IBM Trusteer Fraud Protection

Nella presente Descrizione dei Servizi è descritto il Servizio Cloud che IBM fornisce al Cliente. Il termine "Cliente" include i contraenti, i relativi utenti autorizzati e i destinatari del Servizio Cloud. Il Preventivo e la PoE (Proof of Entitlement) applicabili sono forniti come Documenti d'Ordine separati.

1. Servizio Cloud

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

Servizi Cloud "Rapport":

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

Servizi Cloud "Pinpoint":

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

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

Servizi Cloud "Mobile":

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

- IBM Trusteer Mobile Browser for Retail Premium Support

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

1.1.2 Retail Cloud Services

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

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 Servizi Cloud aggiuntivi per IBM Trusteer Rapport

a. Ulteriori Servizi Cloud disponibili per IBM Trusteer Rapport for Business:
   - IBM Trusteer Rapport Fraud Feeds for Business
   - IBM Trusteer Rapport Phishing Protection for Business

- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Additional Applications For Business

b. Ulteriori Servizi Cloud disponibili per IBM Trusteer Rapport for Retail:

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

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 for Business o IBM Trusteer Rapport 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 e/o IBM Trusteer Pinpoint Malware Detection II

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

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

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

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

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

1.1.5 Ulteriori Servizi Cloud per IBM Trusteer Pinpoint Criminal Detection e/o IBM Trusteer Pinpoint Criminal Detection II

a. Ulteriori Servizi Cloud disponibili per IBM Trusteer Pinpoint Criminal Detection for Business o IBM Trusteer Pinpoint Criminal Detection II:

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. Ulteriori Servizi Cloud disponibili per IBM Trusteer Pinpoint Criminal Detection for Retail e/o IBM Trusteer Pinpoint Criminal Detection II for Retail:

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Il Supporto Premium è disponibile per offerte specifiche, come specificato nel presente documento.

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

1.1.6 Ulteriori Servizi Cloud disponibili per IBM Trusteer Pinpoint Detect Standard e/o IBM Trusteer Pinpoint Detect Premium e/o IBM Pinpoint Detect Standard with access management integration e/o IBM Detect Premium with access management integration

a. Ulteriori Servizi Cloud disponibili per IBM Trusteer Detect Standard for Business e/o IBM Trusteer Pinpoint Detect Premium for Business e/o IBM Pinpoint Detect Standard with access management integration for Business e/o IBM Detect Premium with access management integration for Business:

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

b. Ulteriori Servizi Cloud disponibili per IBM Trusteer Detect Standard for Retail e/o IBM Trusteer Pinpoint Detect Premium for Retail e/o IBM Pinpoint Detect Standard with access management integration for Retail e/o IBM Detect Premium with access management integration for Retail:

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

L'abbonamento a IBM Trusteer Detect Standard o IBM Trusteer Pinpoint Detect Premium o IBM Pinpoint Detect Standard with access management integration o IBM Detect Premium with access management integration è un prerequisito per gli ulteriori Servizi Cloud associati, elencati in questo articolo.

1.1.7 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 software di abilitazione 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 o IBM Trusteer Mobile Browser 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.

2. Servizi Cloud IBM Trusteer Rapport

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

Trusteer Rapport 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.

Per questo Servizio Cloud si applica il calcolo dei corrispettivi relativo al Partecipante Eleggibile. L'offerta "Business" è venduta in pacchetti di 10 Partecipanti Eleggibili. L'offerta "Retail" è venduta in pacchetti di 100 Partecipanti Eleggibili.

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 di 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 software di abilitazione 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'implementazione obbligatoria del Software Client del Titolare del Conto 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 del Conto 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.

2.2 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. L'offerta "Business" è venduta in pacchetti di 10 Partecipanti Eleggibili. L'offerta "Retail" è venduta in pacchetti di 100 Partecipanti Eleggibili.

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 di 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 software di abilitazione 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.

2.3 Ulteriori Servizi Cloud opzionali per IBM Trusteer Rapport for Business e/o IBM Trusteer Rapport for Retail e/o IBMTrusteer Rapport II for Business e/o IBM Trusteer Rapport II for Retail

L'abbonamento ai Servizi Cloud IBM Trusteer Rapport o Servizi Cloud IBM Trusteer Rapport II è un prerequisito per l'abbonamento a uno qualsiasi dei seguenti Servizi Cloud aggiuntivi. 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 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.

2.3.1 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.

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

Il Cliente (e un numero illimitato di 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.

2.3.3 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.

2.3.4 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 o 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.

2.3.5 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.

3. 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.

3.1 IBM Trusteer Pinpoint Malware Detection e IBM Trusteer Pinpoint Criminal Detection

In caso di individuazione di malware nei Servizi Cloud IBM Trusteer Pinpoint Malware Detection o nei Servizi Cloud IBMTrusteer Pinpoint Criminal Detection II o in caso di individuazione di 'account takeover' nei Servizi Cloud IBM Trusteer Pinpoint Criminal Detection o nei Servizi Cloud IBM Trusteer Pinpoint Criminal Detection II, il Cliente deve attenersi alla Guida Pinpoint Best Practices. Non utilizzare in alcun modo i Servizi Cloud IBM Trusteer Pinpoint Malware Detection o i Servizi Cloud IBM Trusteer Pinpoint Malware Detection II o i Servizi Cloud IBM Trusteer Pinpoint Criminal Detection o i Servizi Cloud IBM Trusteer Pinpoint Criminal Detection II in alcun modo che possa compromettere l'esperienza del Partecipante Eleggibile subito 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 esempio, notifiche, messaggi, blocco di dispositivi o blocco dell'accesso all'Applicazione "Business" e/o "Retail" subito dopo l'individuazione di un malware o di un 'account takeover').

3.2 IBM Trusteer Pinpoint Criminal Detection for Business e/o IBM Trusteer Pinpoint Criminal Detection for Retail

Rilevamento senza client di un'attività sospetta di account takeover da parte di browser che si collegano all'Applicazione "Business" o "Retail", mediante ID dei dispositivi, individuazione del phishing e individuazione del furto di credenziali tramite malware. I Servizi Cloud IBM Trusteer Pinpoint Criminal Detection Cloud forniscono un ulteriore 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".

a. Dati sugli eventi:

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

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business e/o IBM Trusteer Pinpoint Criminal Detection II for Retail

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

Rilevamento senza client di un'attività sospetta di account takeover da parte di browser che si collegano all'Applicazione "Business" o "Retail", mediante ID dei dispositivi, individuazione del phishing e individuazione del furto di credenziali tramite malware. I Servizi Cloud IBM Trusteer Pinpoint Criminal Detection II forniscono un ulteriore 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".

a. Dati sugli eventi:

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

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

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

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 di 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", ossia 1000 pacchetti da 100 Partecipanti Eleggibili per le Applicazioni "Retail" o 1000 pacchetti da 10 Partecipanti Eleggibili per le Applicazioni "Business".

c. Standard Edition:

   La versione Standard Edition per l'Applicazione "Business" o "Retail" è una soluzione veloce da installare che fornisce la funzionalità di base di questi servizi SaaS, come descritto nel presente documento.

3.5 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 di 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", ossia 1000 pacchetti da 100 Partecipanti Eleggibili per le Applicazioni "Retail" o 1000 pacchetti da 10 Partecipanti Eleggibili per le Applicazioni "Business".

c. Standard Edition:

La versione Standard Edition per l'Applicazione "Business" o "Retail" è una soluzione veloce da installare che fornisce 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.

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

- Nel caso del Servizio Cloud IBM Trusteer Rapport Remediation for Retail, è richiesto il prerequisito di IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail o IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Nel caso del Servizio Cloud IBM Trusteer Rapport Remediation for Business, è richiesto il prerequisito di IBM Trusteer Pinpoint Malware Detection Standard Edition for Business o IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.
- Nel caso dell'offerta IBM Trusteer Pinpoint Carbon Copy for Retail, è richiesto il prerequisito di IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail o IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Nel caso dell'offerta IBM Trusteer Pinpoint Carbon Copy for Business, è richiesto il prerequisito di IBM Trusteer Pinpoint Malware Detection Standard Edition for Business o IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business e/o IBM Trusteer Pinpoint Carbon Copy for Retail

Le offerte IBM Trusteer Pinpoint Carbon Copy sono progettate per fornire un ulteriore livello di protezione e un servizio di monitoraggio che possono aiutare il Cliente ad individuare quando le credenziali del Partecipante Eleggibile sono state compromesse da attacchi di Phishing sulle Applicazioni "Retail" o "Business" per le quali il Cliente ha sottoscritto l'abbonamento a copertura del Servizio Cloud.

3.6.2 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 di un abbonamento attivo a IBM Trusteer Pinpoint Malware Detection o IBM Trusteer Pinpoint Malware Detection II effettivamente 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.

3.6.3 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 e/o 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.

3.6.4 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 Business o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business, l'installazione su qualsiasi Applicazione "Business" aggiuntiva oltre alla prima Applicazione, richiede la titolarità per 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, l'installazione su qualsiasi Applicazione "Retail" aggiuntiva oltre alla prima Applicazione, richiede la titolarità per IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.

3.7 Ulteriori Servizi Cloud opzionali per IBM Trusteer Pinpoint Criminal Detection for Business e/o IBM Trusteer Pinpoint Criminal Detection for Retail e/o for IBM Trusteer Pinpoint Criminal Detection II for Business e/o IBM Trusteer Pinpoint Criminal Detection II for Retail

3.7.1 IBM Trusteer Pinpoint Criminal 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 Criminal Detection, devono acquistare IBM Trusteer Pinpoint Criminal 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.

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business e/o IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

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

4. 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 di 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 di dipendenti autorizzati del Cliente) può utilizzare l'applicazione TMA per ricevere dati sugli eventi derivanti dalle interazioni online dei Partecipanti Eleggibili con le Applicazioni "Business" e/o "Retail" 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 individuazione 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').

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

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 "Business" o "Retail", 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 Supporto Standard (così come definito nel seguente articolo Supporto Tecnico) è incluso nel presente Servizio Cloud. Per il Supporto Premium, il Cliente deve acquistare Detect Premium.

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.

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

Questo Servizio Cloud combina IBM Trusteer Pinpoint Criminal Detection e IBM Trusteer Pinpoint Malware Detection per offrire una singola soluzione unificata, facile da integrare, con funzionalità e servizi migliorati, inclusi i seguenti: installazione estesa e servizi di setup, policy della sicurezza personalizzate, servizi di indagine, ecc..

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.

4.3 IBM Trusteer Pinpoint Detect Standard with access management integration for Business e/o IBM Trusteer Pinpoint Detect Standard with access management integration for Retail

Il Servizio Cloud IBM Trusteer Pinpoint Detect Standard with access management integration include la funzionalità di IBM Security Pinpoint Detect Standard, come descritto dettagliatamente nel precedente articolo 4.1.

IBM Trusteer Pinpoint Detect Standard with access management integration è usato quando viene acquistato con i sistemi di gestione degli accessi come, ad esempio, IBM Security Access Management ("ISAM"). Quando viene acquistato con ISAM, entrambe le offerte devono essere abilitate. Questa offerta include l'opzione di integrazione con il sistema di gestione degli accessi. Non include la titolarità per il sistema di gestione degli accessi.

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

Il Supporto Standard (così come definito nell'articolo Supporto Tecnico) è incluso nel presente Servizio Cloud. IBM Trusteer Pinpoint Detect Premium with access management integration for Business e/o IBM Trusteer Pinpoint Detect Premium with access management integration for Retail

Il Servizio Cloud IBM Trusteer Pinpoint Detect Premium with access management integration include la funzionalità di IBMPinpoint Detect Premium, come descritto dettagliatamente nel precedente articolo 4.2, e l'opzione di integrazione con il sistema di gestione degli accessi.

IBM Trusteer Pinpoint Detect Premium with access management integration è usato quando viene acquistato con i sistemi di gestione degli accessi come, ad esempio, IBM Security Access Management ("ISAM"). Quando viene acquistato con ISAM, entrambe le offerte devono essere abilitate. Questo Servizio Cloud include l'opzione di integrazione con il sistema di gestione degli accessi. Non include la titolarità per il sistema di gestione degli accessi.

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 nella presente offerta.

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

Per i Servizi Cloud specificati in questo articolo, è necessario avere un prerequisito di titolarità per IBM Trusteer Pinpoint Detect Premium for Retail o IBM Trusteer Pinpoint Detect Standard for Retail.

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

IBM Trusteer Rapport for Mitigation 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.

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

Nel caso dell'offerta IBM Trusteer Pinpoint Standard for Business, l'installazione su qualsiasi Applicazione "Business" aggiuntiva oltre alla prima Applicazione, richiede la titolarità per IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

Nel caso dell'offerta IBM Trusteer Pinpoint Standard for Retail, l'installazione su qualsiasi Applicazione "Retail" aggiuntiva oltre alla prima Applicazione, richiede la titolarità per IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.

Nel caso dell'offerta IBM Trusteer Pinpoint Premium for Business, l'installazione su qualsiasi Applicazione "Business" aggiuntiva oltre alla prima Applicazione, richiede la titolarità per IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

Nel caso dell'offerta IBM Trusteer Pinpoint Premium for Retail, l'installazione su qualsiasi Applicazione "Retail" aggiuntiva oltre alla prima Applicazione, richiede la titolarità per IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.

4.5.2 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.

5. Servizi Cloud IBM Trusteer Mobile

5.1 IBM Trusteer Mobile Browser for Business e/o IBM Trusteer Mobile Browser for Retail

IBM Trusteer Mobile Browser è progettato per aggiungere un ulteriore livello di protezione e ha l'obiettivo di garantire un accesso online protetto dai dispositivi mobili dei 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, la valutazione del rischio dei dispositivi e la protezione dal phishing. L'individuazione di reti Wi-Fi sicure è disponibile solo sulle piattaforme Android. Per gli scopi di questo Servizio Cloud i dispositivi mobili includono i telefoni cellulari o i tablet e non includono i Laptop PC ed i Mac.

Attraverso l'applicazione TMA, il Cliente può ricevere dati sugli eventi, analisi e informazioni statistiche sui Dispositivi i cui Partecipanti Eleggibili hanno: (i) scaricato il Software Client del Titolare dell'Account, un'applicazione gratuita con licenza pubblica disciplinata da un accordo di licenza per l'utente finale ("EULA"), e disponibile per il download sui dispositivi mobili dei Partecipanti Eleggibili, e (ii) hanno accettato l'EULA e si sono autenticati sulle Applicazioni "Business" o "Retail" per le quali il Cliente ha sottoscritto l'abbonamento a copertura del Servizio Cloud. Il Cliente potrà commercializzare il Software Client del Titolare dell'Account solo mediante Trusteer Splash e non potrà utilizzare il Software Client del Titolare dell'Account per attività aziendali interne.

a. Dati sugli eventi:

   Il Cliente (e un numero illimitato di dipendenti autorizzati del Cliente) può utilizzare l'applicazione TMA per ricevere dati sugli eventi derivanti dalle interazioni online dei dispositivi mobili con le Applicazioni "Business" o "Retail" del Cliente, per le quali il Cliente ha sottoscritto l'abbonamento a copertura dei Servizi Cloud.

b. 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 ("Modello 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 o 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.

5.2 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 di 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 di 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 ha eseguito il test sulle applicazioni campione create con gli strumenti per dispositivi mobili forniti nell'IBM Trusteer Mobile SDK (''Strumenti per Dispositivi Mobili''), per determinarne il corretto funzionamento su alcune versioni di piattaforme di sistemi operativi per dispositivi mobili, quali Apple (iOS), Google (Android) e altri (nell'insieme indicati come ''Piattaforme OS per dispositivi mobili''), tuttavia, le Piattaforme OS per dispositivi mobili sono fornite da terze parti e non sono sotto il controllo di IBM e sono soggette a modifiche senza alcun preavviso ad IBM. Pertanto, fatto salvo quanto diversamente stabilito, IBM non garantisce che qualsiasi applicazione o altro output creato tramite gli Strumenti per Dispostivi Mobili funzioneranno correttamente, interagiranno o saranno compatibili con le Piattaforme OS per Dispositivi Mobili o con i dispositivi mobili stessi.

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'', NON FORNISCE ALCUN TIPO GARANZIA, ESPRESSA O IMPLICITA, INCLUSE LE GARANZIE DI TITOLARITÀ, DI NON VIOLAZIONE DI DIRITTI DI PROPRIETÀ INTELLETTUALE O DI NON INTERFERENZA, NONCHÉ QUALSIASI ALTRA GARANZIA O CONDIZIONE ESPRESSA O IMPLICITA DI COMMERCIABILITÀ ED IDONEITÀ PER UNO SCOPO SPECIFICO, FATTO SALVO QUANTO STABILITO DA NORME INDEROGABILI DI LEGGE. 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 (Embededdable) nella relativa CIMA.

Il Cliente accetta di creare, conservare e fornire a IBM e ai suoi revisori un'accurata documentazione scritta, l'output degli strumenti di sistema e altre informazioni di sistema sufficienti a fornire una evidenza che dimostri che l'utilizzo dell'IBM Trusteer Mobile SDK da parte del Cliente è conforme alle condizioni della presente Descrizione dei Servizi.

6. Supporto Premium

Il Cliente ha diritto al Supporto Premium solo per i Servizi Cloud per cui il Cliente ha sottoscritto l'abbonamento relativo all'offerta associata al Supporto Premium.

7. 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.

8. Riservatezza e Sicurezza dei dati

Questo Servizio Cloud si attiene ai principi IBM sulla sicurezza e riservatezza dei dati per i servizi IBM SaaS che sono disponibili alla pagina web http://www.ibm.com/cloud/data-security e ad eventuali condizioni aggiuntive fornite in questo articolo. Eventuali modifiche dei principi IBM sulla sicurezza e riservatezza dei dati non altereranno la sicurezza del Servizio Cloud.

Questo Servizio Cloud può essere usato per trattare contenuto in cui siano presenti dati personali qualora il Cliente, in qualità di titolare del trattamento dei dati, determini che le misure di sicurezza tecniche ed organizzative siano appropriate ai rischi presentati dal trattamento e alla natura dei dati da proteggere. Il Cliente riconosce che questo Servizio Cloud non offre funzionalità per la protezione di dati personali sensibili o dati soggetti ad ulteriori requisiti normativi.

Questo Servizio Cloud è incluso nella certificazione Privacy Shield quando il Cliente sceglie di ospitare il Servizio Cloud in un data center che si trova negli Stati Uniti ed è soggetto alla Policy di IBM su Privacy Shield, disponibile alla pagina web http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

8.1 Funzionalità per la Sicurezza e Responsabilità

Il Servizio Cloud implementa le seguenti funzionalità di sicurezza:

Il Servizio Cloud esegue la crittografia del contenuto durante la trasmissione dei dati verso e dalla rete IBM e quando sono in attesa della trasmissione dati dall'endpoint.

8.2 Utilizzo consentito dalla legge e consenso

Utilizzo consentito dalla legge

L'utilizzo del Servizio Cloud può implicare varie leggi o normative. Il Servizio Cloud può essere utilizzato solo per scopi legali e nei termini consentiti dalla legge. Il Cliente accetta di utilizzare il Servizio Cloud in ottemperanza alle leggi, normative e policy applicabili e se ne assume ogni responsabilità ed obbligazione.

Autorizzazione alla Raccolta ed al Trattamento dei Dati

Il Servizio Cloud raccoglierà le informazioni dei Partecipanti Eleggibili e dai Dispositivi del Cliente che interagiscono con le Applicazioni "Business" o "Retail" per le quali il Cliente ha sottoscritto l'abbonamento per la copertura del Servizio Cloud. Il Servizio Cloud raccoglie informazioni che, singolarmente o insieme, possono essere considerate da alcuni ordinamenti Dati Personali. Per "Dati personali" si intende qualsiasi informazione che può essere utilizzata per identificare una persona fisica, come il nome, l'indirizzo email, l'indirizzo di casa o il numero di telefono forniti ad IBM per essere memorizzati, elaborati o trasferiti per conto del Cliente.

La raccolta e le procedure di trattamento dei dati possono essere aggiornate per migliorare la funzionalità del Servizio Cloud. Un documento con una descrizione completa della raccolta e delle procedure di trattamento dei dati viene aggiornato in base alle esigenze ed è disponibile per il Cliente su richiesta. Il Cliente autorizza IBM a raccogliere tali informazioni e a trattarle in conformità con quanto specificato nell'articolo Trasferimenti oltre confine e nell'articolo Data Privacy della presente Descrizione dei Servizi.

Per le offerte IBM Trusteer che includono Trusteer Management Application (TMA):

I seguenti dati sono raccolti e archiviati in Trusteer Management Application (TMA) per gli amministratori TMA dall'indirizzo email del gruppo aziendale sponsor: indirizzo email (come login), password in formato hash, nome fornito, cognome, titolo professionale e reparto.

Per i Servizi Cloud IBM Trusteer Pinpoint:

i dati raccolti possono includere:

- identificativi utente o endpoint come, ad esempio, l'ID Utente criptato o in formato hash irreversibile (one-way hashed), Persistent User ID, PUID, Rapport Agent Key e l'ID Sessione del Cliente;
- dati relativi all'applicazione protetta come, ad esempio, attributi/elementi specifici provenienti dall'applicazione di online banking del Cliente come emessi dal browser, dalle visite del sito web e dalla cronologia della navigazione dell'utente finale;
- informazioni sull'ambiente software installato, attributi e impostazioni del browser e del dispositivo e lunghezza della cronologia del browser;
- informazioni e registrazione data/ora dell'hardware;
- intestazioni del browser e dati del protocollo di comunicazione come, ad esempio, l'indirizzo IP dell'utente, i cookie, l'intestazione del server di provenienza (referrer) e altre intestazioni HTTP;
- i dati del movimento del mouse dell'utente finale come, ad esempio, le coordinate del puntatore del mouse, i clic e il movimento della rotellina di scorrimento (e loro equivalenti) e la registrazione data/ora durante l'interazione con l'applicazione bancaria online del Cliente;
- siti di phishing e informazioni inviate nei siti di phishing; e
- i dati transazionali, ad esclusiva discrezione del Cliente, (importo, valuta e codici di destinazione della transazione, le credenziali inserite nei siti di phishing, identificativo della banca di destinazione della transazione in formato hash irreversibile, identificativo dell'account di destinazione della transazione in formato hash, valore binario se la transazione riguarda un nuovo beneficiario e la data e l'ora della transazione) e valutazione opzionale del rischio dei dati.
- ad esclusiva scelta del Cliente, digitare i ritmi sulla tastiera e le sequenze familiari di battitura dei tasti utilizzate dall'utente finale per inserire un nome utente, una password e altro testo (ma non le lettere, i numeri o i caratteri speciali stessi e senza la capacità di distinguere il nome utente o la password);

Il Cliente conviene e accetta che IBM non raccoglierà, memorizzerà, gestirà o manterrà i libri ufficiali e/o la documentazione del Cliente.

Quando il Cliente si abbona all'offerta IBM Trusteer Rapport for Remediation, oppure in alcuni scenari di supporto Pinpoint, IBM potrebbe consigliare di installare il Software Client del Titolare dell'Account di Rapport su una macchina del Partecipante Eleggibile, al fine di ricercare e indagare su infezioni malware sospette. I dati raccolti per le offerte Rapport sono definiti di seguito.

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

I dati raccolti possono includere:

- gli indirizzi URL e IP (Internet protocol) dei siti web che il Titolare dell'Account visita, che IBM ritiene essere potenzialmente fraudolenti, di phishing o di sfruttamento, insieme alle informazioni sulla natura delle minacce identificate;
- gli indirizzi URL e IP dei siti web che il Titolare dell'Account visita che sono controllati dal Cliente e protetti dal Servizio Cloud, come i siti di online banking; gli indirizzi IP del Titolare dell'Account;
- informazioni di identificazione dell'hardware, sistemi operativi, software applicativo, hardware periferico, configurazione della sicurezza, impostazioni di sistema e connessioni di rete dell'endpoint, nonché l'ID, il nome, i modelli di utilizzo e altre informazioni di identificazione dell'endpoint;
- informazioni riguardanti l'installazione e il funzionamento del programma, l'ID del programma, la versione del programma, gli eventi di sicurezza generati dall'endpoint e le informazioni sugli errori del programma;

- statistiche di utilizzo e informazioni statistiche sulle minacce rilevate dal programma; file di log che contengono i 'crash' del browser, la data e l'ora delle infezioni e informazioni sulla natura delle minacce o malfunzionamenti identificati;
- affiliazione Cliente, cui si fa riferimento anche come Gruppo Aziendale Sponsor. Un'affiliazione si stabilisce quando un utente finale scarica Rapport dal sito web del Cliente, seleziona un determinato Cliente quando scarica Rapport dal sito di supporto di Trusteer o accede ad un'applicazione bancaria del Cliente. Un utente finale può avere più di un'affiliazione Cliente;
- una copia dell'ID Utente criptato che il Titolare dell'Account usa per interagire con il Cliente (opzionale);
- una copia criptati del numero di carta di credito che il Titolare dell'Account in un sito dopo che il programma informa il Titolare dell'Account che il programma ritiene che il sito sia rischioso;
- file e altre informazioni dall'endpoint che gli esperti di sicurezza IBM ritengono possano essere correlati a malware o altre attività dannose o che possano essere associate a malfunzionamenti generali del programma; e
- informazioni di contatto personali inclusi il nome e l'email, quando l'utente finale contatta il Supporto.

Per le offerte IBM Trusteer Mobile SDK ed i Servizi Cloud IBM Trusteer Mobile Browser:

i dati raccolti possono includere:

- identificativi dell'utente come, ad esempio, l'ID Utente criptato o in formato hash irreversibile;
- informazioni sul dispositivo come, ad esempio, l'indirizzo IP, l'ID del dispositivo in formato hash, la registrazione data/ora, i valori MD5 del pacchetto installato e altre informazioni sui dispositivi hardware e software;
- versione dell'SDK o del Browser per dispositivi mobili e data di installazione;
- visite alle applicazioni protette;
- associazione del Cliente; e
- dati dei dispositivi a rischio (ad esempio, presenza di malware, 'root hiders', stato della crittografia del Wi-Fi, se un dispositivo sia stato sottoposto o meno a 'jailbreak');
- 'crash stack trace' (in caso di interruzione inaspettata dell'applicazione);
- dati di fabbricazione del telefono (ad es., modello, produttore);
- interazioni 'touchscreen' degli utenti finali incluse le coordinate x, y, le aree 'touch' ed il tipo di azione (spostamenti verso l'alto o verso il basso);
- dati del sensore di movimento, utilizzo alimentazione/risorse, impostazioni della connettività, sensori ambientali come, ad esempio, la temperatura, l'illuminazione e la pressione dell'aria, nonché le impostazioni generali del dispositivo (volume, suoneria, luminosità dello schermo, ecc.).

8.3 Consenso Informato degli Interessati

Per i Servizi Cloud IBM Trusteer Pinpoint e per i Servizi Cloud IBM Trusteer Mobile SDK:

Il Cliente dichiara e garantisce di aver ottenuto o che otterrà qualsiasi consenso informato, autorizzazione o licenza completi, necessari per consentire l'utilizzo legale del Servizio Cloud e la raccolta e il trattamento delle informazioni da parte di IBM, quale Responsabile del Trattamento del Cliente, tramite il Servizio Cloud.

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

Il Cliente autorizza IBM ad ottenere i consensi informati completi necessari per consentire l'utilizzo legale del Servizio Cloud, la raccolta e il trattamento delle informazioni come descritto nell'Accordo di licenza per l'utente finale disponibile alla seguente pagina Web https://www.trusteer.com/support/end-user-license-agreement. Qualora il Cliente (e non IBM) determini di dover gestire le comunicazioni con gli utenti finali che necessitano del consenso informato, il Cliente riconosce di aver ottenuto o si impegna ad ottenere qualsiasi consenso informato, autorizzazione o licenza completi, necessari per consentire l'utilizzo legale dei Servizio Cloud e la raccolta e il trattamento delle informazioni da parte di IBM, quale Responsabile del Trattamento del Cliente, tramite il Servizio Cloud.

8.4 Utilizzo de Dati della Sicurezza

Come parte del Servizio Cloud, che include le attività di reportistica, IBM preparerà e manterrà le informazioni disidentificate e/o aggregate raccolte dal Servizio Cloud ("Dati della Sicurezza"). I Dati della Sicurezza non identificheranno il Cliente, i suoi Partecipanti Eleggibili o una persona, salvo quando diversamente specificato nel seguente comma (d). Il Cliente accetta che IBM possa utilizzare e/o copiare perennemente i Dati della Sicurezza solo per i seguenti scopi:

a. pubblicazione e/o distribuzione dei Dati della Sicurezza (ad es., nelle compilazioni e/o analisi relative alla sicurezza informatica),

b. sviluppo o miglioramento di prodotti o servizi,

c. conduzione interna della ricerca o con terzi, e

d. condivisione legale di dati di terzi confermati inerenti a responsabili di reati.

8.5 Trasferimenti oltre confine

Il Cliente accetta che IBM possa trattare il Contenuto, inclusi i Dati Personali, così come identificati nel precedente articolo Utilizzo Consentito dalla Legge e Consenso, ai sensi delle leggi e dei requisiti pertinenti entro i confini nazionali per i responsabili e subincaricati del trattamento nei seguenti paesi al di fuori dell'Area Economica Europea e nei paesi che la Commissione Europea ritiene abbiano livelli di sicurezza adeguati: gli USA.

8.6 Dati Personali

Se il Cliente inserisce Dati personali nel Servizio Cloud all'interno degli Stati membri dell'UE, in Islanda, Liechtenstein, Norvegia o Svizzera, oppure se il Cliente ha Partecipanti Eleggibili o Dispositivi Client in tali paesi, il Cliente, quale unico Titolare del trattamento di tali dati personali, nomina IBM quale Responsabile esterno del trattamento di tali dati ai sensi dell'articolo 29 del D.Lgs 196/2003 e ss.mm.. IBM tratterà tali dati esclusivamente nella misura necessaria per rendere l'offerta dei Servizi Cloud disponibile in conformità alle condizioni contenute nella descrizione dei Servizi Cloud pubblicate da IBM; il Cliente, inoltre, accetta che tale trattamento venga effettuato in conformità alle istruzioni fornite dal Cliente stesso. IBM fornirà un preavviso ragionevole tramite il Portale del Cliente qualora apportasse una modifica materiale alla sede del trattamento o alla modalità di protezione dei Dati Personali come parte integrante del Servizio Cloud. Il Cliente può recedere dal vigente periodo di abbonamento per il Servizio Cloud in questione, mediante preavviso scritto da inviare ad IBM entro trenta (30) giorni dalla comunicazione da parte di IBM della modifica stessa.

Le Parti o le relative consociate possono sottoscrivere separatamente accordi in base alle Clausole Contrattuali Standard Europee, non modificando le stesse, nei loro rispettivi ruoli, in conformità alla Decisione Europea 2010/87/UE, con la rimozione delle clausole facoltative. Qualsiasi controversia o responsabilità derivante da tali accordi, anche se generata da società consociate, sarà considerata dalle Parti come se la controversia o la responsabilità fosse sorta tra le Parti medesime in base alle condizioni del presente Accordo.

a. Il Cliente accetta che, relativamente ai servizi forniti tramite il data center tedesco, così come determinato durante il processo di provisioning, IBM possa trattare il contenuto, inclusi i Dati Personali, entro i confini nazionali dei seguenti paesi per i seguenti responsabili e subincaricati del trattamento:

Nome del Responsabile del Trattamento/Subincaricato	Ruolo (Responsabile del Trattamento dei dati o Subincaricato)	Sede
Ente appaltante IBM	Responsabile del Trattamento	Come indicato nel Documento d'Ordine
Amazon Web Services (Germania)	Subincaricato	Germania
IBM Ireland Ltd.	Responsabile del Trattamento	Irlanda
IBM Israel Ltd.	Responsabile del Trattamento	Israele

Per i servizi forniti tramite il data center tedesco, alcuni servizi di assistenza clienti potrebbero essere forniti dai dipendenti di Trusteer he si trovano in un qualsiasi paese dell'Unione Europea.

b. Il Cliente accetta che, relativamente ai servizi forniti tramite il data center giapponese, così come determinato durante il processo di provisioning, IBM possa trattare il contenuto, inclusi i Dati Personali, entro i confini nazionali dei seguenti paesi per i seguenti responsabili e subincaricati del trattamento:

Nome del Responsabile del Trattamento/Subincaricato	Ruolo (Responsabile del Trattamento dei dati o Subincaricato)	Sede
Ente appaltante IBM	Responsabile del Trattamento	Giappone, come indicato nel Documento d'Ordine
Amazon Web Services (Giappone)	Subincaricato	Giappone
IBM Ireland Ltd.	Responsabile del Trattamento	Irlanda
IBM Israel Ltd.	Responsabile del Trattamento	Israele

c. Il Cliente accetta che, relativamente ai servizi forniti tramite il data center USA, IBM possa trattare il contenuto, inclusi i Dati Personali, entro i confini nazionali dei seguenti paesi per i seguenti responsabili e subincaricati del trattamento:

Nome del Responsabile del Trattamento/Subincaricato	Ruolo (Responsabile del Trattamento dei dati o Subincaricato)	Sede
Ente appaltante IBM	Responsabile del Trattamento	Come indicato nel Documento d'Ordine
Amazon Web Services LLC	Subincaricato	Stati Uniti
IBM Ireland Ltd.	Responsabile del Trattamento	Irlanda
IBM Israel Ltd.	Responsabile del Trattamento	Israele
IBM Corp	Responsabile del Trattamento	Stati Uniti

d. Per i servizi forniti tramite i data center elencati nell'Articolo 8.5.c di cui sopra, "Data center USA", IBM potrà inoltre trattare il contenuto mediante uno o più dei seguenti subincaricati applicabili, così come determinato durante il processo di provisioning:

Nome del Responsabile del Trattamento/Subincaricato	Ruolo (Responsabile del Trattamento dei dati o Subincaricato)	Sede
Amazon Web Services (Australia)	Subincaricato	Australia
Amazon Web Services (Singapore)	Subincaricato	Singapore
Amazon Web Services (Irlanda)	Subincaricato	Irlanda

e. Il Cliente accetta che IBM possa, previo avviso mediante il Portale del Cliente, migrare il trattamento da Amazon Web Services nei data center di IBM. Inoltre, IBM potrà variare, con un avviso mediante il Portale del Cliente, gli elenchi dei precedenti sub-incaricati.

f. 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.

g. I dati del supporto del Cliente sono archiviati nel server cloud Salesforce.com che si trova in Irlanda.

h. 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.

9. Service Level Agreement ("SLA")

IBM fornisce il seguente Service Level Agreement ("SLA") di 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 solo per essere utilizzato negli ambienti di produzione.

9.1 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 ad 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 richiesta di rimedio valida relativa allo SLA sarà un credito di cui verrà dato atto 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 i contenuti, 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 in base alla disponibilità cumulativa del Servizio Cloud durante ciascun mese contrattuale, come mostrato nella tabella seguente. Il rimborso totale rispetto ad un mese contrattuale non può superare il 10 percento di un dodicesimo (1/12) del corrispettivo annuale per il Servizio Cloud.

9.2 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)
< 99,5%	2%
<98,0%	5%
< 96,0%	10%

* Se il Cliente ha acquistato 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 rimedio, scontato del 50%. IBM applicherà uno sconto direttamente al Cliente.

I Livelli di Servizi ed i Crediti di Servizi 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'	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' 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:

43.200 minuti totali in un mese contrattuale di 30 (trenta) giorni
- 230 minuti pesati di Tempo di Fermo
= 42.970 minuti

43.200 minuti totali

= 2% Credito di Disponibilità per il 99,4% di disponibilità in un mese contrattuale

10. 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. 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 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-01.ibm.com/software/security/trusteer/support/.
- Per le opzioni e i dettagli inerenti al supporto, accedere alla Guida al Supporto Software as a Service [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

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 richiest 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-01.ibm.com/software/security/trusteer/support/.
- Per le opzioni e i dettagli inerenti al supporto, accedere alla Guida al Supporto Software as a Service [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

11. Informazioni sulle Titolarità e sulla Fatturazione

11.1 Calcolo dei Corrispettivi

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

a. **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.

b. **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.

c. **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 questo Servizio Cloud, un'applicazione è una singola Applicazione "Business" o "Retail" del Cliente.

d. **Impegno** – è un'unità di misura che consente di ottenere i servizi. Un Impegno consiste in servizi professionali e/o di formazione relativi ai Servizi Cloud. È necessario ottenere titolarità sufficienti a coprire ciascun Impegno.

11.2 Corrispettivi Mensili Parziali

Un Corrispettivo Mensile Parziale così come specificato nel Documento d'Ordine può essere ripartito proporzionalmente.

12. Conformità e Verifica

L'accesso ai Servizi Cloud IBM Trusteer Fraud Protection è soggetto ad un numero massimo di Applicazioni, di Partecipanti Eleggibili e/o di Dispositivi Client come specificato nel Documento d'Ordine. Il Cliente è responsabile di garantire che il relativo numero di Applicazioni, di Partecipanti Eleggibili e/o di Dispositivi Client non superi il numero massimo consentito, come specificato nel Documento d'Ordine.

IBM potrebbe effettuare un controllo per verificare la conformità con il numero massimo consentito di Applicazioni, di Partecipanti Eleggibili e/o di Dispositivi Client.

13. 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 è soggetto a rinnovo automatico, 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 disdetta almeno 90 (novanta) giorni prima della data di scadenza del periodo contrattuale, il Servizio Cloud sarà rinnovato automaticamente per la durata contrattuale specificata nella presente PoE.

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 non voler rinnovare 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.

14. Prerequisiti Software (Software di Abilitazione)

Il presente Servizio Cloud comprende il prerequisito software che potrà essere utilizzato solo in associazione con l'utilizzo da parte del Cliente del Servizio Cloud e solo per la durata del periodo di abbonamento del Servizio Cloud.

15. Aumento annuale della quota di abbonamento di IBM Trusteer

IBM si riserva il diritto di adeguare la quota di abbonamento inerente ai Servizi Cloud. L'adeguamento del canone di abbonamento sarà rispecchiato nei prezzi specificati nel Preventivo applicabile, e per la durata prevista nello stesso Preventivo. Ulteriori adeguamenti del canone di abbonamento, che saranno applicabili non più di una volta ogni dodici (12) mesi mediante una percentuale determinata da IBM che non superi il 3%, potrebbero applicarsi qualora la durata del Servizio Cloud venga prorogata tramite rinnovo automatico o uso continuativo. Tali adeguamenti del canone non modificano la titolarità del Cliente inerente ai Servizi Cloud o il calcolo dei corrispettivi in base al quale è stato ottenuto il Servizio Cloud. I Business Partner IBM sono soggetti indipendenti da IBM e stabiliscono autonomamente i propri prezzi e condizioni.

Accettato da:

_____

Firma e timbro del Cliente

Data:

Ai sensi ed agli effetti degli artt. 1341 e 1342 del Codice Civile italiano, il Cliente approva espressamente i seguenti articoli del presente documento: “Servizi Cloud IBM Trusteer Mobile”; “Service Level Agreement ("SLA")”; “Crediti di Disponibilità”; “Opzioni di Durata e Rinnovo”; “Aumento annuale della quota di abbonamento di IBM Trusteer”.

_____

Firma e timbro del Cliente

Data: