IBM Trusteer Fraud Protection

La presente Descrizione dei Servizi descrive il Servizio Cloud che IBM fornisce al Cliente. Il termine "Cliente" indica il contraente, i relativi utenti autorizzati e i destinatari del Servizio on Cloud. La quotazione economica dei servizi e la PoE (Proof of Entitlement) sono forniti come Documenti d'Ordine separati.

1. Servizio in Cloud

La presente Descrizione dei Servizi è inerente ai seguenti Servizi Cloud:

Servizi Cloud Pinpoint Assure:

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

Servizi 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

Servizi 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

Servizi CloudMobile:

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

1.1 Servizi Cloud Business e Retail

I Servizi Cloud IBM Trusteer sono forniti su licenza per essere utilizzati con Applicazioni specifiche. Un'Applicazione viene definita da una delle seguenti tipologie: "Retail" o "Business". Sono disponibili offerte separate per le Applicazioni "Retail" o "Business".

a. Un'Applicazione "Retail" viene definita come applicazione di online banking, applicazione per dispositivi mobili o applicazione di e-commerce, progettata per fornire assistenza agli utenti. Le policy del Cliente possono classificare come eleggibili alcune aziende di piccole dimensioni per l'accesso alle applicazioni "retail".

b. Un'Applicazione "Business" viene definita come applicazione di online banking, applicazione per dispositivi mobili o applicazione di e-commerce, progettata per fornire assistenza persone

giuridiche, istituzioni o soggetti equivalenti, oppure qualsiasi applicazione che non sia classificata come "Retail".

1.1.1 Servizi 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 Servizi 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

Per ciascun Servizio Cloud di tipo "Business" e "Retail", è disponibile il prodotto Supporto Premium (Premium Support) associato ad un costo aggiuntivo, ad eccezione dei Servizi Cloud IBM Trusteer Mobile SDK.

1.1.3 Ulteriori Servizi Cloud per IBM Trusteer Rapport II

a. Ulteriori Servizi Cloud disponibili per 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. Ulteriori Servizi Cloud disponibili per 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

Per ciascun componente aggiuntivo "Business" e "Retail" per i Servizi Cloud IBM Trusteer Rapport è disponibile ad un costo aggiuntivo il prodotto Supporto Premium associato, ad eccezione dei componenti aggiuntivi IBM Trusteer Rapport Mandatory Service.

L'abbonamento a IBM Trusteer Rapport II for Business o IBM Trusteer Rapport II for Retail è un prerequisito per ulteriori Servizi Cloud associati, elencati in questo articolo.

1.1.4 Ulteriori Servizi Cloud per IBM Trusteer Pinpoint Malware Detection II

a. Ulteriori Servizi Cloud disponibili per IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business o 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. Ulteriori Servizi Cloud disponibili per IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail o 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

Il Supporto Premium è disponibile per offerte specifiche, come specificato nel presente documento. L'abbonamento a IBM Trusteer Pinpoint Malware Detection II for Business o IBM Trusteer Pinpoint Malware Detection II for Retail è un prerequisiti per gli ulteriori Servizi Cloud associati elencati nel presente articolo.

1.1.5 Ulteriori Servizi Cloud disponibili per IBM Trusteer Pinpoint Detect Standard e/o IBM Trusteer Pinpoint Detect Premium e/o IBM Trusteer Pinpoint Detect Standard for Retail e/o IBM Trusteer Pinpoint Detect Premium for Retail e/o IBM Trusteer Pinpoint Detect Standard for Business e/o IBM Trusteer Pinpoint Detect Premium for Business

a. Ulteriori Servizi Cloud disponibili per IBM Trusteer Detect Standard for Business e/o 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. Ulteriori Servizi Cloud disponibili per IBM Trusteer Detect Standard for Retail e/o 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. Ulteriori Servizi Cloud disponibili per IBM Trusteer Pinpoint Detect Standard and/or IBM Trusteer Pinpoint Premium:

- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application

d. Ulteriori Servizi Cloud disponibili per IBM Trusteer Pinpoint Detect Premium

- IBM Trusteer Pinpoint Verify

L'abbonamento a IBM Trusteer Pinpoint Detect Standard o IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard for Retail o IBM Trusteer Pinpoint Detect Premium for Retail o IBM Trusteer Pinpoint Detect Standard for Business o IBM Trusteer Pinpoint Detect Premium for Business rappresenta un prerequisito per i Servizi Cloud aggiuntivi elencati nel presente Articolo.

1.1.6 Ulteriori Servizi Cloud

Qualsiasi ulteriore abbonamento ai Servizi Cloud, inerente agli abbonamenti base di cui sopra, non elencato nel presente documento, attualmente disponibile o in fase di sviluppo, non è considerato un aggiornamento e deve essere fornito separatamente.

1.2 Definizioni

Titolare dell'Account – Indica l'utente finale del Cliente, che ha installato il prerequisito software client, ha accettato l'Accordo di licenza per l'utente finale (End User License Agreement, "EULA") e si è autenticato almeno una volta nell'Applicazione "Retail" o "Business" del Cliente per cui il Cliente ha sottoscritto l'abbonamento per la copertura dei Servizi Cloud.

Software Client del Titolare dell'Account – Indica il software di abilitazione client IBM Trusteer Rapport oppure qualsiasi altro software di abilitazione client fornito con alcuni Servizi Cloud per l'installazione sul dispositivo dell'utente finale.

Trusteer Splash – Indica lo splash (schermata di caricamento) che viene fornito al Cliente in base ai modelli splash disponibili.

Pagina di destinazione – Indica la pagina ospitata da IBM fornita al Cliente insieme agli 'splash' del Cliente e al Software Client del Titolare dell'Account scaricabile.

1.3 Servizi Cloud IBM Trusteer Rapport

1.3.1 IBM Trusteer Rapport II for Retail e/o IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Il Servizio Cloud Trusteer Rapport II è una nuova costruzione di IBM Trusteer Rapport per aiutare a standardizzare i corrispettivi relativi alla protezione di più Applicazioni e sostituisce i corrispettivi una tantum quando si aggiungono le Applicazioni.

Trusteer Rapport II fornisce un livello di protezione dal phishing e dagli attacchi malware di tipo "Man-in-the-Browser" (MitB). Utilizzando una rete di oltre dieci milioni di endpoint in tutto il mondo, IBM Trusteer Rapport raccoglie informazioni sugli attacchi di phishing e malware perpetrati contro le organizzazioni a livello mondiale. IBM Trusteer Rapport applica degli algoritmi comportamentali finalizzati al blocco degli attacchi di phishing e ad impedire l'installazione e le attività dei malware MitB.

Questo Servizio Cloud è autorizzato per il calcolo dei corrispettivi del Partecipante Eleggibile o del Dispositivo Client. L'offerta "Business" è venduta in pacchetti di 10 Partecipanti Eleggibili o 10 Dispositivi Client. L'offerta "Retail" è venduta in pacchetti di 100 Partecipanti Eleggibili o 100 Dispositivi Client.

La presente offerta di Servizio Cloud include:

a. Trusteer Management Application ("TMA"):

   L'applicazione TMA è disponibile nell'ambiente ospitato dal cloud IBM Trusteer, attraverso cui il Cliente (e un numero illimitato dei suoi dipendenti autorizzati del Cliente) può: (i) visualizzare e scaricare la reportistica dei dati di determinati eventi e le valutazioni del rischio, e (ii) visualizzare la configurazione del prerequisito software client fornita su licenza ai Partecipanti Eleggibili, disciplinata da un accordo di licenza per l'utente finale (end user license agreement, "EULA") senza oneri aggiuntivi, disponibile per il download sui desktop o dispositivi dei Partecipanti Eleggibili (PC/MAC), noto anche come suite del software Trusteer Rapport ("Software Client del Titolare dell'Account"). Il Cliente potrà solo commercializzare il Software Client del Titolare dell'Account mediante Trusteer Splash o Rapport API, e non potrà utilizzare il Software Client del Titolare dell'Account per attività aziendali interne o ad uso dei propri dipendenti (usi diversi da quelli personali dei dipendenti).

b. Script Web:

   Per accedere su un sito web allo scopo di accedere ed utilizzare il Servizio Cloud.

c. Dati sugli eventi:

   Il Cliente (e un numero illimitato dei suoi dipendenti autorizzati) può utilizzare l'applicazione TMA per ricevere i dati sugli eventi generati dal Software Client del Titolare dell'Account, derivanti dalle interazioni online del Titolare dell'Account con le proprie Applicazioni "Business" o "Retail" per cui il Cliente ha sottoscritto l'abbonamento per la copertura del Servizio Cloud. I dati sugli eventi saranno ricevuti dal Software Client del Titolare dell'Account dei Partecipanti Eleggibili in esecuzione nei relativi dispositivi, che hanno accettato l'accordo EULA, si sono autenticati almeno una volta con l'Applicazione "Business" o "Retail" del Cliente e la configurazione del Cliente deve includere la raccolta degli ID utente.

d. Trusteer Splash:

   La piattaforma di marketing Trusteer Splash identifica e commercializza il Software Client del Titolare dell'Account per i Partecipanti Eleggibili che accedono alle Applicazioni "Business" e/o "Retail" del Cliente per le quali il Cliente ha sottoscritto l'abbonamento a copertura del Servizio Cloud. Il Cliente può selezionare tra i Modelli Splash disponibili. Gli 'splash' personalizzati possono essere oggetto di contratto in un accordo o allegato (statement of work) separato.

Il Cliente può decidere di fornire i propri marchi, i loghi o le icone per utilizzarli insieme all'applicazione TMA e solo con Trusteer Splash, e per visualizzarli nel Software Client del Titolare dell'Account o sulle pagine di destinazione ospitate da IBM e sul sito web IBM Trusteer. Qualsiasi utilizzo dei marchi, dei loghi o delle icone fornite dal Cliente avverrà in conformità con le policy di IBM in materia di pubblicità ed utilizzo dei marchi.

Il Cliente deve sottoscrivere l'abbonamento al Servizio Cloud IBM Trusteer Rapport Mandatory Service qualora desideri avvalersi di qualsiasi tipo di installazione obbligatoria del Software Client del Titolare dell'Account.

L'installazione obbligatoria del Software Client del Titolare dell'Account include, a titolo esemplificativo ma non esaustivo, qualsiasi meccanismo o strumento che induce, in modo diretto o indiretto, il Partecipante Eleggibile a scaricare il Software Client del Titolare dell'Account o qualsiasi metodo, strumento, procedura, accordo o meccanismo non creato o approvato da IBM, creato per aggirare i requisiti di licenza di questa implementazione obbligatoria del Software Client del Titolare dell'Account.

Trusteer Rapport II for Business e/o Trusteer Rapport II for Retail includono ciascuno la protezione per un'Applicazione. Per ciascuna Applicazione aggiuntiva, il Cliente dovrà ottenere la titolarità per le Applicazioni aggiuntive di IBM Trusteer Rapport.

1.3.2 Ulteriori Servizi Cloud aggiuntivi opzionali per IBM Trusteer Rapport II for Business e/o IBM Trusteer Rapport II for Retail

L'abbonamento ai Servizi Cloud IBM Trusteer Rapport II è un prerequisito per l'abbonamento a qualsiasi ulteriore Servizio IBM Cloud indicato di seguito. Se per il Servizio Cloud è specificato "for Business", anche gli ulteriori Servizi Cloud acquistati devono avere la stessa indicazione "for Business". Se per il Servizio Cloud è specificato "for Retail", anche i Servizi Cloud aggiuntivi acquistati devono avere la stessa indicazione "for Retail". Il Cliente riceverà i dati sugli eventi dai Partecipanti Eleggibili o dai Dispositivi Client che eseguono il Software Client del Titolare dell'Account, hanno accettato l'accordo EULA, si sono autenticati almeno una volta nell'Applicazione "Business" o "Retail" del Cliente e la configurazione del Cliente deve includere la raccolta degli ID utente.

1.3.3 IBM Trusteer Rapport Fraud Feeds for Business e/o IBM Trusteer Rapport Fraud Feeds for Retail

Quando si effettua l'abbonamento a questo Servizio Cloud aggiuntivo, il Cliente (e un numero illimitato di dipendenti autorizzati del Cliente) può utilizzare l'applicazione TMA per visualizzare, sottoscrivere, e configurare la fornitura dei feed sulle minacce dal Servizio Cloud Trusteer Rapport. I feed possono essere inviati mediante email all'indirizzo email designato o tramite SFTP come file di testo.

Questa offerta è autorizzata unicamente per il calcolo dei corrispettivi del Partecipante Eleggibile.

1.3.4 IBM Trusteer Rapport Phishing Protection for Business e/o IBM Trusteer Rapport Phishing Protection for Retail

Il Cliente (e un numero illimitato dei suoi dipendenti autorizzati del Cliente) può utilizzare l'applicazione TMA per ricevere le notifiche sui dati di eventi relativi all'inserimento delle credenziali di accesso del Titolare dell'Account in un sito di phishing o potenzialmente fraudolento. Alcune applicazioni online legittime (URL) potrebbero essere state erroneamente contrassegnate come siti di phishing determinando l'invio da parte del Servizio Cloud di un avviso ai Titolari dell'Account con la segnalazione che un sito legittimo è un sito di phishing. In tal caso, il Cliente è tenuto a segnalare l'errore a IBM, che dovrà correggerlo. Tale operazione rappresenta l'unico rimedio che il Cliente deve mettere in atto per tali tipi di errore.

Questo Servizio Cloud è autorizzato per il calcolo dei corrispettivi del Partecipante Eleggibile o del Dispositivo Client. L'offerta "Business" è venduta in pacchetti di 10 Partecipanti Eleggibili o 10 Dispositivi Client. L'offerta "Retail" è venduta in pacchetti di 100 Partecipanti Eleggibili o 100 Dispositivi Client.

Il supporto Premium può essere ottenuto per questi servizi cloud, per il calcolo dei corrispettivi del Partecipante Eleggibile o del Dispositivo Client. L'offerta "Business" è venduta in pacchetti di 10 Partecipanti Eleggibili o 10 Dispositivi Client. L'offerta "Retail" è venduta in pacchetti di 100 Partecipanti Eleggibili o 100 Dispositivi Client.

1.3.5 IBM Trusteer Rapport Mandatory Service for Business e/o IBM Trusteer Rapport Mandatory Service for Retail

Il Cliente può utilizzare un'istanza della piattaforma di marketing Trusteer Splash per imporre il download del Software Client del Titolare dell'Account ai Partecipanti Eleggibili che accedono alle Applicazioni "Business" e/o "Retail" del Cliente, per le quali il Cliente ha sottoscritto l'abbonamento a copertura dei Servizi Cloud.

IBM Trusteer Rapport Premium Support for Business è un prerequisito per IBM Security Rapport Mandatory Service for Business.

IBM Trusteer Rapport Premium Support for Retail è un prerequisito per IBM Security Rapport Mandatory Service for Retail.

Il Cliente può implementare la funzionalità aggiuntiva IBM Trusteer Rapport Mandatory Service solo se è stata ordinata e configurata per essere utilizzata con l'Applicazione "Business" o "Retail" per la quale il Cliente ha sottoscritto l'abbonamento per la copertura dei Servizi Cloud.

Questo Servizio Cloud è autorizzato per il calcolo dei corrispettivi del Partecipante Eleggibile. L'offerta "Business" è venduta in pacchetti di 10. L'offerta "Retail" è venduta in pacchetti di 100 Partecipanti Eleggibili.

1.3.6 IBM Trusteer Rapport Large Redeployment e/o IBM Trusteer Rapport Small Redeployment

I Clienti che reinstallano le proprie Applicazioni di online banking durante il periodo contrattuale del servizio e che, di conseguenza, richiedono modifiche alla relativa installazione di IBM Trusteer Rapport II, devono acquistare il Servizio Cloud IBM Trusteer Rapport Redeployment.

La reinstallazione può essere dovuta alla modifica da parte del Cliente del dominio dell'Applicazione o dell'host URL, all'applicazione delle modifiche alla configurazione dello splash o allo spostamento su una nuova piattaforma di online banking.

Per il periodo di 6 mesi di transizione della reinstallazione, il Cliente ha diritto ad ulteriori Applicazioni ognuna delle quali viene eseguita oltre alle Applicazioni già sottoscritte.

IBM Trusteer Rapport Large Redeployment si applica agli ambienti con più di 20.000 utenti e IBM Trusteer Rapport Small Redeployment si applica agli ambienti con meno o pari a 20.000 utenti.

1.3.7 IBM Trusteer Rapport Additional Applications for Business e/o IBM Trusteer Rapport Additional Applications for Retail

Nel caso dell'offerta IBM Trusteer Rapport II for Business, l'installazione su qualsiasi Applicazione "Business" aggiuntiva oltre alla prima Applicazione, richiede la titolarità per il Servizio Cloud IBM Trusteer Rapport Additional Applications for Business. Nel caso dell'offerta IBM Trusteer Rapport II for Retail, l'installazione su qualsiasi Applicazione "Retail" aggiuntiva oltre alla prima Applicazione, richiede la titolarità per il Servizio Cloud IBM Trusteer Rapport Additional Applications for Retail.

1.4 Servizi Cloud IBM Trusteer Pinpoint

IBM Trusteer Pinpoint è un servizio basato su cloud progettato per fornire un ulteriore livello di protezione e che aiuta a individuare e ridurre gli attacchi di malware, phishing e account takeover (ATO). Trusteer Pinpoint può essere integrato nelle Applicazioni "Business" o "Retail" per le quali il Cliente ha sottoscritto l'abbonamento a copertura dei Servizi Cloud e dei processi di prevenzione delle frodi.

Questo Servizio Cloud include:

a. TMA:

   TMA è disponibile nell'ambiente ospitato dal cloud di IBM Trusteer, attraverso cui il Cliente (e un numero illimitato dei relativi dipendenti autorizzati) può: (i) visualizzare e scaricare la reportistica dei dati su determinati eventi e le valutazioni del rischio, nonché (ii) visualizzare, sottoscrivere, configurare la fornitura di feed sulle minacce generati dalle offerte Pinpoint.

b. Script Web e/o API:

   per l'accesso ad un sito web allo scopo di accedere o utilizzare il Servizio Cloud.

1.4.1 IBM Trusteer Pinpoint Malware Detection

Nel caso in cui i Servizi Cloud IBM Trusteer Pinpoint Malware Detection II rilevino un evento di malware, il Cliente deve attenersi alla Guida Pinpoint Best Practices. Non utilizzare i Servizi Cloud IBM Trusteer Pinpoint Malware Detection II in alcun modo che possa interferire sulle attività del Partecipante Eleggibile immediatamente dopo l'individuazione del malware o dell'account takeover, tale da consentire ad altri di collegare le azioni del Cliente all'utilizzo dei Servizi Cloud IBM Trusteer Pinpoint (ad es., notifiche, messaggi, blocco di dispositivi o blocco dell'accesso all'Applicazione "Business" e/o "Retail" immediatamente dopo l'individuazione di un malware o di un 'account takeover').

1.4.2 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business e/o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail e/o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business e/o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Pinpoint Malware Detection II è una nuova costruzione di IBM Trusteer Pinpoint Malware Detection per aiutare a standardizzare i corrispettivi relativi alla protezione di più Applicazioni e sostituisce i corrispettivi una tantum quando si aggiungono le Applicazioni.

Rilevamento senza client di browser infetti da malware finanziari "Man in the Browser" (MitB) che si collegano ad un Applicazione "Business" e/o "Retail". I Servizi Cloud IBM Trusteer Pinpoint Malware Detection forniscono un ulteriore livello di protezione e hanno l'obiettivo di consentire alle organizzazioni di concentrarsi sullo sviluppo di processi di prevenzione delle frodi basati sul rischio malware, mediante la valutazione e l'avviso della presenza di malware finanziari MitB.

a. Dati sugli eventi:

   Il Cliente (e un numero illimitato dei suoi dipendenti autorizzati del Cliente) può utilizzare TMA per ricevere i dati sugli eventi generati, derivanti dalle interazioni online dei Partecipanti Eleggibili con una o più Applicazioni "Business" e/o "Retail" del Cliente.

b. Advanced Edition:

   Le versioni Advanced Edition per le Applicazioni "Business" e/o "Retail" offrono un ulteriore livello di individuazione e protezione che viene adeguato e personalizzato per la struttura e il flusso di Applicazioni "Business" e/o "Retail" del Cliente, e possono essere personalizzate per gli scenari di minacce destinati al Cliente. Possono essere integrate in diverse sedi del Cliente nelle Applicazioni "Business" e/o "Retail" del Cliente.

   La versione Advanced Edition viene offerta al Cliente in quantità minime di almeno 100 K di Partecipanti Eleggibili "Retail" oppure di 10 K di Partecipanti Eleggibili "Business", con 1000 pacchetti da 100 Partecipanti Eleggibili per le Applicazioni "Retail" o 1000 pacchetti da 10 Partecipanti Eleggibili per le Applicazioni "Business".

c. Standard Edition:

   Le versioni Standard Edition per l'Applicazione "Business" e/o "Retail" sono soluzioni veloce da installare che forniscono la funzionalità di base di questi servizi SaaS, come descritto nel presente documento.

Questo Servizio Cloud include la protezione di un'Applicazione. Per ogni Applicazione aggiuntiva, il Cliente deve ottenere la titolarità per ulteriori Applicazioni di IBM Trusteer Pinpoint Malware Detection.

1.4.3 Ulteriori Servizi Cloud aggiuntivi opzionali per IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail e/o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail e/o IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business e/o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business:

- Il Servizio Cloud IBM Trusteer Rapport Remediation for Retail ha come prerequisiti IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Il Servizio Cloud IBM Trusteer Rapport Remediation for Business ha come prerequisiti IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

1.4.4 IBM Trusteer Rapport Remediation for Retail e/o IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail e IBM Trusteer Rapport Remediation for Business hanno l'obiettivo di ricercare, porre rimedio, bloccare e rimuovere le infezioni malware di tipo man-in-the-browser (MitB) dai dispositivi infetti (PC/MAC) dei Partecipanti Eleggibili che accedono all'Applicazione del Cliente in modo appropriato al contesto, dove le infezioni malware MitB sono state rilevate dai dati sugli eventi di IBM Trusteer Pinpoint Malware Detection. Il Cliente deve disporre della sottoscrizione ad un abbonamento corrente dell'offerta IBM Trusteer Pinpoint Malware Detection II al momento in esecuzione sull'Applicazione del Cliente. Il Cliente può utilizzare l'offerta di questo Servizio Cloud soltanto insieme ai Partecipanti Eleggibili che accedono all'Applicazione del Cliente ed esclusivamente come strumento con l'obiettivo specifico di ricercare e correggere un determinato dispositivo infetto (PC/MAC). IBM Trusteer Rapport Remediation attualmente deve essere eseguito sui suddetti dispositivi coinvolti (PC/MAC) dei

Partecipanti Eleggibili, i quali devono accettare l'accordo EULA, autenticarsi almeno una volta su una o più Applicazioni del Cliente e la configurazione del Cliente deve includere la raccolta di ID Utente. Per fugare qualsiasi dubbio, l'offerta di questo Servizio Cloud non include il diritto di utilizzare Trusteer Splash e/o promuovere il Software Client del Titolare dell'Account in qualsiasi altro modo per la totalità dei Partecipanti Eleggibili del Cliente.

1.4.5 IBM Trusteer Pinpoint Malware Detection Redeployment

I Clienti che reinstallano le proprie Applicazioni di online banking durante il periodo contrattuale del servizio e che, di conseguenza, richiedono modifiche alla relativa installazione di IBM Trusteer Pinpoint Malware Detection II, devono acquistare IBM Trusteer Pinpoint Malware Detection Redeployment.

La reinstallazione può essere dovuta alla modifica da parte del Cliente del dominio dell'Applicazione o dell'host URL, alla conversione dell'Applicazione online in una nuova tecnologia, allo spostamento su una nuova piattaforma di online banking o all'aggiunta di un nuovo flusso di accesso ad una Applicazione esistente.

Per il periodo di 6 mesi di transizione della reinstallazione, il Cliente ha diritto ad ulteriori Applicazioni ognuna delle quali viene eseguita oltre alle Applicazioni già sottoscritte.

Per IBM Trusteer Pinpoint Malware Detection II Standard Edition o IBM Trusteer Pinpoint Malware Detection II Advanced Edition, la distribuzione su qualsiasi Applicazione aggiuntiva oltre la prima Applicazione richiede la titolarità per IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.4.6 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail e/o IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- Nel caso dell'offerta IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail, la distribuzione di qualsiasi Applicazione "Retail" aggiuntiva oltre alla prima Applicazione, richiede la titolarità per IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.
- Nel caso dell'offerta IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business, la distribuzione di qualsiasi Applicazione "Business" aggiuntiva oltre alla prima Applicazione, richiede la titolarità per IBM Trusteer Pinpoint Malware Detection Additional Applications for Business.

1.5 IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Suite") è un insieme di servizi basati su cloud, progettato per fornire un livello di protezione dalle frodi e può essere integrata con ulteriori prodotti IBM per fornire una soluzione di gestione del ciclo di vita. La Suite include i seguenti servizi basati su cloud:

- IBM Trusteer Pinpoint Detect è pensato per individuare e ridurre gli attacchi di malware, phishing e account takeover (ATO). Trusteer Pinpoint Detect può essere integrato nelle Applicazioni "Business" o "Retail" per le quali il Cliente ha sottoscritto l'abbonamento a copertura del Servizio Cloud e dei processi di prevenzione delle frodi.
- IBM Trusteer Rapport for Mitigation ha l'obiettivo di rimediare e proteggere gli endpoint infetti.

I Servizi Cloud includono:

a. TMA:

   TMA è disponibile nell'ambiente ospitato dal cloud IBM Trusteer, attraverso cui il Cliente (e un numero illimitato dei suoi dipendenti autorizzati) può: (i) ricevere la reportistica dei dati sugli eventi e le valutazioni dei rischi, nonché (ii) visualizzare, configurare ed impostare le policy di sicurezza e quelle relative alla reportistica dei dati sugli eventi.

b. Dati sugli eventi:

   Il Cliente (e un numero illimitato dei suoi dipendenti autorizzati del Cliente) può utilizzare l'applicazione TMA per ricevere dati sugli eventi derivanti dalle interazioni online dei Partecipanti Eleggibili con le Applicazioni del Cliente, per le quali il Cliente ha sottoscritto l'abbonamento a copertura del Servizio Cloud oppure il Cliente può ricevere i dati sugli eventi tramite una modalità di fornitura dell'API di backend.

c. Script Web e/o API:

   per l'accesso ad un sito web allo scopo di accedere o utilizzare il Servizio Cloud.

Pinpoint Best Practices

In caso di rilevamento di malware o account takeover, il Cliente deve attenersi alla Guida Pinpoint Best Practices. Non utilizzare i Servizi Cloud IBM Trusteer Pinpoint Detect in alcun modo che possa interferire sulle attività del Partecipante Eleggibile immediatamente dopo l'individuazione del malware o dell'account takeover, tale da consentire ad altri di collegare le azioni del Cliente all'utilizzo delle offerte IBM Trusteer Pinpoint Detect (ad es., notifiche, messaggi, blocco di dispositivi o blocco dell'accesso all'Applicazione "Business" e/o "Retail" immediatamente dopo l'individuazione di un malware o di un 'account takeover').

1.5.1 IBM Trusteer Pinpoint Detect Standard for Retail e/o IBM Trusteer Pinpoint Detect Standard for Business

Questo Servizio Cloud combina i Servizi Cloud IBM Trusteer Pinpoint Criminal Detection e IBM Trusteer Pinpoint Malware Detection per offrire una singola soluzione unificata.

La soluzione aiuta ad individuare senza client un malware e/o un'attività sospetta di account takeover da parte di browser che si collegano all'Applicazione, mediante ID dispositivo, individuazione di phishing e di furti di credenziali tramite malware. Le offerte IBMTrusteer Pinpoint forniscono un altro livello di protezione e hanno l'obiettivo di rilevare i tentativi di account takeover, nonché fornire direttamente al Cliente il punteggio della valutazione del rischio dei browser o dei dispositivi mobili (tramite il browser nativo o l'applicazione per dispositivi mobili del Cliente) che accedono ad un'Applicazione.

Il Supporto Standard (così come definito nel seguente articolo Supporto Tecnico) è incluso nel presente Servizio Cloud. Per il supporto Premium, il Cliente deve acquistare il servizio Pinpoint Standard Premium Support.

Questo Servizio Cloud include la protezione di un'Applicazione. Per ciascuna Applicazione aggiuntiva, il Cliente dovrà ottenere la titolarità IBM Trusteer Pinpoint Detect Standard Additional Applications.

Il servizio è disponibile per l'acquisto in pacchetti da 100 Partecipanti Eleggibili o 100 Connessioni. Qualora il Cliente decida di acquistare il servizio in base alle Connessioni, è applicabile il corrispettivo per Ulteriori Applicazioni a partire dalla prima applicazione.

1.5.2 IBM Trusteer Pinpoint Detect Premium for Retail e/o IBM Trusteer Pinpoint Detect Premium for Business

Questo Servizio Cloud combina i Servizi IBM Trusteer Pinpoint Criminal Detection e IBM Trusteer Pinpoint Malware Detection per offrire una singola soluzione unificata semplice da integrare.

La soluzione aiuta ad individuare senza client un malware e/o un'attività sospetta di account takeover da parte di browser che si collegano all'Applicazione, mediante ID dispositivo, individuazione di phishing e di furti di credenziali tramite malware. Le offerte IBMTrusteer Pinpoint forniscono un altro livello di protezione e hanno l'obiettivo di rilevare i tentativi di account takeover, nonché fornire direttamente al Cliente il punteggio della valutazione del rischio dei browser o dei dispositivi mobili (tramite il browser nativo o l'applicazione per dispositivi mobili del Cliente) che accedono ad un'Applicazione "Business" o "Retail".

Il servizio include funzionalità e servizi migliorati, inclusi: servizi di setup e distribuzione estesa, policy di sicurezza personalizzate, servizi di indagine e così via. Il servizio include fino a 200 ore di risorse condivise per i servizi di distribuzione per applicazione e 200 di risorse condivise per l'analisi della sicurezza per applicazione dopo il setup. I servizi continuativi includono 20 ore di manutenzione della distribuzione all'anno per applicazione e 100 ore di ricerca della sicurezza per applicazione all'anno. Qualsiasi attività aggiuntiva è soggetta a corrispettivi aggiuntivi.

Pinpoint Detect può utilizzare le transazioni dai canali Mobile e Web. Nel caso in cui siano incluse transazioni Mobile, è applicabile il servizio Pinpoint per Connessione. Questo Servizio Cloud include la protezione di un'Applicazione. Per ciascuna Applicazione aggiuntiva, il Cliente dovrà ottenere la titolarità per IBM Trusteer Pinpoint Detect Premium Additional Applications.

Il supporto Premium è incluso in questo Servizio Cloud.

I servizi IBM Trusteer Pinpoint Detect Premium for Retail e Business sono disponibili per l'acquisto in pacchetti da 100 Partecipanti Eleggibili o IBM Trusteer Pinpoint Detect Premium in pacchetti da 100 Connessioni. Qualora il Cliente decida di acquistare il servizio in base alle Connessioni, è applicabile il corrispettivo per Ulteriori Applicazioni a partire dalla prima applicazione.

Pinpoint Detect Policy Manager:

La funzione Policy Manager è inclusa nel servizio Pinpoint Detect Premium ed è disponibile nell'ambiente ospitato dal cloud IBM Trusteer, attraverso il quale il Cliente (ed un numero illimitato di dipendenti autorizzati) può: (i) progettare, eseguire test ed effettuare implementazioni nella logica dell'ambiente di produzione per rilevare attività fraudolente, (ii) progettare report e dashboard, e (iii) visualizzare, configurare ed impostare le policy di sicurezza e le policy che consentono di rilevare attività sospette sull'Applicazione del Cliente.

Per l'attivazione della funzione Policy Manager e per il supporto richiesto da approfondimenti supplementari, sono richiesti servizi di Consulenza. I dettagli dei servizi di Consulenza saranno descritti separatamente in un Allegato.

Una volta attivata la funzione Policy Manager, IBM si riserva il diritto di accedere all'ambiente del Cliente a scopo di supporto per regolare le policy del Cliente al fine di risolvere gli errori principali derivati dalle modifiche alla policy.

Il Cliente si impegna a proteggere i dati esposti tramite la funzione Policy Manager da un utilizzo improprio.

Una volta attivata la funzione Policy Manager, il Cliente deve seguire le linee guida per l'impostazione delle regole, come indicato nella documentazione. Il Cliente riconosce che IBM non è responsabile per qualsiasi situazione che potrebbe derivare dalla mancata osservazione delle seguenti raccomandazioni da parte del Cliente.

Qualsiasi problema di stabilità e/o riduzione del servizio che potrebbe verificarsi a causa dell'errata configurazione della funzione Policy Manager da parte del Cliente non verrà considerato come Tempo di Fermo per il calcolo dello SLA.

1.5.3 Servizi opzionali per IBM Trusteer Pinpoint Detect Standard e/o IBM Trusteer Pinpoint Detect Premium

Per i Servizi Cloud specificati in questo articolo, è richiesta la titolarità per IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard come prerequisito.

1.5.4 IBM Trusteer Rapport for Mitigation for Retail e/o IBM Trusteer Rapport for Mitigation for Business

- IBM Trusteer Rapport for Mitigation for Retail ha l'obiettivo di ricercare, porre rimedio, bloccare e rimuovere le infezioni malware da dispositivi infetti (PC/MAC) dei Partecipanti Eleggibili del Cliente che accedono all'Applicazione "Retail" del Cliente in modo appropriato al contesto, dove le infezioni malware sono state rilevate dai dati di eventi IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard. Il Cliente deve disporre di un abbonamento attivo alle offerte IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard al momento in esecuzione sull'Applicazione "Retail" del Cliente. Il Cliente può utilizzare questo Servizio Cloud soltanto insieme ai Partecipanti Eleggibili che accedono all'Applicazione "Retail" del Cliente ed esclusivamente come strumento con l'obiettivo specifico di ricercare e correggere un determinato dispositivo infetto (PC/MAC). IBM Trusteer Rapport for Mitigation for Retail deve infatti essere eseguito sui suddetti dispositivi (PC/MAC) dei Partecipanti Eleggibili, i quali devono accettare l'accordo EULA, autenticarsi almeno una volta su una o più Applicazioni "Retail" del Cliente, e la configurazione del Cliente deve includere la raccolta degli ID utente. Per fugare qualsiasi dubbio, questo Servizio Cloud non include il diritto di utilizzare Trusteer Splash e/o promuovere il Software Client del Titolare dell'Account in qualsiasi altro modo per la totalità dei Partecipanti Eleggibili del Cliente.
- IBM Trusteer Rapport for Mitigation for Business ha l'obiettivo di ricercare, porre rimedio, bloccare e rimuovere le infezioni malware da dispositivi infetti (PC/MAC) dei Partecipanti Eleggibili del Cliente che accedono all'Applicazione "Business" del Cliente in modo appropriato al contesto, dove le infezioni malware sono state rilevate dai dati di eventi IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard. Il Cliente deve disporre di un abbonamento attivo alle offerte IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard al momento in esecuzione sull'Applicazione "Business" del Cliente. Il Cliente può utilizzare questo Servizio Cloud soltanto insieme ai Partecipanti Eleggibili che accedono all'Applicazione "Business" del Cliente ed esclusivamente come strumento con l'obiettivo specifico di ricercare e correggere un determinato dispositivo infetto (PC/MAC). IBM Trusteer Rapport for Mitigation for Business deve infatti essere eseguito sui suddetti dispositivi (PC/MAC) dei Partecipanti Eleggibili, i quali devono accettare l'accordo EULA, autenticarsi almeno una volta su una o più Applicazioni "Business" del Cliente, e la

configurazione del Cliente deve includere la raccolta degli ID utente. Per fugare qualsiasi dubbio, questo Servizio Cloud non include il diritto di utilizzare Trusteer Splash e/o promuovere il Software Client del Titolare dell'Account in qualsiasi altro modo per la totalità dei Partecipanti Eleggibili del Cliente.

1.5.5 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail e/o IBM Trusteer Pinpoint Detect Standard Additional Applications for Business e/o IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail e/o IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

Il servizio include fino a 200 ore di risorse condivise per i servizi di distribuzione per applicazione e 200 di risorse condivise per l'analisi della sicurezza per applicazione dopo il setup. I servizi continuativi includono 20 ore di manutenzione della distribuzione all'anno per applicazione e 100 ore di ricerca della sicurezza per applicazione all'anno.

- Un'installazione di IBM Trusteer Pinpoint Detect Standard for Retail di qualsiasi ulteriore Applicazione "Retail" aggiuntiva oltre alla prima Applicazione, richiede la titolarità a IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.
- Un'installazione di IBM Trusteer Pinpoint Detect Standard for Business di qualsiasi ulteriore Applicazione "Business" aggiuntiva oltre alla prima Applicazione, richiede la titolarità a IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.
- Un'installazione di IBM Trusteer Pinpoint Premium for Retail di qualsiasi ulteriore Applicazione "Retail" aggiuntiva oltre alla prima Applicazione, richiede la titolarità a IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.
- Un'installazione di IBM Trusteer Pinpoint Premium for Business di qualsiasi ulteriore Applicazione "Business" aggiuntiva oltre alla prima Applicazione, richiede la titolarità a IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

1.5.6 IBM Trusteer Pinpoint Detect Standard Application e/o IBM Trusteer Pinpoint Detect Premium Application

Questo servizio è applicabile per i canali Web e Mobile.

Il servizio include fino a 200 ore di risorse condivise per i servizi di distribuzione per applicazione e 200 di risorse condivise per l'analisi della sicurezza per applicazione dopo il setup. I servizi continuativi includono 20 ore di manutenzione della distribuzione all'anno per applicazione e 100 ore di ricerca della sicurezza per applicazione all'anno.

- L'installazione IBM Trusteer Pinpoint Detect Standard richiede la titolarità a IBM Trusteer Pinpoint Detect Standard Application per tutte le Applicazioni.
- L'installazione IBM Trusteer Pinpoint Premium richiede la titolarità a IBM Trusteer Pinpoint Detect Premium Application per tutte le Applicazioni.

1.5.7 IBM Trusteer Pinpoint Detect Standard Redeployment e/o IBM Trusteer Pinpoint Detect Premium Redeployment

I Clienti che reinstallano le proprie Applicazioni di online banking durante il periodo contrattuale del servizio e che, di conseguenza, richiedono modifiche alla relativa installazione di IBM Trusteer Pinpoint Detect, devono acquistare IBM Trusteer Pinpoint Detect Detection Redeployment.

La reinstallazione può essere dovuta alla modifica da parte del Cliente del dominio dell'Applicazione o dell'host URL, alla conversione dell'Applicazione online in una nuova tecnologia, allo spostamento su una nuova piattaforma di online banking o all'aggiunta di un nuovo flusso di accesso ad una Applicazione esistente.

Per il periodo di 6 mesi di transizione della reinstallazione, il Cliente ha diritto ad ulteriori Applicazioni ognuna delle quali viene eseguita oltre alle Applicazioni già sottoscritte.

1.5.8 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support e/o IBM Trusteer Pinpoint Detect Standard for Business Premium Support

I Clienti che acquistano il Servizio Cloud Pinpoint Detect Standard possono acquistare il servizio Premium Support. L'ambito dei servizi Premium Support è elencato nel successivo articolo 4.

1.5.9 IBM Trusteer Digital Content Pack for Retail e/o IBM Trusteer Digital Content Pack for Business

IBM Trusteer Digital Content Pack consente agli analisti della sicurezza di integrare modelli di nuove frodi supportando nel contempo la creazione e la modifica di modelli ad-hoc per reagire alle minacce in evoluzione. È costituito da un ampio insieme di regole, approfondimenti e policy che possono essere acquistati come parti aggiuntive e integrali della soluzione. Il pacchetto Digital Content aiuta a rafforzare ulteriormente l'integrazione tra le funzionalità di prevenzione dalle frodi digitali di Trusteer e i canali di pagamento senza contanti di IBM Safer Payments. Utilizzando le regole incorporate e la logica aziendale specifica, Digital Content Pack consente alle banche e altri istituti finanziari di migliorare ulteriormente le funzionalità esistenti per l'individuazione e la prevenzione dalle frodi.

IBM Trusteer Digital Content Pack for Retail è disponibile in pacchetti di 100 Partecipanti Eleggibili. IBM Trusteer Digital Content Pack for Business è disponibile in pacchetti di 10 Partecipanti Eleggibili.

I servizi di consulenza sono richiesti per l'integrazione di Digital Content Pack con Pinpoint Detect e IBM Safer Payments, nonché per i servizi di supporto che richiedono un'attenzione significativa. I servizi di consulenza vengono acquistati separatamente in base ad un accordo separato.

1.5.10 IBM Trusteer New Account Fraud for Retail e/o IBM Trusteer New Account Fraud for Business

Questo servizio, disponibile per i sottoscrittori di Pinpoint è progettato per il rilevamento di anomalie, attività di contrassegno sospetto e per generare avvisi nelle prime fasi del processo di creazione. Il servizio controlla i nuovi account per identificare le nuove attività associate con la creazione di profili post-account e young account fraudolenti in modo da fornire da avvisare tempestivamente, attraverso dei report di utilizzo disponibili nel TMA, che è possibile che il nuovo account sia di tipo mule o comunque utilizzato a scopo fraudolento.

IBM Trusteer New Account Fraud for Retail e IBM Trusteer New Account Fraud for Business sono disponibili in pacchetti da 10 chiamate API.

1.5.11 IBM Trusteer Pinpoint Verify

Il Cliente deve disporre di un abbonamento attivo a IBM Trusteer Pinpoint Detect Premium prima di abbonarsi al presente Servizio Cloud.

Questo Servizio Cloud fornisce funzionalità per richiedere agli utenti un secondo fattore di autenticazione al fine di verificare le loro identità quando accedono a un servizio digitale. È disponibile con Pinpoint Detect Premium al fine di fornire un secondo fattore di autenticazione per applicazioni protette. La decisione su quando richiedere agli utenti l'autenticazione del secondo fattore è derivata dall'applicazione protetta e può essere basata sui suggerimenti restituiti dalla piattaforma Pinpoint Detect Premium o da qualsiasi altra policy definita dall'applicazione protetta.

1.6 IBM Trusteer Pinpoint Assure

Questo servizio contrassegna le attività sospette e genera degli avvisi durante il processo di creazione/generazione di un nuovo account. Il servizio controlla il processo di registrazione dell'account per identificare le attività fraudolente, in modo da avvisare tempestivamente che il nuovo account potrebbe essere di tipo mule o utilizzato a scopo fraudolento, tramite report di utilizzo disponibili in TMA.

Il servizio IBM Trusteer Pinpoint Assure è disponibile in pacchetti di 100 Connessioni.

1.6.1 Servizi opzionali per IBM Trusteer Pinpoint Assure

1.6.2 IBM Trusteer Pinpoint Assure Application

Per la distribuzione di IBM Trusteer Pinpoint Assure su qualsiasi Applicazione è richiesta la titolarità per IBM Trusteer Pinpoint Assure Application.

Il servizio IBM Trusteer Pinpoint Assure è disponibile per l'acquisto in base all'applicazione.

1.6.3 IBM Trusteer Mobile Carrier Intelligence e/o IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Il Cliente deve disporre di un abbonamento attivo a IBM Trusteer Pinpoint Assure o IBM Trusteer Pinpoint Detect prima di abbonarsi al presente Servizio Cloud.

Il presente Servizio Cloud migliora IBM Trusteer Pinpoint Assure e/o IBM Trusteer Pinpoint Detect fornendo ulteriori informazioni e contesto sui numeri di cellulare forniti ai Servizi Cloud, consentendo di determinare il rischio di frode di una determinata sessione. Il Cliente potrà interrogare il Servizio Cloud

per determinare le caratteristiche di un numero di cellulare specifico, quali ad esempio le informazioni sul gestore telefonico associate a tale numero.

I dati forniti da questo Servizio Cloud relativi ai numeri di cellulare ("Mobile Intelligence") possono essere utilizzati solo per scopi interni del Cliente e possono essere conservati per un periodo di 30 (trenta) giorni. Dopo tale periodo di tempo il Cliente dovrà interrogare nuovamente il Servizio Cloud per lo stesso numero di cellulare per ottenere la "Mobile Intelligence" ad esso relativa e non potrà semplicemente riutilizzare la "Mobile Intelligence" ricevuta da una query precedente. Salvo per quanto sopra consentito il Cliente non potrà memorizzare nella cache, riutilizzare, utilizzare in modo congiunto completo o parziale con qualsiasi data mining, o archiviare alcuna Mobile Intelligence.

1.7 IBM Trusteer Remotely Delivered Services

L'offerta IBM Trusteer Remotely Delivered Services è disponibile come componente aggiuntivo opzionale per i Servizi Cloud Pinpoint Detect Premium e Pinpoint Assure.

1.7.1 IBM Trusteer Project Management and Consultancy Services

Questo Servizio fornisce fino a 200 (duecento) ore di servizi di consulenza durante le quali IBM eseguirà alcune o tutte le seguenti attività:

a. Servizi di setup iniziale: riunioni periodiche frequenti, servizi di Project Management

b. Policy Manager: supporto continuativo

L'offerta è disponibile per l'acquisto in base all'Impegno.

1.7.2 IBM Trusteer Security Research Consultancy Services

Questo servizio di consulenza include fino a 200 ore di risorse condivise per l'analisi della sicurezza per fornire ulteriori servizi in aggiunta alla soluzione definita ed al supporto premium (quando applicabile), ed include:

a. Ricerca estesa delle frodi: riunioni settimanali e formazione.

b. Supporto per la release del Cliente ad alta priorità

c. Analisi e supporto continuativi delle regole personalizzate

L'offerta è disponibile per l'acquisto in base all'Impegno.

1.7.3 IBM Trusteer Training Services

Questo servizio di consulenza è progettato per fornire ulteriori servizi in aggiunta alla soluzione definita ed al supporto premium (quando applicabile), ed include i servizi di formazione sul portfolio Trusteer per i dipendenti del Cliente.

L'offerta è disponibile per l'acquisto in base all'Impegno.

1.8 Servizi Cloud IBM Trusteer Mobile

1.8.1 IBM Trusteer Mobile SDK for Business e/o IBM Trusteer Mobile SDK for Retail

I Servizi Cloud IBM Trusteer Mobile SDK sono progettati per fornire un ulteriore livello di protezione che assicuri un accesso web protetto alle Applicazioni "Business" e/o "Retail" del Cliente, per le quali il Cliente ha sottoscritto l'abbonamento a copertura dei Servizi Cloud, la valutazione del rischio dei dispositivi e la protezione dal pharming. L'individuazione di reti Wi-Fi sicure è disponibile solo sulle piattaforme Android.

I Servizi Cloud IBM Trusteer Mobile SDK includono un software developer kit ("SDK") proprietario per dispositivi mobili, un pacchetto software che contiene la documentazione, le librerie del software di programmazione di proprietà ed altri file ed elementi correlati, noti come libreria mobile IBM Trusteer e come "Componente Run-time" o "Ridistribuibile", un codice proprietario generato da IBM Trusteer Mobile SDK che può essere incorporato e integrato nelle applicazioni autonome e protette per dispositivi mobili iOS o Android per le quali il Cliente ha sottoscritto l'abbonamento a copertura del Servizio Cloud. ("App Integrata per Dispositivi Mobili del Cliente").

IBM Trusteer Mobile SDK for Retail è disponibile in pacchetti da 100 Partecipanti Eleggibili o pacchetti da 100 Dispositivi Client e IBM Trusteer Mobile SDK for Business è disponibile in pacchetti da 10 Partecipanti Eleggibili o pacchetti da 10 Dispositivi Client.

Mediante l'applicazione TMA, il Cliente (e un numero illimitato dei suoi dipendenti autorizzati del Cliente) può ricevere la reportistica dei dati sugli eventi e le valutazioni delle tendenze del rischio. Attraverso le

Applicazioni Mobili Integrate del Cliente è possibile ricevere l'analisi del rischio e le informazioni relative ai dispositivi mobili riguardanti i dispositivi mobili dei Partecipanti Eleggibili che hanno scaricato le Applicazioni Mobili Integrate del Cliente consentendogli di formulare una policy preventiva delle frodi, per rafforzare le azioni di mitigazione rispetto a questi rischi. Per gli scopi di questa offerta, i "dispositivi mobili" includono solo i telefoni cellulari e i tablet supportati e non includono i PC portatili o i MAC.

Il Cliente può:

a. utilizzare internamente IBM Trusteer Mobile SDK esclusivamente allo scopo di sviluppare le Applicazioni Mobili Integrate del Cliente;

b. integrare il componente Ridistribuibile (esclusivamente in formato di codice oggetto), in modo integrale, non separabile nelle Applicazioni Mobili Integrate del Cliente. Qualsiasi parte modificata o integrata del software Ridistribuibile, ai sensi della presente concessione di licenza, sarà soggetta alle condizioni della presente Descrizione dei Servizi; e

c. commercializzare e distribuire il componente Ridistribuibile per il download sui dispositivi mobili dei Partecipanti Eleggibili o sul proprietario del Dispositivo Client, a condizione che:

    - Fatto salvo quanto espressamente consentito dal presente Accordo, il Cliente (1) non può utilizzare, copiare, modificare, o distribuire l'SDK; (2) non può disassemblare, decompilare, effettuare il reverse engineering o in altro modo convertire o decodificare l'SDK, salvo quanto previsto da norme inderogabili di legge; (3) non può fornire in sublicenza, in locazione o noleggiare l'SDK; (4) non può rimuovere eventuali file di copyright o di avvisi contenuti nel componente Ridistribuibile; (5) non può utilizzare lo stesso nome di percorso dei file/moduli originali del componente Ridistribuibile; e (6) non può utilizzare i nomi o i marchi dei licenziatari o dei distributori di IBM in connessione con il marketing dell'App Integrata del Dispositivo Mobile del Cliente senza previo consenso scritto di IBM o dei licenziatari o distributori di IBM.
    - Il componente Ridistribuibile deve rimanere integrato in modo non separabile all'interno dell'App Integrata del Dispositivo Mobile del Cliente. Il componente Ridistribuibile deve essere esclusivamente in formato codice oggetto e deve essere conforme a tutte le direttive, istruzioni e specifiche dell'offerta IBM Trusteer Mobile SDK e della relativa documentazione. L'accordo di licenza per l'utente finale per le Applicazioni Mobili Integrate del Cliente deve informare l'utente finale che il componente Ridistribuibile non potrà essere i) utilizzato per scopi diversi dall'attivazione dell'Applicazione Mobile Integrata del Cliente, ii) copiato (tranne per scopi di backup), iii) ulteriormente distribuito o trasferito, salvo quanto previsto da norme inderogabili di legge. L'accordo di licenza del Cliente deve avere la medesima tutela contrattuale, nei confronti di IBM, delle condizioni del presente Accordo
    - L'SDK può essere implementato solo come parte dell'implementazione interna del Cliente e del test dell'unità sui dispositivi mobili del Cliente specificati per il test. Il Cliente non può utilizzare l'SDK per elaborare e simulare i carichi di lavoro di produzione o eseguire il test della scalabilità di qualsiasi codice, applicazione o sistema. Il Cliente non è autorizzato ad utilizzare nessuna parte dell'SDK per nessun altro scopo.

Il Cliente è l'unico responsabile per lo sviluppo, il test e il supporto dell'App per Dispositivi Mobili Integrati del Cliente. Il Cliente è responsabile di tutta l'assistenza tecnica per l'Applicazione Mobile Integrata del Cliente e di qualsiasi modifica del componente Ridistribuibile apportata dal Cliente, così come consentito nel presente documento.

Il Cliente è autorizzato ad installare ed utilizzare il software Ridistribuibile e IBM Security Mobile SDK solo per fornire supporto sull'utilizzo da parte del Cliente dei Servizi Cloud.

IBM non garantisce che qualsiasi applicazione o output creato utilizzando strumenti mobili inclusi con IBM Security Mobile SDK funzionerà, interagirà o sarà compatibile con qualsiasi specifica piattaforma di sistema operativo mobile o dispositivo mobile.

Componenti di Origine e Materiali di Esempio – IBM Trusteer Mobile SDK potrebbe includere alcuni componenti in formato codice sorgente ("Componenti di Origine") e dell'altro materiale identificati come Materiale di Esempio. Il Cliente può copiare e modificare i Componenti di Origine e i Materiali di Esempio solo per uso interno purché rientri nei limiti dei diritti di licenza in base al presente Accordo e purché il Cliente non modifichi o elimini eventuali informazioni o comunicazioni relative al copyright contenute nei Componenti di Origine o nei Materiali di esempio. IBM fornisce i Componenti di Origine e i Materiali di Esempio senza alcun obbligo di assistenza e "NELLO STATO IN CUI SI TROVANO". Si noti che i

Componenti di Origine o i Materiali di Esempio sono forniti esclusivamente come esempio su come implementare gli elementi incorporabili (Embeddable) nella CIMA, i Componenti di Origine o i Materiali di Esempio non possono essere compatibili con l'ambiente di sviluppo del Cliente e il Cliente è l'unico responsabile del test e dell'implementazione degli elementi incorporabili (Embeddable) nella relativa CIMA.

2. Contenuto e Protezione dei Dati Personali

Nelle specifiche tecniche per la Protezione e il Trattamento dei Dati (Specifiche Tecniche o Data Sheet) sono descritte le informazioni specifiche per il Servizio Cloud riguardanti il tipo di Contenuto abilitato al trattamento, le attività di trattamento interessate, le funzionalità per la protezione dei dati e le specifiche sulla conservazione e restituzione del Contenuto. Tutti i dettagli o i chiarimenti e le condizioni, inclusa la responsabilità del Cliente riguardanti l'utilizzo di un Servizio Cloud e le funzionalità di protezione dei dati, se presenti, sono specificati nel presente articolo. Potrebbe essere applicabile più di una Specifica Tecnica per l'utilizzo del Servizio Cloud da parte del Cliente, in base alle opzioni selezionate dal Cliente. Le Specifiche Tecniche potrebbero essere disponibili solo in inglese e non nella lingua locale. Fatte salve eventuali normative e gli usi locali, le parti convengono di comprendere l'inglese e che si tratta di una lingua appropriata per quanto riguarda l'acquisto e l'utilizzo dei Servizi Cloud. Le seguenti Specifiche Tecniche si applicano al Servizio Cloud e alle sue opzioni disponibili. Il Cliente è a conoscenza che i) IBM può modificare una o più Specifiche Tecniche periodicamente, ad esclusiva discrezione di IBM e ii) tali modifiche prevarranno sulle versioni precedenti. Le modifiche apportate ad una o più Specifiche Tecniche avranno il fine di i) migliorare o chiarire gli impegni esistenti, ii) mantenere l'allineamento con gli standard attualmente adottati e le norme applicabili, oppure iii) fornire ulteriori impegni. Nessuna modifica delle Specifiche Tecniche determinerà un peggioramento sostanziale della protezione dei dati del Servizio Cloud.

Uno o più link a una o più Specifiche Tecniche applicabili:

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

(Le specifiche tecniche di IBM Cloud Identity Verify riflettono quelle di IBM Trusteer Pinpoint Verify)

Il Cliente è responsabile di applicare le misure necessarie per ordinare, abilitare o utilizzare le funzioni di protezione dei dati disponibili per un Servizio Cloud e accetta la responsabilità dell'utilizzo dei Servizi Cloud qualora non adotti tali misure, compreso il rispetto dei requisiti di legge per la protezione dei dati o altri requisiti normativi riguardanti il Contenuto.

Il Supplemento per il Trattamento dei Dati Personali (Data Processing Addendum o DPA) di IBM, disponibile alla pagina web http://ibm.com/dpa e le Appendici DPA si applicano e completano l'Accordo qualora, e nella misura in cui, il Regolamento Europeo in materia di Protezione dei Dati Personali (European General Data Protection Regulation), (EU/2016/679) (GDPR) si applica ai dati personali presenti nel Contenuto. Le Specifiche Tecniche applicabili a questo Servizio Cloud costituiscono le Appendici DPA. Se si applica il DPA, l'obbligo da parte di IBM di comunicare qualsiasi modifica riguardante i Subresponsabili e il diritto del Cliente di opporsi a tali modifiche viene applicato come stabilito nel DPA.

2.1 EULA e Basi giuridiche per il trattamento dei dati dei Data Subjects

Per i Servizi Cloud IBM Trusteer Rapport (incluso Rapport for Remediation o Rapport for Mitigation quando implementati insieme ai Servizi Cloud Pinpoint):

Se non diversamente concordato, ed in ottemperanza alla base giuridica per il trattamento che il Cliente ha definito in modo indipendente, il Cliente autorizza IBM a fornire l'EULA (End User License Agreement) riportato alla pagina https://www.trusteer.com/support/end-user-license-agreement per consentire ad IBM di raccogliere e trattare le informazioni necessarie per la fornitura dei Servizi Cloud.

2.2 Uso dei Dati

IBM non utilizzerà o divulgherà i risultati derivanti dall'utilizzo da parte del Cliente del Servizio Cloud che sono specifici del Contenuto del Cliente (Approfondimenti) o che altrimenti identifichino il Cliente. IBM può utilizzare il Contenuto e altre informazioni (tranne gli Approfondimenti) derivanti dal Contenuto durante la fornitura del Servizio Cloud dopo aver rimosso gli identificativi personali, in modo tale che qualsiasi dato personale non possa essere più attribuito ad una specifica persona senza l'utilizzo di ulteriori informazioni. IBM utilizzerà questi dati solo per scopi di ricerca, test e sviluppo dell'offerta IBM.

2.3 Trattamento ed archiviazione dei dati

2.3.1 Ulteriori Informazioni sulla Sede del Trattamento

Per i servizi Trusteer Pinpoint Verify, nelle specifiche tecniche pertinenti vengono specificate tutte le sedi di hosting ed elaborazione.

Per tutti i servizi forniti tramite i data center ubicati in Germania, IBM limiterà il trattamento dei Dati Personali al paese dell'entità appaltante di IBM ed ai seguenti paesi: Germania, Israele, Irlanda, Paesi Bassi e qualsiasi altro paese elencato nelle Specifiche Tecniche applicabili per i Subresponsabili di terze parti di IBM.

Per tutti i servizi forniti tramite i data center ubicati in Giappone, IBM limiterà il trattamento dei Dati Personali al paese dell'entità appaltante di IBM ed ai seguenti paesi: Giappone, Israele, Irlanda e qualsiasi altro paese elencato nelle Specifiche Tecniche applicabili per i Subresponsabili di terze parti di IBM.

Per tutti i servizi forniti tramite i data center ubicati negli Stati Uniti, IBM limiterà il trattamento dei Dati Personali al paese dell'entità appaltante di IBM ed ai seguenti paesi: Stati Uniti, Israele, Singapore, Australia e qualsiasi altro paese elencato nelle Specifiche Tecniche applicabili per i Subresponsabili di terze parti di IBM.

I servizi di manutenzione dell'account e di supporto IBM Trusteer possono anche essere forniti secondo le necessità, in base alla disponibilità del personale IBM rilevante, alla posizione del Cliente ed al data center che ospita i dati.

2.3.2 Dati del Titolare dell'Account

I dati del Titolare dell'Account saranno elaborati nella regione da cui il Titolare dell'Account ha installato inizialmente il Software Client del Titolare dell'Account. Ciò può significare che il contenuto del Titolare d'Account può essere elaborato sia nella regione di origine che nella regione concordata con il Cliente.

2.3.3 Soluzioni integrate

Per chiarezza, poiché Trusteer Fraud Protection è una soluzione integrata, se il Cliente recede da uno di questi Servizi Cloud, IBM potrà conservare i dati del Cliente allo scopo di fornire al Cliente i rimanenti Servizi Cloud in base alla presente Descrizione dei Servizi.

3. Service Level Agreement ("SLA")

IBM fornisce il seguente Service Level Agreement ("SLA") sulla disponibilità per il Servizio Cloud, come specificato nella PoE. Lo SLA non costituisce una garanzia. Lo SLA è disponibile solo per il Cliente e si applica per essere utilizzato esclusivamente negli ambienti di produzione.

3.1 Crediti di Disponibilità

Il Cliente deve registrare un ticket di assistenza di Severità 1 mediante l'help desk del supporto tecnico IBM, entro le 24 ore successive dal momento in cui il Cliente determina che un evento ha avuto un impatto negativo sulla disponibilità del Servizio Cloud. Il Cliente deve fornire a IBM ragionevole assistenza nella diagnosi e risoluzione di qualsiasi problema.

La richiesta di risarcimento per il ticket di assistenza per il mancato adempimento dello SLA dovrà essere inoltrato entro tre giorni lavorativi dal termine del Mese Contrattuale. Il rimborso per una pretesa valida relativa allo SLA verrà accreditato in una fattura successiva per il Servizio Cloud in base al periodo di tempo durante il quale l'elaborazione del sistema di produzione per il Servizio Cloud non è disponibile ("Tempo di Fermo"). Il Tempo di Fermo (Downtime) è misurato dal momento in cui il Cliente segnala l'evento fino a quando il Servizio Cloud viene ripristinato e non include il tempo relativo ad un'interruzione pianificata o annunciata per manutenzione; cause al di fuori del controllo di IBM; problemi con il contenuto le tecnologie, i progetti o le istruzioni del Cliente o di terzi; errori nelle configurazioni di sistema e di piattaforme non supportate o altri errori del Cliente; oppure incidenti di sicurezza causati dal Cliente o da test di sicurezza del Cliente. IBM applicherà il rimborso più elevato calcolato sulla disponibilità cumulativa del Servizio Cloud durante ciascun mese contrattuale, come mostrato nella tabella seguente. Il risarcimento totale rispetto ad un mese contrattuale non può superare il 10 percento di un dodicesimo (1/12) del corrispettivo annuale per il Servizio Cloud.

3.2 Livelli di Servizio

Disponibilità del Servizio Cloud in un mese contrattuale

Disponibilità in un mese contrattuale	**Rimborso (% del Costo* dell'abbonamento mensile per il mese contrattuale oggetto di una richiesta di risarcimento)**
< 99,9%	2%
<99,0%	5%
< 95,0%	10%

* Se il Cliente ha acquisito il Servizio Cloud da un Business Partner IBM, il costo dell'abbonamento mensile sarà calcolato in base al listino prezzi al momento in vigore per il Servizio Cloud attivo nel mese contrattuale che è oggetto della richiesta di risarcimento, scontato del 50%. IBM applicherà lo sconto direttamente al Cliente.

I Livelli di Servizi ed i Crediti di Compensazione associati sono calcolati separatamente per ciascun Servizio e per ciascuna Applicazione del Cliente.

Quando si calcolano i crediti SLA per i Servizi Cloud in base alle titolarità dell'Applicazione, la Disponibilità sarà calcolata in base alle seguenti linee guida:

- a ciascuna Applicazione sarà assegnata una quota pesata in base al numero calcolato del volume di sessioni durante il mese contrattuale.
- Il tempo di fermo di ciascun Servizio Cloud per Applicazione sarà accumulato separatamente per il mese contrattuale.

Segue un esempio di calcolo per un mese di attività e dei relativi pesi associati. Questo esempio è solo a scopo illustrativo:

Applicazioni 'Retail'	Suddivisione del numero totale di sessioni in un determinato mese contrattuale	Tempo di fermo totale in un mese contrattuale	Minuti pesati di tempo di fermo
Applicazioni 'Retail' A	40%	300 minuti	40% x. 300 minuti = 120 minuti
Applicazioni 'Retail' B	20%	250 minuti	20% x 250 minuti = 50 minuti
Applicazioni 'Retail' C	40%	150 minuti	40% x 150 minuti = 60
			Totale minuti pesati del Tempo di fermo = 230

La disponibilità, espressa come percentuale, viene calcolata nel seguente modo: il numero totale di minuti nel mese contrattuale, meno il numero totale di minuti pesati del Tempo di Fermo nel mese contrattuale, diviso per il numero totale di minuti nel mese contrattuale. Il calcolo di esempio in base ai precedenti esempi di calcolo del peso è il seguente:

$$\frac{\text{43.200 minuti totali in un mese contrattuale di 30 (trenta) giorni} - \text{230 minuti pesati di Tempo di Fermo} = \text{42.970 minuti}}{\text{43.200 minuti totali}} = \text{2\% Credito di Disponibilità per il 99,4\% di disponibilità in un mese contrattuale}$$

4. Supporto tecnico

Il Supporto tecnico per i Servizi Cloud è disponibile per il Cliente ed i relativi Partecipanti Eleggibili per assistenza durante l'utilizzo dei Servizi Cloud.

Il Supporto Standard è incluso nell'abbonamento di tutte le offerte. Trusteer Rapport Mandatory Service, che è un componente aggiuntivo di Trusteer Rapport, ha il prerequisito del Supporto Premium per l'abbonamento base di Trusteer Rapport.

Per ciascun Servizio Cloud è disponibile, ad un costo aggiuntivo, un abbonamento per il Supporto Premium, ad eccezione dei Servizi Cloud **IBM Trusteer Mobile SDK** e **IBM Trusteer Rapport Mandatory Service**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital Content Pack** e **IBM Trusteer Mobile Carrier Intelligence**. Contattare il proprio Rappresentante commerciale IBM o il Business Partner IBM.

Supporto Standard:

- Supporto ora locale 08:00 - 17:00.
- I Clienti e i relativi Partecipanti Eleggibili possono inoltrare i ticket elettronicamente, come descritto dettagliatamente nel software IBM come guida di supporto del servizio disponibile alla pagina https://www.ibm.com/software/support/saas_support_guide.html.
- I Clienti possono accedere al Portale del Supporto Clienti per comunicazioni, documenti, report delle casistiche e FAQ alla seguente pagina Web: http://www-01.ibm.com/software/security/trusteer

Supporto Premium:

- Supporto 24 ore al giorno per 7 giorni alla settimana per tutti i tipi di severità.
- I Clienti possono direttamente accedere al supporto, telefonicamente e richiesta di richiamata.
- I Clienti e i relativi Partecipanti Eleggibili possono inoltrare i ticket elettronicamente, come descritto dettagliatamente nella Guida al Supporto di Software as a Service [SaaS].
- I Clienti possono accedere al Portale del Supporto Clienti per comunicazioni, documenti, report delle casistiche e per le FAQ alla seguente pagina Web: http://www.ibm.com/software/security/trusteer/support/.
- Per le opzioni di supporto e per l'accesso ai dettagli del software IBM come guida di supporto del servizio accedere alla pagina https://www.ibm.com/software/support/saas_support_guide.html.

5. Informazioni sulle Titolarità e sulla Fatturazione

5.1 Calcolo dei Corrispettivi

Il Servizio Cloud è disponibile in base al calcolo dei corrispettivi specificato nel Documento d'Ordine:

- Prestazione: è un'unità di misura che definisce le titolarità per ottenere i servizi. Una Prestazione consiste in servizi professionali e/o di formazione relativi al Servizio Cloud. È necessario ottenere titolarità sufficienti a coprire ciascuna Prestazione.
- Partecipante Eleggibile è un'unità di misura che consente di ottenere il Servizio Cloud. Si definisce Partecipante Eleggibile, qualsiasi persona fisica o giuridica idonea a partecipare a qualsiasi programma di erogazione del servizio, gestito o tracciato mediante il Servizio Cloud. È necessario ottenere titolarità sufficienti a coprire tutti i Partecipanti Eleggibili gestiti o tracciati all'interno del Servizio Cloud durante il periodo di misurazione specificato nel Documento d'Ordine del Cliente.

  Ciascun programma per l'erogazione del servizio gestito dal Servizio Cloud, è analizzato separatamente e successivamente annesso nuovamente. Le persone giuridiche o fisiche eleggibili per i programmi di fornitura dei servizi devono ottenere titolarità separate.

  Per gli scopi di titolarità di questi Servizi Cloud, un Partecipante Eleggibile è un utente finale del Cliente che dispone di credenziali di accesso univoche per l'Applicazione "Business" o "Retail" del Cliente.
- "Dispositivo Client" è un'unità di misura che consente di ottenere il Servizio Cloud. Un Dispositivo Client è un dispositivo informatico per singolo utente, un sensore per scopi speciali oppure un dispositivo di telemetria che richiede o accetta per il funzionamento una serie di comandi, procedure o applicazioni o che fornisca dati ad un altro sistema di computer generalmente definito come server oppure gestito dal server. Più Dispositivi Client possono condividere l'accesso ad un server comune. Un Dispositivo Client può avere alcune capacità di elaborazione o essere programmabile per consentire ad un utente di lavorare. Il Cliente deve ottenere titolarità per ciascun Dispositivo Client che esegue, fornisce dati, utilizza i servizi forniti da, o che accede al Servizio Cloud in qualche altro modo, durante il periodo di misurazione specificato nel Documento d'Ordine del Cliente.
- "Applicazione" è un'unità di misura che consente di ottenere il Servizio Cloud. Un'Applicazione è un programma software denominato in modo univoco. È necessario ottenere titolarità sufficienti per ogni Applicazione resa disponibile per accedervi e utilizzarla durante il periodo di misurazione specificato nella PoE del Cliente o nel Documento d'Ordine.

  Per gli scopi di questo Servizio Cloud, un'Applicazione è una singola Applicazione Business o del Cliente.
- "Chiamata API" è un'unità di misura che consente di ottenere il Servizio Cloud. Una chiamata API è rappresentata da una richiesta al Servizio Cloud attraverso un'interfaccia programmabile. È necessario ottenere titolarità sufficienti a coprire il numero totale di Chiamate API, arrotondato alla Decina successiva, durante il periodo di misurazione specificato nella PoE (PoE of Entitlement) del Cliente o nel Documento d'Ordine.
- "Connessione" è un'unità di misura che consente di ottenere il Servizio Cloud. Una Connessione è un collegamento o l'associazione di un database, un'applicazione, un server o di qualsiasi altro tipo di dispositivo per il Servizio Cloud. È necessario ottenere titolarità sufficienti a coprire il numero totale di Connessioni che sono state o vengono realizzate per il Servizio Cloud durante il periodo di misurazione specificato nella PoE del Cliente o nel Documento d'Ordine.

  Per gli scopi di questo Servizio Cloud, una Connessione è una sessione o un flusso nell'Applicazione del Cliente.

5.2 Corrispettivi di sovrapprezzo

Se l'utilizzo effettivo del Servizio Cloud da parte del Cliente durante il periodo di misurazione supera la titolarità per cui è autorizzato nella PoE, sarà addebitato un corrispettivo di sovrapprezzo, secondo quanto stabilito nel Documento d'Ordine nel mese seguente tale eccedenza.

5.3 Frequenza della fatturazione

In base alla frequenza di fatturazione selezionata, IBM fatturerà al Cliente i corrispettivi esigibili all'inizio del periodo della frequenza di fatturazione, ad eccezione dei corrispettivi di sovrapprezzo e di utilizzo che saranno addebitati con fattura posticipata.

6. Opzioni di Durata e Rinnovo

La durata del Servizio Cloud inizia nella data in cui IBM comunica al Cliente che l'accesso al Servizio Cloud è disponibile, così come documentato nella PoE. Nella PoE sarà specificato se il Servizio Cloud sarà rinnovato automaticamente, se procede sulla base di un uso continuativo o se termina alla scadenza.

In caso di rinnovo automatico, salvo comunicazione scritta da parte del Cliente di recesso con preavviso di almeno 90 (novanta) giorni prima della data di scadenza del periodo contrattuale, il Servizio Cloud sarà rinnovato automaticamente per la durata contrattuale specificata nella PoE. I rinnovi sono soggetti ad un aumento sul prezzo annuale come specificato nella quotazione economica. Nel caso in cui il rinnovo automatico si verifichi in seguito ad un avviso da parte di IBM di ritiro del Servizio Cloud, il periodo di rinnovo terminerà prima della fine del periodo di rinnovo corrente o della data di ritiro annunciata.

In caso di utilizzo continuativo, il Servizio Cloud continuerà ad essere disponibile con cadenza mensile fino a quando il Cliente non fornirà una comunicazione scritta di recesso con preavviso di almeno 90 giorni prima della scadenza Il Servizio Cloud continuerà ad essere disponibile fino alla fine del mese solare successivo a tale periodo di 90 (novanta) giorni.

7. Ulteriori condizioni

7.1 Disposizioni Generali

Il Cliente accetta che IBM possa fare pubblicamente riferimento al Cliente come abbonato dei Servizi Cloud in una pubblicità o comunicati commerciale.

Il Cliente non può utilizzare i Servizi Cloud, in modo indipendente o in combinazione con altri servizi o prodotti a supporto delle seguenti attività ad alto rischio: progettazione, costruzione, controllo o manutenzione di attrezzature nucleari, sistemi di trasporto pubblico, sistemi di guida automatica, apparecchiature belliche, navigazione o comunicazioni aeree o altre attività in cui un errore del Servizio Cloud potrebbe comportare materialmente una minaccia di morte o gravi lesioni personali.

7.2 Prerequisiti Software (Software di Abilitazione)

Il Servizio Cloud richiede l'uso del prerequisito software che il Cliente scaricherà nei propri sistemi per facilitare l'uso del Servizio Cloud. Il Cliente potrà utilizzare il prerequisito software solo in relazione all'utilizzo del Servizio Cloud. Il prerequisito software è fornito "NELLO STATO IN CUI SI TROVA".

7.3 Deployment of IBM Trusteer Fraud Protection

Per ciascuna Applicazione sottoscritta dal Cliente, l'abbonamento base del Cliente include le attività di setup e di installazione iniziali richieste sul cloud di IBM Trusteer, quali l'avvio iniziale in un'unica soluzione, la configurazione, i Modelli Splash, i test e la formazione.

Le attività di installazione non includono le attività di implementazione richieste sulle Applicazioni o sistemi del Cliente.

La fase di implementazione dei diversi Servizi Cloud è stata progettata per essere implementata nei tempi previsti, come descritto nelle relative guide di installazione.

Il completamento di queste fasi di implementazione, entro il periodo di tempo assegnato, dipende dal 'commitment' e dalla partecipazione totale della direzione e del personale del Cliente. Il Cliente dovrà fornire le informazioni richieste in modo tempestivo. Le prestazioni di IBM si basano su informazioni e decisioni tempestive da parte del Cliente ed eventuali ritardi possono causare costi aggiuntivi e/o ritardi nel completamento di questi servizi di implementazione.

Per ciascuna Applicazione sottoscritta dal Cliente, l'abbonamento base del Cliente include le attività di setup e di installazione iniziali richieste sul cloud IBM Trusteer, quali l'avvio iniziale in un'unica soluzione, la configurazione, i Modelli Splash, i test e la formazione.

L'abbonamento di base del Cliente include il supporto e il test per le pagine all'interno dell'applicazione del Cliente che saranno contrassegnate come consigliato da IBM nella installazione iniziale. IBM non

sarà responsabile di: (i) implementazioni parziali, (ii) scelta del Cliente di non implementare il Servizio Cloud IBM come consigliato da IBM, o (iii) decisione del Cliente di condurre l'implementazione, il setup e il test per conto proprio. (IV) L'installazione e la protezione parziale derivano da informazioni inappropriate fornite dal Cliente. Ulteriori servizi, incluse le attività di installazione oltre l'implementazione iniziale, possono essere effettuate ad un costo aggiuntivo in base ad un accordo separato.

Accettato da:

_____

Firma e timbro del Cliente

Data:

Ai sensi e per gli effetti degli articoli 1341 e 1342 del Codice Civile Italiano, il Cliente approva specificamente i seguenti articoli del presente documento: “Service Level Agreement (SLA)”, “Crediti di Disponibilità”, “Opzioni di Durata e Rinnovo”, “Disposizioni Generali”, “Prerequisiti Software (Software di Abilitazione)”.

_____

Firma e timbro del Cliente

Data: