Doc publique

- Sécuriser son poste de travail
- Perte et vol d'ordinateur
- Microsoft Defender for Endpoint - Installation
- Microsoft Defender for Endpoint : Analyse un fichier, un répertoire, l'ordinateur
- Désinstallation de Symantec Endpoint Protection

Sécuriser son poste de travail

Pour minimiser les risques liés à l'utilisation de votre ordinateur et les failles de sécurité, il est conseillé de (selon les directives 6.1 et 6.6) :

- **Contacter le Help desk en cas de doute**
- Protéger son ordinateur avec un mot de passe administrateur unique
- Tenir à jour son ordinateur:
  - Appliquer les mises à jour logiciel
  - Appliquer les mises à jour système (≠ passer à un nouveau système d'exploitation, ce qui est conseillé après que l'éditeur ait publié une version x.2 ou 2 mises à jour mineures de son nouvel OS => défauts de jeunesse et compatibilité avec l'essentiel des principaux logiciels du marché en principe assurée, la vérification de la compatibilité avec des logiciels métiers relève néanmoins de la responsabilité de l'utilisateur)
  - Travailler sur un OS maintenu par l'éditeur et donc au bénéfice de régulières mises à jour de sécurité
- Utiliser les logiciels de sécurité de votre système d'exploitation:
  - Sous macOS, le logiciel XProtect est intégré et activé par défaut, pour le personnel sous contrat Unil le Ci propose en supplément la solution Microsoft Defender for EndPoint (protection accrue de la machine et du réseau Unil)
  - Sous Windows, Windows Defender est activé par défaut si vous n'utilisez pas un autre logiciel antivirus, le Ci propose également Microsoft Defender for EndPoint pour le personnel sous contrat Unil (protection accrue de la machine et du réseau Unil)
- Sauvegarder régulièrement vos données sur un support externe (le service Sauvegarde poste de travail propose gratuitement au personnel Unil sous contrat un logiciel de sauvegarde automatique des données sur des serveurs Unil)
- Suivre les règles de sécurité suivantes:
  - Ne jamais télécharger des fichiers de sites web dont on ne connait pas la provenance
  - Ne jamais installer des logiciels de développeurs inconnus
  - Ne jamais ouvrir les pièces jointes d'expéditeurs inconnus (particulièrement les fichiers se terminant par: .exe, .js)
  - Ne jamais répondre aux emails demandant de renvoyer des données confidentielles
- Utiliser des mots de passe uniques pour tous ses comptes (privés et professionnels):
  - Il existe des gestionnaires de mots de passe qui facilitent ce travail

- Mesures particulières à prendre si vous utilisez un laptop que vous déplacez régulièrement ou si vous faites du télétravail (directive 1.40):
  - si vous stockez des données personnelles ou sensibles vous avez l'obligation de chiffrer les données de votre disque, afin d'interdire à un tiers d'accéder à ces informations (par exemple en cas de vol ou de perte de la machine)
    - sur Mac utilisez FileVault (intégré à macOS)
    - sur Windows utilisez BitLocker (intégré à Windows)
    - attention à sauvegarder en lieu sûr la clé de chiffrement générée sous peine de ne plus pouvoir accéder à vos données
  - si vous vous trouvez en dehors du réseau Unil vous avez l'obligation de chiffrer vos communications pour empêcher un tiers malintentionné de les intercepter, en utilisant le VPN eduVPN mis à disposition par l'Unil.
  - pour se prémunir des vols ne jamais laisser son laptop sans surveillance.

Perte et vol d'ordinateur

Machines UNIL

> La marche à suivre découle de la directive 6.6 "Equipement informatique", en particulier son chapitre 6 "VOL ET PERTE D'ÉQUIPEMENTS INFORMATIQUES PHYSIQUES"

Déclaration à faire au plus vite

1. Remplissez au plus vite ce formulaire du service de sécurité UNISEP.
   - Dans le cas d'un vol/perte à l'étranger, une déclaration doit être faite sur place à un poste de police, afin que leur procès verbal soit annexé au formulaire d'UNISEP.
2. Informez votre unité de la perte/vol (secrétariat/hiérarchie).
   - La centrale d'achats de l'UNIL rentrera en contact avec eux·elles pour organiser le remplacement du matériel perdu/volé. Le remplacement du matériel volé sera traité de la même manière qu'un achat selon les procédures en vigueur dans votre unité.

Une fois votre déclaration reçue, UNISEP assurera la coordination avec :

- La police cantonale (pour l'enregistrement du vol et dépôt de plainte)
- L'équipe réseau (pour surveiller si la machine se reconnecte au réseau UNIL)
- La centrale d'achats (pour coordonner le remplacement du matériel avec votre unité).

Informations complémentaires sur vos données

Retrouver vos données

- Votre dossier utilisateur·trice est sauvegardé par COMET backup. Vous pourrez récupérer ces données sauvegardées depuis le site cometbackup.unil.ch, ou depuis l'application COMET backup une fois l'ordinateur de remplacement reçu.
- Si vous utilisez OneDrive, les données relatives sont également conservées et accessibles en ligne depuis m365.cloud.microsoft/onedrive, ou directement depuis l'application sur un autre ordinateur.

Bloquer l'ordinateur à distance

Le Centre informatique n'installe pas de logiciel de contrôle à distance sur les ordinateurs UNIL et n'a donc pas de pouvoir de blocage ou effacement des machines à distance. Néanmoins, si l'ordinateur perdu/volé était un Mac d'Apple, et que vous aviez activé le service de localisation via votre compte personnel iCloud, vous pouvez bloquer l'appareil à distance en suivant ces instructions.

Machines privées

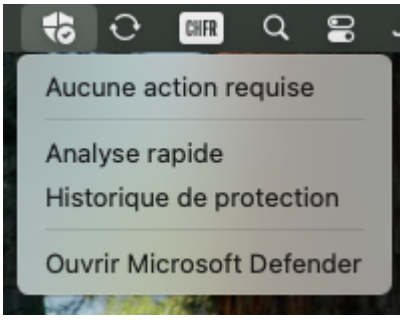
Dans le cas de perte/vol de machine privée, il est toujours possible de déclarer la perte/vol à UNISEP via leur formulaire. UNISEP pourra ainsi informer l'utilisateur·trice au cas où la machine serait retrouvée.

Microsoft Defender for Endpoint - Installation

macOS

Microsoft Defender for Endpoint est installé automatiquement sur les machines livrées dès le 1er janvier 2025.

Lorsque MDE est correctement installé et configuré, il s'affiche dans la barre des menus macOS avec une icône comportant un "vu". Le menu affiche "aucune action requise" :



Si vous n'avez pas Microsoft Defender for Endpoint sur votre Mac, vous pouvez contacter le help desk via le formulaire disponible sur notre page de distribution de logiciel. Une personne de notre équipe vous proposera un rendez-vous pour installer l'antivirus sur votre poste.

Windows

Microsoft Defender for Endpoint est installé automatiquement sur toutes les nouvelles machines standard de UNIL. Aucune action n'est nécessaire.

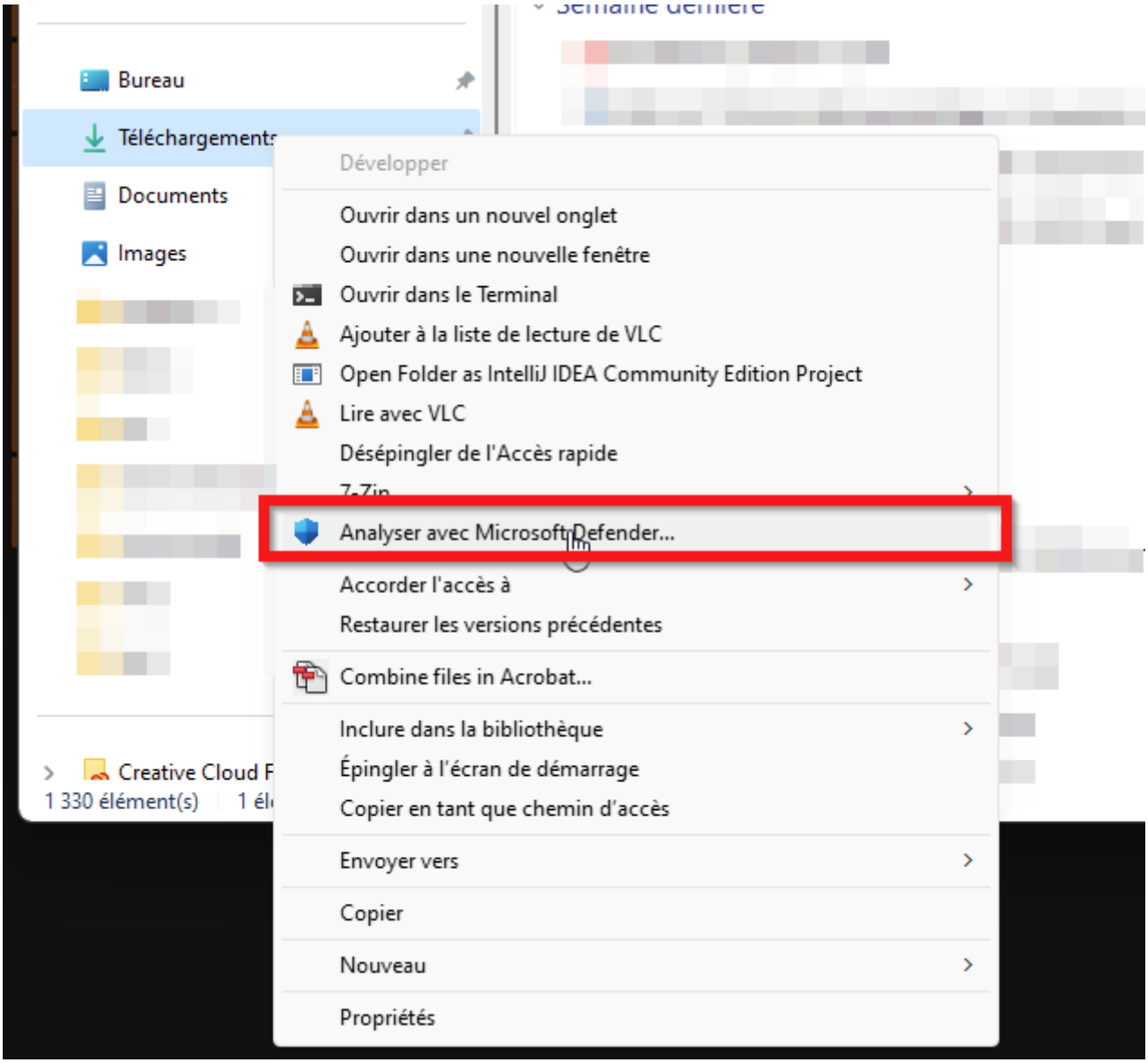
Pour les machines plus anciennes, le déploiement n'a pas été effectué de manière centralisée. Il faut faire une demande comme ci-dessus, et une personne de notre équipe vous proposera un rendez-vous pour installer l'antivirus sur votre poste.

Microsoft Defender for Endpoint : Analyse un fichier, un répertoire, l'ordinateur

Analyser un fichier ou un dossier

Windows 11

Suffit de faire clic droit sur le fichier ou dossier à analyser, et choisir "Analyser avec Microsoft Defender..."

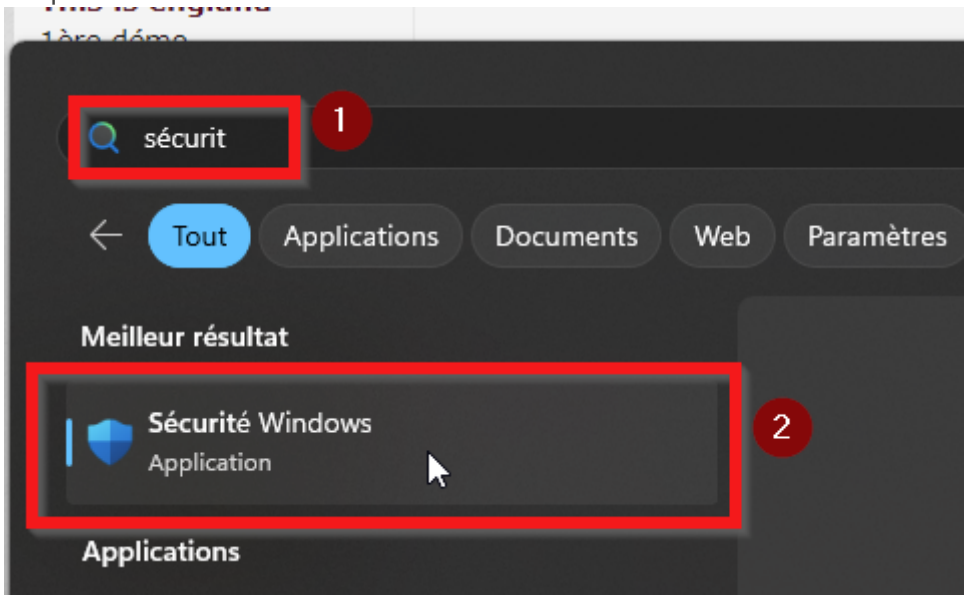


Lancer une analyse complète de votre machine

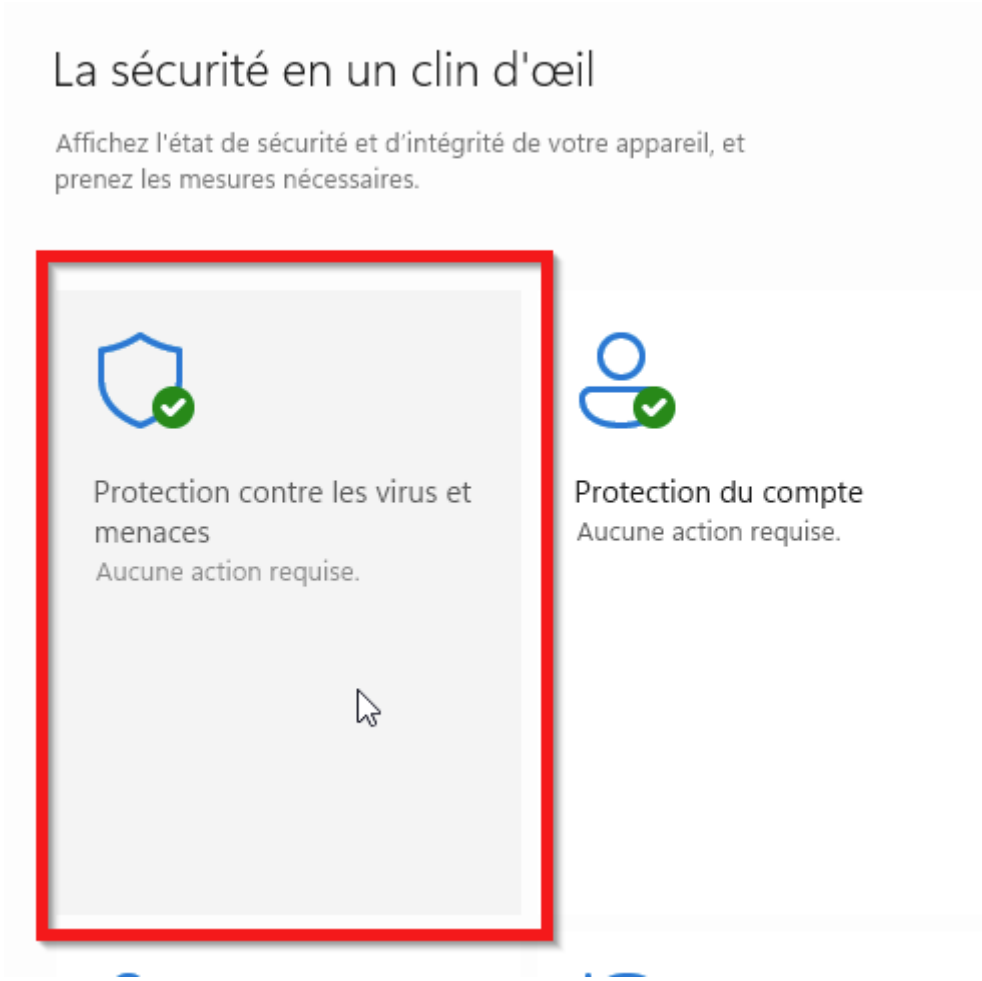
Windows 11

1. Presser sur le bouton "Démarrer"
2. Commencer à taper "sécurité"

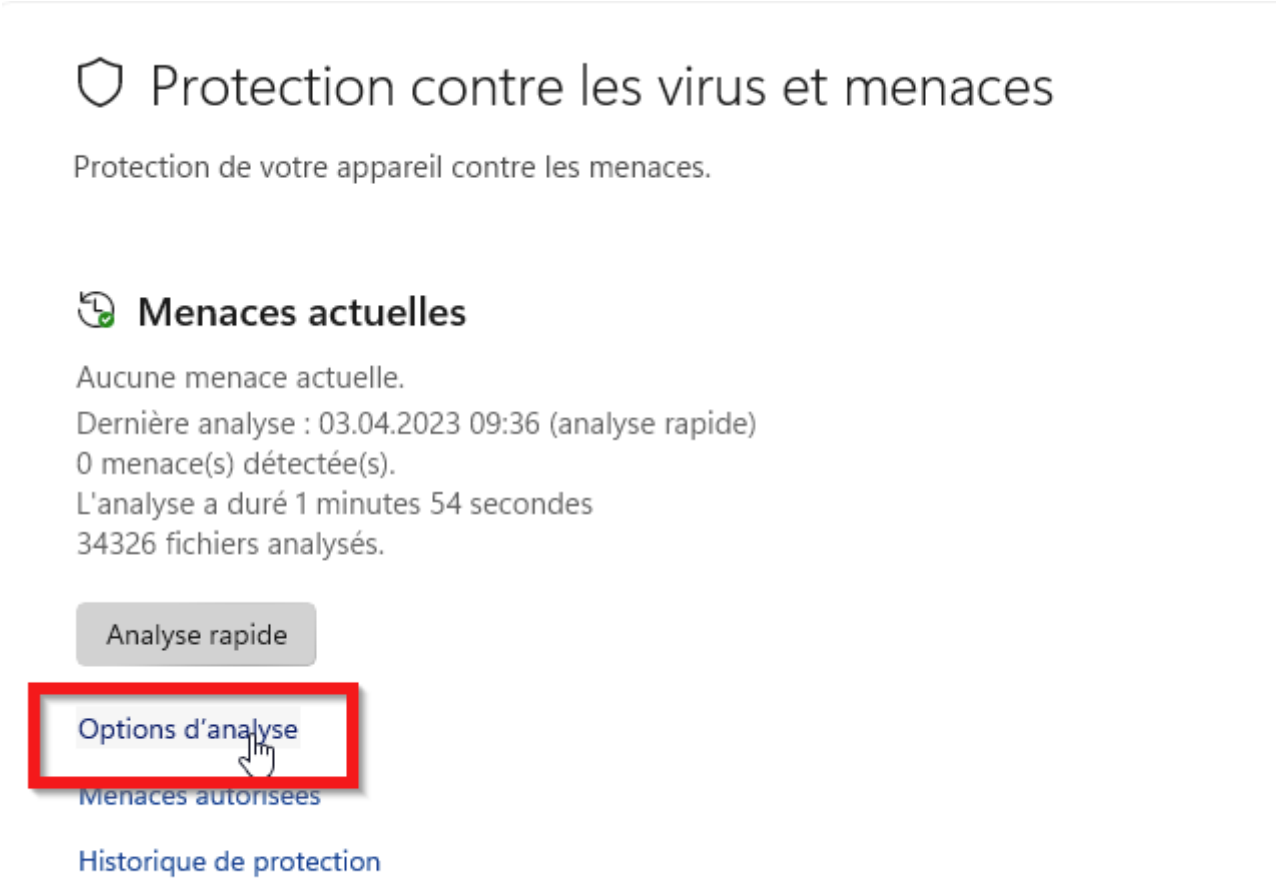
3. Cliquer sur "Sécurité Windows"



4. Sélectionner "Protection contre les virus et menaces



5. Sélectionner "options d'analyse



6. Sélectionner "Analyse complète", ou en cas de menace concrète ou malware difficile a éradiquer "Antivirus Microsoft Defender" et ensuite cliquer sur "Analyser maintenant"

Options d'analyse

Effectuez une analyse à partir des options disponibles sur cette page.

Aucune menace actuelle.
Dernière analyse : 03.04.2023 09:36 (analyse rapide)
0 menace(s) détectée(s).
L'analyse a duré 1 minutes 54 secondes
34326 fichiers analysés.

Menaces autorisées

Historique de protection

- ○ Analyse rapide

  Vérifie les dossiers de votre système où les menaces se trouvent généralement.

- ◉ Analyse complète 1

  Vérifiez tous les fichiers et les programmes en cours d'exécution sur votre disque dur. Cette analyse peut parfois durer plus d'une heure.

- ○ Analyse personnalisée

  Choisissez les fichiers et les emplacements à vérifier.

- ○ Antivirus Microsoft Defender (analyse hors connexion)

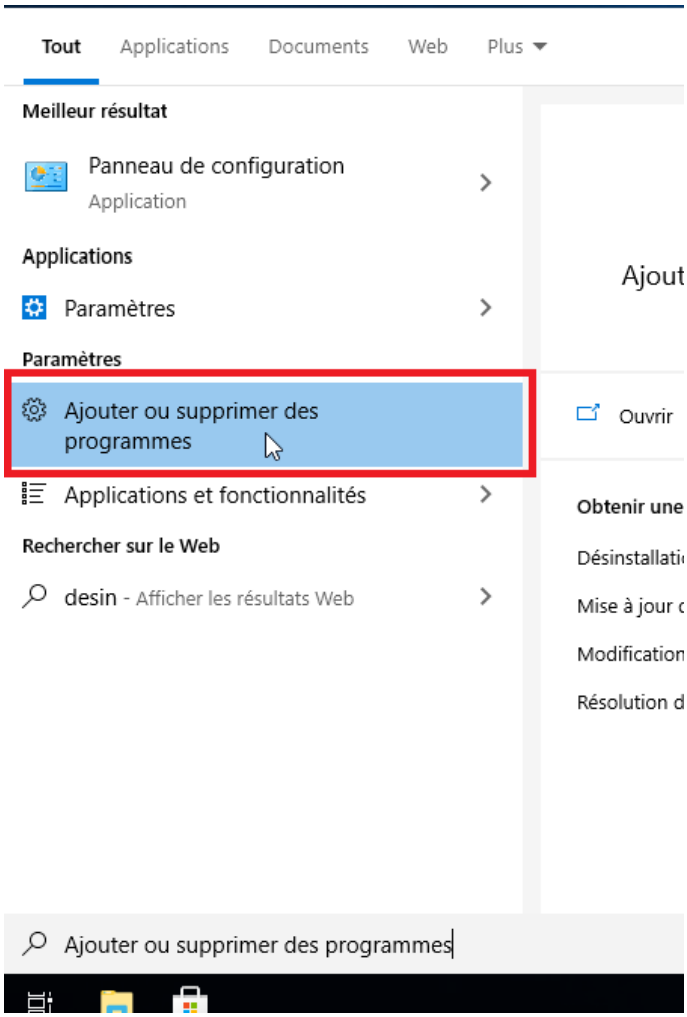
  Certains logiciels malveillants peuvent être particulièrement difficiles à supprimer de votre appareil. L'Antivirus Microsoft Defender (analyse hors connexion) peut vous aider à les détecter et à les supprimer à l'aide de définitions de menaces à jour. Cette opération va redémarrer votre PC et nécessite environ 15 minutes.

Analyser maintenant 2

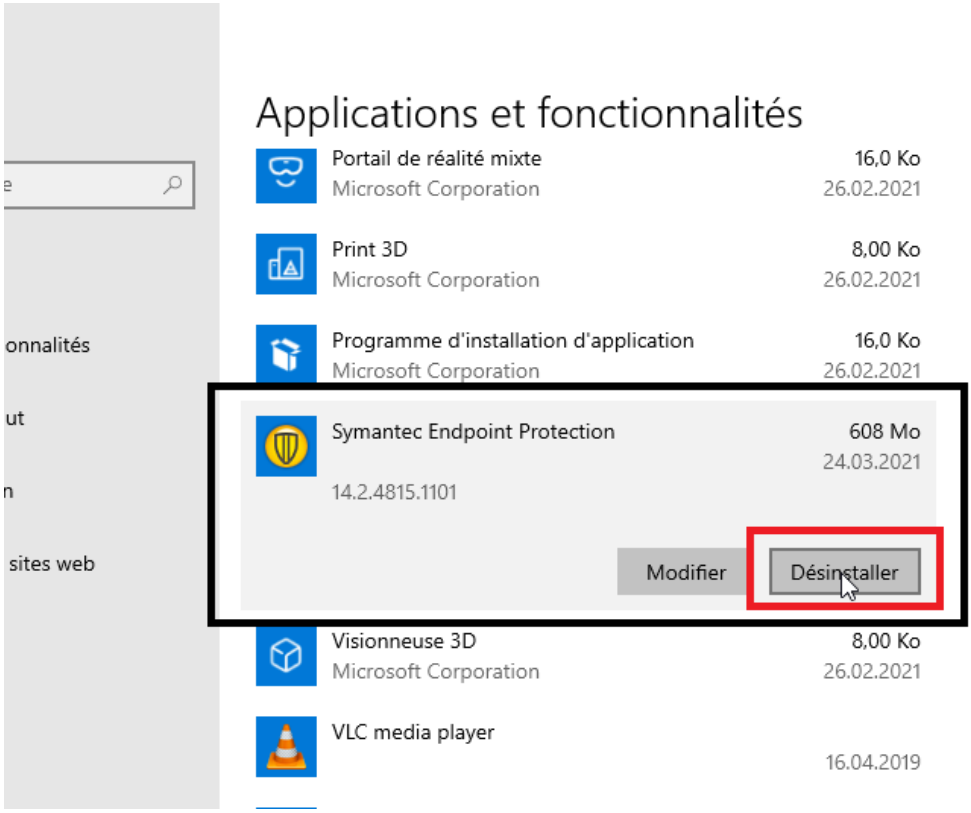
Désinstallation de Symantec Endpoint Protection

Avant d'installer un nouveau produit antivirus, il faut désinstaller Symantec Endpoint Protection si celui-ci est installé sur votre machine.

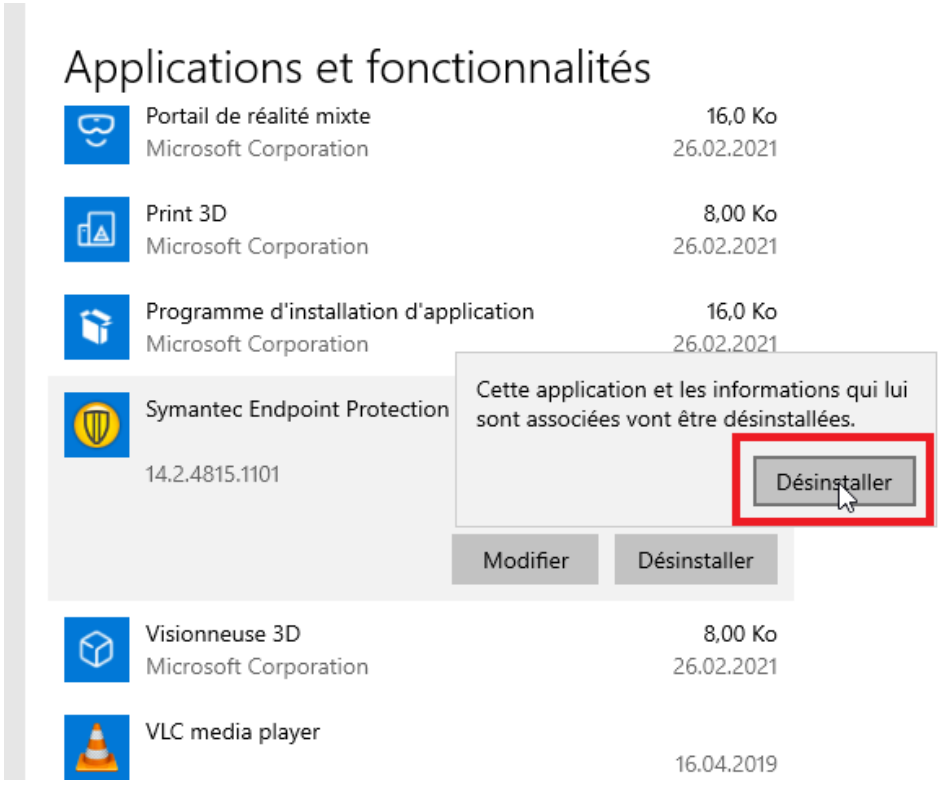
1. Menu démarrer, chercher **Ajouter ou supprimer des programmes**



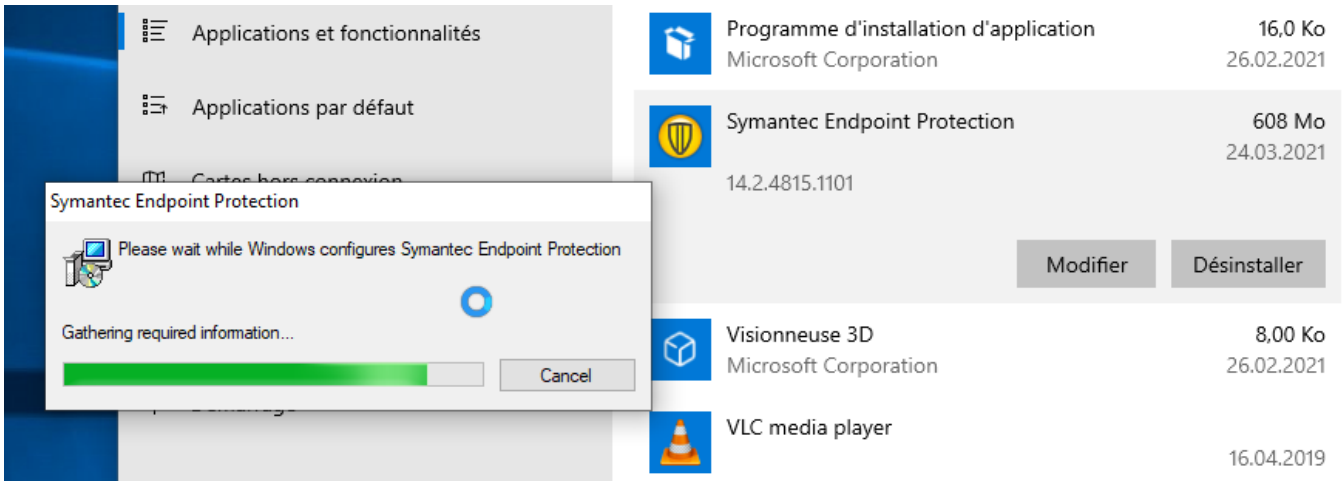
2. Sélectionner **Symantec Endpoint Protection** dans la liste des applications, et choisir **Désinstaller**



3. Sélectionner à nouveau **Désinstaller**



4. Patienter le temps que le produit se désinstalle



5. Lorsque c'est fini, accepter le redémarrage de votre ordinateur (cliquer Yes ici)

