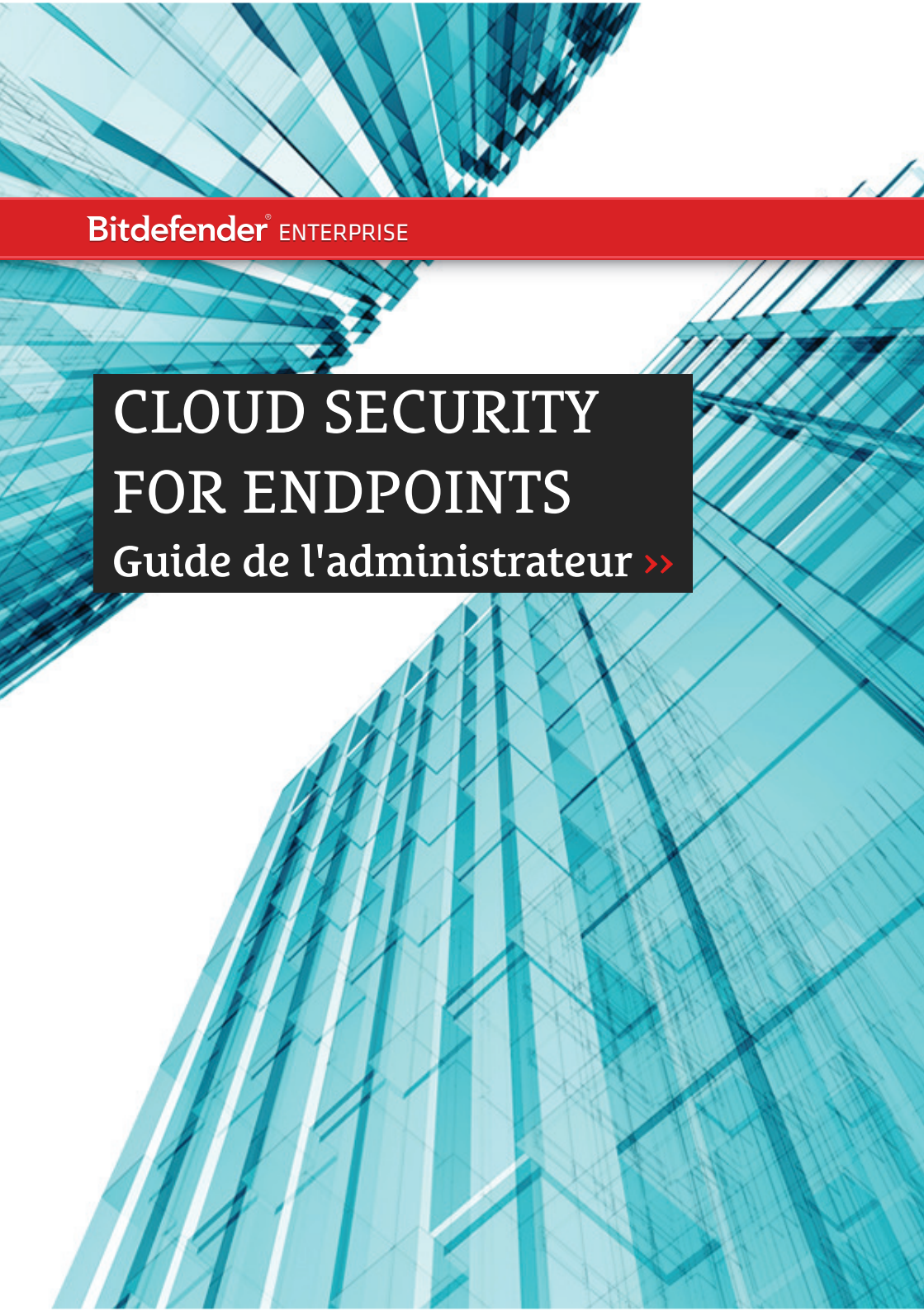

Bitdefender ENTERPRISE
CLOUD SECURITY
FOR ENDPOINTS
Guide de l'administrateur ››

Cloud Security for Endpoints by Bitdefender
Guide de l'administrateur

Date de publication 2013.07.31


Bitdefender

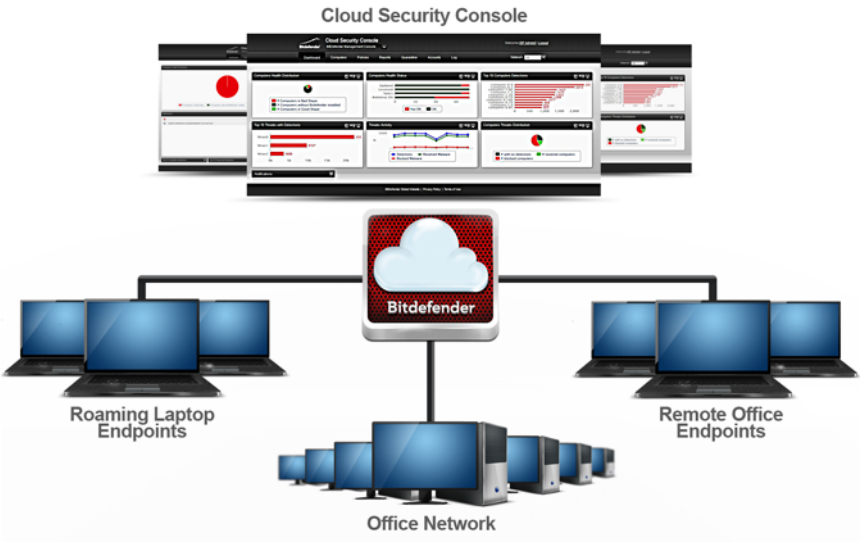
Table des matières

1. À propos de Cloud Security for Endpoints

Cloud Security for Endpoints est un service de protection antimalware cloud développé par Bitdefender pour les ordinateurs avec systèmes d'exploitation Microsoft Windows. Il utilise un modèle de déploiement multiple centralisé de "logiciel en tant que service", adapté aux entreprises, tout en bénéficiant des technologies de protection antimalware éprouvées développées par Bitdefender pour le marché des particuliers.

Ce chapitre fournit un aperçu de Cloud Security for Endpoints :

1.1. Architecture



Architecture de Cloud Security for Endpoints

Le service de sécurité est hébergé sur le cloud public de Bitdefender. Les abonnés ont accès à une interface d'administration web nommée **Cloud Security Console**. Depuis cette interface, les administrateurs peuvent installer et administrer à distance la protection antimalware sur tous leurs ordinateurs Windows tels que : les serveurs et postes de travail du réseau interne, les ordinateurs portables ou les postes de bureaux distants.

Une application locale nommée **Endpoint Security** est installée sur chaque ordinateur protégé. Les utilisateurs locaux ont une visibilité limitée et un accès en lecture seule aux paramètres de sécurité, qui sont administrés de façon centrale par l'administrateur depuis la Cloud Security Console; alors que les analyses, les mises à jour et les modifications de configuration sont généralement effectuées en tâche de fond.

Un **Serveur de mise à jour** optionnel sur site est également disponible. Le serveur de mise à jour centralise la mise à jour et la distribution d'Endpoint Client dans le réseau local, réduisant le trafic Internet des réseaux avec un grand nombre de postes de travail. Le serveur de mise à jour permet également le déploiement de la mise à jour d'Endpoint Security sur les ordinateurs du réseau n'ayant pas accès à Internet.

1.2. Comptes utilisateur

Cloud Security for Endpoints utilise un système de distribution et de déploiement intégré dans lequel différents types de comptes sont connectés dans une structure hiérarchique.

Chaque compte dispose d'une visibilité de ses comptes enfants. Pour des raisons de transparence, les actions de l'utilisateur sont mentionnées dans les journaux d'activité à la fois pour les comptes actuels et enfants.

Il existe quatre types de comptes :

1. **Partenaires** - Les distributeurs et revendeurs Cloud Security for Endpoints utilisent des comptes partenaires. Les comptes partenaires peuvent avoir deux types d'« enfants » : d'autres comptes partenaires ou des comptes clients. Lorsqu'ils étendent leur chaîne de distribution, les partenaires créent des comptes partenaires secondaires. Lorsqu'ils réalisent des ventes directement auprès d'utilisateurs finaux, ils créent des comptes sociétés. Puisque les partenaires peuvent agir en tant que fournisseurs de services de sécurité, ils ont des privilèges d'administration sur les paramètres de sécurité de leurs comptes sociétés « enfants ».
2. **Sociétés** - Les comptes sociétés sont attribués aux clients finaux lorsqu'ils achètent une licence Cloud Security for Endpoints auprès d'un partenaire. Un client disposera toujours d'un compte société unique. Un compte société est un compte maître pour l'ensemble du déploiement du client de Cloud Security for Endpoints, permettant un contrôle de premier niveau sur tous les paramètres de sécurité (sauf si remplacé par son compte partenaire parent dans le cas d'un fournisseur de services de sécurité). Depuis un compte société, les responsabilités opérationnelles peuvent être déléguées à un administrateur subordonné et aux comptes enfants rapporteurs.
3. **Administrateurs** - Les comptes administrateurs sont des comptes internes avec des privilèges d'administration sur l'ensemble du déploiement de Cloud Security for Endpoints dans l'entreprise ou sur un groupe spécifique d'ordinateurs. Les administrateurs sont responsables de la gestion active des paramètres de sécurité de Cloud Security for Endpoints. Pour plus d'informations sur les responsabilités de l'administrateur, reportez-vous à« Workflow » (p. 8).
4. **Rapporteurs** - Les comptes rapporteurs sont des comptes en lecture seule internes. Ils permettent uniquement d'accéder aux rapports et aux journaux. Ces rapports peuvent être alloués au personnel ayant des responsabilités de surveillance ou à d'autres employés devant se maintenir informés de l'état de sécurité.

Le tableau suivant résume les relations entre les types de comptes :

Compte	Utilisateurs du compte	Enfants autorisés
Partenaire	Revendeurs, Distributeurs	Partenaire, Société
Société	Clients finaux/Managers informatiques	Administrateur, Rapporteur
Administrateur	Managers informatiques, administrateurs réseau	Administrateur, Rapporteur
Rapporteur	Managers, personnel informatique divers, etc.	-

1.3. Protection contre les menaces

Cloud Security for Endpoints offre une protection contre une large gamme de menaces à l'aide des modules suivants :

- La protection antimalware basée sur l'analyse des signatures, l'analyse heuristique (B-HAVE) et l'analyse heuristique avancée basée sur le comportement (Active Virus Control) contre : les virus, les vers, les chevaux de Troie, les spywares, les adwares, les keyloggers, les rootkits et les autres types de logiciels malveillants.
- La protection Antiphishing, la barre d'outils du navigateur et Search Advisor contre le spoofing/l'usurpation de sites web et les fraudes sur Internet
- Pare-feu et Système de Détection d'Intrusion contre les attaques réseau
- Protection des données contre les tentatives d'ingénierie sociale et les fuites de données accidentelles
- Le Contrôle de contenu contre le non respect de la politique de l'entreprise liée à l'accès à Internet et à l'utilisation des applications

1.3.1. Antimalware

La technologie d'analyse antimalware de Bitdefender exploite 3 niveaux de protection :

1. Une méthode d'analyse traditionnelle est d'abord utilisée, le contenu analysé est comparé à une **base de données de signatures**. La base de données de signatures contient des morceaux de code spécifiques à certaines menaces et est régulièrement mise à jour par Bitdefender. Cette méthode d'analyse est efficace contre les menaces ayant fait l'objet de recherches et documentées. Cependant, quelle que la soit la vitesse à laquelle la base de données de signatures est mise à jour, il existe toujours une fenêtre de vulnérabilité entre le moment où une nouvelle menace est découverte et la publication de son correctif.
2. **B-HAVE**, le moteur heuristique de Bitdefender fournit un second niveau de protection contre les nouvelles menaces, inconnues. Des algorithmes heuristiques détectent les malwares en fonction de caractéristiques comportementales. B-HAVE exécute des malwares suspects dans un environnement virtuel afin de tester leur impact sur le système et de vérifier qu'ils ne constituent aucune menace. Si une menace est détectée, l'exécution du malware est bloquée.
3. Pour les menaces échappant même au moteur heuristique, un troisième niveau de protection est présent sous la forme d' **Active Virus Control (AVC)**. Active Virus Control surveille en permanence les processus en cours d'exécution et évalue les comportements suspects tels que les tentatives visant à : dissimuler le type de processus, exécuter du code dans l'espace d'un autre processus (détourner la mémoire d'un processus pour obtenir des privilèges plus élevés), se répliquer, déposer des fichiers, éviter que des processus ne soient listés par des applications énumérant des processus etc. Chaque

comportement suspect fait augmenter le score du processus. À partir d'un certain seuil, une alarme est déclenchée.

Cloud Security for Endpoints protège contre différents types de malwares,notamment :

- **Les virus** - Un virus informatique est un programme informatique qui se réplique lorsqu'il est exécuté, souvent caché à l'intérieur de fichiers exécutables légitimes, d'enregistrements d'amorçage, de fichiers de script, de macros de documents etc. Outre leur capacité à se répliquer, de nombreux virus possèdent également une charge utile, ce qui signifie qu'ils peuvent aussi effectuer des actions malveillantes sur le système hôte comme : détruire ou corrompre des données, afficher des messages insultants ou dérangeants, modifier le fonctionnement normal d'une application, installer des chevaux de Troie ou des spywares etc.
- **Les vers** - Les vers informatiques sont également des programmes informatiques capables de se répliquer et pouvant contenir des charges utiles malveillantes. Ils sont différents des virus dans la mesure où il s'agit de programmes informatiques autonomes, et qu'ils ont la capacité de se diffuser automatiquement, généralement via des réseaux informatiques.
- **Les chevaux de Troie** - Les chevaux de Troie sont des programmes informatiques qui exposent le système hôte aux attaquants, d'où leur nom. Les charges utiles typiques comprennent : l'ouverture de backdoors (méthodes permettant de contourner l'authentification), le vol de données, le piratage de systèmes afin de réaliser des envois de spam ou des attaques de déni de services, l'espionnage d'utilisateurs etc. Contrairement aux virus et aux vers, les chevaux de Troie ne se répliquent pas.
- Les **spywares** - Les spywares sont des programmes informatiques recueillant secrètement des informations sur les utilisateurs et les transmettant à une tierce partie. Les spywares sont souvent distribués avec des utilitaires gratuits et effectuent leurs activités d'espionnage des utilisateurs en plus de leur activité « officielle ».
- **Les adwares** - Les adwares sont des packages logiciels affichant de la publicité non sollicitée sous la forme de fenêtres pop-up, ou en corrompant l'interface utilisateur graphique de différentes applications, notamment les navigateurs web. Comme les spywares, ils sont souvent associés à d'autres types de logiciels plus ou moins utiles.
- **Keyloggers** - Les keyloggers enregistrent toutes les frappes de clavier des utilisateurs. Bien qu'il existe des applications de keyloggers légitimes, ceux-ci sont souvent utilisés par les pirates pour obtenir des informations confidentielles telles que des identifiants, des numéros de cartes bancaires, des adresses, etc. Ils sont généralement distribués via un cheval de Troie ou un virus.
- **Les rootkits** - Les rootkits sont des pilotes système modifiant le comportement du système d'exploitation à différentes fins. Comme les keyloggers, ils peuvent présenter des fonctionnalités bénéfiques, mais sont également souvent utilisés pour des actions malveillantes notamment pour masquer des logiciels de sécurité, empêcher la désinfection de malwares, permettre l'attribution de privilèges plus élevés à des utilisateurs non

autorisés, ouvrir des backdoors, etc. Les rootkits corrompant les fonctions de bas niveau du système d'exploitation, ils sont particulièrement difficiles à détecter et à supprimer une fois installés.

1.3.2. Antiphishing

Le module antiphishing fournit des avertissements et une protection contre le spoofing/l'usurpation de sites web et contre les fraudes sur Internet. Le module antiphishing comprend trois composants :

- La protection **Antiphishing** bloque automatiquement les pages web de phishing (usurpation de sites web/spoofing) connues afin d'empêcher que les utilisateurs ne divulguent par inadvertance des informations privées ou confidentielles à des fraudeurs en ligne. Outre l'usurpation de sites web, d'autres types de fraudes sur Internet peuvent être bloquées comme : les fraudes d'achats, les arnaques promettant de s'enrichir rapidement, les fraudes de marketing sur Internet, les fraudes au clic, etc. Au lieu de la page web malveillante, une page d'avertissement spéciale s'affiche dans le navigateur afin d'informer l'utilisateur que la page web requise est dangereuse.
- **La barre d'outils de Bitdefender** informe les utilisateurs du niveau de sécurité des pages web qu'ils consultent. En cliquant sur un petit bouton en haut de la fenêtre du navigateur, les utilisateurs peuvent voir si la page qui s'affiche est sûre, suspecte ou dangereuse.
- **Search advisor** évalue les résultats des moteurs de recherche et des liens Facebook/Twitter, en plaçant une icône devant chaque résultat. Les icônes indiquent si le lien dirige vers une page sûre, suspecte ou non sûre.

Voici les deux types de menaces bloquées par la protection antiphishing de Cloud Security for Endpoints :

- Le **Spoofing** - L'usurpation de site web (spoofing) consiste en des sites web malveillants tentant de se faire passer pour des sites légitimes pour des raisons illicites telles que recueillir les identifiants des utilisateurs ou des informations sur leur carte bancaire.
- **Fraudes sur Internet** - Sites se faisant passer pour des entreprises de confiance, et trompant les gens par différentes arnaques telles que :
  - Les **Fraudes d'achat** - Vendeurs en ligne qui ne livrent pas les produits qu'ils promeuvent
  - **Fraudes financières** - Telles que celles provenant de fausses institutions financières
  - **Les arnaques promettant de s'enrichir rapidement** - telles que les arnaques pyramidales, de travail à domicile et autres « opportunités commerciales »
  - Les **Fraudes de marketing sur Internet** - Sites malveillants recueillant des informations sur des cartes bancaires sous divers prétextes tels que la vérification de l'âge ou la vente de produits de santé douteux

- **Les fraudes au clic** - Sites trompant les visiteurs en les faisant cliquer sur des liens conduisant à d'autres endroits que ceux présentés
- La **Diffusion malhonnête** - Domaines ayant été promus à l'aide de spam, de spam dans les commentaires de blog, de fraudes au clic, d'arnaques sur les réseaux sociaux ou d'autres méthodes malhonnêtes

1.3.3. Pare-feu et Détection des intrusions

Le pare-feu et le Système de Détection d'Intrusion (IDS) protègent le système contre les menaces réseau :

- Le **Pare-feu** contrôle l'accès des applications aux ressources/services du réseau et à Internet. Une base de données complète d'applications connues, légitimes peut se voir accorder l'accès automatiquement. Le pare-feu peut également protéger le système contre le balayage de port, limiter le partage de connexion Internet et prévenir lorsque de nouveaux nœuds rejoignent une connexion Wifi.
- Le **Système de détection d'intrusion** protège le système contre certaines actions potentiellement malveillantes telles que : les injections de dll, l'installation de pilotes malveillants, la modification de fichiers Bitdefender par des applications tierces, des exploits Internet Explorer ou des tentatives de keylogging.

1.3.4. Données

Le module Protection des Données empêche que des utilisateurs ne divulguent accidentellement certaines informations confidentielles en analysant le trafic de messagerie (SMTP) et web (HTTP) sortant et en bloquant l'envoi de chaînes de texte prédéfinies. Ces chaînes de texte peuvent contenir des données sensibles telles que des noms de comptes, des noms de produits ou de technologies en développement, les coordonnées de cadres de l'entreprise etc. Il y a généralement deux situations pour ce type d'exposition :

- **L'ingénierie sociale** - Se produit lorsqu'une tierce partie tente activement de faire révéler à une personne d'une entreprise des informations confidentielles par différentes techniques : en se faisant passer pour un collègue ou un organisme officiel, en simulant de fausses situations ou en manipulant la victime afin qu'elle agisse dans l'intérêt du malfaiteur.
- **Fuites de données accidentelles** - Dans ce cas, l'utilisateur divulgue des informations confidentielles par négligence, sans y être incité en aucune façon par le destinataire. Bien qu'il ne s'agisse pas d'une tentative délibérée de vol de données, les conséquences peuvent être tout aussi graves.

1.3.5. Contrôle de contenu

Le module Controle de contenu limite l'accès des utilisateurs à Internet et aux applications en permanence, ou en fonction d'une planification. Les restrictions de l'accès en ligne peuvent également s'appliquer à : certaines adresses, le trafic HTTP ou SMTP contenant certains mots-clés, ou pour des catégories de sites web prédéfinies. Il existe plus de 30 types de sites web dont l'accès peut être limité dont ceux proposant : des jeux d'argent, du contenu pour adultes, des réseaux sociaux, du partage de fichiers, des jeux en ligne etc.

Le module Contrôle de contenu aide à appliquer les politiques de la société liées à l'accès à Internet, empêchant ainsi les pertes de productivité causées par l'oisiveté des employés et réduisant les coûts liés au trafic des données.

1.4. Workflow

Les administrateurs de Cloud Security for Endpoints peuvent effectuer une large gamme de tâches, les plus importantes concernant :

- Déploiement
- Gestion des postes de travail
- Politiques de sécurité
- Tâches d'analyse
- Rapport

1.4.1. Déploiement

Endpoint Security peut être installé localement ou à distance :

- **Installation locale** - Pour une installation locale, un kit d'installation générique ou personnalisé est exécuté sur l'ordinateur cible à partir d'un périphérique de stockage réseau ou local, ou après avoir été téléchargé à partir du cloud Bitdefender. L'administrateur peut configurer des kits d'installation personnalisés, avec des paramètres prédéfinis pour les modules installés, les mots de passe ou les emplacements de mise à niveau. Dans un déploiement typique, l'administrateur peut définir un kit d'installation personnalisé sur le cloud Bitdefender et envoyer à l'utilisateur local le lien de téléchargement correspondant par e-mail. L'utilisateur télécharge le kit d'installation et l'exécute, sans régler aucun paramètre d'installation.
- **Installation à distance** - Lorsque Endpoint Security est installé sur un ordinateur, il agit en tant qu'agent d'analyse du réseau et qu'assistant du déploiement. Les ordinateurs détectés apparaîtront dans la Cloud Security Console, permettant aux administrateurs de déployer Endpoint Security sur les autres ordinateurs du réseau local à distance.

1.4.2. Gestion des postes de travail

Les postes de travail peut être gérés individuellement ou rassemblés dans des groupes. Les groupes d'ordinateurs permettent aux administrateurs d'appliquer des politiques de sécurité et d'exécuter des rapports et des tâches d'analyse collectivement, sur plusieurs ordinateurs ayant les mêmes besoins de sécurité. Dans de grands réseaux, les groupes d'ordinateurs peuvent être gérés par différents administrateurs pour l'équilibrage de la charge de travail.

1.4.3. Politiques de sécurité

Dans Cloud Security for Endpoints, les paramètres de sécurité sont toujours gérés en tant que lot, via des politiques de sécurité. Une politique de sécurité est une configuration comprenant un ensemble spécifique de valeurs pour :

- Les paramètres de l'interface Endpoint tels que : la visibilité, les alertes d'état et des informations sur le support technique
- Des paramètres généraux tels que : la journalisation, le reporting, la protection par mot de passe et les mises à jour
- Paramètres de sécurité, c'est-à-dire : antimalware, pare-feu et modules de contrôle de contenu

En imposant l'utilisation de politiques de sécurité, les paramètres de sécurité sont toujours appliqués sous la forme de profils tout compris prédéfinis, adaptés à la fonction des ordinateurs cibles. Appliquer des paramètres de sécurité individuels à un ordinateur ou à un groupe d'ordinateurs n'est pas autorisé.

1.4.4. Tâches d'analyse

Les administrateurs peuvent exécuter des analyses manuelles sur des postes de travail administrés depuis la Cloud Security Console à tout moment. De plus, les politiques de sécurité permettent de configurer et de planifier des tâches d'analyse régulières s'exécutant automatiquement sur les ordinateurs cibles. Des tâches rapides et des analyses complètes du système peuvent s'exécuter manuellement ou en tant que tâche planifiée. Les tâches planifiées prennent également en charge des analyses personnalisées.

1.4.5. Rapport

Les rapports fournissent des représentations graphiques et des données de sécurité sur plusieurs ordinateurs ou groupes d'ordinateurs. Les données peuvent couvrir : l'état de la mise à jour d'Endpoint Security, l'état de la protection, l'état de la licence, l'activité du réseau, l'activité des malwares, les 10 malwares les plus détectés etc. Les rapports peuvent être générés manuellement, ou planifiés pour s'exécuter automatiquement, de façon régulière.

2. Pour démarrer

Cloud Security for Endpoints peut être configuré et administré à l'aide de Cloud Security Console, une interface web hébergée par Bitdefender.

En utilisant la Cloud Security Console, vous pouvez effectuer les actions suivantes :

- Installer la protection sur les postes de travail (postes de travail, portables, serveurs).
- Visualiser l'ensemble du réseau (ordinateurs administrés, ordinateurs non protégés détectés dans le réseau).
- Rechercher les informations détaillées concernant un ordinateur administré.
- Exécuter des tâches à distance sur les ordinateurs (modules d'installation, de désinstallation, d'analyse, de configuration et de protection).
- Affecter des politiques aux ordinateurs administrés afin de configurer et de gérer la protection.
- Surveiller la protection.
- Obtenir des rapports centralisés faciles à lire concernant les ordinateurs administrés.
- Consulter et gérer les fichiers en quarantaine à distance.
- Créer et gérer des comptes utilisateur pour d'autres employés de la société.
- Consulter le journal d'activité de l'utilisateur.

2.1. Connexion à la Cloud Security Console

L'accès à la Cloud Security Console se fait via les comptes utilisateur.Vous recevrez vos informations de connexion par e-mail une fois que votre compte aura été créé.

Pour se connecter à la Cloud Security Console :

1. Conditions :
   - Connexion directe à Internet
   - Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari ou Opera
   - Résolution d'écran recommandée : 1024x768 ou supérieure
2. Ouvrez votre navigateur web.
3. Rendez vous sur le site suivant : https://cloud.bitdefender.net
4. Indiquez l'adresse e-mail et le mot de passe de votre compte.
5. Cliquez sur **Connexion**.

Note

Si vous avez oublié votre mot de passe, utilisez le lien de récupération du mot de passe pour recevoir un nouveau mot de passe. Vous devez indiquer l'adresse e-mail de votre compte.

Lorsque vous vous connecterez à la console pour la première fois, on vous demandera de lire les modalités du service et de confirmer que vous les acceptez.Si vous n'acceptez pas ces modalités, vous ne pouvez pas utiliser le service.

2.2. Cloud Security Console Présentation

La Cloud Security Console est organisée afin de permettre un accès facile à toutes les fonctionnalités.

Utilisez la barre de menu de la zone supérieure pour naviguer à travers la console.

Tableau de bord
Voir des graphiques faciles à lire fournissant des informations de sécurité clés au sujet de votre réseau.

Ordinateurs
Installer la protection, gérer des ordinateurs et exécuter des tâches à distance.

Politiques
Créer, appliquer et gérer les politiques de sécurité.

Rapport
Obtenir des rapports de sécurité sur les ordinateurs administrés.

Quarantaine
Administrer à distance les fichiers en quarantaine.

Comptes
Gérer les détails et les préférences de votre compte. Créer et gérer des comptes utilisateur pour d'autres employés de la société.

Journal
Vérifier le journal d'activité de l'utilisateur.

Dans l'angle supérieur droit de la console, vous trouverez les liens suivants :

- **Nom d'utilisateur.** Cliquez sur votre nom d'utilisateur pour gérer les détails et les préférences de votre compte.
- **Aide et Support.** Cliquez sur ce lien pour trouver des informations sur l'aide et le support.
- **Déconnexion.** Cliquez sur ce lien pour vous déconnecter de votre compte.

2.3. Premières étapes

Note
Lorsque vous ouvrez la Cloud Security Console pour la première fois, une invite s'affiche vous demandant de changer de mot de passe. Cliquer dessus ouvre la page configuration ou vous pouvez spécifier un nouveau mot de passe pour votre compte.

Pour commencer :

1. Allez sur la page **Ordinateurs > Zone d'installation** et installez Endpoint Security (le logiciel client) sur les ordinateurs.Deux méthodes d'installation sont disponibles :
   - Utilisez le lien d'installation pour télécharger et installer manuellement la protection sur chaque ordinateur.
   - Installez la protection manuellement sur un ordinateur, puis utilisez l'installation à distance pour les postes de travail non protégés détectés dans le réseau.
2. Si vous administrez un grand nombre d'ordinateurs (des dizaines ou plus), organisez les en groupes afin de les gérer plus efficacement :
   a. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
   b. Créez des groupes dans le panneau de gauche en faisant un clic droit sur le groupe racine (ou sur un groupe que vous avez créé) et en sélectionnant **Créer un groupe**.
   c. Cliquez sur le groupe racine, puis sélectionnez des ordinateurs et glissez-déposez votre sélection dans le groupe souhaité.
3. Les paramètres de protection sur les ordinateurs sont configurés automatiquement en fonction de la politique de sécurité par défaut. Pour consulter les paramètres de protection par défaut, allez sur la page **Politiques > Afficher les politiques** et cliquez sur le nom de la politique par défaut.Vous pouvez modifier les paramètres de sécurité selon les besoins et paramétrer également des fonctions de protection supplémentaires.

   Si vous avez organisé les ordinateurs en groupes, vous pouvez paramétrer et appliquer des politiques différentes à chaque groupe en fonction de leurs exigences de sécurité.Pour créer des politiques supplémentaires :
   a. Allez sur la page **Politiques > Nouvelle politique** et créez une nouvelle politique.
   b. Configurez les paramètres de la politique selon vos besoins.

Veillez à maintenir à jour la protection Cloud Security for Endpoints avec les modifications sur le réseau en suivant les étapes antérieures pour tous les nouveaux ordinateurs ajoutés au réseau.

Ensuite, pour gérer et surveiller la protection, procédez comme suit :

- Consultez régulièrement la page **Tableau de bord** pour voir des informations en temps réel sur la protection Cloud Security for Endpoints.

- Allez sur la page **Rapports > Nouveau Rapport** pour créer les rapports dont vous avez besoin.Nous vous recommandons de créer des rapports planifiés pour les types de rapports dont vous avez besoin régulièrement.Pour afficher un rapport généré, allez sur la page **Rapports > Afficher les rapports** et cliquez sur le nom du rapport.
- Utilisez les tâches de la page **Ordinateurs > Afficher les ordinateurs** pour analyser les ordinateurs administrés, installer la protection à distance sur les ordinateurs non administrés, reconfigurer les modules de protection ou désinstaller complètement la protection.

2.4. Modifier le mot de passe par défaut

Nous vous recommandons de modifier le mot de passe de connexion par défaut reçu par e-mail après votre inscription au service. Nous vous recommandons également de changer régulièrement votre mot de passe de connexion.

Pour changer le mot de passe de connexion :

1. Allez sur la page **Comptes > Mon compte**.
2. Indiquez un nouveau mot de passe dans les champs correspondants (sous **Détails du compte**).
3. Cliquez sur **Soumettre** pour enregistrer les modifications.

2.5. Gérer votre compte

Pour consulter et modifier les détails et les paramètres de votre compte :

1. Allez sur la page **Comptes > Mon compte**.
2. Sous **Détails du compte**, corrigez ou actualisez les détails de votre compte.
   - **Nom et prénom.**
   - **E-mail.** Ceci est votre Login et votre e-mail de contact.Des rapports et d'importantes notifications de sécurité sont envoyés à cette adresse. Des notifications par e-mail sont envoyées automatiquement lorsque des situations présentant un risque important sont détectées dans le réseau.
   - **Mot de passe.** Pour changer votre mot de passe, saisissez-en un nouveau dans les champs correspondants.
   - **Nom de l'entreprise.**
3. **Licence** vous permet de consulter les détails de votre abonnement.Votre abonnement est géré par Bitdefender ou par le partenaire Bitdefender qui vous fournit le service.Pour plus d'informations, reportez-vous à « Abonnement au service » (p. 16).

4. **Paramètres du proxy**. Si l'entreprise utilise un serveur proxy pour se connecter à Internet, vous devez activer et configurer les paramètres proxy. Sinon, les clients installés sur les ordinateurs ne pourront pas communiquer avec Cloud Security Console.

   Note
   Pour les entreprises qui utilisent l'authentification proxy, Endpoint Security peut être installé sur les ordinateurs uniquement à l'aide du kit d'installation complet.

   Avertissement
   Si le serveur proxy de l'entreprise est sur le point d'être changé, vous devez commencer par remplacer les paramètres proxy de l'entreprise par les nouveaux dans la Cloud Security Console avant de passer au nouveau serveur proxy.

5. Sous **Paramètres**, configurez les paramètres du compte en fonction de vos préférences.
   - **Envoyer une notification par e-mail après la connexion**. Activez cette option pour être informé de chaque connexion réussie avec les identifiants de votre compte. Le message envoyé à votre adresse e-mail contiendra l'adresse IP source de la requête ainsi que la date et l'heure de la connexion.
   - **Fuseau horaire.** Choisissez dans le menu le fuseau horaire du compte. La console affichera des informations horaires en fonction du fuseau horaire sélectionné.
   - **Langue.** Choisissez dans le menu la langue d'affichage de la console.
   - Définissez comment les ordinateurs administrés de ce compte société apparaissent dans la Cloud Security Console en sélectionnant l'option appropriée dans le menu **Afficher** :
     - **Nom de l'ordinateur**, pour afficher les ordinateurs en fonction de leurs noms locaux (par exemple, `Nomdel'ordinateur`)
     - **FQDN** (Nom de domaine complet), pour afficher les ordinateurs en fonction de leur nom de système complet, comprenant leur nom local et nom de domaine (par exemple, `Nomdel'ordinateur.domaine.com`). Utilisez cette option pour distinguer plusieurs ordinateurs ayant le même nom et la même adresse IP.

       Note
       Ce paramètre s'appliquera lors de la prochaine synchronisation avec le réseau pour les ordinateurs en ligne (après 30 minutes au maximum, ou moins). Vous pouvez appliquer le paramètre immédiatement en envoyant une tâche ou une politique aux ordinateurs en ligne.

   - **Logo.** Vous pouvez remplacer le logo par défaut de la Cloud Security Console en forme de nuage par le logo de votre société.Cela vous permettra de personnaliser la mise en page du rapport PDF.Pour modifier le logo, cliquez sur **Personnaliser** et téléchargez l'image depuis votre ordinateur.Les restrictions suivantes s'appliquent :
     - Dimensions du logo : 81x41 pixels.

– Formats des fichiers pris en charge : PNG et JPG.

6. Cliquez sur **Soumettre** pour enregistrer les modifications.

Important

Vous ne pouvez pas supprimer votre propre compte.Si vous ne souhaitez plus utiliser le service Cloud Security for Endpoints et que vous souhaitez que votre compte soit supprimé, veuillez contacter votre prestataire de services.

2.6. Travailler avec des données de tableau

Les tableaux sont souvent utilisés dans la console pour organiser les données dans un format facile à utiliser. Ces informations peuvent vous être utiles :

- Les tableaux peuvent comprendre plusieurs pages (seules 10 entrées par page sont affichées par défaut).Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau. Pour modifier le nombre d'entrées affichées sur une page, sélectionnez une option dans le menu à côté des boutons de déplacement.
- Pour trouver facilement ce que vous recherchez, utilisez les zones de recherche ou les options de filtrage sous les en-têtes de colonne.
- Vous pouvez également cliquer sur les en-têtes de colonnes pour trier les données en fonction d'une colonne spécifique.Cliquez de nouveau sur l'en-tête de colonne pour inverser l'ordre de tri.

Pour vérifier que les informations affichées sont à jour, cliquez sur le bouton **Actualiser** dans l'angle inférieur gauche du tableau.

3. Abonnement au service

Vous pouvez essayer Cloud Security for Endpoints gratuitement pendant une période de 30 jours.Pendant la période d'évaluation, toutes les fonctionnalités sont disponibles et vous pouvez utiliser le service sur un nombre illimité d'ordinateurs.Avant la fin de la période d'évaluation, vous devez, si vous souhaitez continuer à utiliser le service, opter pour un plan d'abonnement payant et effectuer l'achat.

Vous pouvez vous abonner au service de deux façons :

- S'abonner via un revendeur Bitdefender.Nos revendeurs vous fourniront toutes les informations dont vous avez besoin et vous aideront à choisir le meilleur plan d'abonnement pour vous.Certains revendeurs proposent des services à valeur ajoutée, tels que le support premium, et d'autres fournissent un service entièrement géré.

  Pour trouver un revendeur Bitdefender dans votre pays :

  1. Allez à http://www.bitdefender.fr/partners/.
  2. Allez dans **Trouver un partenaire**.
  3. Les informations de contact des partenaires de Bitdefender devraient s'afficher automatiquement. Si ce n'est pas le cas, sélectionnez votre pays de résidence pour afficher les informations.
  4. Si vous ne trouvez pas de revendeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse bitdefender@editions-profil.eu.Veuillez rédiger votre e-mail en anglais pour optimiser le traitement de votre demande.

- S'abonner sur le site web Bitdefender.

Votre abonnement est géré par Bitdefender ou par le partenaire Bitdefender qui vous vend le service. Certains partenaires Bitdefender sont des fournisseurs de services de sécurité. Selon les modalités de votre abonnement, le fonctionnement quotidien de Cloud Security for Endpoints peut être géré en interne par votre société ou en externe par le fournisseur de services de sécurité.

3.1. Activer une licence

Lorsque vous achetez un abonnement payant pour la première fois, une clé de licence est générée pour vous. L'abonnement à Cloud Security for Endpoints est activé avec cette clé de licence. De nouvelles clés de licence peuvent également être émises lorsqu'un abonnement est renouvelé ou lorsque le nombre de postes de travail avec une licence augmente.

Avertissement
Activer une licence N'AJOUTE PAS ses fonctionnalités à la licence active. La nouvelle licence remplace l'ancienne. Par exemple, activer une licence de 10 postes de travail sur une licence de 100 postes de travail ne se traduira PAS par un abonnement pour 110 postes. Au contraire, cela réduira le nombre de postes protégés en le faisant passer de 100 à 10.

La clé de licence vous est envoyée par e-mail lorsque vous l'achetez. En fonction de l'accord de service, lorsque la clé de licence est émise, votre fournisseur de service peut l'activer pour vous. Vous pouvez également activer votre licence manuellement, en procédant comme suit :

1. Connectez-vous à la Cloud Security Console à l'aide de votre compte client.
2. Allez sur la page **Comptes > Mon compte**.
3. Dans la section **Licence**, cliquez sur le lien en regard du champ **No. de la licence** ou **La licence expire**. Cela ouvre la page **Informations sur la licence**, qui affiche des informations sur la licence actuelle (si une licence est active en ce moment).
4. Dans le champ **Clé de licence**, saisissez votre clé de licence.
5. Cliquez sur **Modifier la clé** et patientez jusqu'à la fin du processus d'autorisation.

3.2. Renouvellement de licence

Pour étendre une licence ou pour réactiver une licence ayant expiré, contactez votre fournisseur de service.

3.3. Augmenter le nombre de postes de travail avec une licence

Pour augmenter le nombre de postes de travail protégés par la licence actuelle, contactez le support client Bitdefender.

3.4. Vérification de l'état de votre abonnement

Pour vérifier l'état de votre abonnement :

1. Connectez-vous à la Cloud Security Console à l'aide de votre compte client.
2. Allez dans **Comptes > Mon Compte**.
3. Dans la section **Licence**, cliquez sur le lien en regard du champ **No. de la licence** ou **La licence expire**. Cela ouvre la page **Informations sur la licence**, qui affiche des informations sur l'état de votre abonnement.

4. Installer la protection sur les postes de travail

Cloud Security for Endpoints est conçu pour les stations de travail, les portables et les serveurs fonctionnant sous Microsoft® Windows.Pour protéger vos postes de travail avec Cloud Security for Endpoints, vous devez installer Endpoint Security (la solution Client) sur chacun d'entre eux.Endpoint Security gère la protection sur l'ordinateur local. Il communique également avec Cloud Security Console pour recevoir les commandes de l'administrateur et envoyer les résultats de ses actions.

Il y a deux méthodes d'installation :

- **Installation locale.** Téléchargez un kit d'installation ou un programme d'installation web et utilisez-le pour installer Endpoint Security localement, sur chaque ordinateur que vous souhaitez protéger. Les kits d'installation et les programmes d'installation web sont personnalisés à partir de l'abonnement au service pour lier automatiquement Endpoint Security au compte client correspondant.
- **Installation à distance.** Une fois installé sur un ordinateur, Endpoint Security détecte automatiquement les ordinateurs non protégés dans le réseau local.La protection Cloud Security for Endpoints peut ensuite être installée sur ces ordinateurs à distance à partir de la console. L'installation à distance s'effectue en tâche de fond, sans que l'utilisateur ne le sache.

Merci de lire attentivement et de respecter les instructions avant de préparer l'installation.

4.1. Configuration requise

Tous les services de sécurité cloud de Bitdefender sont administrés par Cloud Security Console.Puisque Cloud Security Console est hébergée, il n'y a pas de configuration matérielle et logicielle requise pour l'administration de Cloud Security for Endpoints.Il suffit de disposer d'une connexion à Internet.

Configuration minimale des postes de travail

Systèmes d'exploitation des stations de travail :

- Windows 8
- Windows 7
- Windows Vista avec Service Pack 1
- Windows XP avec Service Pack 3

Systèmes d'exploitation serveurs :

- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Server 2008 R2
- Windows Server 2008
- Windows Small Business Server (SBS) 2003
- Windows Server 2003 R2
- Windows Server 2003 avec le Service Pack 1
- Windows Home Server

Systèmes d'exploitation embarqués et pour tablettes * :

- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded avec Service Pack 2
- Windows XP Tablet PC Edition

*Les modules spécifiques du Système d'exploitation doivent être installé pour que Cloud Security for Endpoints fonctionne.

Configuration matérielle requise :

- Processeur compatible Intel® Pentium :

  Systèmes d'exploitation des stations de travail:
  - 1 GHz ou plus pour Microsoft Windows XP SP3, Windows XP SP2 64 bits et Windows 7 Enterprise (32 et 64 bits)
  - 2 GHz ou plus pour Microsoft Windows Vista SP1 ou version supérieure (32 et 64 bits), Microsoft Windows 7 (32 et 64 bits), Microsoft Windows 7 SP1 (32 et 64 bits), Windows 8
  - 800 MHZ ou plus pour Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded avec Service Pack 2, Microsoft Windows XP Tablet PC Edition

  Systèmes d'exploitation serveurs:

  - Minimum : processeur simple cœur de 2,4 GHz
  - Recommandé : processeur multicœur Intel Xeon 1,86 GHz ou plus
- Mémoire RAM :
  - Minimum : 512 Mo
  - Recommandé : 1 Go
- Disque dur : 1,5 Go d'espace libre

Connexion Internet : Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari ou Opera, pour la navigation depuis les postes de travail/serveurs ou l'accès à la Cloud Security Console

4.2. Préparation de l'Installation

Préparez l'installation comme suit :

1. Vérifiez que les ordinateurs disposent de la configuration système minimale requise.Pour certains ordinateurs, vous pouvez avoir besoin d'installer le dernier service pack du système d'exploitation disponible ou de libérer de l'espace disque.Établissez une liste d'ordinateurs ne correspondant pas aux critères nécessaires afin que vous puissiez les exclure de l'administration.
2. Désinstaller des ordinateurs (ne pas simplement désactiver) tout logiciel antimalware, pare-feu ou de sécurité Internet.Faire fonctionner simultanément Cloud Security for Endpoints avec d'autres logiciels de sécurité installés sur l'ordinateur peut affecter leur fonctionnement et causer d'importants problèmes avec le système.

   Beaucoup de programmes de sécurité sont incompatibles avec Cloud Security for Endpoints, ils seront automatiquement détectés et supprimés lors de l'installation de Endpoint Security.Pour en savoir plus et pour vérifier la liste des logiciels de sécurité détecté, merci de vous référer à cet article.

   Important
   Ne vous occupez pas des fonctionnalités de sécurité Windows (Windows Defender, Pare-Feu Windows) puisqu'elles seront désactivées automatiquement avant le lancement de l'installation.

3. L'installation requiert des privilèges d'administration. Les installations basées sur le programme d'installation web nécessitent également un accès à Internet. Vérifiez que ces conditions sont remplies.

4.3. Installation locale

L'installation locale peut être effectuée par vous-même, en vous connectant à chaque ordinateur, ou vous pouvez demander de l'aide aux utilisateurs des ordinateurs. Elle requiert d'exécuter localement un fichier d'installation, que vous pouvez télécharger à partir de Cloud Security Console.Deux types de fichiers d'installation sont disponibles :

- **Programme d'installation web.** Le programme d'installation web commence par télécharger le kit d'installation complet sur les serveurs cloud Bitdefender avant de démarrer l'installation. Il est peu volumineux et peut être exécuté à la fois sur les systèmes 32 et 64 bits (ce qui facilite sa distribution). Il requiert par contre une connexion active à Internet.

- **Kit d'installation complète.** Il s'agit du package d'installation complet, qui doit être utilisé pour installer la protection sur les ordinateurs sans connexion Internet, ou avec une connexion lente.Téléchargez ce fichier sur un ordinateur connecté à Internet puis transmettez-le à d'autres ordinateurs à l'aide de supports de stockage externes ou d'un partage réseau.Notez que deux versions sont disponibles : l'une pour les systèmes 32 bits et l'autre pour les systèmes 64 bits. Veillez à utiliser la version adaptée à l'ordinateur sur lequel vous l'installez.

Pour obtenir ou distribuer le lien de téléchargement pour l'installation locale :

1. Connectez vous à la Cloud Security Consoleen utilisant votre compte.
2. Allez sur la page **Ordinateurs > Zone d'installation**.
3. Vous pouvez, si vous le souhaitez, configurer les options d'installation en cliquant sur **Personnaliser le package**.Pour plus d'informations, reportez-vous à « Personnalisation du package d'installation » (p. 24).
4. Pour afficher le lien, cliquez sur le bouton **Lien d'installation** et sélectionnez **Afficher**.Utilisez le lien approprié pour télécharger le fichier d'installation souhaité (le programme d'installation web ou le kit d'installation complet), que vous pouvez ensuite exécuter sur l'ordinateur local pour installer la protection.Vous pouvez également copier le fichier sur des supports de stockage externes et l'exécuter sur d'autres ordinateurs.
5. Une autre option consiste à envoyer aux utilisateurs du réseau de l'organisation un e-mail avec le lien d'installation, leur demandant de télécharger et d'installer la protection sur leur ordinateur.(Vous devez avoir un client de messagerie par défaut configuré sur votre ordinateur).Pour envoyer le lien par e-mail, cliquez sur le bouton **Lien d'installation** et sélectionnez **Envoyer par e-mail**.Veuillez noter que les utilisateurs reçoivent le lien du programme d'installation web.

Une fois que le fichier d'installation est stocké en local, pour installer manuellement la protection sur un ordinateur :

1. Localiser le fichier téléchargé et double-cliquez dessus.

Note

En utilisant l'installateur Web, le package d'installation complet est téléchargé d'Internet.Le temps de téléchargement dépend de votre connexion Internet.Une fois le téléchargement terminé, l'installation démarrera automatiquement.

2. Le programme d'installation recherche tout d'abord la présence d'autres logiciels de sécurité sur le système.

   Si un programme antivirus incompatible est détecté, on vous demandera de le désinstaller de votre système.Veuillez suivre les indications pour supprimer les logiciels de votre système, évitant ainsi que des problèmes ne surviennent par la suite.

Note

Il est nécessaire de redémarrer l'ordinateur pour terminer la désinstallation des programmes antivirus détectés. L'installation reprendra automatiquement au redémarrage de l'ordinateur.

3. Patientez jusqu'à la fin de l'installation.Les zones critiques de votre système font l'objet d'une analyse antivirus, les dernières versions des fichiers d'applications sont téléchargées et installées, et les services de Bitdefender sont lancés. Cette étape peut prendre quelques minutes.
4. Cliquez sur **Terminer**.

4.4. Installation à distance

Pour faciliter le déploiement, Cloud Security for Endpoints intègre un mécanisme de découverte automatique du réseau qui permet à la partie poste de travail (Endpoint Security) d'être installée à distance depuis la Cloud Security Console.Les ordinateurs détectés sont affichés en tant que **ordinateurs non administrés** sur la page **Ordinateurs**.Pour plus d'informations sur la fonction Network Discovery, merci de vous référer à « Fonctionnement de la Découverte du réseau » (p. 25).

Pour activer le Network Discovery et l'installation à distance, vous devez déjà avoir installé Endpoint Security sur au moins un ordinateur du réseau. Cet ordinateur sera utilisé pour analyser le réseau et installer Endpoint Security sur les ordinateurs non protégés.

Note

Une fois Endpoint Security installé sur un ordinateur, quelques minutes peuvent être nécessaires pour que les autres ordinateurs du réseau deviennent visibles dans la Cloud Security Console.

Note

Chaque ordinateur cible doit avoir le partage d'administration admin$ activé pour que l'installation fonctionne.

Pour installer à distance la protection :

1. Connectez vous à la Cloud Security Consoleen utilisant votre compte.
2. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
3. Cliquez sur le menu **Afficher** situé au-dessus du tableau (à gauche) et sélectionnez **Ordinateurs non administrés**.
4. Si vous avez organisé les ordinateurs en groupes, sélectionnez le groupe souhaité dans le panneau de gauche. Pour afficher tous vos ordinateurs, faites un clic droit sur le groupe racine et sélectionnez **Afficher tous les ordinateurs**.

5. Cochez les cases correspondant aux ordinateurs sur lesquels vous souhaitez installer la protection.
6. Cliquez sur **Tâches Rapides** et sélectionnez **Installer Client** dans le menu.La fenêtre Options d'installation s'affichera.
7. Configurer les options d'installation :
   a. Sélectionnez les modules de protection que vous voulez installer.Veuillez noter que seule la protection antimalware est disponible pour les systèmes d'exploitation serveurs.
   b. Vous pouvez, si vous le souhaitez, définir un mot de passe pour empêcher les utilisateurs de supprimer la protection. Sélectionnez **Mot de passe de désinstallation** et indiquez le mot de passe souhaité dans les champs correspondants.
   c. Lors de l'installation silencieuse, l'ordinateur fait l'objet d'une analyse antimalware. Un redémarrage du système peut être nécessaire pour terminer la désinfection de malwares.

      Sélectionnez **Redémarrer automatiquement (si nécessaire)** afin de vous assurer que les malwares détectés ont été complètement supprimés avant l'installation.Sinon, l'installation peut échouer.
   d. Si un serveur de mise à jour local Bitdefender est configuré dans le réseau, vous pouvez configurer Endpoint Security pour qu'il se mette à jour à partir de ce serveur plutôt qu'à partir d'Internet.Remplacez l'adresse de mise à jour sur Internet du champ **Emplacement des mises à jour** par l'adresse du serveur local de mise à jour.Utilisez l'une des syntaxes suivantes :
      - `ip_du_serveur_de_mise_à_jour : port`
      - `nom_du_serveur_de_mise_à_jour : port`

      Le port par défaut est 7074.

      Pour en savoir plus, reportez-vous à « Utiliser Update Server » (p. 102).

      Note

      L'adresse de mise à jour configurée ici est utilisée momentanément après l'installation.Dès qu'une politique est appliquée au client, l'emplacement des mises à jour est modifié en fonction des paramètres de la politique.Pour vous assurer que le client continue à se mettre à jour à partir du serveur local de mise à jour, configurez les options de l'emplacement des mises à jour dans les paramètres de la politique.

   e. L'installation à distance est effectuée à partir d'un ordinateur sur lequel Cloud Security for Endpoints est déjà installé (ordinateur de déploiement).Si vous souhaitez utiliser un ordinateur spécifique pour l'installation à distance, décochez la case **Détecter automatiquement l'ordinateur de déploiement**, commencez à taper le nom ou l'adresse IP de l'ordinateur dans le champ correspondant et sélectionnez l'ordinateur dans la liste.

f. Indiquez les informations d'identification d'administration requises pour l'authentification à distance sur les ordinateurs sélectionnés.

   Saisissez le nom d'utilisateur et le mot de passe d'un compte administrateur pour tous les ordinateurs sélectionnés. Si les ordinateurs sont dans un domaine, il suffit d'indiquer les identifiants de l'administrateur du domaine. Utilisez les conventions Windows lorsque vous indiquez le nom d'un compte d'utilisateur de domaine (par exemple, `domaine\utilisateur` ou `utilisateur@domaine.com`).

8. Cliquez sur **Installer**.Une fenêtre de confirmation s'affichera.
9. Vous pouvez afficher et administrer la tâche sur la page **Ordinateurs > Afficher les tâches**.

4.5. Personnalisation du package d'installation

Vous pouvez personnaliser le package d'installation en choisissant les modules de protection à installer et en configurant les options d'installation par défaut. La configuration par défaut est adaptée à la plupart des scénarios d'installation.

Pour personnaliser le package d'installation :

1. Allez sur la page **Ordinateurs > Zone d'installation**.
2. Cliquez sur le bouton **Personnaliser le package** dans l'angle supérieur droit de la page.
3. Sélectionnez les modules de protection que vous voulez installer.

   Antimalware
   Le module Antimalware protège le système contre tous les types de malwares (virus, chevaux de Troie, spywares, rootkits, adwares, etc.).

   Pare-feu
   Le pare-feu protège votre ordinateur contre les tentatives de connexions entrantes et sortantes non autorisées.

   Contrôle de contenu
   Le module Contrôle de contenu vous aide à contrôler l'accès des utilisateurs à Internet et aux applications.Veuillez noter que les paramètres configurés du Contrôle de contenu s'appliqueront à tous les utilisateurs qui se connecteront aux ordinateurs cibles.

   Note
   Veuillez noter que seule la protection antimalware est disponible pour les systèmes d'exploitation serveurs.

4. Vous pouvez, si vous le souhaitez, définir un mot de passe pour empêcher les utilisateurs de supprimer la protection. Sélectionnez **Mot de passe de désinstallation** et indiquez le mot de passe souhaité dans les champs correspondants.

5. Lors de l'installation silencieuse, l'ordinateur fait l'objet d'une analyse antimalware. Un redémarrage du système peut être nécessaire pour terminer la désinfection de malwares.

   Sélectionnez **Redémarrer automatiquement (si nécessaire)** afin de vous assurer que les malwares détectés ont été complètement supprimés avant l'installation.Sinon, l'installation peut échouer.

6. Si un serveur de mise à jour local Bitdefender est configuré dans le réseau, vous pouvez configurer Endpoint Security pour qu'il se mette à jour à partir de ce serveur plutôt qu'à partir d'Internet.Remplacez l'adresse de mise à jour sur Internet du champ **Emplacement des mises à jour** par l'adresse du serveur local de mise à jour.Utilisez l'une des syntaxes suivantes :
   - `ip_du_serveur_de_mise_à_jour : port`
   - `nom_du_serveur_de_mise_à_jour : port`

   Le port par défaut est 7074.

   Pour en savoir plus, reportez-vous à « Utiliser Update Server » (p. 102).

   Note

   L'adresse de mise à jour configurée ici est utilisée momentanément après l'installation.Dès qu'une politique est appliquée au client, l'emplacement des mises à jour est modifié en fonction des paramètres de la politique.Pour vous assurer que le client continue à se mettre à jour à partir du serveur local de mise à jour, configurez les options de l'emplacement des mises à jour dans les paramètres de la politique.

7. Cliquez sur **Enregistrer** pour enregistrer les modifications. Toutes les installations futures à partir de votre compte utiliseront la configuration par défaut que vous avez faite.

4.6. Fonctionnement de la Découverte du réseau

Cloud Security for Endpoints utilise le **service Explorateur d'ordinateurs de Microsoft** pour effectuer la découverte du réseau.Le service Explorateur d'ordinateurs est une technologie de réseau utilisée par les ordinateurs Windows pour maintenir des listes actualisées de domaines, groupes de travail et les ordinateurs qui s'y trouvent et pour fournir ces listes aux ordinateurs clients sur demande.Les ordinateurs détectés dans le réseau par le service Explorateur d'ordinateurs peuvent être consultés en exécutant la commande **net view** dans une fenêtre d'invite de commandes.

Important

Cloud Security for Endpoints n'utilise pas d'informations du réseau d'Active Directory ou de la fonctionnalité Mappage réseau disponible dans Windows Vista et versions ultérieures.Le mappage réseau exploite une technologie de découverte du réseau différente : le protocole LLTD (Link Layer Topology Discovery).

Cloud Security for Endpoints n'est pas impliqué activement dans le fonctionnement du service Explorateur d'ordinateurs. Endpoint Security demande uniquement au service Explorateur d'ordinateurs la liste des postes de travail et serveurs visibles dans le réseau (nommée liste de parcours) puis l'envoie à Cloud Security Console.Cloud Security Console gère la liste de parcours, en ajoutant les ordinateurs détectés récemment à sa liste d'**Ordinateurs non administrés**.Les ordinateurs détectés auparavant ne sont pas supprimés après une nouvelle requête de découverte du réseau, vous devez donc exclure & supprimer manuellement les ordinateurs qui ne sont plus dans le réseau.

La requête initiale de la liste de parcours est effectuée par le premier Endpoint Security installé dans le réseau.

- Si Endpoint Security est installé sur l'ordinateur d'un groupe de travail, seuls les ordinateurs de ce groupe de travail seront visibles dans Cloud Security Console.
- Si Endpoint Security est installé sur l'ordinateur d'un domaine, seuls les ordinateurs de ce domaine seront visibles dans Cloud Security Console.Les ordinateurs d'autres domaines peuvent être détectés s'il y a une relation d'approbation avec le domaine dans lequel Endpoint Security est installé.

Les requêtes de découverte du réseau suivantes sont réalisées régulièrement à chaque heure. Pour chaque nouvelle requête, Cloud Security Console divise l'espace des ordinateurs administrés en des zones de visibilité puis désigne un Endpoint Security dans chaque zone pour effectuer la tâche.Une zone de visibilité est un groupe d'ordinateurs qui se détectent les uns les autres. Une zone de visibilité est généralement définie par un groupe de travail ou domaine, mais cela dépend de la topologie et de la configuration du réseau. Dans certains cas, une zone de visibilité peut consister en de multiples domaines et groupes de travail.

Si un Endpoint Security sélectionné ne parvient pas à effectuer la requête, Cloud Security Console attend la requête suivante planifiée, sans choisir d'autre Endpoint Security pour réessayer.

Pour une visibilité complète du réseau, Endpoint Security doit être installé sur au moins un ordinateur de chaque groupe de travail ou domaine de votre réseau. Idéalement, Endpoint Security devrait être installé sur au moins un ordinateur de chaque sous-réseau.

4.6.1. Plus d'informations sur le service Explorateur d'ordinateurs de Microsoft

Présentation rapide du service Explorateur d'ordinateurs :

- Fonctionne indépendamment d'Active Directory.
- Fonctionne exclusivement sur les réseaux IPv4 et opère de manière indépendante, dans les limites d'un groupe LAN (groupe de travail ou domaine).Une liste de parcours est établie et gérée pour chaque groupe LAN.

- Utilise généralement des diffusions de serveurs sans connexion pour communiquer entre les nœuds.
- Utilise NetBIOS sur TCP/IP (NetBT).
- Nécessite une résolution de noms NetBIOS. Il est recommandé d'avoir une infrastructure WINS (Windows Internet Name Service) opérationnelle dans le réseau.
- N'est pas activé par défaut dans Windows Server 2008 et 2008 R2.

Pour des informations détaillées sur le service Explorateur d'ordinateurs, consultez le sujet technique Computer Browser Service sur Microsoft Technet.

4.6.2. Configuration requise par la découverte du réseau

Afin de découvrir tous les ordinateurs (serveurs et postes de travail) qui seront administrés depuis la Cloud Security Console, les conditions suivantes doivent être remplies :

- Les ordinateurs doivent faire partie d'un groupe de travail ou d'un domaine et être connectés via un réseau local IPv4.Le service Explorateur d'ordinateurs ne fonctionne pas sur les réseaux IPv6.
- Plusieurs ordinateurs dans chaque groupe LAN (groupe de travail ou domaine) doivent exécuter le service Explorateur d'ordinateurs. Les contrôleurs principaux de domaine doivent également exécuter le service.
- NetBIOS sur TCP/IP (NetBT) doit être activé sur les ordinateurs.Le pare-feu local doit autoriser le trafic NetBT.
- Le partage de fichiers doit être activé sur les ordinateurs.Le pare-feu local doit autoriser le partage de fichiers.
- Une infrastructure WINS (Windows Internet Name Service) doit être installée et opérationnelle.
- Pour Windows Vista et les versions ultérieures, la découverte du réseau doit être activée (**Panneau de configuration > Centre Réseau et partage > Modifier les paramètres de partage avancés**).

  Pour pouvoir activer cette fonctionnalité, les services suivants doivent d'abord être lancés :
  - DNS Client
  - Function Discovery Resource Publication
  - SSDP Discovery
  - UPnP Device Host
- Dans les environnements avec plusieurs domaines, il est recommandé d'établir des relations d'approbation entre les domaines afin que les ordinateurs puissent accéder aux listes de parcours d'autres domaines.

Les ordinateurs à partir desquels Endpoint Security demande le service Explorateur d'ordinateurs doivent être capables de résoudre les noms NetBIOS.

Note
Le mécanisme de découverte du réseau fonctionne pour tous les systèmes d'exploitation supportés, y compris les versions Windows Embedded, à condition de disposer de la configuration requise.

5. Gestion des ordinateurs

Pour voir les ordinateurs sous votre compte, allez sur la page **Ordinateurs > Afficher les ordinateurs**.Sur la page **Afficher les ordinateurs** vous pouvez :

- Organisez les ordinateurs dans des groupes pour gérer leur sécurité plus efficacement.Cela est recommandé si vous administrez un grand nombre d'ordinateurs (des dizaines ou plus).
- Vérifiez les détails de l'ordinateur et de la protection.
- Afficher et modifier les paramètres de la politique de sécurité.
- Exécutez des tâches à distance sur les ordinateurs pour les analyser, installer la protection Cloud Security for Endpoints ou modifier l'installation actuelle.Pour en savoir plus, reportez-vous à « Exécuter et gérer des tâches » (p. 38).
- Créez des rapports rapides afin d'obtenir différentes informations de sécurité sur certains ordinateurs.

En plus des ordinateurs protégés par Cloud Security for Endpoints, vous pouvez également voir les autres ordinateurs détectés dans le réseau. Pour en savoir plus, reportez-vous à « Fonctionnement de la Découverte du réseau » (p. 25).

La page est constituée de deux panneaux :

- Le panneau de gauche vous aide à organiser les ordinateurs dans des groupes.
- Le panneau de droite contient un tableau affichant des informations sur les ordinateurs sous votre compte.Toutes les informations utiles concernant les ordinateurs enregistrés sont réparties dans les colonnes du tableau :
  - Nom et adresse IP de l'ordinateur.
  - Système d'exploitation installé sur l'ordinateur.
  - État de la mise à jour de la protection Cloud Security for Endpoints.
  - Quand l'ordinateur a été vu pour la dernière fois.

Note
Il est important de surveiller le champ **Dernière consultation** car de longues périodes d'inactivité peuvent signifier qu'il existe un problème de communication ou qu'un ordinateur est déconnecté.

L'icône située en regard du nom de chaque ordinateur vous informe à propos de l'ordinateur :

Ordinateur sur lequel la protection Cloud Security for Endpoints est installée.

Ordinateur sur lequel la protection Cloud Security for Endpoints n'a pas encore été installée.
L'ordinateur que vous avez exclu de l'administration.

5.1. À propos des ordinateurs administrés, non administrés et exclus

Les ordinateurs sont organisés en trois catégories principales :

- **Ordinateurs administrés** - ordinateurs sur lesquels la protection Cloud Security for Endpoints est installée.
- **Ordinateurs non administrés** - ordinateurs détectés sur lesquels la protection Cloud Security for Endpoints n'est pas encore installée.

> **Note**
> Une fois installé sur un ordinateur, Endpoint Security détecte automatiquement les ordinateurs non protégés dans le réseau local.Par la suite, le Network Discovery est effectué toutes les heures.Les ordinateurs non administrés seront disponibles sur la page **Afficher les ordinateurs** lors de leur détection.

- **Ordinateurs exclus** - ordinateurs que vous avez exclus de l'administration.

Utilisez le menu **Afficher** au-dessus du tableau (à gauche) pour choisir les catégories d'ordinateurs à afficher.

5.2. A propos des ordinateurs hors-ligne

Les ordinateurs hors-ligne ont normalement la protection Cloud Security for Endpoints d'installée, mais il n'y a aucune activité récente de Endpoint Security.Les ordinateurs sont signalés hors-ligne si Endpoint Security est inactif pendant plus d'1 minute.

Les raisons pour lesquelles vos ordinateurs apparaissent hors-ligne :

- L'ordinateur est arrêté, en veille ou en veille prolongée.

> **Note**
> Les ordinateurs apparaissent normalement en ligne, même quand ils sont verrouillés ou que l'utilisateur est déconnecté.

- Endpoint Security a été désinstallé manuellement de l'ordinateur.Dans de tels cas, vous devez supprimer manuellement l'ordinateur à partir de la page **Ordinateurs > Voir les ordinateurs**.
- L'ordinateur n'a pas d'accès Internet ou la communication avec Cloud Security Console est bloquée par un pare-feu.La seconde raison, plus improbable, est que la communication se fasse par le protocole HTTPS.Le problème peut se produire si vous protégez les

ordinateurs en utilisant un autre pare-feu que le pare-feu Endpoint Security. Il pourrait aussi être causé par un pare-feu réseau ou un routeur.

- Endpoint Security pourrait ne pas fonctionner correctement.

Pour connaître le temps d'inactivité des ordinateurs :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Vérifier le champ **Dernière Visite**Pour trouver facilement l'information dont vous avez besoin, choisissez **Hors-ligne** dans le menu correspondant, puis trier les ordinateurs par période d'inactivité en cliquant sur l'en-tête de colonne.

Vous pouvez ignorer les périodes d'inactivité les plus courtes (minutes, heures), car elles sont probablement le résultat d'une condition temporaire.Par exemple, l'ordinateur est actuellement arrêté.

De longues périodes d'inactivité (jours, semaines) indiquent en général un problème avec l'ordinateur.

5.3. Utilisation des groupes d'ordinateurs

Si vous administrez un nombre important d'ordinateurs (des dizaines ou plus), vous aurez probablement besoin de les organiser dans des groupes. Organiser vos ordinateurs dans des groupes vous aide à les gérer plus efficacement. L'un des principaux avantages est que vous pouvez utiliser des politiques de groupes pour répondre à différents besoins en sécurité.

Les groupes d'ordinateurs s'affichent dans le panneau de gauche de la page **Afficher les ordinateurs**.Il n'y a au départ que le groupe racine qui porte le nom de votre société. Tous les ordinateurs sur lesquels vous avez installé la protection Cloud Security for Endpoints ainsi que ceux détectés dans le réseau sont placés automatiquement dans ce groupe. Vous pouvez organiser vos ordinateurs en créant des groupes sous le groupe racine et en plaçant les ordinateurs dans le groupe approprié.

Important
Veuillez noter ceci :

- Un groupe peut contenir à la fois des ordinateurs et d'autres groupes.
- Lors de la sélection d'un groupe dans le panneau de gauche, vous pouvez afficher tous les ordinateurs à l'exception de ceux placés dans ses sous-groupes.Pour afficher tous les ordinateurs du groupe et de ses sous-groupes, faites un clic droit sur le groupe et sélectionnez **Afficher tous les ordinateurs**.

Avant de commencer à créer des groupes, pensez aux raisons pour lesquelles vous en avez besoin et ayez en tête un modèle de regroupement.Vous pouvez par exemple regrouper les ordinateurs en fonction d'un critère ou d'une combinaison des critères suivants :

- Structure de l'organisation (Ventes, Marketing, Assurance Qualité, Développement logiciel, Gestion etc.).

- Besoins en sécurité (Ordinateurs de bureau, Portables, Serveurs etc.).
- Emplacement (siège, bureaux locaux, travailleurs à distance, bureaux à domicile etc.).

Création de groupes

Pour diviser votre réseau en groupes :

1. Faites un clic droit sur le groupe racine du panneau de gauche et sélectionnez **Créer un groupe**.Un nouveau groupe (appelé **Nouveau groupe**) apparaîtra sous le groupe parent dans le menu arborescent.
2. Renommer le groupe créé.
3. Suivez les étapes précédentes pour créer des groupes supplémentaires.
4. Déplacez les ordinateurs du groupe racine vers le groupe approprié.

Pour créer des sous-groupes :

1. Faites un clic droit sur le groupe dans lequel le nouveau sous-groupe doit être incorporé et sélectionnez **Créer un groupe**.Un nouveau groupe (appelé **Nouveau groupe**) apparaîtra sous le groupe parent dans le menu arborescent.
2. Renommer le groupe créé.

Renommer des groupes

Pour renommer un groupe, faites un clic droit dessus, sélectionnez **Renommer le groupe** et entrez le nouveau nom.

Déplacer des groupes

Les groupes peuvent être déplacés n'importe où à l'intérieur de la hiérarchie des groupes. Pour déplacer un groupe, glissez-déposez-le de l'emplacement actuel vers le nouvel emplacement.

Placer les ordinateurs dans un autre groupe

Pour déplacer les ordinateurs du groupe actuel vers un autre :

1. Cochez les cases correspondant aux ordinateurs que vous souhaitez déplacer.
2. Glissez-déposez votre sélection dans le groupe souhaité du panneau de gauche.

Supprimer des groupes

Vous pouvez uniquement supprimer les groupes vides (qui ne contiennent pas d'ordinateurs).

Pour supprimer un groupe :

1. Placez tous les ordinateurs du groupe dans d'autres groupes.Si le groupe comprend des sous-groupes, vous pouvez choisir de déplacer des sous-groupes entiers plutôt que des ordinateurs individuels.
2. Faites un clic droit sur le groupe et sélectionnez **Supprimer le groupe**.Vous devrez confirmer votre action en cliquant sur **Oui**.

5.4. Recherche et tri des ordinateurs

En fonction du nombre d'ordinateurs, le tableau des ordinateurs peut occuper plusieurs pages (seules 10 entrées sont affichées par page par défaut).Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau. Pour modifier le nombre d'entrées affichées sur une page, sélectionnez une option dans le menu à côté des boutons de déplacement.

S'il y a trop d'entrées, vous pouvez utiliser les zones de recherche ou les menus sous les en-têtes de colonne afin de filtrer les données affichées. Vous pouvez, par exemple, rechercher un ordinateur spécifique ou choisir d'afficher uniquement les ordinateurs hors ligne.

Vous pouvez également cliquer sur les en-têtes de colonnes pour trier les données en fonction d'une colonne spécifique.Par exemple, si vous voulez classer les ordinateurs par nom, cliquez sur l'en-tête **Nom de l'ordinateur**.Si vous cliquez de nouveau sur l'en-tête, les ordinateurs s'afficheront dans l'ordre inverse.

Lorsque vous utilisez des groupes, sélectionnez un groupe dans le panneau de gauche pour afficher les ordinateurs qu'il contient. Veuillez noter que les ordinateurs placés dans des sous-groupes ne s'affichent pas par défaut. Pour afficher tous les ordinateurs du groupe et de ses sous-groupes, faites un clic droit sur le groupe et sélectionnez **Afficher tous les ordinateurs**.

5.5. Vérification des détails de l'ordinateur et de la protection.

Vous trouverez sur la page **Afficher les ordinateurs** différentes informations sur les ordinateurs :

- Informations générales sur l'ordinateur, telles que son nom, son adresse IP ou son système d'exploitation.
- Paramètres de la politique de sécurité.
- État de la licence et de la mise à jour de la protection Cloud Security for Endpoints.
- État des modules de protection Cloud Security for Endpoints sur l'ordinateur (installé ou non, activé ou désactivé).
- État de la mise à niveau d'Endpoint Client.

- Informations concernant les malwares détectés sur l'ordinateur.
- Dernier journal d'analyse.

Pour obtenir des détails sur l'ordinateur et la protection :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Si vous avez organisé les ordinateurs en groupes, sélectionnez le groupe souhaité dans le panneau de gauche. Pour afficher tous vos ordinateurs, faites un clic droit sur le groupe racine et sélectionnez **Afficher tous les ordinateurs**.
3. Cliquez sur le nom de l'ordinateur qui vous intéresse. La page détails de l'ordinateur s'affiche.Cliquez sur les liens disponibles pour plus d'informations.

5.6. Vérification et modification des paramètres de sécurité

Les politiques de sécurité sur les ordinateurs sont administrées à l'aide de politiques. Pour plus d'informations, reportez-vous à « Politiques de sécurité » (p. 46).

Pour afficher les paramètres de sécurité appliqués à un ordinateur spécifique :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Cliquez sur le menu **Afficher** situé au-dessus du tableau (à gauche) et sélectionnez **Ordinateurs administrés**.
3. Si vous avez organisé les ordinateurs en groupes, sélectionnez le groupe souhaité dans le panneau de gauche. Pour afficher tous vos ordinateurs, faites un clic droit sur le groupe racine et sélectionnez **Afficher tous les ordinateurs**.
4. Cliquez sur le nom de l'ordinateur qui vous intéresse.
5. Consultez le champ **Politique active**.Cliquez sur le nom de la politique pour afficher ses paramètres.
6. Vous pouvez modifier les paramètres de sécurité selon vos besoins.Veuillez noter que toutes les modifications que vous apporterez s'appliqueront également à tous les autres ordinateurs sur lesquels la politique est active.

5.7. Création de rapports rapides

Pour créer des rapports rapides à partir de la page **Afficher les ordinateurs** :

1. Cliquez sur le menu **Afficher** situé au-dessus du tableau (à gauche) et sélectionnez **Ordinateurs administrés**.
2. Si vous avez organisé les ordinateurs en groupes, sélectionnez le groupe souhaité dans le panneau de gauche. Pour afficher tous vos ordinateurs, faites un clic droit sur le groupe racine et sélectionnez **Afficher tous les ordinateurs**.

3. Cochez les cases correspondant aux ordinateurs que vous souhaitez inclure dans le rapport.
4. Cliquez sur **Rapports** et choisissez le type de rapport dans le menu.Les rapports d'activité contiennent uniquement des données de la semaine précédente.

5.8. Exclusion d'ordinateurs de l'administration

Endpoint Security détecte automatiquement les ordinateurs non protégés du réseau.Les ordinateurs détectés apparaissent dans la Cloud Security Console comme non administrés de sorte que vous pouvez y installer à distance une protection.

Si vous ne prévoyez pas d'administrer certains ordinateurs détectés, vous pouvez les placer dans la liste **Ordinateurs exclus**. De cette façon, ils ne vous dérangeront pas.

Pour exclure les ordinateurs détectés de l'administration :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Cliquez sur le menu **Afficher** situé au-dessus du tableau (à gauche) et sélectionnez **Ordinateurs non administrés**.
3. Cochez les cases correspondant aux ordinateurs que vous souhaitez exclure.
4. Cliquez sur le bouton **Tâches Rapides** dans l'angle supérieur droit de la page et sélectionnez **Exclure**.

Si le protection est installée manuellement sur un ordinateur exclu, celui-ci sera automatiquement placé dans la liste **Ordinateurs administrés**.

Pour voir les ordinateurs exclus :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Dans le menu au-dessus du tableau, choisissez **Ordinateurs exclus**.

5.9. Restaurer / Supprimer les ordinateurs exclus

Les ordinateurs exclus ne peuvent pas être restaurés directement dans la liste **Ordinateurs non administrés**.Si vous souhaitez restaurer un ordinateur exclu, vous devez le supprimer de la console.Si l'ordinateur supprimé est toujours connecté au réseau, il sera finalement détecté et apparaîtra en tant qu'ordinateur non administré dans la console.

Pour supprimer les ordinateurs exclus :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Dans le menu au-dessus du tableau, choisissez **Ordinateurs exclus**.
3. Cochez les cases correspondant aux ordinateurs que vous souhaitez supprimer.
4. Cliquez sur le bouton **Tâches Rapides** dans l'angle supérieur droit de la page et sélectionnez **Supprimer**.

Note

Cela prendra jusqu'à une heure pour que les ordinateurs supprimés soient détectés de nouveau.Certains ordinateurs peuvent être détectés seulement après plusieurs heures.

5.10. Supprimer les ordinateurs administrés

Supprimer les ordinateurs administrés de la console :

- Pour supprimer la protection d'un ordinateur administré.
- Pour supprimer les doublons et les ordinateurs inactifs de la liste des ordinateurs administrés. Lorsque vous réinstallez le système d'exploitation ou supprimez la protection de certains ordinateurs, vous devez supprimer manuellement les entrées correspondantes de la liste.

Si l'ordinateur supprimé est toujours connecté au réseau, il sera finalement détecté et apparaîtra en tant qu'ordinateur non administré dans la console.

Pour supprimer les ordinateurs administrés :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Cliquez sur le menu **Afficher** situé au-dessus du tableau (à gauche) et sélectionnez **Ordinateurs administrés**.
3. Si vous avez organisé les ordinateurs en groupes, sélectionnez le groupe souhaité dans le panneau de gauche. Pour afficher tous vos ordinateurs, faites un clic droit sur le groupe racine et sélectionnez **Afficher tous les ordinateurs**.
4. Cochez les cases correspondant aux ordinateurs que vous souhaitez supprimer.

   Note

   - Consultez le champ **Dernière consultation** pour identifier les ordinateurs inactifs depuis longtemps.
   - Recherchez ou triez les ordinateurs par nom pour identifier les doublons ou les ordinateurs déconnectés en permanence du réseau.

5. Cliquez sur le bouton **Tâches Rapides** dans l'angle supérieur droit de la page et sélectionnez **Désinstaller Endpoint**.La protection sera désinstallée des ordinateurs sélectionnés et ceux-ci seront supprimés de la console.

5.11. Supprimer les ordinateurs non administrés

La liste des ordinateurs non administrés est régulièrement mise à jour avec les nouveaux ordinateurs détectés sur le réseau.Les ordinateurs qui ne sont plus détectés, restent dans la liste jusqu'à ce que vous les supprimiez manuellement.

Vous devez commencer par exclure un ordinateur non administré afin de le supprimer de la console.Si l'ordinateur supprimé est toujours connecté au réseau, il sera finalement détecté et apparaîtra en tant qu'ordinateur non administré dans la console.

Pour supprimer les ordinateurs non administrés :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Exclure les ordinateurs que vous souhaitez supprimer :
   a. Dans le menu au-dessus du tableau, choisissez **Ordinateurs non administrés**.
   b. Cochez les cases correspondant aux ordinateurs que vous souhaitez supprimer.
   c. Cliquez sur le bouton **Tâches Rapides** dans l'angle supérieur droit de la page et sélectionnez **Exclure**.
3. Supprimer les ordinateurs exclus :
   a. Dans le menu au-dessus du tableau, choisissez **Ordinateurs exclus**.
   b. Cochez les cases correspondant aux ordinateurs que vous souhaitez supprimer.
   c. Cliquez sur le bouton **Tâches Rapides** dans l'angle supérieur droit de la page et sélectionnez **Supprimer**.

6. Exécuter et gérer des tâches

La page **Afficher les ordinateurs** vous permet d'exécuter à distance un certain nombre de tâches d'administration sur les ordinateurs.Voici ce que vous pouvez faire :

- Installer la protection sur les ordinateurs détectés..
- Analyser les ordinateurs administrés à la recherche de malwares.
- Désinstaller la protection des ordinateurs.
- Modifier l'installation pour reconfigurer les modules de protection.
- Mettre à niveau Endpoint Client.

6.1. Installer la protection sur les ordinateurs non administrés

Une fois que vous avez installé un client Cloud Security for Endpoints dans un réseau, il détecte automatiquement les ordinateurs non protégés de ce réseau. La protection Cloud Security for Endpoints peut ensuite être installée sur ces ordinateurs à distance à partir de la console. L'installation à distance s'effectue en tâche de fond, sans que l'utilisateur ne le sache.

Avertissement

Avant l'installation, veillez à désinstaller les logiciels antimalware et pare-feu des ordinateurs. Installer Cloud Security for Endpoints sur des logiciels de sécurité existants peut affecter leur fonctionnement et causer d'importants problèmes avec le système.Windows Defender et le Pare-feu Windows seront automatiquement désactivés lorsque l'installation démarrera.

Pour installer à distance la protection Cloud Security for Endpoints sur un ou plusieurs ordinateurs détectés :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Cliquez sur le menu **Afficher** situé au-dessus du tableau (à gauche) et sélectionnez **Ordinateurs non administrés**.
3. Si vous avez organisé les ordinateurs en groupes, sélectionnez le groupe souhaité dans le panneau de gauche. Pour afficher tous vos ordinateurs, faites un clic droit sur le groupe racine et sélectionnez **Afficher tous les ordinateurs**.
4. Cochez les cases correspondant aux ordinateurs sur lesquels vous souhaitez installer la protection.

5. Cliquez sur **Tâches Rapides** et sélectionnez **Installer** dans le menu.La fenêtre Options d'installation s'affichera.
6. Configurer les options d'installation :
   a. Sélectionnez les modules de protection que vous voulez installer.Veuillez noter que seule la protection antimalware est disponible pour les systèmes d'exploitation serveurs.
   b. Vous pouvez, si vous le souhaitez, définir un mot de passe pour empêcher les utilisateurs de supprimer la protection. Sélectionnez **Mot de passe de désinstallation** et indiquez le mot de passe souhaité dans les champs correspondants.
   c. Lors de l'installation silencieuse, l'ordinateur fait l'objet d'une analyse antimalware. Un redémarrage du système peut être nécessaire pour terminer la désinfection de malwares.

      Sélectionnez **Redémarrer automatiquement (si nécessaire)** afin de vous assurer que les malwares détectés ont été complètement supprimés avant l'installation.Sinon, l'installation peut échouer.
   d. Si un serveur de mise à jour local Bitdefender est configuré dans le réseau, vous pouvez configurer Endpoint Security pour qu'il se mette à jour à partir de ce serveur plutôt qu'à partir d'Internet.Remplacez l'adresse de mise à jour sur Internet du champ **Emplacement des mises à jour** par l'adresse du serveur local de mise à jour.Utilisez l'une des syntaxes suivantes :
      - `ip_du_serveur_de_mise_à_jour : port`
      - `nom_du_serveur_de_mise_à_jour : port`

      Pour en savoir plus, reportez-vous à « Utiliser Update Server » (p. 102).

      Note

      L'adresse de mise à jour configurée ici est utilisée momentanément après l'installation.Dès qu'une politique est appliquée au client, l'emplacement des mises à jour est modifié en fonction des paramètres de la politique.Pour vous assurer que le client continue à se mettre à jour à partir du serveur local de mise à jour, configurez les options de l'emplacement des mises à jour dans les paramètres de la politique.

   e. L'installation à distance est effectuée à partir d'un ordinateur sur lequel Cloud Security for Endpoints est déjà installé (ordinateur de déploiement).Si vous souhaitez utiliser un ordinateur spécifique pour l'installation à distance, décochez la case **Détecter automatiquement l'ordinateur de déploiement**, commencez à taper le nom ou l'adresse IP de l'ordinateur dans le champ correspondant et sélectionnez l'ordinateur dans la liste.
   f. Indiquez les informations d'identification d'administration requises pour l'authentification à distance sur les ordinateurs sélectionnés.

Saisissez le nom d'utilisateur et le mot de passe d'un compte administrateur pour tous les ordinateurs sélectionnés. Si les ordinateurs sont dans un domaine, il suffit d'indiquer les identifiants de l'administrateur du domaine. Utilisez les conventions Windows lorsque vous indiquez le nom d'un compte d'utilisateur de domaine (par exemple, `domaine\utilisateur` ou `utilisateur@domaine.com`).

7. Cliquez sur **Installer le Client**.Une fenêtre de confirmation s'affichera.
8. Vous pouvez afficher et administrer la tâche sur la page **Ordinateurs > Afficher les tâches**.

6.2. Analyse des ordinateurs administrés

Il y a trois façons d'analyser les ordinateurs protégés par Cloud Security for Endpoints :

- L'utilisateur connecté à l'ordinateur peut lancer une analyse à partir de l'interface utilisateur Endpoint Security.
- Vous pouvez créer des tâches d'analyse planifiées à l'aide de la politique.
- Exécutez une tâche d'analyse immédiate à partir de la console.

Pour exécuter une tâche d'analyse à distance sur un ou plusieurs ordinateurs :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Cliquez sur le menu **Afficher** situé au-dessus du tableau (à gauche) et sélectionnez **Ordinateurs administrés**.
3. Si vous avez organisé les ordinateurs en groupes, sélectionnez le groupe souhaité dans le panneau de gauche. Pour afficher tous vos ordinateurs, faites un clic droit sur le groupe racine et sélectionnez **Afficher tous les ordinateurs**.
4. Cochez les cases correspondant aux ordinateurs que vous souhaitez analyser.
5. Cliquez sur **Tâches Rapides** et sélectionnez **Analyser** dans le menu.
6. Sélectionnez le type d'analyse à réaliser :
   - **Quick Scan** utilise l'analyse in-the-cloud pour détecter les malwares présents sur le système.La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.
   - L'**Analyse Complète du Système** analyse l'ensemble de votre ordinateur en vue de détecter tous les types de malwares menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.
7. Cliquez sur **Requérir une analyse**.Une fenêtre de confirmation s'affichera.
8. Vous pouvez afficher et administrer la tâche sur la page **Ordinateurs > Afficher les tâches**.

6.3. Désinstaller la protection des ordinateurs

Pour désinstaller à distance la protection Cloud Security for Endpoints sur un ou plusieurs ordinateurs :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Cliquez sur le menu **Afficher** situé au-dessus du tableau (à gauche) et sélectionnez **Ordinateurs administrés**.
3. Si vous avez organisé les ordinateurs en groupes, sélectionnez le groupe souhaité dans le panneau de gauche. Pour afficher tous vos ordinateurs, faites un clic droit sur le groupe racine et sélectionnez **Afficher tous les ordinateurs**.
4. Cochez les cases correspondant aux ordinateurs sur lesquels vous souhaitez désinstaller la protection.
5. Cliquez sur **Tâches Rapides** et sélectionnez **Désinstaller Endpoint** dans le menu.
6. Si vous n'avez pas prévu de réinstaller le service, décochez l'option **Conserver les fichiers mis en quarantaine**.
7. Cliquez sur **Désinstaller** pour créer et envoyer la tâche de désinstallation pour les ordinateurs sélectionnés.Une fenêtre de confirmation vous informe immédiatement si la tâche a été créée avec succès.

Note
Si vous souhaitez réinstaller la protection, vous devez d'abord redémarrer l'ordinateur.

6.4. Configuration des modules installés

Pour modifier les modules de protection installés sur un ou plusieurs ordinateurs :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Cliquez sur le menu **Afficher** situé au-dessus du tableau (à gauche) et sélectionnez **Ordinateurs administrés**.
3. Si vous avez organisé les ordinateurs en groupes, sélectionnez le groupe souhaité dans le panneau de gauche. Pour afficher tous vos ordinateurs, faites un clic droit sur le groupe racine et sélectionnez **Afficher tous les ordinateurs**.
4. Cochez les cases correspondant aux ordinateurs sur lesquels vous souhaitez reconfigurer la protection.
5. Cliquez sur **Tâches Rapides** et sélectionnez **Configurer les modules** dans le menu.
6. Sélectionnez les modules de protection que vous voulez installer.

Antimalware
Le module Antimalware protège le système contre tous les types de malwares (virus, chevaux de Troie, spywares, rootkits, adwares, etc.).

Pare-feu
Le pare-feu protège votre ordinateur contre les tentatives de connexions entrantes et sortantes non autorisées.

Contrôle de contenu
Le module Contrôle de contenu vous aide à contrôler l'accès des utilisateurs à Internet et aux applications.Veuillez noter que les paramètres configurés du Contrôle de contenu s'appliqueront à tous les utilisateurs qui se connecteront aux ordinateurs cibles.

Note
Veuillez noter que seule la protection antimalware est disponible pour les systèmes d'exploitation serveurs.

7. Cliquez sur **Configurer** pour appliquer les modifications aux ordinateurs.

6.5. Mise à niveau d'Endpoint Client

Depuis juillet 2013, Endpoint Client inclus dans Cloud Security for Endpoints a été remplacé par Endpoint Security. Nous vous recommandons de mettre à niveau vers le nouveau client dès que possible. Une nouvelle tâche a été ajoutée à la liste des **Tâches Rapides** ; elle vous permet d'exécuter la mise à niveau du client sur chaque ordinateur avec l'état Non mis à jour.

Pour mettre à niveau le client à distance sur les ordinateurs administrés :

1. Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
2. Cliquez sur le menu **Afficher** situé au-dessus du tableau (à gauche) et sélectionnez **Ordinateurs administrés**.
3. Si vous avez organisé les ordinateurs en groupes, sélectionnez le groupe souhaité dans le panneau de gauche. Pour afficher tous vos ordinateurs, faites un clic droit sur le groupe racine et sélectionnez **Afficher tous les ordinateurs**.
4. Dans l'en-tête de colonne **Mis à jour**, sélectionnez **Non mis à niveau** pour afficher uniquement les anciens postes de travail clients.
5. Cochez les cases des ordinateurs sur lesquels vous souhaitez exécuter une mise à niveau du client.
6. Cliquez sur **Tâches Rapides** et sélectionnez **Mettre à niveau Endpoint** dans le menu.

   La fenêtre Mettre à niveau Endpoint apparaîtra.
7. Configurer les options de mise à niveau :

- Sélectionnez uniquement les modules de protection Endpoint Security que vous voulez installer :

  Antimalware

  Le module Antimalware protège le système contre tous les types de malwares (virus, chevaux de Troie, spywares, rootkits, adwares, etc.).

  Pare-feu

  Le pare-feu protège votre ordinateur contre les tentatives de connexions entrantes et sortantes non autorisées.

  Contrôle de contenu

  Le module Contrôle de contenu vous aide à contrôler l'accès des utilisateurs à Internet et aux applications.Veuillez noter que les paramètres configurés du Contrôle de contenu s'appliqueront à tous les utilisateurs qui se connecteront aux ordinateurs cibles.

  Note
  Veuillez noter que seule la protection antimalware est disponible pour les systèmes d'exploitation serveurs.

- Précisez l'heure à laquelle vous souhaitez que les postes de travail se mettent à niveau :
  - Utilisez l'option **Désactiver la mise à niveau** pour annuler une tâche de mise à niveau créée. Cette option est utile puisque les tâches de mise à niveau ne sont pas administrées sur la page **Ordinateurs > Afficher les tâches**.
  - Sélectionnez **Mettre à niveau** pour effectuer immédiatement la mise à niveau d'Endpoint.
  - Sélectionnez **Planifier la mise à niveau** pour spécifier la fréquence d'exécution de la mise à niveau d'Endpoint Client sur les ordinateurs sélectionnés. Cette option est utile pour les postes de travail qui ne peuvent pas terminer la tâche de mise à niveau (comme les ordinateurs éteints ou hors ligne) et si vous souhaitez exécuter la tâche régulièrement, afin de vous assurer qu'elle s'est bien terminée.

    Vous pouvez planifier une mise à niveau à l'aide des options suivantes :
    - Pour exécuter de nouveau la tâche régulièrement, indiquez la fréquence pour la période sélectionnée (par exemple, exécuter la tâche toutes les 3 heures).
    - Pour exécuter de nouveau la tâche à un certain moment, cochez **Commencer à exécuter la tâche à :** et spécifiez la date et l'heure dans les champs correspondants.
    - Vous pouvez également choisir d'arrêter l'exécution de la tâche de mise à niveau à un certain moment en utilisant l'option **Cesser d'exécuter la tâche à :**. Dans ce cas, toutes les mises à niveau en cours seront arrêtées à l'heure spécifiée.

- Vous pouvez également choisir d'**Exécuter la tâche dès que possible lorsqu'un lancement planifié n'a pas été effectué** en sélectionnant l'option correspondante.

Note
Les options de mise à niveau planifiée fonctionnent les unes avec les autres. Vous pouvez planifier une mise à niveau afin qu'elle s'exécute, par exemple, toutes les deux semaines à partir de dimanche de 1 h à 3 h AM.

8. Cliquez sur **Enregistrer** pour créer la tâche de mise à niveau du client.Une message de confirmation s'affichera. Vous pouvez consulter l'état de la mise à niveau dans les détails des ordinateurs correspondants.

6.6. Afficher et gérer des tâches

Les tâches que vous avez créées peuvent être affichées et administrées sur la page **Ordinateurs > Afficher les tâches**.Vous pouvez voir les tâches existantes et des détails les concernant :

- Nom de la tâche.
- Progression de l'exécution sur les ordinateurs cibles.
- Quand la tâche a été créée.

6.6.1. Vérification de l'état et des résultats de l'exécution

Les tâches commenceront à s'exécuter immédiatement sur les ordinateurs en ligne, mais elles peuvent nécessiter un certain temps pour se terminer (plus ou moins, en fonction de la tâche).

Pour vérifier qu'une tâche s'est exécutée sur les ordinateurs cibles :

1. Allez sur la page **Ordinateurs > Afficher les tâches**.
2. Localisez la tâche dans la liste et sélectionnez le champ **Progression**.Vous pouvez voir sur combien d'ordinateurs cibles la tâche s'est exécutée.
3. Pour accéder au rapport de la tâche, qui fournit des informations sur l'exécution de la tâche, cliquez sur le nom de la tâche.

Le rapport de la tâche est constitué d'une page Résumé et d'une page Détails.

6.6.2. Supprimer des tâches

Une fois qu'une tâche s'est exécutée et que vous n'avez plus besoin du rapport de cette tâche, il vaut mieux le supprimer.

Pour supprimer une ou plusieurs tâches :

1. Allez sur la page **Ordinateurs > Afficher les tâches**.
2. Cochez les cases correspondant aux tâches que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer** situé au-dessus du tableau.Une fenêtre de confirmation s'affichera.

7. Politiques de sécurité

Une fois installée, la protection Cloud Security for Endpoints peut être configurée et gérée à partir de Cloud Security Console à l'aide des politiques de sécurité.Une politique précise les paramètres de sécurité à appliquer aux ordinateurs cibles.

Juste après l'installation, les ordinateurs se voient attribuer la politique par défaut, qui est préconfigurée avec les paramètres de protection recommandés. Vous pouvez modifier les paramètres de sécurité selon les besoins et paramétrer également des fonctions de protection supplémentaires.

Si vous gérez un grand nombre d'ordinateurs (des dizaines ou plus), vous pouvez souhaiter créer plusieurs politiques pour appliquer différents paramètres en fonction des besoins en sécurité.Vous pouvez, par exemple, configurer différentes politiques pour les postes de travail de bureau, les portables et les serveurs.

Voici ce que vous avez besoin de savoir au sujet des politiques :

- Il y a un seul modèle de politique par défaut, qui permet de configurer tous les paramètres de protection.Quand vous créez une nouvelle politique, vous devez choisir un modèle de politique que vous souhaitez utiliser.Vous pouvez choisir un modèle de politique par défaut ou une politique existante.
- Les politiques sont envoyées aux ordinateurs cibles immédiatement après leur création ou leur modification.Les paramètres devraient être appliqués aux ordinateurs en moins d'une minute (à condition qu'ils soient en ligne).Si un ordinateur n'est pas en ligne, les paramètres seront appliqués dès qu'il sera de nouveau en ligne.
- La politique s'applique uniquement aux modules de protection installés.Veuillez noter que seule la protection antimalware est disponible pour les systèmes d'exploitation serveurs.
- Les politiques peuvent être affectées à des ordinateurs individuels ou à des groupes d'ordinateurs.La cible de la politique ne peut pas être composée d'ordinateurs et de groupes.
- Plusieurs politiques peuvent être affectées à un moment donné à un ordinateur ou à un groupe. Cependant, il y aura toujours une seule politique active : la dernière à voir été créée ou modifiée.

Pour afficher et gérer les paramètres et les politiques de sécurité, allez sur la page **Politiques > Afficher les politiques**.Les politiques existantes s'affichent dans le tableau.Pour chaque politique, vous pouvez voir :

- Nom de la politique.
- La cible de la politique (les ordinateurs ou les groupes auxquels s'applique la politique).

- Combien d'ordinateurs cibles respectent la politique.
- Utilisateur qui a créé la politique.
- Heure à laquelle la politique a été modifiée pour la dernière fois.

7.1. Création de nouvelles politiques

Pour créer une nouvelle politique :

1. Allez sur la page **Politiques > Nouvelle politique**.
2. Indiquez un nom explicite pour la politique. Lorsque vous choisissez un nom, prenez en compte l'objectif et la cible de la politique.
3. Choisissez un modèle de politique à partir du menu.La nouvelle politique sera initialisée avec les paramètres de la politique du modèle.Vous pouvez choisir un modèle de politique par défaut ou une politique existante.
4. Configurer la cible de la politique (ordinateurs auxquels la politique s'appliquera).Vous pouvez choisir une des options suivantes :
   - **Groupes.** Sélectionnez cette option pour appliquer la politique aux groupes d'ordinateurs administrés.Cliquez sur le lien correspondant et sélectionnez les groupes d'ordinateurs souhaités.

     Note
     La politique s'appliquera automatiquement à tout ordinateur ajouté par la suite au groupe sélectionné.

   - **Ordinateurs.** Sélectionnez cette option pour appliquer la politique aux ordinateurs individuels.Cliquez sur le lien correspondant et sélectionnez les ordinateurs souhaités.
5. Cliquez sur **Soumettre** pour créer la politique et aller sur la page de la politique.
6. Configurez ensuite les paramètres de la politique.Pour plus d'informations, reportez-vous à « Configuration des paramètres de la politique » (p. 47).
7. Cliquez sur **Enregistrer** pour enregistrer les modifications et appliquer les paramètres de protection aux ordinateurs cibles.La nouvelle politique s'affichera sur la page **Afficher les politiques**.

7.2. Configuration des paramètres de la politique

Les paramètres de la politique peuvent être configurés au départ lors de la création de la politique. Vous pouvez ensuite les modifier selon vos besoins à tout moment.

Pour modifier les paramètres d'une politique :

1. Allez sur la page **Politiques > Afficher les politiques**.

2. Cliquez sur le nom de la politique.Cela ouvrira la page de la politique.
3. Configurez les paramètres de la politique selon vos besoins. Les paramètres sont organisés autour des modules de protection dans les catégories suivantes :
   - Résumé
   - Général
   - Antimalware
   - Pare-feu
   - Contrôle de contenu

   Vous pouvez sélectionnez la catégorie des paramètres à l'aide du menu dans la partie gauche de la page.
4. Cliquez sur **Enregistrer** pour enregistrer les modifications et les appliquer aux ordinateurs cibles.Pour quitter la page de la politique sans enregistrer les modifications, cliquez sur **Annuler**.

7.2.1. Résumé

La page Résumé contient des informations générales sur la politique :

- **Nom de la politique.** Vous pouvez renommer la politique en entrant le nouveau nom dans ce champ.
- **Cible spécifiée.** Si vous souhaitez modifier la cible de la politique, cliquez sur le lien et sélectionnez la nouvelle cible.
- **Conformes.** Ce champ indique le nombre d'ordinateurs cibles respectant la politique.

7.2.2. Général

Les paramètres généraux vous aident à gérer les options d'affichage de l'interface utilisateur, les préférences de mise à jour, la protection par mot de passe et d'autres paramètres de Endpoint Security.

Les paramètres sont organisés sous les onglets suivants :

- Affichage
- Avancé
- Mise à jour

Onglet Affichage

Vous pouvez configurer dans cette section les options d'affichage de l'interface utilisateur.

- **Mode Silencieux.** Utilisez ce bouton pour activer ou désactiver le Mode Silencieux.Le Mode Silencieux est conçu pour vous aider à désactiver facilement l'interaction utilisateur dans Endpoint Security.Lorsque le Mode Silencieux est activé, les modifications suivantes sont apportées à la configuration de la politique :

- Les options **Afficher l'icône dans la zone de notification**, **Afficher les fenêtres pop-up de notification** et **Afficher les fenêtres pop-up d'alertes** seront désactivées dans cette section.
- Le niveau de protection du pare-feu est réglé sur **Ensemble des règles, fichiers connus et autoriser**.

- **Afficher l'icône dans la zone de notification.** Sélectionnez cette option pour afficher l'icône de Bitdefender dans la zone de notification.L'icône informe les utilisateurs de l'état de leur protection et leur permet d'ouvrir la fenêtre principale du programme ou de lancer rapidement une analyse ou une mise à jour.
- **Afficher des fenêtres pop-up de notification.** Sélectionnez cette option si vous souhaitez que les utilisateurs soient informés d'importants événements de sécurité par de petites fenêtres pop-up de notification (par exemple, une fenêtre pop-up informe les utilisateurs lorsqu'un virus a été détecté et bloqué sur leur ordinateur).
- **Afficher des fenêtres pop-up d'alerte.** À la différence des fenêtres pop-up de notification, les fenêtres pop-up d'alertes demandent aux utilisateurs de spécifier une action.Les pop-ups sont générés dans les situations suivantes :
  - Si le pare-feu est configuré pour demander à l'utilisateur quelle action effectuer lorsque des applications inconnues demandent l'accès au réseau ou Internet.Vous pouvez configurer ce paramètre dans la section **Pare-feu > Avancé**
  - Si l'analyse des périphériques est activée elle se lancera à chaque fois qu'un périphérique est connecté au PC.Vous pouvez configurer ce paramètre dans la section **Antimalware > A la demande**
- **Alertes d'état.** Les utilisateurs sont informés de l'état de leur protection de deux façons :
  - La zone d'état de sécurité de la fenêtre principale affiche un message d'état approprié et change de couleur en fonction des problèmes détectés.
  - L'icône de Bitdefender de la zone de notification change d'apparence lorsque des problèmes sont détectés.

  L'état de la protection est déterminé en fonction des alertes d'état sélectionnées et se réfère aux problèmes de configuration de sécurité ou à d'autres risques de sécurité. Par exemple, si l'option **État de l'antimalware** est sélectionnée, les utilisateurs sont informés lorsqu'un problème lié à leur protection antimalware se produit (par exemple, si une analyse à l'accès est désactivée ou si une analyse système est en retard).

  Sélectionnez les aspects de sécurité que vous souhaitez surveiller.Si vous ne souhaitez pas que les utilisateurs soient informés des problèmes existants, décochez toutes les cases.
- **Informations de support technique.** Complétez les champs pour personnaliser les informations de support technique et de contact disponibles dans Endpoint Security.Les utilisateurs peuvent accéder à ces informations à partir de la fenêtre Endpoint Security

en cliquant sur l'icône dans l'angle inférieur droit (ou en faisant un clic droit sur l'icône Endpoint Security de la zone de notification et en sélectionnant **À propos de**).

Onglet Avancé

Cette section vous permet de configurer les paramètres généraux et le mot de passe de désinstallation.

- **Supprimer les événements de plus de {30} jours.** Endpoint Security tient un journal détaillé des événements concernant son activité sur l'ordinateur (comprenant également les activités surveillées par le Contrôle de contenu).Par défaut, les événements sont supprimés du journal après 30 jours.Si vous souhaitez modifier cet intervalle, choisissez une option différente dans le menu.
- **Envoyer les rapports de plantage à Bitdefender.** Sélectionnez cette option afin que les rapports soient envoyés aux Laboratoires Bitdefender afin d'y être analysés en cas de plantage de Endpoint Security. Les rapports aideront nos ingénieurs à découvrir la cause du problème et à éviter qu'il ne se reproduise. Aucune donnée personnelle ne sera envoyée.
- **Configuration du mot de passe.** Pour empêcher que les utilisateurs avec des droits d'administration ne désinstallent la protection, vous devez définir un mot de passe.

  Le mot de passe de désinstallation peut être configuré avant l'installation en personnalisant le package d'installation. Si vous avez procédé ainsi, sélectionnez **Conserver les paramètres actuels** pour conserver le mot de passe actuel.

  Pour définir le mot de passe, ou pour modifier le mot de passe actuel, sélectionnez **Activer le mot de passe** et saisissez le mot de passe souhaité.Pour supprimer la protection par mot de passe, sélectionnez **Désactiver le mot de passe**.

Onglet Mise à jour

Cette rubrique vous permet de configurer les paramètres de mise à jour de Endpoint Security.Les mises à jour sont très importantes car elles permettent de contrer les nouvelles menaces.

- **Fréquence des mises à jour (en heures).** Endpoint Security recherche, télécharge et installe automatiquement des mises à jour toutes les heures (configuration par défaut).Les mises à jour automatiques s'effectuent en silence, en tâche de fond.

  Pour modifier l'intervalle de mise à jour automatique, choisissez une option différente dans le menu. Veuillez noter que la mise à jour automatique ne peut pas être désactivée.
- **Reporter le redémarrage.** Certaines mises à jour requièrent un redémarrage du système pour s'installer et fonctionner correctement. En sélectionnant cette option, le programme continuera à fonctionner avec les anciens fichiers jusqu'au redémarrage de l'ordinateur,

sans en informer l'utilisateur.Sinon, une notification dans l'interface utilisateur demandera à l'utilisateur de redémarrer le système lorsqu'une mise à jour le nécessitera.

Si vous choisissez de reporter un redémarrage, vous pouvez définir une heure qui vous convient, à laquelle les ordinateurs redémarreront automatiquement si besoin. Cela peut être très utile pour les serveurs. Sélectionnez **Redémarrer après l'installation des mises à jour si besoin** et spécifiez quand redémarrer (tous les jours ou toutes les semaines, un certain jour, ou à une certaine heure de la journée).

- **Activer le proxy.** Sélectionnez cette option si les ordinateurs se connectent à Internet (ou au serveur local de mise à jour) via un serveur proxy. Deux options permettent de définir les paramètres du proxy :
  - **Importer les paramètres proxy à partir du navigateur par défaut.** Endpoint Security peut importer les paramètres proxy des principaux navigateurs, y compris des dernières versions d'Internet Explorer, de Mozilla Firefox et d'Opera.
  - **Utiliser les paramètres proxy personnalisés.** Si vous connaissez les paramètres proxy, sélectionnez cette option puis indiquez-les :
    - **Serveur** - saisissez l'adresse IP du serveur proxy.
    - **Port** - entrez le port utilisé pour se connecter au serveur proxy.
    - **Nom d'utilisateur** - indiquez un nom d'utilisateur reconnu par le serveur proxy.
    - **Mot de passe** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.

  Vous devez également cocher la case **Utiliser un proxy** correspondant à l'emplacement des mises à jour auquel les paramètres s'appliquent (l'adresse du serveur de mise à jour Internet ou local).
- **Emplacements des mises à jour.** Si un serveur de mise à jour local Bitdefender est configuré dans le réseau, vous pouvez configurer Endpoint Security pour qu'il se mette à jour à partir de ce serveur plutôt qu'à partir d'Internet.

  Note
  Pour en savoir plus, reportez-vous à « Utiliser Update Server » (p. 102).

  Pour configurer l'adresse de mise à jour locale :

  1. Indiquez l'adresse du serveur local de mise à jour dans le champ **Ajouter un emplacement**.Utilisez l'une des syntaxes suivantes :
     - `ip_du_serveur_de_mise_à_jour : port`
     - `nom_du_serveur_de_mise_à_jour : port`

     Le port par défaut est 7074.
  2. Si des ordinateurs clients se connectent au serveur local de mise à jour via un serveur proxy, sélectionnez **Utiliser un proxy**.
  3. Cliquez sur le bouton ✚ **Ajouter**.

4. Utilisez les flèches Haut/Bas dans la colonne **Action** pour définir l'adresse de mise à jour locale comme première de la liste.Si le premier emplacement des mises à jour n'est pas disponible, les clients essaieront le deuxième et ainsi de suite.

Pour retirer un emplacement de la liste, cliquez sur le bouton ✖ **Supprimer** correspondant.Bien que vous puissiez supprimer l'emplacement des mises à jour Internet par défaut, cela n'est pas recommandé.

7.2.3. Antimalware

Le module Antimalware protège le système contre tous les types de malwares (virus, chevaux de Troie, spywares, rootkits, adwares, etc.).La protection est divisée en deux catégories :

- Analyse à l'accès : empêche les nouvelles menaces d'infecter le système.
- Analyse à la demande : permet de détecter et de supprimer les logiciels malveillants déjà présents dans le système.

Lorsqu'il détecte un virus ou un autre malware, Endpoint Security tente automatiquement de supprimer le code malveillant du fichier infecté et de reconstruire le fichier d'origine.Cette opération est appelée désinfection.Les fichiers qui ne peuvent pas être désinfectés sont placés en quarantaine afin de contenir l'infection. Quand un virus est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté ni lu.

Les utilisateurs avancés peuvent configurer des exceptions d'analyse s'ils ne souhaitent pas que certains fichiers ou types de fichiers soient analysés.

Les paramètres sont organisés sous les onglets suivants :

- À l'accès
- À la demande
- Exclusions
- Quarantaine

Onglet À l'accès

Cette section vous permet de configurer les deux composants de la protection antimalware en temps réel :

- Analyse à l'accès
- Active Virus Control

Paramètres de l'analyse à l'accès

L'analyse à l'accès empêche que de nouveaux malwares n'entrent dans le système - elle analyse les fichiers à l'accès (lorsqu'ils sont ouverts, déplacés, copiés ou exécutés), les e-mails envoyés et reçus et le trafic web.

Pour configurer l'analyse à l'accès :

1. Utilisez ce bouton pour activer ou désactiver l'analyse à l'accès.Si vous désactivez l'analyse à l'accès, les ordinateurs seront vulnérables aux malwares.
2. Choisissez le niveau de protection qui correspond le mieux à vos besoins en termes de sécurité.Pour une configuration rapide, faites glisser le curseur le long de l'échelle vers un niveau de protection prédéfini.Utilisez la description à droite de l'échelle pour faire votre choix.
3. Les utilisateurs avancés peuvent configurer en détail les paramètres de l'analyse en cliquant sur le bouton **Personnalisé**. Une fenêtre de configuration s'affichera. Les paramètres de l'analyse personnalisée sont organisés sous deux onglets, comme suit :

   Général

   - **Types de fichiers.** Utilisez ces options pour spécifier les types de fichiers que vous souhaitez analyser. Les préférences d'analyse peuvent être configurées pour les fichiers locaux (stockés sur l'ordinateur local) ou les fichiers réseau (stockés sur les partages réseau).Si la protection antimalware est installée sur tous les ordinateurs du réseau, vous pouvez désactiver l'analyse des fichiers du réseau pour permettre un accès plus rapide au réseau.

     Vous pouvez configurer Endpoint Security afin qu'il analyse tous les fichiers à l'accès (quelle que soit l'extension des fichiers), ou uniquement les fichiers d'applications ou certaines extensions de fichiers que vous jugez dangereuses.L'analyse de tous les fichiers auxquels on a accédé offre une protection maximale alors que l'analyse des applications uniquement peut être utilisée pour obtenir de meilleures performances du système.

     Note

     Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.Pour plus d'informations, reportez-vous à « Liste des types de fichier d'Application » (p. 116).

     Si vous souhaitez que seules certaines extensions soient analysées, sélectionnez **Extensions définies par l'utilisateur** dans le menu correspondant et indiquez les extensions (séparées par des points-virgules ";") dans le champ correspondant.

   - **Archives.** Sélectionnez **Analyser à l'intérieur des archives** si vous souhaitez activer l'analyse à l'accès des fichiers archivés.L'analyse à l'intérieur des archives est un processus lent et consommant beaucoup de ressources, qui n'est donc pas recommandé pour une protection en temps réel. Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité du système.Les malwares peuvent affecter le système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que l'analyse à l'accès ne soit activée.

     Si vous décidez d'utiliser cette option, vous pouvez configurer les options d'optimisation suivantes :

- **Limiter la taille des archives à {10} Mo.** Vous pouvez définir une limite de taille pour les archives à analyser à l'accès.Cochez la case correspondante et tapez la taille maximale des archives (en Mo).
- **Profondeur maximale des archives (niveaux).** Cochez la case correspondante et sélectionnez la profondeur maximale des archives dans le menu.Pour les meilleures performances, choisissez la valeur la plus faible, pour la protection maximale, choisissez la valeur la plus élevée.

Avancé

- **Divers**. Cochez les cases correspondantes pour activer les options d'analyse souhaitées.
  - **Analyser les secteurs d'amorçage.** Pour analyser les secteurs de boot du système.Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus de boot.Quand un virus infecte le secteur de boot, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.
  - **Analyser uniquement les fichiers nouveaux ou modifiés.** En n'analysant que les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
  - **Analyse différée.** Sélectionnez cette option pour faire passer l'analyse des fichiers auxquels les utilisateurs ont accédé pour des opérations de lecture avant celle de ceux auxquels les utilisateurs ont accédé pour des opérations d'écriture. Cela est destiné à optimiser le processus d'analyse.
  - **Rechercher les keyloggers.** Les keyloggers enregistrent ce que vous tapez sur votre clavier et envoient des rapports sur Internet à une personne malveillante (un hacker).Le pirate peut récupérer des informations sensibles à partir des données volées, comme vos numéros de comptes bancaires ou vos mots de passe pour les utiliser à son propre profit.
- **Action d'analyse**. En fonction du type de fichier détecté, les actions suivantes sont menées automatiquement :
  - **Action à appliquer lorsqu'un fichier infecté est trouvé.** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender.Endpoint Security peut généralement supprimer le code malveillant d'un fichier infecté et reconstruire le fichier d'origine. Cette opération est appelée désinfection.

    Si un fichier infecté est détecté, Endpoint Security tente automatiquement de le désinfecter.Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l’infection.

Important
Pour certains types de malware, la désinfection n'est pas possible car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

– **Action à appliquer lorsqu'un fichier suspect est trouvé.** Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique.B-HAVE étant une technologie d'analyse heuristique, Endpoint Security ne peut pas être certain que le fichier est réellement infecté par des malwares. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.

  Lorsqu'un fichier suspect est détecté, les utilisateurs ne peuvent pas y accéder afin d'éviter une infection potentielle.

Bien que ce ne soit pas recommandé, vous pouvez modifier les actions par défaut.Vous pouvez définir deux actions pour chaque type de fichier.Les actions suivantes sont disponibles :

Désinfecter
Supprimer le code malveillant des fichiers infectés.Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés.

Quarantaine
Déplacer les fichiers détectés de l'emplacement actuel vers le dossier de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.Vous pouvez gérer les fichiers en quarantaine à partir de la page Quarantaine de la console.

Supprimer
Supprime les fichiers détectés du disque, sans avertissement.Nous vous recommandons d'éviter d'utiliser cette action.

Refuser l'accès
Refuser l'accès aux fichiers détectés.

Configuration d'Active Virus Control

Bitdefender Active Virus Control est une technologie de détection proactive innovante qui utilise des méthodes heuristiques de pointe pour détecter de nouvelles menaces potentielles en temps réel.

Active Virus Control surveille en permanence les applications en cours d'exécution sur l'ordinateur, à la recherche d'actions ressemblant à celles des malwares. Chacune de ces actions est notée et un score global est calculé pour chaque processus. Lorsque la note globale d'un processus atteint un seuil donné, le processus est considéré comme malveillant. Active Virus Control bloquera automatiquement le processus détecté.

Note
Pour plus d'informations, rendez-vous sur notre site web et consultez le livre blanc sur la technologie Active Virus Control.

Pour configurer Active Virus Control :

1. Utilisez ce bouton pour activer ou désactiver Active Virus Control.Si vous désactivez Active Virus Control, les ordinateurs seront vulnérables aux malwares inconnus.
2. Choisissez le niveau de protection qui correspond le mieux à vos besoins en termes de sécurité.Déplacez le curseur sur l'échelle pour choisir le niveau de protection souhaité.Utilisez la description à droite de l'échelle pour faire votre choix.

   Note
   Si vous élevez le niveau de protection, Active Virus Control aura besoin de moins de signes de comportements similaires à ceux des malwares pour signaler un processus. Cela conduira au signalement d'un nombre plus important d'applications et, en même temps, à un risque plus élevé de faux positifs (des applications saines détectées comme étant malveillantes).

3. Nous vous recommandons de créer des règles d'exclusion pour les applications fréquemment utilisées ou connues afin d'éviter les faux positifs (applications légitimes détectées à tort comme étant malveillantes).Allez dans l'onglet Exclusions et configurez les **règles d'exclusion des processus AVC/IDS** pour les applications de confiance.

Onglet à la demande

Cette section vous permet de configurer les tâches d'analyse antimalware qui s'exécuteront régulièrement sur les ordinateurs cibles, en fonction de la planification que vous spécifiez.

L'analyse s'effectue discrètement, en tâche de fond.L'utilisateur n'est averti du processus d'analyse en cours que par l'apparition d'une icône dans la barre des tâches.

Bien que ce ne soit pas obligatoire, nous vous recommandons de planifier l'exécution hebdomadaire d'une analyse complète sur tous les ordinateurs.Analyser les ordinateurs régulièrement est une mesure de sécurité proactive qui peut aider à détecter et bloquer les malwares susceptibles d'échapper aux fonctionnalités de protection en temps réel.

Outre les analyses régulières, vous pouvez également configurer la détection et l'analyse automatiques des supports de stockage externes.

Gestion des tâches d'analyse

Le tableau Tâches d'analyse vous informe des tâches d'analyse existantes et fournit d'importantes informations sur chacun d'entre elles :

- Nom et type de tâche.
- Heure à laquelle la tâche a été lancée en premier.

- Planification à partir de laquelle la tâche s'exécute régulièrement (périodicité).
- Actions que vous pouvez appliquer à la tâche d'analyse.

Il y a deux tâches d'analyse système par défaut que vous pouvez configurer si besoin :

- **Quick Scan** utilise l'analyse in-the-cloud pour détecter les malwares présents sur le système.La réalisation d'une analyse rapide dure généralement moins d'une minute et n'utilise qu'une petite partie des ressources du système dont a besoin une analyse antivirus classique.
- L'**Analyse Complète du Système** analyse l'ensemble de votre ordinateur en vue de détecter tous les types de malwares menaçant sa sécurité : virus, spywares, adwares, rootkits et autres.

Les options d'analyse des tâches d'analyse par défaut sont préconfigurées et vous ne pouvez pas les modifier.

En plus des tâches d'analyse par défaut (que vous ne pouvez pas supprimer ou dupliquer), vous pouvez créer autant de tâches d'analyse personnalisées que vous le souhaitez. Une tâche d'analyse personnalisée vous permet de sélectionner les emplacements à analyser et de configurer les options d'analyse.

Pour créer et configurer une nouvelle tâche, cliquez sur **Ajouter une tâche** et sélectionnez le type de tâche que vous souhaitez créer.Pour modifier les paramètres d'une tâche existante, cliquez sur le nom de cette tâche.Reportez-vous à la rubrique suivante pour savoir comment configurer les paramètres de la tâche.

Pour supprimer une tâche de la liste, cliquez sur le bouton ✖ **Supprimer** correspondant.

Configuration des tâches d'analyse

Les paramètres de la tâche d'analyse sont organisés sous trois onglets : Général - pour définir le nom de la tâche, la planification de l'exécution et la cible de l'analyse ; Options - pour sélectionner un profil d'analyse pour une configuration rapide des paramètres de l'analyse ; Avancé - pour configurer les paramètres de l'analyse en détail.L'onglet Avancé est accessible uniquement après avoir coché la case **Personnalisé** de l'onglet Options.

Les options sont décrites ci-après du premier au dernier onglet :

- **Détails de la tâche.** Choisissez un nom de tâche explicite pour permettre d'identifier facilement de quoi il s'agit.Lorsque vous choisissez un nom, prenez en compte la cible de la tâche d'analyse, et, éventuellement, les paramètres de l'analyse.
- **Planificateur.** Utilisez les options de planification pour configurer la planification de l'analyse.Vous pouvez configurer l'analyse pour une exécution régulière, à partir d'une date et d'une heure spécifiées.

  Gardez à l'esprit que les ordinateurs doivent être allumés au moment de la planification.Les analyses planifiées ne s'exécuteront pas si l'ordinateur est éteint, en

veille prolongée ou en veille ou si aucun utilisateur n'est connecté. Dans ces situations, l'analyse sera reportée à la prochaine fois.

- **Cible.** Ajouter la liste de tous les emplacements que vous souhaitez analyser sur les ordinateurs cibles.

  Pour ajouter un nouveau fichier ou dossier à analyser :

  1. Choisissez dans le menu un emplacement prédéfini ou l'option **Chemins spécifiques**.
  2. Indiquez le chemin de l'objet à analyser dans le champ de saisie.
     - Si vous avez choisi un emplacement prédéfini, complétez le chemin selon vos besoins.Par exemple, pour analyser l'ensemble du dossier `Program Files`, il suffit de sélectionner l'emplacement prédéfini correspondant dans le menu.Pour analyser un dossier spécifique de `Program Files`, vous devez compléter le chemin en ajoutant une barre oblique inverse (\) et le nom du dossier.
     - Si vous avez choisi **Chemins spécifiques**, indiquez le chemin complet vers l'objet à analyser. Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin est valide sur tous les ordinateurs cibles.
  3. Cliquez sur le bouton ✚ **Ajouter**.

  Pour modifier un emplacement existant, cliquez dessus. Pour retirer un emplacement de la liste, cliquez sur le bouton ✖ **Supprimer** correspondant.

- **Options d'analyse.** Pour une configuration rapide des options d'analyse, utilisez un des profils d'analyse pré-définis.Déplacez le curseur vers le niveau qui correspond le mieux à vos besoins en termes de niveau de protection.Utilisez la description à droite de l'échelle pour faire votre choix.

  Basées sur le profil sélectionné, les options d'analyse de l'onglet **Avancé** sont configurées automatiquement. Vous pouvez cependant, si vous le souhaitez, les configurer en détail. Pour cela, cochez la case **Personnalisé** puis allez dans l'onglet **Avancé**.

- **Opérations d'analyse.**
  - **Exécuter la tâche en priorité basse.** Diminue la priorité du processus d'analyse. Vous allez permettre aux autres logiciels de s'exécuter à une vitesse supérieure en augmentant le temps nécessaire pour que l'analyse soit finie.
  - **Éteindre l'ordinateur lorsque la tâche est terminée.** Cette option peut être utile si vous effectuez des analyses à des heures creuses.

- **Types de fichiers.** Utilisez ces options pour spécifier les types de fichiers que vous souhaitez analyser. Vous pouvez configurer Endpoint Security afin qu'il analyse tous les fichiers (quelle que soit l'extension des fichiers), ou uniquement les fichiers d'applications ou certaines extensions de fichiers que vous considérez dangereuses.L'analyse de tous les fichiers consultés offre une protection maximale alors que l'analyse des applications uniquement peut être utilisée pour que l'analyse soit plus rapide.

Note

Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.Pour plus d'informations, reportez-vous à « Liste des types de fichier d'Application » (p. 116).

Si vous souhaitez que seules certaines extensions soient analysées, sélectionnez **Extensions définies par l'utilisateur** dans le menu correspondant et indiquez les extensions (séparées par des points-virgules ";") dans le champ correspondant.

- **Archives.** Les archives contenant des fichiers infectés ne constituent pas une menace immédiate pour la sécurité du système.Les malwares peuvent affecter le système uniquement si le fichier infecté est extrait de l'archive et exécuté sans que la protection en temps réel ne soit activée. Il est toutefois recommandé d'utiliser cette option afin de détecter et de supprimer toute menace potentielle, même si celle-ci n'est pas imminente.

  Note

  L'analyse des fichiers compressés augmente le temps d'analyse global et demande plus de ressources système.

  – **Analyser dans les archives.** Sélectionnez cette option si vous souhaitez que les archives fassent l'objet d'une analyse antimalware.Si vous décidez d'utiliser cette option, vous pouvez configurer les options d'optimisation suivantes :

    - **Limiter la taille des archives à {10} Mo.** Vous pouvez définir une limite de taille pour les archives à analyser.Cochez la case correspondante et tapez la taille maximale des archives (en Mo).
    - **Profondeur maximale des archives (niveaux).** Cochez la case correspondante et sélectionnez la profondeur maximale des archives dans le menu.Pour les meilleures performances, choisissez la valeur la plus faible, pour la protection maximale, choisissez la valeur la plus élevée.

  – **Analyser les archives de messagerie.** Sélectionnez cette option si vous souhaitez que les archives de messagerie fassent l'objet d'une analyse antimalware.

- **Divers.** Cochez les cases correspondantes pour activer les options d'analyse souhaitées.

  – **Analyser les secteurs d'amorçage.** Pour analyser les secteurs de boot du système.Ce secteur du disque dur contient le code informatique nécessaire pour faire démarrer le processus de boot.Quand un virus infecte le secteur de boot, le disque peut devenir inaccessible et il est possible que vous ne puissiez pas démarrer votre système ni accéder à vos données.

  – **Analyser la mémoire.** Sélectionnez cette option pour analyser les programmes s'exécutant dans la mémoire du système.

  – **Analyser la base de registre.** Sélectionnez cette option pour analyser les clés de registre. Le Registre Windows est une base de données qui contient les paramètres

et les options de configuration des composants du système d'exploitation Windows, ainsi que des applications installées.

- **Analyser les cookies.** Sélectionnez cette option pour analyser les cookies stockés par les navigateurs sur l'ordinateur.
- **Analyser les rootkits.** Sélectionnez cette option pour rechercher des rootkits et des objets masqués à l'aide de ce logiciel.
- **Analyser uniquement les fichiers nouveaux et modifiés.** En n'analysant que les nouveaux fichiers et ceux ayant été modifiés, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
- **Ignorer les keyloggers commerciaux.** Sélectionnez cette option si un logiciel keylogger commercial est installé sur les ordinateurs cibles. Les keyloggers commerciaux sont des logiciels de surveillance légitimes dont la fonction principale consiste à enregistrer tout ce qui est tapé au clavier.

- **Actions.** En fonction du type de fichier détecté, les actions suivantes sont menées automatiquement :
  - **Action à appliquer lorsqu'un fichier infecté est trouvé.** Les fichiers détectés comme étant infectés correspondent à une signature de code malveillant de la Base de Données de Signatures de Codes Malveillants Bitdefender.Endpoint Security peut généralement supprimer le code malveillant d'un fichier infecté et reconstruire le fichier d'origine. Cette opération est appelée désinfection.

    Si un fichier infecté est détecté, Endpoint Security tente automatiquement de le désinfecter.Si la désinfection échoue, le fichier est placé en quarantaine afin de contenir l'infection.

    Important
    Pour certains types de malware, la désinfection n'est pas possible car le fichier détecté est entièrement malveillant. Dans ce cas, le fichier infecté est supprimé du disque.

  - **Action à appliquer lorsqu'un fichier suspect est détecté.** Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique.B-HAVE étant une technologie d'analyse heuristique, Endpoint Security ne peut pas être certain que le fichier est réellement infecté par des malwares. Les fichiers suspects ne peuvent pas être désinfectés, car aucune routine de désinfection n'est disponible.

    Les tâches d'analyse sont configurées par défaut pour ignorer les fichiers suspects. Vous pouvez souhaiter modifier l'action par défaut afin de placer des fichiers suspects en quarantaine.Les fichiers en quarantaine sont envoyés régulièrement aux Laboratoires Bitdefender pour y être analysés. Si la présence de malwares est confirmée, une signature est publiée afin de permettre de supprimer des malwares.

– **Action à appliquer lorsqu'un fichier rootkit est détecté.** Les rootkits sont des logiciels spécialisés utilisés pour masquer des fichiers au système d'exploitation.Bien que n'étant pas malveillants par nature, les rootkits sont souvent utilisés pour masquer des malwares ou la présence d'un intrus dans le système.

  Les rootkits détectés et les fichiers cachés sont ignorés par défaut.

Bien que ce ne soit pas recommandé, vous pouvez modifier les actions par défaut.Vous pouvez spécifier une deuxième mesure à prendre (action) si la première a échoué, et différentes mesures pour chaque catégorie.Choisissez dans les menus correspondants la première et la seconde mesures (actions) à prendre pour chaque type de fichier détecté.Les actions suivantes sont disponibles :

Désinfecter
Supprimer le code malveillant des fichiers infectés.Nous vous recommandons de toujours la conserver comme première action à appliquer aux fichiers infectés.

Quarantaine
Déplacer les fichiers détectés de l'emplacement actuel vers le dossier de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.Vous pouvez gérer les fichiers en quarantaine à partir de la page Quarantaine de la console.

Supprimer
Supprime les fichiers détectés du disque, sans avertissement.Nous vous recommandons d'éviter d'utiliser cette action.

Ignorer
Aucune action ne sera appliquée aux fichiers détectés. Ces fichiers apparaîtront uniquement dans le journal d'analyse.

Analyse des périphériques

Vous pouvez configurer Endpoint Security pour détecter et analyser automatiquement les périphériques de stockage externe quand ils sont connectés à l'ordinateur.Les périphériques détectés appartiennent à l'une des catégories suivantes :

- CD/DVD
- Des mémoires USB, tels que des clés flash et des disques durs externes
- Lecteurs réseau mappés

Les analyses des périphériques tentent de désinfecter automatiquement les fichiers détectés comme infectés ou tentent de les déplacer vers la quarantaine si la désinfection est impossible.Merci de prendre en compte qu'aucune action ne peut être prise sur les fichiers infectés détectés sur les CD / DVD ou sur les lecteurs réseau mappés qui sont limités à un accès Lecture.

Note
Lors d'une analyse des périphériques, l'utilisateur peut accéder à toutes les données de l'appareil.

Si les fenêtres pop-up d'alertes sont activées dans la section **Général > Affichage**, l'utilisateur devra décider d'analyser ou non le périphérique détecté au lieu de commencer l'analyse automatiquement.

Quand une analyse de périphérique est commencée :

- Un pop-up informe l'utilisateur sur l'analyse des périphériques, à condition que la notification des pop-ups soient activés dans la section **Général > Affichage** .
- Une icône d'analyse apparaît dans la barre des tâches. L'utilisateur peut double-cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Une fois l'analyse terminée, l'utilisateur doit vérifier les menaces détectées, le cas échéant.

Pour paramétrer l'analyse de périphérique, utiliser les options suivantes :

- **Analyser les périphériques détectés.** Sélectionnez cette option pour activer la détection et l'analyse automatiques des dispositifs de stockage. Vous pouvez configurer l'analyse de périphérique individuellement pour chaque type de périphériques à l'aide des options suivantes :
  - **Analyser automatiquement les supports CD/DVD**
  - **Analyser automatiquement les supports de stockage USB**
  - **Analyser automatiquement les disques réseau connectés**
- **Ne pas analyser les périphériques de plus de {0} Mo.** Utilisez cette option pour ne pas analyser automatiquement un périphérique détecté si la taille des données stockées est supérieure à la taille spécifiée. Tapez la taille maximale (en mégaoctets) dans le champ correspondant. Zéro signifie qu'aucune restriction de taille n'est imposée.

  Note
  Cette option s'applique uniquement aux CD/DVD et aux supports de stockage USB.

Onglet Exclusions

Cette section vous permet de configurer des règles d'exclusion d'analyse. Les exclusions peuvent s'appliquer à l'analyse à l'accès ou à la demande, ou aux deux. En fonction de l'objet de l'exclusion, il y a quatre types d'exclusions :

- **Exclusions de fichiers :** le fichier spécifié est exclu de l'analyse.
- **Exclusions du dossier :** tous les fichiers à l'intérieur du dossier spécifié et tous ses sous-dossiers sont exclus de l'analyse.

- **Exclusions d'extensions** - tous les fichiers ayant l'extension spécifiée sont exclus de l'analyse.
- **Exclusions de processus :** tout objet auquel accède le processus exclu est également exclu de l'analyse.Vous pouvez également configurer des exclusions de processus pour les technologies Active Virus Control et Système de détection d'intrusion.

Important

Les exceptions d'analyse sont à utiliser dans des circonstances spécifiques ou selon les recommandations de Microsoft ou de Bitdefender.Pour une liste actualisée des exclusions recommandées par Microsoft, veuillez vous référer à cet article.Si vous avez un fichier test EICAR que vous utilisez régulièrement pour tester la protection antimalware, vous devriez l'exclure de l'analyse à l'accès.

Utilisez ce bouton pour activer ou désactiver les exclusions.

Pour configurer une règle d'exclusion :

1. Sélectionnez le type d'exclusion dans le menu.
2. En fonction du type d'exclusion, spécifiez l'objet à exclure comme suit :
   - **Exclusions d'extensions.** Indiquez l'extension du fichier que vous souhaitez exclure, sans la faire précéder d'un point. Par exemple, saisissez `txt` pour exclure les fichiers texte.Veuillez noter que vous pouvez spécifier une seule extension par règle d'exclusion.

     Note

     Avant de choisir d'exclure des extensions, veillez à vous documenter pour savoir quelles sont celles qui sont les cibles principales des malwares.

   - **Exclusions de fichiers, de dossiers et de processus.** Vous devez spécifier le chemin de l'objet exclu sur les ordinateurs cibles.
     a. Choisissez dans le menu un emplacement prédéfini ou l'option **Chemins spécifiques**.
     b. Si vous avez choisi un emplacement prédéfini, complétez le chemin selon vos besoins.Par exemple, pour exclure l'ensemble du dossier `Program Files`, il suffit de sélectionner l'emplacement prédéfini correspondant dans le menu.Pour exclure un dossier spécifique de `Program Files`, vous devez compléter le chemin en ajoutant une barre oblique inverse (\) et le nom du dossier.Pour les exclusions de processus, vous devez ajouter le nom du fichier exécutable de l'application.
     c. Si vous avez choisi **Chemins spécifiques**, indiquez le chemin complet vers l'objet à exclure. Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin est valide sur tous les ordinateurs cibles.

3. Sélectionnez les types d'analyse auxquels la règle s'appliquera. Certaines exclusions peuvent être pertinentes pour l'analyse à l'accès uniquement, certaines pour les analyses à la demande seulement, tandis que d'autres peuvent être recommandés pour les deux.Des exclusions de processus peuvent être configurées pour l'analyse à l'accès et pour les technologies Active Virus Control et Système de détection d'intrusion

   Note

   Veuillez noter que les exclusions d'analyse à la demande ne s'appliqueront pas à l'analyse contextuelle.L'analyse contextuelle se lance en faisant un clic droit sur un fichier ou un dossier et en sélectionnant **Analyser avec Bitdefender**.

4. Cliquez sur le bouton ✚ **Ajouter**.La nouvelle règle sera ajoutée à la liste.

Pour supprimer une règle de la liste, cliquez sur le bouton ✖ **Supprimer** correspondant.

Onglet Quarantaine

Cette section vous permet de configurer les paramètres de la zone de quarantaine.Vous pouvez configurer Endpoint Security pour qu'il exécute automatiquement les actions suivantes :

- **Supprimer les fichiers de plus de {30} jours.** Par défaut, les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés.Si vous souhaitez modifier cet intervalle, choisissez une option différente dans le menu.
- **Envoyer les fichiers en quarantaine aux Laboratoires Bitdefender toutes les {1} heures.** Maintenez cette option sélectionnée pour envoyer automatiquement les fichiers de la quarantaine aux laboratoires de Bitdefender.Les fichiers exemples seront analysés par les spécialistes des malwares de Bitdefender.Si la présence de malwares est confirmée, une signature est publiée afin de permettre de supprimer des malwares.

  Par défaut, les fichiers en quarantaine sont automatiquement envoyés aux Laboratoires Bitdefender toutes les heures. Si vous souhaitez modifier cet intervalle, choisissez une option différente dans le menu.
- **Analyser de nouveau la quarantaine après la mise à jour des signatures de malwares.** Maintenez cette option sélectionnée pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour des signatures de malwares.Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

7.2.4. Pare-feu

Le pare-feu protège votre ordinateur contre les tentatives de connexions entrantes et sortantes non autorisées.

Les paramètres sont organisés sous les onglets suivants :

- Paramètres

- Profils
- Avancé

Onglet Paramètres

Dans cette section, vous pouvez activer ou désactiver le pare-feu de Bitdefender et configurer les paramètres généraux.

- **Pare-feu.** Utilisez ce bouton pour activer ou désactiver le pare-feu.Si vous désactivez le pare-feu, les ordinateurs seront vulnérables aux attaques via le réseau et l'Internet.
- **Bloquer les analyses de ports.** Les analyses de ports sont fréquemment utilisées par les pirates pour découvrir des ports ouverts sur votre ordinateur.Ils peuvent alors s'introduire dans votre ordinateur, s'ils découvrent un port vulnérable ou moins sécurisé.
- **Autoriser le partage de connexion Internet (ICS).** Sélectionnez cette option pour paramétrer le pare-feu pour qu'il autorise le trafic de partage de connexion Internet.

  Note
  Cette option n'active pas automatiquement le partage de connexion Internet sur le système de l'utilisateur.

- **Surveiller les connexions Wi-Fi.** Endpoint Security peut informer les utilisateurs connectés à un réseau Wifi lorsqu'un nouvel ordinateur rejoint le réseau. Pour afficher ces notifications sur l'écran de l'utilisateur, sélectionnez cette option.
- **Niveau de détail du journal.** Endpoint Security dispose d'un journal d'événements concernant l'utilisation du module Pare-feu (activer/désactiver le pare-feu, bloquer le trafic, modifier les paramètres) ou des événements générés par les activités détectées par ce module (analyse des ports, bloquer les tentatives de connexion ou le trafic selon les règles).Choisissez une option du **Niveau de précision du journal** afin de spécifier la quantité d'informations devant figurer dans le journal.
- **Système de détection d'intrusion .** Le système de détection d'intrusion surveille le système à la recherche d'activités suspectes (par exemple, des tentatives non autorisées de modification de fichiers Bitdefender , des injections de DLL, des tentatives de keylogging etc.)

  Pour configurer le système de détection d'intrusion :

  1. Utilisez ce bouton pour activer ou désactiver le système de détection d'intrusion.
  2. Choisissez le niveau de protection qui correspond le mieux à vos besoins en termes de sécurité.Déplacez le curseur sur l'échelle pour choisir le niveau de protection souhaité.Utilisez la description à droite de l'échelle pour faire votre choix.

  Pour éviter qu'un application légitime soit détectée par le système de détection d'intrusion, merci d'ajouter une **règle d'exclusion du processus AVC/IDS** pour cette application, dans la section **Antimalware > Exclusions**.

Onglet Profils

Cette section vous permet de configurer la façon dont les profils de pare-feu et l'option Mode Furtif sont appliqués aux connexions réseau.

Profils de pare-feu

Un profil de pare-feu est appliqué automatiquement à chaque connexion réseau détectée pour définir les options de base du filtrage du trafic.Il y a quatre profils de pare-feu :

Réseau de confiance
Désactiver le Pare-feu pour l'adaptateur concerné.

Réseau domestique/d'entreprise
Autoriser tout le trafic vers et depuis les ordinateurs du réseau local.

Réseau public
Tout le trafic est filtré.

Réseau non fiable
Bloquer complètement le trafic réseau et Internet via l'adaptateur respectif.

Vous pouvez choisir entre deux façons d'appliquer les profils de pare-feu aux connexions réseau :

- **Appliquer les profils de pare-feu par type de réseau (option par défaut).** Pour chaque connexion réseau, le pare-feu détectera automatiquement le type de réseau à partir de Windows et utilisera le profil pare-feu correspondant. Veuillez noter que le profil **Réseau non fiable** ne sera jamais appliqué avec cette option.

  Si vous souhaitez appliquer un profil de pare-feu par défaut à toutes les nouvelles connexions réseau, sélectionnez l'option correspondante sous le nom du profil.

- **Appliquer le profil de pare-feu par type d'adaptateur.** Choisissez un profil pare-feu spécifique à appliquer à chaque type d'adaptateur réseau (câblé, sans fil et virtuel).

Mode Furtif

Le mode furtif camoufle l'ordinateur face aux logiciels malveillants et pirates du réseau et face à Internet.Configurer, si besoin, le Mode furtif pour chaque type de réseau (ou type d'adaptateur) en sélectionnant une des options suivantes :

- **Activé.** L'ordinateur n'est pas visible depuis le réseau local et Internet.
- **Désactivé.** N'importe qui sur le réseau local ou sur Internet peut détecter l'ordinateur (via la commande ping).
- **Distant.** L'ordinateur ne peut pas être détecté depuis Internet.N'importe qui sur le réseau local peut détecter l'ordinateur via la commande ping.

Onglet Avancé

Cette section vous permet de configurer les règles de trafic des données et d'accès au réseau des applications appliquées par le pare-feu.Veuillez noter que les paramètres disponibles s'appliquent uniquement aux profils pare-feu Domicile/Bureau et Public.

Accès au réseau de l'application

Vous pouvez configurer les paramètres suivants :

- **Niveau de protection.** Le niveau de protection sélectionné définit la logique de prise de décisions du pare-feu utilisée lorsque des applications demandent l'accès à des services réseau et Internet.Voici les options proposées :

  Ensemble de règles et autoriser
  Appliquer les règles de pare-feu existantes et autoriser automatiquement toutes les autres tentatives de connexion.À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

  Ensemble de règles et demander
  Appliquer les règles de pare-feu existantes et demander à l'utilisateur de spécifier l'action à appliquer à toutes les autres tentatives de connexion.Une fenêtre d'alerte contenant des informations détaillées sur la tentative de connexion inconnue apparaît sur l'écran de l'utilisateur.À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

  Ensemble de règles et refuser
  Appliquer les règles de pare-feu existantes et refuser automatiquement toutes les autres tentatives de connexion.À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

  Ensemble de règles, fichiers connus et autoriser
  Appliquer les règles de pare-feu existantes, autoriser automatiquement les tentatives de connexion faites par des applications connues et autoriser automatiquement toutes les autres tentatives de connexion inconnues.À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

  Ensemble de règles, fichiers connus et demander
  Appliquer les règles de pare-feu existantes, autoriser automatiquement les tentatives de connexion faites par des applications connues et demander à l'utilisateur l'action à appliquer à toutes les autres tentatives de connexion inconnues.Une fenêtre d'alerte contenant des informations détaillées sur la tentative de connexion inconnue apparaît sur l'écran de l'utilisateur.À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

  Ensemble de règles, fichiers connus et refuser
  Appliquer les règles de pare-feu existantes, autoriser automatiquement les tentatives de connexion faites par des applications connues et refuser automatiquement toutes

les autres tentatives de connexion inconnues.À chaque nouvelle tentative de connexion, une règle est créée et ajoutée à l'ensemble des règles.

Note
Les fichiers connus constituent un vaste ensemble d'applications sûres, de confiance, établi et actualisé en permanence par Bitdefender.

- **Créer des règles agressives.** Si cette option est sélectionnée, le pare-feu Bitdefender va créer des règles pour chaque processus qui ouvre une application demandant un accès au réseau ou à Internet.
- **Surveiller les modifications des processus.** Sélectionnez cette option si vous souhaitez que toute application essayant de se connecter à Internet soit examinée, de manière à voir si elle a été modifiée depuis l'ajout de la règle contrôlant ses accès Internet.Si l'application a été modifiée, une nouvelle règle sera créée en fonction du niveau de protection existant.

  Note
  De manière générale, ce sont les mises à jours qui modifient les applications.Il existe toutefois un risque qu'elles soient modifiées par des logiciels malveillantes ayant pour objectif d'infecter ordinateur local ainsi que d'autres ordinateurs du réseau.

  Les applications signées sont en principe fiables et présentent un niveau de sécurité plus élevé.Vous pouvez sélectionner **Ignorer les processus signés** pour autoriser automatiquement les applications signées modifiées à se connecter à Internet.

Règles de trafic des données

Le tableau Règles dresse la liste des règles de pare-feu existantes, fournissant des informations importantes sur chacune d'entre elles :

- Nom de la règle ou application à laquelle il se réfère.
- Protocole auquel s'applique la règle.
- Action de la règle (autoriser ou refuser les paquets).
- Actions que vous pouvez appliquer à cette règle.

Note
Voici les règles de pare-feu appliquées expressément par la politique.Des règles supplémentaires peuvent être configurées sur les ordinateurs suite à l'application des paramètres du pare-feu.

Certaines règles de pare-feu par défaut vous aident à autoriser ou refuser facilement les types de trafic les plus courants.Sélectionnez l'option souhaitée dans le menu **Permission**.

DNS sur UDP / TCP
Autoriser ou refuser DNS sur UDP et TCP.Par défaut, ce type de connexion est autorisé.

ICMP / ICMPv6 entrants
Autoriser ou refuser les messages ICMP / ICMPv6.Les messages ICMP sont souvent utilisés par des hackers pour perpétrer des attaques contre les réseaux informatiques. Par défaut, ce type de connexion est refusé.

Connexions Bureau à distance entrantes
Autoriser ou refuser l'accès à d'autres ordinateurs sur des Connexions Bureau à distance.Par défaut, ce type de connexion est autorisé.

Envoi d'e-mails
Autoriser ou refuser l'envoi d'e-mails sur SMTP.Par défaut, ce type de connexion est autorisé.

HTTP navigation web
Autoriser ou refuser la navigation web HTTP.Par défaut, ce type de connexion est autorisé.

Impression dans un autre réseau
Autoriser ou refuser l'accès aux imprimantes dans un autre réseau local.Par défaut, ce type de connexion est refusé.

Trafic Windows Explorer sur HTTP / FTP
Autoriser ou refuser le trafic HTTP et FTP de Windows Explorer. Par défaut, ce type de connexion est refusé.

Outre les règles par défaut, vous pouvez créer des règles de pare-feu supplémentaires pour d'autres applications installées sur des ordinateurs. Cette configuration est cependant réservée aux administrateurs avec de fortes compétences réseaux.

Pour créer et configurer une nouvelle règle, cliquez sur le bouton ✚ **Ajouter**.Reportez-vous à la rubrique suivante pour plus d'informations.

Pour supprimer une règle de la liste, cliquez sur le bouton ✖ **Supprimer** correspondant.

Note
Vous ne pouvez ni supprimer ni modifier les règles par défaut du pare-feu.

Configuration des règles personnalisées

Pour créer et configurer une nouvelle règle, cliquez sur le bouton ✚ **Ajouter**.Pour modifier une règle existante, cliquez sur le nom de la règle.

Les paramètres suivants peuvent être configurés :

- **Nom de la règle.** Indiquez le nom sous lequel la règle apparaîtra dans le tableau des règles (par exemple, le nom de l'application à laquelle la règle s'applique).

- **Chemin de l'application.** Vous devez spécifier le chemin du fichier exécutable de l'application sur les ordinateurs cibles.
  - Choisissez un emplacement prédéfini dans le menu et complétez le chemin selon vos besoins. Par exemple, pour une application installée dans le dossier `Program Files`, sélectionnez `%ProgramFiles%` et complétez le chemin en ajoutant une barre oblique inverse (\) et le nom du dossier de l'application.
  - Indiquez le chemin complet dans le champ de saisie. Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin est valide sur tous les ordinateurs cibles.
- **Ligne de commande.** Si vous souhaitez que la règle soit appliquée uniquement quand l'application spécifiée est ouverte à l'aide d'une commande spécifique dans l'interface de commande en ligne Windows, entrez la commande respective dans le champ de saisie. Sinon laissez-le vide.
- **MD5 de l'application.** Si vous souhaitez que la règle vérifie l'intégrité des données du fichier de l'application en fonction de son code de hachage MD5, indiquez-le dans le champ de saisie. Dans le cas contraire, laissez le champ vide.
- **Adresse locale.** Spécifiez l'adresse IP locale et le port auxquels s'applique la règle.Si vous avez plus d'un adaptateur réseau, vous pouvez décocher la case **Tous** et entrer une adresse IP spécifique.De même, pour filtrer les connexions sur un port ou une plage de ports spécifique, décochez la case **Tous** et indiquez le port ou la plage de ports souhaité dans le champ correspondant.
- **Adresse distante.** Spécifiez l'adresse IP distante et le port auxquels s'applique la règle.Pour filtrer le trafic depuis et vers un ordinateur spécifique, décochez la case **Tous** et entrez son adresse IP.
- **Appliquer la règle uniquement pour les ordinateurs connectés directement.** Vous pouvez filtrer l'accès en fonction de l'adresse Mac.
- **Événements.** En fonction du protocole sélectionné, choisissez les événements réseau auxquels la règle s'applique.Les événements suivants sont susceptibles d'être consignés :

Evénement	Description
Connexion	Échange préliminaire de messages standard, réalisé par les protocoles orientés connexion (tels que TCP) afin d'établir une connexion.Avec les protocoles orientés connexion, le trafic de données entre deux ordinateurs n'intervient qu'une fois qu'une connexion est établie.
Trafic	Flux de données entre deux ordinateurs.
Ecouter	État dans lequel une application surveille le réseau, dans l'attente de l'établissement d'une connexion ou de la réception d'informations provenant d'une application de même niveau.

- **Protocole.** Sélectionnez le protocole IP auquel s'applique la règle.
  - Si vous voulez que la règle s'applique à tous les protocoles, sélectionnez **Toutes**.
  - Si vous souhaitez que la règle s'applique au protocole TCP, sélectionnez **TCP**.
  - Si vous souhaitez que la règle s'applique au protocole UDP, sélectionnez **UDP**.
  - Si vous voulez que la règle s'applique à un protocole spécifique, sélectionnez **Autre**.Un champ de saisie apparaît.Saisissez dans ce champ le numéro attribué au protocole que vous voulez filtrer.

Note

Les numéros des protocoles IP sont attribués par l'IANA (Internet Assigned Numbers Authority, l'organisation de gestion de l'adressage IP sur Internet).Vous pouvez obtenir la liste complète des numéros de protocoles IP attribués à l'adresse http://www.iana.org/assignments/protocol-numbers.

- **Direction.** Sélectionnez la direction du trafic à laquelle s'applique la règle.

Direction	Description
Sortant	La règle s'applique seulement pour le trafic sortant.
Entrant	La règle s'applique seulement pour le trafic entrant.
Tous les deux	La règle s'applique dans les deux directions.

- **Version IP.** Sélectionnez la version du protocole IP (IPv4, IPv6 ou autre) à laquelle s'applique la règle.
- **Type de Réseau.** Sélectionnez le type de réseau auquel s'applique la règle.
- **Définir la permission.** Sélectionnez l'une des permissions disponibles :

Permission	Description
Autoriser	L'application spécifiée se verra autoriser l'accès réseau/Internet dans les circonstances spécifiées.
Refuser	L'application spécifiée se verra refuser l'accès réseau/Internet dans les circonstances spécifiées.

Cliquez sur **Enregistrer** pour ajouter la règle.

7.2.5. Contrôle de contenu

Utilisez le module Contrôle de contenu pour configurer vos préférences concernant le filtrage du contenu et la protection des données pour l'activité des utilisateurs y compris la navigation web, les applications de messagerie et logicielles. Vous pouvez limiter ou autoriser l'accès

à Internet et l'utilisation des applications, configurer l'analyse du trafic, l'antiphishing et les règles de protection des données.

Les paramètres du contrôle de contenu sont organisés sous les onglets suivants :

- Trafic
- Web
- Données
- Applications

Onglet Trafic

Configurez les préférences de sécurité du trafic à l'aide des paramètres sous les sections suivantes :

- Options
- Analyse du trafic
- Exclusions de l'analyse du trafic

Options

- **Analyse SSL**. Sélectionnez cette option si vous souhaitez que le trafic web SSL (Secure Sockets Layer) soit inspecté par les modules de protection Endpoint Security.
- **Afficher la barre d'outils du navigateur**. La barre d'outils de Bitdefender informe les utilisateurs de la note attribuée aux pages web qu'ils consultent. La barre d'outils de Bitdefender n'est pas votre barre d'outils de navigateur typique. La seule chose qu'il ajoute au navigateur est un petit bouton  en haut de chaque page web. Cliquer sur le bouton ouvre la barre d'outils.

  En fonction de la façon dont Bitdefender classifie la page web, l'un des résultats suivants s'affiche dans la partie gauche de la barre d'outils :

  – Le message "Cette page n'est pas sûre" apparaît sur un fond rouge.

  – Le message "Nous vous recommandons d'être vigilant" apparaît sur un fond orange.

  – Le message "Cette page est sûre" apparaît sur un fond vert.
- **Search Advisor.** Search advisor évalue les résultats des recherches Google, Bing et Yahoo!, ainsi que tous les liens Facebook et Twitter en plaçant une icône devant chaque résultat.Icônes utilisées et leur signification :

  Nous vous déconseillons de consulter cette page web.

  Cette page web peut contenir du contenu dangereux. Soyez prudent si vous décidez de le consulter.

  Cette page peut être consultée en toute sécurité.

Analyse du trafic

Les e-mails entrants et le trafic web sont analysés en temps réel pour empêcher le téléchargement de malwares sur l'ordinateur. Les e-mails sortants sont analysés afin d'éviter que des malwares n'infectent d'autres ordinateurs. L'analyse du trafic web peut ralentir un peu la navigation sur Internet, mais elle bloquera les malwares provenant d'Internet, y compris les téléchargements de type "drive-by".

Lorsqu'un e-mail infecté est détecté, il est remplacé automatiquement par un e-mail standard informant le destinataire que l'e-mail original était infecté. Si une page Web contient ou distribue des malwares, elle est automatiquement bloquée. Une page d'avertissement spéciale s'affiche à la place afin d'informer l'utilisateur que la page web requise est dangereuse.

Bien que ce ne soit pas recommandé, vous pouvez désactiver l'analyse du trafic de messagerie et web pour améliorer les performances du système. Il ne s'agit pas d'une menace majeure tant que l'analyse à l'accès des fichiers locaux demeure activée.

Exclusions de l'analyse du trafic

Vous pouvez choisir de ne pas analyser une partie du trafic à la recherche de malwares lorsque les options d'analyse du trafic sont activées.

Pour définir une exception à l'analyse du trafic :

1. Sélectionnez le type d'exclusion dans le menu.
2. En fonction du type d'exception, spécifiez comme suit l'élément du trafic à exclure de l'analyse :
   - **IP**. Saisissez l'adresse IP pour laquelle vous ne souhaitez pas analyser le trafic entrant et sortant.
   - **URL**. Exclut de l'analyse les adresses Internet spécifiées. Pour exclure une URL de l'analyse :
     – Saisissez une URL spécifique telle que `www.exemple.com/exemple.html`
     – Utilisez les caractères génériques pour spécifier des schémas d'adresses Internet :
       - L'astérisque (*) remplace zéro caractère ou plus.
       - Le point d'interrogation (?) remplace exactement un caractère. Vous pouvez utiliser plusieurs points d'interrogation pour définir toute combinaison d'un nombre spécifique de caractères. Par exemple, ??? remplace toute combinaison de 3 caractères précisément.

     Dans le tableau suivant, vous trouverez des exemples de syntaxe pour les adresses Internet spécifiques.

Syntaxe	Application des exceptions
`www.exemple*`	Chaque site web ou page web commençant par `www.exemple` (sans tenir compte de l'extension de domaine). L'exclusion ne s'appliquera pas aux sous-domaines du site web spécifié, comme `sousdomaine.exemple.com`.
`*exemple.com`	Tout site Internet se terminant par `exemple.com`, y compris les pages et sous-domaines de celui-ci.
`*chaîne*`	Tout site Internet ou page web dont l'adresse contient la chaîne spécifiée.
`*.com`	Chaque site Internet ayant l'extension de domaine `.com`, y compris les pages et sous-domaines de celui-ci. Utilisez cette syntaxe pour exclure de l'analyse des domaines entiers de premier niveau.
`www.exemple?.com`	Toutes les adresses web commençant par `www.example?.com`, où le ? peut être remplacé avec n'importe quel caractère unique.Ces sites Web pourraient inclure : `www.exemple1.com` ou `www.exempleA.com`.

- **Application**. Exclut de l'analyse le processus ou l'application spécifié(e). Pour définir une exception à l'analyse des applications :
  - Saisissez le chemin de l'application complet. Par exemple, `C:\Program Files\Internet Explorer\iexplore.exe`
  - Utilisez les variables d'environnement pour spécifier le chemin de l'application. Par exemple : `%programfiles%\Internet Explorer\iexplore.exe`
  - Utilisez des caractères génériques pour spécifier des applications dont le nom correspond à un certain schéma. Par exemple :
    - `c*.exe` pour toutes les applications commençant par un « c »(chrome.exe).
    - `??????.exe` pour toutes les applications ayant un nom à six caractères (chrome.exe, safari.exe, etc.).
    - `[^c]*.exe` pour toutes les applications à l'exception de celles commençant par un « c ».
    - `[^ci]*.exe` pour toutes les applications à l'exception de celles commençant par un « c » ou un « i ».

3. Cliquez sur le bouton ✚ **Ajouter**.

Pour retirer un élément de la liste, cliquez sur le bouton✖ **Supprimer** correspondant.

Onglet Web

Cette section vous permet de configurer vos préférences en matière de sécurité pour la navigation sur Internet.

Les paramètres sont organisés dans les sections suivantes :

- Contrôle de l'accès à Internet
- Filtrage par catégories web
- Antiphishing

Contrôle de l'accès à Internet

Le Contrôle de l'accès à Internet fonctionne conjointement avec le Filtrage par catégories web pour vous permettre de filtrer l'accès à Internet. Le Contrôle de l'accès à Internet vous permet d'autoriser ou de bloquer l'accès à Internet pour des utilisateurs ou des applications aux moments indiqués. Les pages Web bloquées par le Contrôle de l'accès à Internet ne s'affichent pas dans le navigateur. Ce qui s'affiche est une page Web par défaut, qui informe l'utilisateur que la page Web demandée a été bloquée par le Contrôle de l'accès à Internet. Utilisez ce bouton pour activer ou désactiver le **Contrôle de l'accès à Internet**.

Vous avez trois options de configuration :

- Sélectionnez **Autoriser** pour autoriser l'ensemble du trafic Web puis **bloquez** explicitement l'accès à certaines catégories de contenu Web et adresses Web à l'aide du Filtrage par catégories web et du Contrôle de l'accès à Internet respectivement.
- Sélectionnez **Bloquer** pour bloquer l'ensemble du trafic web puis **autorisez** explicitement l'accès à certaines catégories de contenu Internet et adresses Internet à l'aide du Filtrage par catégories web et du Contrôle de l'accès à Internet respectivement.
- Définissez des restrictions horaires pour l'accès à Internet puis **autorisez ou bloquez** explicitement l'accès à certaines catégories de contenus Internet et à certaines adresses Web en utilisant respectivement le Filtrage par catégories web et le Contrôle de l'accès à Internet. Pour limiter l'accès à Internet à certaines heures de la journée sur une base hebdomadaire :
  1. Sélectionnez **Planifier**.
  2. Cliquez sur **Modifier les paramètres**.
  3. Allez dans l'onglet **Planificateur**.
  4. Sélectionnez dans la grille les intervalles pendant lesquels vous souhaitez bloquer l'accès à Internet. Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes. Pour commencer une nouvelle sélection, cliquez sur **Tout effacer**.
  5. Cliquez sur **Enregistrer**.

Note
Endpoint Security effectuera des mises à jour toutes les heures même si l'accès à Internet est bloqué.

Vous pouvez également définir des règles Web pour bloquer ou autoriser expressément certaines adresses Internet, écrasant ainsi les paramètres du Contrôle de l'accès à Internet. Les utilisateurs pourront ainsi accéder à une adresse web spécifique même lorsque la navigation sur Internet est bloquée par le Contrôle de l'accès à Internet.

Pour créer une règle Internet :

1. Cliquez sur **Modifier les paramètres**.
2. Cliquez sur l'onglet **Règles Internet**.
3. Utilisez le bouton **Utiliser des exceptions** pour permettre les exceptions web.
4. Saisissez l'adresse que sous souhaitez autoriser ou bloquer dans le champ **Adresses Web**.
5. Sélectionnez **Autoriser** ou **Bloquer** dans le menu **Permission**.
6. Cliquez sur le bouton ✚ **Ajouter** à droite du tableau pour ajouter l'adresse à la liste d'exceptions.
7. Cliquez sur **Enregistrer**.

Le contrôle de l'accès à Internet peut également être utilisé pour écraser le Filtrage par catégories web dans certaines situations. Vous pouvez créer une règle de Contrôle de l'accès à Internet pour autoriser expressément les utilisateurs à accéder à un site Web qui est bloqué par le Filtrage par catégories web. Les règles de Contrôle de l'accès à Internet avec la mention **Autoriser** pour certaines adresses Web sont également prises en compte lors des intervalles où l'accès à Internet est bloqué par le Contrôle d'accès Web.

Filtrage par catégories web

Le Filtrage par catégories web filtre de façon dynamique l'accès aux sites Web en fonction de leur contenu. En utilisant le Filtrage par catégories web, vous pouvez autoriser ou bloquer l'accès à des catégories entières de sites Web comme les réseaux sociaux ou les sites de partage de vidéos. Les permissions **Autoriser** fonctionnent uniquement lorsque l'accès àInternet est bloqué par le Contrôle de l'accès à Internet alors que les permissions **Bloquer** fonctionnent uniquement lorsque l'accès à Internet est autorisé par le Contrôle de l'accès à Internet.

Note
Vous pouvez écraser la permission de la catégorie d'adresses Web individuelles en les ajoutant avec la permission opposée dans Contrôle de l'accès à Internet > Modifier les paramètres > Règles Internet. Par exemple, si une adresse Web est bloquée par le Filtrage par catégories web, ajoutez une règle de Contrôle de l'accès à Internet pour cette adresse avec la mention **Autoriser**.

Pour configurer le filtrage par catégories web :

1. Utilisez le bouton pour activer le Filtrage par catégories web.
2. Pour une configuration rapide, cliquez sur l'un des profils prédéfinis (Agressif, Normal, Tolérant). Utilisez la description à droite de l'échelle pour faire votre choix.
3. Si vous n'êtes pas satisfait des paramètres par défaut, vous pouvez définir un filtre personnalisé :
   a. Sélectionnez **Personnalisé**.
   b. Cliquez sur **Modifier les paramètres**.
   c. Recherchez la catégorie qui vous intéresse dans la liste et sélectionnez l'action souhaitée dans le menu.
   d. Cliquez sur **Enregistrer**.

Antiphishing

La protection antiphishing bloque automatiquement les pages web de phishing connues afin d'empêcher les utilisateurs de divulguer par inadvertance des informations privées ou confidentielles à des fraudeurs en ligne. Au lieu de la page web de phishing, une page d'avertissement spéciale s'affiche dans le navigateur afin d'informer l'utilisateur que la page web requise est dangereuse.

Utilisez ce bouton pour activer ou désactiver l'Antiphishing. Vous pouvez affiner le paramétrage de l'antiphishing en configurant les paramètres suivants :

- **Protection contre les escroqueries**. Sélectionnez cette option si vous souhaitez étendre la protection à d'autres types d'arnaques que le phishing. Par exemple, des sites web représentant de fausses entreprises, qui ne requièrent pas directement de données personnelles, mais qui essaient de se faire passer pour des entreprises légitimes et de réaliser des profits en convainquant les gens de faire appel à leurs services.
- **Protection contre le phishing**. Maintenez cette option sélectionnée pour protéger les utilisateurs contre les tentatives de phishing.

Si une page web légitime est détectée à tort comme étant une page de phishing et est bloquée, vous pouvez l'ajouter à la liste blanche afin de permettre aux utilisateurs d'y accéder. La liste ne doit contenir que des sites web de confiance.

Pour gérer les exceptions de l'antiphishing :

1. Cliquez sur **Liste Blanche**.
2. Saisissez l'adresse web et cliquez sur le bouton ➕ **Ajouter**.

   Pour retirer une exception de la liste, cliquez sur le bouton **Supprimer** correspondant.
3. Cliquez sur **Enregistrer**.

Onglet Protection des données

La Protection des données empêche la divulgation non autorisée de données sensibles grâce à des règles définies par l'administrateur.Vous pouvez créer des règles pour protéger toute information personnelle ou confidentielle, telle que :

- Informations personnelles du client
- Noms et informations clés des produits et technologies en cours de développement
- Informations de contact de cadres de l'entreprise

Les informations protégées peuvent contenir des noms, des numéros de téléphone, des informations de cartes et de comptes bancaires, des adresses e-mail etc.

En fonction des règles de protection que vous créez, Endpoint Security analyse le trafic web et de messagerie quittant l'ordinateur à la recherche de chaînes de caractères spécifiques (par exemple, un numéro de carte bancaire). Si une correspondance est trouvée, la page web ou l'e-mail est alors bloqué afin de bloquer l'envoi des données protégées.L'utilisateur est immédiatement informé de l'action prise par Endpoint Security par une page web d'alerte ou un e-mail.

Pour configurer la protection des données :

1. Utilisez ce bouton pour activer la Protection des données.
2. Créez des règles de protection des données pour toutes les données sensibles que vous souhaitez protéger. Pour créer une règle :
   a. Cliquez sur le bouton ✚ **Ajouter une règle**.Une fenêtre de configuration s'affiche.
   b. Indiquez le nom sous lequel la règle figurera dans le tableau des règles.Choisissez un nom explicite afin que la règle soit facilement identifiable par vous ou un autre administrateur.
   c. Saisissez les données que vous souhaitez protéger (par exemple, le numéro de téléphone d'un cadre de l'entreprise ou le nom interne d'un nouveau produit sur lequel l'entreprise travaille).Toute combinaison de mots, chiffres ou chaînes de caractères alphanumériques et spéciaux (tels que @, # or $) est acceptée.

      Veillez à entrer au moins cinq caractères de manière à éviter un blocage par erreur d'e-mails et de pages Web.

      ### Important

      Les données fournies sont stockées de manière chiffrée sur les ordinateurs protégés, mais sont visibles à partir de votre compte Cloud Security Console.Pour plus de sécurité, n'indiquez pas toutes les données que vous souhaitez protéger.Dans ce cas, vous devez décocher l'option **Chercher les mots entiers**.

   d. Configurez les options d'analyse du trafic selon vos besoins.

- **Analyse web (trafic HTTP)** - analyse le trafic Web (HTTP) et bloque les données sortantes correspondant aux données de la règle.
- **Analyse email (trafic SMTP)** - analyse le trafic mail (SMTP) et bloque les emails sortants qui contiennent les éléments déterminés dans la règle de gestion des données.

Vous pouvez choisir d'appliquer la règle uniquement si les données de la règle correspondent à tous les mots ou à la chaîne de caractères détectée.

e. Cliquez sur **Enregistrer**.La nouvelle règle sera ajoutée à la liste.

3. Configurez des exceptions aux règles de protection des données afin que les utilisateurs puissent envoyer des données protégées aux sites web et aux destinataires autorisés.Les exclusions peuvent s'appliquer globalement (à toutes les règles) ou uniquement à certaines règles.Pour ajouter une exclusion, utilisez la dernière ligne du tableau **Exclusions** :

   a. Sélectionnez le type d'exclusion (adresse web ou e-mail).

   b. Indiquez l'adresse web ou e-mail à laquelle les utilisateurs sont autorisés à divulguer des données protégées.

   c. Cliquez sur le bouton ✚ **Ajouter**.La nouvelle règle d'exclusion sera ajoutée à la liste.

Note
Si un e-mail contenant des données bloquées est adressé à plusieurs destinataires, ceux pour lesquels des exclusions ont été définies le recevront.

Pour retirer une règle ou une exclusion de la liste, cliquez sur le bouton ✖ **Supprimer** correspondant.

Onglet Applications

Cette section vous permet de configurer le Contrôle des applications. Le Contrôle des applications vous aide à bloquer complètement ou à limiter l'accès des utilisateurs aux applications sur leurs ordinateurs. Les jeux, logiciels de messagerie, comme d'autres catégories de logiciels (y compris malveillants) peuvent être bloqués de cette façon.

Pour configurer le Contrôle des applications :

1. Utilisez le bouton pour activer le contrôle des applications.
2. Spécifiez les applications auxquelles vous souhaitez limiter l'accès. Pour limiter l'accès à une application :

   a. Cliquez sur le bouton ✚ **Ajouter une règle**. Une fenêtre de configuration s'affiche.

   b. Vous devez spécifier le chemin du fichier exécutable de l'application sur les ordinateurs cibles. Il y a deux façons de procéder :

      - Choisissez un emplacement prédéfini dans le menu et complétez le chemin selon vos besoins dans le champ de saisie. Par exemple, pour une application installée

dans le dossier `Program Files`, sélectionnez `%ProgramFiles` et complétez le chemin en ajoutant une barre oblique inverse (\) et le nom du dossier de l'application.

- Indiquez le chemin complet dans le champ de saisie. Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin est valide sur tous les ordinateurs cibles.

c. Configurer la permission désirée :

- **Bloquer** - pour bloquer complètement l'accès à l'application.
- **Limiter** - pour limiter l'accès à l'application à certaines plages horaires.

  Si vous choisissez de limiter l'accès à l'application et non de la bloquer complètement, vous devez également sélectionner dans la grille les jours de la semaine et les heures pendant lesquels l'accès est bloqué. Vous pouvez cliquer sur des cellules individuelles pour choisir des heures ou cliquer et faire glisser la souris sur plusieurs cellules pour bloquer de plus longues périodes. Pour commencer une nouvelle sélection, cliquez sur **Tout effacer**.
- **Autoriser** - pour autoriser l'accès momentanément, tout en conservant la planification des restrictions.

d. Cliquez sur **Enregistrer**. La nouvelle règle sera ajoutée à la liste.

Pour supprimer une règle de la liste, cliquez sur le bouton ✖ **Supprimer** correspondant. Pour modifier une règle existante, cliquez sur le nom de l'application.

7.3. Surveiller l'exécution de la politique

Pour vérifier qu'une politique a été appliquée aux ordinateurs cibles :

1. Allez sur la page **Politiques > Afficher les politiques**.
2. Vérifier l'état dans la colonne **Conformes**.Vous pouvez voir combien d'ordinateurs cibles sont compatibles.
3. Cliquez sur le lien pour ouvrir une fenêtre avec plus d'informations. Tous les ordinateurs auxquels la politique à été affectée s'affichent dans un tableau.Vous pouvez consulter l'état de la conformité pour chaque ordinateur cible.

Note

S'il y a trop d'entrées, vous pouvez utiliser les zones de recherche ou les menus sous les en-têtes de colonne afin de filtrer les données affichées. Vous pouvez également cliquer sur les en-têtes de colonnes pour trier les données en fonction d'une colonne spécifique.Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau.

7.4. Vérification et modification des affectations de politiques

Les politiques peuvent être affectées à des ordinateurs individuels ou à des groupes d'ordinateurs.

Pour vérifier et modifier les affectations de politiques :

1. Allez sur la page **Politiques > Afficher les politiques**.
2. Cliquez sur le nom de la politique.Cela ouvrira la page de la politique.
3. La liste des ordinateurs et groupes affectés apparaît dans le champ **Cibles spécifiées**.Cliquez sur le lien pour voir plus de détails et modifier les affectations actuelles.Veuillez noter que vous ne pouvez pas modifier le type de cible (ordinateurs ou groupes).
4. Pour modifier les affectations actuelles, procédez comme suit :
   a. En fonction du type de cible, procédez comme suit :
      - Si la politique a été à l'origine affectée à des groupes, sélectionnez les nouveaux groupes auxquels vous souhaitez que la politique s'applique.
      - Si la politique a été à l'origine affectée à des ordinateurs, vous devez sélectionner les nouveaux ordinateurs auxquels vous souhaitez que la politique s'applique.Commencez par décocher la case **Afficher uniquement les ordinateurs sélectionnés** dans l'angle supérieur gauche de la fenêtre.Ensuite, cochez les cases correspondant aux ordinateurs souhaités.

        Note

        S'il y a trop d'entrées, vous pouvez utiliser les zones de recherche ou les menus sous les en-têtes de colonne afin de filtrer les données affichées. Vous pouvez également cliquer sur les en-têtes de colonnes pour trier les données en fonction d'une colonne spécifique.Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau.

   b. Cliquez sur **Modifier** pour enregistrer la nouvelle cible.
   c. Cliquez sur **Enregistrer** pour appliquer les modifications des politiques.

7.5. Renommer des politiques

Les politiques devraient porter des noms explicites afin que vous ou un autre administrateur puissiez les identifier rapidement.

Pour renommer une politique :

1. Allez sur la page **Politiques > Afficher les politiques**.

2. Cliquez sur le nom de la politique.Cela ouvrira la page de la politique.
3. Indiquez un nouveau nom pour la politique.
4. Cliquez sur **Enregistrer** pour appliquer les modifications des politiques.

7.6. Suppression de politiques

Si vous n'avez plus besoin d'une politique, supprimez-la.Une fois la politique supprimée, les ordinateurs auxquels elle s'appliquait se verront attribuer la politique du groupe parent.Si aucune autre politique ne s'applique, la politique par défaut sera finalement appliquée.

Pour supprimer une politique :

1. Allez sur la page **Politiques > Afficher les politiques**.
2. Cochez la case correspondante.
3. Cliquez sur le bouton **Supprimer** dans l'angle supérieur droit de la page. Vous devrez confirmer votre action en cliquant sur **Oui**.

8. Tableau de bord de supervision

À chaque fois que vous vous connectez à la Cloud Security Console, la page **Tableau de bord** s'affiche automatiquement. Le tableau de bord est une page d'état constituée de 7 portlets, qui vous fournit un aperçu rapide de la sécurité de tous les postes de travail protégés (postes de travail, portables, serveurs).

Les portlets du tableau de bord affichent différentes informations de sécurité sous la forme de graphiques faciles à lire, vous permettant d'identifier rapidement tout problème susceptible de requérir votre attention.Chaque portlet du tableau de bord comprend un rapport détaillé en arrière-plan, accessible d'un simple clic sur le graphique.

Certains portlets fournissent des informations sur l'état, alors que d'autres font des rapports sur les événements de sécurité au cours de la dernière période.Vous pouvez consulter et configurer la période de reporting d'un portlet en cliquant sur le bouton  de sa barre de titre.

8.1. Portlets du tableau de bord

Le tableau de bord se compose des portlets suivants :

État du réseau

Vous fournit des informations détaillées sur l'état de sécurité global du réseau.Les ordinateurs sont regroupés en fonction de ces critères :

- Les ordinateurs non administrés ne disposent pas d'une protection Cloud Security for Endpoints installée et leur état de sécurité ne peut pas être évalué.
- Les ordinateurs hors-ligne ont normalement la protection Cloud Security for Endpoints d'installée, mais il n'y a aucune activité récente de Endpoint Security.Le statut de sécurité des ordinateurs en mode hors-ligne ne peut pas être évalué avec précision, car l'information d'état n'est pas à jour.Pour plus d'informations, reportez-vous à « A propos des ordinateurs hors-ligne » (p. 30).
- Les ordinateurs protégés ont la protection Cloud Security for Endpoints installée et aucun risque de sécurité n'a été détecté.
- Les ordinateurs vulnérables ont la protection Cloud Security for Endpoints installée, mais certaines conditions peuvent empêcher la protection de l'ordinateur. Les détails du rapport affichent les aspects de la sécurité ayant besoin d'être corrigés.

État de l'ordinateur

Vous fournit diverses informations d'état concernant les ordinateurs sur lesquels la protection Cloud Security for Endpoints est installée.

- État de la mise à jour de la protection
- État de la protection antimalware
- État de la licence
- État de l'activité du réseau (en ligne/hors ligne)

Vous pouvez appliquer les filtres par aspect et état de la sécurité pour trouver les informations que vous recherchez.

Les 10 ordinateurs les plus infectés
Liste le top 10 des ordinateurs les plus infectés du réseau au cours d'une période donnée.

Les 10 malwares les plus détectés
Liste le top 10 des malwares détectés sur le réseau au cours d'une période donnée.

Activité des logiciels malveillants
Vous fournit des informations globales et par ordinateur sur les malwares détectés dans le réseau pendant une certaine période.Vous pouvez voir :

- Nombre de détections (fichiers ayant été détectés comme infectés par des malwares)
- Nombre d'infections résolues (fichiers désinfectés ou isolés dans le dossier de quarantaine locale)
- Nombre d'infections bloquées (fichiers n'ayant pas pu être désinfectés, mais dont l'accès a été refusé ; par exemple, un fichier infecté stocké dans un format d'archive propriétaire)

État des malwares de l'ordinateur
Vous aide à découvrir combien et quels ordinateurs du réseau ont été affectés par des malwares pendant une période spécifique et comment les menaces ont été gérées.Les ordinateurs sont regroupés en fonction de ces critères :

- Ordinateurs sans détection (aucun malware n'a été détecté pendant la période spécifiée)
- Les ordinateurs avec des malwares résolus (tous les fichiers détectés ont bien été désinfectés ou isolés dans le dossier de quarantaine local)
- Ordinateurs avec des malwares bloqués (certains des fichiers détectés dont l'accès a été refusé)

Notifications
Ce portlet, qui est réduit par défaut, vous informe des risques de sécurité présents dans le réseau.Des notifications vous sont également envoyées par e-mail.

8.2. Gestion des portlets

Le tableau de bord est facile à configurer en fonction des préférences individuelles.

Vous pouvez réduire les portlets pour vous concentrer sur les informations qui vous intéressent.Lorsque vous réduisez un portlet il disparaît du tableau de bord et sa barre de titre apparaît en bas de la page.Les portlets restants sont automatiquement adaptés à la taille de l'écran. Tous les portlets réduits peuvent être restaurés à tout moment.

Pour gérer un portlet, utilisez les boutons de la barre de titre :

 L'option actualiser re-chargera les données de chaque portlet.

 Cliquez sur ce bouton pour configurer les options de portlet.Certains portlets comprennent des données d'une période spécifique.

 Réduisez le portlet en bas de la page.

 Restaurer un portlet réduit.

9. Utilisation des rapports

Cloud Security for Endpoints vous permet de créer et d'afficher des rapports centralisés sur l'état de sécurité des ordinateurs administrés.Les rapports peuvent être utilisés à diverses fins comme pour :

- Surveiller et garantir le respect des politiques de sécurité de l'organisation.
- Vérifier et évaluer l'état de sécurité du réseau.
- Identifier les problèmes de sécurité, les menaces et les vulnérabilités du réseau.
- Surveiller les incidents de sécurité et l'activité des malwares.
- Fournir à la direction des données faciles à interpréter sur la sécurité du réseau.

Plusieurs types de rapports différents sont disponibles afin que vous puissiez obtenir facilement les informations dont vous avez besoin.Les informations sont présentées sous la forme de camemberts, de tableaux et de graphiques faciles à consulter, qui vous permettent de vérifier rapidement l'état de la sécurité du réseau et d'identifier les problèmes.

Les rapports peuvent regrouper des données de l'ensemble du réseau d'ordinateurs administrés ou uniquement de certains groupes. Ainsi, dans un rapport unique, vous pouvez trouver :

- Des informations statistiques sur tous les groupes d'ordinateurs administrés.
- Des informations détaillées sur chaque ordinateur administré.
- La liste des ordinateurs répondant à certains critères (par exemple, ceux dont la protection antimalware est désactivée.)

Tous les rapports générés sont disponibles par défaut dans la Cloud Security Console pendant 90 jours, mais vous pouvez les enregistrer sur votre ordinateur ou les envoyer par e-mail.Les formats PDF (Portable Document Format) et CSV (comma-separated values) sont disponibles.

9.1. Types de rapports disponibles

Voici la liste des types de rapports disponibles :

État de la mise à jour

Affiche l'état de la mise à jour de la protection Cloud Security for Endpoints installée sur les ordinateurs sélectionnés.Les filtres vous permettent de connaître facilement les clients ayant été ou non mis à jour au cours d'une période donnée.

État de l'ordinateur

Vous fournit diverses informations d'état concernant les ordinateurs sélectionnés sur lesquels la protection Cloud Security for Endpoints est installée.

- État de la mise à jour de la protection
- État de la licence
- État de l'activité du réseau (en ligne/hors ligne)
- État de la protection antimalware

Vous pouvez appliquer les filtres par aspect et état de la sécurité pour trouver les informations que vous recherchez.

Activité des logiciels malveillants

Vous fournit des informations globales et par ordinateur sur les malwares détectés pendant une certaine période sur les ordinateurs sélectionnés.Vous pouvez voir :

- Nombre de détections (fichiers ayant été détectés comme infectés par des malwares)
- Nombre d'infections résolues (fichiers désinfectés ou isolés dans le dossier de quarantaine locale)
- Nombre d'infections bloquées (fichiers n'ayant pas pu être désinfectés, mais dont l'accès a été refusé ; par exemple, un fichier infecté stocké dans un format d'archive propriétaire)

État du module de protection

Vous informe de l'état des modules de protection Cloud Security for Endpoints (Antimalware, Pare-feu, Contrôle de contenu) sur les ordinateurs sélectionnés.L'état de la protection peut être Activé, Désactivé ou Non installé.Le rapport fournit également des informations sur l'état de la mise à jour.

Vous pouvez appliquer les filtres par module et état de la protection pour trouver les informations que vous recherchez.

Les 10 ordinateurs les plus infectés

Vous indique les 10 ordinateurs les plus infectés pendant une période spécifique parmi les ordinateurs sélectionnés.

Les 10 malwares les plus détectés

Vous indique les 10 principaux malwares détectés au cours d'une période donnée sur les ordinateurs sélectionnés.

État du réseau

Vous fournit des informations détaillées sur l'état de sécurité global des ordinateurs sélectionnés.Les ordinateurs sont regroupés en fonction de ces critères :

- Les ordinateurs non administrés ne disposent pas d'une protection Cloud Security for Endpoints installée et leur état de sécurité ne peut pas être évalué.
- Les ordinateurs hors-ligne ont normalement la protection Cloud Security for Endpoints d'installée, mais il n'y a aucune activité récente de Endpoint Security.Le statut de sécurité des ordinateurs en mode hors-ligne ne peut pas être évalué avec précision,

car l'information d'état n'est pas à jour.Pour plus d'informations, reportez-vous à « A propos des ordinateurs hors-ligne » (p. 30).

- Les ordinateurs protégés ont la protection Cloud Security for Endpoints installée et aucun risque de sécurité n'a été détecté.
- Les ordinateurs vulnérables ont la protection Cloud Security for Endpoints installée, mais certaines conditions peuvent empêcher la protection de l'ordinateur. Les détails du rapport affichent les aspects de la sécurité ayant besoin d'être corrigés.

État des malwares de l'ordinateur

Vous aide à découvrir combien et quels ordinateurs sélectionnés ont été affectés par des malwares pendant une période spécifique et comment les menaces ont été gérées.Les ordinateurs sont regroupés en fonction de ces critères :

- Ordinateurs sans détection (aucun malware n'a été détecté pendant la période spécifiée)
- Les ordinateurs avec des malwares résolus (tous les fichiers détectés ont bien été désinfectés ou isolés dans le dossier de quarantaine local)
- Ordinateurs avec des malwares bloqués (certains des fichiers détectés dont l'accès a été refusé)

Exécutif

Vous permet d'exporter les graphiques des portlets du tableau de bord vers un fichier PDF.

9.2. Création de rapports

Pour créer un rapport :

1. Allez sur la page **Rapports > Nouveau Rapport**.

Note
Si vous êtes sur la page **Afficher les rapports** ou **Rapports Planifiés** cliquez simplement sur le bouton **Nouveau** situé au-dessus du tableau.

2. Sélectionnez le type de rapport souhaité dans le menu. Pour plus d'informations, reportez-vous à « Types de rapports disponibles » (p. 86).
3. Indiquez un nom explicite pour le rapport. Lorsque vous choisissez un nom, prenez en compte le type et la cible du rapport, et, éventuellement, les options du rapport.
4. Configurer la cible du rapport.Sélectionnez l'une des options disponibles et cliquez sur le lien correspondant pour choisir les groupes d'ordinateurs ou les ordinateurs individuels à inclure dans le rapport.

5. Configurer la périodicité du rapport (planification).Vous pouvez choisir une création du rapport immédiate, quotidienne, hebdomadaire (un jour spécifique de la semaine) ou mensuelle (un jour spécifique du mois).
6. Configurer les options de rapports.
   a. Pour la plupart des types de rapport, lorsque vous créez un rapport immédiat, vous devez spécifier la période qu'il couvre. Le rapport comprendra uniquement des données sur la période sélectionnée.
   b. Plusieurs types de rapports fournissent des options de filtrage pour vous aider à trouver facilement les informations qui vous intéressent. Utilisez les options de filtrage pour obtenir uniquement les informations souhaitées. Par exemple, pour un rapport **État de la mise à jour**, vous pouvez choisir d'afficher uniquement la liste des ordinateurs mis à jour (ou, au contraire, ceux qui n'ont pas été mis à jour) pendant la période sélectionnée.

      Note
      Lorsque vous affichez le rapport dans la console, toutes les informations seront disponibles, quelles que soient les options sélectionnées. Si vous téléchargez ou envoyez le rapport par e-mail, seul le résumé du rapport et les informations sélectionnées figureront dans le fichier PDF. Les données du rapport complet seront uniquement disponibles au format CSV.

   c. Pour recevoir le rapport par e-mail, sélectionnez l'option correspondante.
7. Cliquez sur **Générer** pour créer le rapport.
   - Si vous avez choisi de créer un rapport immédiat, il s'affichera sur la page Afficher les rapports.Le temps nécessaire à la création des rapports peut varier en fonction du nombre d'ordinateurs administrés. Veuillez patienter le temps que le rapport demandé soit créé.Une fois le rapport créé, vous pouvez l'afficher en cliquant sur son nom.
   - Si vous avez choisi de créer un rapport planifié, il s'affichera sur la page Rapports planifiés.

9.3. Affichage et gestion des rapports générés

Pour afficher et gérer les rapports générés, allez sur la page **Rapports > Afficher les rapports**.Cette page s'affiche automatiquement après la création d'un rapport immédiat.

Note
Les rapports planifiés peuvent être administrés dans la page Rapports > Rapports planifiés.

Vous pouvez afficher les rapports planifiés et des informations utiles les concernant :

- Nom et type de rapport.

- Quand le rapport a été généré.

Pour trier les rapports en fonction d'une colonne, cliquez simplement sur l'en-tête de cette colonne. Cliquez de nouveau sur l'en-tête de colonne pour modifier l'ordre de tri.

Chaque rapport porte l'une des icônes suivantes vous indiquant si le rapport est ou non planifié :

Indique un rapport à usage unique.

Indique un rapport planifié.

Pour afficher les informations les plus récentes, cliquez sur le bouton **Actualiser** dans l'angle inférieur gauche du tableau.

9.3.1. Afficher les rapports

Pour afficher un rapport :

1. Allez sur la page **Rapports > Afficher les rapports**.
2. Cliquez sur le nom du rapport que vous souhaitez afficher.Pour trouver facilement le rapport que vus recherchez, vous pouvez trier les rapports par nom, type, ou date de création.

Tous les rapports sont constitués d'une page Résumé et d'une page Détails.

- La page Résumé vous fournit des données statistiques (graphiques circulaires et autres) pour tous les ordinateurs ou groupes cibles.En bas de chaque page figurent des informations générales sur le rapport, comme la période qu'il couvre (si applicable), la cible du rapport etc.
- La page Détails vous fournit des informations détaillées sur chaque ordinateur administré.Pour certains rapports, vous pouvez avoir besoin de cliquer sur une partie d'un graphique de la page Résumé pour plus d'informations.

Utilisez les onglets de la partie supérieure gauche du rapport pour afficher la page souhaitée.

9.3.2. Recherche des détails du rapport

Les données des rapports sont présentées dans un tableau de plusieurs colonnes fournissant différentes informations. Le tableau peut comprendre plusieurs pages (seules 10 entrées par page sont affichées par défaut).Pour parcourir les pages "détails", utilisez les boutons en bas du tableau.

Pour trouver facilement ce que vous recherchez, utilisez les zones de recherche ou les options de filtrage sous les en-têtes de colonne.

Pour trier les données d'un rapport en fonction d'une colonne, cliquez simplement sur l'en-tête de cette colonne. Cliquez de nouveau sur l'en-tête de colonne pour modifier l'ordre de tri.

9.3.3. Enregistrer des rapports

Par défaut, les rapports générés sont disponibles dans Cloud Security Console pendant 90 jours. Après cette période, ils sont supprimés automatiquement.

Si vous avez besoin que des rapports soient disponibles plus longtemps, vous pouvez les enregistrer sur votre ordinateur. Le résumé du rapport et les données du rapport sélectionnées seront disponibles au format PDF, alors que les données du rapport complet seront disponibles au format CSV.

Pour enregistrer le rapport que vous consultez sur votre ordinateur :

1. Cliquez sur le bouton **Exporter** dans l'angle supérieur droit de la page du rapport. Une fenêtre de téléchargement s'affichera.
2. Téléchargez l'archive `.zip` sur votre ordinateur.En fonction des paramètres de votre navigateur, le fichier peut être téléchargé automatiquement vers un emplacement de téléchargement par défaut.

9.3.4. Impression des rapports

Cloud Security for Endpoints ne prend pas en charge actuellement la fonctionnalité du bouton imprimer. Pour imprimer un rapport, vous devez d'abord l'enregistrer sur votre ordinateur.

9.3.5. Envoyer des rapports par e-mail

Pour envoyer par e-mail le rapport que vous consultez :

1. Cliquez sur le bouton **E-mail** dans l'angle supérieur droit de la page du rapport. Une fenêtre s'affichera.
2. Vous pouvez, si vous le souhaitez, modifier le nom du rapport.
3. Indiquez les adresses e-mail des personnes auxquelles vous souhaitez envoyer le rapport, en les séparant par des points-virgules (;).
4. Cliquez sur **Envoyer un e-mail**.

9.3.6. Suppression automatique de rapports

Par défaut, les rapports générés sont disponibles dans Cloud Security Console pendant 90 jours. Après cette période, ils sont supprimés automatiquement.

Pour modifier la fréquence de la suppression automatique des rapports générés :

1. Allez sur la page **Rapports > Afficher les rapports**.
2. Cliquez sur le lien en-dessous du tableau.
3. Sélectionnez la nouvelle période dans le menu.

4. Cliquez sur **OK**.

9.3.7. Suppression des rapports

Pour supprimer un rapport :

1. Allez sur la page **Rapports > Afficher les rapports**.
2. Sélectionner le rapport.
3. Cliquez sur le bouton **Supprimer** situé au-dessus du tableau.

9.4. Gestion des rapports planifiés

Lors de la création d'un rapport, vous pouvez choisir de configurer une planification à partir de laquelle le rapport sera automatiquement généré (à intervalles réguliers). Ces rapports sont appelés "rapports planifiés".

Les rapports générés seront disponibles sur la page **Rapports > Afficher les rapports** pendant 90 jours par défaut. Ils vous seront également envoyés par e-mail si vous avez sélectionné cette option.

Pour gérer les rapports planifiés, allez sur la page **Rapports > Rapports planifiés**.Vous pouvez afficher tous les rapports planifiés et des informations utiles les concernant :

- Nom et type de rapport.
- Planification en fonction de laquelle le rapport est automatiquement généré.
- Quand le rapport a été généré pour la dernière fois.

9.4.1. Affichage du dernier rapport généré

La page **Rapports > Rapports planifiés** vous permet de voir facilement le rapport le plus récent en cliquant sur le lien de la colonne **Dernier rapport généré**.

9.4.2. Renommer les rapports planifiés

Les rapports générés par un rapport planifié portent son nom.Renommer un rapport planifié n'affectera pas les rapports générés auparavant.

Pour renommer un rapport planifié :

1. Allez sur la page **Rapports > Rapports planifiés**.
2. Cliquez sur le nom du rapport.
3. Modifiez le nom du rapport dans le champ correspondant.Choisissez un nom de rapport explicite pour permettre d'identifier facilement de quoi il s'agit.Lorsque vous choisissez un nom, prenez en compte le type et la cible du rapport, et, éventuellement, les options du rapport.

4. Cliquez sur **Générer** pour enregistrer les modifications.

9.4.3. Modifier les rapports planifiés

Note
Vous pouvez uniquement modifier les rapports planifiés ayant été générés au moins une fois. Si le rapport n'a pas encore été généré, supprimez-le et définissez-en un nouveau avec de nouveaux paramètres.
Lorsqu'un rapport planifié est modifié, toutes les mises à jour sont appliquées à partir de la prochaine génération du rapport. Les rapports générés auparavant ne seront pas affectés par la modification.

Pour modifier les paramètres d'un rapport planifié :

1. Allez sur la page **Rapports > Rapports planifiés**.
2. Cliquez sur le nom du rapport.
3. Modifiez les paramètres du rapport selon vos besoins.Vous pouvez modifier les options suivantes :
   - **Nom du rapport.** Choisissez un nom de rapport explicite pour permettre d'identifier facilement de quoi il s'agit.Lorsque vous choisissez un nom, prenez en compte le type et la cible du rapport, et, éventuellement, les options du rapport.Les rapports générés par un rapport planifié portent son nom.
   - **Cible du rapport.** L'option sélectionnée indique le type de cible du rapport actuel (les groupes ou les ordinateurs individuels).Cliquez sur le lien correspondant pour afficher la cible du rapport actuel. Pour la modifier, cliquez sur l'un des deux liens et sélectionnez les groupes ou ordinateurs à inclure dans le rapport.
   - **Périodicité des rapports (planification).** Vous pouvez configurer une génération automatique du rapport quotidienne, hebdomadaire (un jour spécifique de la semaine) ou mensuelle (un jour spécifique du mois).En fonction de la planification sélectionnée, le rapport contiendra uniquement des données de la veille, de la semaine ou du mois précédent, respectivement.
   - **Options du rapport.** Vous pouvez choisir de recevoir le rapport par e-mail.La plupart des rapports fournissent des options de filtrage pour vous aider à trouver facilement les informations qui vous intéressent. Lorsque vous affichez le rapport dans la console, toutes les informations seront disponibles, quelles que soient les options sélectionnées. Si vous téléchargez ou envoyez le rapport par e-mail, seul le résumé du rapport et les informations sélectionnées figureront dans le fichier PDF. Les données du rapport complet seront uniquement disponibles au format CSV.
4. Cliquez sur **Générer** pour enregistrer les modifications.

9.4.4. Supprimer les rapports planifiés

Lorsqu'un rapport planifié n'est plus nécessaire, il vaut mieux le supprimer.Supprimer un rapport planifié ne supprimera pas les rapports qu'il a générés automatiquement jusqu'à présent.

Pour supprimer un rapport planifié :

1. Allez sur la page **Rapports > Rapports planifiés**.
2. Sélectionner le rapport.
3. Cliquez sur le bouton **Supprimer** situé au-dessus du tableau.

10. Quarantaine

Le logiciel client de Cloud Security for Endpoints isole les fichiers suspects et les fichiers infectés par des malwares qu'il ne peut pas désinfecter dans une zone sécurisée nommée quarantaine.Quand un virus est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté ni lu.

Chaque client a son propre dossier de quarantaine.Pour vous simplifier les choses, le contenu de la quarantaine est géré automatiquement.

Par défaut, des fichiers de la quarantaine sont automatiquement envoyés aux Laboratoires Bitdefender afin d'être analysés par les spécialistes des malwares de Bitdefender.Si la présence de malwares est confirmée, une signature est publiée afin de permettre de supprimer des malwares.

De plus, les fichiers en quarantaine sont analysés après chaque mise à jour des signatures de malwares. Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

Cloud Security Console fournit des informations détaillées sur tous les fichiers placés en quarantaine sur les ordinateurs administrés de votre compte.Pour consulter et gérer les fichiers de la quarantaine, allez sur la page **Quarantaine**.

Des informations sur les fichiers en quarantaine sont affichées dans un tableau. Vous disposez des informations suivantes :

- Nom donné à la menace malware par les chercheurs de sécurité de Bitdefender.
- Chemin vers le fichier infecté ou suspect sur l'ordinateur où il a été détecté.
- Ordinateur sur lequel la menace a été détectée.
- Heure à laquelle le fichier a été placé en quarantaine.
- Action en attente requise par l'administrateur à appliquer au fichier en quarantaine.

Pour afficher les informations les plus récentes, cliquez sur le bouton **Actualiser** dans l'angle inférieur gauche du tableau.Cela peut être nécessaire lorsque vous passez plus de temps sur la page.

10.1. Navigation et Recherche

En fonction du nombre d'ordinateurs administrés et de la nature des infections, le nombre de fichiers en quarantaine peut être important.Le tableau peut comprendre plusieurs pages (seules 10 entrées par page sont affichées par défaut).

Pour parcourir les pages, utilisez les boutons de navigation en bas du tableau. Pour modifier le nombre d'entrées affichées sur une page, sélectionnez une option dans le menu à côté des boutons de déplacement.

S'il y a trop d'entrées, vous pouvez utiliser les zones de recherche sous les en-têtes de colonnes afin de filtrer les données affichées. Vous pouvez par exemple rechercher une menace spécifique détectée dans le réseau ou un ordinateur. Vous pouvez également cliquer sur les en-têtes de colonnes pour trier les données en fonction d'une colonne spécifique.

10.2. Restaurer les fichiers en quarantaine

Vous pouvez parfois avoir besoin de restaurer des fichiers en quarantaine, à leur emplacement d'origine ou à un autre emplacement.Vous pouvez, par exemple, souhaiter récupérer d'importants fichiers contenus dans une archive infectée placée en quarantaine.

Pour restaurer un ou plusieurs fichiers en quarantaine :

1. Allez sur la page **Quarantaine**.
2. Vérifiez la liste des fichiers en quarantaine et cochez les cases correspondant à ceux que vous souhaitez restaurer.
3. Cliquez sur le bouton **Restaurer** dans l'angle supérieur droit de la page.
4. Choisissez l'emplacement où vous souhaitez que les fichiers sélectionnés soient restaurés (soit l'emplacement d'origine soit un emplacement personnalisé sur l'ordinateur cible).

   Si vous choisissez de restaurer à un emplacement personnalisé, vous devez indiquer le chemin dans le champ correspondant. Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin est valide sur tous les ordinateurs cibles. Pour plus d'informations, reportez-vous à « Utilisation des variables du système » (p. 116).
5. Cliquez sur **Restaurer** pour demander une restauration du fichier. Vous pouvez remarquer l'action en attente dans la colonne **Action**.
6. L'action requise est envoyée aux ordinateurs cibles immédiatement ou dès qu'ils sont connectés de nouveau.Une fois un fichier restauré, l'entrée correspondante disparaîtra du tableau Quarantaine.

10.3. Suppression automatique des fichiers en quarantaine

Par défaut, les fichiers placés en quarantaine depuis plus de 30 jours sont automatiquement supprimés.Ce paramètre peut être modifié en éditant la politique affectée aux ordinateurs.

Pour modifier l'intervalle de suppression automatique des fichiers en quarantaine :

1. Allez sur la page **Politiques > Afficher les politiques**.

2. Trouvez la politique affectée aux ordinateurs sur lesquels vous souhaitez modifier le paramètre et cliquez sur son nom.
3. Allez dans la section **Antimalware > Quarantaine**.
4. Sélectionnez dans le menu la fréquence de la suppression automatique souhaitée.
5. Cliquez sur **Enregistrer** pour enregistrer les modifications.

10.4. Supprimer les fichiers en quarantaine

Si vous souhaitez supprimer des fichiers de la quarantaine manuellement, nous vous recommandons de vérifier que les fichiers que vous souhaitez supprimer ne sont pas nécessaires.Suivez ces conseils lors de la suppression des fichiers en quarantaine :

- Un fichier peut constituer le malware lui-même. Si vos recherches aboutissent à cette situation, vous pouvez rechercher cette menace dans la quarantaine et la supprimer.
- Vous pouvez supprimer en toute sécurité :
  - Fichiers d'archive sans importance.
  - Fichiers d'installation infectés.

Pour supprimer un ou plusieurs fichiers en quarantaine :

1. Allez sur la page **Quarantaine**.
2. Vérifiez la liste des fichiers en quarantaine et cochez les cases correspondant à ceux que vous souhaitez supprimer.
3. Cliquez sur le bouton **Supprimer** dans l'angle supérieur droit de la page. Vous pouvez remarquer l'action en attente dans la colonne **Action**.
4. L'action requise est envoyée aux ordinateurs cibles immédiatement ou dès qu'ils sont connectés de nouveau.Une fois un fichier supprimé, l'entrée correspondante disparaîtra du tableau Quarantaine.

11. Comptes utilisateur

Le service Cloud Security for Endpoints peut être configuré et géré à partir du compte Cloud Security Console reçu après l'inscription au service.Il s'agit du compte administrateur de votre entreprise.

Pour autoriser d'autres employés de la société à accéder à Cloud Security Console, vous pouvez créer des comptes utilisateur internes.Les comptes utilisateur peuvent être utilisés pour limiter l'accès aux fonctionnalités de Cloud Security Console ou à certaines parties du réseau de l'entreprise.

Vous pouvez créer deux types de comptes :

Administrateur

Les comptes administrateur fournissent un accès à l'ensemble de la console, apportant aux utilisateurs un contrôle total de Cloud Security for Endpoints.Vous pouvez autoriser l'accès à l'ensemble du réseau ou à un groupe d'ordinateurs spécifique uniquement.

Rapporteur

Les comptes rapporteurs disposent d'un accès limité aux fonctionnalités de la console.Les utilisateurs peuvent uniquement consulter les sections tableau de bord, rapports et journal d'activité, et ne peuvent pas consulter ou modifier la configuration du réseau ou de la sécurité.Vous pouvez autoriser l'accès à l'ensemble du réseau ou à un groupe d'ordinateurs spécifique uniquement.

Pour créer et administrer des comptes utilisateur, rendez-vous sur la page **Comptes > Utilisateurs**.

Les comptes existants s'affichent dans le tableau.Pour chaque compte, vous pouvez voir :

- Nom du propriétaire du compte.
- L'adresse e-mail du compte (utilisée pour se connecter à la Cloud Security Console ainsi que comme adresse de contact).Des rapports et d'importantes notifications de sécurité sont envoyés à cette adresse. Des notifications par e-mail sont envoyées automatiquement lorsque des situations présentant un risque important sont détectées dans le réseau.
- Groupe d'ordinateurs dont l'utilisateur est chargé.
- Rôle utilisateur (administrateur / rapporteur).

11.1. Créer des comptes utilisateur

Créer des comptes utilisateur pour déléguer des responsabilités administratives ou de reporting à d'autres personnes.

Pour créer un compte utilisateur :

1. Allez sur la page **Comptes > Utilisateurs**.
2. Cliquez sur le bouton **Nouveau** dans l'angle supérieur droit de la page.
3. Sous **Détails du compte**, saisissez les détails de votre compte.
   - **Prénom & Nom .** Indiquez le nom complet du propriétaire du compte.
   - **E-mail.** Indiquez l'adresse e-mail de l'utilisateur (qui sera utilisée par l'utilisateur pour se connecter à la Cloud Security Console).Les informations de connexion seront envoyées à cette adresse immédiatement après la création du compte.
   - **Rôles.** Sélectionnez le rôle utilisateur :
     - L'**Administrateur** - dispose de droits d'administration sur les ordinateurs affectés.
     - **Rapporteur** - dispose d'un accès limité à la console, et peut uniquement surveiller et créer des rapports sur la sécurité des ordinateurs affectés.
   - **Groupe.** Choisissez le groupe d'ordinateurs dont l'utilisateur sera responsable.Le reste du réseau de l'entreprise ne sera pas visible par l'utilisateur.Par défaut, l'utilisateur peut voir le réseau entier.
4. Sous **Paramètres**, vous pouvez configurer les paramètres du compte.
   - **Envoyer une notification par e-mail après la connexion**. Activez cette option pour informer l'utilisateur de chaque connexion réussie avec les identifiants du compte de l'utilisateur. Le message envoyé à l'adresse e-mail de l'utilisateur contiendra l'adresse IP source de la requête ainsi que la date et l'heure de la connexion.
   - **Fuseau horaire.** Choisissez dans le menu le fuseau horaire du compte. La console affichera des informations horaires en fonction du fuseau horaire sélectionné.
   - **Langue.** Choisissez dans le menu la langue d'affichage de la console.
5. Cliquez sur **Envoyer**.Le nouveau compte apparaîtra dans la liste des comptes utilisateur.

11.2. Modification des comptes

Modifiez les comptes pour actualiser leurs données ou modifier leurs paramètres.

Pour modifier un compte utilisateur :

1. Allez sur la page **Comptes > Utilisateurs**.
2. Cliquez sur le nom de l'utilisateur.
3. Modifier les détails et les paramètres des comptes selon vos besoins.
4. Cliquez sur **Soumettre** pour enregistrer les modifications.

11.3. Supprimer des comptes

Supprimer les comptes quand ils ne sont plus utiles.Si le propriétaire du compte, par exemple, a quitté l'entreprise.

Pour supprimer un compte :

1. Allez sur la page **Comptes > Utilisateurs**.
2. Sélectionnez le compte dans la liste.
3. Cliquez sur le bouton **Supprimer** dans l'angle supérieur droit de la page.

11.4. Réinitialiser les mots de passe de connexion

Les propriétaires de comptes qui oublient leur mot de passe peuvent le réinitialiser à l'aide du lien de récupération du mot de passe de la page de connexion. Vous pouvez également réinitialiser un mot de passe de connexion oublié en modifiant le compte correspondant à partir de la console.

Pour réinitialiser le mot de passe de connexion d'un utilisateur :

1. Allez sur la page **Comptes > Utilisateurs**.
2. Cliquez sur le nom de l'utilisateur.
3. Indiquez un nouveau mot de passe dans les champs correspondants (sous **Détails du compte**).
4. Cliquez sur **Soumettre** pour enregistrer les modifications. Veillez à informer le propriétaire du compte du nouveau mot de passe.

12. Journal d'activité de l'utilisateur

La Cloud Security Console enregistre toutes les opérations et actions effectuées par les utilisateurs.Les événements enregistrés comprennent :

- Connexion et déconnexion
- Créer, éditer, renommer et supprimer des comptes d'utilisateur
- Créer, éditer, renommer et supprimer des politiques
- Créer, éditer, renommer et supprimer des rapports
- Supprimer, restaurer les fichiers en quarantaine
- Supprimer ou déplacer des ordinateurs entre des groupes
- Créer, déplacer, renommer et supprimer des groupes

Pour consulter les enregistrements de l'activité de l'utilisateur, allez sur la page **Journal**.

Les événements enregistrés s'affichent dans un tableau.Les colonnes du tableau vous donnent les informations utiles sur les événements de la liste.

- Nom de l'utilisateur ayant effectué l'action.
- Type de compte utilisateur.
- Action ayant causé l'événement.
- Type d'objet console affecté par l'action.
- Objet spécifique affecté par l'action.
- L'adresse IP à partir de laquelle l'utilisateur est connecté.
- Heure à laquelle l'événement s'est produit.

Pour trouver facilement ce que vous recherchez, utilisez les zones de recherche ou les options de filtrage sous les en-têtes de colonne.Pour trier les événements en fonction d'une colonne, cliquez simplement sur l'en-tête de cette colonne. Cliquez de nouveau sur l'en-tête de colonne pour inverser l'ordre de tri.

Pour afficher des informations détaillées sur un événement, sélectionnez-le et consultez la section sous le tableau.

Pour afficher les informations les plus récentes, cliquez sur le bouton **Actualiser** dans l'angle inférieur gauche du tableau.

13. Utiliser Update Server

Update Server vous permet de créer un emplacement pour les mises à jour de Bitdefender sur le réseau local.Votre serveur local de mise à jour vous permet de configurer et d'affecter des politiques aux clients Bitdefender afin qu'ils se mettent à jour à partir du miroir local plutôt que sur Internet.

En utilisant un emplacement local des mises à jour de Bitdefender, vous réduisez le trafic Internet (un seul ordinateur se connecte à Internet pour télécharger les mises à jour) et obtenez des mises à jour plus rapides.

Update Server est complètement automatisé. Pour mettre à jour les clients Bitdefender à partir du réseau local, installez simplement Update Server et affectez-leur des politiques avec l'adresse du serveur local de mise à jour.L'emplacement des mises à jour peut être configuré dans la catégorie paramètres de la politique **Général**, onglet **Mise à jour**.

L'adresse des mises à jour locales devant être configurée sur les produits clients Bitdefender doit respecter l'une des syntaxes suivantes :

- `ip_du_serveur_de_mise_à_jour : port_du_serveur_de_mise_à_jour`
- `nom_du_serveur_de_mise_à_jour : port_du_serveur_de_mise_à_jour`

Le port par défaut est `7074`.

Note
Update Server peut être utilisé pour mettre à jour non seulement les clients Cloud Security for Endpoints, mais également d'autres produits Bitdefender. Reportez-vous à leur documentation pour savoir comment les configurer pour effectuer des mises à jour à partir d'un serveur de mise à jour local.

13.1. Installation

Vous trouverez ici toutes les informations nécessaires pour installer Update Server dans le réseau local.

13.1.1. Configuration requise

Vous pouvez installer Update Server sur tout ordinateur fonctionnant avec Windows XP ou un système d'exploitation Windows plus récent.

Navigateurs pris en charge (pour la configuration et l'administration) :

- Internet Explorer 8 (+)
- Firefox 8 (+)
- Chrome 10 (+)
- Safari 4 (+)

13.1.2. Récupération du Fichier d'Installation

Pour obtenir le fichier d'installation de Update Server :

1. Connectez vous à la Cloud Security Consoleen utilisant votre compte.
2. Allez sur la page **Ordinateurs > Zone d'installation**.
3. Cliquez sur le bouton **Lien d'installation** et sélectionnez **Afficher**.
4. Selon la plateforme sur laquelle vous installez Update Server, choisissez la version 32 bits ou 64 bits du fichier d'installation.

13.1.3. Installer Update Server

L'ordinateur sur lequel vous installez Update Server doit être connecté à Internet en permanence et accessible depuis les ordinateurs protégés par Bitdefender.

Pour installer Update Server :

1. Copiez ou téléchargez le fichier d'installation sur l'ordinateur désigné.
2. Double-cliquez sur le fichier d'installation pour lancer l'assistant d'installation.
3. Cliquez sur **Suivant**.
4. Veuillez lire le contrat de licence, sélectionnez **J'accepte les termes du contrat de licence** et cliquez sur **Suivant**.

   Note
   Si vous n'acceptez pas ces termes cliquez sur **Annuler**. Le processus d'installation sera abandonné et vous quitterez l'installation.

5. Choisissez un des types d'installation disponibles pour continuer :
   - **Par défaut** - pour une installation avec les options par défaut.
   - **Personnalisé** - pour configurer les paramètres d'installation.

   Si vous optez pour l'installation par défaut, passez directement à l'étape 8.
6. **Installation personnalisée!** Update Server sera installé dans `?:\Program Files\Bitdefender\Update Server`.Pour changer de dossier d'installation, cliquez sur **Parcourir** et sélectionnez un autre dossier.

   Cliquez sur **Suivant**.

7. **Installation personnalisée!** Le port par défaut est `7074`.Si vous souhaitez changer le port par défaut, entrez une autre valeur dans le champ de saisie.

   Important
   Veuillez tenir compte des précisions suivantes :

   - Indiquez des valeurs de port entre 1 et 65535.
   - Configurez le pare-feu sur l'ordinateur où Update Server est installé afin de permettre l'utilisation de ce port.
   - Le port de Update Server ne doit pas être utilisé par d'autres applications installées sur le système.

   Cliquez sur **Suivant**.Si le port est utilisé, vous serez invité à définir un nouveau port. Dans le cas contraire, une nouvelle fenêtre s'affichera.
8. Cliquez sur **Installer** pour lancer l'installation.
9. Patientez jusqu'à ce que l'installation soit complète puis cliquez sur **Terminer**.

13.2. Configuration et administration

Reportez-vous aux sujets suivants pour savoir comment configurer et administrer l'emplacement de mise à jour Bitdefender dans le réseau local à l'aide de Update Server.

13.2.1. Accès au panneau d'administration

Update Server dispose d'une interface web, qui permet une configuration et un contrôle faciles à partir de tout ordinateur connecté au réseau.

Pour accéder au panneau d'administration de Update Server, appliquez l'une des actions suivantes :

- Ouvrez un navigateur web et tapez l'adresse du serveur en utilisant l'une des syntaxes suivantes :
  - `http://update_server_ip:port`
  - `http://update_server_name:port`
- Sur l'ordinateur sur lequel Update Server est installé, allez dans le menu Démarrer de Windows et suivez le chemin suivant : **Démarrer** → **Programmes** → **Update Server** → **Update Server**.

Saisissez le mot de passe dans le champ correspondant et cliquez sur **Connexion**.Le mot de passe par défaut est `admin`.

13.2.2. À faire après l'installation

Voici ce que vous devez faire après l'installation :

1. Modifiez le mot de passe `administrateur` par défaut pour empêcher l'accès non autorisé. Pour plus d'informations, reportez-vous à « Changer de mot de passe de connexion » (p. 108).
2. Si l'ordinateur sur lequel Update Server est installé se connecte à Internet via un serveur proxy, vous devez configurer les paramètres du proxy.
   a. Accédez à la page **Configuration**.
   b. Cochez la case **Utiliser les paramètres du proxy**.
   c. Indiquez les paramètres du proxy à utiliser. Pour plus d'informations, reportez-vous à « Configuration des paramètres » (p. 106).
3. Configurez les produits clients installés dans le réseau pour que les mises à jour soient téléchargées à partir du serveur local de mise à jour. Utilisez la politique pour configurer Endpoint Security avec l'adresse de mise à jour locale (catégorie paramètres **Général**, onglet **Mise à jour**).

   L'adresse des mises à jour locales devant être configurée sur les produits clients Bitdefender doit respecter l'une des syntaxes suivantes :
   - `ip_du_serveur_de_mise_à_jour : port`
   - `nom_du_serveur_de_mise_à_jour : port`

   Le port par défaut est `7074`.

13.2.3. Administration des produits clients et des mises à jour téléchargées

Pour administrer les produits clients pour lesquels des mises à jour sont téléchargées et consulter des informations sur les mises à jour, rendez-vous dans la page **Produits** (elle s'affiche par défaut après la connexion au panneau d'administration).

Vous pouvez consulter les statistiques de Update Server et la liste des produits clients pour lesquels des mises à jour sont téléchargées. L'état et l'heure de la dernière mise à jour de chaque produit client sont indiqués.

Téléchargement des dernières mises à jour

Pour télécharger les mises à jour disponibles pour tous les produits de la liste, cliquez sur le bouton **Mettre à jour maintenant**.

Ajouter de Nouveaux Produits

Pour sélectionner d'autres produits devant être mis à jour par Update Server, cliquez sur le bouton **Ajouter des produits**.Une nouvelle page s'affiche.

Vous pouvez afficher la liste de produits clients Bitdefender supplémentaires pouvant être mis à jour avec Update Server. Pour parcourir cette liste facilement, vous pouvez filtrer les produits par type, plateforme et langue.

Cochez la case correspondant aux produits souhaités et cliquez sur le bouton **Enregistrer**.

Désinstaller des Produits

Pour retirer un produit de la liste des produits mis à jour, cliquez sur le lien correspondant **Supprimer** dans la colonne **Actions**. Si vous retirez un produit client de la liste :

1. Update Server ne téléchargera plus de mises à jour pour ce produit client. Cependant, si le produit client se connecte par la suite à Update Server afin de rechercher des mises à jour, il sera automatiquement ajouté à la liste.
2. Les mises à jour téléchargées pour ce produit client sont supprimées si elles ne sont pas utilisées par un autre produit de la liste. Par exemple, les signatures de malwares sont les mêmes pour toutes les versions linguistiques d'un produit et d'une plateforme (32 bits ou 64 bits).

13.2.4. Configuration des paramètres

Pour configurer les paramètres de Update Server, accédez à la page **Configuration**.Les paramètres suivants peuvent être configurés :

- **Update Server.** Par défaut, Update Server téléchargera les mises à jour sur l'ordinateur local à partir de `upgrade.bitdefender.com:80`.Il s'agit d'une adresse générique qui est résolue automatiquement pour correspondre au serveur le plus proche qui stocke les signatures de logiciels malveillants Bitdefender dans votre zone géographique.

  Pour rechercher et télécharger des mises à jour à partir d'un serveur local de mise à jour (configuration en cascade), remplacez l'adresse de mise à jour sur Internet par l'adresse du serveur local de mise à jour.Utilisez l'une des syntaxes suivantes :
  - `ip_du_serveur_de_mise_à_jour : port`
  - `nom_du_serveur_de_mise_à_jour : port`

  Le port par défaut est `7074`.
- **Répertoire local.** Pour changer le dossier dans lequel les mises à jour sont téléchargées, tapez le chemin du nouveau dossier dans ce champ.
- **Port de l'Update Server.** Vous pouvez modifier dans ce champ le port de Update Server configuré pendant l'installation. Le port par défaut est `7074`.Le port de Update Server ne doit pas être utilisé par d'autres applications installées sur le système.

Note
Si vous modifiez le port à un moment où Update Server est déjà en cours d'utilisation, l'emplacement des mises à jour de tous les produits Bitdefender configurés pour télécharger des mises à jour à partir du serveur de mise à jour local doit être modifié en conséquence.

- **Fréquence des mises à jour.** Par défaut, Update Server télécharge des mises à jour à partir de l'emplacement des mises à jour Internet toutes les heures. Pour modifier la fréquence des mises à jour, tapez une nouvelle valeur dans ce champ.
- **Durée de la session.** Par défaut, vous êtes automatiquement déconnecté(e) du panneau d'administration après 5 minutes d'inactivité. Pour modifier la durée maximale d'inactivité autorisée, tapez une nouvelle valeur dans ce champ. Vous pouvez indiquer une durée entre 1 et 30 minutes.
- **Afficher les paramètres avancés.** Cochez cette case pour afficher et configurer les paramètres avancés.
  - **Rôles de passerelle.** Update Server peut agir en tant que passerelle pour les données envoyées par les produits clients Bitdefender installés dans le réseau aux serveurs Bitdefender. Ces données peuvent comprendre des rapports anonymes concernant l'activité des virus et de spam, les rapports de plantage du produit et les données utilisées pour l'inscription en ligne.Activer les rôles de passerelle est utile pour le contrôle de trafic dans les réseaux n'ayant pas accès à Internet.

    Note
    Vous pouvez désactiver à tout moment les modules du produit qui envoient des données statistiques ou sur les plantages aux Laboratoires Bitdefender.Vous pouvez utiliser des politiques pour contrôler ces options à distance sur les ordinateurs administrés par Cloud Security Console.

  - **Télécharger les emplacements non sélectionnés.** Update Server télécharge automatiquement les mises à jour de tout produit client Bitdefender les nécessitant (même si vous n'avez pas sélectionné ce produit sur la page Produits).Si vous souhaitez que seules les mises à jour des produits autorisés soient téléchargées, décochez cette case.
  - **Autoriser la mise à jour des produits non utilisés.** Update Server recherche et télécharge des mises à jour régulièrement pour tous les produits Bitdefender ayant besoin de mises à jour. Si vous souhaitez arrêter de télécharger des mises à jour qui n'ont pas été demandées pendant un certain temps, décochez cette case et spécifiez la période d'inactivité.
- **Utiliser les paramètres du proxy .** Cochez cette case si votre entreprise se connecte à Internet via un proxy. Vous devez entrer les informations requises dans les champs suivants :
  - **Adresse du proxy** - saisissez l'adresse IP du serveur proxy.
  - **Port Proxy** - saisissez le port utilisé pour se connecter au serveur proxy.

- **Nom d'utilisateur Proxy** - indiquez un nom d'utilisateur reconnu par le serveur proxy.
- **Mot de passe Proxy** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.

Si vous sélectionnez **Utiliser le cache du proxy**, Update Server recherchera d'abord dans le cache du serveur proxy les mises à jour téléchargées récemment et utilisera ces mises à jour, si elles sont disponibles. Cette option n'est pas recommandée, mais peut être utile si vous payez votre connexion Internet en fonction du trafic.

Cliquez sur le bouton **Enregistrer** pour enregistrer les modifications.

13.2.5. Changer de mot de passe de connexion

Pour changer le mot de passe de connexion :

1. Sélectionnez **Changer de mot de passe** dans le menu **Administrateur** dans l'angle supérieur droit du panneau d'administration.Une nouvelle page s'affiche.
2. Vous devez entrer les informations requises dans les champs suivants :
   - **Ancien mot de passe** - entrez l'ancien mot de passe.
   - **Nouveau mot de passe** - entrez le nouveau mot de passe.
   - **Confirmer le mot de passe** - resaisissez le nouveau mot de passe.
3. Cliquez sur **Changer de mot de passe** pour enregistrer le nouveau mot de passe.

13.3. Configuration en cascade

Vous pouvez configurer les serveurs locaux de mise à jour Bitdefender pour télécharger les mises à jour Bitdefender à partir d'un serveur local de mise à jour au lieu d'Internet. Cette configuration est connue sous le nom de "configuration en cascade".

La configuration en cascade est généralement utilisée dans des réseaux informatiques répartis géographiquement, lorsque l'une des conditions suivantes est remplie :

- Seul le réseau central a un accès direct à Internet (les autres réseaux peuvent se connecter via le réseau central ou n'ont pas du tout accès à Internet).
- La connexion au réseau central est plus rapide (ou plus pratique d'une façon ou d'une autre) que la connexion directe à Internet.

Pour définir une configuration en cascade :

1. Installez et configurez le serveur local de mise à jour qui téléchargera les mises à jour Bitdefender sur Internet. Aucune configuration particulière n'est nécessaire pour que ce serveur de mise à jour permette la distribution de mises à jour Bitdefender à d'autres serveurs locaux de mise à jour (les mises à jour sont automatiquement disponibles à la fois pour les clients Bitdefender et les autres serveurs locaux de mise à jour, s'ils sont correctement configurés).

2. Configurez les serveurs de mise à jour des réseaux isolés pour que les mises à jour soient téléchargées à partir du serveur principal de mise à jour. Voici ce que vous devez faire :

   a. Accédez à la page **Configuration**.

   b. Dans le champ **Serveur de mise à jour**, remplacez l'adresse de mise à jour sur Internet par l'adresse du serveur local de mise à jour qui télécharge des mises à jour sur Internet. Utilisez l'une des syntaxes suivantes :

      - `ip_du_serveur_principal_de_mise_à_jour : port_du_serveur_principal_de_mise_à_jour`
      - `nom_du_serveur_principal_de_mise_à_jour : port_du_serveur_principal_de_mise_à_jour`

      Le port par défaut est `7074`.

   c. Vérifiez que les serveurs de mise à jour peuvent communiquer.La façon la plus simple de le tester est d'aller sur la page Produits, d'ajouter un nouveau produit à la liste et de lancer une mise à jour. Si la mise à jour ne peut pas être effectuée, vérifiez les configurations de votre réseau et de votre pare-feu.

3. Il n'y a pas de changement dans la façon dont vous configurez les produits clients Bitdefender pour se mettre à jour à partir de leur serveur local de mise à jour.

14. Obtenir de l'aide

Bitdefender fait le maximum pour apporter à ses clients une aide hors pair, rapide et efficace.Si vous rencontrez le moindre problème ou si avez une question à poser concernant votre produit Bitdefender, consultez notre Centre d'assistance en ligne. Il propose de la documentation que vous pouvez utiliser pour trouver rapidement une solution ou obtenir une réponse.Si vous le préférez, vous pouvez également contacter l'équipe du Service Clients de Bitdefender. Nos membres du support technique répondront à vos questions aussi rapidement que possible et vous fourniront l'assistance dont vous avez besoin.

Note
Vous trouverez des informations sur les services d'aide et de support que nous fournissons ainsi que des détails sur notre politique d'assistance.

14.1. Centre de support de Bitdefender

Le Centre de support de Bitdefender, disponible à l'adresse http://www.bitdefender.fr/businesshelp, est l'endroit où vous trouverez toute l'assistance dont vous avez besoin concernant votre produit Bitdefender.

Vous pouvez utiliser différentes ressources pour trouver rapidement une solution ou une réponse :

- Articles de la base de connaissances
- Forum du Support Bitdefender
- Documentation du produit

Vous pouvez également utiliser votre moteur de recherche favori pour obtenir plus d'informations sur la sécurité informatique, les produits et l'entreprise Bitdefender.

Articles de la base de connaissances

La base de connaissances de Bitdefender est un ensemble d'informations en ligne concernant les produits Bitdefender. Il contient, dans un format facilement accessible, les rapports d'incidents survenus et constatés par le support technique, les équipes de réparation des bugs de Bitdefender. Ainsi que des articles généraux sur la prévention antivirus, la gestion des solutions Bitdefender, des informations détaillées et beaucoup d'autres articles.

La base de connaissances de Bitdefender est accessible au public et peut être consultée gratuitement. Cet ensemble d'informations est une autre manière de fournir aux clients de Bitdefender les informations techniques dont ils ont besoin. Toutes les requêtes valides

d'informations ou de rapports de bugs provenant de clients Bitdefender trouvent une réponse dans la base de connaissances de Bitdefender, comme les rapports de corrections de bugs, les solutions de rechange ou les articles d'informations venant compléter les fichiers d'aide des produits.

La base de connaissances des produits pour Entreprises de Bitdefender est accessible à tout moment à l'adresse http://www.bitdefender.fr/businesshelp.

Forum du Support Bitdefender

Le Forum du Support Bitdefender fournit aux utilisateurs de Bitdefender une manière simple d'obtenir de l'aide et d'aider les autres. Vous pouvez poster tout problème ou toute question concernant votre produit Bitdefender.

Les techniciens du support Bitdefender surveillent le forum à la recherche de nouvelles publications afin de vous aider. Vous pouvez également obtenir une réponse ou une solution d'un utilisateur Bitdefender plus expérimenté.

Avant de publier un problème ou une question, recherchez s'il existe une rubrique similaire ou connexe dans le forum.

Le forum de support de Bitdefender est disponible à http://forum.bitdefender.com, dans 5 langues différentes : français, anglais, allemand, espagnol et roumain.Cliquez sur le lien **Protection des entreprises** pour accéder à la section dédiée aux produits pour entreprises.

Documentation du produit

La documentation de votre produit est la source d'informations la plus riche.

Vous pouvez consulter et télécharger la version la plus récente de la documentation sur les produits Bitdefender pour entreprises dans Centre de Support > Documentation.

14.2. Demande d'aide

Vous pouvez nous contacter pour nous demander de l'aide grâce à notre Centre de support en ligne :

1. Allez à http://www.bitdefender.fr/site/Main/nousContacter/.
2. Utilisez le formulaire de contact pour faire une demande par e-mail ou accéder aux autres options de contact disponibles.

14.3. Utiliser l'Outil de Support

L'Outil de Support Cloud Security for Endpoints est conçu pour aider les utilisateurs et les techniciens du support à obtenir facilement les informations dont ils ont besoin pour la résolution des problèmes.Exécutez l'Outil de Support sur les ordinateurs affectés et envoyez

l'archive créée avec les informations de résolution de problèmes au représentant du support Bitdefender.

Pour utiliser l'Outil de Support :

1. Téléchargez l'Outil de Support et diffusez-le aux ordinateurs affectés.Pour télécharger l'Outil de Support :
   a. Connectez vous à la Cloud Security Consoleen utilisant votre compte.
   b. Cliquez sur le lien **Aide et Support**, dans l'angle supérieur droit de la console.
   c. Les liens de téléchargement sont disponibles dans la section **Outil de Support**.Deux versions sont disponibles : l'une pour les systèmes 32 bits et l'autre pour les systèmes 64 bits. Vérifiez que vous utilisez la version correcte lorsque vous exécutez l'Outil de Support sur un ordinateur.
2. Exécuter l'Outil de Support localement sur chacun des ordinateurs affectés.
   a. Cochez la case d'accord et cliquez sur **Suivant**.
   b. Compléter le formulaire de soumission avec les données nécessaires :
      i. Indiquez votre adresse e-mail.
      ii. Saisissez votre nom.
      iii. Sélectionnez à partir du menu correspondant le type de problème que vous avez rencontré.
      iv. Sélectionnez votre pays dans le menu correspondant.
      v. Décrivez le problème que vous avez rencontré.
   c. Cliquez sur **Suivant**.L'Outil de Support recueille des informations sur le produit, liées aux autres applications installées sur la machine et à la configuration matérielle et logicielle.
   d. Patientez jusqu'à la fin du processus.
   e. Cliquez sur **Terminer** pour fermer la fenêtre.Une archive zip a été créée sur votre bureau.

      Vous pouvez envoyer l'archive zip avec votre demande de support afin de réduire le temps nécessaire à la résolution du problème.

14.4. Contacts

Une communication efficace est la clé d'une relation réussie. Au cours des dix dernières années, Bitdefender s'est bâti une réputation incontestable dans sa recherche constante d'amélioration de la communication pour dépasser les attentes de ses clients et de ses partenaires. N'hésitez pas à nous contacter pour toute question.

14.4.1. Adresses Web

Ventes : bitdefender@editions-profil.eu
Centre de support :http://www.bitdefender.fr/businesshelp
Documentation : documentation@bitdefender.com
Distributeurs Locaux :http://www.bitdefender.fr/partners/
Partner Program: partners@bitdefender.com
Relations Presse : communication@editions-profil.eu
Job Opportunities: jobs@bitdefender.com
Virus Submissions: virus_submission@bitdefender.com
Spam Submissions: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Site web :http://www.bitdefender.fr

14.4.2. Distributeurs Locaux

Les distributeurs locaux Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux.

Pour trouver un distributeur Bitdefender dans votre pays :

1. Allez à http://www.bitdefender.fr/partners/.
2. Allez dans **Trouver un partenaire**.
3. Les informations de contact des distributeurs locaux de Bitdefender devraient s'afficher automatiquement. Si ce n'est pas le cas, sélectionnez votre pays de résidence pour afficher les informations.
4. Si vous ne trouvez pas de distributeur Bitdefender dans votre pays, n'hésitez pas à nous contacter par e-mail à l'adresse bitdefender@editions-profil.eu.Veuillez rédiger votre e-mail en anglais pour optimiser le traitement de votre demande.

14.4.3. Bureaux de Bitdefender

Les bureaux de Bitdefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de sujets commerciaux ou généraux. Leur adresse respective et contacts sont listés ci-dessous.

Etats-Unis

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Téléphone (Service commercial et support technique) : 1-954-776-6262

Ventes : sales@bitdefender.com
Site Web : http://www.bitdefender.com
Centre de support : http://www.bitdefender.com/businesshelp

Allemagne

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Téléphone (services administratif et commercial) : +49 (0)2301 91 84 222
Téléphone (support technique) : +49 (0)2301 91 84 444
Ventes : vertrieb@bitdefender.de
Site Internet : http://www.bitdefender.de
Centre de support : http://www.bitdefender.de/businesshelp

Royaume-Uni et Irlande

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Téléphone (Service commercial et support technique) : +44 (0) 8451-305096
E-mail : info@bitdefender.co.uk
Ventes : sales@bitdefender.co.uk
Site Internet : http://www.bitdefender.co.uk
Centre de support : http://www.bitdefender.co.uk/businesshelp

Espagne

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax : (+34) 93 217 91 28
Téléphone (services administratif et commercial) : (+34) 93 218 96 15
Téléphone (support technique) : (+34) 93 502 69 10
Ventes : comercial@bitdefender.es
Site Internet : http://www.bitdefender.es
Centre de support : http://www.bitdefender.es/businesshelp

Roumanie

BITDEFENDER SRL
DV24 Offices, Building A
24 Delea Veche Street
024102 Bucharest, Sector 2
Fax : +40 21 2641799
Téléphone (Service commercial et support technique) : +40 21 2063470
Ventes : sales@bitdefender.ro
Site Internet : http://www.bitdefender.ro
Centre de support : http://www.bitdefender.ro/businesshelp

Emirats arabes unis

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Téléphone (Service commercial et support technique) : 00971-4-4588935 / 00971-4-4589186
Fax : 00971-4-44565047
Ventes : sales@bitdefender.com
Site Web : http://www.bitdefender.com/world
Centre de support : http://www.bitdefender.com/businesshelp

A. Annexes

A.1. Liste des types de fichier d'Application

Les moteurs d'analyse antimalware inclus dans les solutions de sécurité Bitdefender peuvent être configurés pour limiter l'analyse aux fichiers d'applications (ou de programmes)Les fichiers d'applications sont bien plus vulnérables aux attaques de malwares que les autres types de fichiers.

Cette catégorie comprend des fichiers avec les extensions suivantes :

```
386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu;
acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat;
bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek;
dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe;
ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd;
ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam;
maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt;
mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one;
onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx;
ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub;
puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr;
script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx;
tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm;
wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls;
xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
```

A.2. Utilisation des variables du système

Certains paramètres disponibles dans la console requièrent de spécifier le chemin sur les ordinateurs cibles.Il est recommandé d'utiliser les variables du système (le cas échéant) afin de s'assurer que le chemin est valide sur tous les ordinateurs cibles.

Voici la liste des variables du système prédéfinies :

`%ALLUSERSPROFILE%`
: Le dossier de profil All Users.Chemin typique :

  `C:\Documents and Settings\All Users`

`%APPDATA%`
: Le dossier Application Data de l'utilisateur connecté.Chemin typique :

- Windows XP :

  `C:\Documents and Settings\{username}\Application Data`

- Windows Vista/7 :

  `C:\Users\{username}\AppData\Roaming`

`%HOMEPATH%`

Les dossiers utilisateurs.Chemin typique :

- Windows XP :

  `\Documents and Settings\{username}`

- Windows Vista/7 :

  `\Users\{username}`

`%LOCALAPPDATA%`

Les fichiers temporaires d'applications.Chemin typique :

`C:\Users\{username}\AppData\Local`

`%PROGRAMFILES%`

Le dossier Program Files. Le chemin d'accès est généralement `C:\Program Files`.

`%PROGRAMFILES(X86)%`

Le dossier Program Files pour les applications 32 bits (sur les systèmes 64 bits).Chemin typique :

`C:\Program Files (x86)`

`%COMMONPROGRAMFILES%`

Le dossier Fichiers communs.Chemin typique :

`C:\Program Files\Common Files`

`%COMMONPROGRAMFILES(X86)%`

Le dossier Fichiers communs pour les applications 32 bits (sur les systèmes 64 bits).Chemin typique :

`C:\Program Files (x86)\Common Files`

`%WINDIR%`

Le répertoire Windows ou SYSROOT. Le chemin d'accès est généralement `C:\Windows`.

Glossaire

ActiveX

ActiveX est un modèle pour écrire des programmes afin que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour faire des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent poser ou répondre à des questions, utiliser des boutons et interagir de multiples façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic.

Active X est connu pour son manque total de commandes de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Adware

Les adwares sont souvent associés à des applications gratuites mais exigeant leur acceptation par l'utilisateur. Ces adwares étant généralement installés une fois que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant, les « pop up » publicitaires peuvent devenir contrariants et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.

Applette Java

Il s'agit d'un programme Java conçu pour s'exécuter uniquement dans une page Web. Pour utiliser un applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels) qu'il peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applet depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications par le fait qu'ils sont régis par un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, ils ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applets sont également limités pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

Archive

Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

Backdoor

Il s'agit d'une faille dans la sécurité d'un système délibérément laissée en place par des développeurs ou des personnes chargées de la maintenance. Les intentions ne sont pas toujours malveillantes ; quelques systèmes d'exploitation, par exemple, permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Chemin

Directions exactes vers un fichier d'un ordinateur. Ces directions sont généralement décrites par arborescence, de haut en bas.

La connexion entre deux points, telle le canal de communication entre deux ordinateurs.

Client de messagerie

Un client de messagerie est une application qui vous permet d'envoyer et recevoir des e-mails.

Code malveillant

« Malware » est un terme générique regroupant les logiciels conçus pour faire du tort ; il s'agit de la contraction de « malicious software » (logiciels malveillants) L'emploi de ce terme n'est pas encore universel, mais sa popularité pour désigner les virus, les chevaux de Troie, les vers et les codes mobiles malveillants progresse.

Cookies

Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une arme à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent car vous voyez seulement les annonces vous intéressant. Mais cela implique également le "pistage" et le "suivi" des sites que vous consultez et de ce sur quoi vous cliquez. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple "numéro SKU" (le code barres se trouvant au dos des produits). Bien que ce point de vue puisse paraître extrême, il est parfois justifié.

Disk drive

C'est une appareil qui lit et écrit des données sur un disque.

Une unité de disque dur lit et écrit sur un disque dur.

Un lecteur de disquette accède à des disquettes.

Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

E-mail

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Événements

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme le manque de mémoire.

Extension de fichier

La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier.

De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS-DOS. Elles comportent communément une à trois lettres (certains anciens OS n'en supportent pas plus de trois). Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Fausse alerte

Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

Fichier journal (Log)

Fichier qui enregistre les actions ayant eu lieu. La Bitdefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Heuristique

Méthode basée sur des règles permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter les variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP

Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Keylogger

Application qui enregistre tout ce qui est tapé.

Les keyloggers ne sont pas nécessairement malveillants. Ils peuvent être utilisés à des fins légitimes, comme pour surveiller les activités d'employés ou d'enfants. Ils sont toutefois de plus en plus utilisés par les cybercriminels à des fins malveillantes (par exemple, pour recueillir des informations confidentielles, telles que des identifiants de connexion ou des numéros de sécurité sociale).

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Mémoire

Zones de stockage internes dans l'ordinateur. Le terme mémoire définit le stockage de données sous la forme de composants électroniques, le mot stockage étant utilisé pour définir le stockage de données sur bande magnétique ou disques amovibles. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Mise à jour

Nouvelle version d'un logiciel ou d'un produit hardware, destinée à remplacer une version antérieure du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, et si ce n'est pas le cas, la mise à jour ne se fait pas.

Bitdefender a son propre module de mise à jour permettant à l'utilisateur de rechercher manuellement les mises à jour ou de les programmer automatiquement.

Navigateur

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les deux navigateurs les plus populaires sont Netscape Navigator et Microsoft Internet Explorer. Les deux sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugins) pour certains formats.

Non-heuristique

Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut sembler être un virus et ne génère donc pas de fausses alertes.

Objets menu démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage de l'ordinateur. Par exemple, un écran de démarrage, un fichier son pour le démarrage de l'ordinateur, un calendrier, des programmes, peuvent être placés dans ce dossier. C'est généralement un raccourci vers le fichier qui est placé dans le dossier, et pas le fichier.

Phishing

Action d'envoyer un e-mail à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire de l'e-mail. Cet e-mail oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Port

Une interface sur un ordinateur auquel vous pouvez connecter un appareil. Les ordinateurs comportent plusieurs sortes de ports. Il existe plusieurs ports internes permettant de connecter des lecteurs de disques, des écrans et des claviers. A l'extérieur, les ordinateurs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Programmes empaquetés

Fichier dans un format compressé. Beaucoup de systèmes d'exploitation et d'applications contiennent des commandes vous permettant de compresser un fichier afin qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide" à la suite. Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui compresse des fichiers remplace la série d'espaces par un caractère spécial pour les séries d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant un accès de niveau administrateur à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX et se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs système.

Le principal rôle des rootkits est de masquer des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseau ou des périphériques, s'ils incluent les logiciels appropriés.

Les rootkits ne sont pas nécessairement malveillants. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, modifier des fichiers et des logs et passer inaperçus.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Secteur de boot

Secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, du cluster, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge le système d'exploitation.

Signature du malware

Les signatures de malwares sont des fragments de codes extraits à partir de malwares réels. Elles sont utilisées par les programmes antivirus pour rechercher certaines caractéristiques et détecter les malwares. Les signatures sont également utilisées pour supprimer le code malveillant des fichiers infectés.

La base de données de signatures de malwares de Bitdefender rassemble des signatures de malwares mises à jour toutes les heures par les chercheurs de malwares de Bitdefender.

Spam

Messages électroniques ou messages de groupes de discussion indésirables. Souvent répertoriés comme des emails non sollicités.

Spyware

Tout type de logiciel récupérant les informations des utilisateurs via leur connexion Internet à leur insu, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels sharewares ou freewares pouvant être téléchargés sur Internet. Notons toutefois que la plupart des applications sharewares ou freewares ne comportent pas de spywares. Une fois installé, le spyware surveille l'activité de l'utilisateur sur Internet et transmet discrètement ces informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même, les numéros de cartes bancaires.

Leur point commun avec les chevaux de Troie est le fait que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une des manières les plus classiques d'être victime de spywares est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les spywares volent les ressources de l'ordinateur de l'utilisateur en utilisant sa bande passante lors de l'envoi d'informations à leur base via la connexion Internet. En raison de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.

TCP/IP

Transmission Control Protocol/Internet Protocol - Ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés d'ordinateurs avec diverses architectures matérielles et divers systèmes d'exploitation.

TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Télécharger

Copie des données (généralement un fichier entier) d'une source principale vers un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

Trojan (Cheval de Troie)

Programme destructeur qui prétend être une application normale. Contrairement aux virus, les chevaux de Troie ne se répliquent pas, mais ils peuvent être tout aussi destructeurs. Un des types de chevaux de Troie les plus insidieux est un logiciel qui prétend désinfecter votre PC mais qui au lieu de cela l'infecte.

Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Troyens, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Ver

Programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure de sa propagation. Il ne peut pas se joindre à d'autres programmes.

Virus

Programme ou morceau de code chargé dans votre ordinateur à votre insu et qui fonctionne contre votre gré. La plupart des virus peuvent également se répliquer. Tous les virus informatiques sont créés par des personnes. Un virus simple peut se copier très rapidement et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est par exemple capable de se transmettre via un réseau et de déjouer les systèmes de sécurité.

Virus de boot

Virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.

Virus Macro

Type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent de puissants langages macro.

Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

Virus polymorphique

Virus qui change de forme avec chaque fichier qu'il infecte. Ces virus n'ayant pas de forme unique bien définie, ils sont plus difficiles à identifier.

Zone de notification

Introduite avec Windows 95, la zone de notification se situe dans la barre de tâches Windows (en général, à côté de l'horloge) et contient des icônes miniatures permettant d'accéder facilement aux fonctions système : fax, imprimante, modem, volume, etc. Double-cliquez ou faites un clic-droit sur une icône pour afficher les options.