IBM Security Trusteer Fraud Protection

Les Conditions d'Utilisation regroupent les présentes Conditions d'Utilisation IBM – Conditions Spécifiques de l'Offre SaaS (« Conditions Spécifiques de l'Offre SaaS ») et un document intitulé Conditions d'Utilisation IBM – Conditions Générales (« Conditions Générales ») disponibles à l'adresse URL suivante : http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

En cas de conflit, les Conditions Spécifiques de l'Offre IBM SaaS prévalent sur les Conditions Générales. En accédant à l'Offre IBM SaaS, en la commandant ou en l'utilisant, le Client de l'Offre IBM SaaS accepte les présentes Conditions d'Utilisation.

Les Conditions d'Utilisation sont régies par le Contrat International IBM Passport Advantage, le Contrat International IBM Passport Advantage Express ou le Contrat International IBM relatif à une Sélection d'Offres IBM SaaS, selon le cas (ci-après le « Contrat ») qui, avec les Conditions d'Utilisation, représentent l'intégralité de l'accord entre les parties.

1. Offres IBM SaaS

Les Conditions Spécifiques de l'Offre SaaS s'appliquent aux Offres IBM SaaS suivantes :

1.1 Offres IBM SaaS - 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 IBM SaaS - 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
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 Offres IBM SaaS - 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. Unités de mesure des redevances

L'Offre IBM SaaS est vendue en fonction d'une des unités de mesure de redevance suivantes dans le Document de Transaction :

a. **Participant Eligible** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Tout individu ou entité habilité à prendre part à un programme de prestation de service géré ou suivi par l'Offre IBM SaaS constitue un Participant Admissible. Des Droits d'Utilisation suffisants doivent être obtenus pour couvrir tous les Participants Admissibles gérés ou suivis dans l'Offre IBM SaaS pendant la période de mesure indiquée dans le Document de Transaction du Client.

Chaque programme de prestation de service géré par l'Offre IBM SaaS est analysé séparément puis ajouté ensemble. Les personnes physiques ou morales éligibles à plusieurs programmes de prestation de service nécessitent des Droits d'Utilisation distincts.

Pour ces offres, un programme de prestation de service comprend une Application Business ou Retail unique du Client, comprenant une page de connexion principale ainsi que des pages associées pour chaque Application Business ou Retail. Un Participant Admissible est un Utilisateur Final d'un Client, qui dispose de données de connexion sur l'Application Business ou Retail.

b. **Unité Client** : unité de mesure par laquelle l'offre IBM SaaS peut être acquise. Une Unité Client est un système informatique utilisateur unique ou un capteur spécial ou une unité de télémétrie demandant l'exécution de, ou recevant à des fins d'exécution, un ensemble de commandes, de procédures ou d'applications à partir de ou fournissant des données à un autre système informatique qui est généralement désigné par serveur ou géré par le serveur. Plusieurs Unités Client peuvent partager l'accès à un serveur commun. Une Unité Client peut être dotée de certaines fonctionnalités de traitement ou peut être programmable afin de permettre à un utilisateur d'effectuer le travail. Le Client doit se procurer des Droits d'Utilisation pour chaque Unité Client qui exécute l'Offre IBM SaaS, lui fournit des données, utilise des services fournis par l'Offre IBM SaaS ou autrement accède à l'Offre IBM SaaS pendant la période de mesure indiquée dans le Document de Transaction du Client.

3. Redevances et Facturation

Le montant à régler pour l'Offre IBM SaaS est indiqué dans un Document de Transaction.

3.1 Redevances Mensuelles Partielles

Une redevance mensuelle partielle, comme indiqué dans le Document de Transaction, peut être estimée au prorata.

4. Conformité et Audit

L'accès aux offres IBM Security Trusteer Fraud Protection est soumis à un nombre maximal de Participants Admissibles ou d'Unités Client, comme indiqué dans le Document de Transaction. Le Client est tenu de s'assurer que le nombre de ses Participants Admissibles ou Unités Client ne dépasse pas le nombre maximal indiqué dans le Document de Transaction.

Un audit peut être mené pour vérifier le respect du nombre maximal de Participants Admissibles ou d'Unités Client.

5. Options de Renouvellement de la Période d'Abonnement à l'Offre IBM SaaS

Le Document de Transaction du Client indiquera si l'Offre IBM SaaS sera renouvelée à la fin de la Période d'Abonnement, en désignant l'une des options suivantes :

5.1 Renouvellement automatique

Si le Document de Transaction du Client indique que le renouvellement est automatique, le Client est autorisé, moyennant une demande écrite adressée à l'Ingénieur commercial IBM ou au Partenaire Commercial IBM du Client, à résilier la Période d'Abonnement à l'Offre IBM SaaS arrivant à expiration, au moins quatre-vingt-dix (90) jours avant la date d'expiration, comme indiqué dans le Document de Transaction. Si IBM ou son Partenaire Commercial IBM ne reçoit pas ladite notification de résiliation avant la date d'expiration, la Période d'Abonnement arrivant à expiration sera automatiquement renouvelée pour un an ou pour la même durée que celle de la Période d'Abonnement, telle qu'elle est stipulée dans le Document de Transaction.

5.2 Facturation continue

Lorsque le Document de Transaction indique que la facturation du Client est continue, le Client continuera à avoir accès à l'Offre IBM SaaS et sera facturé pour l'utilisation de l'Offre IBM SaaS au moyen d'une facturation continue. Pour cesser d'utiliser l'Offre IBM SaaS et d'arrêter le processus de facturation continue, le Client doit fournir à IBM ou à son Partenaire Commercial IBM une notification écrite de quatre-vingt-dix (90) jours demandant l'annulation de son Offre IBM SaaS. Une fois l'accès du Client annulé, le Client sera facturé pour toutes les redevances d'accès impayées jusqu'au mois au cours duquel l'annulation a pris effet.

5.3 Renouvellement Requis

Lorsque le Document de Transaction indique que le renouvellement du Client est de type « résiliation », l'Offre IBM SaaS sera résiliée à la fin de la Période d'Abonnement et l'accès du Client à l'Offre IBM SaaS sera supprimé. Pour continuer d'utiliser l'Offre IBM SaaS au-delà de la date de fin, le Client doit passer une commande auprès de l'ingénieur commercial IBM ou du Partenaire Commercial IBM du Client pour acheter une nouvelle Période d'Abonnement.

6. Support Technique

Le Support Technique de l'Offre IBM SaaS est accessible au Client et à ses Participants Admissibles pour les aider à utiliser l'Offre IBM SaaS.

Le Support Standard est compris dans l'abonnement à toutes les offres. Trusteer Rapport Mandatory Service, un additif à Trusteer Rapport, requiert au préalable le Support Premium pour l'abonnement de base à Trusteer Rapport.

Pour chaque Offre IBM SaaS, un abonnement au Support Premium est disponible moyennant un supplément, à l'exception des offres IBM Security Trusteer Mobile SDK et IBM Security Trusteer Rapport Mandatory Service.

Support Standard :

- Assistance de 8h00 à 17h00, heure locale.
- Les Clients et leurs Participants Admissibles peuvent soumettre des tickets de support par voie électronique, comme détaillé dans le Guide de Support SaaS [Software as a Service].
- Les Clients peuvent accéder au Portail de Support Client pour consulter les notifications, la documentation, les rapports d'utilisation et les questions/réponses à l'adresse suivante : http://www-01.ibm.com/software/security/trusteer/support/.
- Pour les options et les détails de support, accédez au Guide de Support IBM SaaS [Software as a Service] à l'adresse suivante : http://www-01.ibm.com/software/support/handbook.html.

Support Premium :

- Assistance 24 heures sur 24 et 7 jours sur 7 pour tous les niveaux de gravité.
- Les Clients peuvent accéder au service d'assistance directement par téléphone.
- Les Clients et leurs Participants Admissibles peuvent soumettre des tickets de support par voie électronique, comme détaillé dans le Guide de Support SaaS [Software as a Service].
- Les Clients peuvent accéder au Portail de Support Client pour consulter les notifications, la documentation, les rapports d'utilisation et les questions/réponses à l'adresse suivante : http://www-01.ibm.com/software/security/trusteer/support/.
- Pour les options et les détails de support, accédez au Guide de Support IBM SaaS [Software as a Service] à l'adresse suivante : http://www-01.ibm.com/software/support/handbook.html.

7. Dispositions supplémentaires spécifiques à l'Offre IBM SaaS

7.1 Conformité Safe Harbor

IBM se soumet aux principes américano-européens (US-UE) de Safe Harbor établis par le Department of Commerce des États-Unis en coordination avec la Commission Européenne. Les produits IBM Security Trusteer sont inclus dans la certification US-EU de Safe Harbor d'IBM. Des informations complémentaires sur Safe Harbor et la liste des sociétés Safe Harbor sont disponibles à l'adresse suivante : http://export.gov/safeharbor/.

7.2 Augmentation du Montant Annuel de l'Abonnement du Client

IBM se réserve le droit d'ajuster le montant de l'abonnement à l'Offre IBM SaaS au maximum une fois tous les douze (12) mois d'un pourcentage à déterminer par IBM et n'excédant pas 3 %. L'ajustement du montant de l'abonnement prendra effet à la date anniversaire de début de la période de couverture initiale. Cet ajustement ne modifie pas le droit d'utilisation de l'Offre IBM SaaS par le Client ou l'unité de mesure des redevances par laquelle l'Offre IBM SaaS est acquise. Les Partenaires commerciaux IBM sont indépendants d'IBM et déterminent unilatéralement leurs prix et modalités.

7.3 Support Premium

Le Client n'a droit au Support Premium que pour les Offres IBM SaaS pour lesquelles le Client a souscrit à l'offre de Support Premium associée.

7.4 Utilisation et Autorisation Légales

Autorisation de Collecte et de Traitement de Données

L'Offre IBM SaaS est conçue pour aider le Client à améliorer son environnement et ses données de sécurité. L'Offre IBM SaaS collectera des informations auprès des Participants Admissibles et des Unités Client qui interagissent avec les Applications Business ou Retail pour lesquelles le Client a souscrit aux Offres IBM SaaS couvertes. L'Offre IBM SaaS collecte des informations qui, seules ou conjointement, peuvent être considérées comme Données Personnelles dans certaines juridictions. Par « Données Personnelles », on entend toute information permettant d'identifier une personne, telle que le nom, l'adresse électronique, l'adresse personnelle ou le numéro de téléphone, fournie à IBM à des fins de stockage, de traitement ou de transfert pour le compte du Client.

Les procédures de collecte et de traitement de données peuvent être mises à jour pour améliorer les fonctionnalités de l'Offre IBM SaaS. Un document contenant une description complète des procédures de collecte et de traitement de données est mis à jour selon les besoins et est mis à la disposition du Client à la demande. Le Client autorise IBM à collecter ces informations et à les traiter conformément aux Clauses « Transferts Hors du Territoire » et « Confidentialité des Données » des présentes Conditions d'Utilisation et à la Clause « Confidentialité et Sécurité des Données » des Dispositions Générales des Conditions d'Utilisation.

Pour les Offres IBM Security Trusteer Pinpoint :

Les données collectées peuvent comprendre l'adresse IP de l'utilisateur, l'ID utilisateur chiffré ou haché unidirectionnel, des cookies de domaine s'ils ne sont pas filtrés, des visites d'Applications protégées et de sites de « phishing », l'emplacement géographique, ainsi que des données d'identification entrées dans les sites de « phishing ».

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

Les données collectées peuvent comprendre l'adresse IP de l'utilisateur, l'ID utilisateur chiffré ou haché unidirectionnel, l'emplacement géographique, ainsi que des visites d'Applications protégées, des informations relatives à la carte SIM, le nom de l'appareil et l'affiliation Client.

Pour les Offres IBM Security Trusteer Rapport :

Les données collectées peuvent comprendre l'adresse IP de l'utilisateur, l'ID utilisateur chiffré ou haché unidirectionnel, des événements de sécurité, le nom d'utilisateur et l'adresse e-mail fournis en vue de contacter IBM pour obtenir une assistance, l'Affiliation Client, les mots de passe chiffrés entrés sur des sites protégés, des visites d'Applications protégées et de sites de « phishing », le numéro de carte de paiement chiffré, ainsi que les fichiers et données collectés à distance par le personnel IBM pour inspecter tout programme ou activité malveillant ou toute anomalie.

Consentement en connaissance de cause des Personnes Concernées :

L'utilisation de la présente Offre IBM SaaS peut être soumise à diverses lois ou réglementations. L'Offre IBM SaaS ne peut être utilisée qu'à des fins légales et de manière légale. Le Client s'engage à utiliser l'Offre IBM SaaS conformément aux lois, règlements et réglementations applicables et assume toutes les responsabilités relatives au respect desdites lois, règlements et réglementations.

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

Le Client convient qu'il a obtenu ou qu'il obtiendra tous les consentements, autorisations ou licences en pleine connaissance de cause, nécessaires pour permettre l'utilisation légale de l'Offre IBM SaaS, ainsi que la collecte et le traitement des informations par IBM par le biais de l'Offre IBM SaaS.

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

Le Client autorise IBM à obtenir des consentements en pleine connaissance de cause, nécessaires pour permettre l'utilisation de l'Offre IBM SaaS et pour collecter et traiter les informations décrites dans le Contrat de Licence d'Utilisateur Final disponible sur le site https://www.trusteer.com/support/end-user-license-agreement. Dans le cas où le Client détermine qu'il (et non IBM) traitera les communications de consentement avec les Utilisateurs Finaux, le Client convient qu'il a obtenu ou qu'il obtiendra tous les consentements, autorisations ou licences en pleine connaissance de cause, nécessaires pour permettre l'utilisation légale de l'Offre IBM SaaS et pour permettre la collecte et le traitement des informations par IBM en tant que sous-traitant du traitement des données du Client par le biais de l'Offre IBM SaaS.

7.5 Transferts Hors du Territoire

Le Client accepte qu'IBM traite le contenu, y compris toutes Données Personnelles, en vertu des lois et obligations applicables, hors du territoire à destination de sous-traitants ou sous-traitants ultérieurs du traitement des données dans les pays suivants hors de l'Espace Économique Européen et dans les pays considérés par la Commission Européenne comme ayant des niveaux de sécurité adéquats : les États-Unis.

7.6 Confidentialité des Données

Si le Client rend des Données Personnelles accessibles à l'Offre IBM SaaS dans les États Membres de l'Union Européenne, en Islande, au Liechtenstein, en Norvège ou en Suisse ou, si le Client dispose de Participants Admissibles ou d'Unités Client dans ces pays, le Client, en tant que seul responsable du traitement, désigne IBM en tant que sous-traitant du traitement des données pour traiter (ces termes étant définis dans la Directive EU 95/46/EC) les Données Personnelles. IBM ne traitera ces Données Personnelles que dans les limites requises pour mettre à disposition l'Offre IBM SaaS conformément aux descriptions publiées d'IBM de l'Offre IBM SaaS et le Client accepte que ledit traitement est conforme aux instructions du Client. IBM adressera un préavis raisonnable si elle apporte une modification significative au site du traitement ou à la façon dont elle sécurise les Données Personnelles dans le cadre de l'Offre IBM SaaS. Le Client est autorisé à résilier la Période d'Abonnement en cours pour l'Offre IBM SaaS concernée, à condition d'adresser à IBM une notification écrite dans les trente (30) jours suivant la notification par IBM de la modification au Client. Le Client accepte qu'IBM transfère du contenu, y compris des Données Personnelles, hors du territoire à destination des sous-traitants ou sous-traitants ultérieurs du traitement des données suivants :

Nom du Sous-traitant/Sous-traitant ultérieur du traitement des données	Rôle (Sous-traitant/Sous-traitant ultérieur du traitement des données)	Emplacement*
L'entité adjudicatrice IBM	Sous-traitant du traitement des données	Comme indiqué dans le Document de Transaction
Amazon Web Services LLC	Sous-traitant ultérieur du traitement de données	410 Terry Ave. N Seattle, WA 98109 États-Unis
Connectria Corp.	Sous-traitant ultérieur du traitement de données	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 États-Unis
IBM Israel Ltd.	Sous-traitant ultérieur du traitement de données	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israël
IBM Corp	Sous-traitant ultérieur du traitement de données	1 New Orchard Rd. Armonk, NY 10504 États-Unis

Le Client accepte qu'IBM pourra, sur préavis, modifier cette liste de pays d'implantation lorsqu'elle juge cela raisonnablement nécessaire pour la fourniture de l'Offre IBM SaaS.

Le Client accepte, en ce qui concerne le service fourni via le centre de données en Allemagne, comme déterminé pendant le processus de mise à disposition, qu'IBM transfère du contenu, y compris des Données Personnelles, hors du territoire à destination des sous-traitants ou sous-traitants ultérieurs du traitement des données suivants :

Nom du Sous-traitant/Sous-traitant ultérieur du traitement des données	Rôle (Sous-traitant/Sous-traitant ultérieur du traitement des données)	Emplacement*
L'entité adjudicatrice IBM	Sous-traitant du traitement des données	Comme indiqué dans le Document de Transaction
Amazon Web Services (Allemagne)	Sous-traitant ultérieur du traitement de données	Munich, Allemagne
IBM Israel Ltd.	Sous-traitant ultérieur du traitement de données	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israël

Le Client accepte, en ce qui concerne le service fourni via le centre de données au Japon, comme déterminé pendant le processus de mise à disposition, qu'IBM transfère du contenu, y compris des Données Personnelles, hors du territoire à destination des sous-traitants ou sous-traitants ultérieurs du traitement des données suivants :

Nom du Sous-traitant/Sous-traitant ultérieur du traitement des données	Rôle (Sous-traitant/Sous-traitant ultérieur du traitement des données)	Emplacement*
L'entité adjudicatrice IBM	Sous-traitant du traitement des données	Comme indiqué dans le Document de Transaction
Amazon Web Services (Japon)	Sous-traitant ultérieur du traitement de données	Tokyo, Japon
IBM Israel Ltd.	Sous-traitant ultérieur du traitement de données	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israël

* Les emplacements indiqués dans les tableaux ci-dessus incluent les adresses des bureaux du sous-traitant/sous-traitant ultérieur du traitement des données. Les centres de données sont situés dans le même pays identifié.

Les parties ou leurs sociétés affiliées concernées pourront conclure des Clauses Contractuelles Types correspondantes adoptées par la Commission Européenne, conformément à la Décision 2010/87/EU de la Commission Européenne, en supprimant les clauses facultatives. Tout différend ou obligation

découlant de ces contrats, même s'ils sont conclus par des sociétés affiliées, sera traité comme si le différend ou l'obligation existait entre les parties au titre du présent Contrat.

Annexe A

1. Offres IBM SaaS

IBM fournit ces services sous forme de services et d'offres autonomes ou de services et d'offres additionnels. Les Offres IBM SaaS spécifiques commandées sont indiquées dans l'Autorisation d'Utilisation du Client.

1.1 Définitions des termes Business et Retail

Les produits IBM Security Trusteer de protection contre la fraude sont concédés sous licence pour utilisation avec des types d'Applications spécifiques. Une Application est définie comme l'un des types suivants : Business ou Retail. Des offres distinctes sont disponibles pour les Applications Retail et les Applications Business.

- Une Application Retail est définie comme une application bancaire en ligne, une application mobile ou une application e-commerce conçue pour les consommateurs. La politique du Client peut classer certaines entreprises de petite taille comme ayant droit à l'accès Retail.
- Une Application Business est définie comme une application bancaire en ligne, une application mobile ou une application e-commerce conçue pour les sociétés, institutions ou entités équivalentes, ou toute application non classée dans la catégorie Retail.

1.2 Offres d'Abonnement de base IBM SaaS

Offres Business :

- 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 Retail :

- 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

A chacune des offres Business et Retail est associé un produit Support Premium disponible moyennant un supplément, à l'exception des offres IBM Security Trusteer Mobile SDK.

1.3 Offres d'Abonnement IBM SaaS Additionnelles pour les Offres IBM Security Trusteer Rapport

Offres Additionnelles disponibles pour 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 Additionnelles disponibles pour 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

A chacun des additifs Business et Retail des offres IBM Security Trusteer Rapport, à l'exception des additifs IBM Security Trusteer Rapport Mandatory Service, est associé un produit Support Premium disponible moyennant un supplément.

L'Abonnement aux offres IBM Security Trusteer Rapport for Business ou à IBM Security Trusteer Rapport for Retail est une condition préalable aux offres d'abonnement IBM SaaS additionnelles associées énumérées dans la présente clause.

1.4 Offres d'Abonnement IBM SaaS Additionnelles pour les Offres IBM Security Trusteer Pinpoint Malware Detection

Offres additionnelles 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 additionnelles 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

L'abonnement au Support Premium est disponible moyennant un supplément pour chacune des offres IBM SaaS additionnelles énumérées dans la présente clause.

L'Abonnement aux offres IBM Security Trusteer Pinpoint Malware Detection for Business ou IBM Security Trusteer Pinpoint Malware Detection for Retail est une condition préalable aux offres d'abonnement IBM SaaS additionnelles associées énumérées dans la présente clause.

1.5 Autres Abonnements IBM SaaS Additionnels

Tout abonnement IBM SaaS additionnel pour les abonnements de base ci-dessus non énuméré dans les présentes, qui serait actuellement disponible ou en cours de développement, n'est pas considéré comme une mise à jour et doit faire l'objet d'une concession de licence distincte.

1.6 Définitions

Détenteur de Compte : désigne l'Utilisateur Final du Client, qui a installé le logiciel d'activation client, qui a accepté le contrat de licence d'Utilisateur Final (« EULA ») et qui s'est authentifié au moins une fois sur l'Application Retail ou Business du Client pour laquelle le Client a souscrit aux Offres IBM SaaS couvertes.

Logiciel du Client Détenteur de Compte : signifie le logiciel d'activation client IBM Security Trusteer Rapport ou le logiciel d'activation client IBM Security Trusteer Mobile Browser ou tout autre logiciel d'activation client fourni avec certains abonnements IBM SaaS à des fins d'installation sur l'appareil de l'Utilisateur Final.

Trusteer Splash : désigne le splash fourni au Client sur la base des modèles de splash disponibles.

Page d'Accueil : désigne la page hébergée par IBM qui est fournie au Client avec le splash Client et le Logiciel Client téléchargeable du Détenteur de Compte.

2. Offres IBM Security Trusteer Rapport

2.1 IBM Security Trusteer Rapport for Retail et/ou IBM Security Trusteer Rapport for Business (ci-après « Trusteer Rapport »)

Trusteer Rapport fournit une couche de protection contre les attaques de phishing et de programme malveillant MitB (Man-in-the-Browse). A l'aide d'un réseau de dizaines de millions de nœuds finaux dans le monde entier, IBM Security Trusteer Rapport collecte des informations sur les attaques de phishing et de programme malveillant actives contre les organisations mondiales. IBM Security Trusteer Rapport applique des algorithmes de comportement visant à bloquer les attaques de phishing et d'empêcher l'installation et le fonctionnement de programmes malveillants MitB.

Cette Offre IBM SaaS est dotée d'une unité de mesure de prix Participant Admissible. L'offre Business est vendue par lots de 10 Participants Admissibles. L'offre Retail est vendue par lots de 100 Participants Admissibles.

Cette Offre IBM SaaS comprend :

a. Trusteer Management Application (« TMA ») :

   TMA est disponible dans l'environnement d'hébergement cloud d'IBM Security Trusteer, au moyen duquel le Client (et un nombre illimité des membres de son personnel autorisé) peut (i) recevoir la communication de données d'événements et d'évaluations de risques, (ii) visionner, configurer et déterminer des règles relatives à la communication des données d'événements et (iii) visionner la configuration du logiciel d'activation client concédé sous licence au public dans le cadre d'un contrat de licence d'Utilisateur Final (« EULA ») sans contrepartie, et rendu disponible à des fins de téléchargement sur les ordinateurs de bureau et les appareils mobiles (PC/MAC) du Participant Admissible, également désigné par suite de logiciels Trusteer Rapport (ci-après le « Logiciel du Client Détenteur de Compte »). Le Client ne pourra commercialiser le Logiciel du Client Détenteur de Compte qu'à l'aide de Trusteer Splash ou de l'API Rapport et n'est pas autorisé à utiliser le Logiciel du Client Détenteur de Compte dans le cadre de l'exploitation de ses activités commerciales internes ou à des fins d'utilisation par ses salariés (autrement que dans le cadre d'une utilisation personnelle des salariés).

b. Script Web :

   Permet sur un site Web d'accéder aux offres IBM SaaS ou de les utiliser.

c. Données d'événements :

   Le Client (et un nombre illimité des membres de son personnel autorisé) peut utiliser l'application TMA pour recevoir des données d'événements générées à partir du Logiciel du Client Détenteur de Compte par suite des interactions en ligne des Détenteurs de Compte avec son Application Business ou Retail pour laquelle le Client a souscrit aux Offres IBM SaaS couvertes. Les données d'événements seront reçues du Logiciel du Client Détenteur de Compte des Participants Admissibles en cours d'exécution sur leurs appareils, qui ont accepté le contrat EULA, qui se sont authentifiés au moins une fois sur l'Application Business ou Retail du Client, et la configuration du Client doit inclure la collection d'ID utilisateur.

d. Trusteer Splash :

   La plateforme de commercialisation Trusteer Splash identifie et commercialise le Logiciel du Client Détenteur de Compte pour les Participants Admissibles accédant aux Applications Business et/ou Retail du Client pour lesquelles ce dernier a souscrit aux Offres IBM SaaS couvertes. Le Client peut faire son choix parmi les Modèles de Splash disponibles. Le splash personnalisé peut être souscrit dans le cadre d'un contrat ou d'un descriptif de service distinct.

Le Client peut s'engager à fournir ses marques, logos ou icônes pour une utilisation dans le cadre de TMA et uniquement pour une utilisation avec Trusteer Splash et à des fins d'affichage dans le Logiciel du Client Détenteur de Compte ou sur les pages d'accueil hébergées par IBM et sur le site Web d'IBM Security Trusteer. Toute utilisation de ses marques, logos ou icônes fournis se conformera aux règles raisonnables d'IBM concernant la communication et l'utilisation des marques.

Le Client doit souscrire à l'Offre SaaS IBM Security Trusteer Rapport Mandatory Service s'il souhaite employer tout type de déploiement obligatoire du Logiciel du Client Détenteur de Compte.

Le Déploiement obligatoire du Logiciel du Client Détenteur de Compte inclut, sans s'y limiter, tout type de déploiement obligatoire à l'aide d'un mécanisme ou d'un moyen qui force directement ou indirectement un Participant Admissible à télécharger le Logiciel du Client Détenteur de Compte, ou tout outil, méthode, procédure, accord ou mécanisme n'ayant pas été élaboré ou approuvé par IBM, en vue de contourner les exigences de concession de licence de ce déploiement obligatoire du Logiciel du Client Détenteur de Compte.

2.2 Offres IBM SaaS additionnelles en option pour IBM Security Trusteer Rapport for Business et/ou IBM Security Trusteer Rapport for Retail

L'abonnement aux offres IBM Security Trusteer Rapport est une condition préalable à tout abonnement à l'une des offres IBM SaaS additionnelles ci-dessous. Si l'Offre IBM SaaS est désignée par « for Business », l'offre IBM SaaS additionnelle acquise doit également être désignée par « for Business ». Si l'Offre IBM SaaS est désignée par « for Retail », l'offre IBM SaaS additionnelle

acquise doit également être désignée par « for Retail». Le Client recevra des données d'événements des Participants Admissibles exécutant le Logiciel du Client Détenteur de Compte qui ont accepté le contrat EULA, qui se sont authentifiés au moins une fois sur les Applications Business et/ou Retail du Client, et la configuration du Client doit inclure la collection d'ID utilisateur.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business et/ou IBM Security Trusteer Rapport Fraud Feeds for Retail

Le Client (et un nombre illimité des membres de son personnel autorisé) peut utiliser l'application TMA pour recevoir des données d'événements relatives aux attaques de programmes malveillants et autres vulnérabilités de nœud final sur l'ordinateur de bureau d'un Détenteur de Compte particulier.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business et/ou IBM Security Trusteer Rapport Phishing Protection for Retail

Le Client (et un nombre illimité des membres de son personnel autorisé) peut utiliser l'application TMA pour recevoir des notifications de données d'événements relatives à la soumission des données de connexion du Détenteur de Compte à un site de phishing suspect ou un site potentiellement frauduleux. Il se peut que des applications en ligne légitimes (URL) soient signalées par erreur comme des sites de phishing et que l'Offre IBM SaaS informe les Détenteurs de Compte qu'un site légitime est un site de phishing. Dans ce cas, le Client doit notifier cette erreur à IBM qui devra la corriger. Il s'agit du seul recours du Client pour cette erreur.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business et/ou IBM Security Trusteer Rapport Mandatory Service for Retail

Le Client pourra utiliser une instance de la plateforme de commercialisation Trusteer Splash pour imposer le téléchargement du Logiciel du Client Détenteur de Compte vers les Participants Admissibles accédant aux Applications Business et/ou Retail du Client pour lesquelles ce dernier a souscrit aux Offres IBM SaaS couvertes.

IBM Security Trusteer Rapport Premium Support for Business est une condition préalable à IBM Security Rapport Mandatory Service for Business.

IBM Security Trusteer Rapport Premium Support for Retail est une condition préalable à IBM Security Rapport Mandatory Service for Retail.

Le Client ne pourra mettre en œuvre la fonctionnalité additionnelle d'IBM Security Trusteer Rapport Mandatory Service que si elle a été commandée et configurée pour utilisation avec une Application Retail ou Business du Client pour laquelle le Client a souscrit aux Offres IBM SaaS couvertes.

3. Offres IBM Security Trusteer Pinpoint

IBM Security Trusteer Pinpoint est un service Cloud conçu pour fournir une autre couche de protection et vise à détecter et atténuer les attaques de programme malveillant, les attaques de phishing et les piratages de compte. Trusteer Pinpoint peut être intégré aux Applications Business et/ou Retail du Client pour lesquelles ce dernier a souscrit aux Offres IBM SaaS couvertes et aux processus de prévention de fraude.

Cette Offre IBM SaaS comprend :

a. TMA :

   TMA est disponible dans l'environnement d'hébergement cloud d'IBM Security Trusteer, au moyen duquel le Client (et un nombre illimité des membres du personnel autorisé) peut (i) recevoir la communication de données d'événements et d'évaluations de risques et (ii) visionner, configurer et déterminer des règles en matière de sécurité et des règles relatives à la communication des données d'événements.

b. Script Web et/ou API :

   Permet le déploiement sur un site Web afin d'accéder aux Offres IBM SaaS ou de les utiliser.

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

Dans l'hypothèse d'une détection de programmes malveillants dans les offres IBM Security Trusteer Pinpoint Malware Detection ou d'une détection de piratage de compte dans les offres IBM Security Trusteer Pinpoint Criminal Detection, le Client doit se conformer au Guide des meilleures pratiques Pinpoint (Pinpoint Best Practices Guide). Le Client ne doit pas utiliser les offres IBM Security Trusteer

Pinpoint Malware Detection ou IBM Security Trusteer Pinpoint Criminal Detection d'une quelconque manière qui puisse influer sur l'expérience du Participant Admissible immédiatement après la détection d'un programme malveillant ou d'un piratage de compte, telle qu'elle puisse permettre à d'autres de corréler les actions du Client avec l'utilisation des offres IBM Security Trusteer Pinpoint (par exemple, notifications, messages, blocages d'appareils ou blocages d'accès à l'Application Business et/ou Retail immédiatement après la détection d'un programme malveillant ou d'un piratage de compte).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business et/ou IBM Security Trusteer Pinpoint Criminal Detection for Retail

Détection sans client d'une activité de piratage de compte suspecte des navigateurs qui se connectent à une Application Business ou Retail, à l'aide d'un ID appareil, détection de phishing et détection de vol des données d'identification par un programme malveillant. Les offres IBM Security Trusteer Pinpoint Criminal Detection fournissent une autre couche de protection et visent à détecter les tentatives de piratage de compte et à fournir directement au Client des scores d'évaluation de risque des navigateurs ou des appareils mobiles (par le biais du navigateur natif ou de l'application mobile du client) accédant à une Application Business ou Retail.

a. Données d'événements :

Le Client (et un nombre illimité des membres de son personnel autorisé) peut utiliser l'application TMA pour recevoir des données d'événements générées par suite des interactions en ligne des Participants Admissibles avec les Applications Business et/ou Retail du Client pour lesquelles le Client a souscrit aux Offres IBM SaaS couvertes, ou bien le Client peut recevoir les données d'événements via un mode de distribution d'API dorsale.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile et/ou 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 autre couche de protection et visent à prévenir contre les piratages de compte et les activités frauduleuses en identifiant les accès criminels aux comptes et en fournissant une recommandation au Client. Cette Offre IBM SaaS collecte des informations provenant de l'Application Business et/ou Retail du Client à l'aide de l'API PPCD Mobile et celles provenant des appareils mobiles des Participants Admissibles. Les offres IBM Security Trusteer PPCD Mobile sont conçues pour corréler des informations complexes liées aux appareils mobiles des Participants Eligibles avec d'autres sources de données, par exemple les attaques de programmes malveillants en temps réel et les incidents de phishing intégrés via les autres offres IBM SaaS d'IBM Security Trusteer indiquées dans les présentes Conditions d'Utilisation.

Le Client peut accéder aux offres IBM Security Trusteer PPCD Mobile et les utiliser dans l'environnement d'hébergement cloud d'IBM Security Trusteer pour recevoir les données des évaluations des risques à partir des appareils mobiles des Participants Admissibles, générées par suite des interactions en ligne de ces appareils mobiles avec l'Application Business ou Retail du Client pour laquelle ce dernier a souscrit aux Offres IBM SaaS couvertes. Pour les besoins de ces offres, les « appareils mobiles » n'incluent que les téléphones mobiles et les tablettes pris en charge et non les ordinateurs PC ou MAC.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition et/ou IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition et/ou IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition et/ou IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Détection sans client des navigateurs financiers MitB (Man in the Browser) infectés par un programme malveillant qui se connectent à une Application Business et/ou Retail. Les offres IBM Security Trusteer Pinpoint Malware Detection fournissent une autre couche de protection et visent à permettre aux organisations de se focaliser sur les processus de prévention de fraude basés sur le risque de programme malveillant en fournissant au Client des évaluations et des alertes concernant la présence d'un programme malveillant financier MitB.

a. Données d'événements :

Le Client (et un nombre illimité des membres de son personnel autorisé) peut utiliser l'application TMA pour recevoir des données d'événements générées par suite des interactions en ligne des Participants Admissibles avec les Applications Business et/ou Retail du Client.

b. Advanced Edition :

La version Advanced Edition des offres Business et/ou Retail fournit une autre couche de détection et de protection adaptée et personnalisée en fonction de la structure et du flux des Applications Business et/ou Retail du Client, et peut être personnalisée en fonction du paysage des menaces spécifiques ciblant le Client. Elle peut être incorporée à divers emplacements des Applications Business et/ou Retail du Client.

La version Advanced Edition est proposée au Client avec des quantités minimales d'au moins 100 000 Participants Admissibles Retail ou 10 000 Participants Admissibles Business, ce qui représente 1000 lots de 100 Participants Admissibles pour la catégorie Retail ou 1000 lots de 10 Participants Admissibles pour la catégorie Business.

c. Standard Edition :

La version Standard Edition pour la catégorie Business ou Retail est une solution rapide à déployer qui fournit les fonctionnalités principales de cette offre IBM SaaS, comme décrit dans le présent document.

3.2 Offres IBM SaaS additionnelles en option pour Security Trusteer Pinpoint Malware Detection for Business Advanced Edition et/ou IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition et/ou IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition et/ou IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition ou IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition est une condition préalable aux offres IBM Security Trusteer Rapport Remediation for Retail.

IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition ou IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition est une condition préalable à IBM Security Trusteer Pinpoint Carbon Copy for Retail. IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition ou IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition est une condition préalable à IBM Security Trusteer Pinpoint Carbon Copy for Business.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business et/ou IBM Security Trusteer Pinpoint Carbon Copy for Retail

Les offres IBM Security Trusteer Pinpoint Carbon Copy sont conçues pour fournir une autre couche de protection et un service de surveillance aidant à identifier le moment où les données d'identification d'un Participant Admissible ont été compromises par des attaques de phishing au niveau des Applications Business ou Retail du Client pour lesquelles le Client a souscrit aux Offres IBM SaaS couvertes.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail vise à identifier, résoudre, bloquer et supprimer les attaques de programme malveillant MitB (Main-in-the-Browser) sur les appareils infectés (PC/MAC) des Participants Admissibles du Client qui accèdent ponctuellement à l'Application Retail du Client où des attaques de programme malveillant MitB ont été détectées par les données d'événements d'IBM Security Trusteer Pinpoint Malware Detection. Le Client doit tenir à jour son abonnement au Service IBM Security Trusteer Pinpoint Malware Detection qui fonctionne réellement sur l'Application Retail du Client. Le Client n'est autorisé à utiliser cette offre IBM SaaS qu'en rapport avec les Participants Admissibles qui accèdent à l'Application Retail du Client et exclusivement sous forme d'outil visant à identifier et résoudre ponctuellement un appareil infecté particulier (PC/MAC). IBM Security Trusteer Rapport Remediation for Retail doit réellement s'exécuter sur l'appareil (PC/MAC) dudit Participant Admissible concerné et ce dernier doit accepter le contrat EULA, s'authentifier au moins une fois sur l'Application Retail du Client, et la configuration du Client doit inclure la collection d'ID utilisateur. Pour mémoire, cette offre IBM SaaS ne comprend pas le droit d'utilisation de Trusteer Splash et/ou de promotion du Logiciel du Client Détenteur de Compte de quelque autre manière que ce soit pour la population générale des Participants Admissibles.

4. Offres IBM Security Trusteer Mobile

4.1 IBM Security Trusteer Mobile Browser for Business et/ou IBM Security Trusteer Mobile Browser for Retail

L'offre IBM Security Trusteer Mobile Browser est conçue pour ajouter une autre couche de protection et vise à fournir l'accès en ligne sécurisé des appareils mobiles des Participants Admissibles accédant aux Applications Business ou Retail du Client pour lesquelles ce dernier a souscrit aux Offres IBM SaaS couvertes, à l'évaluation des risques des appareils mobiles et à la protection contre le phishing. La détection Wi-Fi sécurisée n'est disponible que pour les plateformes Android. Pour les besoins de cette offre IBM SaaS, les appareils mobiles incluent les téléphones mobiles ou les tablettes et non les ordinateurs portables et Mac.

TMA permet au Client (et un nombre illimité des membres de son personnel autorisé) de recevoir des données d'événements, des informations d'analyse et des statistiques relatives aux Appareils dont les Participants Admissibles (i) ont téléchargé le Logiciel du Client Détenteur de Compte, une application concédée sous licence au public dans le cadre d'un contrat de licence d'Utilisateur Final (« EULA ») sans contrepartie, et rendue disponible à des fins de téléchargement sur les appareils mobiles des Participants Admissibles, et (ii) ont accepté le contrat EULA et se sont authentifiés au moins une fois sur les Applications Business ou Retail du Client pour lesquelles le Client a souscrit aux Offres IBM SaaS couvertes. Le Client ne pourra commercialiser le Logiciel du Client Détenteur de Compte qu'à l'aide de Trusteer Splash et n'est pas autorisé à utiliser le Logiciel du Client Détenteur de Compte dans le cadre de l'exploitation de ses activités commerciales internes.

a. Données d'événements :

   Le Client (et un nombre illimité des membres de son personnel autorisé) peut utiliser l'application TMA pour recevoir des données d'événements générées par suite des interactions en lignes des appareils mobiles avec les Applications Business ou Retail du Client pour lesquelles ce dernier a souscrit aux Offres IBM SaaS couvertes.

b. Trusteer Splash :

   La plateforme de commercialisation Trusteer Splash identifie et commercialise le Logiciel du Client Détenteur de Compte pour les Participants Admissibles accédant aux Applications Business et/ou Retail du Client pour lesquelles ce dernier a souscrit aux Offres IBM SaaS couvertes. Le Client peut faire son choix parmi les modèles de splash disponibles (« Modèle de Splash »). Le splash personnalisé peut être souscrit dans le cadre d'un contrat ou d'un descriptif de service distinct.

Le Client peut s'engager à fournir ses marques, logos ou icônes pour une utilisation dans le cadre de TMA et uniquement pour une utilisation avec Trusteer Splash et à des fins d'affichage dans le Logiciel du Client Détenteur de Compte ou sur les pages d'accueil hébergées par IBM ou sur le site Web d'IBM Security Trusteer. Toute utilisation de ses marques, logos ou icônes fournis se conformera aux règles raisonnables d'IBM concernant la communication et l'utilisation des marques.

4.2 IBM Security Trusteer Mobile SDK for Business et/ou IBM Security Trusteer Mobile SDK for Retail

Les offres IBM Security Trusteer Mobile SDK sont conçues pour ajouter une autre couche de protection afin de fournir un accès Web sécurisé aux Applications Business et/ou Retail du Client pour lesquelles le Client a souscrit aux Offres IBM SaaS couvertes, à l'évaluation des risques des appareils et à la protection contre le détournement d'adresse. La détection Wi-Fi sécurisée n'est disponible que pour les plateformes Android.

Les offres IBM Security Trusteer Mobile SDK comprennent un kit d'éditeur de logiciels mobiles (« SDK ») propriétaire, un progiciel contenant de la documentation, des bibliothèques de logiciels propriétaires de programmation et d'autres fichiers et éléments associés, désignés par bibliothèque mobile IBM Security Trusteer ainsi que le « Composant d'Exécution » ou le « Composant Redistribuable », un code propriétaire généré par IBM Security Trusteer Mobile SDK qui peut être imbriqué et intégré aux applications mobiles iOS ou Android autonomes protégées du Client pour lesquelles ce dernier a souscrit aux Offres IBM SaaS couvertes (ci-après « Application Mobile Intégrée du Client »).

IBM Security Trusteer Mobile SDK for Retail est disponible par lots de 100 Participants Admissibles ou par lots de 100 Unités Client, et IBM Security Trusteer Mobile SDK for Business est disponible par lots de 10 Participants Admissibles ou par lots de 10 Unités Client.

TMA permet au Client (et à un nombre illimité des membres de son personnel autorisé) de recevoir la communication de données d'événements et les évaluations des tendances en matière de risques. L'Application Mobile Intégrée du Client permet à ce dernier de recevoir des informations d'analyse de risque et des statistiques relatives aux appareils mobiles des Participants Admissibles qui ont téléchargé l'Application Mobile Intégrée du Client, afin de permettre au Client d'élaborer une politique de lutte contre la fraude en appliquant des mesures visant à atténuer ces risques. Pour les besoins de cette offre, les « appareils mobiles » n'incluent que les téléphones mobiles et les tablettes pris en charge et non les ordinateurs PC ou MAC.

Le Client peut :

a. utiliser en interne IBM Security Trusteer Mobile SDK uniquement à des fins de développement de l'Application Mobile Intégrée du Client ;

b. intégrer le Composant Redistribuable (uniquement au format code objet), sous forme intégrale et indissociable, à l'Application Mobile Intégrée du Client. Toute partie modifiée ou fusionnée du Composant Redistribuable conformément à cette concession de licence sera soumise aux dispositions des présentes Conditions d'Utilisation ; et

c. commercialiser et distribuer le Composant Redistribuable pour téléchargement sur les appareils mobiles des Participants Admissibles ou sur le support d'Unité Client, sous réserve que :

   - Sauf autorisation expresse dans le présent Contrat, le Client n'est pas autorisé (1) à utiliser, copier, modifier ou distribuer le SDK ; (2) à désassembler, décompiler ou traduire de quelque façon que ce soit le SDK ou soumettre le SDK à l'ingénierie inverse, à moins d'y être autorisé par une disposition légale d'ordre public ; (3) à concéder des sous-licences ou donner le SDK en location ; (4) à supprimer les fichiers de droits d'auteur ou de mentions légales inclus dans le Composant Redistribuable ; (5) à utiliser le même nom de chemin que celui des fichiers/modules Redistribuables d'origine ; et (6) à utiliser les noms ou les marques d'IBM, de ses concédants de licence ou distributeurs en rapport avec la commercialisation de l'Application Mobile Intégrée du Client, sans l'accord préalable écrit d'IBM ou desdits concédants de licence ou distributeurs.
   - Le Composant Redistribuable demeure intégré sous forme indissociable dans l'Application Mobile Intégrée du Client. Il doit être uniquement au format code objet et doit être conforme à toutes les instructions et spécifications figurant dans le SDK et sa documentation. Le contrat de licence d'utilisateur final destiné à l'Application Mobile Intégrée du Client doit notifier à l'utilisateur final que le Composant Redistribuable ne pourra pas être (i) utilisé à des fins autres que l'activation de l'Application Mobile Intégrée du Client, ii) copié (sauf à des fins de sauvegarde), iii) distribué ou transféré, ou iv) désassemblé, décompilé ou traduit de quelque manière que ce soit, à moins d'y être autorisé par une disposition légale d'ordre public et sans qu'il soit possible d'y déroger contractuellement. Le contrat de licence du Client doit être au moins aussi protecteur d'IBM que les dispositions du présent Contrat.
   - Le SDK ne peut être déployé que dans le cadre des environnements de développement et de test d'unité internes du Client sur les appareils de test mobile spécifiés du Client. Le Client n'est pas à autorisé à utiliser le SDK pour traiter ou simuler des charges de travail de production ou pour tester l'évolutivité de tout code, application ou système. Le Client n'est pas autorisé à utiliser une quelconque partie du SDK à toutes autres fins.

Le Client est responsable de toute l'assistance technique relative à l'Application Mobile Intégrée du Client et des éventuelles modifications apportées par le Client aux Composants Redistribuables, comme autorisé dans les présentes.

Le Client est autorisé à installer et utiliser les Composants Redistribuables et IBM Security Mobile SDK uniquement dans le cadre de son utilisation de l'Offre IBM SaaS.

IBM a testé des exemples d'application créés à l'aide des outils mobiles fournis dans IBM Security Trusteer Mobile SDK (« Outils Mobiles ») pour déterminer s'ils s'exécutent correctement sur certaines versions des plateformes de Système d'Exploitation mobiles d'Apple (iOS), de Google (Android) et d'autres plateformes (ci-après dénommées collectivement « Plateformes de Système d'Exploitation Mobiles ») ; cependant, les Plateformes de Système d'Exploitation Mobiles sont fournies par des tiers, ne sont pas sous le contrôle d'IBM et peuvent être modifiées sans préavis à IBM. A ce titre et nonobstant toute disposition contraire, IBM ne garantit pas que les applications ou autres sorties créées à l'aide des Outils Mobiles s'exécuteront correctement sur, interopèreront ou seront compatibles avec les Plateformes de Système d'Exploitation Mobiles ou les périphériques mobiles.

Le Client s'engage à créer, conserver et fournir à IBM et ses auditeurs des enregistrements écrits exacts, des sorties d'outil système et d'autres informations système permettant à IBM de vérifier au moyen d'un audit que l'utilisation d'IBM Security Trusteer Mobile SDK par le Client est conforme aux termes des présentes Conditions d'Utilisation.

5. Déploiement des Offres IBM SaaS de protection contre la fraude

L'abonnement de base du Client comprend des activités de configuration et de déploiement initial requises, notamment le démarrage, la configuration, le Modèle de Splash, les essais et la formation lors d'une occasion unique.

Des services additionnels peuvent être souscrits moyennant un supplément dans le cadre d'un contrat distinct.

Annexe B

IBM fournit l'Accord relatif aux Niveaux de Service (ci-après dénommé « SLA » ou « Accord relatif aux Niveaux de Service ») de disponibilité suivant pour l'Offre IBM SaaS, qui est applicable s'il est spécifié dans le Document de Transaction du Client :

La version de cet Accord relatif aux Niveaux de Service en vigueur à la date de commencement ou de renouvellement de l'abonnement du Client s'appliquera. Le Client reconnaît que l'Accord relatif aux Niveaux de Service ne constitue pas une garantie pour le Client.

1. Définitions

a. **Contact Agréé** : signifie la personne que le Client a indiquée à IBM, autorisée à soumettre des Réclamations aux termes du présent Accord relatif aux Niveaux de Service.

b. **Crédit de Disponibilité** : signifie la réparation fournie par IBM pour une Réclamation validée. Le Crédit de Disponibilité sera appliqué sous la forme d'un avoir ou d'une remise sur une future facture des redevances d'abonnement à l'Offre IBM SaaS.

c. **Réclamation** : signifie une réclamation soumise par le Contact Agréé du Client à IBM, conformément au présent Accord relatif aux Niveaux de Service, selon laquelle un Niveau de Service n'a pas été satisfait pendant un Mois Contractuel.

d. **Mois Contractuel** : signifie chaque mois complet pendant la durée de l'Offre IBM SaaS, mesuré entre le premier jour du mois à minuit (heure GMT) et le dernier jour du mois à 23h59 (heure GMT).

e. **Client** : signifie une entité souscrivant à l'Offre IBM SaaS directement auprès d'IBM et qui ne manque pas à ses obligations substantielles, y compris ses obligations de paiement, au titre de son contrat avec IBM pour l'Offre IBM SaaS.

f. **Durée d'Indisponibilité** : signifie une période de temps pendant laquelle le traitement du système de production pour le Service s'est arrêté et que tous les utilisateurs du Client ne peuvent pas utiliser tous les aspects du Service pour lequel ils disposent des droits appropriés. La Durée d'Indisponibilité ne comprend pas la période pendant laquelle le Service n'est pas disponible pour les raisons suivantes :

- durée d'Indisponibilité Planifiée du Système ;
- cas de Force Majeure ;
- incidents liés aux applications, équipements et données du Client ou d'un tiers ;
- actes ou omissions du Client ou d'un tiers (y compris toute personne ayant accès à l'Offre IBM SaaS au moyen des mots de passe ou équipements du Client) ;
- non-respect des configurations système requises et des plateformes prises en charge pour l'accès à l'Offre IBM SaaS ; ou
- conformité d'IBM à toute conception, spécification ou instruction fournie par le Client ou par un tiers pour le compte du Client.

g. **Evénement** : signifie une circonstance ou un ensemble de circonstances réunies, donnant lieu au non-respect d'un Niveau de Service.

h. **Force Majeure** : signifie catastrophes naturelles, terrorisme, action sociale, incendie, inondation, tremblement de terre, émeute, guerre, mesures, ordonnances ou restrictions gouvernementales, virus, attaque par saturation et toute autre conduite malveillante, incidents de connectivité des utilitaires ou du réseau ou toute autre cause d'indisponibilité de l'Offre IBM SaaS échappant au contrôle raisonnable d'IBM.

i. **Durée d'Indisponibilité Planifiée du Système** : signifie une indisponibilité planifiée du Service IBM SaaS pour maintenance.

j. **Niveau de Service** : signifie la norme exposée ci-dessous permettant à IBM de mesurer le Niveau de Service qu'elle fournit au titre du présent Accord relatif aux Niveaux de Service.

2. Crédits de Disponibilité

a. Pour pouvoir soumettre une Réclamation, le Client doit avoir soumis un ticket de support pour chaque Événement auprès du centre de support clients IBM pour l'Offre IBM SaaS concernée, conformément à la procédure IBM pour la déclaration des incidents relevant du support de Gravité 1. Le Client doit fournir toutes les informations détaillées nécessaires relatives à l'Événement et aider de manière raisonnable IBM à diagnostiquer et résoudre l'Événement dans les limites requises pour les tickets de support de Gravité 1. Ce ticket doit être soumis dans les 24 heures suivant la première fois où le Client a eu connaissance que l'Événement a eu une incidence sur son utilisation de l'Offre IBM SaaS.

b. Le Contact Agréé du Client doit soumettre la Réclamation du Client pour un Crédit de Disponibilité au plus tard dans les trois (3) jours ouvrables suivant la fin du Mois Contractuel objet de la Réclamation.

c. Le Contact Agréé du Client doit fournir à IBM tous les détails raisonnables de la Réclamation, y compris et de façon non limitative, des descriptions détaillées de tous les Événements concernés et du Niveau de Service allégué comme n'ayant pas été satisfait.

d. IBM mesurera en interne la Durée d'Indisponibilité cumulée au cours de chaque Mois Contractuel applicable au Niveau de Service correspondant dans le tableau ci-dessous. Les Crédits de Disponibilité seront basés sur la Durée d'Indisponibilité mesurée depuis la première fois que le Client a signalé des problèmes relatifs à la Durée d'Indisponibilité. Si le Client signale simultanément un Evénement de Durée d'Indisponibilité d'Application et un Evénement de Temps d'Indisponibilité de Traitement des Données Entrantes, IBM traitera les périodes de chevauchement de la Durée d'Indisponibilité comme une seule Durée d'Indisponibilité, et non comme deux périodes distinctes d'indisponibilité. Pour chaque Réclamation valide, IBM appliquera le Crédit de Disponibilité applicable le plus élevé, en fonction du Niveau de Service Obtenu lors de chaque Mois Contractuel, comme indiqué dans les tableaux ci-dessous. IBM décline toute responsabilité en cas de Crédits de Disponibilité multiples pour un ou plusieurs Événement(s) identique(s) ayant lieu dans le même Mois Contractuel.

e. Pour les Services Regroupés (Services individuels conditionnés et vendus ensemble pour un prix combiné unique), le Crédit de Disponibilité sera calculé en fonction du prix mensuel combiné unique du Service Regroupé, et non de la redevance d'abonnement mensuel pour chaque Offre IBM SaaS prise séparément. Le Client ne pourra soumettre que des Réclamations relatives à une seule Offre IBM SaaS dans une offre groupée au cours de tout Mois Contractuel et IBM ne sera pas redevable des Crédits de Disponibilité concernant plusieurs Offres IBM SaaS dans une offre groupée au cours de tout Mois Contractuel.

f. Si le Client a acquis l'Offre IBM SaaS auprès d'un revendeur IBM agréé dans le cadre d'une transaction de revente dont la principale responsabilité d'IBM consiste à remplir les obligations relatives aux Offres IBM SaaS et aux Accords relatifs aux Niveaux de Service, le Crédit de Disponibilité sera basé sur le Niveau de Prix Conseillé (Relationship Suggested Value Price ou RSVP) en vigueur à ce moment-là pour l'Offre IBM SaaS concernée pendant le Mois Contractuel qui fait l'objet d'une Réclamation, avec une réduction de cinquante pour cent (50 %).

g. Le nombre total de Crédits de Disponibilité accordés concernant tout Mois Contractuel ne doit en aucun cas dépasser dix pour cent (10 %) d'un douzième (1/12e) de la redevance annuelle que le Client a payée à IBM pour l'Offre IBM SaaS.

h. IBM validera les Réclamations, à sa discrétion et en toute bonne foi, en fonction des informations disponibles dans les enregistrements d'IBM, qui prévaudront en cas de conflit avec les données des enregistrements du Client.

i. LES CRÉDITS DE DISPONIBILITÉ FOURNIS AU CLIENT CONFORMÉMENT AU PRÉSENT ACCORD RELATIF AUX NIVEAUX DE SERVICE REPRÉSENTENT LE RECOURS EXCLUSIF DU CLIENT EN CE QUI CONCERNE TOUTE RÉCLAMATION.

3. Niveaux de Service

Disponibilité de l'Offre IBM SaaS pendant un Mois Contractuel

Niveau de Service Obtenu (pendant un Mois Contractuel)	Crédit de Disponibilité (% de Redevance d'Abonnement Mensuel pour le Mois Contractuel objet d'une Réclamation)
< 99,5 %	2 %
< 98,0 %	5%
< 96,0 %	10 %

Le « Niveau de Service Obtenu », exprimé en pourcentage, est calculé comme suit : (a) le nombre total de minutes au cours d'un Mois Contractuel moins (b) le nombre total de minutes de la Durée d'Indisponibilité au cours d'un Mois Contractuel, divisé par (c) le nombre total de minutes d'un Mois Contractuel.

Exemple : 250 minutes de Durée d'Indisponibilité totale pendant un Mois Contractuel

Au total 43 200 minutes dans un Mois contractuel de 30 jours - 250 minutes de Durée d'Indisponibilité = 42 950 minutes _____ Au total 43 200 minutes	= Crédit de Disponibilité de 2 % pour 99,4 % de Niveau de Service Obtenu au cours du Mois Contractuel

3.1 Exclusions

Le présent Accord relatif aux Niveaux de Service n'est disponible que pour les Clients IBM. Il ne s'applique pas :

- aux Services bêta et d'essai ;
- aux environnements non destinés à la production, y compris et de façon non limitative, aux environnements de test, de reprise après incident, d'assurance qualité ou de développement ;
- aux Réclamations déposées par les utilisateurs, participants et invités autorisés de l'Offre IBM SaaS d'un Client IBM ;
- si le Client a manqué à l'une de ses obligations essentielles, telles que définies dans les Conditions d'Utilisation, y compris et de façon non limitative, pour non-respect de toute obligation de paiement.