IBM Trusteer Pinpoint Detect

Ce Descriptif de Services détaille le Service Cloud. Les bons de commande applicables contiennent les prix et des détails supplémentaires concernant la commande du Client.

1. Service Cloud

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. Trusteer Management Application (TMA) et Trustboard :

TMA est une application de gestion traditionnelle de Trusteer qui permet aux Client d'évaluer et de classifier les alertes. Trustboard est une application de gestion plus récente qui est utilisée essentiellement pour la recherche. Les Clients peuvent choisir d'utiliser soit TMA, soit Trustboard à un moment donné. TMA et Trustboard sont chacun disponibles dans l'environnement d'hébergement cloud d'IBM Trusteer, au moyen desquels 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, souscrire et configurer la distribution des flux de menace générés à partir des offres Pinpoint. IBM Trusteer Pinpoint Detect et IBM Trusteer Pinpoint Verify sont utilisés dans le cadre de la connexion TMA et Trustboard.

b. Script Web et/ou API :

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

Une « Session » est une interaction entre l'Application (Web ou Mobile) du Client et le Service Cloud qui génère une ou plusieurs évaluations des risques en temps réel. Une Session est mesurée entre le début de l'interaction et la fin de l'interaction. La fin d'une interaction est enregistrée lorsqu'un des événements suivants se produit :

- L'interaction est réinitialisée selon la procédure normale de déconnexion de l'application.
- Le navigateur, l'application ou l'onglet est fermé.
- Les cookies sont supprimés.
- Le délai d'expiration est dépassé.

Une Session peut inclure n'importe quel nombre d'activités telles que la connexion, la navigation, la réservation, la configuration du paiement et d'autres activités définies par l'Application du Client. Il est précisé, dans le cadre de ce Service Cloud, qu'une Connexion (telle qu'elle est définie ci-dessous) représente une Session.

1.1 Offres

Le Client peut faire son choix parmi les offres disponibles qui suivent.

1.1.1 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. Ce Service peut

également être utilisé pour les accès à distance du personnel afin d'évaluer les risques à partir de périphériques gérés et non gérés.

Le support Premium (tel qu'il est défini dans la clause Support Technique ci-dessous) est inclus dans ce Service Cloud.

Le service est disponible à l'achat par lots de 100 Participants Admissibles ou de 100 Connexions.

1.1.2 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 supplémentaire 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.

1.1.3 IBM Trusteer Pinpoint Detect for Connections

Ce Service Cloud assure la protection, vise à détecter les tentatives de piratage de compte et fournit des scores d'évaluation de risque/fiabilité des navigateurs et/ou des appareils mobiles (par le biais du navigateur natif de l'application mobile du Client) accédant à une Application Business ou Retail. La solution utilise divers indicateurs de risque analysant l'appareil, la connexion et le comportement de l'utilisateur final et les compare à l'historique de l'utilisateur pour identifier toute utilisation suspecte.

Le Service Cloud peut consommer les connexions des canaux Mobile et Web. IBM Trusteer Pinpoint Detect inclut le droit d'utilisation d'IBM Trusteer Mobile SDK, le cas échéant.

Le Service Cloud est disponible à l'achat par lots de 100 Connexions par an.

1.2 Services Optionnels

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

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

Une Application Client désigne une Application Web et/ou une Application Mobile. Une Application Web regroupe toutes les fonctions fournies aux Participants Admissibles du Client par le biais de plusieurs pages Web, à partir d'un écran de connexion ou d'identification et surveillées sous la forme d'une Application unique dans la console Trusteer (Trusteer Management Application). Une Application Mobile regroupe toutes les fonctions fournies aux Participants Admissibles du Client par le biais d'un seul programme logiciel qui peut être téléchargé à partir d'un magasin d'applications (magasin), à partir d'un écran de connexion ou d'identification et surveillées sous la forme d'une Application unique dans la console Trusteer (Trusteer Management Application).

L'intégration d'IBM Trusteer Pinpoint nécessite des droits d'utilisation d'IBM Trusteer Pinpoint Application pour chaque Application.

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

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

Une Application Client désigne une Application Web et/ou une Application Mobile. Une Application Web regroupe toutes les fonctions fournies aux Participants Admissibles du Client par le biais de plusieurs pages Web, à partir d'un écran de connexion ou d'identification et surveillées sous la forme d'une Application unique dans la console Trusteer (Trusteer Management Application). Une Application Mobile regroupe toutes les fonctions fournies aux Participants Admissibles du Client par le biais d'un seul programme logiciel qui peut être téléchargé à partir d'un magasin d'applications (magasin), à partir d'un écran de connexion ou d'identification et surveillées sous la forme d'une Application unique dans la console Trusteer (Trusteer Management Application).

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 Premium nécessite des droits d'utilisation d'IBM Trusteer Pinpoint Detect Premium Application pour chaque Application.

1.2.3 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.

1.2.4 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.

1.2.5 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).

1.2.6 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.

1.2.7 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.

1.2.8 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 :

Les Clients peuvent choisir d'utiliser soit TMA, soit Trustboard à un moment donné. Le Client (et un nombre illimité des membres de son personnel autorisé) peut utiliser l'application TMA ou Trustboard 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.

1.2.9 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 :

Les Clients peuvent choisir d'utiliser soit TMA, soit Trustboard à un moment donné. Le Client (et un nombre illimité des membres de son personnel autorisé) peut utiliser l'application TMA ou Trustboard 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.

1.2.10 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. Aux fins du présent Descriptif de Services, le Détenteur du Compte désigne l'utilisateur final du Client, ayant installé le logiciel d'activation client, accepté le contrat de licence utilisateur final (« CLUF ») et s'étant authentifié au moins une fois avec l'Application Business ou Retail du Client pour laquelle le Client a souscrit à la couverture du Service Cloud. Le Logiciel Client Détenteur du Compte désigne le logiciel client IBM Trusteer Rapport ou tout autre logiciel client fourni avec certains Services Cloud pour être installé sur l'appareil de l'utilisateur final.

1.2.11 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.

1.2.12 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.

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

- 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.

1.2.14 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 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.

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

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

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

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

Ce Service Cloud améliore 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.

1.3 Services d'accélération

1.3.1 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.

1.3.2 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.

1.3.3 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.

2. Fiches Techniques sur le Traitement et la Protection des Données

L'Addendum d'IBM relatif au Traitement de Données à caractère personnel, disponible sur http://ibm.com/dpa (DPA) et la ou les Fiches Techniques (désignées par fiche(s) technique(s) ou Annexe(s) DPA) dans les liens ci-dessous contiennent des informations additionnelles sur la protection des données pour les Services Cloud et leurs options concernant les types de Contenus pouvant être traités, les activités de traitement impliquées, les dispositifs de protection des données et les détails de conservation et de retour de Contenu. Le DPA s'applique aux Données à caractère personnel du Contenu dans la mesure où i) Le Règlement Général sur la Protection des Données (UE/2016/679) (RGPD) ; ou ii) d'autres lois relatives à la protection des données identifiées sur http://ibm.com/dpa/dpl s'appliquent.

Il est précisé que les Fiches Techniques répertorient généralement tous les sites dans lesquels IBM (y compris tout sous-traitant ultérieur tiers) héberge et traite des Données à caractère personnel, quel que soit le centre de données à partir duquel les services sont déployés. Pour obtenir la liste des sites d'hébergement et de traitement spécifiques au centre de données à partir duquel les services sont déployés, voir la clause 5.2 ci-dessous (Informations supplémentaires concernant les pays de traitement).

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 Mobile SDK

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

3. Niveaux de Service et Support Technique

3.1 Accord Relatif aux Niveaux de Service

IBM fournit au Client l'Accord relatif aux Niveaux de Service (« SLA ») de disponibilité ci-dessous. IBM appliquera le dédommagement correspondant le plus élevé, en fonction de la disponibilité cumulée du Service Cloud, comme indiqué dans le tableau ci-dessous. Le pourcentage de disponibilité est calculé comme suit : le nombre total de minutes d'un mois contractuel moins le nombre total de minutes d'indisponibilité du Service au cours du mois contractuel, divisé par le nombre total de minutes du mois contractuel. La définition de l'indisponibilité du Service, la procédure de réclamation et les moyens de contacter IBM concernant les problèmes de disponibilité de service figurent dans le guide de support de Services Cloud d'IBM à l'adresse https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilité	Avoir (% de redevance d'abonnement mensuelle*)
Inférieure à 99,9 %	2 %
Inférieure à 99,0 %	5 %
Inférieure à 95,0 %	10 %

* La redevance d'abonnement est le prix contractuel pour le mois objet de la réclamation.

3.2 Support Technique

Le support technique destiné au Service Cloud, y compris les coordonnées des personnes à contacter, les niveaux de gravité, les heures de disponibilité, les temps de réponse ainsi que d'autres informations et processus relatifs au support technique sont disponibles en sélectionnant le Service Cloud dans le guide de support IBM disponible à l'adresse https://www.ibm.com/support/home/pages/support-guide/.

Support Premium :

Un abonnement au Support Premium est disponible pour le Service Cloud moyennant un supplément et comprend ce qui suit :

- 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/.

4. Montant des Redevances

4.1 Unités de mesure des redevances

Les unités de mesure des redevances du Service Cloud sont indiquées dans le Document de Transaction.

Les unités de redevances suivantes s'appliquent à ce Service Cloud :

- Un Engagement est un service professionnel ou de formation relatif aux Services Cloud.
- Un Participant Admissible est un individu ou une entité habilitée à prendre part à un programme de prestation de service géré ou suivi par les Services Cloud.
- Une Application est un logiciel portant un nom unique qui est développé ou mis à disposition pour accéder aux Services Cloud ou être utilisé par les Services Cloud.
- Un Appel d'API désigne l'invocation des Services Cloud par le biais d'une interface programmable.
- 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 mis ou qui a été mis à disposition des Services Cloud.

4.2 Redevances des Services à Distance

Un service à distance arrive à expiration 90 jours suivant l'acquisition, que le service à distance ait été utilisé ou non.

5. Dispositions Additionnelles

Pour les Contrats de Services Cloud (ou des contrats Cloud de base équivalents) signés avant le 1er janvier 2019, les dispositions énoncées à l'adresse https://www.ibm.com/acs s'appliquent.

5.1 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 d'Utilisateur Final disponible sur https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA pour permettre à IBM de collecter et traiter les informations nécessaires à la prestation des Services Cloud.

Pour les Services Cloud IBM Trusteer Rapport, le Client autorise IBM, en tant que sous-traitant de données de l'Entreprise Participante, à utiliser le Logiciel pour collecter des logiciels malveillants et des artefacts malveillants, par exemple des fichiers associés à des activités malveillantes, ou des fichiers associés à un dysfonctionnement inhabituel du Logiciel. IBM n'utilise pas le Logiciel pour cibler des fichiers contenant les informations personnelles de l'utilisateur final ; cependant, les fichiers collectés peuvent contenir des données à caractère personnel obtenues par le logiciel malveillant sans l'autorisation de l'utilisateur final. IBM s'engage 1) à supprimer rapidement les fichiers non pertinents pour une telle analyse, et 2) à conserver les fichiers pertinents uniquement pendant la durée de l'analyse et en aucun cas plus de trois mois.

5.2 Informations supplémentaires concernant les pays de traitement

Tous les services d'hébergement et de traitement des Données à caractère personnel, y compris par des sous-traitants ultérieurs tiers cités dans la Fiche Technique, seront réalisés dans les sites indiqués ci-dessous :

Pour tous les services fournis via le centre de données allemand, IBM limitera l'hébergement et le traitement des Données à caractère personnel au pays de l'entité contractante d'IBM et aux pays suivants: Allemagne, Israël, Irlande et Pays-Bas.

Pour tous les services fournis via le centre de données japonais, IBM limitera l'hébergement et le traitement des Données à caractère personnel au pays de l'entité contractante d'IBM et aux pays suivants: Japon, Israël et Irlande.

Pour tous les services fournis via le centre de données américain, IBM limitera l'hébergement et le traitement des Données à caractère personnel au pays de l'entité contractante d'IBM et aux pays suivants : Etats-Unis, Israël, Irlande, Singapour et Australie.

Outre les sites susmentionnés, en ce qui concerne tous les services fournis via les centres de données en Allemagne, au Japon et aux Etats-Unis, (1) les données de support peuvent être hébergées ou traitées en Allemagne et en France par Salesforce.Com en tant que sous-traitant ultérieur tiers d'IBM et (2) pour les clients qui choisissent d'envoyer des données aux fournisseurs Mobile Carrier Intelligence, les Données à caractère personnel peuvent être hébergées et traitées dans les pays des sous-traitants

ultérieurs tiers concernés, comme indiqué dans la Fiche Technique. Nonobstant toute disposition contraire dans la Fiche Technique, il est possible que les sous-traitants ultérieurs tiers indiqués dans la clause (2) de la phrase précédente ne soient pas conformes à la norme ISO 27001 ou SOC2.

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.

5.3 Données du Détenteur de Compte

A des fins d'éclaircissement, si plusieurs clients d'IBM sont affiliés au Logiciel du Client Détenteur de Compte d'un Détenteur de Compte particulier (ces clients d'IBM étant dénommés « Clients Affiliés ») et que les services objet du présent Descriptif de Services sont fournis par IBM à ces Clients Affiliés par le biais de centres de données dans différentes régions, les données du Détenteur de Compte peuvent être traitées dans tous les sites associés à chacun desdits centres de données, comme indiqué dans la clause 5.2 ci-dessus.

5.4 Solutions Intégrées

A des fins d'éclaircissement, les diverses offres sous la marque Trusteer peuvent constituer une solution intégrée. Par conséquent, si le Client résilie l'un des présents Services Cloud, IBM peut conserver les données du Client en vue de fournir au Client les Services Cloud restants ainsi que d'autres services Trusteer, conformément aux descriptions de service applicables à ces autres services Trusteer.

5.5 Logiciels d'Activation

Le Service Cloud contient le Logiciel d'Activation suivant :

- IBM Rapport Agents

5.6 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).

5.7 Données collectées dans le cadre du déploiement

Le déploiement du Service Cloud peut comporter la fourniture de certaines données du Client à IBM. Ces données ne devront pas comprendre des informations susceptibles de remonter à l'identité ou d'être attribuées à certaines personnes en particulier. Des directives supplémentaires applicables aux données fournies à IBM dans le cadre du déploiement sont incluses dans les Instructions de Déploiement Trusteer devant être fournies au Client.

6. Dispositions dérogatoires

6.1 Utilisation de Données

La disposition suivante prévaut sur toute disposition contraire dans la clause « Contenu et protection des données » des conditions cadre de Service Cloud entre les parties : IBM n'utilisera ou ne communiquera pas les résultats découlant de l'utilisation du Service Cloud par le Client qui sont exclusivement liés au Contenu (Observations) du Client ou qui identifient le Client de quelque autre manière. IBM utilisera cependant le Contenu et d'autres informations issues du Contenu (à l'exception des analyses) dans le cadre du Service Cloud en vue d'améliorer le Service Cloud. IBM peut également partager des identificateurs de menaces et d'autres informations de sécurité intégrées au Contenu à des fins de détection des menaces et de protection.