d'accueil indiquant la migration des configurations : **Vos paramètres ont été transférés vers la nouvelle version**.

> Si vous avez déjà mis à niveau ESET Cyber Security de la version 6 vers la version 7 ou 7.1, vous pouvez toujours migrer vos configurations lors d'une mise à niveau vers une version ultérieure. Pour obtenir des instructions, consultez l'article de la base de connaissances ESET sur la migration.

Toutes les configurations disponibles dans la version 7.X seront migrées depuis la version 6, sauf les exceptions suivantes :

- Configurations des privilèges (non prises en charge dans la version 7)
- Serveur proxy personnalisé pour les mises à jour (le proxy personnalisé n'est pas pris en charge dans la version 7)
- Contenu en quarantaine
- Niveaux de nettoyage des analyses
- Profils cibles pour l'analyse à la demande

Les paramètres des fonctionnalités suivantes sont stockés dans le fichier de migration .xml et peuvent être chargés lorsque les fonctionnalités seront présentes dans la prochaine version d'ESET Cyber Security :

- Contrôle de périphérique
- Logs
- Protection de l’accès Web
- Mode de présentation

Configuration système requise

Pour garantir le fonctionnement correct, le système doit répondre à la configuration suivante :

	Configuration système :
Architecture du processeur	Intel 64-bit, M1, M2
Système d'exploitation	macOS Big Sur (11.0) et versions ultérieures
Mémoire	300 Mo
Espace disponible	600 Mo
Autre	Une connexion Internet est nécessaire pour activer ou mettre à niveau votre produit.

ESET Cyber Security version 7 offre une prise en charge native des puces Apple avec une architecture ARM.

Installation

Avant de commencer l'installation, fermez tous les programmes informatiques ouverts. ESET Cyber Security contient des composants qui peuvent être en conflit avec les autres antivirus installés sur votre ordinateur. Il est donc vivement recommandé de supprimer tous les autres antivirus pour éviter tout problème éventuel.

Pour lancer l’assistant d'installation, ouvrez le fichier que vous avez téléchargé depuis le site web ESET et double-cliquez sur l'icône **Installer ESET Cyber Security**. L'assistant d'installation vous guide tout au long de la configuration.

Le fichier d'installation d'ESET Cyber Security peut être téléchargé aussi depuis ESET HOME. Pour plus d'informations, consultez cet article de la base de connaissances ESET.

Intégration

Après l'installation d'ESET Cyber Security, l'**Assistant d'intégration** apparaît : il s'agit d'un ensemble d'écrans qui vous guident tout au long des étapes recommandées et obligatoires pour un fonctionnement optimal d'ESET Cyber Security.

1. Activez **Paramètres de protection recommandés**, sélectionnez vos options préférées, puis cliquez sur **Continuer**. Pour plus d'informations sur **ESET LiveGrid®** ou les **applications potentiellement indésirables**, consultez le glossaire d'ESET.

2. Étape obligatoire : Activer les **extensions système ESET** Suivez les instructions à l'écran pour continuer la configuration.

3. Étape obligatoire : Ajouter une **configuration de proxy**. Dans la fenêtre d'alerte, cliquez sur **Autoriser**.

4. Étape obligatoire : Accorder à ESET Cyber Security l'**accès complet au disque**. Suivez les instructions à l'écran et autorisez l'accès complet au disque.

5. L'assistant vous invite ensuite à **activer ESET Cyber Security**. Vous trouverez plusieurs options d'activation dans le chapitre Activation.

6. **Autoriser les notifications**. Il est recommandé d'autoriser les notifications à rester informées des menaces détectées sur votre système.

Ignorer l'assistant d'intégration ESET Cyber Security.
En cliquant sur **Configurer plus tard**, vous pouvez ignorer la configuration obligatoire. Sachez toutefois que votre protection ne sera que partiellement fonctionnelle.

Redémarrage de l'assistant d'intégration
Ouvrez **Finder** > **Applications** > cliquez en maintenant la touche Contrôle enfoncée (ou cliquez avec le bouton droit) sur l'icône **ESET Cyber Security**, sélectionnez **Afficher le contenu du paquet** dans le menu contextuel, puis ouvrez **Contents** > **Helpers** > **Intégration**. Vous pouvez également configurer manuellement les paramètres de sécurité obligatoires en lisant les chapitres Autoriser les extensions système et Autoriser l'accès complet au disque.

Après l'installation de ESET Cyber Security, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse** > **Analyser maintenant**. Consultez la section Analyse de l'ordinateur à la demande pour plus d'informations sur les analyses de l'ordinateur à la demande.

Autoriser les extensions système

Si vous installez ESET Cyber Security pour la première fois, vous devez autoriser les **extensions système** pour être protégé par ESET Cyber Security. Cette opération peut être effectuée dans le cadre du processus d'intégration. Vous pouvez également **autoriser les extensions système** manuellement en suivant les étapes ci-dessous :

Si vous disposez de macOS Ventura (13.x) et versions ultérieures, procédez comme suit

1. Ouvrez **Paramètres système**.
2. Sélectionnez **Confidentialité et sécurité** dans le menu de gauche.
3. Faites défiler la section **Sécurité**, puis cliquez sur le bouton **Détails** sous le message « Certains logiciels système requièrent votre attention avant de pouvoir être utilisés ».

Si le message **« Certains logiciels système requièrent votre attention avant de pouvoir être utilisés »** et que le **bouton** Détails ne sont pas disponibles, les extensions système ont été précédemment autorisées et aucune action supplémentaire n'est nécessaire.

4. Utilisez le **Touch ID** ou cliquez sur **Utiliser un mot de passe**, saisissez votre **nom d'utilisateur** et **votre mot de passe**, puis cliquez sur **Déverrouiller**.
5. Activez **Protection en temps réel du système de fichiers ESET** et **Protection Internet et messagerie ESET** en cliquant sur les boutons bascules.
6. Cliquez sur **OK**.
7. Lorsque l'alerte **Protection Internet et messagerie ESET** s'affiche en vous invitant d'**ajouter une configuration proxy**, sélectionnez **Autoriser**. Si vous n'autorisez pas la configuration du proxy lorsque l'alerte s'affiche, vous devez redémarrer votre ordinateur pour lancer l'alerte et autoriser de nouveau la configuration du proxy.
Pour obtenir un guide détaillé, consultez notre article de la base de connaissances. Les articles de la base de connaissances ne sont pas disponibles dans toutes les langues.

Si vous disposez de macOS Monterey (12.x) et versions antérieures, procédez comme suit

1. Ouvrir **Préférences Système**.
2. Sélectionnez **Sécurité et confidentialité**.
3. Cliquez sur l'icône représentant un cadenas dans la partie inférieure gauche pour autoriser les modifications dans la fenêtre des paramètres.
4. Utilisez le **Touch ID** ou cliquez sur **Utiliser un mot de passe,** saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Déverrouiller**.
5. Cliquez sur **Détails**.
6. Sélectionnez toutes les options **ESET Cyber Security**.
7. Cliquez sur **OK**.

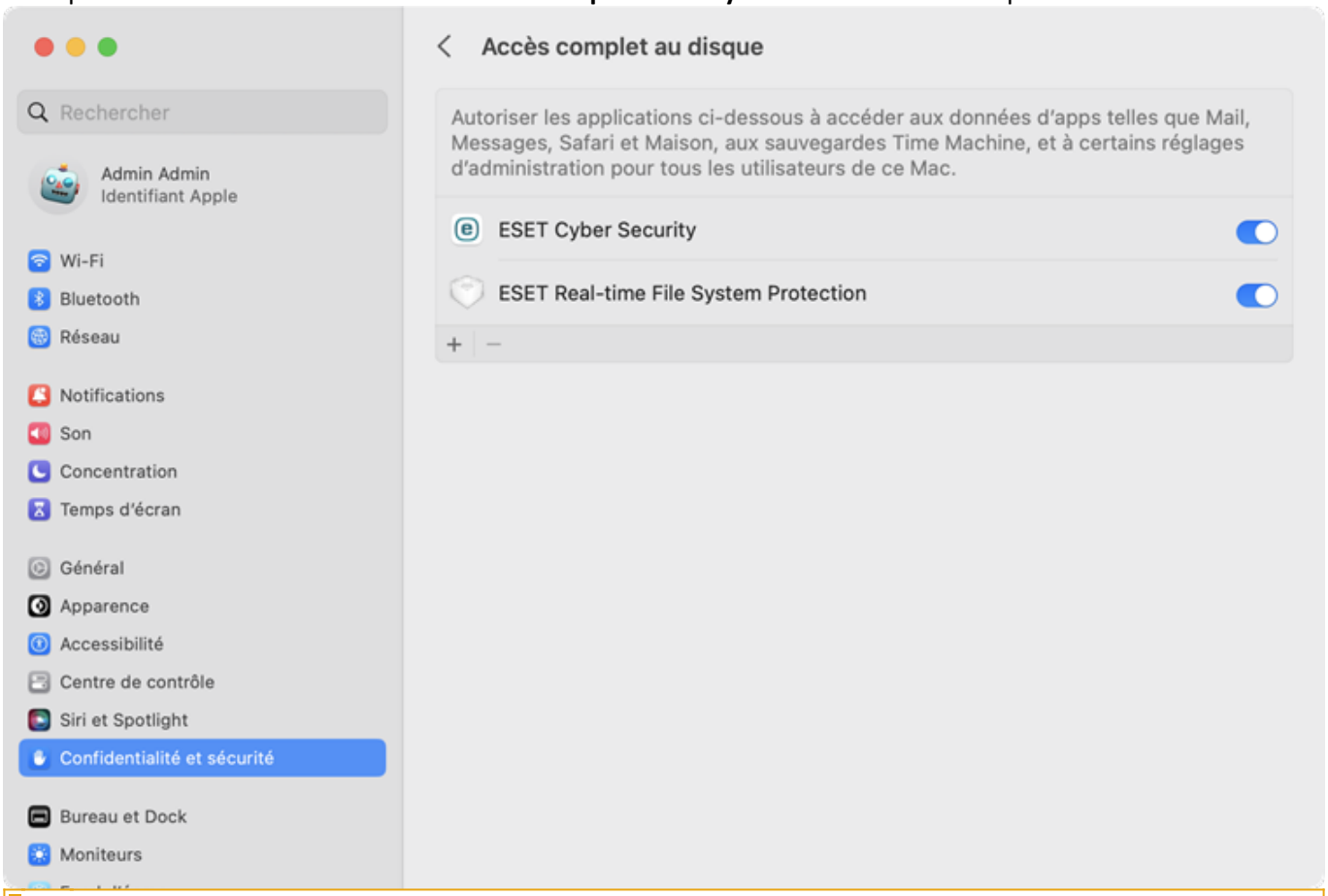
Redémarrage de l'assistant d'intégration
Ouvrez **Finder** > **Applications** > cliquez en maintenant la touche Contrôle enfoncée (ou cliquez avec le bouton droit) sur l'icône **ESET Cyber Security**, sélectionnez **Afficher le contenu du paquet** dans le menu contextuel, puis ouvrez **Contents** > **Helpers** > **Intégration**. L'assistant d'intégration vous guide tout au long des étapes nécessaires pour une protection complète d'ESET Cyber Security.

Autoriser l’accès complet au disque

Si vous installez ESET Cyber Security pour la première fois, vous devez autoriser l'**accès complet au disque** pour être protégé par ESET Cyber Security. Cette opération peut être effectuée dans le cadre du processus d'intégration. Vous pouvez également **autoriser l'accès complet au disque** manuellement en suivant les étapes ci-dessous :

Si vous disposez de macOS Ventura (13.x) et versions ultérieures, procédez comme suit

1. Ouvrez **Paramètres système**.
2. Sélectionnez **Confidentialité et sécurité** dans le menu de gauche.
3. Cliquez sur l'option **Accès complet au disque**, puis cliquez sur le bouton bascule ESET Cyber Security pour l'activer.
4. Utilisez le **Touch ID** ou cliquez sur **Utiliser un mot de passe**, saisissez votre nom d’utilisateur et votre mot de passe, puis cliquez sur **Déverrouiller**.
5. Si une invite de redémarrage ESET Cyber Security s'affiche, cliquez sur **Ultérieurement**.
6. Cliquez sur le bouton bascule **Protection en temps réel du système de fichiers ESET** pour l'activer.



Si l'option **Protection en temps réel du système de fichiers** n'est pas disponible, vous devez autoriser les extensions système pour votre produit ESET.

7. Une fois les extensions système et l'accès complet au disque activés, redémarrez votre ordinateur. Pour plus d’informations, consultez notre article de la base de connaissances.

Si vous disposez de macOS Monterey (12.x) et versions antérieures, procédez comme suit

1. Ouvrir **Préférences Système**.
2. Accédez à l'onglet **Confidentialité** et sélectionnez **Accès complet au disque** dans le menu de gauche.
3. Cliquez sur l'icône représentant un cadenas dans la partie inférieure gauche pour autoriser les modifications dans la fenêtre des paramètres.
4. Utilisez le **Touch ID** ou cliquez sur **Utiliser un mot de passe**, saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Déverrouiller**.
5. Sélectionnez **ESET Cyber Security** dans la liste.
6. Une notification de redémarrage d'ESET Cyber Security s'affiche. Cliquez sur **Ultérieurement**.
7. Sélectionnez **Protection en temps réel du système de fichiers ESET** dans la liste.

Si l'option **Protection en temps réel du système de fichiers** n'est pas disponible, vous devez autoriser les extensions système pour votre produit ESET.

8. Cliquez sur **Redémarrer** dans la fenêtre d'alerte pour redémarrer ESET Cyber Security et refléter les modifications, ou redémarrez votre ordinateur. Pour plus d'informations, consultez notre article de la base de connaissances.

Redémarrage de l'assistant d'intégration
Ouvrez **Finder** > **Applications** > cliquez en maintenant la touche Contrôle enfoncée (ou cliquez avec le bouton droit) sur l'icône **ESET Cyber Security**, sélectionnez **Afficher le contenu du paquet** dans le menu contextuel, puis ouvrez **Contents** > **Helpers** > **Intégration**. L'assistant d'intégration vous guide tout au long des étapes nécessaires pour une protection complète d'ESET Cyber Security.

Activation du produit

La fenêtre **Activation du produit** s'affiche en tant qu'une des étapes d'intégration. Si l'activation du produit n'a pas été effectuée pendant l'intégration, elle est accessible à tout moment dans l'application ESET Cyber Security. Pour lancer l'application, cliquez sur l'icône ESET Cyber Security située dans la barre de menus macOS (dans la partie supérieure de l'écran), puis sélectionnez Afficher ESET Cyber Security. L'alerte **Activation du produit** s'affiche dans la section **Vue d'ensemble**. L'alerte contient un lien vers la **boîte de dialogue d'activation**. Une fois la boîte de dialogue d'activation ouverte, indiquez les informations suivantes :

- **Activer avec une clé d'activation** : saisissez votre clé d'activation, qui identifie le titulaire de l'abonnement et active ce dernier. La clé d'activation est une chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX ou XXXX-XXXXXXXX.
- **Version d'essai gratuite** : sélectionnez cette option pour évaluer ESET Cyber Security avant l'achat. Saisissez vos informations, puis cliquez sur **Enregistrer** pour activer ESET Cyber Security pour une période limitée. Les versions d'essai ne peuvent être activées qu'une seule fois par client.
- **Acheter un abonnement** : cliquez sur cette option pour acheter un abonnement. Vous êtes alors redirigé vers le site web de votre distributeur local ESET.
- Utiliser votre compte **ESET HOME** : connectez-vous à votre compte ESET HOME et choisissez un abonnement pour activer le produit ESET sur votre appareil.
- **Activer ultérieurement** : cliquez sur cette option si vous ne souhaitez pas procéder à l'activation pour l'instant.

Pour plus d'informations sur l'emplacement des clés d'activation, consultez cet article de la base de connaissances ESET.

Où puis-je trouver mon abonnement ?

Si vous avez acheté un abonnement en ligne, vous avez reçu un e-mail d'ESET contenant votre clé d'activation (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX), votre ID public (xxx-xxx-xxx), le nom du produit (ou la liste des produits) et la quantité. Si vous avez acheté le produit au détail dans un coffret, la clé d'activation se trouve à l'intérieur ou au dos du coffret.

Si votre clé d'activation ne fonctionne pas, consultez cet article de la base de connaissances ESET.

Désinstaller

Pour supprimer ESET Cyber Security, procédez comme suit :

1.Lancez le **Finder**.

2.Ouvrez le dossier **Applications** sur le disque dur.

3.Cliquez en maintenant la touche Contrôle enfoncée (ou cliquez avec le bouton droit) sur l'icône **ESET Cyber Security**.

4.Sélectionnez **Afficher le contenu du paquet** dans le menu contextuel.

5.Ouvrez le dossier **Contents** > **Helpers** et double-cliquez sur l'icône **Uninstaller**.

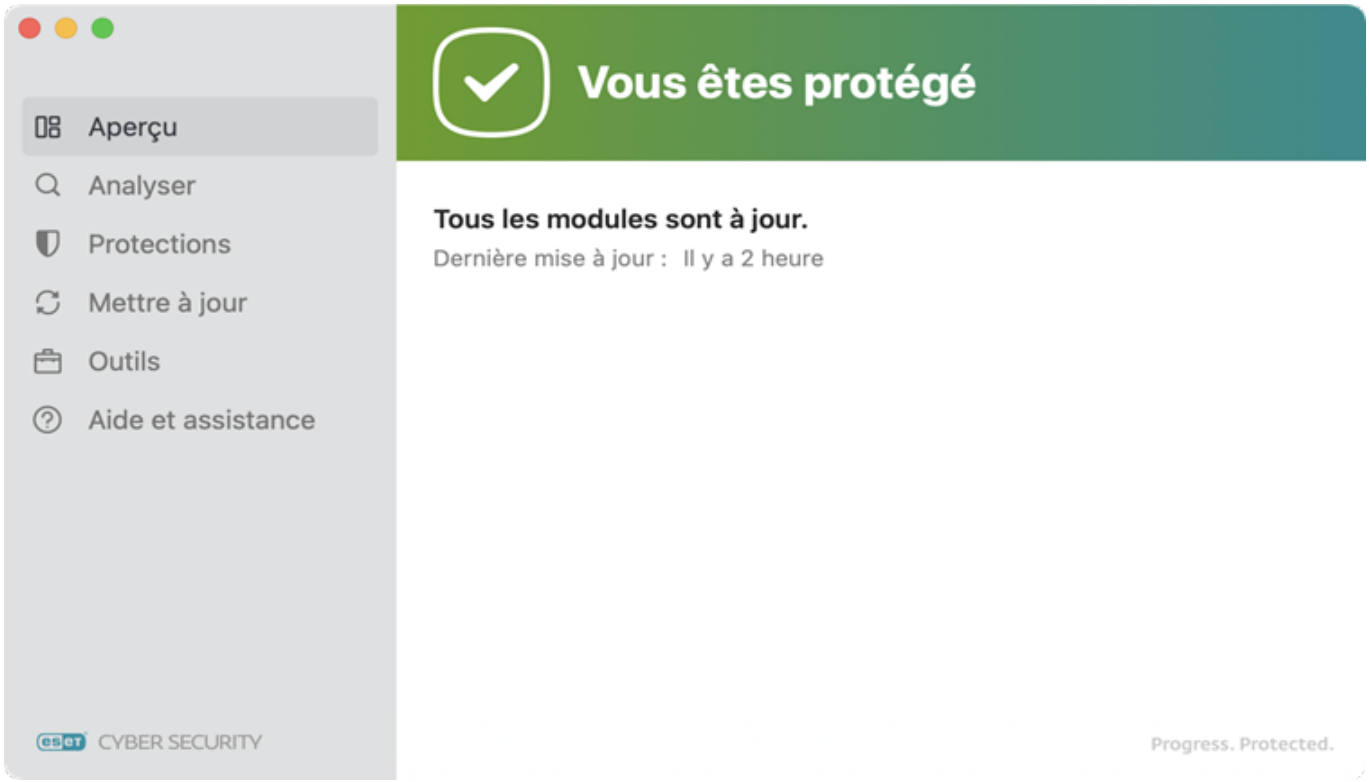
Si vous avez conservé le fichier d'installation d'ESET Cyber Security (.dmg), ouvrez-le, puis double-cliquez sur **Désinstaller**.

Utilisation d'ESET Cyber Security

La fenêtre principale d'ESET Cyber Security est divisée en deux sections principales. La fenêtre principale de droite affiche les informations correspondant à l'option sélectionnée dans le menu principal à gauche.

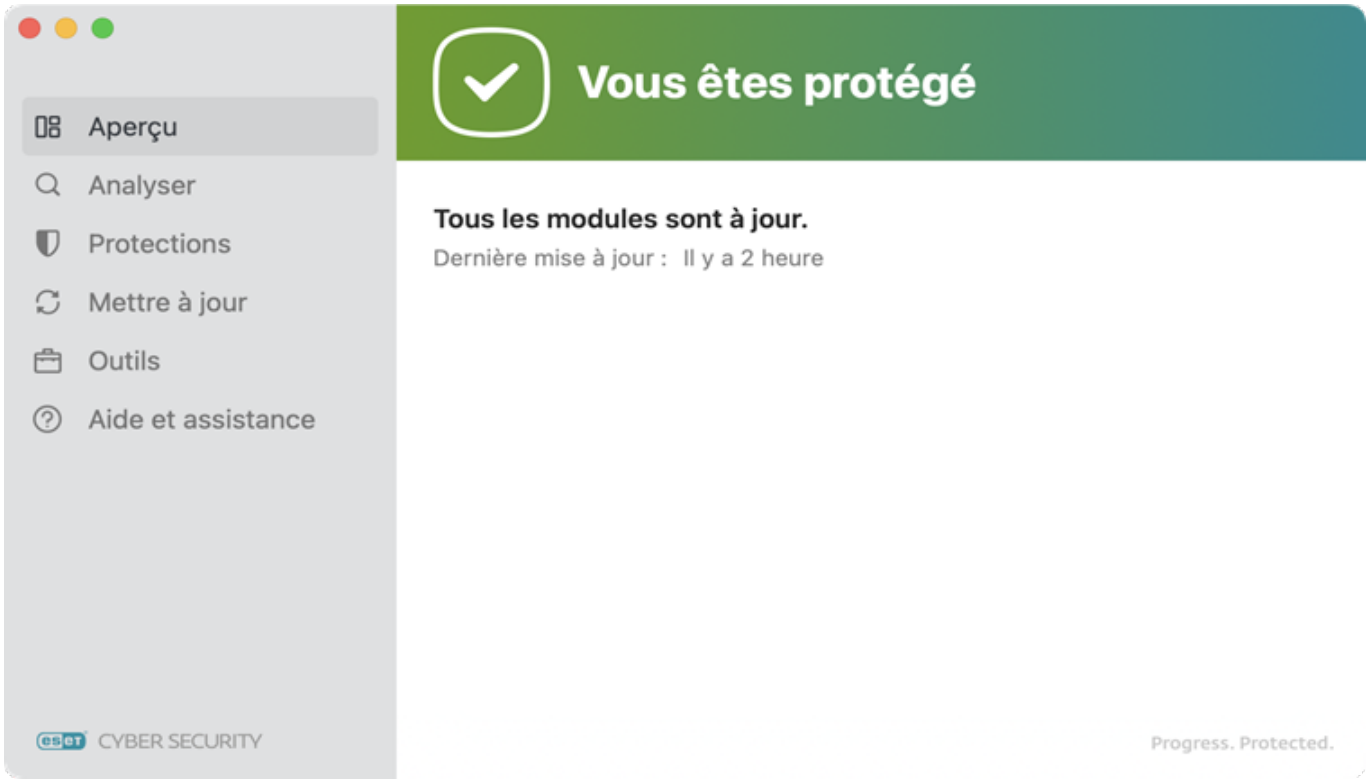
Vous pouvez accéder aux sections suivantes à partir du menu principal :

- **Vue d'ensemble** :fournit un résumé de l'état des informations sur le fonctionnement des modules ESET Cyber Security.
- **Analyse de l'ordinateur** : permet d'analyser tous les disques locaux ou d'exécuter une analyse personnalisée.
- **Protections** : permet de régler le niveau de sécurité de votre ordinateur.
- **Mise à jour** : affiche des informations sur les mises à jour des modules de détection.
- **Outils** : permet d'accéder aux fichiers journaux et à la quarantaine.
- **Aide et assistance** : permet d'accéder aux fichiers d'aide, à la base de connaissances ESET, au formulaire de demande d'assistance et à d'autres informations sur le programme.



Vérification de l'état de la protection

Pour afficher l'état de la protection, cliquez sur **Aperçu** dans le menu principal. La fenêtre principale affiche un résumé de l'état de fonctionnement des modules de ESET Cyber Security.



Aide et assistance

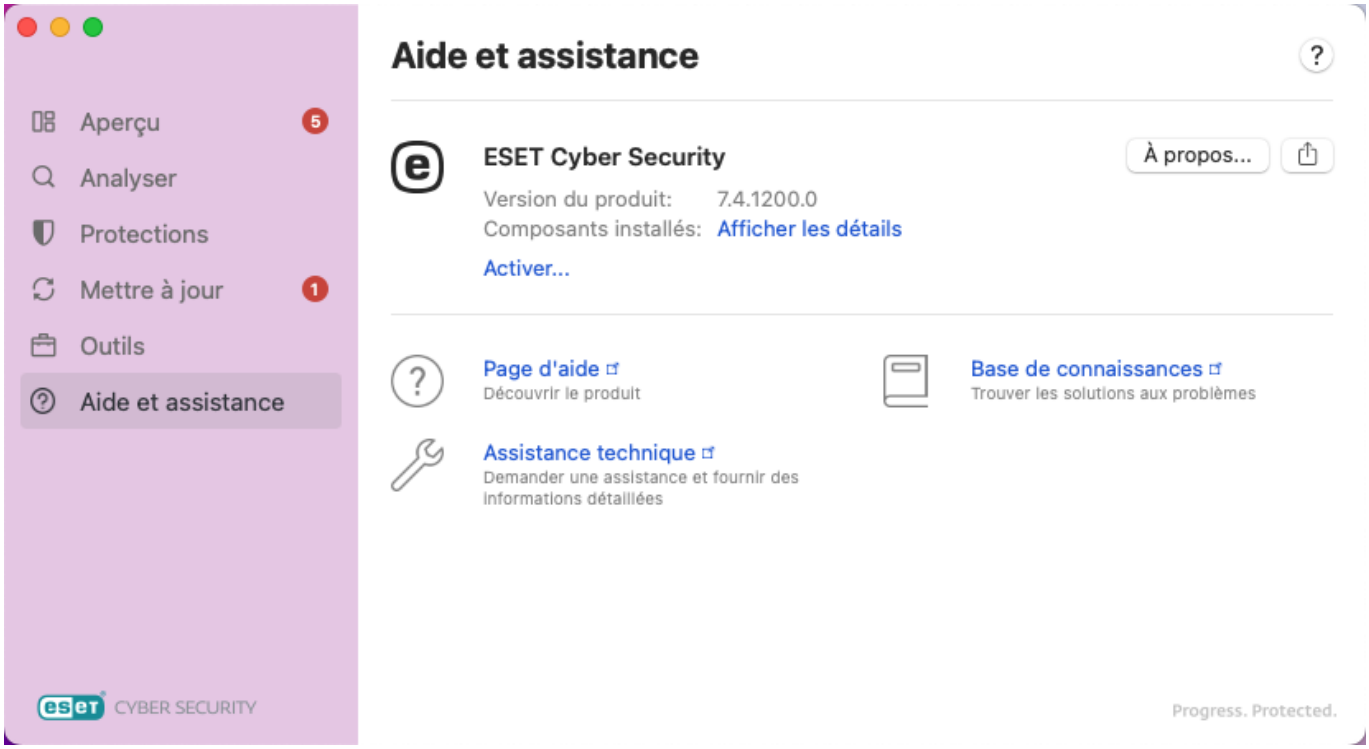
ESET Cyber Security contient des outils de dépannage et des informations d'assistance qui vous aideront à résoudre les problèmes que vous pouvez rencontrer. La section Aide et assistance se trouve dans la fenêtre principale de l'application. Pour afficher la liste des composants installés, cliquez sur **Afficher les détails** en regard de l'option **Composants installés**. Pour copier la liste dans le Presse-papiers, cliquez avec le bouton droit à n'importe quel endroit dans la fenêtre Composants installés, puis cliquez sur **Copier tout**. Ce procédé peut être utile pour la résolution des problèmes ou lorsque vous contactez l'assistance technique.

La version du produit **ESET Cyber Security** s'affiche, ainsi que l'ID d'abonnement du produit. Une option permet de changer d'abonnement. Cliquez sur cette option pour ouvrir la fenêtre d'activation et activer votre produit. En cliquant sur le bouton **À propos**, vous pouvez afficher d'autres détails sur ESET Cyber Security.

Page d'aide – Cliquez sur ce lien pour lancer les pages d'aide ESET Cyber Security.

Assistance technique : si vous ne pouvez pas résoudre le problème à l'aide des pages d'aide, contactez l'assistance technique ESET.

Base de connaissances – La base de connaissances ESET contient des réponses aux questions les plus fréquentes et les solutions recommandées pour résoudre divers problèmes. Régulièrement mise à jour par les spécialistes techniques d'ESET, la base de connaissances est l'outil le plus puissant pour résoudre différents problèmes.



Importer et exporter les paramètres

Pour importer une configuration existante ou exporter votre configuration ESET Cyber Security, ouvrez la fenêtre principale de l'application ESET Cyber Security, puis, dans la barre de menus macOS située dans la partie supérieure gauche de l'écran, cliquez sur **Fichier** > **Importer ou exporter les paramètres**.

Ces opérations sont utiles si vous devez sauvegarder votre configuration actuelle de ESET Cyber Security pour l'utiliser ultérieurement. Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration préférée de ESET Cyber Security sur plusieurs systèmes. Il est facile d'importer un fichier de configuration afin de transférer les paramètres souhaités.

Pour importer une configuration, sélectionnez **Importer les paramètres** pour accéder au fichier de configuration à importer. Pour procéder à l'exportation, sélectionnez **Exporter les paramètres**, puis utilisez le navigateur pour sélectionner l'emplacement d'enregistrement du fichier de configuration sur votre navigateur.

Raccourcis clavier

Vous pouvez utiliser les raccourcis clavier suivants dans ESET Cyber Security :

- cmd+, : affiche les préférences de ESET Cyber Security.
- cmd+Q : masque la fenêtre principale de ESET Cyber Security. Vous pouvez ouvrir l'application en cliquant sur l'icône ESET Cyber Security dans la barre de menus macOS (en haut de l'écran), puis en sélectionnant **Afficher ESET Cyber Security**.
- cmd+W : ferme la fenêtre principale de ESET Cyber Security.

Que faire lorsque le programme ne fonctionne pas correctement

Lorsque tous les modules fonctionnent correctement, un en-tête vert **Vous être protégé** s'affiche dans la section **Vue d'ensemble**. En cas de défaillance d'un module, un en-tête rouge **Alerte de sécurité** ou un en-tête orange **Attention requise** s'affiche. ESET Cyber Security affiche des informations supplémentaires sur le module et une suggestion de solution aux problèmes. Pour changer l'état des différents modules, cliquez sur le lien bleu affiché sous chaque message de notification.

Si vous ne parvenez pas à résoudre le problème à l'aide des solutions suggérées, effectuez des recherches dans la base de connaissances ESET ou contactez l'assistance technique ESET.

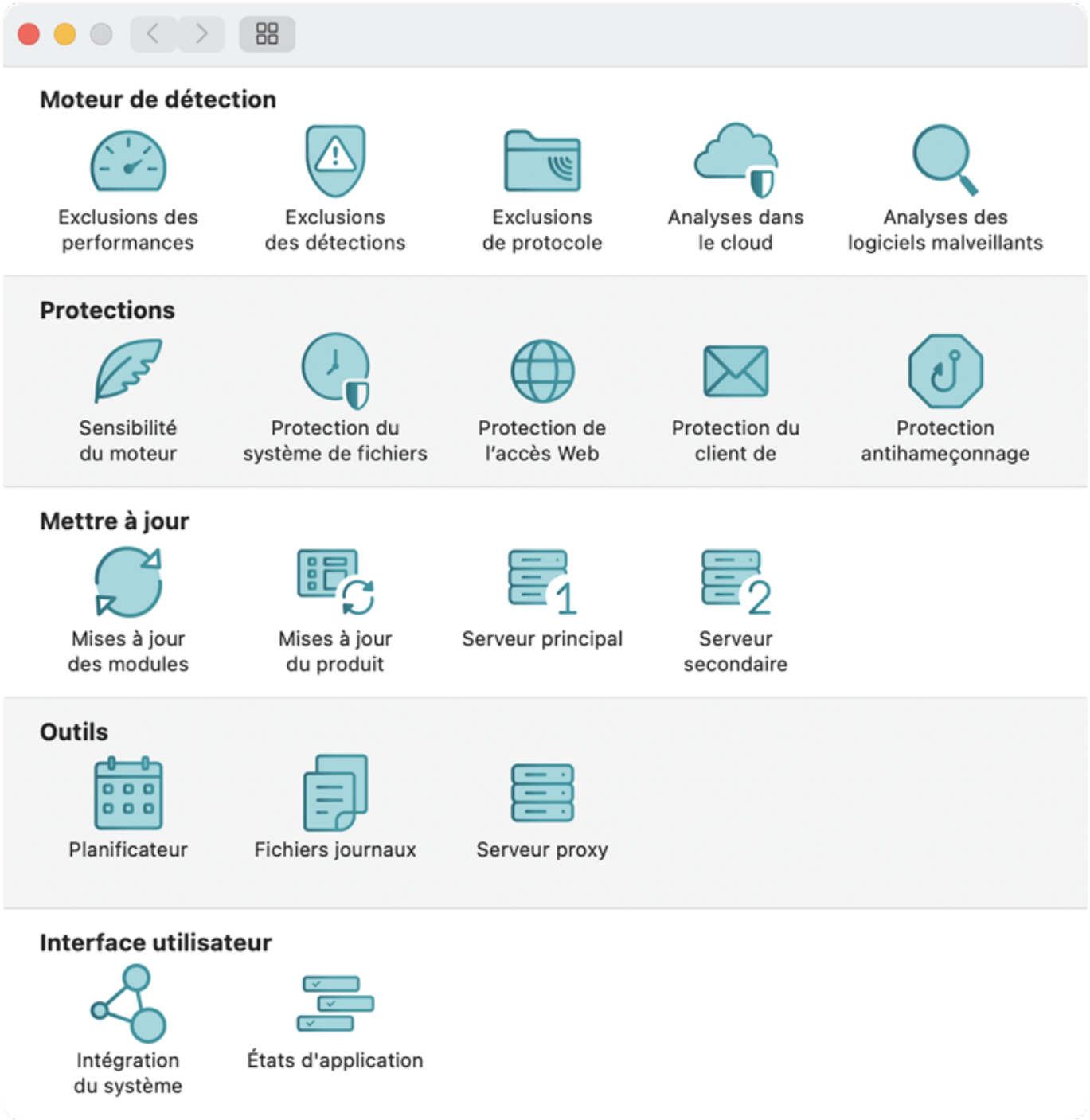
Préférences de l'application

Pour modifier les paramètres avancés d'ESET Cyber Security, ouvrez les **Préférences de l'application** en utilisant cmd+, ou en cliquant sur ESET Cyber Security dans la barre de menus macOS et en sélectionnant **Préférences** (Paramètres).

Vous pouvez configurer les paramètres des modules des catégories suivantes :

- Moteur de détection
- Protections
- Mettre à jour
- Outils

- Interface utilisateur



Moteur de détection

Le moteur de détection protège des attaques malveillantes contre le système en contrôlant les fichiers. Par exemple, si un objet classé comme logiciel malveillant est détecté, la correction commence. Le moteur de détection peut l'éliminer en le bloquant dans un premier temps, puis en le nettoyant, en le supprimant ou en le mettant en quarantaine.

Pour modifier les paramètres avancés du **moteur de détection** d'ESET Cyber Security, ouvrez les **Préférences de l'application** en utilisant cmd+, ou en cliquant sur ESET Cyber Security dans la barre de menus macOS et en sélectionnant **Préférences** (Paramètres).

Exclusions des performances

Dans la section **Exclusions des performances**, vous pouvez exclure de l'analyse certains fichiers/dossiers, applications ou adresses IP/IPv6. Si vous excluez des chemins (dossiers) de l'analyse, vous pouvez considérablement réduire le temps nécessaire pour analyser le système afin de rechercher des logiciels malveillants.

-  : crée une exclusion. Saisissez le chemin d'accès à un objet.
-  : supprime les entrées sélectionnées.

Vous ne devez exclure des fichiers de l'analyse que lorsque vous rencontrez de graves problèmes avec la protection en temps réel, car l'exclusion de fichiers de l'analyse diminue la protection globale.

Exclusions des détections

Permettent d'exclure des objets du nettoyage en filtrant le nom de la détection, le chemin de l'objet ou son hachage.

Lors de la mise en place d'exclusions de détection, des critères d'exclusion particuliers doivent être spécifiés. Un nom de détection ou un hachage SHA-1 valide doit être fourni. Pour un nom de détection ou un hachage SHA-1 valide, consultez les fichiers journaux, puis sélectionnez Détections dans le menu déroulant Fichiers journaux. Cela s'avère utilise lorsqu'un échantillon faux positif est détecté dans ESET Cyber Security. Les exclusions pour les infiltrations réelles sont très dangereuses ; envisagez d'exclure uniquement les fichiers ou répertoires pendant une période temporaire. Les exclusions s'appliquent également aux applications potentiellement indésirables, aux applications potentiellement dangereuses et aux applications suspectes.

Les types de **critères d'exclusion** suivants sont proposés :

- **Fichier exact** – Permet d'exclure un fichier selon le hachage spécifié SHA-1, indépendamment du type de fichier, de l'emplacement ou de l'extension de celui-ci.
- **Détection** – Exclure chaque fichier par son nom de détection.
- **Chemin et détection** – Exclure chaque fichier par nom de détection et chemin, notamment le nom de fichier (`file:///Users/documentation/Downloads/eicar_com.zip`, par exemple).

Vous ne devez utiliser les exclusions de détection que si vous rencontrez de sérieux problèmes de détection d'un logiciel malveillant, par exemple, car l'exclusion d'un logiciel malveillant de l'analyse diminue la protection globale.

Exclusions de protocole

Les adresses figurant dans cette listes d'exclusions sont exclues du filtrage du contenu des protocoles. Il est recommandé d'utiliser cette option uniquement pour les applications ou les adresses que vous savez être fiables.

Analyses dans le cloud

Activation du système de réputation ESET LiveGrid® (recommandé)

Le système de réputation ESET LiveGrid® améliore l'efficacité des solutions de protection contre les logiciels malveillants en comparant les fichiers analysés à une base de données d'éléments mis en liste blanche et noire dans le cloud.

Activation du système de commentaires ESET LiveGrid®

Les données sont envoyées au laboratoire ESET Virus Lab pour des analyses plus poussées.

Soumission des échantillons

Soumission automatique des échantillons infectés : Selon l'option sélectionnée, des échantillons infectés peuvent être soumis au laboratoire ESET Research Lab pour analyse et améliorer les prochaines détections.

- Tous les échantillons détectés
- Tous les échantillons à l'exception des documents
- Ne pas envoyer

Soumission automatique des échantillons suspects : Les échantillons suspects ressemblant à des menaces et des échantillons aux caractéristiques ou au comportement inhabituels peuvent être envoyés pour analyse au laboratoire ESET Research Lab.

- Exécutables – Comprend les fichiers exécutables suivants : .exe, .dll, .sys
- Archives – Comprend les types de fichiers d'archive suivants : .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- Scripts – Comprend les types de fichiers de script suivants : .bat, .cmd, .hta, .vbs, .js, .ps1
- Documents – Comprend les documents créés dans Microsoft Office, Libre Office ou d’autres outils de bureautiques, ou des fichiers PDF avec du contenu actif.
- Autres – Comprend les types de fichiers suivants : .jar, .reg, .msi, .swf, .lnk

Exclusions de la soumission automatique : Les fichiers exclus ne seront pas envoyés au laboratoire ESET Research Lab même s’ils contiennent du code suspect.

Envoyer les rapports de défaillance et les données de diagnostic

Permet d'envoyer des données telles que des rapports de défaillance et des fichiers d'image mémoire ou des modules.

Participez à l'amélioration du produit en envoyant des statistiques d'utilisation anonymes

Autorise ESET à collecter des informations anonymes concernant les nouvelles menaces détectées (nom, date et l'heure de détection, méthode de détection et métadonnées associées), les fichiers analysés (hachage, nom du fichier, origine du fichier, télémétrie), les URL suspectes et bloquées et la version et la configuration du produit, notamment des informations sur votre système.

Courriel de contact (facultative)

Votre adresse électronique peut être envoyée avec les fichiers suspects. Nous pourrons l'utiliser pour vous contacter si des informations complémentaires sont nécessaires pour l'analyse. Veuillez noter que vous ne recevrez pas de réponse de la part de ESET sauf si d'autres renseignements sont requis.

Analyses des logiciels malveillants

L'analyseur à la demande est une partie importante de votre solution antivirus. Il permet d'analyser des fichiers et des répertoires de votre ordinateur. Pour votre sécurité, il est essentiel que l'ordinateur soit analysé régulièrement dans le cadre de mesures de sécurité routinières, pas seulement en cas de suspicion d'une infection. Dans la section **Analyses des logiciels malveillants**, vous pouvez configurer des options pour les profils d'analyse à la demande :

Liste des profils – Pour créer un profil ou supprimer un profil existant, cliquez sur  ou  . Lors de l'ajout d'un nouveau profil, saisissez un nom, puis cliquez sur **OK**. Le nouveau profil s'affiche dans le menu déroulant Profil sélectionné qui répertorie les profils d'analyse existants.

Paramètres ThreatSense – Options de configuration des profils d'analyse, telles que les extensions de fichier que vous souhaitez contrôler, les objets à analyser, les méthodes de détection utilisées, etc.

Protections

Pour modifier les paramètres de **protection** avancés d'ESET Cyber Security, ouvrez les **Préférences de l'application** en utilisant cmd+, ou en cliquant sur ESET Cyber Security dans la barre de menus macOS et en sélectionnant **Préférences** (Paramètres).

Sensibilité du moteur

La sensibilité du moteur permet de configurer les rapports et les niveaux de protection des catégories suivantes pour tous les modules de protection.

- **Logiciel malveillant** : code malveillant qui fait partie des fichiers existants sur votre ordinateur.

- **Applications potentiellement indésirables** : un grayware (ou application potentiellement indésirable) est un type de logiciel dont l'objectif n'est pas nécessairement malveillant, contrairement à d'autres types de logiciels malveillants comme les virus et les chevaux de Troie. Il peut toutefois installer d'autres logiciels non souhaités, modifier le comportement de l'appareil numérique, ou effectuer des activités non approuvées ou non attendues par l'utilisateur. Pour plus d'informations sur ce type de protection,

reportez-vous au glossaire.

• **Applications suspectes** : ces applications comprennent les programmes compressés à l'aide d'empaqueteurs ou de protecteurs. Ces types de protections sont souvent exploités par des créateurs de logiciels malveillants pour contourner les détections. Un empaqueteur est un programme exécutable compressé auto-extractible qui regroupe plusieurs sortes de logiciels malveillants dans une seule archive. Les empaqueteurs les plus courants sont au format UPX, PE_Compact, PKLite ou ASPack. Un même logiciel malveillant peut être détecté différemment suivant l'empaqueteur dans lequel il est compressé. Les empaqueteurs ont également la possiblité de modifier leur « signature » au fil du temps, rendant ainsi le logiciel malveillant plus difficile à détecter et à supprimer.

• **Applications potentiellement dangereuses** : cette appellation fait référence à des logiciels commerciaux légitimes qui peuvent être mis à profit par des pirates, s'ils ont été installés à l'insu de l'utilisateur. Cette classification inclut des programmes tels que des outils d'accès à distance. Cette option est désactivée par défaut.

Protection du système de fichiers

La protection en temps réel du système de fichiers utilise la technologie ESET LiveGrid® (décrite dans la section Configuration des paramètres du moteur ThreatSense) et peut être différente pour les nouveaux fichiers et les fichiers existants. Les fichiers nouvellement créés peuvent être plus précisément contrôlés.

Vous pouvez exclure les types de supports suivants de l’analyseur Real-time :

• **Disques locaux** : disques durs système

• **Supports amovibles** : périphériques USB, appareils Bluetooth, etc.

• **Supports réseau** : tous les lecteurs mappés

Par défaut, tous les fichiers sont analysés à l'**ouverture** et à la **création**. ESET recommande de conserver ces paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur :

Vous pouvez également exclure des processus spécifiques de l'analyse.

ESET recommande d'utiliser les paramètres par défaut et de ne modifier les exclusions d'analyse que dans des cas spécifiques, par exemple lorsque l'analyse de certains supports ralentit de manière significative les transferts de données.

Protection de l'accès Web

La protection de l'accès Web surveille la communication entre les navigateurs Web et les serveurs distants pour la conformité avec le protocole HTTP (Hypertext Transfer Protocol).

Vous pouvez réaliser le filtrage internet en définissant les numéros de port pour la communication HTTP et les adresses URL.

Protocoles Web

Dans la section Protocoles Web, vous pouvez activer ou désactiver le contrôle de protocole HTTP et définir les

numéros de port utilisés pour les communications HTTP. Par défaut, les numéros de port 80, 8080 et 3128 sont prédéfinis.

Gestion d'adresse URL

Cette section permet de spécifier des adresses HTTP à bloquer, à autoriser ou à exclure du contrôle. Les sites web figurant dans la liste des adresses bloquées ne seront pas accessibles. Les sites Web répertoriés dans la liste des adresses exclues sont accessibles sans recherche de code malveillant.

Pour activer une liste d'adresses autorisées, bloquées ou exclues, sélectionnez-la et activez l'option **Liste active**. Si vous souhaitez être averti lors de la saisie d'une adresse figurant dans la liste actuelle, sélectionnez l'option **Notifier lors de l'application**.

Dans n'importe quelle liste, vous pouvez utiliser les symboles spéciaux *** (astérisque) et *?* (point d'interrogation). L'astérisque remplace toute chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Faites très attention lors la définition des adresses exclues, car la liste ne doit contenir que des adresses fiables et sûres. De même, vous devez veiller à utiliser correctement les symboles * et ? dans cette liste.

Protection du client de messagerie

Protection du client de messagerie : permet de contrôler la communication par courrier électronique effectuée via les protocoles POP3 et IMAP. Lorsqu'il examine les messages entrants, ESET Cyber Security utilise toutes les méthodes d'analyse avancées comprises dans le moteur d'analyse ThreatSense. L'analyse des communications via le protocole POP3 et IMAP est indépendante du client de messagerie utilisé. Les paramètres suivants sont disponibles :

Protocoles de messagerie

Vous pouvez également activer/désactiver ici la vérification des communications par e-mail effectuées via les protocoles POP3 et IMAP.

Vérification par protocole POP3

Le protocole POP3 est le protocole le plus répandu pour la réception de courrier électronique dans un client de messagerie. ESET Cyber Security assure la protection de ce protocole quel que soit le client de messagerie utilisé.

Le module de protection qui fournit ce contrôle est automatiquement initié au démarrage du système et est alors actif dans la mémoire. Pour que le filtrage des protocoles fonctionne correctement, vérifiez que le module est activé. La vérification par protocole POP3 est effectuée automatiquement sans qu'il soit nécessaire de reconfigurer le client de messagerie. Par défaut, toutes les communications sur le port 110 sont analysées, mais vous pouvez ajouter d'autres ports de communication au besoin. Les numéros de port doivent être séparés par une virgule.

Si vous activez l'option **Vérification par protocole POP3**, tout le trafic POP3 est surveillé pour rechercher des logiciels malveillants.

Vérification par protocole IMAP

Le protocole IMAP (Internet Message Access Protocol) est un autre protocole Internet destiné à la récupération de courrier électronique. IMAP présente certains avantages par rapport à POP3. Il permet notamment la connexion simultanée de plusieurs clients à la même boîte aux lettres et permet de conserver les informations

d'état des messages telles que le fait de savoir si le message a été lu, si une réponse a été envoyée ou s'il a été supprimé. ESET Cyber Security offre une protection pour ce protocole quel que soit le client de messagerie utilisé.

Le module de protection qui fournit ce contrôle est automatiquement initié au démarrage du système et est alors actif dans la mémoire. Assurez-vous que la vérification par protocole IMAP est activée pour que le module fonctionne correctement. La vérification par protocole IMAP est effectuée automatiquement sans qu'il soit nécessaire de reconfigurer le client de messagerie. Par défaut, toutes les communications sur le port 143 sont analysées, mais vous pouvez ajouter d'autres ports de communication au besoin. Les numéros de port doivent être séparés par une virgule.

Si vous activez l'option **Vérification par protocole IMAP**, tout le trafic IMAP fait l'objet d'un contrôle des logiciels malveillants.

Notifications d'e-mail

L'utilisation de notifications d'e-mail permet d'ajouter une notification à la note de bas de l'e-mail. Après l'analyse d'un message, une notification peut y être ajoutée avec les résultats de l'analyse. Ces notifications sont utiles, mais elles ne doivent pas être utilisées comme résultat final de la sécurité des messages, car elles peuvent ne pas figurer dans des messages HTML problématiques et être contrefaites par certains virus. Les options disponibles sont les suivantes :

- **Pour recevoir et lire des e-mails lorsqu'une détection a lieu** : seuls les e-mails contenant des logiciels malveillants sont marqués comme vérifiés.
- **À tous les e-mails lors de l'analyse** : des notifications sont ajoutées à tous les e-mails analysés.
- **Jamais** : aucune notification n'est ajoutée à un e-mail.

Mettre à jour l'objet d'un e-mail reçu : cochez cette case si vous souhaitez que la protection de la messagerie ajoute un avertissement de menace au message infecté. Cette fonctionnalité permet un filtrage simple des messages infectés. Elle augmente aussi le niveau de crédibilité vis-à-vis du destinataire et, en cas de détection d'une infiltration, elle fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur donné.

Texte ajouté à l'objet des messages détectés – Modifiez ce texte si vous souhaitez modifier le format du préfixe de l'objet d'un e-mail infecté.

Paramètres ThreatSense

La configuration avancée de l'analyseur permet de configurer les niveaux de nettoyage, les options d'analyse et les extensions de fichiers exclues de l'analyse.

Protection antihameçonnage

L'anti-hameçonnage offre une autre couche de protection qui protège des tentatives d'acquisition de mots de passe ou d'autres informations sensibles par des sites web non légitimes. L'anti-hameçonnage est activé par défaut et il est recommandé de conserver cette fonctionnalité activée.

Mettre à jour

Cette section spécifie les informations sur la source de mise à jour, comme les serveurs de mise à jour utilisés et les données d'authentification pour ces serveurs. Pour modifier les paramètres de **mise à jour** avancés d'ESET Cyber Security, ouvrez les **Préférences de l'application** en utilisant cmd+, ou en cliquant sur ESET Cyber Security dans la barre de menus macOS et en sélectionnant **Préférences** (Paramètres).

Mises à jour des modules et du produit

Mises à jour des modules

Type de mise à jour

- **Mise à jour régulière**. Il s'agit du type de mise à jour par défaut. La base des signatures de détection et les modules du produit sont mis à jour automatiquement à partir des serveurs de mise à jour ESET.

- Les **mises à jour préliminaires** incluent les corrections de bogues et les méthodes de détection les plus récentes, bientôt disponibles pour le grand public. Cependant, ils ne sont pas toujours stables ; il n'est donc pas recommandé de les utiliser dans un environnement de production.

- Les **mises à jour différées** permettent une mise à jour à partir de serveurs de mise à jour spéciaux fournissant de nouvelles versions de bases de virus avec un délai d'au moins X heures (c'est-à-dire des bases de données testées dans un environnement réel et considérées comme stables).

Restauration des modules

Si vous pensez qu'une mise à jour du moteur de détection ou que des modules du programme sont instables ou corrompus, vous pouvez restaurer la version précédente et désactiver temporairement les mises à jour.

Créer des instantanés des modules

ESET Cyber Security enregistre des instantanés du moteur de détection et de modules du programme à utiliser avec la fonctionnalité de restauration. Pour créer des instantanés de la base de données de modules, conservez l'option **Créer des instantanés des modules** activée. Lorsque cette option est activée, le premier instantané est créé pendant la première mise à jour. Le deuxième est créé après 48 heures. Le champ **Nombre d'instantanés stockés localement** définit le nombre d'instantanés du moteur de détection stockés.

> Lorsque le nombre maximal d'instantanés est atteint (3, par exemple), l'instantané le plus ancien est remplacé par un nouveau toutes les 48 heures. ESET Cyber Security pour macOS restaure les versions des mises à jour du moteur de détection et des modules du programme en fonction de l'instantané le plus ancien.

Mises à jour du produit

Les mises à jour du produit garantissent que vous utilisez toujours la dernière version du produit. Activez le bouton bascule **Mises à jour automatiques** pour que les mises à jour du produit soient installées automatiquement au prochain redémarrage et conserver un accès constant aux dernières fonctionnalités et à la meilleure protection possible.

Serveur principal et serveur secondaire

L’option permettant de choisir automatiquement les serveurs de mise à jour principal et secondaire est activée par défaut. Les deux serveurs peuvent être spécifiés une fois que le choix automatique est désactivé.

Outils

Pour modifier les paramètres avancés des **outils** d'ESET Cyber Security, ouvrez les **Préférences de l'application** en utilisant cmd+, ou en cliquant sur ESET Cyber Security dans la barre de menus macOS et en sélectionnant **Préférences** (Paramètres).

Planificateur

Configurer des tâches d'analyse à la demande qui sont exécutées automatiquement à une date spécifiée. Pour créer une tâche planifiée ou supprimer une tâche existante, sélectionnez + ou −. Vous pouvez également définir le ou les jours où la tâche doit être répétée.

Fichiers journaux

Verbosité du journal

La verbosité des journaux définit le niveau de détails des fichiers journaux.

- **Avertissements critiques** – Comprend uniquement les erreurs critiques (par exemple : **Impossible de démarrer la protection antivirus**).
- **Erreurs** – Enregistre les erreurs du type **« Erreur de téléchargement du fichier »** en plus des avertissements critiques.
- **Avertissements** – Les erreurs critiques et les messages d’avertissement seront enregistrés en plus des erreurs.
- **Enregistrements informatifs** – Enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.
- **Enregistrements de diagnostic** – Contient les informations nécessaires au réglage du programme et de toutes les entrées ci-dessus.

Nettoyage des fichiers journaux

Supprimer automatiquement les entrées plus anciennes que (jours) – Les entrées de journal plus anciennes que le nombre de jours spécifiés seront automatiquement supprimées.

Optimisation des fichiers journaux

Optimiser automatiquement les fichiers journaux – Si cette option est activée, les fichiers journaux sont

automatiquement défragmentés si le pourcentage de fragmentation est supérieur à la valeur spécifiée dans le champ **Si le nombre d'entrées inutilisées dépasse (%)**. Toutes les entrées vides des journaux sont supprimées pour améliorer les performances et accélérer le traitement des journaux. Cette amélioration se constate notamment si les journaux comportent un grand nombre d'entrées.

Configuration du serveur proxy

Vous pouvez spécifier ici les paramètres du serveur proxy. Les paramètres définis ici seront utilisés par tous les modules qui nécessitent une connexion à Internet.

Pour configurer le serveur proxy :

1. Activez l'option **Utiliser un serveur proxy** et saisissez l'adresse du serveur proxy dans le champ Serveur proxy et le numéro de port du serveur proxy.

2. Activez l'option **Utiliser une connexion directe** si le proxy HTTP n'est pas disponible pour communiquer directement avec les serveurs ESET.

3. Si la communication avec le serveur proxy exige une authentification, activez l'option **Le serveur proxy nécessite une authentification**, puis saisissez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants.

Interface utilisateur

Pour modifier les paramètres avancés de l'**interface utilisateur** d'ESET Cyber Security, ouvrez les **Préférences de l'application** en utilisant cmd+, ou en cliquant sur ESET Cyber Security dans la barre de menus macOS et en sélectionnant **Préférences** (Paramètres).

Intégration du système

Éléments de l'interface utilisateur

Autoriser un utilisateur à ouvrir l'interface utilisateur graphique – Désactivez ce paramètre pour empêcher les utilisateurs d'accéder à l'interface graphique. Cela peut être utile dans les environnements gérés ou dans les situations où vous devez préserver les ressources du système.

Afficher l'icône dans les éléments de la barre des menus – Désactivez ce paramètre pour supprimer l'icône ESET Cyber Security de la barre de menu Extras de la barre de menu de macOS (en haut de l'écran).

Notifications

Afficher les notifications sur le Bureau – Les notifications du bureau (telles que les messages de mise à jour réussie, l'achèvement des tâches d'analyse de virus ou les nouvelles menaces trouvées) sont représentées par une petite fenêtre contextuelle à côté de la barre de menus de macOS. Si elles sont activées, ESET Cyber Security peut vous informer lorsqu'un nouvel événement se produit.

États d'application

Vous pouvez sélectionner ici les états d'application à afficher dans votre produit ESET Cyber Security. Lorsque le bouton bascule **Afficher l'état** est désactivé et qu'un problème est signalé, l'application ESET Cyber Security conserve l'état vert **Vous êtes protégé**.

Protections

L'option **Protections** de la fenêtre principale de l'application permet d'ajuster le niveau de protection de votre ordinateur, d'Internet et de la messagerie. Les sections Protection de l'ordinateur et Protection Internet et Messagerie contiennent des modules de protection qui peuvent être activés ou désactivés. Il est vivement recommandé de conserver tous les modules activés pour tirer pleinement parti d'ESET Cyber Security et garder l'ordinateur protégé.

Protection de l'ordinateur

La configuration de la protection de l'ordinateur se trouve dans **Protections** > **Ordinateur**. Cette fenêtre indique l'état de la **protection en temps réel du système de fichiers** et des modules du **système de réputation ESET LiveGrid®**. Il est recommandé de conserver les deux modules activés. L'arrêt de l'un des modules peut diminuer la protection de votre ordinateur.

Vous pouvez cliquer sur le bouton bascule pour activer ou désactiver la fonctionnalité **Mise à jour automatique** dans la section **Mise à jour**. Lorsque la mise à jour automatique est activée, ESET Cyber Security recherche les dernières mises à jour du produit et les télécharge automatiquement.

Protection web et de la messagerie

Pour accéder à la protection Internet et de la messagerie, cliquez dans le menu principal sur **Protections** > **Internet et messagerie**. Pour gérer les paramètres plus avancés de chaque module, ouvrez **Préférences de l'application** en utilisant cmd+, ou cliquez sur ESET Cyber Security dans la barre de menus macOS et sélectionnez **Préférences** (Paramètres). Les modules de protection suivants sont disponibles dans le cadre de la protection Internet et messagerie :

- **Web** : surveille la communication HTTP entre les navigateurs et les serveurs distants.
- **Anti-hameçonnage** : bloque les éventuelles attaques de hameçonnage en provenance de sites Web ou de domaines.
- **E-mail** : permet de contrôler la communication par courrier électronique effectuée via les protocoles POP3 et IMAP.

Exceptions d'analyse
ESET Cyber Security n'analyse pas les protocoles chiffrés HTTPS, POP3S et IMAPS.

Protection antihameçonnage

L'hameçonnage est une activité criminelle qui utilise l'ingénierie sociale (manipulation des utilisateurs pour obtenir des informations confidentielles). Il est souvent utilisé pour obtenir des données sensibles, comme des numéros de compte bancaire ou de carte de crédit, des codes PIN, des noms d'utilisateur ou des mots de passe. Vous trouverez des informations supplémentaires sur l'hameçonnage dans le glossaire ESET.

Il est recommandé de conserver la fonctionnalité d'anti-hameçonnage activée (Protections > Internet et messagerie > Anti-hameçonnage). Toutes les attaques par hameçonnage potentielles en provenance de sites web ou de domaines dangereux seront bloquées. Une notification d'avertissement sera également affichée pour vous informer de l'attaque.

Pour tester le fonctionnement de l'anti-hameçonnage, reportez-vous à la page de test AMTSO.

Protection antivirus et antispyware

La protection antivirus vous protège contre les attaques malveillantes du système en modifiant les fichiers qui représentent des menaces potentielles. Si une menace comportant du code malveillant est détectée, le module Antivirus peut l'éliminer en la bloquant et en la nettoyant, en la supprimant ou en la mettant en quarantaine.

Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers vérifie tous les types de supports et déclenche une analyse en fonction de différents événements. La protection en temps réel du système de fichiers utilise la technologie ESET LiveGrid® (décrite dans la section Configuration des paramètres du moteur ThreatSense) et peut être différente pour les nouveaux fichiers et les fichiers existants. Les fichiers nouvellement créés peuvent être plus précisément contrôlés.

Pour modifier les paramètres avancés de la protection en temps réel du système de fichiers, ouvrez **Préférences de l'application** en utilisant cmd+, ou cliquez sur **ESET Cyber Security** dans la barre de menus macOS et sélectionnez **Préférences** (Paramètres) > **Protection en temps réel**.

Par défaut, tous les fichiers sont analysés pendant **l'ouverture** et **la création**. ESET recommande de conserver ces paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur : La protection en temps réel est lancée au démarrage du système, assurant ainsi une analyse ininterrompue. Dans des cas particuliers (par exemple, en cas de conflit avec un autre analyseur en temps réel), vous pouvez arrêter la protection en temps réel depuis la fenêtre principale du programme (cliquez sur **Protections** > **Ordinateur** et désactivez **Protection en temps réel du système de fichiers**).

Vous pouvez exclure les types de supports suivants de l'analyseur Real-time :

- **Disques locaux** : disques durs système
- **Supports amovibles** : CD, DVD, périphériques USB, appareils Bluetooth, etc.
- **Supports réseau** : tous les lecteurs mappés

Vous pouvez également exclure des processus spécifiques de l'analyse.

Il est recommandé d'utiliser les paramètres par défaut et de ne modifier les exclusions d'analyse que dans des cas spécifiques, par exemple lorsque l'analyse de certains supports ralentit de manière significative les transferts de données.

Quand modifier la configuration de la protection en temps réel

La protection en temps réel est essentielle pour conserver un système sécurisé avec ESET Cyber Security. Procédez avec prudence lorsque vous modifiez les paramètres de protection en temps réel. Il est recommandé de ne modifier ces paramètres que dans des cas spécifiques, par exemple lorsqu'il existe un conflit avec une autre application.

Après l'installation de ESET Cyber Security, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité.

Vérifier la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne et qu'elle détecte les virus éventuels, téléchargez le fichier de test eicar.com et vérifiez que ESET Cyber Security l'identifie en tant que menace. Ce fichier de test est un fichier inoffensif particulier qui est détectable par tous les programmes antivirus. L'institut EICAR (European Institute for Computer Antivirus Research) a créé le fichier pour tester les fonctionnalités des antivirus.

Que faire si la protection en temps réel ne fonctionne

pas ?

Vous trouverez ici les problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel et la façon de les résoudre.

La protection en temps réel est désactivée

Si un utilisateur désactive par mégarde la protection en temps réel, vous devez réactiver la protection. Pour réactiver la protection en temps réel à partir du menu principal, cliquez sur le bouton bascule **Protection en temps réel du système de fichiers** pour l'activer. Vous pouvez également accéder à la fenêtre des préférences de l'application et cliquer sur le bouton bascule **Protection en temps réel** pour activer la protection en temps réel du système de fichiers.

La protection en temps réel ne détecte et ne nettoie pas les infiltrations

Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Il est recommandé de désinstaller tout autre antivirus de votre système.

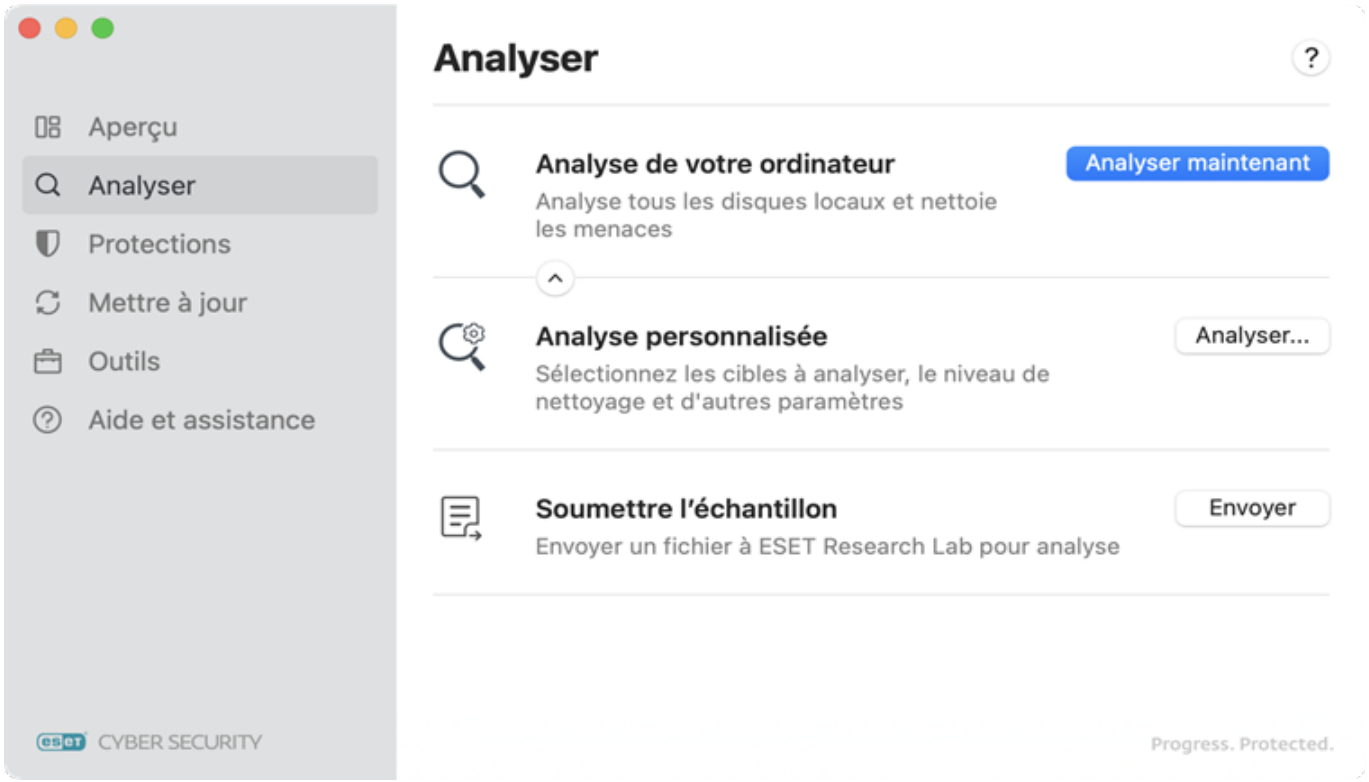
La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée pendant le démarrage du système, il peut y avoir des conflits avec d'autres programmes. Si la protection en temps réel ne démarre pas, contactez l'assistance technique ESET.

Analyse de l'ordinateur à la demande

Si vous pensez que votre ordinateur est infecté (parce qu'il se comporte anormalement), sélectionnez **Analyse** dans la fenêtre principale de l'application, puis cliquez sur **Analyser maintenant** pour examiner votre ordinateur à la recherche d'infiltrations. Pour une protection maximale, lancez régulièrement des analyses de l'ordinateur dans le cadre des mesures de sécurité de routine, et pas seulement lorsque vous soupçonnez une infection. Une analyse régulière peut permettre de trouver des infiltrations non détectées par l'analyseur en temps réel lorsqu'elles ont été enregistrées sur le disque. Cela peut se produire si l'analyseur en temps réel est désactivé au moment de l'infection ou si les modules de détection ne sont pas à jour.

ESET recommande d'exécuter une analyse d'ordinateur à la demande au moins une fois par mois.



Vous pouvez configurer l'analyse en tant que tâche planifiée à partir des préférences de l'application, dans la section **Outils** > **Planificateur**.

Analyse personnalisée

Dans la fenêtre principale de l'application, accédez à la section **Analyser**, cliquez sur l'icône de flèche pour afficher les options **Analyse personnalisée** et **Soumettre un échantillon**.

Analyse personnalisée

Il est la solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. Elle permet en effet de configurer les paramètres avec grande précision.

Cliquez sur **Analyser** dans la section **Analyse personnalisée** pour ouvrir la fenêtre Analyse personnalisée. Faites glisser les fichiers à analyser dans la zone désignée au sein de la fenêtre. Vous pouvez également spécifier une **cible à analyser** en cliquant sur le bouton **Parcourir** et en accédant au dossier ou aux fichiers à inclure.

En cliquant sur l'icône de menu représentant trois points de suspension : plus d'options s'offrent à vous : **Sélectionnez** le **profil d'analyse** et **Configurer les exclusions**.

Sélectionner le profil d'analyse

Vous pouvez sélectionner ici le **profil d'analyse** préféré et configurer le **niveau de nettoyage**.

Profils d'analyse

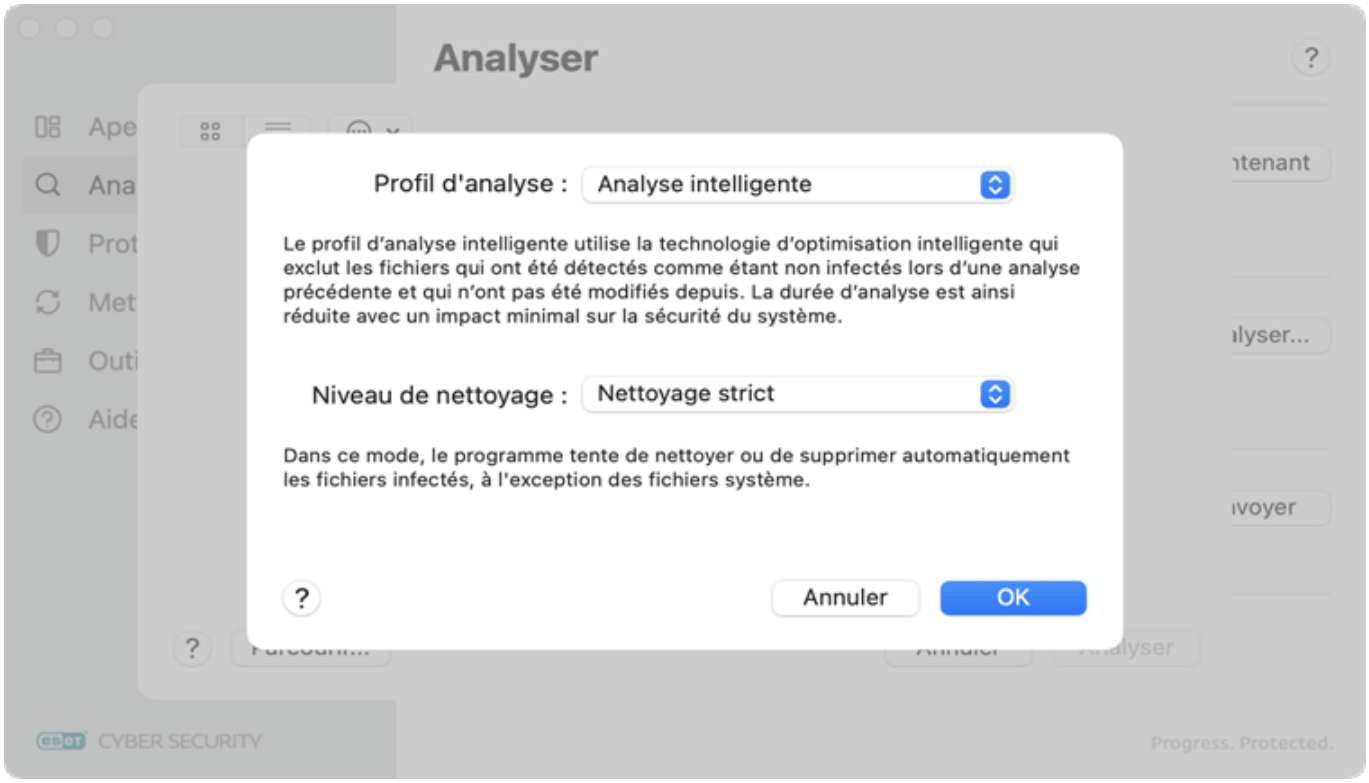
L'**analyse intelligente** permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. Elle présente l'avantage d'être facile à utiliser, sans aucune configuration d'analyse détaillée. L'analyse intelligente vérifie tous les fichiers de tous les dossiers, et nettoie ou supprime

automatiquement les infiltrations détectées. Le profil d'analyse intelligente utilise la technologie d'optimisation intelligente qui exclut les fichiers qui ont été détectés comme étant non infectés lors d'une analyse précédente et qui n'ont pas été modifiés depuis.

Le profil d'**analyse approfondie** n'utilise pas l'optimisation intelligente. Par conséquent, aucun fichier n'est exclu de l'analyse.

Niveau de nettoyage

Vous pouvez sélectionner ici la façon dont l'analyseur traite les fichiers infectés. Pour en savoir plus sur les niveaux de nettoyage, consultez Nettoyage.



Configurer les exclusions

Ajoutez des fichiers ou des dossiers à exclure de l'analyse. Faites glisser les fichiers à exclure dans la zone désignée au sein de la fenêtre affichée.

> L'exécution d'**analyse personnalisée** est recommandée pour les utilisateurs chevronnés qui maîtrisent l'utilisation de programmes antivirus.

Soumettre l'échantillon

Cette option vous permet d'envoyer un fichier au laboratoire ESET Research Lab pour analyse. Pour plus d'informations sur l'envoi d'un fichier échantillon, consultez Soumettre un échantillon.

Configuration du moteur ThreatSense

ThreatSense est une technologie ESET exclusive, constituée de plusieurs méthodes complexes de détection des menaces. Cette technologie est proactive : elle fournit une protection dès les premières heures de propagation d'une nouvelle menace. ThreatSense combine plusieurs méthodes (analyse de code, émulation de code,

signatures génériques, etc.) qui se conjuguent pour améliorer sensiblement la sécurité du système. Ce moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, optimisant ainsi l'efficacité et le taux de détection. La technologie ThreatSense parvient également à supprimer les rootkits.

Les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

- les types de fichiers et les extensions à analyser ;
- la combinaison de plusieurs méthodes de détection ;
- les niveaux de nettoyage, etc.

Vous pouvez modifier les configurations ThreatSense dans Préférences de l'application (que vous pouvez ouvrir en utilisant cmd+, ou en cliquant sur ESET Cyber Security dans la barre de menus macOS et en sélectionnant **Préférences** ([Paramètres]). Différents scénarios de sécurité peuvent nécessiter des configurations différentes. Dans cette optique, Threatsense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers
- Analyses des logiciels malveillants
- Protection de l'accès Web
- Protection du client de messagerie

Les paramètres ThreatSense sont optimisés pour chaque module et leur modification peut avoir une incidence significative sur le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les fichiers exécutables compressés ou pour activer l'analyse heuristique avancée dans le module de protection en temps réel du système de fichiers, vous pouvez dégrader les performances du système. Il est donc recommandé de ne pas modifier les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module Analyse de l'ordinateur.

Options d'analyse

Les options d'analyse peuvent être configurées dans la section Préférences de l'application de ces modules de protection : Protection en temps réel du système de fichiers, analyses des logiciels malveillants, protection de l'accès web et protection du client de messagerie. Pour chacun des modules de protection, vous pouvez choisir les méthodes utilisées lors d'une analyse du système. Les options disponibles sont les suivantes :

- **Heuristique** : l'heuristique utilise un algorithme qui analyse l'activité (malveillante) des programmes. La détection heuristique présente l'avantage de détecter les nouveaux logiciels malveillants qui n'existaient pas auparavant.

- **Heuristique avancée** : cette option utilise un algorithme heuristique unique développé par ESET et optimisé pour la détection de vers informatiques et de chevaux de Troie écrits dans des langages de programmation de haut niveau. L'heuristique avancée améliore de manière significative la capacité de détection du programme.

- **Optimisation intelligente** : lorsqu'elle est activée, l'optimisation intelligente offre le niveau d'analyse le plus efficace tout en maintenant les vitesses d'analyse les plus élevées. Les différents modules de protection analysent intelligemment, en appliquant différentes méthodes d'analyse à des types de fichiers

spécifiques.

Niveau de nettoyage

Les niveaux de nettoyage peuvent être configurés dans la section Préférences de l'application de ces modules de protection : Protection en temps réel du système de fichiers, analyses des logiciels malveillants, protection de l'accès web et protection du client de messagerie. Les niveaux individuels déterminent comment l'analyseur nettoie les fichiers infectés. Les niveaux de nettoyage suivants sont disponibles :

- **Aucun nettoyage** - Les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche alors une fenêtre d'avertissement et vous laisse choisir une action.
- **Nettoyage normal** - Le programme tente de nettoyer ou de supprimer automatiquement tout fichier infecté. S'il ne peut pas sélectionner automatiquement la bonne action, le programme proposera différentes actions complémentaires. Les actions de suivi sont également affichées si une action prédéfinie ne peut pas être effectuée.
- **Nettoyage strict** - Le programme nettoiera ou supprimera tous les fichiers infectés (y compris les archives). Les seules exceptions sont les fichiers système. S'il est impossible de nettoyer un fichier, vous recevrez une notification vous demandant de sélectionner le type d'action à entreprendre.
- **Nettoyage rigoureux** : Dans ce mode, le programme tente de nettoyer ou de supprimer automatiquement tous les fichiers infectés.
- **Supprimer** : supprime tous les fichiers infectés.

Analyse de l'archive
Dans le mode de nettoyage normal par défaut, les fichiers d'archive ne sont entièrement supprimés que si tous les fichiers qu'ils contiennent sont infectés. Si une archive contient des fichiers légitimes et des fichiers infectés, elle n'est pas supprimée. Si un fichier d'archive infecté est détecté dans le mode Nettoyage strict, le fichier entier est supprimé, même s'il contient également des fichiers intacts.

Exclusions

L'extension est la partie du nom d'un fichier située après le point. L'extension définit le type de fichier et le contenu. Vous pouvez définir les types de fichiers à exclure de l'analyse dans la section Préférences de l'application de ces modules de protection :

- Protection en temps réel du système de fichiers
- Analyses des logiciels malveillants
- Protection de l'accès Web
- Protection du client de messagerie

Par défaut, tous les fichiers sont analysés, quelle que soit leur extension. Toutes les extensions peuvent être ajoutées à la liste des fichiers exclus de l'analyse. Les boutons Plus + et Moins − permettent d'activer ou d'empêcher l'analyse d'extensions spécifiques.

L'exclusion de certains fichiers de l'analyse peut être utile si l'analyse de ces fichiers provoque un dysfonctionnement du programme. Par exemple, il peut être conseillé d'exclure les fichiers log, cfg et tmp. Le format correct de saisie des extensions de fichiers est le suivant :

- log
- cfg
- tmp

Mettre à jour

Des mises à jour régulières de ESET Cyber Security sont nécessaires pour conserver le niveau maximum de sécurité. Le module de mise à jour garantit que le programme est toujours à jour en téléchargeant les modules de détection les plus récents.

Cliquez sur **Mettre à jour** dans le menu principal pour afficher l'état actuel de la mise à jour de ESET Cyber Security, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire. Pour lancer une recherche de nouvelles mises à jour, cliquez sur le bouton **Rechercher les mises à jour**. Si une mise à jour de produits est disponible, des informations sur la version actuelle et disponible sont affichées, ainsi que la taille de la mise à jour et la date de publication. Vous avez le choix entre **Mettre à jour maintenant** ou **Mettre à jour au redémarrage**. Pour afficher plus de détails sur les versions individuelles des produits, cliquez sur le lien **Voir le journal des modifications**.

Mise à jour de ESET Cyber Security vers une nouvelle version

Pour bénéficier d'une protection maximale, il est important d'utiliser la dernière version de ESET Cyber Security. Pour être sûr de disposer toujours de la dernière version, il est recommandé d'activer les **mises à jour automatiques du produit** (menu principal de l'application > **Protections** > **Ordinateur**).

Outils

Le menu **Outils** contient des modules qui simplifient l'administration du programme et offrent des options supplémentaires pour les utilisateurs chevronnés. Ce menu comprend les éléments suivants :

- Fichiers journaux
- Quarantaine

Fichiers journaux

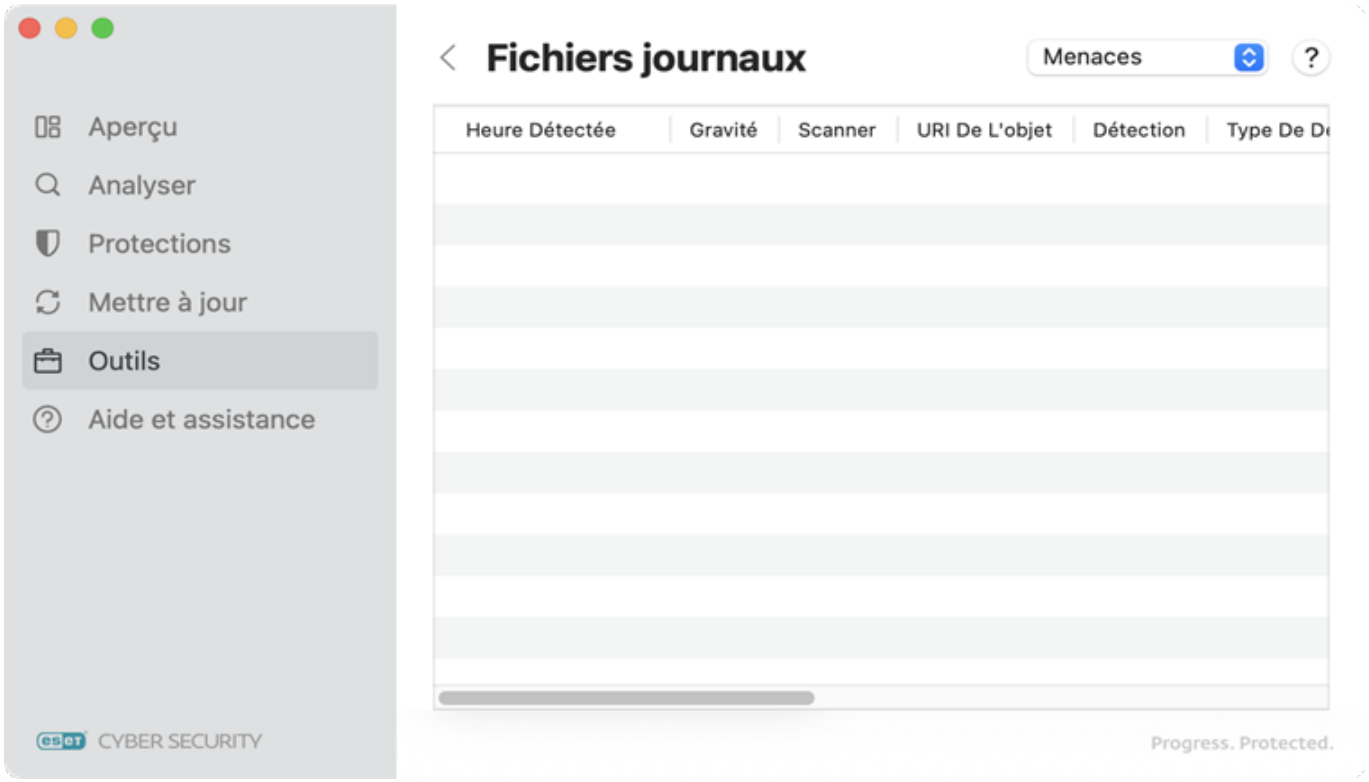
Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La consignation est essentielle pour l'analyse système, la détection de menaces et le dépannage. La consignation est effectuée en arrière-plan sans interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres de verbosité. Vous pouvez consulter les messages texte et les journaux directement à partir de l'environnement ESET Cyber Security. Vous pouvez aussi archiver les journaux.

Vous pouvez accéder aux fichiers journaux depuis le menu principal ESET Cyber Security en cliquant sur **Outils** > **Fichiers journaux**. Sélectionnez le type de journal souhaité dans le menu déroulant en haut à droite de la fenêtre. Les journaux suivants sont disponibles :

- **Détections** : affiche toutes les informations sur les événements liés à la détection des infiltrations.
- **Analyse de l'ordinateur** : ce journal affiche les résultats de toutes les analyses effectuées. Pour afficher les détails d'une analyse de l'ordinateur à la demande, double-cliquez sur l'entrée correspondante.
- **Événements** : permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Toutes les actions importantes exécutées par ESET Cyber Security sont enregistrées dans les journaux des événements.

• **Sites Web filtrés** : affiche la liste des sites web bloqués par la protection de l’accès web. Ces journaux permettent de voir l'heure, l'URL, l'état, l'adresse IP, l'utilisateur et l'application ayant ouvert une connexion au site Web en question.

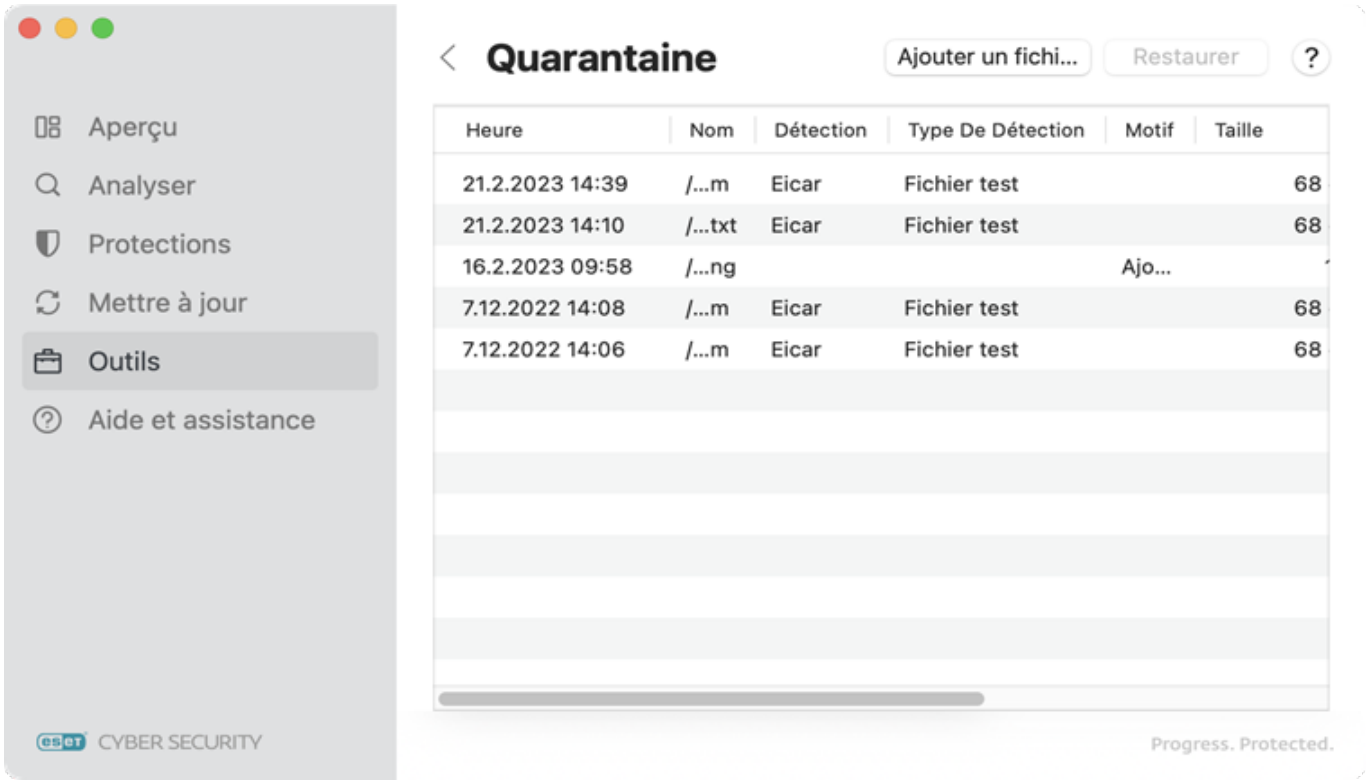
• **Fichiers envoyés** – Contient les entrées des échantillons envoyés pour analyse.



Quarantaine

Le principal objectif de la quarantaine est de stocker les fichiers infectés en toute sécurité. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET Cyber Security.

Vous pouvez afficher les fichiers du dossier de quarantaine dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin d'accès à l'emplacement d'origine du fichier infecté, la taille en octets, la raison (par exemple, ajouté par l'utilisateur) et le nombre de menaces (s'il s'agit d'une archive contenant plusieurs infiltrations par exemple). Le dossier de quarantaine des fichiers en quarantaine (*/Library/Application Support/Eset/security/cache/quarantine*) reste dans le système même après la suppression d'ESET Cyber Security. Les fichiers en quarantaine sont stockés en toute sécurité dans un format crypté et peuvent être restaurés après l'installation de ESET Cyber Security.



Mettre les fichiers en quarantaine

ESET Cyber Security met automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas désactivé cette option dans la fenêtre d'alerte). Pour mettre manuellement en quarantaine tout fichier suspect, cliquez sur **Ajouter un fichier**. Effectuez un glisser-déposer du fichier ou du dossier manuellement en cliquant dessus, en déplaçant le pointeur de la souris vers la zone marquée tout en maintenant le bouton de la souris enfoncé, puis en le relâchant.

Restoring from Quarantine

Sélectionnez un fichier en quarantaine, puis cliquez sur **Restaurer** pour le restaurer à son emplacement d'origine. Cette fonctionnalité est également disponible lorsque vous cliquez en maintenant la touche Contrôle enfoncée (ou cliquez avec le bouton droit) sur un fichier donné dans la fenêtre **Quarantaine** et cliquez sur **Restaurer**. Le menu contextuel propose également l'option **Restaurer vers** qui permet de restaurer un fichier vers un autre emplacement que celui de sa suppression.

Soumission d'un fichier de quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré infecté par erreur (par l'analyse heuristique du code, par exemple) et placé en quarantaine, envoyez ce fichier au laboratoire de recherche sur les menaces d'ESET. Pour soumettre un fichier mis en quarantaine, cliquez en maintenant la touche Contrôle enfoncée (ou cliquez avec le bouton droit) sur le fichier et sélectionnez l'option **Soumettre l'échantillon** dans le menu contextuel. Pour plus d'informations sur l'envoi d'un fichier échantillon, consultez Soumettre un échantillon.

Soumettre un échantillon pour analyse

Dans la fenêtre principale de l'application, sélectionnez **Analyser** dans le menu de gauche, cliquez sur l'icône de flèche  pour afficher l'option **Soumettre un échantillon**.

Cette option vous permet de sélectionner un fichier au comportement suspect trouvé sur votre ordinateur, ou un site suspect trouvé en ligne, et de l'envoyer au laboratoire ESET Research Lab pour analyse.

Avant de soumettre des échantillons à ESET
L'échantillon que vous soumettez doit répondre à au moins l'un des critères suivants :
- L'échantillon n'est pas détecté par votre produit ESET.
- Le fichier est détecté à tort comme une menace.
- L'échantillon n'est pas un fichier personnel. ESET n'accepte pas vos fichiers personnels (que vous souhaitez faire analyser par ESET pour détecter des logiciels malveillants) en tant qu'échantillons. De plus, le laboratoire de recherche d' ESET n'effectue pas d'analyses à la demande pour les utilisateurs.

Cliquez sur **Envoyer** pour spécifier le fichier que vous souhaitez envoyer pour analyse. Dans le formulaire **Soumettre un échantillon pour analyse**, indiquez les informations suivantes :

- **Motif de la soumission** : effectuez une sélection dans le menu contextuel.
- **Échantillon** : indiquez le chemin d'accès au fichier que vous souhaitez soumettre ou effectuez ungglisser-déposer du fichier dans la zone indiquée
- **Contact** : coordonnées fournies pour que nous puissions vous contacter au cas où nous aurions besoin de plus d'informations sur le fichier ; vous pouvez ne pas inclure votre adresse e-mail en activant le bouton Envoyer de manière anonyme.

En cliquant sur **Suivant**, vous accédez à la dernière étape où vous fournissez des informations supplémentaires sur le fichier échantillon, telles que les signes ou symptômes observés d'une infection par un logiciel malveillant et l'origine du fichier. La fourniture d'informations supplémentaires aidera nos laboratoires à identifier et à traiter les échantillons.

Il est possible que vous ne receviez pas de réponse d'ESET.
Vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires sont nécessaires à l'analyse. Nos serveurs reçoivent, en effet, chaque jour, des milliers de fichiers, ce qui ne permet pas de répondre à tous les envois.
Si l'échantillon s'avère être une application malveillante, sa détection sera intégrée à une prochaine mise à jour du produit ESET.

Contrat de licence de l'utilisateur final

En vigueur à compter du 19 octobre 2021.

IMPORTANT : Veuillez lire soigneusement les termes et conditions d'application du produit stipulés ci-dessous avant de télécharger, d'installer, de copier ou d'utiliser le produit. **EN TÉLÉCHARGEANT, INSTALLANT, COPIANT OU UTILISANT LE LOGICIEL, VOUS ACCEPTEZ CES TERMES ET CONDITIONS ET RECONNAISSEZ AVOIR PRIS CONNAISSANCE DE LA POLITIQUE DE CONFIDENTIALITÉ.**

Contrat de licence de l'utilisateur final

Selon les termes du présent Contrat de Licence pour l'Utilisateur Final (« Contrat ») signé par et entre ESET, spol. s r. o., dont le siège social se situe au Einsteinova 24, 85101 Bratislava, Slovak Republic, inscrite au Registre du Commerce du tribunal de Bratislava I. Section Sro, Insertion No 3586/B, numéro d'inscription des entreprises : 31333532 (« ESET » ou « Fournisseur ») et vous, personne physique ou morale, (« vous » ou « Utilisateur Final »), vous êtes autorisé à utiliser le Logiciel défini à l'article 1 du présent Contrat. Dans le cadre des modalités indiquées ci-dessous, le Logiciel défini à l'article 1 du présent Contrat peut être enregistré sur un support de données, envoyé par courrier électronique, téléchargé sur Internet, téléchargé à partir de serveurs du Fournisseur ou obtenu à partir d'autres sources.

CE DOCUMENT N'EST PAS UN CONTRAT D'ACHAT, MAIS UN ACCORD LIÉ AUX DROITS DE L'UTILISATEUR FINAL. Le Fournisseur reste le propriétaire de la copie du Logiciel et du support physique fourni dans l'emballage commercial, et de toutes les copies du Logiciel que l'Utilisateur Final est autorisé à faire dans le cadre du présent Contrat.

En cliquant sur « J'accepte » ou « J'accepte... » lorsque vous téléchargez, installez, copiez ou utilisez le Logiciel, vous acceptez les termes et conditions du présent Contrat et reconnaissez avoir pris connaissance de la Politique de confidentialité. Si vous n'êtes pas d'accord avec tous les termes et conditions du présent Contrat et/ou de la Politique de confidentialité, cliquez immédiatement sur l'option d'annulation, annulez le téléchargement ou l'installation, détruisez ou renvoyez le Logiciel, le support d'installation, la documentation connexe et une facture au Fournisseur ou à l'endroit où vous avez obtenu le Logiciel.

VOUS RECONNAISSEZ QUE VOTRE UTILISATION DU LOGICIEL INDIQUE QUE VOUS AVEZ LU ET COMPRIS LE PRÉSENT CONTRAT ET ACCEPTÉ D'EN RESPECTER LES TERMES ET CONDITIONS.

1. **Logiciel.** Dans le cadre du présent Contrat, le terme « Logiciel » désigne : (i) le programme informatique et tous ses composants ; (ii) le contenu des disques, des CD-ROM, des DVD, des courriers électroniques et de leurs pièces jointes, ou de tout autre support auquel le présent Contrat est attaché, dont le formulaire de code objet fourni sur un support de données, par courrier électronique ou téléchargé par le biais d'Internet ; (iii) tous documents explicatifs écrits et toute documentation relative au Logiciel, en particulier, toute description du Logiciel, ses caractéristiques, description des propriétés, description de l'utilisation, description de l'interface du système d'exploitation sur lequel le Logiciel est utilisé, guide d'installation ou d'utilisation du Logiciel ou description de l'utilisation correcte du Logiciel (« Documentation ») ; (iv) les copies du Logiciel, les correctifs d'erreurs du Logiciel, les ajouts au Logiciel, ses extensions, ses versions modifiées et les mises à jour des parties du Logiciel, si elles sont fournies, au titre desquels le Fournisseur vous octroie la Licence conformément à l'article 3 du présent Contrat. Le Logiciel est fourni exclusivement sous la forme d'un code objet exécutable.

2. **Installation, Ordinateur et Clé de licence**. Le Logiciel fourni sur un support de données, envoyé par courrier électronique, téléchargé à partir d'Internet ou de serveurs du Fournisseur ou obtenu à partir d'autres sources nécessite une installation. Vous devez installer le Logiciel sur un Ordinateur correctement configuré, qui doit au moins satisfaire les exigences spécifiées dans la Documentation. La méthode d'installation est décrite dans la Documentation. L'Ordinateur sur lequel le Logiciel sera installé doit être exempt de tout programme ou matériel susceptible de nuire au bon fonctionnement du Logiciel. Le terme Ordinateur désigne le matériel, notamment les ordinateurs personnels, ordinateurs portables, postes de travail, ordinateurs de poche, smartphones, appareils électroniques portatifs ou autres appareils électroniques, pour lequel le Logiciel a été conçu et sur lequel il sera installé et/ou utilisé. Le terme Clé de licence désigne la séquence unique de symboles, lettres, chiffres ou signes spéciaux fournie à l'Utilisateur Final afin d'autoriser l'utilisation légale du Logiciel, de sa version spécifique ou de l'extension de la durée de la Licence conformément au présent Contrat.

3. **Licence**. Sous réserve que vous ayez accepté les termes du présent Contrat et que vous respectiez tous les termes et conditions stipulés dans le présent Contrat, le Fournisseur vous accorde les droits suivants (« Licence ») :

a) **Installation et utilisation.** Vous détenez un droit non exclusif et non transférable d'installer le Logiciel sur le disque dur d'un ordinateur ou sur un support similaire de stockage permanent de données, d'installer et de stocker le Logiciel dans la mémoire d'un système informatique et d'exécuter, de stocker et d'afficher le Logiciel.

b) **Précision du nombre de licences.** Le droit d'utiliser le Logiciel est lié au nombre d'Utilisateurs Finaux. On entend par « Utilisateur Final » : (i) l'installation du Logiciel sur un seul système informatique, ou (ii) si l'étendue de la Licence est liée au nombre de boîtes aux lettres, un Utilisateur Final désigne un utilisateur d'ordinateur qui reçoit un courrier électronique par le biais d'un client de messagerie. Si le client de messagerie accepte du courrier électronique et le distribue automatiquement par la suite à plusieurs utilisateurs, le nombre d'Utilisateurs Finaux doit être déterminé en fonction du nombre réel d'utilisateurs auxquels le courrier électronique est distribué. Si un serveur de messagerie joue le rôle de passerelle de courriel, le nombre d'Utilisateurs Finaux est égal au nombre de serveurs de messagerie pour lesquels la passerelle fournit des services. Si un certain nombre d'adresses de messagerie sont affectées à un seul et même utilisateur (par l'intermédiaire d'alias) et que ce dernier les accepte et si les courriels ne sont pas distribués automatiquement du côté du client à d'autres utilisateurs, la Licence n'est requise que pour un seul ordinateur. Vous ne devez pas utiliser la même Licence au même moment sur plusieurs ordinateurs. L'Utilisateur Final n'est autorisé à saisir la Clé de licence du Logiciel que dans la mesure où il a le droit d'utiliser le Logiciel conformément à la limite découlant du nombre de licences accordées par le Fournisseur. La Clé de licence est confidentielle. Vous ne devez pas partager la Licence avec des tiers ni autoriser des tiers à utiliser la Clé de licence, sauf si le présent Contrat ou le Fournisseur le permet. Si votre Clé de licence est endommagée, informez-en immédiatement le Fournisseur.

c) **Home/Business Edition.** Une version Home Edition du Logiciel doit être utilisée exclusivement dans des environnements privés et/ou non commerciaux, pour un usage domestique et familial uniquement. Une version Business Edition du Logiciel est requise pour l'utiliser dans un environnement commercial ainsi que pour utiliser le Logiciel sur des serveurs de messagerie, relais de messagerie, passerelles de messagerie ou passerelles Internet.

d) **Durée de la Licence.** Le droit d'utiliser le Logiciel est limité dans le temps.

e) **Logiciel acheté à un fabricant d'équipement informatique.** Les logiciels classés comme achetés à un fabricant d'équipement informatique sont limités à l'ordinateur avec lequel vous les avez obtenus. Elle ne peut pas être transférée à un autre ordinateur.

f) **Version d'évaluation ou non destinée à la revente.** Un Logiciel classé comme non destiné à la revente ou comme version d'évaluation ne peut pas être vendu et ne doit être utilisé qu'aux fins de démonstration ou d'évaluation des caractéristiques du Logiciel.

g) **Résiliation de la Licence.** La Licence expire automatiquement à la fin de la période pour laquelle elle a été accordée. Si vous ne respectez pas les dispositions du présent Contrat, le Fournisseur est en droit de mettre fin au Contrat, sans renoncer à tout droit ou recours juridique ouvert au Fournisseur dans de tels cas. En cas d'annulation du présent Contrat, vous devez immédiatement supprimer, détruire ou renvoyer à vos frais le Logiciel et toutes les copies de sauvegarde à ESET ou à l'endroit où vous avez obtenu le Logiciel. Lors de la résiliation de la Licence, le Fournisseur est en droit de mettre fin au droit de l'Utilisateur final à l'utilisation des fonctions du Logiciel, qui nécessitent une connexion aux serveurs du Fournisseur ou à des serveurs tiers.

4. **Fonctions avec des exigences en matière de connexion Internet et de collecte de données.** Pour fonctionner correctement, le Logiciel nécessite une connexion Internet et doit se connecter à intervalles réguliers aux serveurs du Fournisseur ou à des serveurs tiers et collecter des données en conformité avec la Politique de confidentialité. Une connexion Internet et une collecte de données sont requises pour les fonctions suivantes du Logiciel :

a) **Mises à jour du Logiciel.** Le Fournisseur est autorisé de temps à autre à publier des mises à jour ou des mises à niveau du Logiciel (« Mises à jour »), mais n'en a pas l'obligation. Cette fonction est activée dans la configuration standard du Logiciel ; les Mises à jour sont donc installées automatiquement, sauf si l'Utilisateur Final a désactivé

l’installation automatique des Mises à jour. Pour la mise à disposition de Mises à jour, une vérification de l'authenticité de la Licence est requise. Elle comprend notamment la collecte d'informations sur l'Ordinateur et/ou la plate-forme sur lesquels le Logiciel est installé, en conformité avec la Politique de confidentialité.

La fourniture des mises à jour peut être soumise à la Politique de fin de vie (« Politique de fin de vie »), qui est disponible à l'adresse suivante : https://go.eset.com/eol. Aucune mise à jour ne sera fournie après que le Logiciel ou l'une de ses fonctionnalités ait atteint la date de fin de vie telle que définie dans la Politique de fin de vie.

b) **Réacheminement des infiltrations et des données au Fournisseur.** Le Logiciel contient des fonctions qui collectent des échantillons de virus, d'autres programmes informatiques également nuisibles et d'objets problématiques, suspects, potentiellement indésirables ou dangereux tels que des fichiers, des URL, des paquets IP et des trames Ethernet (« Infiltrations »), puis les envoient au Fournisseur, en incluant, sans s'y limiter, des informations sur le processus d'installation, l'Ordinateur ou la plateforme hébergeant le Logiciel et des informations sur les opérations et fonctions du Logiciel (« Informations »). Les Informations et les Infiltrations sont susceptibles de contenir des données (y compris des données personnelles obtenues par hasard ou accidentellement) concernant l’Utilisateur final et/ou d’autres usagers de l’ordinateur sur lequel le Logiciel est installé et les fichiers affectés par les Infiltrations et les métadonnées associées.

Les informations et les infiltrations peuvent être collectées pat les fonctions suivantes du Logiciel :

i. La fonction Système de réputation LiveGrid collecte et envoie les hachages unidirectionnelles liés aux Infiltrations au Fournisseur. Cette fonction est activée dans les paramètres standard du Logiciel.

ii. La fonction Système de commentaires LiveGrid collecte et envoie les Infiltrations avec les Informations et les métadonnées associées au Fournisseur. Cette fonction peut être activée par l'Utilisateur Final pendant le processus d'installation du Logiciel.

Le Fournisseur utilisera les Informations et Infiltrations reçues uniquement pour effectuer des analyses et des recherches sur les Infiltrations et améliorer le Logiciel et la vérification de l'authenticité de la Licence. Il prendra en outre les mesures adéquates afin de protéger les Infiltrations et Informations reçues. Si vous activez cette fonction du Logiciel, les Infiltrations et Informations peuvent être collectées et traitées par le Fournisseur, comme stipulé dans la Politique de confidentialité et conformément aux réglementations en vigueur. Vous pouvez désactiver ces fonctions à tout moment.

Aux fins du présent Contrat, il est nécessaire de collecter, traiter et stocker des données permettant au Fournisseur de vous identifier conformément à la Politique de confidentialité. Vous acceptez que le Fournisseur vérifie à l'aide de ses propres moyens si vous utilisez le Logiciel conformément aux dispositions du présent Contrat. Vous reconnaissez qu'aux fins du présent Contrat, il est nécessaire que vos données soient transférées pendant les communications entre le Logiciel et les systèmes informatiques du Fournisseur ou de ceux de ses partenaires commerciaux, dans le cadre du réseau de distribution et de support du Fournisseur, afin de garantir les fonctionnalités du Logiciel, l'autorisation d'utiliser le Logiciel et la protection des droits du Fournisseur.

Après la conclusion du présent Contrat, le Fournisseur et ses partenaires commerciaux, dans le cadre du réseau de distribution et de support du Fournisseur, sont autorisés à transférer, à traiter et à stocker des données essentielles vous identifiant, aux fins de facturation, d'exécution du présent Contrat et de transmission de notifications sur votre Ordinateur.

Des informations détaillées sur la vie privée, la protection des données personnelles et Vos droits en tant que personne concernée figurent dans la Politique de confidentialité, disponible sur le site Web du Fournisseur et directement accessible à partir de l'installation. Vous pouvez également la consulter depuis la section d'aide du Logiciel.

5. **Exercice des droits de l’Utilisateur Final**. Vous devez exercer les droits de l'Utilisateur Final en personne ou par

l'intermédiaire de vos employés. Vous n'êtes autorisé à utiliser le Logiciel que pour assurer la sécurité de vos opérations et protéger les Ordinateurs ou systèmes informatiques pour lesquels vous avez obtenu une Licence.

6. **Restrictions des droits.** Vous ne pouvez pas copier, distribuer, extraire des composants ou créer des travaux dérivés basés sur le Logiciel. Vous devez respecter les restrictions suivantes lorsque vous utilisez le Logiciel :

a) Vous pouvez effectuer une copie de sauvegarde archivée du Logiciel sur un support de stockage permanent, à condition que cette copie de sauvegarde archivée ne soit pas installée ni utilisée sur un autre ordinateur. Toutes les autres copies que vous pourriez faire du Logiciel seront considérées comme une violation du présent Contrat.

b) Vous n'êtes pas autorisé à utiliser, modifier, traduire, reproduire ou transférer les droits d'utilisation du Logiciel ou des copies du Logiciel d'aucune manière autre que celles prévues dans le présent Contrat.

c) Vous ne pouvez pas vendre, concéder en sous-licence, louer à bail ou louer le Logiciel ou utiliser le Logiciel pour offrir des services commerciaux.

d) Vous ne pouvez pas rétroconcevoir, décompiler ou désassembler le Logiciel ni tenter de toute autre façon de découvrir le code source du Logiciel, sauf dans la mesure où cette restriction est expressément interdite par la loi.

e) Vous acceptez de n'utiliser le Logiciel que de façon conforme à toutes les lois applicables de la juridiction dans laquelle vous utilisez le Logiciel, notamment les restrictions applicables relatives aux droits d'auteur et aux droits de propriété intellectuelle.

f) Vous acceptez de n'utiliser le Logiciel et ses fonctions que de façon à ne pas entraver la possibilité des autres Utilisateurs Finaux à accéder à ces services. Le Fournisseur se réserve le droit de limiter l'étendue des services fournis à chacun des Utilisateurs Finaux, pour permettre l'utilisation des services au plus grand nombre possible d'Utilisateurs Finaux. Le fait de limiter l'étendue des services implique aussi la résiliation totale de la possibilité d'utiliser toute fonction du Logiciel ainsi que la suppression des Données et des informations présentes sur les serveurs du Fournisseur ou sur des serveurs tiers, qui sont afférentes à une fonction particulière du Logiciel.

g) Vous acceptez de ne pas exercer d'activités impliquant l'utilisation de la Clé de licence, qui soit contraire aux termes du présent Contrat, ou conduisant à fournir la Clé de licence à toute personne n'étant pas autorisée à utiliser le logiciel (comme le transfert d'une Clé de licence utilisée ou non utilisée ou la distribution de Clés de licence dupliquées ou générées ou l'utilisation du Logiciel suite à l'emploi d'une Clé de licence obtenue d'une source autre que le Fournisseur).

7. **Droit d'auteur**. Le Logiciel et tous les droits inclus, notamment les droits d'auteur et les droits de propriété intellectuelle sont la propriété d'ESET et/ou de ses concédants de licence. ESET est protégée par les dispositions des traités internationaux et par toutes les lois nationales applicables dans le pays où le Logiciel est utilisé. La structure, l'organisation et le code du Logiciel sont des secrets commerciaux importants et des informations confidentielles appartenant à ESET et/ou à ses concédants de licence. Vous n'êtes pas autorisé à copier le Logiciel, sauf dans les exceptions précisées en 6 (a). Toutes les copies que vous êtes autorisé à faire en vertu du présent Contrat doivent contenir les mentions relatives aux droits d'auteur et de propriété qui apparaissent sur le Logiciel. Si vous rétroconcevez, décompilez ou désassemblez le Logiciel ou tentez de toute autre façon de découvrir le code source du Logiciel, en violation des dispositions du présent Contrat, vous acceptez que les données ainsi obtenues doivent être automatiquement et irrévocablement transférées au Fournisseur dans leur totalité, dès que de telles données sont connues, indépendamment des droits du Fournisseur relativement à la violation du présent Contrat.

8. **Réservation de droits**. Le Fournisseur se réserve tous les droits sur le Logiciel, à l'exception des droits qui vous sont expressément garantis en vertu des termes du présent Contrat en tant qu'Utilisateur final du Logiciel.

9. **Versions multilingues, logiciel sur plusieurs supports, copies multiples**. Si le Logiciel est utilisé sur plusieurs

plateformes et en plusieurs langues, ou si vous recevez plusieurs copies du Logiciel, vous ne pouvez utiliser le Logiciel que pour le nombre de systèmes informatiques ou de versions pour lesquels vous avez obtenu une Licence. Vous ne pouvez pas vendre, louer à bail, louer, concéder en sous-licence, prêter ou transférer des versions ou des copies du Logiciel que vous n'utilisez pas.

10. **Début et fin du Contrat.** Ce Contrat entre en vigueur à partir du jour où vous en acceptez les modalités. Vous pouvez résilier ce Contrat à tout moment en désinstallant de façon permanente, détruisant et renvoyant, à vos frais, le Logiciel, toutes les copies de sauvegarde et toute la documentation associée remise par le Fournisseur ou ses partenaires commerciaux. Votre droit d'utiliser le Logiciel et l'une de ses fonctionnalités peut être soumis à la Politique de fin de vie. Lorsque le logiciel ou l'une de ses fonctionnalités atteint la date de fin de vie définie dans la Politique de fin de vie, votre droit d'utiliser le logiciel prend fin. Quelle que soit la façon dont ce Contrat se termine, les dispositions énoncées aux articles 7, 8, 11, 13, 19 et 21 continuent de s'appliquer pour une durée illimitée.

11. **DÉCLARATIONS DE L'UTILISATEUR FINAL**. EN TANT QU'UTILISATEUR FINAL, VOUS RECONNAISSEZ QUE LE LOGICIEL EST FOURNI « EN L'ÉTAT », SANS AUCUNE GARANTIE D'AUCUNE SORTE, QU'ELLE SOIT EXPRESSE OU IMPLICITE, DANS LA LIMITE PRÉVUE PAR LA LOI APPLICABLE. NI LE FOURNISSEUR, NI SES CONCÉDANTS DE LICENCE, NI SES FILIALES, NI LES DÉTENTEURS DE DROIT D'AUTEUR NE FONT UNE QUELCONQUE DÉCLARATION OU N'ACCORDENT DE GARANTIE EXPRESSE OU IMPLICITE QUELCONQUE, NOTAMMENT DES GARANTIES DE VENTE, DE CONFORMITÉ À UN OBJECTIF PARTICULIER OU SUR LE FAIT QUE LE LOGICIEL NE PORTE PAS ATTEINTE À DES BREVETS, DROITS D'AUTEURS, MARQUES OU AUTRES DROITS DÉTENUS PAR UN TIERS. NI LE FOURNISSEUR NI AUCUN AUTRE TIERS NE GARANTIT QUE LES FONCTIONS DU LOGICIEL RÉPONDRONT À VOS ATTENTES OU QUE LE FONCTIONNEMENT DU LOGICIEL SERA CONTINU ET EXEMPT D'ERREURS. VOUS ASSUMEZ L'ENTIÈRE RESPONSABILITÉ ET LES RISQUES LIÉS AU CHOIX DU LOGICIEL POUR L'OBTENTION DES RÉSULTATS ESCOMPTÉS ET POUR L'INSTALLATION, L'UTILISATION ET LES RÉSULTATS OBTENUS.

12. **Aucune obligation supplémentaire**. À l'exception des obligations mentionnées explicitement dans le présent Contrat, aucune obligation supplémentaire n'est imposée au Fournisseur et à ses concédants de licence.

13. **LIMITATION DE GARANTIE**. DANS LA LIMITE MAXIMALE PRÉVUE PAR LES LOIS APPLICABLES, LE FOURNISSEUR, SES EMPLOYÉS OU SES CONCÉDANTS DE LICENCE NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES D'UNE QUELCONQUE PERTE DE PROFIT, REVENUS, VENTES, DONNÉES, OU DES FRAIS D'OBTENTION DE BIENS OU SERVICES DE SUBSTITUTION, DE DOMMAGE MATÉRIEL, DOMMAGE PHYSIQUE, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES COMMERCIALES, OU DE TOUT DOMMAGE DIRECT, INDIRECT, FORTUIT, ÉCONOMIQUE, DE GARANTIE, PUNITIF, SPÉCIAL OU CORRÉLATIF, QUELLE QU'EN SOIT LA CAUSE ET QUE CE DOMMAGE DÉCOULE D'UNE RESPONSABILITÉ CONTRACTUELLE, DÉLICTUELLE OU D'UNE NÉGLIGENCE OU DE TOUTE AUTRE THÉORIE DE RESPONSABILITÉ, LIÉE À L'INSTALLATION, À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISER LE LOGICIEL, MÊME SI LE FOURNISSEUR OU SES CONCÉDANTS DE LICENCE ONT ÉTÉ AVERTIS DE L'ÉVENTUALITÉ D'UN TEL DOMMAGE. CERTAINS PAYS ET CERTAINES LOIS N'AUTORISANT PAS L'EXCLUSION DE RESPONSABILITÉ, MAIS AUTORISANT LA LIMITATION DE RESPONSABILITÉ, LA RESPONSABILITÉ DU FOURNISSEUR, DE SES EMPLOYÉS OU DE SES CONCÉDANTS DE LICENCE SERA LIMITÉE AU MONTANT QUE VOUS AVEZ PAYÉ POUR LA LICENCE.

14. Aucune disposition du présent Contrat ne porte atteinte aux droits accordés par la loi de toute partie agissant comme client si l'exécution y est contraire.

15. **Assistance technique**. ESET ou des tiers mandatés par ESET fourniront une assistance technique à leur discrétion, sans garantie ni déclaration solennelle. Aucune assistance technique ne sera fournie après que le Logiciel ou l'une de ses fonctionnalités ait atteint la date de fin de vie telle que définie dans la Politique de fin de vie. L'Utilisateur Final devra peut-être sauvegarder toutes les données, logiciels et programmes existants avant que l'assistance technique ne soit fournie. ESET et/ou les tiers mandatés par ESET ne seront en aucun cas tenus responsables d'un quelconque dommage ou d'une quelconque perte de données, de biens, de logiciels ou de matériel, ou d'une quelconque perte de profit en raison de la fourniture de l'assistance technique. ESET et/ou les

tiers mandatés par ESET se réservent le droit de décider si l'assistance technique couvre la résolution du problème. ESET se réserve le droit de refuser, de suspendre l'assistance technique ou d'y mettre fin à sa discrétion. Des informations de licence, d'autres informations et des données conformes à la Politique de confidentialité peuvent être requises en vue de fournir une assistance technique.

16. **Transfert de Licence**. Le Logiciel ne peut pas être transféré d'un système informatique à un autre, à moins d'une précision contraire dans les modalités du présent Contrat. L'Utilisateur Final n'est autorisé qu'à transférer de façon définitive la Licence et tous les droits accordés par le présent Contrat à un autre Utilisateur Final avec l'accord du Fournisseur, si cela ne s'oppose pas aux modalités du présent Contrat et dans la mesure où (i) l'Utilisateur Final d'origine ne conserve aucune copie du Logiciel ; (ii) le transfert des droits est direct, c'est-à-dire qu'il s'effectue directement de l'Utilisateur Final original au nouvel Utilisateur Final ; (iii) le nouvel Utilisateur Final assume tous les droits et devoirs de l'Utilisateur Final d'origine en vertu du présent Contrat ; (iv) l'Utilisateur Final d'origine transmet au nouvel Utilisateur Final toute la documentation permettant de vérifier l'authenticité du Logiciel, conformément à l'article 17.

17. **Vérification de l'authenticité du Logiciel.** L'Utilisateur final peut démontrer son droit d'utiliser le Logiciel de l'une des façons suivantes : (i) au moyen d'un certificat de licence émis par le Fournisseur ou un tiers mandaté par le Fournisseur ; (ii) au moyen d'un contrat de licence écrit, si un tel contrat a été conclu ; (iii) en présentant un courrier électronique envoyé au Fournisseur contenant tous les renseignements sur la licence (nom d'utilisateur et mot de passe). Des informations de licence et des données d'identification de l'Utilisateur Final conformes à la Politique de confidentialité peuvent être requises en vue de vérifier l'authenticité du Logiciel.

18. **Licence pour les pouvoirs publics et le gouvernement des États-Unis**. Le Logiciel est fourni aux pouvoirs publics, y compris le gouvernement des États-Unis, avec les droits de Licence et les restrictions mentionnés dans le présent Contrat.

19. **Conformité aux contrôles à l'exportation**.

a) Vous ne devez en aucun cas, directement ou indirectement, exporter, réexporter, transférer ou mettre le Logiciel à la disposition de quiconque, ou l'utiliser d'une manière ou participer à un acte qui pourrait entraîner ESET ou ses sociétés de holding, ses filiales et les filiales de l'une de ses sociétés de holding, ainsi que les entités contrôlées par ses sociétés de holding (« Sociétés affiliées ») à enfreindre ou faire l'objet des conséquences négatives de l'enfreinte des Lois sur le contrôle à l'exportation, qui comprennent

i. les lois qui contrôlent, limitent ou imposent des exigences en matière de licence pour l'exportation, la réexportation ou le transfert de marchandises, de logiciels, de technologies ou de services, émises ou adoptées par un gouvernement, un état ou un organisme de réglementation des États-Unis d'Amérique, de Singapour, du Royaume-Uni, de l'Union européenne ou de l'un de ses États membres, ou tout pays dans lequel les obligations au titre de l'accord doivent être exécutées, ou dans lequel ESET ou l'une de ses filiales est établie ou mène ses activités et

ii. toute sanction économique, financière, commerciale ou autre, sanction, restriction, embargo, interdiction d'importation ou d'exportation, interdiction de transfert de fonds ou d'actifs ou de prestation de services, ou mesure équivalente imposée par un gouvernement, un État ou un organisme de réglementation des États-Unis d'Amérique, de Singapour, du Royaume-Uni, de l'Union européenne ou de l'un de ses États membres, ou tout pays dans lequel les obligations au titre de l'accord doivent être exécutées, ou dans lequel ESET ou l'une de ses filiales est établie ou mène ses activités.

(les actes juridiques mentionnés aux points i, et ii. ci-dessus étant appelés ensemble « Lois sur le contrôle à l'exportation »).

b) ESET a le droit de suspendre ses obligations en vertu des présentes Conditions ou d'y mettre fin avec effet immédiat dans le cas où :

i. ESET estime raisonnablement que l'Utilisateur a enfreint ou est susceptible d'enfreindre la disposition de l'Article 19 a) du Contrat ; ou

ii. l'Utilisateur final et/ou le Logiciel deviennent soumis aux Lois sur le contrôle à l'exportation et, par conséquent, ESET estime raisonnablement que l'exécution continue de ses obligations en vertu de l'accord pourrait entraîner ESET ou ses affiliés à enfreindre ou faire l'objet des conséquences négatives de l'enfreinte des Lois sur le contrôle à l'exportation.

c) Rien dans le Contrat ne vise, et rien ne doit être interprété comme incitant ou obligeant l'une des parties à agir ou à s'abstenir d'agir (ou à accepter d'agir ou à s'abstenir d'agir) d'une manière qui soit incompatible, pénalisée ou interdite en vertu de toute loi sur le contrôle à l'exportation applicable.

20. **Avis**. Tous les avis, les renvois du Logiciel et la documentation doivent être adressés à : ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sans préjudice du droit d'ESET de Vous communiquer toute modification du présent Contrat, des Politiques de confidentialité, de la Politique de fin de vie et de la documentation conformément à l'article 22 du Contrat. ESET peut Vous envoyer des e-mails, des notifications intégrés à l'application via le Logiciel ou publier la communication sur son site web. Vous acceptez de recevoir des communications légales d'ESET sous forme électronique, y compris toute communication sur la modification des Conditions, des Conditions particulières ou des Politiques de confidentialité, toute proposition/acceptation de contrat ou invitation à traiter, avis ou autres communications légales. Ces communications électroniques sont réputées avoir été reçues par écrit, sauf si les lois applicables exigent spécifiquement une autre forme de communication.

21. **Loi applicable**. Le présent Contrat est régi par la loi de la République Slovaque et interprété conformément à celle-ci. L'Utilisateur Final et le Fournisseur conviennent que les principes relatifs aux conflits de la loi applicable et la Convention des Nations Unies sur les contrats pour la Vente internationale de marchandises ne s'appliquent pas. Vous acceptez expressément que le tribunal de Bratislava I. arbitre tout litige ou conflit avec le Fournisseur ou en relation avec votre utilisation du Logiciel, et vous reconnaissez expressément que le tribunal a la juridiction pour de tels litiges ou conflits.

22. **Dispositions générales**. Si une disposition du présent Contrat s'avère nulle et inopposable, cela n'affectera pas la validité des autres dispositions du présent Contrat. Ces dispositions resteront valables et opposables en vertu des conditions stipulées dans le présent Contrat. Le présent Contrat a été signé en anglais. Si une traduction du Contrat est préparée pour des raisons de commodité ou pour toute autre raison, ou en cas de discordance entre les versions linguistiques du présent Contrat, seule la version en langue anglaise fait foi.

ESET se réserve le droit d'apporter des modifications au Logiciel ainsi que de réviser les conditions du présent Contrat, des Annexes, des Addendums, de la Politique de confidentialité, de la Politique de fin de vie et de la Documentation ou toute partie de celle-ci à tout moment en mettant à jour le document approprié (i) pour refléter les modifications apportées au Logiciel ou dans la façon dont ESET mène ses activités, (ii) pour des raisons légales, réglementaires ou de sécurité, ou (iii) pour éviter tout abus ou dommage. Vous serez averti de toute révision du Contrat par e-mail, par le biais d'une notification intégrée à l'application ou par d'autres moyens électroniques. Si vous n'êtes pas d'accord avec les modifications proposées au Contrat, vous pouvez le résilier conformément à l'article 10, dans les 30 jours suivant la réception d'une notification de la modification. À moins que Vous ne résiliez le Contrat dans ce délai, les modifications proposées seront considérées comme acceptées et prendront effet à Votre égard à la date à laquelle vous avez reçu une notification de la modification.

Cela constitue l'intégralité du Contrat entre le Fournisseur et vous en relation avec le Logiciel, et il remplace toute représentation, discussion, entreprise, communication ou publicité antérieure en relation avec le Logiciel.

EULAID: EULA-PRODUCT-LG; 3537.0

Politique de confidentialité

La protection des données personnelles revêt une importance particulière pour ESET, spol. s r.o., dont le siège social est établi au Einsteinova 24, 851 01 Bratislava, Slovak Republic, inscrite au registre du commerce administré par le Tribunal de district de Bratislava I, Section Sro, Entrée No 3586/B, Numéro d'identification de l'entreprise : 31333532 en tant que Responsable du traitement des données ("ESET" ou « Nous"). Nous souhaitons nous conformer à l'exigence de transparence telle qu'elle est légalement normalisée par le Règlement général sur la protection des données de l'UE ("RGPD"). Pour atteindre cet objectif, nous publions la présente Politique de confidentialité dans le seul but d'informer notre client ("Utilisateur final" ou "Vous"), en tant que personne concernée, des sujets suivants relatifs à la protection des données personnelles :

- Base juridique du traitement des données personnelles,
- Partage des données et confidentialité,
- Sécurité des données,
- Vos Droits en tant que Personne concernée,
- Traitement de Vos données personnelles
- Coordonnées.

Traitement de Vos données personnelles

Les services ESET qui sont implémentés dans le produit sont fournis selon les termes du CLUF, mais certains d'entre eux peuvent nécessiter une attention particulière. Nous souhaitons Vous donner plus de détails sur la collecte de données liée à la fourniture de nos services. Nous proposons différents services qui sont décrits dans le Contrat de Licence de l'utilisateur final et la documentation. Pour que tous ces services soient fonctionnels, Nous devons collecter les informations suivantes :

- Mise à jour et autres statistiques relatives aux informations concernant l'installation et votre ordinateur, notamment la plate-forme sur laquelle notre produit est installé, et informations sur les opérations et fonctionnalités de nos produits (système d'exploitation, informations matérielles, identifiants d'installation, identifiants de licence, adresse IP, adresse MAC, paramètres de configuration du produit).
- Hachages unidirectionnels liés aux infiltrations dans le cadre du système de réputation ESET LiveGrid® qui améliore l'efficacité de nos solutions contre les logiciels malveillants en comparant les fichiers analysés à une base de données d'éléments en liste blanche et liste noire dans le cloud.
- Échantillons suspects et métadonnées génériques dans le cadre du système de commentaires ESET LiveGrid® qui permet à ESET de réagir immédiatement face aux besoins des utilisateurs finaux et de rester réactifs face aux dernières menaces. Nous dépendons de Vous pour l'envoi
    - d'infiltrations (échantillons potentiels de virus et d'autres programmes malveillants et suspects), d'objets problématiques, potentiellement indésirables ou potentiellement dangereux (fichiers exécutables), de messages électroniques que Vous avez signalés comme spam ou détectés par notre produit ;
    - d'informations sur les appareils du réseau local, telles que le type, le fabricant, le modèle et/ou le nom de l'appareil ;
    - d'informations concernant l'utilisation d'Internet, telles que l'adresse IP et des informations géographiques, les paquets IP, les URL et les trames Ethernet ;
    - de fichiers de vidage sur incident et des informations qu'ils contiennent.

Nous ne souhaitons pas collecter vos données en dehors de ce cadre, mais cela s'avère parfois impossible. Des données collectées accidentellement peuvent être incluses dans des logiciels malveillants (informations collectées à votre insu ou sans votre consentement) ou dans des noms de fichier ou des URL. Nous ne souhaitons pas que ces données fassent partie de nos systèmes ni qu'elles soient traitées dans le but déclaré dans la présente

Politique de confidentialité.

- Des informations de licence, telles que l'identifiant de la licence, et des données personnelles comme le nom, le prénom, l'adresse, l'adresse e-mail sont nécessaires pour la facturation, la vérification de l'authenticité de la licence et la fourniture de nos services.
- Des coordonnées et des données contenues dans vos demandes d'assistance sont requises pour la fourniture du service d'assistance. Selon le canal que Vous choisissez pour nous contacter, Nous pouvons collecter votre adresse e-mail, votre numéro de téléphone, des informations sur la licence, des détails sur le produit et la description de votre demande d'assistance. Nous pouvons Vous demander de nous fournir d'autres informations pour faciliter la fourniture du service d'assistance.

Partage des données et confidentialité

Nous ne partageons pas vos données avec des tiers. Cependant, ESET est une entreprise présente dans le monde entier par le biais de sociétés affiliées et de partenaires du réseau de vente, de service et d'assistance ESET. Les informations relatives aux licences, à la facturation et à l'assistance technique traitées par ESET peuvent être transférées depuis et vers les sociétés affiliées ou les partenaires dans le but de respecter le Contrat de licence pour l'utilisateur final (pour la fourniture de services ou l'assistance, par exemple).

ESET préfère traiter ses données dans l'Union européenne (EU). Toutefois, en fonction de votre localisation (utilisation de nos produits et/ou services en dehors de l'UE) et/ou du service que vous choisissez, il peut être nécessaire de transférer vos données vers un pays situé en dehors de l'UE. Nous utilisons par exemple des services tiers dans le cadre du cloud computing. Dans ces cas, nous sélectionnons soigneusement nos fournisseurs de services et garantissons un niveau approprié de protection des données par des mesures contractuelles, techniques et organisationnelles. En règle générale, nous nous mettons d'accord sur les clauses contractuelles types de l'UE et, si nécessaire, sur des dispositions contractuelles complémentaires.

Pour certains pays hors de l'UE, comme le Royaume-Uni et la Suisse, l'UE a déjà déterminé un niveau comparable de protection des données. En raison du niveau comparable de protection des données, le transfert de données vers ces pays ne nécessite aucune autorisation ou accord particulier.

Droits des personnes concernées

Les droits de chaque Utilisateur final sont importants et Nous aimerions vous informer que tous les Utilisateurs finaux (de n'importe quel pays de l'UE ou hors de l'UE) ont les droits ci-après garantis chez ESET. Pour exercer les droits de la personne concernée, vous pouvez nous contacter par le biais du formulaire d'assistance ou par e-mail à l'adresse suivante : dpo@eset.sk. À des fins d'identification, nous vous demandons les informations suivantes : Nom, adresse e-mail et - le cas échéant - clé de licence ou numéro de client et affiliation à la société. Veuillez vous abstenir de nous envoyer d'autres données personnelles, telles que votre date de naissance. Nous tenons à souligner que pour pouvoir traiter votre demande, ainsi qu'à des fins d'identification, nous traiterons vos données personnelles.

Droit de retirer le consentement. Le droit de retirer le consentement est applicable en cas de traitement fondé sur le consentement uniquement. Si Nous traitons vos données personnelles sur la base de votre consentement, vous avez le droit de retirer ce consentement à tout moment sans donner de raisons. Le retrait de votre consentement n'est effectif que pour l'avenir et n'affecte pas la légalité des données traitées avant le retrait.

Droit d'opposition. Le droit de s'opposer au traitement est applicable en cas de traitement fondé sur l'intérêt légitime d'ESET ou d'un tiers. Si Nous traitons vos données personnelles pour protéger un intérêt légitime, Vous, en tant que personne concernée, avez le droit de vous opposer à l'intérêt légitime nommé par nous et au traitement de vos données personnelles à tout moment. Votre opposition n'a d'effet que pour l'avenir et n'affecte pas la licéité des données traitées avant l'opposition. Si nous traitons vos données personnelles à des

fins de marketing direct, il n'est pas nécessaire de motiver votre objection. Il en est de même pour le profilage, dans la mesure où il est lié au marketing direct. Dans tous les autres cas, nous vous demandons de nous informer brièvement de vos plaintes contre l'intérêt légitime d'ESET à traiter vos données personnelles.

Veuillez noter que dans certains cas, malgré le retrait de votre consentement, nous avons le droit de traiter ultérieurement vos données personnelles sur la base d'une autre base juridique, par exemple, pour l'exécution d'un contrat.

Droit d'accès. En tant que personne concernée, vous avez le droit d'obtenir gratuitement et à tout moment des informations sur vos données stockées par ESET.

Droit à la rectification. Si nous traitons par inadvertance des données personnelles incorrectes vous concernant, vous avez le droit de les faire corriger.

Droit à l'effacement et droit à la restriction du traitement. En tant que personne concernée, vous avez le droit de demander la suppression ou la restriction du traitement de vos données personnelles. Si nous traitons vos données personnelles, par exemple avec votre consentement, que vous le retirez et qu'il n'existe pas d'autre base juridique, par exemple un contrat, nous supprimons immédiatement vos données personnelles. Vos données personnelles seront également supprimées dès qu'elles ne seront plus nécessaires aux fins énoncées à la fin de notre période de conservation.

Si nous utilisons vos données personnelles dans le seul but de marketing direct et que vous avez révoqué votre consentement ou que vous vous êtes opposé à l'intérêt légitime sous-jacent d'ESET, Nous limiterons le traitement de vos données personnelles dans la mesure où nous inclurons vos coordonnées dans notre liste noire interne afin d'éviter tout contact non sollicité. Dans le cas contraire, vos données personnelles seront supprimées.

Veuillez noter que Nous pouvons être tenus de conserver vos données jusqu'à l'expiration des obligations et périodes de conservation émises par le législateur ou les autorités de contrôle. Les obligations et les périodes de conservation peuvent également résulter de la législation slovaque. Par la suite, les données correspondantes seront systématiquement supprimées.

Droit à la portabilité des données. Nous sommes heureux de vous fournir, en tant que personne concernée, les données personnelles traitées par ESET au format xls.

Droit de porter plainte. En tant que personne concernée, Vous avez le droit de déposer une plainte auprès d'une autorité de contrôle à tout moment. ESET est soumise à la réglementation des lois slovaques et est tenue de respecter la législation en matière de protection des données de l'Union européenne. L'autorité de contrôle des données compétente est l'Office pour la protection des données personnelles de la République slovaque, situé à Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Coordonnées

Si vous souhaitez exercer vos droits en tant que personne concernée ou si vous avez une question ou un doute, envoyez-nous un message à l'adresse suivante :

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk