# IBM Trusteer Fraud Protection

Ce Descriptif de Service détaille le Service Cloud qu'IBM fournit au Client. Le terme « Client » signifie la partie contractante et ses destinataires et utilisateurs autorisés du service Cloud. Le Devis et l'Autorisation d'Utilisation sont fournis séparément sous la forme de Documents de Transaction.

## 1. Service Cloud

Les Services Cloud suivants sont couverts par le présent Descriptif de Service :

**Services Cloud Rapport :**

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport for Retail Premium Support
- IBM Trusteer Rapport II for Business
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications For Retail
- IBM Trusteer Rapport Additional Applications For Business
- IBM Trusteer Rapport Large Redeployment
- IBM Trusteer Rapport Small Redeployment

**Services Cloud Pinpoint :**

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

- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Criminal Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Rapport for Mitigation for Retail
- IBM Trusteer Rapport for Mitigation for Retail Premium Support
- IBM Trusteer Rapport for Mitigation for Business
- IBM Trusteer Rapport for Mitigation for Business Premium Support
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support
- IBM Trusteer Pinpoint Detect Standard For Business Premium Support

**Services Cloud Mobile :**

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

- IBM Trusteer Mobile Browser for Retail Premium Support

## 1.1 Services Cloud Business et Retail

Les Services Cloud IBM Trusteer sont octroyés à des fins d'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.

a. 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.

b. 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.

### 1.1.1 Services Cloud Business

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business

### 1.1.2 Services Cloud Retail

- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Retail

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

### 1.1.3 Services Cloud Additionnels pour IBM Trusteer Rapport

a. Services Cloud Additionnels disponibles pour IBM Trusteer Rapport for Business :

- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Additional Applications For Business

b. Services Cloud Additionnels disponibles pour IBM Trusteer Rapport for Retail :

- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications For Retail

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

L'Abonnement à IBM Trusteer Rapport for Business ou à IBM Trusteer Rapport for Retail est une condition préalable aux Services Cloud additionnels associés énumérés dans la présente Clause.

### 1.1.4 Services Cloud Additionnels disponibles pour IBM Trusteer Pinpoint Malware Detection et/ou IBM Trusteer Pinpoint Malware Detection II

a. Services Cloud additionnels disponibles pour IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition ou IBM Trusteer Pinpoint Malware Detection for Business Standard Edition ou pour IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business :

- IBM Trusteer Pinpoint Carbon Copy for Business
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. Services Cloud additionnels disponibles pour IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition ou IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition ou pour IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition ou IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition :

- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

Le support Premium est disponible pour des offres spécifiques indiquées dans le présent document. L'Abonnement à IBM Trusteer Pinpoint Malware Detection for Business ou IBM Trusteer Pinpoint Malware Detection for Retail ou IBM Trusteer Pinpoint Malware Detection II for Business ou IBM Trusteer Pinpoint Malware Detection II for Retail est une condition préalable aux Services Cloud additionnels associés énumérés dans la présente Clause.

### 1.1.5 Services Cloud Additionnels disponibles pour IBM Trusteer Pinpoint Criminal Detection et/ou IBM Trusteer Pinpoint Criminal Detection II

a. Services Cloud Additionnels disponibles pour IBM Trusteer Pinpoint Criminal Detection for Business ou IBM Trusteer Pinpoint Criminal Detection II :

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. Services Cloud Additionnels disponibles pour IBM Trusteer Pinpoint Criminal Detection for Retail et/ou IBM Trusteer Pinpoint Criminal Detection II for Retail :

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Le support Premium est disponible pour des offres spécifiques indiquées dans le présent document.

L'Abonnement à IBM Trusteer Pinpoint Criminal Detection for Business ou IBM Trusteer Pinpoint Criminal Detection for Retail ou IBM Trusteer Pinpoint Criminal Detection II for Business ou IBM Trusteer Pinpoint

Criminal Detection II for Retail est une condition préalable aux Services Cloud additionnels associés énumérés dans la présente Clause.

**1.1.6 Services Cloud additionnels pour IBM Trusteer Pinpoint Detect Standard et/ou IBM Trusteer Pinpoint Detect Premium et/ou IBM Pinpoint Detect Standard with access management integration et/ou IBM Detect Premium with access management integration**

a. Services Cloud additionnels disponibles pour IBM Trusteer Detect Standard for Business et/ou IBM Trusteer Pinpoint Detect Premium for Business et/ou IBM Pinpoint Detect Standard with access management integration for Business et/ou IBM Detect Premium with access management integration for Business :

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

b. Services Cloud additionnels disponibles pour IBM Trusteer Detect Standard for Retail et/ou IBM Trusteer Pinpoint Detect Premium for Retail et/ou IBM Pinpoint Detect Standard with access management integration for Retail et/ou IBM Detect Premium with access management integration for Retail :

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

L'Abonnement à IBM Trusteer Detect Standard ou IBM Trusteer Pinpoint Detect Premium ou IBM Pinpoint Detect Standard with access management integration ou IBM Detect Premium with access management integration est une condition préalable aux Services Cloud additionnels associés énumérés dans la présente Clause.

**1.1.7 Autres Services Cloud Additionnels**

Tout abonnement aux Services Cloud additionnels pour les abonnements de base ci-dessus qui n'est pas énuméré dans le présent document, qu'il soit 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.

### 1.2 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 Services Cloud couverts.

**Logiciel du Client Détenteur de Compte** : signifie le logiciel d'activation client IBM Trusteer Rapport ou le logiciel d'activation client IBM Trusteer Mobile Browser ou tout autre logiciel d'activation client fourni avec certains Services Cloud 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. IBM Trusteer Rapport Cloud Services

### 2.1 IBM Trusteer Rapport for Retail et/ou IBM 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-Browser). A l'aide d'un réseau de dizaines de millions de nœuds finaux dans le monde entier, IBM Trusteer Rapport collecte des informations sur les attaques de phishing et de programme malveillant actives contre les organisations mondiales. IBM 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.

Ce Service Cloud est doté d'une unité de mesure de redevance 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 de Service Cloud comprend les éléments suivants :

a. Trusteer Management Application (« TMA ») :

TMA est disponible dans l'environnement d'hébergement cloud d'IBM Trusteer, au moyen duquel le Client (et un nombre illimité des membres de son personnel autorisé) peut (i) visionner et

télécharger la communication et l'évaluation de risques de certaines données d'événements et (ii) visionner la configuration du logiciel d'activation client concédé sous licence aux Participants Admissibles du Client 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 au Service Cloud ou de l'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 Services Cloud couverts. 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 Services Cloud couverts. 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 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 au Service Cloud IBM 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 IBM Trusteer Rapport II for Retail et/ou IBM Trusteer Rapport II for Business (ci-après « Trusteer Rapport II »)

Le Service Cloud Trusteer Rapport II est une nouvelle construction d'IBM Trusteer Rapport aidant à normaliser les redevances liées à la protection de plusieurs Applications et remplace les redevances ponctuelles lors de l'ajout d'Applications.

Trusteer Rapport II fournit une couche de protection contre les attaques de phishing et de programme malveillant MitB (Man-in-the-Browser). A l'aide d'un réseau de dizaines de millions de nœuds finaux dans le monde entier, IBM Trusteer Rapport collecte des informations sur les attaques de phishing et de programme malveillant actives contre les organisations mondiales. IBM 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.

Ce Service Cloud est autorisé dans le cadre de l'unité de mesure de redevance 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 de Service Cloud comprend les éléments suivants :

a. Trusteer Management Application (« TMA ») :

   TMA est disponible dans l'environnement d'hébergement cloud d'IBM Trusteer, au moyen duquel le Client (et un nombre illimité des membres de son personnel autorisé) peut (i) visionner et télécharger la communication et l'évaluation de risques de certaines données d'événements et (ii) visionner la configuration du logiciel d'activation client concédé sous licence aux Participants Admissibles du Client 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 au Service Cloud ou de l'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 Services Cloud couverts. 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 Services Cloud couverts. 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 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 au Service Cloud IBM 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.

Trusteer Rapport II for Business et/ou Trusteer Rapport II for Retail incluent chacune la protection d'une seule Application. Pour chaque Application supplémentaire, le Client doit se procurer des droits d'utilisation pour IBM Trusteer Rapport Additional Applications.

## 2.3 Services Cloud additionnels en option pour IBM Trusteer Rapport for Business et/ou IBM Trusteer Rapport for Retail et/ou IBM Trusteer Rapport II for Business et/ou IBM Trusteer Rapport II for Retail

L'abonnement aux Services Cloud IBM Trusteer Rapport ou IBM Trusteer Rapport II est une condition préalable à tout abonnement à l'un Services Cloud additionnels ci-dessous. Si le Service Cloud est désigné par "for Business", les Services Cloud additionnels acquis doivent également être désignés par "for Business". Si le Service Cloud est désigné par "for Retail", les Services Cloud additionnels acquis

doivent également être désignés 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.

### 2.3.1 IBM Trusteer Rapport Fraud Feeds for Business et/ou IBM Trusteer Rapport Fraud Feeds for Retail

Lors de l'abonnement à ce Service Cloud complémentaire, le Client (et un nombre illimité des membres de son personnel autorisé) peut utiliser l'application TMA pour visionner, souscrire et configurer la distribution des flux de menaces générés à partir du Service Cloud Trusteer Rapport. Les flux peuvent être envoyés par e-mail aux adresses e-mail désignées ou via SFTP sous forme de fichiers texte.

### 2.3.2 IBM Trusteer Rapport Phishing Protection for Business et/ou IBM 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 les applications en ligne légitimes (URL) soient signalées par erreur comme des sites de phishing et que les Services Cloud informent 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.

### 2.3.3 IBM Trusteer Rapport Mandatory Service for Business et/ou IBM 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 Services Cloud couverts.

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

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

Le Client ne pourra mettre en œuvre la fonctionnalité additionnelle d'IBM 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 Services Cloud couverts.

### 2.3.4 IBM Trusteer Rapport Large Redeployment et/ou IBM Trusteer Rapport Small Redeployment

Les Clients qui redéploient leurs Applications bancaires en ligne pendant la durée du service et, par conséquent, qui nécessitent des modifications de leur déploiement d'IBM Trusteer Rapport ou d'IBM Trusteer Rapport II doivent acheter le Service Cloud IBM Trusteer Rapport Redeployment.

Le redéploiement peut être dû au fait que le Client modifie le domaine ou l'URL hôte de l'Application, apporte des modifications à la configuration du splash ou passe à une nouvelle plateforme bancaire en ligne.

Pour la période de transition du redéploiement de 6 mois, le Client est autorisé à utiliser des Applications supplémentaires une par une fonctionnant au-dessus des Applications déjà souscrites.

IBM Trusteer Rapport Large Redeployment s'applique aux environnements comptant plus de 20 000 utilisateurs, et IBM Trusteer Rapport Small Redeployment s'applique aux environnements comptant au maximum 20 000 utilisateurs.

### 2.3.5 IBM Trusteer Rapport Additional Applications for Business et/ou IBM Trusteer Rapport Additional Applications for Retail

Le déploiement d'IBM Trusteer Rapport II for Business sur toute Application Business supplémentaire au-delà de la première Application nécessite des droits d'utilisation pour le Service Cloud IBM Trusteer Rapport Additional Applications for Business. Le déploiement d'IBM Trusteer Rapport II for Retail sur toute Application Retail supplémentaire au-delà de la première Application nécessite des droits d'utilisation pour le Service Cloud IBM Trusteer Rapport Additional Applications for Retail.

## 3. Services Cloud IBM Trusteer Pinpoint

IBM 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 Services Cloud couverts et aux processus de prévention de fraude.

Ce Service Cloud comprend :

a. TMA :

   TMA est disponible dans l'environnement d'hébergement cloud d'IBM Trusteer, au moyen duquel le Client (et un nombre illimité des membres de son personnel autorisé) peut (i) visionner et télécharger recevoir la communication et l'évaluation de risques de certaines données d'événements (ii) visionner, souscrire et configurer la distribution des flux de menace générés à partir des offres Pinpoint.

b. Script Web et/ou API :

   Permet le déploiement sur un site Web afin d'accéder au Service Cloud ou de l'utiliser.

### 3.1 Guide des meilleures pratiques IBM Trusteer Pinpoint Malware Detection et IBM Trusteer Pinpoint Criminal Detection

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

### 3.2 IBM Trusteer Pinpoint Criminal Detection for Business et/ou IBM 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 Services Cloud IBM 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 Services Cloud couverts, ou bien le Client peut recevoir les données d'événements via un mode de distribution d'API dorsale.

### 3.3 IBM Trusteer Pinpoint Criminal Detection II for Business et/ou IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Pinpoint Criminal Detection II est une nouvelle construction d'IBM Trusteer Pinpoint Criminal Detection aidant à normaliser les redevances liées à la protection de plusieurs Applications et remplace les redevances ponctuelles lors de l'ajout d'Applications.

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 Services Cloud IBM Trusteer Pinpoint Criminal Detection II 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 Services Cloud couverts, ou bien le Client peut recevoir les données d'événements via un mode de distribution d'API dorsale.

Ce Service Cloud inclut la protection d'une seule Application. Pour chaque Application supplémentaire, le Client doit se procurer des droits d'utilisation pour IBM Trusteer Pinpoint Criminal Detection Additional Applications.

### 3.4 IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition et/ou IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition et/ou IBM Trusteer Pinpoint Malware Detection for Business Standard Edition et/ou IBM 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 Services Cloud IBM 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 ce Service Cloud, comme décrit dans le présent document.

### 3.5 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business et/ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail et/ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business et/ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Pinpoint Malware Detection II est une nouvelle construction d'IBM Trusteer Pinpoint Malware Detection aidant à normaliser les redevances liées à la protection de plusieurs Applications et remplace les redevances ponctuelles lors de l'ajout d'Applications.

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 Services Cloud IBM 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 ce Service Cloud, comme décrit dans le présent document.

Ce Service Cloud inclut la protection d'une seule Application. Pour chaque Application supplémentaire, le Client doit se procurer des droits d'utilisation pour IBM Trusteer Pinpoint Malware Detection Additional Applications.

## 3.6 Services Cloud additionnels en option pour IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition et/ou IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition et/ou IBM Trusteer Pinpoint Malware Detection for Business Standard Edition et/ou IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition et/ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail et/ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business et/ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail et/ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail ou IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail est une condition préalable au Service Cloud IBM Trusteer Rapport Remediation for Retail.
- IBM Trusteer Pinpoint Malware Detection Standard Edition for Business ou IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business est une condition préalable au Service Cloud IBM Trusteer Rapport Remediation for Business.
- IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail ou IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail est une condition préalable à IBM Trusteer Pinpoint Carbon Copy for Retail.
- IBM Trusteer Pinpoint Malware Detection Standard Edition for Business ou IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business ou IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business est une condition préalable à IBM Trusteer Pinpoint Carbon Copy for Business.

### 3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business et/ou IBM Trusteer Pinpoint Carbon Copy for Retail

Les offres IBM 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 de Service Cloud couvertes.

### 3.6.2 IBM Trusteer Rapport Remediation for Retail et/ou IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail et IBM Trusteer Rapport Remediation for Business visent 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 du Client où des attaques de programme malveillant MitB ont été détectées par les données d'événements d'IBM Trusteer Pinpoint Malware Detection. Le Client doit tenir à jour son abonnement à l'offre IBM Trusteer Pinpoint Malware Detection ou IBM Trusteer Pinpoint Malware Detection II qui fonctionne réellement sur l'Application du Client. Le Client n'est autorisé à utiliser cette offre de Service Cloud qu'en rapport avec les Participants Admissibles qui accèdent à l'Application du Client et exclusivement sous forme d'outil visant à identifier et résoudre ponctuellement un appareil infecté particulier (PC/MAC). IBM Trusteer Rapport Remediation 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 du Client, et la configuration du Client doit inclure la collection d'ID utilisateur. Pour mémoire, cette offre de Service Cloud 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.

### 3.6.3 IBM Trusteer Pinpoint Malware Detection Redeployment

Les Clients qui redéploient leurs Applications bancaires en ligne pendant la durée du service et, par conséquent, qui nécessitent des modifications de leur déploiement d'IBM Trusteer Pinpoint Malware Detection et/ou d'IBM Trusteer Pinpoint Malware Detection II doivent acheter IBM Trusteer Pinpoint Malware Detection Redeployment.

Le redéploiement peut être dû au fait que le Client modifie le domaine ou l'URL hôte de l'Application, convertit l'Application en ligne en une nouvelle technologie, passe à une nouvelle plateforme bancaire en ligne ou ajoute un nouveau flux de connexions à une Application existante.

Pour la période de transition du redéploiement de 6 mois, le Client est autorisé à utiliser des Applications supplémentaires une par une fonctionnant au-dessus des Applications déjà souscrites.

### 3.6.4 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail et/ou IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

Le déploiement d'IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ou d'IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business sur toute Application Business supplémentaire au-delà de la première Application nécessite des droits d'utilisation pour IBM Trusteer Pinpoint Malware Detection Additional Applications for Business. Le déploiement d'IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ou d'IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail sur toute Application Retail supplémentaire au-delà de la première Application nécessite des droits d'utilisation pour IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.

## 3.7 Services Cloud additionnels en option pour IBM Trusteer Pinpoint Criminal Detection for Business et/ou IBM Trusteer Pinpoint Criminal Detection for Retail et/ou pour IBM Trusteer Pinpoint Criminal Detection II for Business et/ou IBM Trusteer Pinpoint Criminal Detection II for Retail

### 3.7.1 IBM Trusteer Pinpoint Criminal Detection Redeployment

Les Clients qui redéploient leurs Applications bancaires en ligne pendant la durée du service et, par conséquent, qui nécessitent des modifications de leur déploiement du Service Cloud IBM Trusteer Pinpoint Criminal Detection doivent acheter IBM Trusteer Pinpoint Criminal Detection Redeployment.

Le redéploiement peut être dû au fait que le Client modifie le domaine ou l'URL hôte de l'Application, convertit l'Application en ligne en une nouvelle technologie, passe à une nouvelle plateforme bancaire en ligne ou ajoute un nouveau flux de connexions à une Application existante.

Pour la période de transition du redéploiement de 6 mois, le Client est autorisé à utiliser des Applications supplémentaires une par une fonctionnant au-dessus des Applications déjà souscrites.

### 3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business et/ou IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Le déploiement d'IBM Trusteer Pinpoint Criminal Detection II for Business sur toute Application Business supplémentaire au-delà de la première Application nécessite des droits d'utilisation pour IBM Trusteer

Pinpoint Criminal Detection Additional Applications for Business. Le déploiement d'IBM Trusteer Pinpoint Criminal Detection II for Retail sur toute Application Retail supplémentaire au-delà de la première Application nécessite des droits d'utilisation pour IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail.

## 4. IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite (« Suite ») est une collection de services Cloud conçue pour fournir une couche de protection contre la fraude et peut s'intégrer à d'autres produits IBM pour apporter une solution de gestion de cycle de vie. La Suite inclut les services Cloud suivants :

- IBM Trusteer Pinpoint, qui vise à détecter et atténuer les attaques de programme malveillant, les attaques de phishing et les piratages de compte. Trusteer Pinpoint Detect peut être intégré aux Applications Business et/ou Retail du Client pour lesquelles ce dernier a souscrit aux Services Cloud couverts et aux processus de prévention de fraude.
- IBM Trusteer Rapport for Mitigation, qui vise à corriger et protéger les nœuds finaux infectés.

Les Services Cloud comprennent les fonctionnalités suivantes :

a. TMA :

TMA est disponible dans l'environnement d'hébergement cloud d'IBM 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. 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 Services Cloud couverts, ou bien le Client peut recevoir les données d'événements via un mode de distribution d'API dorsale.

c. Script Web et/ou API :

Permet le déploiement sur un site Web afin d'accéder au Service Cloud ou de l'utiliser.

**Meilleures Pratiques Pinpoint**

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

### 4.1 IBM Trusteer Pinpoint Detect Standard for Business et/ou IBM Trusteer Pinpoint Detect Standard for Retail

Ce Service Cloud combine les Services Cloud IBM Trusteer Pinpoint Criminal Detection et IBM Trusteer Pinpoint Malware Detection pour apporter une solution unifiée unique.

La solution aide à la détection sans client d'un programme malveillant et/ou 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, à la détection de phishing et à la détection de vol des données d'identification par un programme malveillant. Les offres IBM Trusteer Pinpoint 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.

Le support Standard (tel qu'il est défini dans la section Support Technique ci-dessous) est inclus dans ce Service Cloud. Pour le support Premium, le Client doit acheter Detect Premium.

Ce Service Cloud inclut la protection d'une seule Application. Pour chaque Application supplémentaire, le Client doit se procurer des droits d'utilisation pour IBM Trusteer Pinpoint Detect Standard Additional Applications.

## 4.2 IBM Trusteer Pinpoint Detect Premium for Business et/ou IBM Trusteer Pinpoint Detect Premium for Retail

Ce Service Cloud combine IBM Trusteer Pinpoint Criminal Detection et IBM Trusteer Pinpoint Malware Detection pour apporter une solution unifiée unique facilement intégrable.

La solution aide à la détection sans client d'un programme malveillant et/ou 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, à la détection de phishing et à la détection de vol des données d'identification par un programme malveillant. Les offres IBM Trusteer Pinpoint 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.

Ce service est inclut des fonctionnalités et des services améliorés, notamment des services de configuration et de déploiement étendus, des règles de sécurité personnalisées, des services d'investigation, etc.

Ce Service Cloud inclut la protection d'une seule Application. Pour chaque Application supplémentaire, le Client doit se procurer des droits d'utilisation pour IBM Trusteer Pinpoint Detect Premium Additional Applications.

Le support Premium est inclus dans ce Service Cloud.

**Pinpoint Detect Policy Manager :**

Policy Manager est inclus dans le service Pinpoint Detect Premium et est disponible dans l'environnement d'hébergement cloud d'IBM Trusteer, au moyen duquel le Client (et un nombre illimité des membres du personnel autorisé) peut (i) concevoir, tester et déployer dans l'environnement de production une logique d'environnement permettant de détecter les activités frauduleuses, (ii) concevoir des rapports et des tableaux de bord et (iii) visionner, configurer et déterminer des règles en matière de sécurité et des règles permettant de détecter les activités suspectes dans l'Application client.

Des services de conseils sont nécessaires pour l'activation du module Policy Manager et pour le support nécessaire à une analyse approfondie supplémentaire. Les détails des services de conseils seront indiqués séparément dans un descriptif de service.

Une fois Policy Manager activé, IBM se réserve le droit d'accéder à l'environnement du Client au cas où une assistance serait nécessaire pour ajuster les règles du Client en matière de résolution des problèmes majeurs découlant des changements de règles.

Le Client s'engage à protéger contre toute utilisation abusive les données exposées par le biais de Policy Manager.

Lorsque le module Policy Manager est activé, le Client doit se conformer au guide de bonnes pratiques d'IBM en matière de définition des règles, comme indiqué dans la documentation. Le Client reconnaît qu'IBM ne sera en aucun cas tenue pour responsable pour toute situation découlant du non respect de ces recommandations par le Client.

Tout problème de stabilité et/ou de dégradation de service dû à un problème de configuration du module Policy Manager par le Client ne sera pas considéré comme une Indisponibilité pour le calcul de SLA.

## 4.3 IBM Trusteer Pinpoint Detect Standard with access management integration for Business et/ou IBM Trusteer Pinpoint Detect Standard with access management integration for Retail

Le Service Cloud IBM Trusteer Pinpoint Detect Standard with access management integration inclut les fonctionnalités d'IBM Pinpoint Detect Standard détaillées dans la Clause 4.1 ci-dessus.

L'offre IBM Trusteer Pinpoint Detect Standard with access management integration est utilisée lorsqu'elle est achetée avec des systèmes de gestion des accès, tels qu'IBM Access Management (« ISAM »). Lorsqu'elles sont achetées avec ISAM, les deux offres doivent être activées. Cette offre inclut l'option d'intégration au système de gestion des accès. Il ne comprend pas les droits d'utilisation du système de gestion des accès.

Cette offre inclut la protection d'une seule Application. Pour chaque Application supplémentaire, le Client doit se procurer des droits d'utilisation pour IBM Trusteer Pinpoint Detect Standard Additional Applications.

Le support Standard (tel qu'il est défini dans la section Support Technique) est inclus dans ce Service Cloud. IBM Trusteer Pinpoint Detect Premium with access management integration for Business et/ou IBM Trusteer Pinpoint Detect Premium with access management integration for Retail

Le Service Cloud IBM Trusteer Pinpoint Detect Premium with access management integration inclut les fonctionnalités d'IBM Pinpoint Detect Premium détaillées dans la Clause 4.2 ci-dessus, ainsi que l'option d'intégration au système de gestion des accès.

L'offre IBM Trusteer Pinpoint Detect Premium with access management integration est utilisée lorsqu'elle est achetée avec des systèmes de gestion des accès, tels qu'IBM Access Management (« ISAM »). Lorsqu'elles sont achetées avec ISAM, les deux offres doivent être activées. Ce Service Cloud inclut l'option d'intégration au système de gestion des accès. Il ne comprend pas les droits d'utilisation du système de gestion des accès.

Ce Service Cloud inclut la protection d'une seule Application. Pour chaque Application supplémentaire, le Client doit se procurer des droits d'utilisation pour IBM Trusteer Pinpoint Detect Premium Additional Applications.

Le support Premium est inclus dans cette offre.

## 4.4 Services en option pour IBM Trusteer Pinpoint Detect Standard et/ou IBM Trusteer Pinpoint Detect Premium

Les droits d'utilisation d'IBM Trusteer Pinpoint Detect Premium for Retail ou d'IBM Trusteer Pinpoint Detect Standard for Retail sont une condition préalable aux Services Cloud présentés dans cette section.

## 4.5 IBM Trusteer Rapport for Mitigation for Retail et/ou IBM Trusteer Rapport for Mitigation for Business

IBM Trusteer Rapport for Mitigation vise à identifier, résoudre, bloquer et supprimer les attaques de programme malveillant 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 ont été détectées par les données d'événements d'IBM Trusteer Pinpoint Detect Premium ou d'IBM Trusteer Pinpoint Detect Standard. Le Client doit tenir à jour son abonnement à l'offre IBM Trusteer Pinpoint Detect Premium ou IBM Trusteer Pinpoint Standard qui fonctionne réellement sur l'Application Retail du Client. Le Client n'est autorisé à utiliser ce Service Cloud 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 réparer ponctuellement un appareil infecté particulier (PC/MAC). IBM Trusteer Rapport for Mitigation 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, ce Service Cloud 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.

### 4.5.1 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business et/ou IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail et/ou IBM Trusteer Pinpoint Detect Premium Additional Applications for Business et/ou IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

Le déploiement d'IBM Trusteer Pinpoint Detect Standard for Business sur toute Application Business supplémentaire au-delà de la première Application nécessite des droits d'utilisation pour IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

Le déploiement d'IBM Trusteer Pinpoint Detect Standard for Retail sur toute Application Retail supplémentaire au-delà de la première Application nécessite des droits d'utilisation pour IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.

Le déploiement d'IBM Trusteer Pinpoint Premium for Business sur toute Application Business supplémentaire au-delà de la première Application nécessite des droits d'utilisation pour IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

Le déploiement d'IBM Trusteer Pinpoint Premium for Retail sur toute Application Retail supplémentaire au-delà de la première Application nécessite des droits d'utilisation pour IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.

#### 4.5.2 IBM Trusteer Pinpoint Detect Standard Redeployment et/ou IBM Trusteer Pinpoint Detect Premium Redeployment

Les Clients qui redéploient leurs Applications bancaires en ligne pendant la durée du service et, par conséquent, qui nécessitent des modifications de leur déploiement d'IBM Trusteer Pinpoint Detect doivent acheter IBM Trusteer Pinpoint Detect Redeployment.

Le redéploiement peut être dû au fait que le Client modifie le domaine ou l'URL hôte de l'Application, convertit l'Application en ligne en une nouvelle technologie, passe à une nouvelle plateforme bancaire en ligne ou ajoute un nouveau flux de connexions à une Application existante.

Pour la période de transition du redéploiement de 6 mois, le Client est autorisé à utiliser des Applications supplémentaires une par une fonctionnant au-dessus des Applications déjà souscrites.

## 5. IBM Trusteer Mobile Cloud Services

### 5.1 IBM Trusteer Mobile Browser for Business and/or IBM Trusteer Mobile Browser for Retail

Le Service Cloud IBM Trusteer Mobile Browser est conçu 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 Services Cloud couverts, 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 ce Service Cloud, les appareils mobiles incluent les téléphones mobiles ou les tablettes et non les ordinateurs portables et Mac.

TMA permet au Client 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 Services Cloud couverts. Le Client ne pourra commercialiser le Logiciel du Client Détenteur de Compte qu'à l'aide de Trusteer Splash et ne pourra pas 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 Services Cloud couverts.

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 Services Cloud couverts. 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 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.

### 5.2 IBM Trusteer Mobile SDK for Business et/ou IBM Trusteer Mobile SDK for Retail

Les Services Cloud IBM Trusteer Mobile SDK sont conçus pour ajouter une autre couche de protection afin de fournir un accès Web sécurisé aux Applications Business ou Retail du Client pour lesquelles le Client a souscrit aux Services Cloud couverts, 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 Services Cloud IBM 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 Trusteer ainsi que le « Composant d'Exécution » ou le « Composant Redistribuable », un code propriétaire généré par IBM 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 Services Cloud couverts (ci-après « Application Mobile Intégrée du Client »). (« Application Mobile Intégrée du Client »).

IBM Trusteer Mobile SDK for Retail est disponible par lots de 100 Participants Admissibles ou par lots de 100 Unités Client, et IBM 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 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 du présent Descriptif de Service ; 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 seul responsable du développement, du test et du support de son Application Mobile Intégrée. 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 le présent document.

Le Client est autorisé à installer et utiliser les Composants Redistribuables et IBM Security Mobile SDK uniquement dans le cadre de son utilisation des Services Cloud.

IBM a testé des exemples d'application créés à l'aide des outils mobiles fournis dans IBM 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.

Composants Source et Echantillons – L'Offre IBM Trusteer Mobile SDK pourra inclure certains composants au format de code source (« Composants Source ») et d'autres éléments désignés comme « Echantillons ». Le Client est autorisé à copier et modifier les Composants Source et les Echantillons uniquement à des fins d'utilisation interne, à condition que ladite utilisation soit comprise dans les limites des droits de licence objet du présent Contrat, étant entendu toutefois que le Client ne pourra pas modifier ou supprimer les mentions ou informations relatives aux droits d'auteur contenues dans les Composants Source ou les Echantillons. IBM fournit les Composants Source et les Echantillons sans aucune obligation de support et « EN L'ETAT », SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE, Y COMPRIS AUCUNE GARANTIE DE TITRE, GARANTIE EN MATIERE DE DROIT DE PROPRIETE, DE NON-CONTREFAÇON OU DE NON-INGERENCE, ET AUCUNE GARANTIE OU CONDITION IMPLICITE DE QUALITE MARCHANDE OU D'ADEQUATION A UNE FIN PARTICULIERE. Il est à noter que les Composants Source ou les Echantillons sont fournis uniquement à titre d'exemple de la façon dont l'Elément Intégrable est implémenté dans le CIMA, que les Composants Source ou les Echantillons peuvent ne pas être compatibles avec l'environnement de développement du Client et que le Client est seul responsable des tests et de l'implémentation de l'Elément Intégrable dans son CIMA.

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 Trusteer Mobile SDK par le Client est conforme aux dispositions du présent Descriptif de Service.

## 6. Support Premium

Le Client n'a droit au Support Premium que pour les Services Cloud pour lesquels le Client a souscrit à l'offre de Support Premium associée.

## 7. Déploiement d'IBM Trusteer Fraud Protection

Pour chaque Application à laquelle le Client souscrit, l'abonnement de base du Client comprend des activités de configuration et de déploiement initial requises sur le cloud IBM Trusteer, notamment le démarrage, la configuration, le Modèle de Splash, les essais et la formation lors d'une occasion unique.

Les activités de déploiement ne comprennent pas les activités d'implémentation requises sur les Applications ou systèmes du Client.

La phase d'implémentation des divers Services Cloud est prévue dans les délais détaillés dans les guides de déploiement correspondants.

L'achèvement de ces phases d'implémentation dans le délai imparti est fonction de l'engagement total et de la participation de la direction et du personnel du Client. Le Client doit fournir dans les meilleurs délais les informations requises. La prestation d'IBM dépend de la rapidité des informations et décisions du Client et tout retard peut donner lieu à des coûts supplémentaires et/ou un retard dans l'achèvement de ces services d'implémentation.

Pour chaque Application à laquelle le Client souscrit, l'abonnement de base du Client comprend des activités de configuration et de déploiement initial requises sur le cloud IBM Trusteer, notamment le démarrage, la configuration, le Modèle de Splash, les essais et la formation lors d'une occasion unique.

L'abonnement du Client comprend des activités de support et de test pour les pages de l'application du Client qui seront balisées comme recommandé par IBM dans le déploiement initial. IBM n'est pas responsable (i) de tout déploiement partiel, (ii) de la décision du Client de ne pas déployer les Services IBM Cloud comme recommandé par IBM, (iii) de la décision du Client de réaliser lui-même le déploiement, la configuration et le test, ou (IV) d'une protection ou d'un déploiement partiel dû aux

informations inadéquates fournies par le Client. Des services additionnels, y compris des activités de déploiement en plus du déploiement initial, peuvent être souscrits moyennant un supplément dans le cadre d'un contrat distinct.

## 8. Confidentialité et Sécurité des Données

Ce Service Cloud se conforme aux principes de confidentialité et de sécurité de données d'IBM pour les Services Cloud, qui sont disponibles à l'adresse http://www.ibm.com/cloud/data-security, ainsi qu'à toutes dispositions additionnelles stipulées dans la présente clause. Les éventuelles modifications des principes de sécurité et de confidentialité de données d'IBM ne dégraderont pas la sécurité du Service Cloud.

Ce Service Cloud peut être utilisé pour traiter du contenu comportant des Données à caractère personnel si le Client, en tant que responsable du traitement des données, détermine que les mesures de sécurité techniques ou organisationnelles sont appropriées pour les risques présentés par le traitement et la nature des données à protéger. Le Client reconnaît que ce Service Cloud ne propose pas de fonctions permettant la protection des Données à caractère personnel sensibles ou des données soumises à des obligations réglementaires supplémentaires.

Ce Service Cloud est inclus dans la certification Privacy Shield d'IBM qui s'applique lorsque le Client choisit de faire héberger le Service Cloud dans un centre de données aux Etats-Unis, et est soumis aux règles de confidentialité Privacy Shield d'IBM, disponibles à l'adresse http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

### 8.1 Dispositifs de Sécurité et Responsabilités

Le Service Cloud implémente les dispositifs de sécurité suivants :

Le Service Cloud chiffre le contenu pendant la transmission de données à destination et à partir du réseau IBM et le contenu stocké attendant la transmission de données depuis le point de terminaison.

### 8.2 Utilisation et Autorisation Légales

**Utilisation Légale**

L'utilisation du présent Service Cloud peut être soumise à diverses lois ou réglementations. Le Service Cloud ne peut être utilisé qu'à des fins légales et de manière légale. Le Client s'engage à utiliser le Service Cloud conformément aux lois, règlements et réglementations applicables et assume toutes les responsabilités relatives au respect desdites lois, règlements et réglementations.

**Autorisation de Collecte et de Traitement de Données**

Le Service Cloud 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 au Service Cloud couvert. Le Service Cloud collecte des informations qui, seules ou conjointement, peuvent être considérées comme Données à caractère personnel dans certaines juridictions. Par « Données à caractère personnel », 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 du Service Cloud. 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 » du présent Descriptif de Service.

**Pour les offres IBM Trusteer incluant l'application TMA (Trusteer Management Application) :**

Les données suivantes sont collectées et stockées dans l'application TMA (Trusteer Management Application) pour les administrateurs TMA de l'entreprise participante : adresse e-mail (en tant qu'identifiant de connexion), mot de passe haché, prénom, nom de famille, fonction et département.

**Pour les Services Cloud IBM Trusteer Pinpoint :**

Les données collectées peuvent inclure ce qui suit :

- identifiants d'utilisateur ou de nœud final, tels que l'ID Utilisateur chiffré ou haché unidirectionnel, l'ID Utilisateur Persistant (PUID), la Clé d'Agent de Rapport et l'ID Session Client ;

- données relatives à l'application protégée, telles que les attributs/éléments spécifiques issus de l'application bancaire en ligne du Client, tels qu'ils sont affichés dans le navigateur de l'utilisateur final, les visites de site Web et l'historique de navigation ;
- informations relatives à l'environnement logiciel installé, attributs et paramètres des périphériques et navigateurs et durée de l'historique de navigation ;
- informations matérielles et horodatage ;
- en-têtes de navigateur et données du protocole de communication, par exemple l'adresse IP de l'utilisateur, les cookies, l'en-tête de page de référence ainsi que d'autres en-têtes HTTP ;
- données de mouvement de la souris de l'utilisateur final, telles que les coordonnées du pointeur de la souris, les clics et le mouvement de la molette de défilement (et leurs équivalents), ainsi que l'horodatage pendant l'interaction avec l'application bancaire en ligne du Client ;
- sites de phishing et informations soumises aux sites de phishing ; et
- à l'entière discrétion du Client, données transactionnelles (montant, devise et codes de destination de la transaction, code d'identification bancaire cible haché unidirectionnel de la transaction, identifiant de compte cible haché unidirectionnel de la transaction, valeur binaire si la transaction correspond à un nouveau bénéficiaire, ainsi que la date/heure de la transaction) et score des données de risque en option.
- à l'entière discrétion du Client, rythmes de saisie sur le clavier et séquences de frappes utilisées par l'utilisateur final pour saisir un nom d'utilisateur, un mot de passe ou autre (mais pas les lettres, chiffres ou caractères spéciaux en eux-mêmes, ainsi que sans la possibilité de distinguer le nom d'utilisateur ou le mot de passe) ;

Lorsque Policy Manager est activé, toutes les données étendues utilisées relèvent de la seule responsabilité du Client. IBM recommande de hacher ou chiffrer les données pouvant être considérées comme Identifiants personnels.

Le Client reconnaît et convient qu'IBM ne collecte, stocke, gère ou conserve pas les livres officiels et/ou dossiers du Client.

Lorsque le Client souscrit à l'offre IBM Trusteer Rapport for Remediation ou dans certains cas de support Pinpoint, IBM peut recommander que le Logiciel du Client Détenteur de Compte des offres Rapport soit installé sur la machine d'un Participant Admissible afin de rechercher et d'enquêter sur les attaques de programme malveillant détectées. Les données collectées pour les offres Rapport sont définies ci-dessous.

**Pour les Services Cloud IBM Trusteer Rapport (y compris Rapport for Remediation ou Rapport for Mitigation lorsqu'ils sont déployés en rapport avec les offres Pinpoint) :**

Les données collectées peuvent inclure ce qui suit :

- URL et adresses IP (Internet Protocol) des sites Web visités par un Détenteur de Compte qu'IBM juge potentiellement frauduleux, abusifs ou de type phishing, ainsi que les informations sur la nature des menaces identifiées ;
- URL et adresses IP des sites Web visités par un Détenteur de Compte qui sont contrôlés par le Client et protégés par le Service Cloud, par exemple les sites bancaires en ligne et les adresses IP du Détenteur de Compte ;
- informations sur l'identification du matériel, les systèmes d'exploitation, les logiciels d'application, le matériel périphérique, la configuration des paramètres de sécurité, les paramètres système et les connexions réseau du nœud final, ainsi que l'ID, le nom, les habitudes d'utilisation et d'autres données d'identification du nœud final ;
- informations liées à l'installation et au fonctionnement du logiciel, l'ID du logiciel, la version du logiciel, les événements de sécurité générés à partir du nœud final, ainsi que les informations sur les erreurs du logiciel ;
- caractéristiques d'utilisation et informations statistiques sur les menaces détectées par le logiciel ; fichiers journaux contenant les pannes du navigateur, la date et l'heure d'une attaque et les informations sur la nature des menaces identifiées ou du dysfonctionnement ;
- affiliation du Client, également référencée en tant qu'Entreprise Participante. Une affiliation est établie lorsqu'un utilisateur final télécharge un Rapport sur le site Web du Client, sélectionne un

Client particulier lors du téléchargement du Rapport sur le site de support Trusteer ou se connecte à l'application bancaire du Client. Un utilisateur final peut disposer de plusieurs affiliations Client ;

- copie de l'ID Utilisateur chiffré que le Détenteur de Compte utilise pour interagir avec le Client (en option) ;
- copie chiffrée d'un numéro de carte de crédit que le Détenteur de Compte entre dans un site après que le logiciel informe le Détenteur de Compte que le logiciel considère le site à risque ;
- fichiers et autres informations issus du nœud final que les spécialistes de la sécurité IBM soupçonnent être liés à un programme malveillant ou toute autre activité malveillante, ou qui peuvent être associés au dysfonctionnement général du logiciel ; et
- coordonnées personnelles, y compris le nom et l'adresse e-mail, lorsque l'utilisateur final contact le service de support.

**Pour les Services Cloud IBM Trusteer Mobile SDK et IBM Trusteer Mobile Browser :**

Les données collectées peuvent inclure ce qui suit :

- identifiants d'utilisateur, tels que l'ID Utilisateur chiffré ou haché unidirectionnel ;
- informations sur l'appareil, telles que l'adresse IP, l'ID appareil haché, l'horodatage, les valeurs MD5 du package installé et autres informations matérielles et logicielles de l'appareil ;
- version et date d'installation de Mobile SDK ou Mobile Browser ;
- visites des applications protégées ;
- affiliation Client ;
- données de risque des périphériques (par exemple, présence de programme malveillant, root hider, statut de chiffrement Wi-Fi, vérification de l'état d'un périphérique (bloqué ou non)) ;
- trace de pile de crash (dans le cas d'un arrêt inattendu de l'application) ;
- données de fabrication de téléphone (par exemple, modèle, fabricant) ;
- interactions des utilisateurs finaux via l'écran tactile, y compris coordonnées x et y, zone de contact et type d'action (vers le bas, vers le haut et déplacement) ; et
- données du détecteur de mouvement, consommation électrique, utilisation des ressources, paramètres de connectivité, capteurs d'environnement, tels que la température, la lumière et la pression de l'air, ainsi que les paramètres généraux des périphériques (volume, sonnerie, luminosité de l'écran, etc.).

## 8.3 Consentement en Connaissance de Cause des Personnes Concernées

**Pour les Services Cloud IBM Trusteer Pinpoint et IBM 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 du Service Cloud et pour permettre la collecte et le traitement des informations par IBM par le biais du Service Cloud.

**Pour les Services Cloud IBM Trusteer Rapport (y compris Rapport Remediation ou Rapport for Mitigation lorsqu'ils sont déployés en rapport avec les Services Pinpoint) et IBM Trusteer Mobile Browser :**

Le Client autorise IBM à obtenir des consentements en pleine connaissance de cause, nécessaires pour permettre l'utilisation légale du Service Cloud 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 du Service Cloud 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 du Service Cloud.

## 8.4 Utilisation des Données de Sécurité

Dans le cadre du Service Cloud, qui comprend des activités de production de rapport, IBM préparera et gérera les informations anonymes et/ou cumulées extraites du Service Cloud (« Données de Sécurité »). Sauf disposition contraire stipulée dans le paragraphe (d) ci-dessous, les Données de Sécurité n'identifieront pas le Client, ses Participants Admissibles ou un individu. Le Client accepte qu'IBM puisse utiliser et/ou copier en permanence les Données de Sécurité uniquement aux fins suivantes :

a. publication et/ou distribution des Données de Sécurité (par exemple, dans les compilations et/ou analyses liées à la cybersécurité) ;

b. développement ou amélioration des produits ou services ;

c. réalisation d'étude en interne ou auprès de tiers ;

d. partage légal des informations confirmées relatives à un contrevenant tiers ; et

e. règles anonymes de Policy Manager.

## 8.5 Transferts hors du Territoire

Le Client accepte qu'IBM traite le contenu, y compris toutes Données à caractère personnel telles qu'elles sont identifiées dans la clause ci-dessus intitulée « Utilisation et Autorisation Légales », 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 Economique Européen et dans les pays considérés par la Commission Européenne comme assurant des niveaux de sécurité adéquats : les Etats-Unis.

## 8.6 Confidentialité des Données

Si le Client rend des Données à caractère personnel accessibles au Service Cloud dans les Etats 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 à caractère personnel. IBM ne traitera ces Données à caractère personnel que dans les limites requises pour mettre à disposition l'offre de Service Cloud conformément aux descriptions publiées d'IBM du Service Cloud et le Client accepte que ledit traitement est conforme aux instructions du Client. IBM adressera un préavis raisonnable via le Portail Client si elle apporte une modification significative au site du traitement ou à la façon dont elle sécurise les Données à caractère personnel dans le cadre du Service Cloud. Le Client est autorisé à résilier la période d'abonnement en cours pour le Service Cloud concerné, à condition d'adresser à IBM une notification écrite dans les trente (30) jours suivant la notification par IBM de la modification au Client.

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. Tous les litiges ou réclamations relatif à ces accords, même si ceux-ci sont signés par des sociétés affiliées, seront traités par les parties conformément aux dispositions du présent Contrat comme si lesdits litiges ou réclamations étaient survenus entre les parties.

a. Le Client accepte, en ce qui concerne les services fournis via le centre de données en Allemagne, comme déterminé pendant le processus de mise à disposition, qu'IBM puisse traiter le contenu, y compris les Données à caractère personnel, hors du territoire à destination des sous-traitants ou sous-traitants ultérieurs du traitement des données suivantes :

| 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 | Allemagne |
| IBM Ireland Ltd. | Sous-traitant du traitement des données | Irlande |
| IBM Israel Ltd. | Sous-traitant du traitement des données | Israël |

Pour les services fournis via le centre de données d'Allemagne, certains services clients peuvent être exécutés par des employés Trusteer basés dans un pays de l'Union européenne.

b. Le Client accepte, en ce qui concerne les services fournis via le centre de données au Japon, comme déterminé pendant le processus de mise à disposition, qu'IBM puisse traiter le contenu, y compris les Données à caractère personnel, 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 | Japon, comme indiqué dans le Document de Transaction |
| Amazon Web Services (Japon) | Sous-traitant ultérieur du traitement de données | Japon |
| IBM Ireland Ltd. | Sous-traitant du traitement des données | Irlande |
| IBM Israel Ltd. | Sous-traitant du traitement des données | Israël |

c. Le Client accepte, en ce qui concerne les services fournis via le centre de données aux Etats-Unis, qu'IBM traite le contenu, y compris des Données à caractère personnel, 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 | Etats-Unis |
| IBM Ireland Ltd. | Sous-traitant du traitement des données | Irlande |
| IBM Israel Ltd. | Sous-traitant du traitement des données | Israël |
| IBM Corp | Sous-traitant du traitement des données | Etats-Unis |

d. Pour les services fournis via les centres de données énumérés dans la Clause 8.5.c ci-dessus, « Centre de données aux Etats-Unis », IBM pourra également traiter des données par l'intermédiaire d'un ou de plusieurs des sous-traitants ultérieurs du traitement de données suivants, comme déterminé pendant le processus de mise à disposition :

| Nom du Sous-traitant/Sous-traitant ultérieur du traitement des données | Rôle (Sous-traitant/Sous-traitant ultérieur du traitement des données) | Emplacement |
|---|---|---|
| Amazon Web Services (Australie) | Sous-traitant ultérieur du traitement de données | Australie |
| Amazon Web Services (Singapour) | Sous-traitant ultérieur du traitement de données | Singapour |
| Amazon Web Services (Ireland) | Sous-traitant ultérieur du traitement de données | Irlande |

e. Le Client accepte qu'IBM puisse, sur préavis via le Portail Client, faire migrer le traitement depuis Amazon Web Services vers les centres de données d'IBM. En outre, IBM pourra, sur préavis via le Portail Client, modifier les listes des sous-traitants ultérieurs du traitement de données énumérés ci-dessus.

f. Les données du Détenteur de Compte seront traitées dans la région à partir de laquelle le Détenteur de Compte a initialement installé le Logiciel du Client Détenteur de Compte. Cela peut signifier que le contenu du Détenteur de Compte peut être traité tant dans la région d'origine que dans la région convenue avec le Client.

g. Les données de service de support clients sont stockées sur un serveur Cloud Salesforce.com situé en Irlande.

h. A des fins d'éclaircissement, Trusteer Fraud Protection étant une solution intégrée, si le Client résilie l'un des présents Services Cloud, IBM peut conserver les données du Client en vue de fournir les Services Cloud restants au Client, conformément à la présente Description de services.

## 9. Accord Relatif aux Niveaux de Service

IBM fournit l'Accord Relatif aux Niveaux de Service (ci-après dénommé « Accord Relatif aux Niveaux de Service » ou « SLA ») de disponibilité ci-dessous pour le Service Cloud, comme indiqué dans une Autorisation d'Utilisation. Le SLA ne constitue pas une garantie. Il n'est disponible que pour le Client et ne peut être utilisé que dans les environnements de production.

### 9.1 Crédits de Disponibilité

Le Client doit consigner un ticket de support de Gravité 1 auprès du centre d'assistance technique IBM dans les 24 heures suivant la première fois où le Client a eu connaissance qu'un événement a eu une incidence sur la disponibilité du Service Cloud. Le Client doit raisonnablement aider IBM dans le cadre du diagnostic et de la résolution des problèmes.

Une demande de ticket de support pour non-respect d'un SLA doit être soumise dans les trois jours ouvrables suivant la fin du mois contractuel. Le dédommagement relatif à une réclamation de SLA valide sera un avoir sur une future facture du Service Cloud en fonction de la période de temps pendant laquelle le traitement du système de production pour le Service Cloud n'est pas disponible (« Durée d'Indisponibilité »). La Durée d'Indisponibilité est calculée depuis le moment où le Client signale l'événement jusqu'au moment où le Service Cloud est restauré ; elle ne comprend pas les périodes d'indisponibilité pour les raisons suivantes : indisponibilité de maintenance programmée ou annoncée, causes échappant au contrôle d'IBM, incidents liés au contenu, à la technologie, aux conceptions ou aux instructions du Client ou d'un tiers, plateformes et configurations système non prises en charge ou autres erreurs du Client, incident de sécurité du fait du Client ou test de sécurité mené par le Client. IBM appliquera le dédommagement correspondant le plus élevé, en fonction de la disponibilité cumulée du Service Cloud pendant chaque mois contractuel, comme indiqué dans le tableau ci-dessous. Le dédommagement total relatif à tout mois contractuel ne pourra pas dépasser dix pour cent (10 %) d'un douzième (1/12ème) de la redevance annuelle du Service Cloud.

### 9.2 Niveaux de service

Disponibilité du Service Cloud pendant un mois contractuel

| Disponibilité pendant un mois contractuel | Indemnisation (% de redevance d'abonnement mensuelle* pour le mois contractuel objet d'une réclamation) |
|---|---|
| < 99,5 % | 2 % |
| < 98,0 % | 5 % |
| < 96,0 % | 10 % |

* Si le Service Cloud a été acquis auprès d'un Partenaire Commercial IBM, la redevance d'abonnement mensuelle sera calculée sur le prix en vigueur à ce moment-là pour le Service Cloud concerné pendant le mois contractuel qui fait l'objet d'une réclamation, avec une réduction de cinquante pour cent (50 %). IBM accordera une remise directement au Client.

Les Niveaux de Service et les Crédits de Service associés sont mesurés séparément par Service Cloud et par Application Client.

Lors du calcul des crédits SLA pour les Services Cloud en fonction des droits d'utilisation d'Application, la Disponibilité sera calculée selon les critères suivants :

- Une part pondérée sera affectée à chaque Application en fonction du nombre calculé de volumes des sessions pendant le mois contractuel.
- La Durée d'Indisponibilité de chaque Service Cloud par Application sera cumulée séparément pour le moins contractuel.

L'exemple ci-dessous montre un calcul pour un mois d'activité ainsi que la pondération associée. Il n'est présenté qu'à titre indicatif :

| Applications Retail | Part du nombre total de sessions au cours d'un mois contractuel donné | Durée d'Indisponibilité totale pendant un mois contractuel | Minutes pondérées de Durée d'Indisponibilité |
|---|---|---|---|
| Application Retail A | 40 % | 300 minutes | 40 % x. 300 minutes = 120 minutes |
| Application Retail B | 20 % | 250 minutes | 20 % x 250 minutes = 50 minutes |
| Application Retail C | 40 % | 150 minutes | 40 % x 150 minutes = 60 |
| | | | Nombre total de minutes pondérées de la Durée d'Indisponibilité = 230 |

La disponibilité, exprimée en pourcentage, est calculée comme suit : le nombre total de minutes d'un mois contractuel moins le nombre total de minutes pondérées de la Durée d'Indisponibilité au cours du mois contractuel, divisé par le nombre total de minutes du mois contractuel. Le calcul suivant est basé sur l'exemple de pondération ci-dessus :

$$\frac{\text{Au total 43 200 minutes dans un mois contractuel de 30 jours} - \text{230 minutes de Durée d'Indisponibilité pondérée} = \text{42 970 minutes}}{\text{Au total 43 200 minutes}} = \text{2 \% de crédit de Disponibilité pour 99,4 \% de disponibilité pendant le mois contractuel}$$

## 10. Support Technique

Le Support Technique des Services Cloud est accessible au Client et à ses Participants Admissibles pour les aider à utiliser les Services Cloud.

Le Support Standard est compris dans l'abonnement de 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 Service Cloud, un abonnement au Support Premium est disponible moyennant un supplément, à l'exception des Services Cloud IBM Trusteer Mobile SDK et IBM Trusteer Rapport Mandatory Service. Veuillez contacter votre interlocuteur IBM habituel ou votre Partenaire Commercial IBM.

**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 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 ou en envoyant une demande de rappel.
- 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 SaaS [Software as a Service] à l'adresse suivante : http://www-01.ibm.com/software/support/handbook.html.

## 11. Droit d'Utilisation et Informations de Facturation

### 11.1 Unités de mesure des redevances

Le Service Cloud est disponible en fonction des unités de mesure de redevance indiquées dans le Document de Transaction :

a. Participant Admissible : unité de mesure par laquelle le Service Cloud peut être acheté. Tout individu ou entité habilité à prendre part à un programme de prestation de service géré ou suivi par le Service Cloud constitue un Participant Admissible. Des droits d'utilisation suffisants doivent être obtenus pour couvrir tous les Participants Admissibles gérés ou suivis dans le Service Cloud pendant la période de mesure indiquée dans le Document de Transaction du Client.

   Chaque programme de prestation de service géré par le Service Cloud 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 les besoins relatifs aux droits d'utilisation de ces Services Cloud, un Participant Admissible est un Utilisateur Final d'un Client, qui dispose de données de connexion uniques sur une Application Business ou Retail du Client.

b. Unité Client : unité de mesure par laquelle le Service Cloud peut être acquis. 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 le Service Cloud, lui fournit des données, utilise des services fournis par le Service ou autrement accède au Service Cloud pendant la période de mesure indiquée dans le Document de Transaction du Client.

c. Application : unité de mesure par laquelle le Service Cloud peut être acheté. Une Application est un logiciel portant un nom unique. Des droits d'utilisation suffisants sont nécessaires pour chaque Application mise à disposition à des fins d'accès et d'utilisation pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (« PoE ») ou le Document de Transaction du Client.

   Pour le Service Cloud, une application est une Application Business ou Retail unique du Client.

d. Engagement : unité de mesure par laquelle les services peuvent être acquis. Un Engagement comprend des services professionnels et/ou de formation relatifs aux Services Cloud. Des Droits d'Utilisation suffisants sont nécessaires pour couvrir chaque Engagement.

## 12. Conformité et Audit

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

Un audit peut être mené par IBM pour vérifier le respect du nombre maximal d'Applications, de Participants Admissibles et/ou d'Unités Client.

## 13. Durée et Options de Renouvellement

La durée du Service Cloud commence à la date à laquelle IBM notifie au Client que ce dernier a accès au Service Cloud, comme décrit dans l'Autorisation d'Utilisation. L'Autorisation d'Utilisation indiquera si le Service Cloud est renouvelé automatiquement, s'il se poursuit en continu ou s'il prend fin à l'issue de la durée.

Pour un renouvellement automatique, le Service Cloud est automatiquement renouvelé pour la durée indiquée dans l'Autorisation d'Utilisation, sauf si le Client notifie par écrit, au moins 90 jours avant la date d'expiration de la durée, son intention de ne pas renouveler.

Pour une utilisation en continu, le Service Cloud continuera d'être disponible mois par mois jusqu'à ce que le Client notifie la résiliation moyennant un préavis écrit de 90 jours. Le Service Cloud demeure disponible jusqu'à la fin du mois suivant ladite période de 90 jours.

## 14. Dispositions Additionnelles

### 14.1 Logiciel d'Activation

Ce Service Cloud comprend un logiciel d'activation, qui ne doit être utilisé qu'en rapport avec l'utilisation du Service Cloud par le Client et uniquement pendant la durée du Service Cloud.

### 14.2 Augmentation du Montant Annuel de l'Abonnement à IBM Trusteer

IBM se réserve le droit d'ajuster le montant de l'abonnement aux Services Cloud. L'ajustement du montant de l'abonnement sera reflété dans les prix indiqués pour la durée de validité du Devis. Des ajustements des frais d'abonnement supplémentaires, appliqués une fois tous les douze (12) mois par le biais d'un pourcentage déterminé par IBM et n'excédant pas les 3 %, peuvent s'appliquer lorsque la durée des Services Cloud est prolongée par renouvellement automatique ou utilisation continue. Ils ne modifient pas le droit d'utilisation des Services Cloud par le Client ou l'unité de mesure des redevances par laquelle le Service Cloud est acquis. Les Partenaires Commerciaux IBM sont indépendants d'IBM et déterminent unilatéralement leurs prix et modalités.