

Bitdefender® ENTERPRISE

CLOUD SECURITY FOR ENDPOINTS

Guide de démarrage rapide



Cloud Security for Endpoints by Bitdefender

Guide de démarrage rapide

Date de publication 2013.07.31

Copyright© 2013 Bitdefender

Notice Légale

Tous droits réservés. Aucune partie de ce manuel ne peut être reproduite ou transmise, sous aucune forme et d'aucune façon, électronique ou physique, y compris photocopies, enregistrement, ou par quelque moyen de sauvegarde ou de restauration que ce soit, sans une autorisation écrite d'un représentant officiel de Bitdefender. L'inclusion de courtes citations dans des tests n'est possible qu'avec la mention de la source. Le contenu ne peut en aucun cas être modifié.

Avertissement. Ce produit et sa documentation sont protégés par copyright. Les informations de ce document sont données « à titre indicatif », sans garantie. Bien que toutes les précautions aient été prises lors de l'élaboration de ce document, ses auteurs ne sauraient être tenus pour responsables envers toute personne ou entité des pertes ou dommages directs ou indirects consécutifs à l'utilisation des informations qu'il contient.

Ce manuel contient des liens vers des sites Web de tiers qui ne sont pas sous le contrôle de Bitdefender, et Bitdefender n'est pas responsable du contenu de ces sites. Si vous accédez à l'un des sites web d'une tierce partie fourni dans ce document, vous le ferez à vos propres risques. Bitdefender indique ces liens uniquement à titre informatif, et l'inclusion d'un lien n'implique pas que Bitdefender assume ou accepte la responsabilité du contenu de ce site Web d'un tiers.

Marques commerciales. Des noms de marques peuvent apparaître dans ce manuel. Toutes les marques, enregistrées ou non, citées dans ce document, sont la propriété exclusive de leurs propriétaires respectifs.



Table des matières

Utilisation de ce guide	v
1. À propos de Cloud Security for Endpoints	1
1.1. Architecture	2
1.2. Comptes utilisateur	2
1.3. Protection contre les menaces	4
1.3.1. Antimalware	4
1.3.2. Antiphishing	6
1.3.3. Pare-feu et Détection des intrusions	7
1.3.4. Données	7
1.3.5. Contrôle de contenu	8
1.4. Workflow	8
1.4.1. Déploiement	8
1.4.2. Gestion des postes de travail	9
1.4.3. Politiques de sécurité	9
1.4.4. Tâches d'analyse	9
1.4.5. Rapport	9
2. Pour démarrer	10
2.1. Connexion à la Cloud Security Console	10
2.2. Cloud Security Console Présentation	10
2.3. Gérer votre compte	11
2.4. Modifier le mot de passe par défaut	13
3. Abonnement au service	14
3.1. Activer une licence	14
3.2. Renouvellement de licence	15
3.3. Augmenter le nombre de postes de travail avec une licence	15
3.4. Vérification de l'état de votre abonnement	15
4. Installation et configuration	16
4.1. Étape 1 - Préparation à l'installation	16
4.2. Étape 2 - Installer le service sur les ordinateurs	17
4.3. Étape 3 - Organiser les ordinateurs (Facultatif)	20
4.4. Étape 4 - Créer et configurer une politique de sécurité	21
5. Surveillance de l'état de sécurité	23
6. Analyse des ordinateurs administrés	25
7. Obtenir de l'aide	26
A. Configuration requise	27
A.1. Configuration requise	27
A.2. Configuration requise par la découverte du réseau	28

Utilisation de ce guide

Le guide de démarrage rapide est conçu pour les administrateurs informatiques qui souhaitent utiliser le service Cloud Security for Endpoints pour protéger et contrôler les ordinateurs de l'entreprise (postes de travail, ordinateurs portables et serveurs). Il leur fournit les éléments nécessaires pour commencer à utiliser le service, le configurer et l'administrer.

Ce guide est conçu pour aider les nouveaux utilisateurs à rendre Cloud Security for Endpoints rapidement opérationnel sur les ordinateurs de l'entreprise.

Les informations présentées ici devraient être faciles à comprendre pour toute personne capable de travailler sous Windows.

Nous vous souhaitons un apprentissage agréable et utile.

Comment utiliser ce guide

Ce guide est organisé afin de trouver facilement les informations dont vous avez besoin.

[« À propos de Cloud Security for Endpoints » \(p. 1\)](#)

Découvrir Cloud Security for Endpoints.

[« Pour démarrer » \(p. 10\)](#)

Commencer à utiliser Cloud Security Console (la console d'administration du service).

[« Abonnement au service » \(p. 14\)](#)

Ce que vous devez savoir sur l'abonnement au service.

[« Installation et configuration » \(p. 16\)](#)

Étapes à suivre pour rendre le service fonctionnel sur les ordinateurs.

[« Surveillance de l'état de sécurité » \(p. 23\)](#)

Découvrez comment surveiller l'état de sécurité du réseau.

[« Analyse des ordinateurs administrés » \(p. 25\)](#)

Découvrez comment analyser les ordinateurs administrés à la recherche de virus et d'autres malwares.

[« Obtenir de l'aide » \(p. 26\)](#)

Sachez où regarder et à qui demander de l'aide si quelque chose d'inattendu apparaît.

[« Configuration requise » \(p. 27\)](#)

Pré-requis pour l'utilisation du service.

Documentation supplémentaire

Voici une liste de la documentation supplémentaire pour Cloud Security for Endpoints :

Aide

Documentation complète disponible dans Cloud Security Console (cliquez sur le lien **Aide et Support** dans l'angle supérieur droit).

Guide de l'administrateur

Documentation complète au format PDF pour les administrateurs de services.

Guide du rapporteur

Documentation complète au format PDF pour les utilisateurs de Cloud Security Console avec rôle Rapporteur.

Guide utilisateur de Endpoint Security

Documentation complète au format PDF pour les utilisateurs finaux sur les ordinateurs protégés.

Toute la documentation PDF est disponible dans le [Centre de Support Bitdefender en ligne](#). Le Centre de Support vous fournit également des articles utiles de la Base de connaissances.

Conventions utilisées dans ce guide

Plusieurs styles de texte sont utilisés dans ce guide pour une meilleure lisibilité. Leur aspect et signification sont présentés dans le tableau ci-dessous.

Apparence	Description
https://cloud.bitdefender.net	Les liens URL pointent vers un emplacement externe comme un serveur http ou ftp.
« Utilisation de ce guide » (p. v)	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
option	Toutes les options de l'interface utilisateur sont imprimées à l'aide de caractères gras .
mot clé	Les mots-clés et les expressions importantes sont mises en évidence à l'aide de caractères gras .
exemple de syntaxe	Les exemples de syntaxe sont imprimés avec des caractères séparés d'un espace.

Les avertissements sont des notes textes graphiquement marquées, offrant à votre attention des informations additionnelles relatives au paragraphe actuel.



Note

La note consiste simplement en une courte observation. Bien que vous puissiez les ignorer, les notes apportent des informations non négligeables, comme des fonctions spécifiques ou un lien vers un thème proche.

**Important**

Cette icône requiert votre attention et il n'est pas recommandé de la passer. Elle fournit généralement des informations non essentielles mais importantes.

**Avertissement**

Marque une information critique que vous devrez lire attentivement. Rien de négatif ne se passera si vous suivez les indications. A lire très attentivement car décrit une opération potentiellement très risquée.

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 :

- « [Architecture](#) » (p. 2)
- « [Comptes utilisateur](#) » (p. 2)
- « [Protection contre les menaces](#) » (p. 4)
- « [Workflow](#) » (p. 8)

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 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 Contrôle 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 peuvent 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. L'accès à la Cloud Security Console se fait via les comptes utilisateur.

Suite à votre inscription pour une version d'essai ou à votre achat du service, vous recevrez un e-mail du Service Inscription de Bitdefender. L'e-mail contient vos informations de connexion.

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. 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. 14).
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.

2.4. 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.

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. Installation et configuration

Une fois que vous avez reçu vos informations d'identification, vous pouvez vous connecter à Cloud Security Console et commencer à installer le service sur les ordinateurs.

L'installation et la configuration sont assez simples. Voici les étapes principales :

1. [Préparation de l'installation.](#)
2. [Installer le service sur les ordinateurs.](#)
3. [Organiser les ordinateurs en groupes \(facultatif\).](#)
4. [Créer et configurer une politique de sécurité.](#)

4.1. Étape 1 - Préparation à l'installation

Avant l'installation, suivez ces étapes préparatoires pour vous assurer de son bon déroulement :

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.
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 et un accès à Internet. Vérifiez que ces conditions sont remplies.

4.2. Étape 2 - Installer le service sur les ordinateurs

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.** Utilisez le lien d'installation de votre compte Cloud Security Console pour télécharger et installer Endpoint Security localement sur des ordinateurs individuels. 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. L'installation locale est guidée par un assistant.
- **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.

Endpoint Security dispose d'une interface utilisateur minimale. Elle permet uniquement aux utilisateurs de consulter l'état de la protection et d'exécuter des tâches de sécurité de base (mises à jour et analyses) sans fournir d'accès aux paramètres.

La langue d'affichage de l'interface utilisateur sur les ordinateurs protégés est définie au moment de l'installation en fonction de la langue de votre compte. Pour installer l'interface utilisateur dans une autre langue sur certains ordinateurs, vous devez momentanément [modifier la langue de votre compte](#) et ensuite seulement procéder à l'installation (en utilisant le nouveau lien d'installation ou l'installation à distance).

Installation locale

L'installation locale requiert d'exécuter un fichier d'installation, que vous pouvez télécharger à partir de Cloud Security Console, sur chaque ordinateur à protéger. 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 une installation locale :

1. Connectez vous à la Cloud Security Console en utilisant votre compte.
2. Allez sur la page **Ordinateurs > Zone d'installation**.
3. Vous pouvez configurer les options d'installation par défaut en cliquant sur **Personnaliser le package**.
 - 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 **Désinstaller la protection par mot de passe** 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`



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.

4. 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. Pour afficher le lien, cliquez sur le bouton **Lien d'installation** et sélectionnez **Afficher**.

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. 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.

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 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. Pour que la découverte du réseau fonctionne, certaines conditions doivent être remplies. Pour en savoir plus, reportez-vous à « [Configuration requise par la découverte du réseau](#) » (p. 28).



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 une installation à distance :

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 sur lesquels vous souhaitez installer la protection.
4. Cliquez sur **Tâches** et sélectionnez **Installer** dans le menu. La fenêtre Options d'installation s'affichera.
5. Vous pouvez modifier les options d'installation par défaut selon vos besoins.
6. 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.

- 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`).

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

4.3. Étape 3 - Organiser les ordinateurs (Facultatif)

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.

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

Pour organiser votre réseau en groupes :

- Allez sur la page **Ordinateurs > Afficher les ordinateurs**.
- 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.
- Renommer le groupe créé.
- Suivez les étapes précédentes pour créer des groupes supplémentaires.
- Déplacez les ordinateurs du groupe racine vers le groupe approprié.
 - Cochez les cases correspondant aux ordinateurs que vous souhaitez déplacer.

- b. Glissez-déposez votre sélection dans le groupe souhaité du panneau de gauche.

4.4. Étape 4 - Créer et configurer une politique 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. 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 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.

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.
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. 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. Les paramètres de sécurité par défaut sont recommandés dans la plupart des situations. Quelques fonctionnalités que vous pouvez souhaiter configurer :

- **Protection par mot de passe** . Pour empêcher que les utilisateurs avec des droits d'administration ne désinstallent la protection, vous devez définir un mot de passe. Allez dans **Général > Avancé** et définissez le mot de passe souhaité.
 - **Préférences de mise à jour**. Endpoint Security recherche, télécharge et installe automatiquement des mises à jour toutes les heures (configuration par défaut). Pour modifier la fréquence de mise à jour et d'autres paramètres, allez dans **Général > Mise à jour**. Si votre entreprise se connecte à Internet via un serveur proxy, vous devez spécifier les paramètres du proxy. 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.
 - **Tâches d'analyse planifiées**. Vous pouvez créer et configurer des tâches d'analyse planifiées afin qu'elles s'exécutent régulièrement sur les ordinateurs. Pour créer et configurer une nouvelle tâche d'analyse, allez dans **Antimalware > À la demande** et cliquez sur **Ajouter une tâche**.
 - **Permissions et règles de pare-feu**. Vous pouvez aller dans **Pare-feu > Avancé** pour consulter et configurer les permissions de pare-feu et créer des règles de pare-feu pour les applications ayant besoin d'un accès aux services réseau et Internet.
 - **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. Voici ce que vous pouvez faire :
 - Configurer l'analyse du trafic
 - Autoriser ou bloquer l'accès à Internet pour les utilisateurs ou applications à différents moments
 - Utiliser le Filtrage par catégories web filtre pour autoriser ou bloquer l'accès à des catégories entières de sites web
 - Créer des règles de protection des données pour toutes les données sensibles que vous souhaitez protéger
 - Configurer le Contrôle des applications pour bloquer complètement ou limiter l'accès des utilisateurs aux applications sur leurs ordinateurs
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**.

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.

5. Surveillance de l'état de sécurité

L'outil de surveillance principal de Cloud Security for Endpoints est le tableau de bord de Cloud Security Console. Consultez régulièrement la page **Tableau de bord** pour voir des informations en temps réel sur l'état de sécurité du réseau.

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.

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.
- 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.

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.

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.

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.

6. 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**. Si vous ne l'avez pas déjà fait, vous serez invité à sélectionner la société cliente que vous souhaitez gérer.
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**.

7. Obtenir de l'aide

Pour trouver des ressources d'aide supplémentaires ou pour obtenir de l'aide de Bitdefender :

- Cliquez sur le lien **Aide et Support**, dans l'angle supérieur droit de Cloud Security Console.
- Consultez notre [Centre d'assistance en ligne](#).

Pour contacter le support technique, merci d'utiliser ce [formulaire en ligne](#).

A. Configuration requise

A.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 Entreprise (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

A.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.