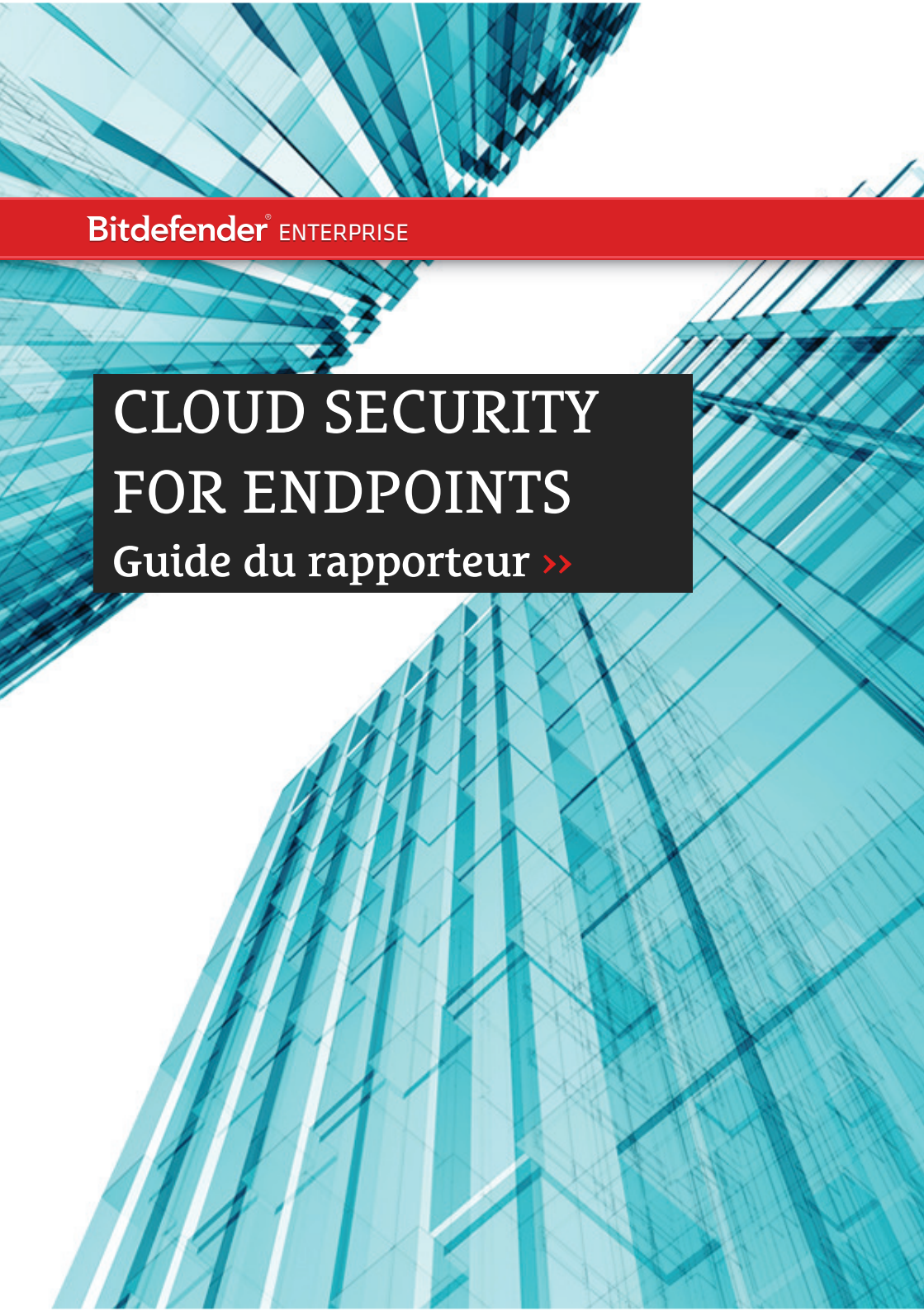

Bitdefender ENTERPRISE
CLOUD SECURITY
FOR ENDPOINTS
Guide du rapporteur ››

Cloud Security for Endpoints by Bitdefender
Guide du rapporteur

Date de publication 2013.07.31


Bitdefender

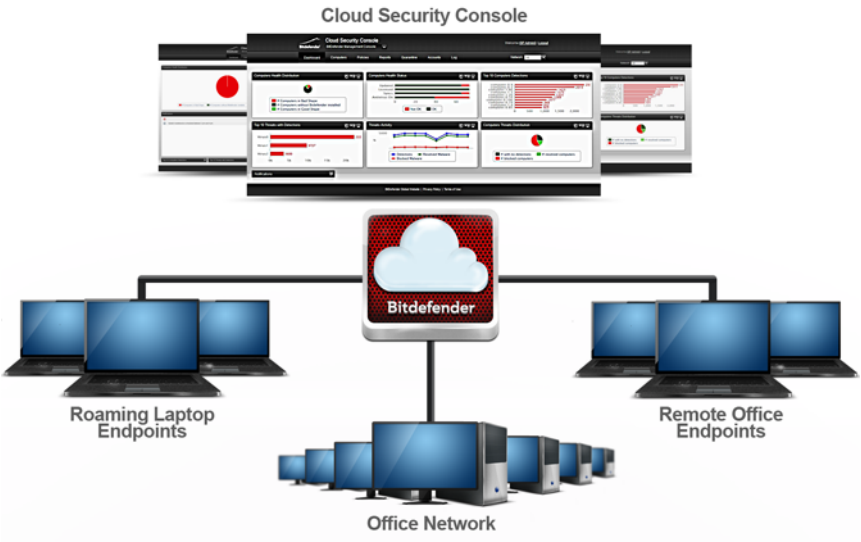
Table des matières

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 tant qu'utilisateur d'un compte rapporteur, vous pouvez uniquement surveiller la protection Cloud Security for Endpoints et créer et consulter des rapports de sécurité.

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.

Rapport
Obtenir des rapports de sécurité sur les ordinateurs administrés.

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 **Tableau de bord** pour voir des informations en temps réel sur la protection Cloud Security for Endpoints.
2. 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.

2.4. Modifier le mot de passe par défaut

Nous vous recommandons de modifier le mot de passe de connexion par défaut. Nous vous recommandons également de changer régulièrement votre mot de passe de connexion.

Pour changer le mot de passe de connexion :

1. Cliquez sur votre nom d'utilisateur dans l'angle supérieur droit de la console.
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. Cliquez sur votre nom d'utilisateur dans l'angle supérieur droit de la console.
2. Sous **Détails du compte**, corrigez ou actualisez les détails de votre compte.
   - **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.
   - **Rôles et Groupe.** Ces champs correspondent à votre type de compte et au groupe d'ordinateurs dont vous êtes en charge.
   - **Mot de passe.** Pour changer votre mot de passe, saisissez-en un nouveau dans les champs correspondants.
3. 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.
4. Cliquez sur **Soumettre** pour enregistrer les modifications.

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. 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.

3.1. 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.
- 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.

3.2. 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.

4. 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.

4.1. 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.

- 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.

4.2. 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. 17).
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.

4.3. 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.

4.3.1. 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.

4.3.2. 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.

4.3.3. 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.

4.3.4. 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.

4.3.5. 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**.

4.3.6. 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**.

4.3.7. 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.

4.4. 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.

4.4.1. 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**.

4.4.2. 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.

4.4.3. 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.

4.4.4. 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.

5. 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.

6. Obtenir de l'aide

Pour tout problème ou toute question concernant la Cloud Security Console, contactez un administrateur.

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.