Symantec™ Email Security.cloud

Description de service

Mars 2019

Cette Description de service décrit Symantec Email Security.cloud (le « Service »). Tous les termes en majuscules de cette description ont la signification indiquée dans le Contrat (défini ci-dessous) ou dans la section Définitions.

Cette Description de service, ainsi que toute pièce jointe incluse par référence, fait partie et est intégrée dans le contrat passé avec Symantec pourvu d'une signature manuelle ou électronique qui régit l'utilisation du Service ou, en l'absence d'un tel contrat signé, les Conditions générales de Symantec Online Services (ci-après désignées sous le terme « Contrat »).

Sommaire

1 : Fonctionnalités techniques et opérationnelles

Présentation du Service

Symantec™ Email Security.cloud est un Service hébergé qui filtre les Messages électroniques et protège les entreprises contre les Malwares (notamment les attaques ciblées et le phishing), les Spams et l'envoi massif de Messages électroniques indésirables. Le Service propose des options de chiffrement et de Protection des données pour contrôler les informations sensibles envoyées par Message électronique. Le Service prend en charge plusieurs types de boîte aux lettres provenant de différents fournisseurs.

Caractéristiques du Service

- Les Administrateurs Client peuvent accéder à la console de gestion du Service à l'aide d'une connexion protégée par mot de passe. La console de gestion permet au Client de configurer et de gérer le Service, d'accéder aux rapports, d'afficher les données et les statistiques lorsqu'ils sont disponibles dans le cadre du Service.
- Le Service est opérationnel 24 h/24, 7 j/7 et fait l'objet d'une surveillance au niveau de la disponibilité matérielle, de la capacité de service et de l'utilisation des ressources réseau. La conformité du Service aux niveaux de service prévus fait l'objet d'une surveillance régulière et, le cas échéant, des ajustements sont effectués.
- Des rapports sur le Service sont disponibles dans la console de gestion. Les rapports peuvent comprendre des journaux d'activité et/ou des statistiques. Dans la console de gestion, le Client peut décider de générer des rapports, qui peuvent être configurés pour être envoyés par Courrier électronique à intervalles réguliers ou téléchargés à partir de la console d'administration.
- Le Service a pour but de permettre au Client de mettre en œuvre une politique d'utilisation des PC valable et applicable, ou son équivalent.
- Les listes de mots suggérés et les règles de modèles ou politiques fournies par Symantec contiennent des mots pouvant être considérés comme offensants.
- En cas de suspension ou de résiliation du Service pour quelque motif que ce soit, Symantec annulera tous les changements de configuration effectués lors du provisionnement du Service. Il incombe également au Client de procéder à tous les autres changements de configuration nécessaires une fois le Service rétabli.

Fonctionnalités et options du Service

Le Service propose deux (2) options : Email Protect ou Email Safeguard. Chaque Utilisateur de l'option sélectionnée ou du module additionnel doit avoir acheté le Service (sous réserve des restrictions mentionnées dans la présente Description de service).

Fonctionnalités par Option de service

	Email Protect	Email Safeguard
Email Antimalware : protection contre les Malwares incluant une protection contre le Phishing et les Attaques ciblées	✓	✓
Email Antispam : protection contre les Spams et le Phishing (avec un suivi de lien en temps réel) et contre l'Envoi massif de messages électroniques	✓	✓
Email Data Protection : contrôles des données à l'aide de Politiques de filtrage de contenu personnalisables		✓

Email Image Control : détection d'images choquantes		✓
Filtrage sortant	✓	✓
Chiffrement TLS activé		✓
Chiffrement TLS opportuniste	✓	✓
Enregistrement d'adresse : gestion des destinataires non valides	✓	✓
Outil de synchronisation LDAP des utilisateurs et des groupes	✓	✓
Suivi des messages	✓	✓
Tableau de bord de reporting	✓	✓
Rapports synthétiques (PDF) et détaillés (CSV)	✓	✓
Notifications et portail de mise en quarantaine du spam des utilisateurs	✓	✓
Gestion des exclusions de responsabilité	✓	✓
Policy Based Encryption Essentials		✓
Email Impersonation Controls		✓

Des informations complémentaires sur chaque fonctionnalité du Service sont disponibles dans l'Aide en ligne, à l'adresse suivante : http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=FR_FR.

Modules complémentaires du Service

	Email Protect	Email Safeguard
Advanced Threat Protection : Email	Disponible	Disponible
Policy Based Encryption Advanced	_	Disponible
Email Fraud Protection	Disponible	Disponible
Email Threat Isolation	Disponible	Disponible

Des informations complémentaires sur chaque module additionnel du Service sont disponibles dans l'Aide en ligne, à l'adresse suivante : http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=FR_FR. La Description de service d'Email Fraud Protection est disponible à l'adresse suivante : https://www.symantec.com/about/legal/repository.

Advanced Threat Protection : Email détecte grâce à la sandbox Symantec Cynic™ les menaces avancées envoyées par Courrier électronique, il identifie les attaques ciblées par Courrier électronique qui sont dirigées contre l'entreprise ou l'utilisateur destinataire et repère, grâce à Symantec Click-time™ URL Protection, les URL qui deviennent malveillantes une fois le Message électronique distribué. Il peut supprimer les messages électroniques que notre sandbox Cynic™ considère comme malveillants après la distribution pour les clients Office 365. De plus, il peut aider les clients à remédier aux attaques de message électronique en mettant sur liste noire les messages électroniques en fonction d'indicateurs de compromission (IOC). Il fournit des rapports détaillés sur les malwares, notamment des informations sur les URL, la catégorie de malware, la méthode de détection et les hachages de fichier. Une API de flux de données est incluse pour permettre la génération de rapports sur les malwares via une URL authentifiée, sans avoir à importer de fichier ou à envoyer des données par message électronique. Advanced Threat Protection : Email donne également accès au service Phishing Readiness, un simulateur d'attaque de phishing utilisé pour le risque d'exposition du personnel à ces attaques. L'utilisation du service Phishing Readiness est régie par les conditions générales disponibles à l'adresse (https://www.symantec.com/about/legal/repository).

Le service Policy Based Encryption Advanced offre : (i) un portail de récupération web en mode pull ; (ii) un support de distribution PGP et S/MIME ; (iii) la possibilité d'essayer d'appliquer un chiffrement TLS avant de revenir à des technologies de chiffrement moins transparentes ; et (iv) une distribution de type push chiffrée au format PDF (la seule méthode de chiffrement fournie dans le cadre de la fonctionnalité Policy Based Encryption Essentials du programme Email Safeguard). Policy Based Encryption Advanced est octroyé sous licence par Utilisateur expéditeur ; cela peut correspondre à un sous-ensemble du nombre total d'Utilisateurs de l'option Email Safeguard. Si un Client souhaite utiliser l'option Policy Based Encryption Advanced pour l'envoi sécurisé de messages, Symantec peut l'autoriser à acheter des licences Utilisateur supplémentaires en fonction du nombre de messages à envoyer, selon une formule définie par Symantec.

Symantec™ Email Fraud Protection est un service cloud qui automatise l'application de DMARC (Domain-based Message Authentication, Reporting, and Conformance). Symantec Email Fraud Protection simplifie toutes les étapes de l'application de DMARC par rapport à la méthode manuelle. L'application réduit le risque d'attaques entrantes d'usurpation d'identité, car tous les messages électroniques provenant de sources non authentifiées sont mis en quarantaine ou rejetés. Une fois l'application effectuée, les destinataires des messages électroniques ou les agents de transfert de messagerie savent qu'ils peuvent faire confiance au domaine du client, ce qui permet d'augmenter les taux de délivrabilité des messages électroniques.

Symantec™ Email Threat Isolation renforce la protection contre le spear phishing, le vol d'informations d'authentification et les attaques par message électronique avancées en isolant les liens malveillants et en sécurisant les pages web dangereuses. Grâce à Email Threat Isolation, Symantec peut fournir la meilleure protection contre les menaces de messagerie sophistiquées qui exploitent les liens malveillants, telles que les attaques de spear phishing avancées ou les attaques par vol d'informations d'authentification.

Email Threat Isolation crée un environnement d'exécution sécurisé entre les utilisateurs et leurs liens ou pièces jointes de message électronique en exécutant des sessions web à distance et en envoyant uniquement des informations de rendu sécurisées aux navigateurs des utilisateurs. . En conséquence, Symantec aide à empêcher les menaces contenant des pièces jointes ou liens malveillants d'atteindre les utilisateurs. Email Threat Isolation bloque également les attaques de phishing et de vol d'identifiants en affichant les sites web de phishing en lecture seule, empêchant ainsi les utilisateurs de saisir des informations d'authentification d'entreprise ou d'autres informations sensibles.

Contrat de niveau de service

- Symantec fournit un contrat de niveau de service (« SLA ») applicable au Service, comme indiqué dans l'Annexe A.

Plates-formes prises en charge et exigences techniques

- Les plates-formes prises en charge et exigences techniques relatives au Service sont explicitées à l'adresse suivante : http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=FR_FR.

Composants logiciels du Service hébergé

- Le Service inclut les Composants logiciels du Service disponibles dans la console de gestion, qui elle-même est accessible après paiement des frais applicables.

2 : Responsabilités du Client

Symantec ne peut exécuter le Service que si le Client fournit les informations nécessaires ou prend les mesures requises. Dans le cas contraire, la fourniture du Service par Symantec peut être retardée, perturbée ou entravée et/ou l'éligibilité du Contrat de niveau de service peut être jugée nulle, comme décrit ci-après.

- Mise en œuvre : Le Client doit fournir les informations requises pour que Symantec puisse mettre en œuvre le Service.
- Personnel client compétent : Le Client doit mettre à disposition des personnes compétentes afin d'aider Symantec à fournir le Service, à la demande raisonnable de Symantec.
- Le Client est responsable des informations, mots de passe et autres informations de connexion de son compte.
- Le Client accepte d'utiliser des moyens raisonnables pour protéger ses informations d'authentification et informera immédiatement Symantec de toute utilisation non autorisée connue du compte Client.
- Codes de renouvellement : Le cas échéant, le Client doit appliquer les informations d'authentification de renouvellement fournies dans la Confirmation de commande ou le Document d'abonnement correspondant accessible sur son compte d'administration, pour continuer à bénéficier du Service ou pour conserver les informations du compte et les données Client qui sont disponibles pendant toute la Durée du Service.
- Configurations du Client ou paramètres par défaut : Le Client doit configurer les fonctionnalités du Service via la console de gestion, le cas échéant, sinon les paramètres par défaut sont utilisés. Dans certains cas, il n'existe pas de paramètres par défaut et le Service ne peut donc pas être fourni au Client tant qu'il n'a pas défini de paramètres. La configuration et l'utilisation du Service sont sous le contrôle total du client. Par conséquent, Symantec n'est en aucun cas responsable de l'utilisation du Service par le client, même si la responsabilité civile ou pénale du client est engagée suite à l'exploitation du Service.

Politique d'utilisation acceptable

- Le Client est tenu de se conformer à la Politique d'utilisation acceptable de Symantec Online Services.

3 : Informations liées aux droits et abonnements

Statistiques de charge

Le Service est disponible sous le Compteur suivant, tel que spécifié dans la Confirmation de commande :

- « **Utilisateur** » désigne un individu et/ou un périphérique autorisé à utiliser et/ou à profiter de l'utilisation du Service, ou qui utilise en fait une partie du Service.

Modification d'abonnement

Si un Client a reçu un Abonnement ou des Droits Client directement de la part de Symantec, les demandes concernant les modifications autorisées de l'Abonnement ou des Droits Client doivent être envoyées à l'adresse suivante (ou à l'adresse de remplacement publiée par Symantec) : CLD_cancellations_MLABS@symantec.com, sauf indication contraire spécifiée dans le contrat du Client conclu avec Symantec. Tout préavis transmis conformément à cette procédure est considéré comme donné à la date de réception. Si le Client reçoit un Abonnement ou un Droit acquis par le biais d'un revendeur Symantec, veuillez contacter le revendeur du Client.

4 : Assistance et Support technique

Remarque : Cette section ne s'applique que si le Client est autorisé à recevoir une Assistance client et un Support direct de la part de Symantec (« Support »). Si un Client est en droit de recevoir une Assistance et un Support de la part d'un revendeur Symantec, reportez-vous au contrat Client passé avec ce revendeur pour connaître les détails concernant ce Support ; le Support décrit dans l'annexe A ne s'appliquera pas au Client.

Assistance client

Dans le cadre du Service, Symantec assure les prestations d'assistance suivantes pendant les heures ouvrées des différentes régions :

- Réception et traitement des commandes pour l'installation du Service
- Réception et traitement des demandes de modification des fonctions du Service

- Réponses aux questions sur la facturation

Support technique

Le Support de base est inclus dans le cadre du Service, comme indiqué ci-dessous.

- Le Support est disponible vingt-quatre (24) heures sur vingt-quatre et sept (7) jours sur sept afin d'aider le Client à configurer les fonctions du Service et à résoudre les problèmes signalés concernant le Service. Le Support des Services sera dispensé conformément aux conditions générales et aux politiques de support technique publiées à l'adresse https://support.symantec.com/en_US/article.TECH236428.html.
- Une fois qu'un niveau de gravité est assigné à un envoi Client pour le Support, Symantec fera tous les efforts raisonnables pour répondre aux objectifs d'intervention définis dans le tableau ci-dessous. Les pannes imputables à des actions du Client ou nécessitant l'intervention d'autres fournisseurs de services échappent au contrôle de Symantec et sont donc expressément exclues de ce Support.

Gravité du problème	Objectifs d'intervention du Support (24 h/24, 7 j/7)*
Gravité 1 : Un problème pour lequel aucune solution de contournement n'est disponible immédiatement s'est produit dans l'une des situations suivantes : (i) le serveur de production du Client ou un autre système stratégique est en panne ou a subi une perte substantielle de service, ou (ii) une partie considérable des données stratégiques du Client est exposée à un risque de perte ou de corruption élevé.	Dans un délai de 30 minutes
Gravité 2 : Un problème entraînant une altération grave d'une fonctionnalité essentielle est survenu. L'activité du Client peut se poursuivre de manière restreinte, mais la productivité à long terme risque d'être affectée de manière négative.	Dans un délai de deux heures
Gravité 3 : Un problème ayant un impact négatif limité sur les activités du Client est survenu.	Au plus tard à la même heure le jour ouvré suivant**
Gravité 4 : Un problème qui n'a pas eu d'impact négatif sur les activités du Client est survenu.	Le jour ouvré suivant ; Symantec recommande par ailleurs que le Client soumette ses suggestions de nouvelles fonctionnalités ou d'améliorations sur les forums de Symantec.

Les Objectifs d'intervention de Support détaillés ci-dessus sont réalisables pendant les opérations de service normales et ne s'appliquent pas pendant la Maintenance du Service et/ou de l'infrastructure associée, comme décrit dans la section Maintenance ci-dessous.

** La durée des Objectifs d'intervention correspond au temps nécessaire pour répondre à la demande, et non à la durée de résolution (le temps nécessaire pour fermer la demande).*

*** Un « jour ouvré » désigne les heures ouvrées standard dans la région et les jours de la semaine dans le fuseau horaire local du Client, à l'exclusion des week-ends et des jours fériés locaux. Dans la plupart des cas, les « heures ouvrées » sont comprises entre 9 h et 17 h dans le fuseau horaire du Client.*

Maintenance du Service et/ou de l'Infrastructure de service associée

Symantec doit assurer la maintenance ponctuellement. Symantec déploiera tous les efforts commercialement raisonnables pour effectuer les tâches de Maintenance périodique durant les périodes de faible activité du Client, afin de minimiser les risques d'indisponibilité de la console. Le Client ne recevra aucune notification préalable pour ces activités de maintenance périodique. Pour tous les autres types de maintenance et comme indiqué ci-dessous, Symantec s'efforcera d'informer les parties affectées à l'avance en publiant une alerte sur la page Symantec Status (https://status.symantec.com/). Pour plus d'informations sur l'état du Service, la maintenance planifiée et les problèmes connus, rendez-vous sur la page Symantec Status et abonnez-vous à la page Symantec Email Security.cloud pour recevoir les dernières mises à jour. **Les principales fonctions**

du service, telles que l'analyse de sécurité et la distribution du courrier électronique, ne sont pas interrompues durant toutes les activités de maintenance.

- ***Maintenance planifiée :*** Maintenance planifiée désigne les périodes de maintenance planifiée pendant lesquelles le Service peut être perturbé ou interrompu en raison de l'indisponibilité de l'Infrastructure du Service. Symantec s'efforcera d'effectuer les tâches de Maintenance planifiée durant les périodes de faible activité du client, dans le fuseau horaire où est située l'infrastructure concernée et uniquement sur une partie du réseau. Durant la Maintenance planifiée, le Service pourra être renvoyé vers des sections de l'Infrastructure non soumises à maintenance ce qui peut éviter les perturbations du Service.Pour la Maintenance planifiée, Symantec met en œuvre tous les moyens commerciaux raisonnables pour envoyer un préavis de sept (7) jours civils au Client, publié sur la page Symantec Status. Les Clients peuvent également recevoir des notifications via SMS, message électronique ou Twitter en s'abonnant à la page Symantec Status.
- ***Maintenance non planifiée :*** Maintenance non planifiée désigne les périodes de maintenance prévues qui ne permettent pas d'envoyer la notification standard de sept (7) jours et pendant lesquelles le Service peut être perturbé ou interrompu en raison de l'indisponibilité de l'Infrastructure du Service. Symantec met en œuvre tous les moyens commerciaux raisonnables pour envoyer un préavis d'au moins un (1) jour civil au Client, publié sur la page Symantec Status.Durant la Maintenance non planifiée, le Service pourra être renvoyé vers des sections de l'Infrastructure non soumises à maintenance ce qui peut éviter les perturbations du Service.Symantec effectuera de temps en temps des Maintenances d'urgence. Une maintenance d'urgence est définie comme une maintenance qui *doit être mise en œuvre aussi rapidement que possible afin de résoudre ou d'empêcher un incident majeur*. Symantec s'efforcera d'informer les parties affectées à l'avance en publiant une alerte sur la page Symantec Status au moins une (1) heure avant le début de la maintenance.
- ***Maintenance de la console de gestion :*** Pour la Maintenance de la console de gestion, Symantec met en œuvre tous les moyens commerciaux raisonnables pour envoyer un préavis de quatorze (14) jours civils au Client, publié sur la page Symantec Status. Symantec s'efforcera d'effectuer les tâches de maintenance sur la console de gestion durant les périodes de faible activité du client, afin de minimiser les risques d'indisponibilité. À l'occasion, Symantec peut effectuer des mises à jour mineures dans la console de gestion et le Client ne recevra aucune notification préalable pour ces activités de maintenance périodique.

5 : Conditions supplémentaires

- Le Service est accessible et utilisable partout dans le monde et soumis aux limitations techniques et de la conformité à la réglementation sur les exportations stipulées par les normes Symantec alors en vigueur.
- Symantec se réserve le droit de modifier et de mettre à jour les fonctions et fonctionnalités du Service, dans le but de fournir un Service identique ou amélioré (tant que Symantec ne réduit pas considérablement la fonctionnalité principale du Service). Le Client reconnaît et accepte que Symantec se réserve le droit de mettre à jour cette Description de service à tout moment pendant la Durée de l'abonnement pour refléter avec précision le Service fourni. La Description de service mise à jour sera effective au moment de sa publication.
- L'utilisation d'un Composant de Service sous la forme d'un logiciel devra être régie par le contrat de licence accompagnant le logiciel. Si aucun CLUF n'accompagne le Composant de Service, ce dernier devra être régi par les conditions générales définies ici (http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf). Les éventuels autres droits et obligations portant sur l'utilisation dudit Composant de Service sont ceux énoncés dans la présente Description de service.
- Sauf indication contraire dans la Description de service, le Service (y compris tout composant logiciel de service hébergé fourni avec celui-ci) peut utiliser des logiciels libres ou d'autres ressources provenant de tiers et dont l'utilisation est soumise à une licence distincte.
- Symantec peut mettre le Service à jour à tout moment afin d'en maintenir l'efficacité.
- Les modèles fournis par Symantec servent uniquement à guider le Client lors de la création de politiques personnalisées et d'autres modèles.
- Les limitations suivantes s'appliquent au Service :
    - Messages entrants et sortants, par utilisateur et par mois civil : dix mille (10 000). Cette limite n'inclut pas le spam et les malwares dirigés vers le Client.
    - Symantec se réserve le droit de facturer un nombre d'utilisateurs supplémentaire au client, après notification, pour les mois restants sur le contrat de Service lorsque la limite d'utilisation est dépassée.
    - Planification de nouvelle tentative pour les messages électroniques entrants et sortants : sept (7) jours civils.
    - Taille maximale des messages par défaut = cinquante méga-octets (50 Mo). Le client peut spécifier une taille maximale de mille méga-octets (1 000 Mo). Tout Message électronique reçu par le Service qui dépasse la limite indiquée est bloqué et supprimé. Une alerte est envoyée par Courrier électronique à l'expéditeur, au destinataire prévu et à un Administrateur.

- Suivi des messages = des données sont disponibles pour des recherches de pannes pendant 30 jours ; des limites additionnelles s'appliquent au nombre de résultats renvoyés par une simple recherche.
- Mise en quarantaine des malwares = les Messages électroniques sont automatiquement supprimés au bout de trente (30) jours.
- Mise en quarantaine des Spams : les Messages électroniques sont automatiquement supprimés après quatorze (14) jours, sauf configuration contraire.
- Disponibilité des données de reporting des tableaux de bord = quarante (40) jours pour les informations détaillées, douze (12) mois pour les informations synthétiques.
- Disponibilité des données des rapports synthétiques (PDF) = douze (12) mois.
- Disponibilité des données (CSV) des rapports détaillés = quarante (40) jours.

- Les limitations suivantes s'appliquent à Policy Based Encryption :
  - Nombre de Messages sortants par Utilisateur et par mois pour Policy Based Encryption (Z) : trois cents (300).
  - Nombre de Messages sortants par Utilisateur et par mois pour Policy Based Encryption Essentials/Advanced : quatre cent quatre-vingts (480).
  - En cas d'envoi à plusieurs destinataires, chaque adresse sera comptabilisée comme un Message électronique sécurisé. Si le Client dépasse la limite autorisée de messages sécurisés pour un mois du calendrier, Symantec se réserve le droit de facturer l'utilisation réelle au Client.
  - La taille des Messages électroniques acheminés via Policy Based Encryption Service est limitée : pas plus de cinquante méga-octets (50 Mo).
  - Si vous utilisez le chiffrement Pull avec le service Policy Based Encryption (Z), par défaut, les Messages électroniques seront stockés pendant 90 jours sur le portail sécurisé avant d'expirer.
  - Si vous utilisez le chiffrement Pull avec le service Policy Based Encryption Advanced Service, par défaut, les Messages électroniques seront stockés pendant 30 jours sur le portail de récupération sécurisé avant d'expirer.
  - Les niveaux de service en matière de disponibilité et de latence ne s'appliquent pas à ce Service.

- Pour garantir que les messages sont sécurisés à tous les niveaux pendant la transmission, Symantec recommande que le Client configure des domaines qui seront utilisés pour le service Policy Based Encryption, de sorte que le chiffrement TLS soit appliqué à tous les messages entrants et sortants en provenance et à destination de l'Infrastructure du Service.
- Les Clients doivent acheminer leurs messages entrants via Symantec en utilisant les informations d'acheminement fournies par Symantec et doivent acheminer chaque message vers une Tour ou une adresse IP spécifique.
- Le Service n'est disponible que si le Client dispose de son propre nom de domaine de Messagerie et s'il a la possibilité de configurer les enregistrements MX et/ou les DNS pour ce nom de domaine.
- Le Client doit accepter les Messages électroniques entrants provenant de toutes les plages d'adresses IP requises. Cela permet d'assurer la continuité de service en cas d'indisponibilité d'une partie de l'Infrastructure.
- Le Client doit spécifier l'adresse IP ou le nom d'hôte de chaque serveur de messagerie utilisé pour la réception des Messages électroniques entrants dans leur entreprise.
- Le Client doit vérifier que tous les domaines (y compris les sous-domaines) qui nécessitent le Service sont couverts. Le Client accepte le fait que les fonctionnalités du Service ne fonctionneront pas correctement et que la distribution du Courrier électronique sera impossible pour les domaines non couverts. Le Client accepte de fournir et de tenir à jour une liste d'adresses électroniques valides pour bénéficier du Service (« Liste de validation »). Il lui incombe de vérifier ladite Liste de validation avant la mise à disposition du Service et pendant toute la durée du Contrat. Les Messages électroniques envoyés à des adresses électroniques qui ne sont pas dans la Liste de validation, ou qui ne sont pas correctement saisies, seront rejetés par le Service. Le Client accepte que les contrats de niveaux de services ne soient pas respectés pour les Messages électroniques envoyés à des adresses incorrectes. Pour éviter toute ambiguïté, les Clients qui utilisent le système Spam Quarantine doivent conserver une Liste de validation et avoir activé la fonction Enregistrement d'adresse. Si le Client n'est pas en mesure de fournir une telle Liste de validation et demande à désactiver la fonctionnalité d'enregistrement des adresses, Symantec étudiera chacune de ces demandes au cas par cas et se réserve le droit de décliner les demandes, à sa seule et unique discrétion.
- Le Client peut libérer des Messages électroniques considérés comme comportant un Malware ou un Spam, ou demander à Symantec de libérer ce type de Message dans le domaine du Client. LE CLIENT ACCEPTE QUE SYMANTEC DÉCLINE TOUTE RESPONSABILITÉ EN CAS D'ENVOI DESDITS MESSAGES ÉLECTRONIQUES À LA DEMANDE DU CLIENT.

- Symantec décline toute responsabilité en cas de perte ou de dommage causé directement ou indirectement par l'échec de l'identification d'un Spam par le Service ou par une mauvaise identification d'un Message électronique en tant que Malware ou Spam. Symantec se réserve le droit d'analyser tous les Messages électroniques sortants.
- Un message d'exclusion de responsabilité par défaut sera appliqué aux Messages électroniques analysés par le Service pendant la période de provisionnement du Service. Ce texte pourra être modifié par le Client par le biais de la console de gestion. Symantec se réserve le droit de modifier à tout moment le message d'exclusion de responsabilité par défaut.
- Le Client doit respecter toutes les lois en vigueur en ce qui concerne l'utilisation du Service. Certains pays peuvent exiger le consentement de chaque membre du personnel. La configuration et l'utilisation du ou des Services sont entièrement sous le contrôle du Client ; par conséquent, Symantec ne peut être tenue responsable de l'utilisation du ou des Services par le Client, ni de la responsabilité civile ou pénale qui peut être engagée par le Client suite à l'utilisation du Service.
- Si l'accès continu du Client au Service compromet la sécurité du Service, en raison notamment, mais sans s'y limiter, de tentatives de piratage, d'attaques de déni de service, d'envoi massif de messages électroniques ou de toute autre activité malveillante dirigée contre ou provenant des domaines du Client, ce dernier accepte que Symantec bloque provisoirement son accès au Service. Dans un tel cas de figure, Symantec informera rapidement le Client et travaillera avec lui à la résolution des problèmes. Symantec rétablira le Service une fois la menace levée.
- En cas de suspension du Service pour quelque motif que ce soit, le Service ne sera pas appliqué aux Messages électroniques du Client et les Messages ne seront pas acheminés vers l'Infrastructure de Symantec. Il est de la responsabilité du Client de rediriger ses Messages électroniques pendant la suspension du Service et de confirmer que toutes les configurations sont correctes lorsque le Service est réinstallé.
- En cas de résiliation du Service pour une raison quelconque, le compte du Client est supprimé et il n'a plus accès au Service.
- Le Client ne doit pas autoriser ses systèmes à : (i) agir en tant que Relais ouvert ou Proxy ouvert ; ou (ii) envoyer des Spams. Symantec se réserve le droit de vérifier à tout moment le respect de cette clause par le Client. Pour éviter toute ambiguïté, toute violation de la présente clause constitue une violation déterminante du Contrat. Symantec se réserve alors le droit de suspendre immédiatement tout ou partie du Service jusqu'à la disparition de l'infraction, ou de mettre fin au Contrat pour les dispositions du Service concernées.
- Si, à un moment quelconque, (i) les systèmes de Messagerie électronique du Client se retrouvent sur liste noire, ou (ii) les systèmes Symantec se retrouvent sur liste noire du fait de l'envoi de Spam par le Client, ou (iii) le Client ne respecte pas les obligations stipulées dans la présente Description de service, Symantec se réserve le droit, à sa seule discrétion, de refuser immédiatement l'accès au Service, de le suspendre ou d'y mettre fin en totalité ou en partie, et en informe le Client.
- Le Client a le droit d'utiliser le Service uniquement dans le cadre de ses propres activités. Le Client accepte de ne pas revendre, accorder de sous-licence, louer ou mettre à disposition de toute autre manière que ce soit le Service et la documentation associée à un tiers. Le Client accepte de ne pas utiliser le Service dans le but de développer un produit ou un service concurrent, de copier ses fonctionnalités ou son interface utilisateur, de réaliser des évaluations du Service, des tests de benchmarking ou tout autre type d'analyse comparative devant être publiée en dehors de l'entreprise du Client sans l'accord préalable écrit de Symantec.

6 : Définitions

« **Enregistrement d'adresse** » est une fonction obligatoire du Service qui rejette les Messages électroniques entrants envoyés aux Adresses électroniques qui ne sont pas incluses dans la liste d'Adresses électroniques valides du Client (la « Liste de validation »).

« **Administrateur** » désigne un utilisateur (côté client) autorisé à gérer le Service pour le compte du client. Les Administrateurs peuvent avoir la capacité de gérer le Service en totalité ou en partie selon les indications du client.

« Paramètres de pratique d'excellence AntiSpam » désigne les recommandations de configuration fournies par Symantec pour le Service, communiquées au Client durant le processus de provisionnement ou publiées dans l'aide en ligne.

"**Gestionnaire de connexion**" : correspond aux méthodes de détection utilisées lors de la phase de négociation SMTP.

« **Demande de crédit** » désigne la notification que le Client doit envoyer à Symantec par Courrier électronique à l'adresse support.cloud@symantec.com, avec l'objet « Demande de crédit » (sauf indication contraire de la part de Symantec).

« **Cluster de tours désignées** » désigne au moins deux (2) Tours désignées pour fournir Email Security Services au Client.

« **Paramètres de niveau de domaine** » désigne les paramètres personnalisables d'un domaine particulier au sein de la console de gestion pour Email Security Services.

« **Courrier électronique, Message électronique ou Messagerie électronique** » désigne tout message SMTP entrant ou sortant qui transite par le Service.

« **Email Security Services** » désigne les options Email Safeguard et Email Protect et tous les services additionnels disponibles.

« **Faux positif de Malware de Message électronique** » désigne un Message électronique identifié à tort comme contenant un Malware.

« **Contrat de licence utilisateur final (CLUF)** » fait référence aux conditions générales qui accompagnent le Logiciel (défini ci-dessous).

« **Paramètres globaux** » désigne les actions au sein de la console de gestion qui sont appliquées à tous les domaines et niveaux de groupe pour les Services.

« **Paramètres de niveau de groupe** » désigne les paramètres personnalisables d'un groupe particulier au sein de la console de gestion pour les fonctionnalités applicables du Service.

« **Infrastructure** » désigne la technologie et la propriété intellectuelle de Symantec ou du concédant de licence utilisées pour fournir les Services.

« **Malware connu** » désigne un Malware pour lequel, au moment de la réception du contenu par Symantec, une signature a déjà été rendue disponible depuis au moins une (1) heure pour les technologies antivirus déployées par Symantec.

« **Malware** » ou « **logiciel malveillant** » désigne tout logiciel visant à perturber le fonctionnement d'un ordinateur ou appareil mobile, ou à collecter des informations sensibles et/ou accéder à des systèmes privés sans autorisation appropriée.

« **Faux positif de Malware** » désigne un Message électronique identifié à tort comme contenant un Malware.

« **Membre** » désigne le Client et les tiers avec lesquels le Client établit un réseau chiffré au moyen du Service additionnel hérité Email Boundary Encryption.

« **Frais mensuels** » désigne les frais mensuels pour le ou les Services concernés, tels que définis dans le Contrat.

« **Aide en ligne** » désigne les informations supplémentaires disponibles à l'adresse http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=FR_FR.

« **Proxy ouvert** » désigne un serveur proxy configuré pour autoriser des tiers inconnus ou non autorisés à consulter, stocker ou transférer les pages web, DNS ou autre données pour le Service.

« **Relais ouvert** » désigne un serveur de Messagerie configuré de manière à recevoir les Messages électroniques envoyés par des tiers inconnus ou non autorisés, et à les transférer à un ou plusieurs destinataires qui ne sont pas des utilisateurs du système de Messagerie auquel ce serveur de messagerie est connecté. Un Relais ouvert peut également être appelé « Relais Spam » ou « Relais public ».

La définition de **« Confirmation de commande »** se trouve dans les Conditions générales de Symantec Online Services, le cas échéant. S'il n'existe aucune condition générale applicable à ce Service, « Confirmation de commande » désigne le Document d'abonnement, comme défini dans les présentes.

« **Service** » désigne l'option Protect ou Safeguard de Symantec Email Security.cloud, achetée par le Client.

« **Composant de Service** » désigne certains logiciels d'activation, des périphériques matériels et la documentation associée qui peuvent être fournis séparément par Symantec en complément d'un Service.

« **Crédit de service** » correspond à la somme qui sera créditée sur la prochaine facture du Client après envoi d'une Demande de crédit et validation par Symantec d'un crédit en faveur du Client.

« Logiciel de service » désigne un Logiciel (défini ci-dessous), éventuellement requis par un Service et que le client doit installer sur chaque ordinateur afin de bénéficier du Service. Le Logiciel de service comprend le Logiciel et la documentation associée susceptibles d'être fournis séparément par Symantec dans le cadre du Service.

« **Logiciel** » désigne chaque programme logiciel de Symantec ou d'un concédant, sous forme de code objet, concédé sous licence au Client par Symantec et régi par les conditions du CLUF qui l'accompagne, y compris mais sans s'y limiter les nouvelles versions ou mises à jour fournies au titre des présentes.

« **Spam** » désigne les Messages électroniques publicitaires non sollicités.

« **Faux négatif de Spam** » désigne un Message électronique de Spam qui n'est pas identifié comme Spam par le Service.

« **Faux positif de Spam** » désigne un Message électronique identifié à tort comme Spam par le Service.

« **Paramètres recommandés de Spam** » désigne les recommandations de configuration fournies par Symantec pour le Service, communiquées au Client durant le processus de provisionnement ou publiées dans l'aide en ligne.

« **Document d'abonnement** » désigne un ou plusieurs des documents applicables suivants, qui définissent davantage les droits et obligations du Client par rapport au Service : un certificat de Symantec ou un document similaire émis par Symantec, ou un contrat écrit entre le Client et Symantec, qui accompagne, précède ou suit le Service.

« **Conditions de Symantec Hosted Services** » désigne les Conditions de Symantec Hosted Services situées à l'adresse ou accessibles via l'adresse https://www.symantec.com/about/legal/service-agreements.jsp.

« **Conditions générales de Symantec Online Services** » désigne les Conditions générales de Online Services situées à l'adresse ou accessibles via l'adresse https://www.symantec.com/about/legal/service-agreements.jsp.

« **Processus de suivi de Symantec** » désigne un outil Symantec permettant de mesurer les niveaux Disponibilité du Service et Temps de latence pour le Service.

« **Tour** » désigne un cluster de serveurs de Messagerie à répartition de charge.

« **Utilisateur** » désigne une personne qui envoie et reçoit des Messages électroniques et qui est protégé par une partie du Service.

Annexe A

Contrat de niveau de service

Dispositions générales

- Le Client peut avoir droit à un Crédit de service si Symantec ne respecte pas le niveau de service défini. Si le Client pense avoir droit à un Crédit de service, il doit envoyer une Demande de crédit dans un délai de dix (10) jours ouvrables suivant la fin du mois civil durant lequel la rupture suspectée du niveau de service s'est produite. Le Client prend acte du fait que les journaux ne sont conservés que pendant un nombre limité de jours et que, par conséquent, toute Demande de crédit soumise en dehors du délai prévu sera jugée non valide.
- Pour effectuer une Demande de crédit, veuillez contacter le support technique de Symantec. Accédez à la page de destination du support produit pour obtenir des instructions détaillées : https://support.symantec.com/en_US/email-security-cloud..html.
- Toutes les Demandes de crédit font l'objet d'une vérification par Symantec conformément aux dispositions applicables du présent Contrat de niveau de service. Symantec peut demander des informations supplémentaires au Client pour valider la Demande de crédit.
- Le présent Contrat de niveau de service n'est pas applicable : (i) durant les périodes de Maintenance planifiée ou de Maintenance d'urgence, les périodes de non-disponibilité en raison de cas de force majeure, d'actes ou d'oublis du Client ou d'un tiers ; (ii) durant toute période d'interruption de service par Symantec, conformément aux conditions du Contrat ; (iii) si le Client enfreint le Contrat (y compris, mais sans s'y limiter, si le Client a des factures impayées) ; (iv) si le Client n'a pas configuré le Service conformément au Contrat ; ou (v) pendant les périodes d'essai du service.
- Les recours définis dans le présent Contrat de niveau de service constituent le seul et unique recours du Client pouvant être fondé, dans le cadre des présentes, en responsabilité contractuelle, civile (y compris, sans s'y limiter, la négligence) ou autre.
- La responsabilité cumulée maximale de Symantec dans le cadre du présent Contrat de niveau de service pour tout mois civil doit être un crédit égal à la valeur la plus basse entre 100 % des Frais mensuels ou dix mille dollars/cinq mille livres sterling/dix mille euros (10 000 $/5 000 £/10 000€) (en fonction de la devise de facturation du Client).
- Si le Service concerné est acheté au sein d'un lot de Services, le Crédit de service sera calculé en fonction du Service concerné et non du lot de Services entier.

Exceptions au Contrat de niveau de service pour Email Security Services

Le présent Contrat de niveau de service n'est pas applicable : (i) à tout Message électronique qui n'est pas passé par le Service (y compris, mais sans s'y limiter, si le Client n'a pas pris les mesures appropriées pour n'accepter que les Messages entrants de l'Infrastructure de Symantec) ; (ii) à tout Message électronique entrant ou sortant initialement envoyé à Symantec contenant plus de 500 destinataires par session SMTP ; (iii) à tout Client qui utilise le Service sur toute Tour désignée comme Tour de cluster en masse ; ou (iv) à tout Message électronique entrant ou sortant sur les domaines de Client qui ne sont pas configurés pour le Service.

Disponibilité du Service

Le Niveau de service de Disponibilité du Service est défini par la capacité à établir une session SMTP sur le port 25 depuis l'agent de transfert de messagerie du Client vers l'Infrastructure de Symantec, conformément à la RFC 5321. Le Niveau de disponibilité du Service ne s'applique ni au portail d'administration, ni au système Spam Quarantine. Ce Niveau de service ne s'applique pas si le Client a configuré le Service de manière incorrecte ou en raison de circonstances ou causes imprévues, en dehors du contrôle raisonnable de Symantec, y compris, mais sans s'y limiter, toute catastrophe naturelle, guerre, attaque terroriste, émeute, intervention des pouvoirs publics, ou toute défaillance de réseau ou d'appareil hors des centres de données de Symantec, y compris sur le site du Client ou entre le site du Client et le centre de données de Symantec.

Si la Disponibilité du Service est inférieure à cent pour cent (100 %) au cours de tout mois civil, le Client peut envoyer une Demande de crédit et recevoir un Crédit de service pour le prochain crédit en pourcentage équivalent à la valeur la plus basse entre 100 % des Frais mensuels ou dix mille dollars/cinq mille livres sterling/dix mille euros (10 000 $/5 000 £/10 000 €) (selon la devise de facturation du Client) :

Pourcentage disponible par mois calendaire	Crédit en % des Frais mensuels
inférieur à 100 % et supérieur ou égal à 99 %	25 %

inférieur à 99 % et supérieur ou égal à 98 %	50 %
inférieur à 98 %	100 %

Si la Disponibilité du Service est inférieure à quatre-vingt-dix-huit pour cent (98 %) pour tout mois civil, comme confirmé par Symantec, le Client est en droit de mettre fin au Service affecté et de bénéficier d'un remboursement au prorata des frais payés à l'avance pour la période après la prise d'effet de la résiliation.

Distribution du Courrier électronique

Le Niveau de service de distribution du Courrier électronique est défini comme la capacité de Symantec à distribuer 100 % de tous les Messages électroniques envoyés ou reçus par le Client, sous réserve des conditions suivantes :

a) Le Message électronique doit avoir été reçu par Symantec ; et

b) le Message électronique ne doit pas contenir de Malware, Spam ou autre contenu qui a provoqué son interception par le Service.

Sous réserve des conditions ci-dessus, dans le cas où Symantec ne parvient pas à distribuer un Message électronique depuis ou vers le Client, et si le Client ne viole pas les conditions du Contrat, le Client est en droit de mettre fin au Service après un avis écrit de trente (30) jours civils.

Latence de la Messagerie électronique

Le Niveau de service de temps de latence de la messagerie électronique est défini comme suit : si le temps d'aller-retour moyen, comme mesuré par le Processus de suivi de Symantec, pour les Messages électroniques envoyés toutes les cinq (5) minutes depuis et vers chaque Tour au sein du Cluster de tours désignées du Client dépasse le délai indiqué dans le tableau ci-dessous, au cours d'un mois civil. Si un Client estime que le Niveau de service de temps de latence n'a pas été respecté, il peut envoyer une Demande de crédit et peut recevoir un Crédit de service conformément au tableau ci-dessous :

Délai moyen d'aller-retour (secondes)	Crédit en % des Frais mensuels
supérieur à 60 et inférieur ou égal à 90	25 %
supérieur à 90 et inférieur ou égal à 120	50 %
supérieur à 120 et inférieur ou égal à 180	75 %
supérieur à 180	100 %

Ce Niveau de service de latence ne s'applique pas dans les cas suivants :

a) si le Client n'a pas fourni à Symantec une Liste de validation et s'il est victime d'une attaque de déni de service ;

b) des Périodes de retard sont provoquées par une boucle de Message électronique en provenance/à destination des systèmes du Client ; ou

c) le Serveur de messagerie principal du Client n'est pas en mesure d'accepter les Messages électroniques lors de la première tentative de distribution.

Faux positifs de Spam

Le Niveau de service de Faux positifs de Spam définit le taux maximum de capture de Faux positifs de Spam. Le Niveau de service de Faux positifs de Spam s'applique uniquement si le Client applique les Paramètres de pratiques d'excellence antispam, comme indiqués dans la ressource d'Aide en ligne. Si le taux de capture moyen de Faux positifs de Spam dépasse 0,0003 % du trafic des Messages électroniques entrants du Client au cours d'un mois civil, le Client peut envoyer une Demande de crédit et recevoir un Crédit de service conformément au tableau ci-dessous :

Taux en % de Faux positifs de spam capturés	Crédit en % des Frais mensuels

supérieur à 0,0003 et inférieur ou égal à 0,003	25 %
supérieur à 0,003 et inférieur ou égal à 0,03	50 %
supérieur à 0,03 et inférieur ou égal à 0,3	75 %
supérieur à 0,3	100 %

Les Messages électroniques suivants ne constituent pas des Faux positifs de Spam dans le cadre de ce niveau de service :
a) Messages électroniques qui ne sont pas des Messages électroniques professionnels légitimes
b) Messages électroniques contenant plus de 20 destinataires
c) Messages électroniques où l'expéditeur se trouve sur la liste d'expéditeurs bloqués du Client, y compris mais sans s'y limiter, ceux définis par un Utilisateur individuel si le Client a activé les paramètres au niveau de l'utilisateur
d) Messages électroniques envoyés à partir d'un ordinateur infecté
e) Messages électroniques envoyés à partir d'un ordinateur figurant sur une liste d'expéditeurs bloqués d'un tiers
f) Messages électroniques interceptés par l'analyse antispam sortante

Pour être éligible à un Crédit de service, le Client doit signaler les faux positifs suspectés de Messages électroniques au support technique de Symantec dans un délai de cinq (5) jours civils à compter de la réception du Message électronique. Symantec enquêtera et confirmera s'il s'agit ou non d'un Faux positif de Spam et enregistrera le verdict.

Taux de capture du Spam

Le Niveau de service de Taux de capture du Spam définit le taux minimum de capture de Spam. Ce niveau de service s'applique uniquement si le Client applique les paramètres de pratique d'excellence AntiSpam comme indiqués dans la ressource d'Aide en ligne. Le niveau de service correspond au nombre de Faux négatifs de Spam mesurés au cours d'un mois civil. Le Client peut envoyer une Demande de crédit et peut recevoir un Crédit de service conformément au tableau ci-dessous :

% de capture du spam	Crédit en % des Frais mensuels
supérieur à 98 et inférieur ou égal à 99	25 %
supérieur à 97 et inférieur ou égal à 98	50 %
supérieur à 96 et inférieur ou égal à 97	75 %
inférieur à 96	100 %

Ce Niveau de service de Taux de capture de Spam ne sera pas appliqué si le Message électronique n'a pas été envoyé à une Adresse électronique valide. Un Taux de capture de Spam inférieur de quatre-vingt-quinze pour cent (95 %) doit s'appliquer aux Messages électroniques contenant plus de cinquante pour cent (50 %) de jeux de caractères codés sur deux octets. Dans le cas où ce Taux de capture de Spam passe sous quatre-vingt-quinze pour cent (95 %), le Client a droit à un Crédit de service de vingt-cinq pour cent (25 %) des frais mensuels. Dans le cas où le Taux de capture de Spam passe sous quatre-vingt-dix pour cent (90 %), le Client peut avoir droit à un Crédit de service de cent pour cent (100 %) des frais mensuels.

Pour être éligible à un Crédit de service, le Client doit signaler les faux négatifs suspectés de Messages électroniques au support technique de Symantec dans un délai de cinq (5) jours civils à compter de la réception du Message électronique. Symantec enquêtera et confirmera s'il s'agit ou non d'un Faux négatif de Spam et enregistrera le verdict.

Protection contre les Malwares

Si les systèmes du Client sont infectés par un Malware connu ou inconnu qui se propage via des Messages électroniques analysés par le service d'analyse cloud, le Client peut avoir droit à un Crédit de service du montant défini ci-dessous. Le Client doit avertir Symantec dans un délai de cinq (5) jours après avoir pris connaissance du Malware et cette notification doit être consignée, examinée et validée par Symantec. Le Client doit envoyer une Demande de crédit et, si validée, recevoir un Crédit de service égal à la valeur la plus basse entre cent pour cent (100 %) des Frais mensuels ou dix mille dollars/cinq mille livres sterling/dix mille euros (10 000 $/5 000 £/10 000€) (en fonction de la devise de facturation du Client). Le recours présenté dans cette section est le seul et unique recours contractuel, en responsabilité civile délictuelle (y compris, mais sans s'y limiter, la négligence) ou autre, en cas d'infection par un Malware transmis à un Client ou un tiers via le Service. Pour lever toute ambiguïté, le recours établi dans la présente clause ne s'applique pas dans les cas d'auto-infection délibérée.

Les systèmes du Client sont considérés comme infectés si un Malware joint à un Message électronique a été reçu par le biais du Service et que le Malware a été activé au sein des systèmes du Client, automatiquement ou manuellement. Dans le cas où Symantec détecte, mais ne bloque pas un Message électronique dont la pièce jointe contient un Malware, et publie une mise à jour sur la Page Symantec Status ou avertit autrement les Clients, en fournissant suffisamment d'informations pour leur permettre d'identifier et de supprimer le Message électronique infecté, le recours présenté ci-dessus n'est pas applicable.

Le Service analyse le plus grand nombre possible de Messages électroniques et de pièces jointes associées. Il peut ne pas être possible d'analyser les pièces jointes dont le contenu est sous le contrôle direct de l'expéditeur (*par exemple*, pièces jointes chiffrées et/ou protégées par mot de passe et/ou dans les cas où le mot de passe est envoyé séparément du Message électronique). Ces Messages électroniques et/ou pièces jointes sont exclus du Niveau de service et le recours présenté ci-dessus ne s'applique pas.

Ce Niveau de service de Protection contre les Malwares ne s'applique pas aux Malwares qui ont été intentionnellement propagés par le Client ou par Symantec à la demande du Client.

Ce Niveau de service de Protection contre les Malwares s'applique uniquement aux Malwares comme définis dans la présente Description de service, et ne s'applique pas aux éléments suivants : spywares, logiciels publicitaires, liens URL vers des sites web hébergeant du contenu malveillant ou des chevaux de Troie inconnus.

Faux positifs de Malware

Le Niveau de service de Faux positifs de Malware définit le taux maximum de capture de Faux positifs de Malware. Si le taux de capture de Faux positifs de Malware de Message électronique dépasse 0,0001 % du trafic des Messages électroniques du Client au cours d'un mois civil, le Client peut envoyer une Demande de crédit et recevoir un Crédit de service conformément au tableau ci-dessous :

Taux en % de Faux positifs de Malware capturés	Crédit en % des Frais mensuels
supérieur à 0,0001 et inférieur ou égal à 0,001	25 %
supérieur à 0,001 et inférieur ou égal à 0,01	50 %
supérieur à 0,01 et inférieur ou égal à 0,1	75 %
supérieur à 0,1	100 %

Support technique 24 h/24, 7 j/7 et réponse aux pannes

Le support technique est disponible vingt-quatre (24) heures sur vingt-quatre et sept (7) jours sur sept afin de :
a) fournir un support technique au Client en cas de problèmes avec le Service ; et
b) communiquer avec le Client afin de résoudre ces problèmes.