IBM Trusteer Fraud Protection

Ce Descriptif de Services détaille le Service Cloud qu'IBM fournit au Client. Le terme « Client » se réfère à la partie contractante et aux 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 Services :

Services Cloud Pinpoint Assure :

- IBM Trusteer Pinpoint Assure
- IBM Trusteer Pinpoint Assure Application
- IBM Trusteer Mobile Carrier Intelligence

Services Cloud Rapport :

- IBM Trusteer Rapport for Business Premium Support
- 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 Standard Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail

- IBM Trusteer Pinpoint Malware Detection Advanced Edition II 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 Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- 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 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 Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail Premium Support
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Project Management and Consultancy Services
- IBM Trusteer Security Research Consultancy Services
- IBM Trusteer Training Services
- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application
- IBM Trusteer Pinpoint Detect Standard
- IBM Trusteer Pinpoint Detect Premium
- IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect
- IBM Trusteer Pinpoint Verify

Services Cloud Mobile :

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail

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 II for Business
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer Mobile SDK for Business

1.1.2 Services Cloud Retail

- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Mobile SDK 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 II

a. Services Cloud additionnels disponibles pour IBM Trusteer Rapport II 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 II 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 II 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 II

a. Services Cloud additionnels disponibles pour IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business ou IBM Trusteer Pinpoint Malware Detection Standard Edition II 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 Advanced Edition II for Retail ou IBM Trusteer Pinpoint Malware Detection Standard Edition II 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 II for Business ou à 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 Detect Standard et/ou IBM Trusteer Pinpoint Detect Premium et/ou IBM Trusteer Pinpoint Detect Standard for Retail et/ou IBM Trusteer Pinpoint Detect Premium for Retail et/ou IBM Trusteer Pinpoint Detect Standard for Business et/ou IBM Trusteer Pinpoint Detect Premium for Business

a. Services Cloud additionnels disponibles pour IBM Trusteer Detect Standard for Business et/ou 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 Digital Content Pack for Business
   - IBM Trusteer New Account Fraud for Business

b. Services Cloud additionnels disponibles pour IBM Trusteer Detect Standard for Retail et/ou IBM Trusteer Pinpoint Detect Premium for Retail :
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
   - IBM Trusteer Digital Content Pack for Retail
   - IBM Trusteer New Account Fraud for Retail

c. Services Cloud additionnels disponibles pour IBM Trusteer Pinpoint Detect Standard et/ou IBM Trusteer Pinpoint Premium :
   - IBM Trusteer Pinpoint Detect Standard Application
   - IBM Trusteer Pinpoint Detect Premium Application

d. Services Cloud additionnels disponibles pour IBM Trusteer Pinpoint Detect Premium
   - IBM Trusteer Pinpoint Verify

L'abonnement à IBM Trusteer Pinpoint Detect Standard ou IBM Trusteer Pinpoint Detect Premium ou IBM Trusteer Pinpoint Detect Standard for Retail ou IBM Trusteer Pinpoint Detect Premium for Retail ou IBM Trusteer Pinpoint Detect Standard for Business ou IBM Trusteer Pinpoint Detect Premium for Business est une condition préalable aux Services Cloud additionnels associés énumérés dans la présente Clause.

1.1.6 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 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.

1.3 Services Cloud IBM Trusteer Rapport

1.3.1 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 ou Dispositif Client. L'offre Business est vendue par lots de 10 Participants Admissibles ou 10 Dispositifs Client. L'offre Retail est vendue par lots de 100 Participants Admissibles ou 100 Dispositifs Client.

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 services 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.

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

L'abonnement aux Services Cloud IBM Trusteer Rapport II est une condition préalable à tout abonnement à l'un des 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 ou Dispositifs Client 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.

1.3.3 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.

Cette offre est applicable uniquement dans le cadre de l'unité de mesure de redevance Participant Admissible.

1.3.4 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.

Ce Service Cloud est autorisé dans le cadre de l'unité de mesure de redevance Participant Admissible ou Dispositif Client. L'offre Business est vendue par lots de 10 Participants Admissibles ou 10 Dispositifs Client. L'offre Retail est vendue par lots de 100 Participants Admissibles ou 100 Dispositifs Client.

Un support Premium peut être obtenu pour ces services cloud dans le cadre de l'unité de mesure de redevance Participant Admissible ou Dispositif Client. L'offre Business est vendue par lots de 10 Participants Admissibles ou 10 Dispositifs Client. L'offre Retail est vendue par lots de 100 Participants Admissibles ou 100 Dispositifs Client.

1.3.5 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.

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. L'offre Retail est vendue par lots de 100 Participants Admissibles.

1.3.6 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 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.

1.3.7 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.

1.4 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.

1.4.1 IBM Trusteer Pinpoint Malware Detection

Dans l'hypothèse d'une détection de programmes malveillants dans les Services Cloud IBM Trusteer Pinpoint Malware 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 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).

1.4.2 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, avec 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 des offres Business et/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.

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

- 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 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.

1.4.4 IBM Trusteer Rapport Remediation for Retail et/ou IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation 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 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.

1.4.5 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 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.

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

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

- Pour IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail, le déploiement de 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.
- Pour IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ou IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business, le déploiement de 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.

1.5 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 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).

1.5.1 IBM Trusteer Pinpoint Detect Standard for Retail et/ou IBM Trusteer Pinpoint Detect Standard for Business

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 Retail ou Business à l'aide d'un ID appareil, de la détection de phishing et de la détection de vol des données d'identification par un programme malveillant. Les offres IBM Trusteer Pinpoint fournissent une couche supplémentaire 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 Retail ou Business.

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

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.

Le service est disponible à l'achat par lots de 100 Participants Admissibles ou de 100 Connexions. Si le Client choisit d'acheter le service par lots de Connexions, les frais d'Application Additionnelle s'appliquent dès la première application.

1.5.2 IBM Trusteer Pinpoint Detect Premium for Retail et/ou IBM Trusteer Pinpoint Detect Premium for Business

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 Retail ou Business à l'aide d'un ID appareil, de la détection de phishing et de 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 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. Il inclut également jusqu'à 200 heures de ressources partagées pour les services de déploiement par application et 200 heures de ressources partagées pour l'analyse de sécurité par application lors de la configuration. Les services continus comprennent 20 heures de maintenance de déploiement par an et par application, et 100 heures de recherche de sécurité par application et par an. Tout effort supplémentaire sera soumis à des frais supplémentaires.

Pinpoint Detect peut consommer les transactions des canaux Mobile et Web. La détection par Connexion s'applique si les transactions mobiles sont incluses. 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.

Les services IBM Trusteer Pinpoint Detect Premium for Retail et Business sont disponibles à l'achat par lots de 100 Participants Admissibles ou, pour IBM Trusteer Pinpoint Detect Premium, par lots de 100 Connexions. Si le Client choisit d'acheter le service par lots de Connexions, les frais d'Application Additionnelle s'appliquent dès la première application.

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 services.

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.

1.5.3 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 ou d'IBM Trusteer Pinpoint Detect Standard sont une condition préalable aux Services Cloud présentés dans cette clause.

1.5.4 IBM Trusteer Rapport for Mitigation for Retail et/ou IBM Trusteer Rapport for Mitigation for Business

- IBM Trusteer Rapport for Mitigation for Retail 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.
- IBM Trusteer Rapport for Mitigation for Business 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 Business 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 Business du Client. Le Client n'est autorisé à utiliser ce Service Cloud qu'en rapport avec les Participants Admissibles qui accèdent à l'Application Business

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 Business 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 Business 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.

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

Ce service inclut jusqu'à 200 heures de ressources partagées pour les services de déploiement par application et 200 heures de ressources partagées pour l'analyse de sécurité par application lors de la configuration. Les services continus comprennent 20 heures de maintenance de déploiement par an et par application, et 100 heures de recherche de sécurité par application et par an.

- Pour IBM Trusteer Pinpoint Detect Standard for Retail, le déploiement de 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.
- Pour IBM Trusteer Pinpoint Detect Standard for Business, le déploiement de 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.
- Pour IBM Trusteer Pinpoint Premium for Retail, le déploiement de 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.
- Pour IBM Trusteer Pinpoint Premium for Business, le déploiement de 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.

1.5.6 IBM Trusteer Pinpoint Detect Standard Application et/ou IBM Trusteer Pinpoint Detect Premium Application

Ce service s'applique aux canaux Web et Mobile.

Ce service inclut jusqu'à 200 heures de ressources partagées pour les services de déploiement par application et 200 heures de ressources partagées pour l'analyse de sécurité par application lors de la configuration. Les services continus comprennent 20 heures de maintenance de déploiement par an et par application, et 100 heures de recherche de sécurité par application et par an.

- Le déploiement d'IBM Trusteer Pinpoint Detect Standard nécessite des droits d'utilisation d'IBM Trusteer Pinpoint Detect Standard Application pour chaque Application.
- Le déploiement d'IBM Trusteer Pinpoint Premium nécessite des droits d'utilisation d'IBM Trusteer Pinpoint Detect Premium Application pour chaque Application.

1.5.7 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.

1.5.8 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support et/ou IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Les Clients qui achètent Pinpoint Detect Standard Cloud Service peuvent acheter le service Premium Support. Le champ d'application des services Premium Support est décrit dans la clause 4 ci-dessous.

1.5.9 IBM Trusteer Digital Content Pack for Retail et/ou IBM Trusteer Digital Content Pack for Business

IBM Trusteer Digital Content Pack permet aux analystes de sécurité d'intégrer de nouveaux modèles de fraude tout en prenant entièrement en charge la création et la modification de modèles ad hoc pour réagir aux menaces croissantes. Il comprend de nombreuses règles, observations et politiques qui peuvent être achetées en complément et en tant que partie intégrante de la solution. Digital Content Pack aide à renforcer davantage l'intégration entre les fonctionnalités de prévention de fraude numériques de Trusteer et les canaux de paiement sans espèces d'IBM Safer Payments. En optimisant ses règles intégrées et logiques métier spécifiques, Digital Content Pack permet aux banques et autres établissements financiers d'améliorer davantage les fonctionnalités de détection et de prévention de fraude existantes.

IBM Trusteer Digital Content Pack for Retail est disponible par lots de 100 Participants Admissibles. IBM Trusteer Digital Content Pack for Business est disponible par lots de 10 Participants Admissibles.

Des services de conseils sont requis pour l'intégration de Digital Content Pack à Pinpoint Detect et IBM Safer Payments, ainsi que des services de support nécessitant une attention particulière. Les services de conseils sont acquis séparément dans le cadre d'un descriptif de services distinct.

1.5.10 IBM Trusteer New Account Fraud for Retail et/ou IBM Trusteer New Account Fraud for Business

Ce service, disponible pour les abonnés Pinpoint, a été conçu pour détecter des anomalies, signaler des activités douteuses et générer des alertes rapidement dans le nouveau processus de création de compte. Le service surveille les nouveaux comptes pour identifier de nouvelles activités associées au profilage de la fraude des comptes récents et après la création de compte pour envoyer rapidement un avertissement indiquant que le nouveau compte peut être un faux compte ou utilisé pour pratiquer la fraude, via des rapports d'utilisation disponible dans le TMA.

IBM Trusteer New Account Fraud for Retail et IBM Trusteer New Account Fraud for Business sont disponibles par lots de 10 Appels d'API.

1.5.11 IBM Trusteer Pinpoint Verify

Le Client doit tenir à jour son abonnement à IBM Trusteer Pinpoint Detect Premium avant de s'abonner à ce Service Cloud.

Ce Service Cloud offre des fonctionnalités demandant aux utilisateurs de s'authentifier pour un second facteur d'authentification afin de vérifier leur identité lorsqu'ils accèdent à un service numérique. Il est disponible pour Pinpoint Detect Premium, afin de fournir un second facteur d'authentification pour les applications protégées. La décision déterminant à quel moment demander aux utilisateurs une authentification à deux facteurs est générée par l'application protégée et peut être fondée sur les recommandations renvoyées par la plateforme Pinpoint Detect Premium ou toute autre politique définie par l'application protégée.

1.6 IBM Trusteer Pinpoint Assure

Ce service signale les activités suspectes et génère des alertes lors de la création/du processus d'enregistrement d'un nouveau compte. Le service surveille le processus d'enregistrement de compte pour identifier les activités associées à une fraude et envoyer rapidement un avertissement indiquant que le nouveau compte peut être un faux compte ou utilisé à des fins de fraude, via des rapports d'utilisation disponible dans le TMA.

IBM Trusteer Pinpoint Assure est disponible par lots de 100 Connexions.

1.6.1 Services en option pour IBM Trusteer Pinpoint Assure

1.6.2 IBM Trusteer Pinpoint Assure Application

Le déploiement d'IBM Trusteer Pinpoint Assure sur toute Application nécessite des droits d'utilisation pour IBM Trusteer Pinpoint Assure Application.

IBM Trusteer Pinpoint Assure est disponible à l'achat par application.

1.6.3 IBM Trusteer Mobile Carrier Intelligence et/ou IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Le Client doit tenir à jour son abonnement à IBM Trusteer Pinpoint Assure ou IBM Trusteer Pinpoint Detect avant de s'abonner à ce Service Cloud.

Ce Service Cloud améliore IBM Trusteer Pinpoint Assure et/ou IBM Trusteer Pinpoint Detect en fournissant du contexte et des informations supplémentaires sur les numéros d'appareil mobile fournis à l'un de ces Services Cloud, afin de déterminer le risque de fraude d'une session donnée. Le Client peut interroger le Service Cloud pour connaître les caractéristiques d'un numéro d'appareil mobile donné, par exemple les informations d'opérateur de téléphonie associées à ce numéro.

Les données fournies par ce Service Cloud relatives aux numéros d'appareil mobile (ci-après les « Renseignements Mobiles ») ne peuvent être utilisées que pour les opérations internes du Client et ne peuvent être conservées que pendant une période de trente (30) jours. Le Client doit ré-interroger le Service Cloud à propos du même numéro d'appareil mobile après ladite période, afin d'obtenir des Renseignements Mobiles relatifs à ce numéro et ne pourra pas tout simplement réutiliser les Renseignements Mobiles reçus d'une interrogation précédente. Le Client n'est pas autorisé, sauf dans les cas permis ci-dessus, à mettre en cache, réutiliser ou utiliser conjointement, en tout ou en partie, avec toute exploration de données, ou à archiver l'un quelconque des Renseignements Mobiles.

1.7 IBM Trusteer Remotely Delivered Services

L'offre IBM Trusteer Remotely Delivered Services est disponible en tant que module complémentaire (add-on) en option des Services Cloud Pinpoint Detect Premium et Pinpoint Assure.

1.7.1 IBM Trusteer Project Management and Consultancy Services

Ce service propose jusqu'à 200 heures de services de conseils pendant lesquels IBM réalisera certaines des tâches suivantes :

a. Services de configuration initiale : réunions périodiques fréquentes, services de gestion de projet

b. Policy Manager : support continu

L'offre est disponible à l'achat par Engagement.

1.7.2 IBM Trusteer Security Research Consultancy Services

Ce service de consultation comprend jusqu'à 200 heures de ressources partagées pour l'analyse de sécurité, afin de fournir des services supplémentaires par rapport à la solution définie ainsi qu'un support premium (le cas échéant), et comprend les éléments suivants :

a. Recherche anti-fraude approfondie : réunions hebdomadaires et formation.

b. Support pour les clients prioritaires

c. Enquête et support continus par rapport aux règles personnalisées

L'offre est disponible à l'achat par Engagement.

1.7.3 IBM Trusteer Training Services

Ce service de consultation est conçu pour fournir des services supplémentaires par rapport à la solution définie ainsi qu'un support premium (le cas échéant), et comprend des services de formation au portefeuille Trusteer destinés aux employés du Client.

L'offre est disponible à l'achat par Engagement.

1.8 Services Cloud IBM Trusteer Mobile

1.8.1 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 »).

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 Services ; 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 ne garantit pas que toute création d'application ou de sortie à l'aide des outils mobiles inclus dans IBM Security Mobile SDK fonctionnera, interopérera ou sera compatible avec la plateforme de système d'exploitation mobile ou l'appareil mobile concerné.

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 Échantillons sans aucune obligation de support et « EN L'ÉTAT ». 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.

2. Contenu et protection des données

La Fiche Technique relative au Traitement et à la Protection des données (« Fiche Technique ») contient des informations spécifiques au Service Cloud concernant le type de Contenu autorisé à être traité, les activités de traitement impliquées, les dispositifs de protection des données et les particularités relatives à la restitution du Contenu. Les détails ou clarifications et dispositions, y compris les responsabilités du Client, concernant l'utilisation du Service Cloud et les dispositifs de protection de données, le cas échéant, sont énoncés dans la présente clause. Plusieurs Fiches Techniques peuvent être applicables à l'utilisation du Service Cloud par le Client, en fonction des options sélectionnées par le Client. La Fiche Technique n'est disponible qu'en anglais. Elle n'est pas disponible dans la langue locale. En dépit des pratiques des lois ou coutumes locales, les parties attestent qu'elles comprennent l'anglais qui est une langue appropriée pour l'acquisition et l'utilisation des Services Cloud. La ou les Fiches Techniques ci-dessous s'appliquent au Service Cloud et ses options disponibles. Le Client accepte i) qu'IBM peut, à son entière discrétion, modifier de temps en temps la Fiche Technique et ii) que de telles modifications remplaceront les versions précédentes. Les modifications apportées à la Fiche Technique auront pour objectif i) d'améliorer ou de clarifier les engagements existants ii) de conserver la conformité aux normes actuelles et aux lois applicables ou iii) de fournir des engagements supplémentaires. La sécurité du service Cloud ne sera en aucun cas affectée par les modifications apportées à la Fiche Technique.

Lien(s) vers la ou les Fiches Techniques applicables :

IBM Trusteer Mobile SDK

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439

IBM Trusteer Mobile Secure Browser

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492579396

IBM Trusteer Pinpoint Assure

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=CF0C527046E011E8ADCBA344DE8FB657

IBM Trusteer Pinpoint Criminal Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489853624

IBM Trusteer Pinpoint Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=3D3DA0C0E5F711E5A3808DA17FABE9B1

IBM Trusteer Pinpoint Malware Detection

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489595035

IBM Trusteer Rapport

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402483908375

IBM Trusteer Pinpoint Verify

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

(La fiche technique d'IBM Cloud Identity Verify reflète IBM Trusteer Pinpoint Verify)

Le Client est tenu de prendre les mesures nécessaires pour commander, activer ou utiliser les dispositifs de protection de données disponibles pour un Service Cloud et reconnaît être responsable de l'utilisation des Services Cloud si le Client ne parvient pas à prendre lesdites mesures, notamment à se conformer à toute obligation de protection de données ou autre exigence légale relative au Contenu.

L'addendum d'IBM relatif au Traitement de Données à caractère personnel, disponible sur http://ibm.com/dpa (DPA), s'applique à ou aux Annexes DPA et en fait partie intégrante, si et dans la mesure où le Règlement général européen sur la protection des données (EU/2016/679) (RGPD) s'applique aux données à caractère personnel figurant dans le Contenu. La ou les Fiches Techniques applicables pour ce Service Cloud constitueront la ou les Annexes DPA. Si le DPA s'applique, l'obligation d'IBM d'informer les Sous-traitants ultérieurs des modifications et le droit du Client à s'opposer à de telles modifications s'appliquent comme défini dans le DPA.

2.1 Contrat EULA et Bases pour le Traitement de Données pour les Personnes Concernées

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

Sauf indication contraire et conformément aux principes de traitement que le Client a établis lui-même, le Client autorise IBM à fournir le Contrat de Licence Utilisateur Final disponible sur https://www.trusteer.com/support/end-user-license-agreement pour permettre à IBM de collecter et traiter les informations nécessaires à la prestation des Services Cloud.

2.2 Utilisation de Données

IBM n'utilisera ou ne communiquera pas les résultats découlant de l'utilisation du Service Cloud par le Client qui sont exclusivement liés à au Contenu du Client (Observations) ou qui identifient le Client de quelque autre manière. IBM peut cependant utiliser le Contenu et d'autres informations (sauf les Observations) issues du Contenu lors de la fourniture du Service Cloud après avoir supprimé les identifiants personnels de sorte que les données à caractère personnel ne puissent plus être attribuées à un individu en particulier sans l'utilisation d'informations supplémentaires. IBM utilisera de telles données uniquement à des fins de recherche, de test et de développement d'offres.

2.3 Traitement et Stockage des Données

2.3.1 Informations supplémentaires concernant les pays de traitement

Pour les services Trusteer Pinpoint Verify, tous les sites d'hébergement et de traitement sont indiqués dans la Fiche Technique correspondante.

Pour tous les autres services fournis via le centre de données allemand, IBM limitera le traitement des Données à caractère personnel au pays de l'entité contractante d'IBM et aux pays suivants : Allemagne, Israël, Irlande, Pays-Bas, ainsi qu'à tout autre pays énuméré dans la fiche technique applicable pour les Sous-traitants ultérieurs tiers d'IBM.

Pour tous les autres services fournis via le centre de données japonais, IBM limitera le traitement des Données à caractère personnel au pays de l'entité contractante d'IBM et aux pays suivants : Japon, Israël, Irlande, ainsi qu'à tout autre pays énuméré dans la fiche technique applicable pour les Sous-traitants ultérieurs tiers d'IBM.

Pour tous les autres services fournis via le centre de données américain, IBM limitera le traitement des Données à caractère personnel au pays de l'entité contractante d'IBM et aux pays suivants : Etats-Unis, Israël, Irlande, Singapour, Australie, ainsi qu'à tout autre pays énuméré dans la fiche technique applicable pour les Sous-traitants ultérieurs tiers d'IBM.

Le support et les services de maintenance de compte IBM Trusteer peuvent également être fournis selon les besoins, en fonction de la disponibilité du personnel IBM concerné, de l'emplacement du Client et du centre de données où les données sont hébergées.

2.3.2 Données du Détenteur de Compte

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.

2.3.3 Solutions Intégrées

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.

3. 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.

3.1 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.

3.2 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)
< 99,9 %	2 %
< 99,0 %	5 %
< 95,0 %	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 Dédommagement 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 :

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

4. 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 Support est disponible moyennant un supplément, à l'exception des Services Cloud **IBM Trusteer Mobile SDK**, **IBM Trusteer Rapport Mandatory Service**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital Content Pack** et **IBM Trusteer Mobile Carrier Intelligence**. 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 disponible sur https://www.ibm.com/software/support/saas_support_guide.html.
- 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 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.ibm.com/software/security/trusteer/support/.
- Pour les options de support et des détails, accédez au Guide de Support SaaS IBM disponible sur https://www.ibm.com/software/support/saas_support_guide.html.

5. Droits d'Utilisation et Informations de Facturation

5.1 Unités de mesure des redevances

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

- Engagement : unité de mesure par laquelle les services peuvent être acquis. Un Engagement comprend des services professionnels et/ou de formation relatifs au Service Cloud. Des droits d'utilisation suffisants sont nécessaires pour couvrir chaque Engagement.
- 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.
- 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.
- 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 les besoins de ce Service Cloud, une Application est une Application Business ou Retail unique du Client.
- Appel API : unité de mesure par laquelle le Service Cloud peut être acquis. Un Appel d'API désigne l'invocation du Service Cloud par le biais d'une interface programmable. Des droits d'utilisation suffisants sont nécessaires pour couvrir le nombre total d'Appels d'API, arrondi à la dizaine la plus proche, pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (« PoE ») ou le Document de Transaction du Client.
- Connexion : unité de mesure par laquelle le Service Cloud peut être acheté. Une Connexion est une liaison ou une association d'une base de données, d'un serveur, d'une application ou de tout autre type de périphérique au Service Cloud. Des Droits d'Utilisation suffisants doivent être obtenus pour couvrir le nombre total de Connexions établies avec le Service Cloud pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (« PoE ») ou le Document de Transaction du Client.

Pour les besoins de ce Service Cloud, une Connexion est une session ou un flux dans l'Application du Client.

5.2 Redevances de dépassement

Si l'utilisation réelle du Service Cloud pendant la période de mesure dépasse les droits indiqués dans l'Autorisation d'Utilisation (ou « PoE »), un excédent sera facturé au prix indiqué dans le Document de Transaction au cours du mois suivant ledit excédent.

5.3 Fréquence de facturation

En fonction de la fréquence de facturation sélectionnée, IBM facturera au Client les redevances exigibles au début de la période de la fréquence de facturation, à l'exception des redevances dues pour dépassement et des frais d'utilisation qui seront facturés à terme échu.

6. 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. Les renouvellements sont soumis à une augmentation de prix annuelle tel que spécifié dans le devis. En cas de renouvellement automatique à la suite d'une notification de retrait du Service Cloud de la part d'IBM, la durée de renouvellement prend fin au plus tôt à la fin de la durée de renouvellement actuelle ou à la date du retrait annoncé.

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.

7. Dispositions Additionnelles

7.1 Dispositions générales

Le Client accepte qu'IBM puisse désigner publiquement le Client en tant qu'abonné aux Services Cloud dans les communications publicitaires ou marketing.

Le Client ne pourra pas utiliser les Services Cloud, seuls ou conjointement avec d'autres services ou produits, à l'appui de l'une quelconque des activités à haut risque suivantes : conception, construction, contrôle ou maintenance d'installations nucléaires, de systèmes de transport en commun, de systèmes de contrôle du trafic aérien, de systèmes de contrôle automobiles, de systèmes d'armement, de systèmes de navigation ou de communication aériennes ou toute autre activité où toute défaillance du Service Cloud pourrait entraîner un risque matériel de mort ou de blessures corporelles graves.

7.2 Logiciels d'Activation

Le Service Cloud nécessite des logiciels d'activation que le Client télécharge vers ses systèmes pour faciliter l'utilisation du Service Cloud. Le Client est autorisé à utiliser les logiciels d'activation uniquement en association avec son utilisation du Service Cloud. Les logiciels d'activation sont fournis « EN L'ETAT ».

7.3 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.