

Conditions d'utilisation IBM – Modalités relatives aux offres de Logiciel-service

IBM Security Trusteer Fraud Protection

Les Conditions d'utilisation se composent du présent document intitulé «Conditions d'utilisation IBM – Modalités relatives aux offres de Logiciel-service» (les «Modalités des offres de Logiciel-service») et d'un document intitulé «Conditions d'utilisation IBM – Modalités générales» (les «Modalités générales»), qui est disponible à l'adresse <http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/>.

Advenant une incompatibilité entre les Modalités générales et les présentes Modalités des offres de Logiciel-service, ces dernières prévaudront. Le Client accepte les présentes Conditions d'utilisation en commandant le Logiciel-service IBM, en y accédant ou en l'utilisant.

Ces Conditions d'utilisation sont régies par le Contrat Passport Advantage international IBM, le Contrat Passport Advantage Express international IBM ou le Contrat international régissant les offres désignées relatives aux Logiciels-services IBM (aussi appelés Logiciels sous forme de services), selon le cas (le «Contrat»), et celui-ci, de pair avec les Conditions d'utilisation, constitue l'entente intégrale.

1. Logiciel-service IBM

L'offre de Logiciel-service IBM suivante est régie par les présentes Modalités des offres de Logiciel-service :

1.1 Offres de Logiciel-service IBM Rapport

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 Offres de Logiciel-service IBM Pinpoint

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail

- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- Offre IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 Offres de Logiciel-service IBM Mobile

- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Business
- IBM Security Trusteer Mobile Browser for Business Premium Support
- IBM Security Trusteer Mobile Browser for Retail
- IBM Security Trusteer Mobile Browser for Retail Premium Support

2. Paramètres de calcul des frais

Le Logiciel-service IBM est vendu en fonction d'un des paramètres de calcul des frais suivants, comme spécifié dans le Document transactionnel :

- a. Un **Participant admissible** est une unité de mesure servant de base pour obtenir le Logiciel-service IBM. Chaque personne ou entité admissible à participer à tout programme de prestation de services géré ou suivi par un Logiciel-service IBM est un Participant admissible. Il faut obtenir un nombre suffisant d'autorisations pour couvrir tous les Participants admissibles gérés ou suivis par le Logiciel-service IBM pendant la période de mesure indiquée dans le Document transactionnel du Client.

Chaque programme de prestation de services géré par le Logiciel-service IBM est analysé séparément puis regroupé avec les autres programmes. Les personnes ou les entités qui sont admissibles à de multiples programmes de prestation de services nécessitent des autorisations d'utilisation séparées.

Pour ces offres, un programme de prestation de services comprend une seule Application d'affaires ou de vente au détail du Client, accompagnée d'une page d'ouverture de session principale et de pages qui s'y rattachent (pour chaque Application d'affaires ou de vente au détail). Un Participant admissible est un utilisateur final du Client qui dispose de justificatifs d'identité pour ouvrir une session dans l'Application d'affaires ou de vente au détail.

- b. Un **Appareil du Client** est une unité de mesure servant de base pour obtenir le Logiciel-service IBM. Il peut s'agir d'un appareil informatique mono-utilisateur, d'un détecteur ou d'un dispositif de télémessure servant à un usage spécial qui demande l'exécution d'un ensemble de commandes, de procédures ou d'applications à un autre système informatique ou qui les reçoit aux fins d'exécution d'un tel système, normalement appelé un serveur, ou qui est géré autrement par un serveur. De multiples Appareils du Client peuvent partager un accès à un serveur commun. Un tel Appareil du Client peut avoir une certaine capacité de traitement ou être programmé pour permettre à un utilisateur d'effectuer des travaux. Le Client doit obtenir des autorisations pour chaque Appareil du Client qui exécute le Logiciel-service IBM, qui lui envoie des données, qui utilise les services dudit Logiciel-service IBM ou qui accède autrement audit Logiciel-service IBM pendant la période de mesure indiquée dans le Document transactionnel du Client.

3. Frais et facturation

Le montant exigible pour le Logiciel-service IBM est indiqué dans un Document transactionnel.

3.1 Frais mensuels partiels

Des frais mensuels partiels spécifiés dans le Document transactionnel et calculés au prorata peuvent être exigés.

4. Conformité et vérification

L'accès aux offres IBM Security Trusteer Fraud Protection est limité au nombre maximal de Participants admissibles ou d'Appareils du Client qui est spécifié dans le Document transactionnel. Le Client a la responsabilité de s'assurer que le nombre de ses Participants admissibles ou d'Appareils du Client n'excède pas le nombre maximal spécifié dans le Document transactionnel.

Il se peut qu'un audit soit mené pour vérifier le respect du nombre maximal de Participants admissibles ou d'Appareils du Client.

5. Options de renouvellement de la Période d'abonnement pour le Logiciel-service IBM

Le Document transactionnel du Client indiquera si l'abonnement au Logiciel-service IBM se renouvelle à la fin de la Période d'abonnement, en désignant cette période de l'une des façons décrites ci-dessous.

5.1 Renouvellement automatique

Si le Document transactionnel du Client indique que le renouvellement de l'abonnement se fait de manière automatique, le Client peut mettre fin à son abonnement au Logiciel-service IBM en faisant parvenir une demande écrite au représentant IBM ou au Partenaire commercial IBM, selon le cas, au moins quatre-vingt-dix (90) jours avant la date d'expiration de la Période d'abonnement alors en cours qui est spécifiée dans le Document transactionnel. Si IBM ou le Partenaire commercial IBM ne reçoit pas un tel avis de cessation au plus tard à la date d'expiration, la Période d'abonnement qui se termine se renouvellera automatiquement pour une période d'un (1) an ou pour la durée originale indiquée dans le Document transactionnel.

5.2 Facturation continue

Lorsque le Document transactionnel indique que la Période d'abonnement du Client se renouvelle de manière continue, le Logiciel-service IBM continuera d'être accessible au Client et son utilisation sera facturée en continu. Pour cesser l'utilisation du Logiciel-service IBM et stopper le processus de facturation continue, le Client doit faire parvenir à IBM ou au Partenaire commercial IBM, selon le cas, un préavis écrit de quatre-vingt-dix (90) jours, dans lequel il demande d'annuler son utilisation du Logiciel-service IBM. Dès l'annulation de l'accès au Logiciel-service IBM, les frais d'accès impayés qui s'appliquent jusqu'au mois au cours duquel l'annulation a pris effet seront facturés au Client.

5.3 Renouvellement requis

Lorsque le Document transactionnel indique que la Période d'abonnement du Client ne se renouvelle pas, l'abonnement au Logiciel-service IBM et l'accès du Client à ce Logiciel-service sont révoqués à la fin de cette période. S'il désire continuer d'utiliser le Logiciel-service IBM après la date d'expiration, le Client doit passer une commande auprès d'un représentant IBM ou du Partenaire commercial IBM, selon le cas, en vue d'obtenir une nouvelle Période d'abonnement.

6. Assistance technique

De l'assistance technique est offerte au Client et à ses Participants admissibles, afin de les aider à utiliser le Logiciel-service IBM.

L'assistance standard est incluse dans l'abonnement à toutes les offres. Le module Trusteer Rapport Mandatory Service, qui est complémentaire à l'offre Trusteer Rapport, nécessite l'assistance Élite pour l'abonnement de base à l'offre Trusteer Rapport.

Un abonnement à l'assistance Élite est offert moyennant des frais supplémentaires pour chaque offre de Logiciel-service IBM, sauf pour les offres IBM Security Trusteer Mobile SDK et IBM Security Trusteer Rapport Mandatory Service.

Assistance standard

- Assistance de 8 h à 17 h (heure locale).
- Le Client et ses Participants admissibles peuvent soumettre une demande d'assistance par voie électronique, comme décrit en détail dans le document de référence sur l'assistance relative aux Logiciels-services IBM.
- Le Client peut accéder au Portail d'assistance pour obtenir des avis, des documents, des rapports sur un dossier et des foires aux questions, à l'adresse suivante : <http://www-01.ibm.com/software/security/trusteer/support/>.
- Pour connaître les options d'assistance et obtenir plus de détails, veuillez accéder au document de référence sur l'assistance relative aux Logiciels-services IBM («IBM Software as a Service [SaaS] Support Handbook»), à l'adresse <http://www-01.ibm.com/software/support/handbook.html>.

Assistance Élite

- Assistance 24 heures sur 24, 7 jours sur 7 pour tous les niveaux de gravité.
- Le Client peut obtenir de l'assistance directement par téléphone.
- Le Client et ses Participants admissibles peuvent soumettre une demande d'assistance par voie électronique, comme décrit en détail dans le document de référence sur l'assistance relative aux Logiciels-services IBM.
- Le Client peut accéder au Portail d'assistance pour obtenir des avis, des documents, des rapports sur un dossier et des foires aux questions, à l'adresse suivante : <http://www-01.ibm.com/software/security/trusteer/support/>.
- Pour connaître les options d'assistance et obtenir plus de détails, veuillez accéder au document de référence sur l'assistance relative aux Logiciels-services IBM («IBM Software as a Service [SaaS] Support Handbook»), à l'adresse <http://www-01.ibm.com/software/support/handbook.html>.

7. Modalités supplémentaires relatives aux offres de Logiciel-service IBM

7.1 Certification Safe Harbor

IBM respecte le cadre américano-européen «U.S. – EU Safe Harbor Framework» élaboré par le département du Commerce des États-Unis en coordination avec la Commission européenne. Les produits IBM Security Trusteer sont inclus dans la certification EU-U.S. Safe Harbor d'IBM. Le site suivant contient plus de renseignements sur Safe Harbor et la liste des sociétés Safe Harbor : <http://export.gov/safeharbor/>.

7.2 Augmentation annuelle des frais d'abonnement du Client

IBM se réserve le droit de rajuster les frais d'abonnement pour le Logiciel-service IBM, au plus une (1) fois tous les douze (12) mois, selon un pourcentage que déterminera IBM et qui n'excédera pas trois pour cent (3 %). Le rajustement des frais d'abonnement prendra effet à l'anniversaire de la date du début de la couverture initiale. Ce rajustement des frais d'abonnement ne modifie nullement l'autorisation du Client d'utiliser le Logiciel-service IBM, ni les paramètres de calcul des frais utilisés pour obtenir le Logiciel-service IBM. Les Partenaires commerciaux IBM sont indépendants d'IBM et déterminent unilatéralement leurs prix et leurs modalités.

7.3 Assistance Élite

Le Client a droit à l'assistance Élite seulement pour les offres de Logiciel-service IBM pour lesquelles il s'est abonné à l'offre d'assistance Élite correspondante.

7.4 Utilisation légitime et consentement

Autorisation de recueillir et de traiter des données

Le Logiciel-service IBM est conçu pour aider le Client à améliorer son environnement de sécurité et ses données. Le Logiciel-service IBM recueillera de l'information à partir des Participants admissibles et des Appareils du Client qui interagissent avec les Applications d'affaires ou de vente au détail pour lesquelles le Client s'est abonné aux offres de Logiciel-service IBM. L'information que recueille le Logiciel-service IBM, seule ou combinée à d'autres renseignements, peut être considérée comme des Renseignements personnels dans certains territoires. Les Renseignements personnels sont toute information pouvant servir à identifier une personne, comme un nom, une adresse courriel, une adresse à domicile ou un

numéro de téléphone, qui est fournie à IBM et qui peut être enregistrée, traitée ou transférée au nom du Client.

Les pratiques de collecte et de traitement des données peuvent être modifiées pour améliorer l'aspect fonctionnel du Logiciel-service IBM. Un document décrivant intégralement les pratiques de collecte et de traitement des données est mis à jour au besoin et sera fourni au Client à sa demande. Le Client autorise IBM à recueillir cette information et à la traiter conformément aux articles «Transferts transfrontaliers» et «Protection des renseignements personnels» des présentes et à l'article «Confidentialité et sécurité des données» des Modalités générales.

Pour les offres IBM Security Trusteer Pinpoint :

Les données recueillies peuvent inclure les adresses IP des utilisateurs, les ID utilisateurs chiffrés ou hachés à sens unique, les témoins de domaine, s'ils ne sont pas filtrés, les visites aux Applications protégées et à des sites d'hameçonnage, l'emplacement géographique, ainsi que les justificatifs d'identité entrés dans les sites d'hameçonnage.

Pour les offres IBM Security Trusteer Mobile SDK et IBM Security Trusteer Mobile Browser :

Les données recueillies peuvent inclure les adresses IP des utilisateurs, les ID utilisateurs chiffrés ou hachés à sens unique, l'emplacement géographique, les visites aux Applications protégées, l'information sur les cartes SIM, le nom de l'appareil et l'affiliation du Client.

Pour les offres IBM Security Trusteer Rapport :

Les données recueillies peuvent inclure les adresses IP des utilisateurs, les ID utilisateurs chiffrés ou hachés à sens unique, les événements de sécurité, le nom d'utilisateur et l'adresse courriel fournis pour communiquer avec IBM afin d'obtenir de l'assistance, l'affiliation du Client, les mots de passe chiffrés entrés sur les sites protégés, les visites aux Applications protégées et à des sites d'hameçonnage, le numéro chiffré des cartes de paiement, ainsi que les fichiers et les données recueillis à distance par le personnel d'IBM pour inspecter des logiciels et des activités soupçonnés d'être malveillants ou dans le cas du mauvais fonctionnement d'un élément.

Consentement éclairé des personnes visées par les données

L'utilisation de ce Logiciel-service IBM peut être assujettie à diverses lois et à différents règlements. Le Logiciel-service IBM peut être utilisé uniquement à des fins licites et de manière légitime. Le Client convient d'utiliser le Logiciel-service IBM conformément aux lois, aux règlements et aux politiques applicables et assume la responsabilité de cette conformité.

Pour les offres IBM Security Trusteer Pinpoint et IBM Security Trusteer Mobile SDK :

Le Client convient qu'il a obtenu ou qu'il obtiendra les consentements pleinement éclairés, les autorisations ou les licences nécessaires pour permettre une utilisation légitime du Logiciel-service IBM, ainsi que pour autoriser IBM à recueillir et à traiter l'information en utilisant le Logiciel-service IBM.

Pour les offres IBM Security Trusteer Rapport et IBM Security Trusteer Mobile Browser :

Le Client autorise IBM à obtenir les consentements pleinement éclairés nécessaires pour permettre une utilisation légitime du Logiciel-service IBM, ainsi que la cueillette et le traitement de l'information comme décrit dans le Contrat de licence utilisateur final qui se trouve à l'adresse <https://www.trusteer.com/support/end-user-license-agreement>. Si le Client détermine que c'est lui (et non IBM) qui gérera les communications sur le consentement avec les utilisateurs finals, il convient qu'il a obtenu ou qu'il obtiendra les consentements pleinement éclairés, les autorisations ou les licences nécessaires pour permettre une utilisation légitime du Logiciel-service IBM, ainsi que pour autoriser IBM à recueillir et à traiter l'information, en tant que sous-traitant du Client, en utilisant le Logiciel-service IBM.

7.5 Transferts transfrontaliers

Le Client convient qu'IBM peut traiter le Contenu, dont les Renseignements personnels, au-delà d'une frontière nationale, en vertu des lois et selon les exigences pertinentes, par l'intermédiaire de sous-traitants du traitement et de sous-traitants ultérieurs du traitement qui se trouvent dans le pays suivant, qui est situé hors de l'Espace économique européen, mais qui, selon la Commission européenne, offre des niveaux de sécurité adéquats : les États-Unis.

7.6 Protection des renseignements personnels

Si le Client met en disponibilité des Renseignements personnels pour le Logiciel-service IBM dans les États membres de l'Union européenne que sont l'Islande, le Liechtenstein, la Norvège ou la Suisse, ou si le Client a des Participants admissibles ou des Appareils du Client dans ces pays, alors ce dernier,

agissant à titre de seul responsable du traitement, désigne IBM comme sous-traitant du traitement (selon la définition de ces appellations dans la Directive 95/46/EC de l'Union européenne) pour traiter les Renseignements personnels. IBM traitera ces Renseignements personnels seulement dans la mesure requise pour mettre en disponibilité l'offre de Logiciel-service IBM conformément aux descriptions du Logiciel-service publiées par IBM. Le Client convient pour sa part qu'un tel traitement est conforme à ses instructions. IBM fournira un préavis raisonnable si elle apporte un changement important à l'emplacement de traitement ou à la façon dont elle protège les Renseignements personnels dans le cadre du Logiciel-service IBM. Le Client peut mettre fin à la Période d'abonnement en cours, pour le Logiciel-service IBM visé, en fournissant un avis écrit à IBM dans les trente (30) jours qui suivent sa réception de l'avis d'IBM concernant cette modification. Le Client convient qu'IBM peut traiter le Contenu, y compris les Renseignements personnels, au-delà d'une frontière nationale par l'intermédiaire des sous-traitants du traitement et des sous-traitants ultérieurs du traitement suivants :

Nom du sous-traitant ou du sous-traitant ultérieur	Rôle (sous-traitant ou sous-traitant ultérieur)	Emplacement*
Entité IBM contractante	Sous-traitant	Comme indiqué dans le Document transactionnel
Amazon Web Services LLC	Sous-traitant ultérieur	410 Terry Ave. N Seattle, WA 98109 États-Unis
Connectria Corp.	Sous-traitant ultérieur	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 États-Unis
IBM Israel Ltd.	Sous-traitant ultérieur	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israël
IBM Corporation	Sous-traitant ultérieur	1 New Orchard Rd. Armonk, NY 10504 États-Unis

Le Client convient qu'IBM peut, en transmettant un avis à ce sujet, modifier cette liste de pays si elle détermine de manière raisonnable que cette modification est nécessaire pour fournir le Logiciel-service IBM.

Le Client convient que pour le service fourni par l'entremise du centre informatique de l'Allemagne, comme déterminé au cours du processus d'allocation des ressources, IBM peut traiter le Contenu, y compris les Renseignements personnels, au-delà d'une frontière nationale par l'intermédiaire des sous-traitants du traitement et des sous-traitants ultérieurs du traitement suivants :

Nom du sous-traitant ou du sous-traitant ultérieur	Rôle (sous-traitant ou sous-traitant ultérieur)	Emplacement*
Entité IBM contractante	Sous-traitant	Comme indiqué dans le Document transactionnel
Amazon Web Services (Allemagne)	Sous-traitant ultérieur	Munich, Allemagne
IBM Israel Ltd.	Sous-traitant ultérieur	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israël

Le Client convient que pour le service fourni par l'entremise du centre informatique du Japon, comme déterminé au cours du processus d'allocation des ressources, IBM peut traiter le Contenu, y compris les Renseignements personnels, au-delà d'une frontière nationale par l'intermédiaire des sous-traitants du traitement et des sous-traitants ultérieurs du traitement suivants :

Nom du sous-traitant ou du sous-traitant ultérieur	Rôle (sous-traitant ou sous-traitant ultérieur)	Emplacement*
Entité IBM contractante	Sous-traitant	Comme indiqué dans le Document transactionnel
Amazon Web Services (Japon)	Sous-traitant ultérieur	Tokyo, Japon
IBM Israel Ltd.	Sous-traitant ultérieur	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israël

* Les emplacements indiqués dans les tableaux ci-dessus correspondent à l'adresse du siège social du sous-traitant ou du sous-traitant ultérieur. Les centres informatiques sont situés dans le pays identifié.

Les parties ou leurs sociétés affiliées pertinentes peuvent conclure des contrats distincts contenant les clauses modèles standards pour l'Union européenne, dans leur rôle respectif, conformément à la décision 2010/87/EU de la Commission européenne, en retirant les clauses facultatives. Les différends ou les responsabilités qui découlent de ces contrats (même ceux conclus par des sociétés affiliées) seront traités par les parties comme si ces différends ou ces responsabilités découlaient des modalités du présent Contrat.

Annexe A

1. Offres de Logiciel-service IBM

Les offres de Logiciel-service IBM se présentent sous la forme de services et d'offres autonomes ou supplémentaires. Les offres de Logiciel-service IBM commandées sont spécifiées dans l'Autorisation d'utilisation du Client.

1.1 Applications d'affaires et de vente au détail

Les produits IBM Security Trusteer contre la fraude sont autorisés sous licence pour s'utiliser avec des types d'Applications spécifiques : les Applications de vente au détail ou les Applications d'affaires. Des offres différentes sont disponibles pour chacun de ces types d'Applications.

- Une Application de vente au détail se définit comme une application bancaire en ligne, une application mobile ou une application de commerce électronique qui dessert des consommateurs. Dans sa politique, un Client peut spécifier que certaines petites entreprises sont admissibles à un accès aux Applications de vente au détail.
- Une Application d'affaires se définit comme une application bancaire en ligne, une application mobile ou une application de commerce électronique qui dessert une société, une institution ou des entités semblables, ou comme une application qui n'est pas considérée comme une Application de vente au détail.

1.2 Offres d'abonnement de base au Logiciel-service IBM

Offres pour les Applications d'affaires

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

Offres pour les Applications de vente au détail

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

Un abonnement à l'assistance Élite est offert moyennant des frais supplémentaires pour chaque offre de Logiciel-service destinée aux Applications d'affaires et aux Applications de vente au détail, sauf pour les offres IBM Security Trusteer Mobile SDK.

1.3 Offres d'abonnement supplémentaires aux Logiciels-services IBM Security Trusteer Rapport

Offres supplémentaires disponibles pour le Logiciel-service IBM Security Trusteer Rapport for Business :

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Mandatory Service for Business

Offres supplémentaires disponibles pour le Logiciel-service IBM Security Trusteer Rapport for Retail :

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

Un abonnement à l'assistance Élite est offert moyennant des frais supplémentaires pour chaque complément aux offres IBM Security Trusteer Rapport qui est ajouté pour les Applications d'affaires ou les Applications de vente au détail, sauf pour les compléments IBM Security Trusteer Rapport Mandatory Service.

L'abonnement au Logiciel-service IBM Security Trusteer Rapport for Business ou IBM Security Trusteer Rapport for Retail constitue une exigence préalable pour profiter des offres d'abonnement aux Logiciels-services IBM supplémentaires correspondantes énumérées dans cette section.

1.4 Offres d'abonnement supplémentaires aux Logiciels-services IBM Security Trusteer Pinpoint Malware Detection

Offres supplémentaires disponibles pour IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition ou IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition :

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Offres supplémentaires disponibles pour IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition ou IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition :

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

Un abonnement à l'assistance Élite est offert, moyennant des frais supplémentaires, pour chacune des offres de Logiciel-service IBM additionnelles énumérées dans cette section.

L'abonnement au Logiciel-service IBM Security Trusteer Pinpoint Malware Detection for Business ou IBM Security Trusteer Pinpoint Malware Detection for Retail constitue une exigence préalable pour profiter des offres d'abonnement aux Logiciels-services IBM supplémentaires correspondantes énumérées dans cette section.

1.5 Autres abonnements supplémentaires aux Logiciels-services IBM

Tout abonnement supplémentaire aux Logiciels-services IBM qui s'ajoute à l'abonnement de base décrit plus haut, mais qui n'est pas énuméré aux présentes, qu'il soit déjà offert ou en développement, n'est pas considéré comme une mise à jour et doit être accordé séparément.

1.6 Définitions

Titulaire de compte - Désigne l'utilisateur final du Client qui a installé le logiciel de soutien du côté client, qui a accepté le contrat de licence utilisateur final («CLUF») et dont l'identité a été authentifiée au moins une (1) fois par l'Application de vente au détail ou d'affaires pour laquelle le Client s'est abonné aux offres de Logiciel-service IBM.

Logiciel client du titulaire de compte – Désigne le logiciel de soutien côté client pour l'offre IBM Security Trusteer Rapport ou l'offre IBM Security Trusteer Mobile Browser, ou encore le logiciel de soutien côté client qui est fourni avec certains abonnements au Logiciel-service IBM et qui doit être installé dans l'appareil de l'utilisateur final.

Page de garde Trusteer – Désigne la page de garde qui est fournie au Client et qui est fondée sur les modèles de pages de garde disponibles.

Page de renvoi – Désigne la page hébergée par IBM qui est fournie au Client avec la page de garde et le Logiciel client du titulaire de compte téléchargeable.

2. Offres IBM Security Trusteer Rapport

2.1 IBM Security Trusteer Rapport for Retail et IBM Security Trusteer Rapport for Business («Trusteer Rapport»)

Le Logiciel-service Trusteer Rapport fournit une couche de protection contre les attaques d'hameçonnage et de programmes malveillants de type MitB («Man-in-the-Browser»). Le Logiciel-service IBM Security Trusteer Rapport se sert d'un réseau comportant des dizaines de millions de points d'extrémité dans le monde pour recueillir de l'information sur les attaques actives d'hameçonnage et de programmes

malveillants contre des organisations à l'échelle mondiale. IBM Security Trusteer Rapport applique des algorithmes comportementaux visant à bloquer les attaques d'hameçonnage et à empêcher l'installation et l'exécution de souches de programmes malveillants de type MitB.

Les frais pour cette offre de Logiciel-service IBM sont établis en fonction du nombre de Participants admissibles. L'offre pour les Applications d'affaires se vend par tranche de dix (10) Participants admissibles, alors que l'offre pour les Applications de vente au détail se vend par tranche de cent (100) Participants admissibles.

Cette offre de Logiciel-service IBM comprend ce qui suit :

a. Application de gestion Trusteer («TMA»)

L'application de gestion Trusteer («Trusteer Management Application» ou «TMA») est mise en disponibilité dans l'environnement infonuagique hébergé d'IBM Security Trusteer. Cette application permet au Client et à un nombre illimité de membres de son personnel autorisés : (i) de recevoir des rapports sur les événements et des évaluations des risques; (ii) de voir, de configurer et de définir des politiques liées au signalement des événements; et (iii) de voir la configuration du logiciel de soutien côté client, autorisé sans frais pour le public aux termes d'un contrat de licence utilisateur final («CLUF»), qui est mis en disponibilité aux fins de téléchargement dans les ordinateurs de bureau ou les appareils (PC ou MAC) des Participants admissibles, aussi appelé «Trusteer Rapport software suite» («Logiciel client du titulaire de compte»). Le Client peut mettre en marché le Logiciel client du titulaire de compte uniquement en utilisant la Page de garde Trusteer ou l'API Rapport. Le Client n'est pas autorisé à utiliser le Logiciel client du titulaire de compte pour ses activités d'entreprise internes, ni pour ses employés (autrement que pour l'usage personnel des employés).

b. Script Web

Pour accéder à un site Web en vue d'avoir accès aux offres de Logiciel-service IBM ou de les utiliser.

c. Données sur les événements

Le Client et un nombre illimité de membres de son personnel autorisés peuvent utiliser l'application TMA pour recevoir des données sur les événements générées par le Logiciel client du titulaire de compte à la suite des interactions en ligne du Titulaire de compte avec l'Application d'affaires ou de vente au détail pour laquelle le Client s'est abonné aux offres de Logiciel-service IBM. Les données sur les événements seront reçues du Logiciel client du titulaire de compte des Participants admissibles qui s'exécute dans leurs appareils. Ces Participants admissibles doivent avoir accepté le CLUF, avoir été authentifiés au moins une (1) fois par l'Application d'affaires ou de vente au détail, et la configuration du Client doit inclure l'ensemble des ID utilisateurs.

d. Page de garde Trusteer

La plateforme de mise en marché de la Page de garde Trusteer identifie le Logiciel client du titulaire de compte et le met en marché auprès des Participants admissibles qui accèdent à l'Application d'affaires ou de vente au détail du Client pour laquelle le Client s'est abonné aux offres de Logiciel-service IBM. Le Client peut choisir sa page de garde dans un ensemble de modèles disponibles. Il est possible de personnaliser une page de garde aux termes d'un contrat distinct ou d'une description du travail séparée.

Le Client peut décider de fournir ses marques de commerce, logos et icônes afin de les utiliser en lien avec l'application TMA, mais seulement avec la Page de garde Trusteer et aux fins d'affichage dans le Logiciel client du titulaire de compte ou dans les Pages de renvoi hébergées par IBM et sur le site Web d'IBM Security Trusteer. Toute utilisation de ces marques de commerce, logos et icônes se fera conformément aux politiques raisonnables d'IBM concernant l'utilisation de la publicité et des marques de commerce.

Le Client doit s'abonner à l'offre de Logiciel-service IBM Security Trusteer Rapport Mandatory Service s'il désire utiliser tout type de déploiement obligatoire du Logiciel client du titulaire de compte.

Le déploiement obligatoire du Logiciel client du titulaire de compte inclut, notamment, tout déploiement obligatoire à l'aide d'un mécanisme ou d'un moyen quelconque qui force directement ou indirectement un Participant admissible à télécharger le Logiciel client du titulaire de compte, ou encore une méthode, un outil, une procédure ou un mécanisme non créés ou approuvés par IBM ayant pour but de contourner les exigences de licence relatives au déploiement obligatoire du Logiciel client du titulaire de compte.

2.2 Offres de Logiciel-service IBM supplémentaires facultatives pour IBM Security Trusteer Rapport for Business et IBM Security Trusteer Rapport for Retail

L'abonnement aux offres IBM Security Trusteer Rapport constitue une exigence préalable pour l'abonnement à l'une ou l'autre des offres de Logiciel-service IBM supplémentaires qui suivent. Si le Logiciel-service IBM est désigné «for Business» (pour affaires), l'offre de Logiciel-service supplémentaire acquise doit aussi être désignée «for Business». Si le Logiciel-service IBM est désigné «for Retail» (pour vente au détail), l'offre de Logiciel-service supplémentaire acquise doit aussi être désignée «for Retail». Le Client recevra les données sur les événements de Participants admissibles qui exécutent le Logiciel client du titulaire de compte, qui ont accepté le CLUF et qui ont été authentifiés au moins une (1) fois par l'Application d'affaires ou de vente au détail du Client. La configuration du Client doit aussi inclure l'ensemble des ID utilisateurs.

2.2.1 Offres IBM Security Trusteer Rapport Fraud Feeds for Business et IBM Security Trusteer Rapport Fraud Feeds for Retail

Le Client et un nombre illimité de membres de son personnel autorisés peuvent utiliser l'application TMA pour recevoir des données sur les événements liées à des infections par un programme malveillant et d'autres vulnérabilités de point d'extrémité dans un ordinateur de bureau particulier du Titulaire de compte.

2.2.2 Offres IBM Security Trusteer Rapport Phishing Protection for Business et IBM Security Trusteer Rapport Phishing Protection for Retail

Le Client et un nombre illimité de membres de son personnel autorisés peuvent utiliser l'application TMA pour recevoir des données sur les événements qui sont liées à la soumission des justificatifs d'identité d'ouverture de session du Titulaire de compte dans un site soupçonné d'hameçonnage ou un site potentiellement frauduleux. Il est possible que des applications en ligne légitimes (adresses URL) soient considérées par erreur comme étant des sites d'hameçonnage et que le Logiciel-service IBM avise ainsi le Titulaire de compte qu'un site légitime est un site d'hameçonnage. Dans un cas pareil, le Client doit aviser IBM d'une telle erreur et IBM doit corriger cette erreur. Cette correction sera d'ailleurs le seul recours du Client dans le cas d'une erreur de ce genre.

2.2.3 Offres IBM Security Trusteer Rapport Mandatory Service for Business et IBM Security Trusteer Rapport Mandatory Service for Retail

Le Client peut utiliser une instance de la plateforme de mise en marché de la Page de garde Trusteer pour imposer le téléchargement du Logiciel client du titulaire de compte aux Participants admissibles qui accèdent à l'Application d'affaires ou de vente au détail du Client pour laquelle le Client s'est abonné aux offres de Logiciel-service IBM.

L'abonnement à l'offre IBM Security Trusteer Rapport Premium Support for Business est une exigence préalable pour l'abonnement à l'offre IBM Security Rapport Mandatory Service for Business.

L'abonnement à l'offre IBM Security Trusteer Rapport Premium Support for Retail est une exigence préalable pour l'abonnement à l'offre IBM Security Rapport Mandatory Service for Retail.

Le Client peut mettre en œuvre le module supplémentaire IBM Security Trusteer Rapport Mandatory Service seulement si ce module a été commandé et configuré pour s'utiliser avec l'Application de vente au détail ou d'affaires du Client pour laquelle le Client s'est abonné aux offres de Logiciel-service IBM.

3. Offres IBM Security Trusteer Pinpoint

Le Logiciel-service IBM Security Trusteer Pinpoint est un service infonuagique qui est conçu pour fournir une couche de protection supplémentaire et qui vise à détecter et à atténuer les attaques de programmes malveillants, d'hameçonnage et de prise de contrôle de comptes. Le Logiciel-service Trusteer Pinpoint peut être intégré aux Applications d'affaires ou de vente au détail du Client pour lesquelles le Client s'est abonné aux offres de Logiciel-service IBM, ainsi qu'aux processus de prévention des fraudes.

Cette offre de Logiciel-service IBM comprend ce qui suit :

a. Application TMA

L'application de gestion Trusteer («Trusteer Management Application» ou «TMA») est mise en disponibilité dans l'environnement infonuagique hébergé d'IBM Security Trusteer. Cette application permet au Client et à un nombre illimité de membres de son personnel autorisés : (i) de recevoir des rapports sur les événements et des évaluations des risques; et (ii) de voir, de configurer et de définir des politiques de sécurité et d'autres politiques liées au signalement des événements.

- b. Script Web et interfaces de programmation d'applications

Pour le déploiement sur un site Web, afin d'accéder au Logiciel-service IBM ou de l'utiliser.

3.2 IBM Security Trusteer Pinpoint Malware Detection et IBM Security Trusteer Pinpoint Criminal Detection

Advenant la détection d'un programme malveillant dans les offres IBM Security Trusteer Pinpoint Malware Detection ou la détection d'une prise de contrôle de comptes dans les offres IBM Security Trusteer Pinpoint Criminal Detection, le Client doit suivre les instructions du «Pinpoint Best Practices Guide» (guide Pinpoint sur les meilleures pratiques). Le Client ne doit pas se servir des offres IBM Security Trusteer Pinpoint Malware Detection ou IBM Security Trusteer Pinpoint Criminal Detection d'une manière qui modifiera l'expérience du Participant admissible immédiatement après la détection d'un programme malveillant ou d'une prise de contrôle de comptes, de telle sorte que d'autres puissent lier les actions du Client à l'utilisation des offres IBM Security Trusteer Pinpoint (p. ex., les notifications, les messages, le blocage d'appareils ou le blocage de l'accès à l'Application d'affaires ou de vente au détail immédiatement après la détection d'un programme malveillant ou d'une prise de contrôle de comptes).

3.2.1 Offres IBM Security Trusteer Pinpoint Criminal Detection for Business et IBM Security Trusteer Pinpoint Criminal Detection for Retail

Ces offres permettent de détecter sans logiciel client une activité suspecte de prise de contrôle de comptes par des navigateurs qui se connectent à une Application d'affaires ou de vente au détail, à l'aide de l'ID de l'appareil, de la détection de l'hameçonnage et de la détection du vol de justificatifs d'identité par des programmes malveillants. Les offres IBM Security Trusteer Pinpoint Criminal Detection fournissent une couche de protection supplémentaire et visent à détecter les tentatives de prise de contrôle de comptes et à livrer au Client les résultats d'évaluations des risques concernant des navigateurs ou des appareils mobiles (par l'intermédiaire du navigateur en mode natif ou de l'application mobile du Client) qui accèdent directement à une Application d'affaires ou de vente au détail.

- a. Données sur les événements

Le Client et un nombre illimité de membres de son personnel autorisés peuvent utiliser l'application TMA pour recevoir des données sur les événements générées à la suite des interactions en ligne des Participants admissibles avec l'Application d'affaires ou de vente au détail du Client pour laquelle le Client s'est abonné aux offres de Logiciel-service IBM. Le Client peut aussi recevoir les données sur les événements par l'intermédiaire d'une interface de programmation d'applications du système principal.

3.2.2 Offres IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile et IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

Les offres IBM Security Trusteer Pinpoint Criminal Detection for Mobile («PPCD Mobile») sont conçues pour fournir une couche de protection supplémentaire et visent à prévenir les prises de contrôle de comptes et les activités frauduleuses en identifiant les accès illicites aux comptes et en fournissant une recommandation au Client. Cette offre de Logiciel-service IBM recueille de l'information qui provient à la fois de l'Application d'affaires ou de vente au détail du Client utilisant l'interface de programmation d'applications de PPCD Mobile, et des appareils mobiles des Participants admissibles. Les offres IBM Security Trusteer PPCD Mobile sont conçues pour établir une corrélation entre l'information complexe liée aux appareils mobiles des Participants admissibles et d'autres sources de données, comme les incidents en temps réel d'infection par un programme malveillant et d'hameçonnage, qui sont intégrées par l'intermédiaire d'autres offres de Logiciel-service IBM spécifiées dans les présentes Conditions d'utilisation.

Le Client peut accéder aux offres IBM Security Trusteer PPCD Mobile et les utiliser dans l'environnement infonuagique hébergé d'IBM Security Trusteer, puis recevoir, depuis les appareils mobiles des Participants admissibles, des données sur les évaluations des risques générées à la suite des interactions en ligne entre ces appareils mobiles et l'Application d'affaires ou de vente au détail du Client pour laquelle le Client s'est abonné aux offres de Logiciel-service IBM. Aux fins de ces offres, le terme «appareils mobiles» englobe seulement les téléphones cellulaires et les tablettes et non les ordinateurs portables (PC ou Mac).

3.2.3 Offres IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition, IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition, IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition et IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Ces offres permettent la détection sans logiciel client de navigateurs infectés par un programme financier malveillant de type MitB qui se connectent à une Application d'affaires ou de vente au détail. Les offres IBM Security Trusteer Pinpoint Malware Detection fournissent une couche de protection supplémentaire et visent à permettre aux organisations de se concentrer sur les processus de prévention des fraudes qui sont basés sur les risques des programmes malveillants, en fournissant au Client des évaluations et des alertes de présence d'un programme financier malveillant de type MitB.

a. Données sur les événements

Le Client et un nombre illimité de membres de son personnel autorisés peuvent utiliser l'application TMA pour recevoir des données sur les événements générées à la suite des interactions en ligne des Participants admissibles avec l'Application d'affaires ou de vente au détail du Client.

b. Édition évoluée

L'édition évoluée («Advanced Edition») pour les Applications d'affaires ou de vente au détail fournit une couche supplémentaire pour la détection et la protection, qui est ajustée et personnalisée en fonction de la structure et du flux des Applications d'affaires et de vente au détail du Client. L'édition évoluée peut aussi être personnalisée selon le type de menaces spécifiques auxquelles le Client doit faire face. Ces éditions peuvent être incorporées à divers endroits des Applications d'affaires ou de vente au détail du Client.

L'édition évoluée est offerte au Client par tranche minimale de cent mille (100 000) Participants admissibles, pour les Applications de vente au détail, et par tranche de dix mille (10 000) Participants admissibles pour les Applications d'affaires, ce qui revient à mille (1 000) tranches de cent (100) Participants admissibles pour les Applications de vente au détail ou à mille (1 000) tranches de dix (10) Participants admissibles pour les Applications d'affaires.

c. Édition standard

L'édition standard pour les Applications d'affaires ou de vente au détail est une solution à déploiement rapide qui fournit les fonctions de base de cette offre de Logiciel-service IBM, comme décrit aux présentes.

3.3 Offres de Logiciel-service IBM supplémentaires facultatives pour IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition, IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition, IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition et IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Pour les offres IBM Security Trusteer Rapport Remediation for Retail, il faut au préalable obtenir le Logiciel-service IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition ou IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition.

Dans le cas de l'offre IBM Security Trusteer Pinpoint Carbon Copy for Retail, il faut au préalable obtenir le Logiciel-service IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition ou IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition. Pour ce qui est de l'offre IBM Security Trusteer Pinpoint Carbon Copy for Business, il faut au préalable obtenir le Logiciel-service IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition ou IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition.

3.3.1 Offres IBM Security Trusteer Pinpoint Carbon Copy for Business et IBM Security Trusteer Pinpoint Carbon Copy for Retail

Les offres IBM Security Trusteer Pinpoint Carbon Copy sont conçues pour fournir une couche de protection supplémentaire et un service de surveillance qui peuvent aider à déterminer si les justificatifs d'identité d'un Participant admissible ont été compromis par des attaques d'hameçonnage dans les Applications de vente au détail ou d'affaires du Client pour lesquelles le Client s'est abonné aux offres de Logiciel-service IBM.

3.3.2 Offre IBM Security Trusteer Rapport Remediation for Retail

Le Logiciel-service IBM Security Trusteer Rapport Remediation for Retail a pour but d'investiguer les infections par un programme malveillant de type MitB dans un navigateur d'un ordinateur (PC ou Mac) d'un Participant admissible qui accède de manière ponctuelle à l'Application de vente au détail du Client, d'appliquer des mesures de réparation, de bloquer et de retirer ce type d'infection qui a été détecté par les données sur les événements du Logiciel-service IBM Security Trusteer Pinpoint Malware Detection. Le Client doit être abonné au Logiciel-service IBM Security Trusteer Pinpoint Malware Detection qui s'exécute dans l'Application de vente au détail du Client. Le Client peut utiliser cette offre de Logiciel-service IBM seulement en lien avec les Participants admissibles qui accèdent à l'Application de vente au détail du Client, et uniquement comme outil dont le but consiste à investiguer et à réparer un appareil infecté (PC ou Mac) en particulier, de manière ponctuelle. Le Logiciel-service IBM Security Trusteer Rapport Remediation for Retail doit dans les faits s'exécuter dans l'appareil du Participant admissible (PC ou Mac), et ce Participant admissible doit accepter le CLUF, avoir été authentifié au moins une (1) fois par la ou les Applications de vente au détail, et la configuration du Client doit inclure l'ensemble des ID utilisateurs. Afin de dissiper tout doute, cette offre de Logiciel-service IBM n'inclut pas le droit d'utiliser la Page de garde Trusteer ou de faire la promotion du Logiciel client du titulaire de compte de toute autre façon à la population générale de Participants admissibles du Client.

4. Offres IBM Security Trusteer Mobile

4.1 Offres IBM Security Trusteer Mobile Browser for Business et IBM Security Trusteer Mobile Browser for Retail

Le Logiciel-service IBM Security Trusteer Mobile Browser est conçu pour fournir une couche de protection supplémentaire et vise à assurer un accès en ligne sécurisé pour les appareils mobiles des Participants admissibles qui accèdent aux Applications de vente au détail ou d'affaires du Client pour lesquelles le Client s'est abonné aux offres de Logiciel-service IBM. Ce Logiciel-service fournit aussi une évaluation des risques des appareils et une protection contre l'hameçonnage. La détection des connexions Wi-Fi sécurisées est disponible uniquement pour les plateformes Android. Aux fins de la présente offre de Logiciel-service IBM, le terme «appareils mobiles» englobe seulement les téléphones cellulaires et les tablettes et non les ordinateurs portables (PC ou Mac).

En utilisant l'application TMA, le Client et un nombre illimité de membres de son personnel autorisés peuvent recevoir des données sur les événements, des analyses et des statistiques qui concernent les Appareils pour lesquels les Participants admissibles : (i) ont téléchargé le Logiciel client du titulaire de compte, une application autorisée sans frais pour le public aux termes d'un contrat de licence utilisateur final («CLUF») et téléchargeable dans les appareils mobiles des Participants admissibles; (ii) ont accepté le CLUF et ont été authentifiés au moins une (1) fois par les Applications d'affaires ou de vente au détail du Client pour lesquelles le Client s'est abonné aux offres de Logiciel-service IBM. Le Client peut mettre en marché le Logiciel client du titulaire de compte uniquement en utilisant la Page de garde Trusteer. Le Client n'est pas autorisé à utiliser le Logiciel client du titulaire de compte pour ses activités d'entreprise internes.

a. Données sur les événements

Le Client et un nombre illimité de membres de son personnel autorisés peuvent utiliser l'application TMA pour recevoir des données sur les événements générées à la suite des interactions en ligne des appareils mobiles avec l'Application d'affaires ou de vente au détail pour laquelle le Client s'est abonné aux offres de Logiciel-service IBM.

b. Page de garde Trusteer

La plateforme de mise en marché de la Page de garde Trusteer identifie le Logiciel client du titulaire de compte et le met en marché auprès des Participants admissibles qui accèdent à l'Application d'affaires ou de vente au détail du Client pour laquelle le Client s'est abonné aux offres de Logiciel-service IBM. Le Client peut choisir sa page de garde dans un ensemble de modèles disponibles («Modèle de page de garde»). Il est possible de personnaliser une page de garde aux termes d'un contrat distinct ou d'une description du travail séparée.

Le Client peut décider de fournir ses marques de commerce, logos et icônes afin de les utiliser en lien avec l'application TMA, mais seulement avec la Page de garde Trusteer et aux fins d'affichage dans le Logiciel client du titulaire de compte ou dans les Pages de renvoi hébergées par IBM ou sur le site Web d'IBM Security Trusteer. Toute utilisation de ces marques de commerce, logos et icônes se fera

conformément aux politiques raisonnables d'IBM concernant l'utilisation de la publicité et des marques de commerce.

4.2 Offres IBM Security Trusteer Mobile SDK for Business et IBM Security Trusteer Mobile SDK for Retail

Les offres de Logiciel-service IBM Security Trusteer Mobile SDK sont conçues pour fournir une couche de protection supplémentaire et visent à assurer un accès Web sécurisé aux Applications d'affaires et de vente au détail du Client pour lesquelles le Client s'est abonné aux offres de Logiciel-service IBM, ainsi qu'une évaluation des risques des appareils et une protection contre le détournement d'adresses. La détection des connexions Wi-Fi sécurisées est disponible uniquement pour les plateformes Android.

Les offres IBM Security Trusteer Mobile SDK comprennent une trousse exclusive destinée aux développeurs de logiciels mobiles («Trousse SDK»), un progiciel contenant de la documentation, des bibliothèques de logiciels exclusives pour la programmation et d'autres fichiers et articles connexes, aussi appelée «IBM Security Trusteer mobile library», ainsi que le «Composant d'exécution» ou le «Code redistribuable», qui est un code exclusif généré par le Logiciel-service IBM Security Trusteer Mobile SDK qui peut être intégré aux applications mobiles iOS ou Android autonomes et protégées du Client pour lesquelles le Client s'est abonné aux offres de Logiciel-service IBM («Applications mobiles intégrées du Client»).

Le Logiciel-service IBM Security Trusteer Mobile SDK for Retail est offert par tranche de cent (100) Participants admissibles ou par tranche de cent (100) Appareils du Client. Pour sa part, le Logiciel-service IBM Security Trusteer Mobile SDK for Business est disponible par tranche de dix (10) Participants admissibles ou par tranche de dix (10) Appareils du Client.

L'application TMA permet au Client et à un nombre illimité de membres de son personnel autorisés de recevoir des données sur les événements et des évaluations des tendances en matière de risques. L'Application mobile intégrée du Client permet au Client de recevoir des données sur les analyses de risques et sur les appareils mobiles des Participants admissibles qui ont téléchargé cette même application. Aux fins de ces offres, le terme «appareils mobiles» englobe seulement les téléphones cellulaires et les tablettes et non les ordinateurs portables (PC ou Mac).

Le Client peut :

- a. utiliser à l'interne le Logiciel-service IBM Security Trusteer Mobile SDK seulement pour développer des Applications mobiles intégrées du Client;
- b. imbriquer le Code redistribuable (seulement en format de code exécutable) dans une Application mobile intégrée du Client, en tant que composant intégral inséparable. Toute portion modifiée ou fusionnée du Code redistribuable aux termes de la licence qui est accordée aux présentes est régie par les présentes Conditions d'utilisation; et
- c. mettre en marché et distribuer le Code redistribuable aux fins de téléchargement dans les appareils mobiles des Participants admissibles ou du Client, sous réserve des dispositions suivantes :
 - Sauf autorisation expresse prévue au présent Contrat, le Client convient de ne pas 1) utiliser, copier, modifier ou distribuer la Trousse SDK; 2) convertir le langage machine en langage assembleur ou compilateur ou traduire autrement la Trousse SDK, sauf comme le permet expressément la loi sans possibilité de renonciation contractuelle; 3) concéder en sous-licence, louer ou donner à bail la Trousse SDK; 4) retirer les fichiers de mention légale ou de droit d'auteur contenus dans le Code redistribuable; 5) utiliser le même nom de chemin que celui des fichiers/modules du Code redistribuable d'origine; et 6) utiliser les noms ou les marques de commerce d'IBM, de ses concédants de licences ou de ses agents de distribution dans le cadre de la mise en marché de l'Application mobile intégrée du Client, sans obtenir au préalable leur consentement écrit.
 - Le Code redistribuable doit demeurer intégré de manière inséparable à l'Application mobile intégrée du Client. Le Code redistribuable doit être sous forme de code exécutable et respecter toutes les indications, instructions et spécifications fournies dans la Trousse SDK et la documentation y afférente. Le contrat de licence utilisateur final pour l'Application mobile intégrée du Client doit aviser l'utilisateur final que le Code redistribuable ne peut pas i) servir à une autre fin que l'activation de l'Application mobile intégrée du Client; ii) être copié (sauf aux fins de sauvegarde); iii) être redistribué ou transféré; ou iv) faire l'objet d'une conversion du langage machine en langage assembleur ou compilateur, ni être traduit autrement, sauf comme le permet la loi, sans possibilité de renonciation contractuelle. Le contrat de licence du

Client doit protéger IBM au moins dans la même mesure que les modalités du présent Contrat.

- La Trousse SDK peut uniquement être déployée dans le cadre du développement et des tests à l'interne du Client sur les appareils de test mobile désignés du Client. Le Client n'est pas autorisé à utiliser la Trousse SDK pour traiter des charges de travail de production, simuler des charges de travail de production ou tester l'évolutivité de tout code, application ou système. Le Client n'est pas autorisé à utiliser toute partie de la Trousse SDK à quelque autre fin que ce soit.

Le Client est responsable de toute l'assistance technique pour l'Application mobile intégrée du Client et de toutes les modifications qu'il apporte au Code redistribuable; tel qu'il y est autorisé aux termes des présentes.

Le Client est autorisé à installer et à utiliser le Code redistribuable et la trousse du Logiciel-service IBM Security Trusteer Mobile SDK seulement pour permettre son utilisation de l'offre de Logiciel-service IBM.

IBM a testé des applications créées avec les outils mobiles fournis dans la trousse du Logiciel-service IBM Security Trusteer Mobile SDK («Outils mobiles») pour vérifier si elles s'exécutaient correctement sous certaines versions de systèmes d'exploitation mobiles, comme ceux d'Apple (iOS) et de Google (Android), collectivement appelés «plateformes de systèmes d'exploitation mobiles». Cependant, les plateformes de systèmes d'exploitation mobiles sont fournies par des tiers, ne sont pas sous le contrôle d'IBM et peuvent être modifiées sans qu'IBM en soit avisée. Par conséquent et nonobstant toute indication contraire, IBM ne garantit pas que les applications ou d'autres œuvres créées à l'aide des Outils mobiles fonctionneront correctement avec les plateformes de systèmes d'exploitation mobiles ou les appareils mobiles, ni qu'elles seront compatibles ou qu'elles pourront interagir avec de telles plateformes ou de tels appareils.

Le Client convient de créer, de conserver et de fournir à IBM et à ses vérificateurs des dossiers écrits, des résultats d'outils de système et d'autre information sur les systèmes qui sont exacts et suffisants pour permettre de vérifier que l'utilisation que fait le Client de la trousse du Logiciel-service IBM Security Trusteer Mobile SDK respecte les modalités des présentes Conditions d'utilisation.

5. Déploiement des offres de Logiciel-service IBM pour la protection contre les fraudes

L'abonnement de base du Client couvre les activités de mise en place et de déploiement initial requises, dont le démarrage unique initial, la configuration, le modèle de Page de garde, les essais et la formation.

Il est possible d'obtenir d'autres services, moyennant des frais supplémentaires, en concluant un contrat distinct.

Annexe B

La présente Entente de niveau de service sur la disponibilité s'applique au Logiciel-service IBM si elle est spécifiée dans le Document transactionnel du Client.

C'est la version de cette Entente de niveau de service qui est en vigueur au début du terme de l'abonnement du Client ou lors de son renouvellement qui s'appliquera. Le Client comprend que cette entente de niveau de service ne constitue pas une garantie qui lui est offerte.

1. Définitions

- a. **Réclamant autorisé** – Personne désignée par le Client, qui est autorisée à soumettre des Réclamations en vertu de la présente Entente de niveau de service.
- b. **Crédit pour la disponibilité** – Recours qu'IBM accorde pour une Réclamation validée. Ce recours s'appliquera sous la forme d'un crédit ou d'une remise sur une facture à venir des frais d'abonnement pour le Logiciel-service IBM.
- c. **Réclamation** – Réclamation que le Réclamant autorisé du Client soumet à IBM, conformément à la présente Entente de niveau de service, selon laquelle un Niveau de service n'a pas été respecté au cours d'un Mois de la période contractuelle.
- d. **Mois de la période contractuelle** – Chaque mois complet durant la période d'utilisation du Logiciel-service IBM, calculé à partir de 0 h (temps universel) le premier jour du mois, jusqu'à 23 h 59 (temps universel) le dernier jour du mois.
- e. **Client** – Entité qui s'abonne au Logiciel-service IBM directement auprès d'IBM et qui respecte toutes ses obligations importantes, y compris ses obligations de paiement, aux termes du contrat conclu avec IBM pour le Logiciel-service IBM.
- f. **Temps d'arrêt** – Période pendant laquelle le traitement du système de production a cessé pour le Service et empêche l'ensemble des utilisateurs du Client d'utiliser tous les aspects du Service pour lesquels ils disposent des droits d'utilisation appropriés. Le Temps d'arrêt n'inclut pas le temps pendant lequel le Service n'est pas disponible en raison des circonstances suivantes :
 - Temps d'arrêt prévu du système;
 - Cas de force majeure;
 - Problèmes avec les applications, l'équipement ou les données du Client ou d'un tiers;
 - Actes ou omissions du Client ou d'un tiers (y compris toute personne qui accède au Logiciel-service IBM au moyen des mots de passe ou de l'équipement du Client);
 - Non-respect des configurations requises du système et des plateformes prises en charge pour accéder au Logiciel-service IBM; ou
 - Respect par IBM des conceptions, des spécifications ou des instructions fournies par le Client ou par un tiers au nom du Client.
- g. **Événement** – Circonstance ou ensemble de circonstances pris collectivement, ayant pour conséquence le non-respect d'un Niveau de service.
- h. **Cas de force majeure** – Cas fortuit, acte de terrorisme, action syndicale, incendie, inondation, tremblement de terre, émeute, guerre, actes, ordonnances ou restrictions d'un gouvernement, virus, attaques par déni de service et autres conduites malveillantes, défaillances des services publics ou de la connectivité aux réseaux, ou toute autre cause entraînant l'indisponibilité du Logiciel-service IBM qui est indépendante de la volonté raisonnable d'IBM.
- i. **Temps d'arrêt prévu du système** – Interruption prévue du Logiciel-service IBM aux fins de maintenance.
- j. **Niveau de service** – Norme définie ci-après selon laquelle IBM mesure le niveau de service qu'elle fournit dans la présente Entente de niveau de service.

2. Crédits pour la disponibilité

- a. Afin d'être admissible à soumettre une Réclamation, le Client doit avoir ouvert un dossier d'assistance pour chaque Événement au centre d'assistance à la clientèle IBM pour le Logiciel-service IBM applicable, conformément à la procédure d'IBM relative à la signalisation de problèmes de Gravité 1. Le Client doit fournir toute l'information détaillée nécessaire au sujet de l'Événement et apporter l'aide raisonnable à IBM pour établir le diagnostic et résoudre l'Événement, dans la mesure requise pour les dossiers d'assistance de Gravité 1. Ces dossiers d'assistance doivent être soumis dans les vingt-quatre (24) heures après que le Client a constaté pour la première fois que l'Événement a eu une incidence sur son utilisation du Logiciel-service IBM.
- b. Le Réclamant autorisé du Client doit soumettre la Réclamation relative à un Crédit pour la disponibilité au plus tard dans les trois (3) jours ouvrables suivant la fin du Mois de la période contractuelle qui fait l'objet de la Réclamation.
- c. Le Réclamant autorisé du Client doit fournir à IBM tous les détails raisonnables concernant la Réclamation, y compris, notamment, une description détaillée de tous les Événements pertinents, ainsi que le Niveau de service qui n'a prétendument pas été respecté.
- d. IBM calculera le Temps d'arrêt total global au cours de chaque Mois de la période contractuelle applicable au Niveau de service indiqué dans le tableau ci-dessous. Les Crédits pour la disponibilité seront calculés d'après la durée du Temps d'arrêt mesurée à partir du moment où le Client signale que le Temps d'arrêt a eu une incidence sur ses activités pour la première fois. Si le Client signale un Événement relatif à un Temps d'arrêt des Applications et un Événement relatif à un Temps d'arrêt du traitement des données entrantes qui ont lieu en même temps, IBM traitera les périodes de Temps d'arrêt qui se chevauchent comme une seule période plutôt que deux périodes distinctes. Pour chacune des Réclamations valides, IBM appliquera le Crédit pour la disponibilité le plus élevé en se basant sur le Niveau de service atteint au cours de chaque Mois de la période contractuelle, comme il est indiqué dans les tableaux ci-dessous. IBM n'accordera pas de multiples Crédits pour la disponibilité concernant les mêmes Événements au cours du même Mois de la période contractuelle.
- e. Dans le cas des Forfaits (Logiciels-services IBM individuels offerts en groupe à un seul prix global), le Crédit pour la disponibilité sera calculé en se basant sur le prix mensuel global du Forfait et non en fonction des frais d'abonnement mensuels pour chaque Logiciel-service IBM composant le Forfait. Le Client peut seulement soumettre des Réclamations pour un (1) seul Logiciel-service IBM dans un Forfait pour tout Mois de la période contractuelle. IBM n'accordera pas de Crédits pour la disponibilité pour plus d'un (1) Logiciel-service IBM dans un Forfait au cours d'un Mois de la période contractuelle quelconque.
- f. Si le Client a acheté le Logiciel-service IBM auprès d'un intermédiaire IBM valide dans le cadre d'une transaction de remise en marché où IBM assume la responsabilité primaire pour l'exécution du Logiciel-service IBM et les engagements relatifs à l'Entente de niveau de service, le Crédit pour la disponibilité sera alors calculé d'après le Prix de volume suggéré (prix RSVP) pour le Logiciel-service IBM en vigueur au cours du Mois de la période contractuelle faisant l'objet d'une Réclamation, auquel s'appliquera un escompte de cinquante pour cent (50 %).
- g. Le montant total des Crédits pour la disponibilité accordés au cours de tout Mois de la période contractuelle ne pourra en aucune circonstance excéder dix pour cent (10 %) d'un douzième (1/12^e) des frais annuels que le Client a payés à IBM pour le Logiciel-service IBM.
- h. IBM fera preuve de jugement raisonnable pour valider les Réclamations, en se fondant sur l'information contenue dans ses dossiers, laquelle prévaudra en cas de divergence avec les données des dossiers du Client.
- i. **LES CRÉDITS POUR LA DISPONIBILITÉ QUI SONT ACCORDÉS AU CLIENT CONFORMÉMENT À LA PRÉSENTE ENTENTE DE NIVEAU DE SERVICE CONSTITUENT LES SEULS ET UNIQUES RECOURS DU CLIENT CONCERNANT TOUTE RÉCLAMATION.**

3. Niveaux de service

Disponibilité du Logiciel-service IBM au cours d'un Mois de la période contractuelle

Atteinte du Niveau de service (au cours d'un Mois de la période contractuelle)	Crédit pour la disponibilité (Pourcentage des frais d'abonnement mensuels pour un Mois de la période contractuelle visé par une Réclamation)
< 99,5 %	2 %
< 98 %	5 %
< 96 %	10 %

Le pourcentage d'«atteinte du Niveau de service» est calculé comme suit : (a) le nombre total de minutes dans un Mois de la période contractuelle, moins (b) le nombre total de minutes de Temps d'arrêt dans ce même mois, divisé par (c) le nombre total de minutes dans ce même mois. La fraction obtenue est ensuite exprimée sous la forme d'un pourcentage.

Exemple : Temps d'arrêt total de 250 minutes au cours d'un Mois de la période contractuelle

$\frac{43\,200 \text{ (nombre total de minutes dans un Mois de la période contractuelle comptant 30 jours)} - 250 \text{ minutes de Temps d'arrêt} = 42\,950 \text{ minutes}}{43\,200 \text{ (nombre total de minutes)}}$	= Crédit pour la disponibilité de 2 % pour un Niveau de service qui a été atteint dans une proportion de 99,4 % au cours du Mois de la période contractuelle
---	--

3.1 Exclusions

La présente Entente de niveau de service est offerte uniquement aux Clients d'IBM. Elle ne s'applique pas dans les cas suivants :

- Les Services en version bêta ou d'essai.
- Les environnements hors production, notamment, les environnements d'essai, de reprise après sinistre, d'assurance de la qualité ou de développement.
- Les Réclamations faites par un utilisateur, un invité ou un participant du Client d'IBM autorisé à utiliser le Logiciel-service IBM.
- Le non-respect de la part du Client de ses obligations substantielles aux termes des Conditions d'utilisation, notamment de ses obligations de paiement.