IBM Trusteer Pinpoint Detect

Nella presente Descrizione dei Servizi viene illustrato il Servizio Cloud. I documenti d'ordine applicabili riportano prezzi e dettagli aggiuntivi sull'ordine del Cliente.

1. Servizio in Cloud

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. Trusteer Management Application (TMA) e Trustboard:

   TMA è la tradizionale applicazione di gestione di Trusteer che consente ai Clienti di valutare e classificare gli avvisi. Trustboard è una nuova applicazione di gestione che viene utilizzata principalmente per la ricerca. I Clienti possono scegliere di utilizzare TMA o Trustboard in qualsiasi momento. TMA e Trustboard vengono rese disponibili nell'ambiente su cloud di IBM Trusteer, attraverso cui il Cliente (e un numero illimitato di suoi dipendenti autorizzati) potrà: (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. IBM Trusteer Pinpoint Detect e IBM Trusteer Pinpoint Verify sono utilizzati come parte della procedura di accesso a TMA e Trustboard.

b. Script Web e/o API:

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

Una "Sessione" rappresenta un'interazione tra l'Applicazione del Cliente (Web o mobile) e il Servizio Cloud che genera una o più valutazioni in tempo reale del rischio. La misurazione di una Sessione parte dal momento dell'inizio dell'interazione fino al termine della stessa. La fine dell'iterazione si registra quando si verifica uno dei seguenti eventi:

- L'iterazione viene ripristinata attraverso la regolare modalità che prevede lo scollegamento dalle applicazioni.
- Browser, applicazione o schede chiuse.
- Cancellazione dei cookie.
- Timeout.

Una Sessione può includere un numero qualsiasi di attività, quali: accesso, navigazione, checkout, impostazione dei pagamenti e altre, come definito dall'applicazione del Cliente. È bene chiarire che ai fini di questo Servizio Cloud, una Connessione (come definita di seguito) rappresenta una Sessione.

1.1 Offerte

Il Cliente può selezionare le seguenti offerte disponibili.

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

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

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

Nel presente Servizio Cloud è incluso il Supporto Premium (così come definito nel seguente Art. "Supporto Tecnico").

Il servizio è disponibile per l'acquisto in pacchetti da 100 Partecipanti Eleggibili o 100 Connessioni.

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

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

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

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

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

Il supporto Premium è incluso in questo Servizio Cloud.

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

Pinpoint Detect Policy Manager:

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

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

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

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

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

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

1.1.3 IBM Trusteer Pinpoint Detect for Connections

Questo Servizio Cloud fornisce protezione ed ha l'obiettivo di rilevare i tentativi di account takeover, nonché fornire direttamente al Cliente il punteggio della valutazione del rischio o dell'attendibilità dei browser e/o dei dispositivi mobili (tramite il browser nativo dell'applicazione per dispositivi mobili del Cliente) che accedono ad un'Applicazione "Business" o "Retail". La soluzione utilizza diversi indicatori di rischio, analizzando i dispositivi, la connessione ed il comportamento dell'utente e confrontandoli con la cronologia dell'utente per identificare un eventuale utilizzo sospetto.

Il Servizio Cloud può utilizzare le connessioni provenienti sia da dispositivi mobili che da canali web. IBM Trusteer Pinpoint Detect include titolarità per IBM Trusteer Mobile SDK, ove necessario.

Il Servizio Cloud è disponibile per l'acquisto in pacchetti di 100 Connessioni annuali.

1.2 Servizi Opzionali

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

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

Per Applicazione Client s'intende un'Applicazione Web e/o un'Applicazione per dispositivi mobili. Un'Applicazione Web raggruppa tutte le funzioni offerte ai Partecipanti Eleggibili del Cliente attraverso diverse pagine web, a partire da un pannello di accesso o identificazione, per proseguire con la possibilità di monitorare le singole Applicazioni nella console Trusteer (Trusteer Management Application). Un'Applicazione per dispositivi mobili raggruppa tutte le funzioni offerte ai Partecipanti Eleggibili del Cliente attraverso un programma software che è possibile scaricare da uno store di applicazioni (store), a partire da un pannello di accesso o identificazione, per proseguire con la possibilità di monitorare le singole Applicazioni nella console Trusteer (Trusteer Management Application).

L'integrazione di IBM Trusteer Pinpoint richiede la titolarità a IBM Trusteer Pinpoint Application per tutte le Applicazioni.

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

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

Per Applicazione Client s'intende un'Applicazione Web e/o un'Applicazione per dispositivi mobili. Un'Applicazione Web raggruppa tutte le funzioni offerte ai Partecipanti Eleggibili del Cliente attraverso diverse pagine web, a partire da un pannello di accesso o identificazione, per proseguire con la possibilità di monitorare le singole Applicazioni nella console Trusteer (Trusteer Management Application). Un'Applicazione per dispositivi mobili raggruppa tutte le funzioni offerte ai Partecipanti Eleggibili del Cliente attraverso un programma software che è possibile scaricare da uno store di applicazioni (store), a partire da un pannello di accesso o identificazione, per proseguire con la possibilità di monitorare le singole Applicazioni nella console Trusteer (Trusteer Management Application).

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

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

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

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

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

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

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

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

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

1.2.5 IBM Trusteer Pinpoint Malware Detection

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

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

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

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

a. Dati sugli eventi:

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

b. Advanced Edition:

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

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

c. Standard Edition:

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

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

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

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

1.2.8 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:

   I Clienti possono scegliere di utilizzare TMA o Trustboard in qualsiasi momento. Il Cliente (e un numero illimitato dei suoi dipendenti autorizzati del Cliente) può utilizzare sia l'applicazione TMA che quella Trustboard 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.

1.2.9 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:

   I Clienti possono scegliere di utilizzare TMA o Trustboard in qualsiasi momento. Il Cliente (e un numero illimitato dei suoi dipendenti autorizzati del Cliente) può utilizzare sia l'applicazione TMA che quella Trustboard 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.

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

IBM Trusteer Rapport Remediation for Retail e IBM Trusteer Rapport Remediation for Business hanno l'obiettivo di ricercare, porre rimedio, bloccare e rimuovere le infezioni malware di tipo man-in-the-browser (MitB) dai dispositivi infetti (PC/MAC) dei Partecipanti Eleggibili che accedono all'Applicazione del Cliente

in modo appropriato al contesto, dove le infezioni malware MitB sono state rilevate dai dati sugli eventi di IBM Trusteer Pinpoint Malware Detection. Il Cliente deve disporre della sottoscrizione ad un abbonamento corrente dell'offerta IBM Trusteer Pinpoint Malware Detection II al momento in esecuzione sull'Applicazione del Cliente. Il Cliente può utilizzare l'offerta di questo Servizio Cloud soltanto insieme ai Partecipanti Eleggibili che accedono all'Applicazione del Cliente ed esclusivamente come strumento con l'obiettivo specifico di ricercare e correggere un determinato dispositivo infetto (PC/MAC). IBM Trusteer Rapport Remediation attualmente deve essere eseguito sui suddetti dispositivi coinvolti (PC/MAC) dei Partecipanti Eleggibili, i quali devono accettare l'accordo EULA, autenticarsi almeno una volta su una o più Applicazioni del Cliente e la configurazione del Cliente deve includere la raccolta di ID Utente. Per fugare qualsiasi dubbio, l'offerta di questo Servizio Cloud non include il diritto di utilizzare Trusteer Splash e/o promuovere il Software Client del Titolare dell'Account in qualsiasi altro modo per la totalità dei Partecipanti Eleggibili del Cliente. Per gli scopi della presente Descrizione del Servizio, il Titolare dell'Account indica l'utente finale del Cliente, che ha installato il prerequisito software client, ha accettato l'Accordo di licenza per l'utente finale (End User License Agreement, "EULA") e si è autenticato almeno una volta nell'Applicazione "Retail" o "Business" del Cliente per cui il Cliente ha sottoscritto l'abbonamento per la copertura del Servizio Cloud. Software Client del Titolare dell'Account - Indica il software di abilitazione client IBM Trusteer Rapport oppure qualsiasi altro software di abilitazione client fornito con alcuni Servizi Cloud per l'installazione sul dispositivo dell'utente finale.

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

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

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

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

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

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

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

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

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

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

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

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

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

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

Il presente Servizio Cloud migliora IBM Trusteer Pinpoint Detect fornendo ulteriori informazioni e contesto sui numeri di cellulare forniti ai Servizi Cloud, consentendo di determinare il rischio di frode di una determinata sessione. Il Cliente potrà interrogare il Servizio Cloud per determinare le caratteristiche di un numero di cellulare specifico, quali ad esempio le informazioni sul gestore telefonico associate a tale numero.

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

1.3 Servizi di accelerazione

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

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

La reinstallazione può essere dovuta alla modifica da parte del Cliente del dominio dell'Applicazione o dell'host URL, alla conversione dell'Applicazione online in una nuova tecnologia, allo spostamento su una

nuova piattaforma di online banking o all'aggiunta di un nuovo flusso di accesso ad una Applicazione esistente.

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

1.3.2 IBM Trusteer Pinpoint Malware Detection Redeployment

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

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

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

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

1.3.3 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.

2. Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)

Il Supplemento al Trattamento dei Dati Personali (DPA o Data Processing Addendum) di IBM, disponibile alla pagina web http://ibm.com/dpa e le Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Sheet o Appendice DPA) nei seguenti link forniscono ulteriori informazioni sulla protezione dei dati per i Servizi Cloud e per le opzioni relative ai tipi di Contenuto che potrebbe essere trattato, per le attività di trattamento interessate, le funzionalità per la protezione dei dati e le specifiche sulla conservazione e restituzione del Contenuto. Il DPA si applica ai dati personali presenti nel Contenuto, nella misura in cui si applichino i) il Regolamento Europeo in materia di Protezione dei Dati Personali (European General Data Protection Regulation, EU/2016/679, GDPR); o ii) altre leggi sulla protezione dei dati riportate alla pagina http://ibm.com/dpa/dpl.

Le Specifiche Tecniche solitamente riportano tutte le sedi in cui IBM (compreso qualsiasi subresponsabile di terze parti) ospita e tratta i Dati Personali, senza considerare il data center da cui vengono erogati i servizi. Per un elenco delle sedi di hosting e trattamento specifiche del data center da cui vengono erogati i servizi, consultare l'Articolo 5.2 riportato di seguito (Ulteriori Informazioni sulla Sede del Trattamento).

IBM Trusteer Pinpoint Criminal Detect

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

IBM Trusteer Pinpoint Detect

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

IBM Trusteer Pinpoint Malware Detection

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

IBM Trusteer Mobile SDK

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

3. Livelli di Servizio e Supporto Tecnico

3.1 Service Level Agreement ("SLA")

IBM fornisce al Cliente il seguente Service Level Agreement ("SLA"). IBM applicherà il Rimborso più elevato applicabile sulla base della disponibilità cumulativa del Servizio Cloud raggiunta, come mostrato nella tabella seguente. La percentuale di disponibilità viene calcolata nel seguente modo: il numero totale di minuti nel mese contrattuale, meno il numero totale di minuti di Inattività del Servizio nel mese contrattuale, diviso per il numero totale di minuti nel mese contrattuale. La definizione di Inattività del Servizio, il processo di reclamo e le modalità per contattare IBM in relazione ai problemi di disponibilità del servizio sono riportati nel manuale di supporto al Servizio Cloud di IBM all'indirizzo https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilità	Credito (% della quota di abbonamento mensile*)
Inferiore al 99,9%	2%
Inferiore al 99,0%	5%
Inferiore al 95,0%	10%

* La quota di abbonamento rappresenta il prezzo contrattuale per il mese soggetto al reclamo.

3.2 Supporto tecnico

Il supporto tecnico per il Servizio Cloud, inclusi i dettagli di contatto di assistenza, i livelli di gravità, le ore di disponibilità del supporto, i tempi di risposta e altre informazioni e processi relativi al supporto, possono essere consultati selezionando il Servizio Cloud nella guida di supporto IBM disponibile alla pagina https://www.ibm.com/support/home/pages/support-guide/.

Supporto Premium:

È disponibile ad un costo aggiuntivo un abbonamento per il Supporto Premium per il Servizio Cloud che include:

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

4. Corrispettivi

4.1 Calcolo dei Corrispettivi

Le metriche dei corrispettivi per il Servizio Cloud sono specificate nel Documento d'Ordine.

Al presente Servizio Cloud si applica il seguente calcolo dei corrispettivi:

- Per Impegno si intende un servizio professionale o di formazione correlato ai Servizi Cloud.
- Si definisce Partecipante Eleggibile, qualsiasi persona fisica o giuridica idonea a partecipare a qualsiasi programma di erogazione del servizio, gestito o tracciato mediante i Servizi Cloud.
- Per Applicazione si intende un programma software denominato in modo univoco, fornito o reso disponibile, per accedere ai Servizi Cloud o da questi utilizzato.

- Una chiamata API è rappresentata da una richiesta ai Servizi Cloud attraverso un'interfaccia programmabile.
- Una Connessione è un collegamento o l'associazione di un database, un'applicazione, un server o di qualsiasi altro tipo di dispositivo, che è o è stato reso disponibile al Servizio Cloud.

4.2 Corrispettivi per i Servizi in Remoto

Un Servizio in Remoto scade 90 dopo l'acquisto, indipendentemente dal fatto che il servizio in remoto sia stato utilizzato.

5. Ulteriori condizioni

Agli Accordi per i Servizi Cloud (o agli accordi equivalenti per il cloud di base), stipulati prima del 1 gennaio 2019, si applicano le condizioni riportate alla pagina web https://www.ibm.com/acs.

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

Per i Servizi Cloud IBM Trusteer Rapport (incluso Rapport Remediation o Rapport for Mitigation, distribuito assieme con i Servizi Cloud Pinpoint): Se non diversamente concordato, ed in ottemperanza alla base giuridica per il trattamento che il Cliente ha definito in modo indipendente, il Cliente autorizza IBM a fornire l'EULA (End User License Agreement) riportato alla pagina https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA per consentire ad IBM di raccogliere e trattare le informazioni necessarie per la fornitura dei Servizi Cloud.

Per i Servizi Cloud For IBM Trusteer Rapport, il Cliente autorizza IBM, in qualità di responsabile del trattamento dei dati del Gruppo Aziendale Sponsor del Cliente, ad usare il Programma per raccogliere malware e gli elementi di malware come, ad esempio, file correlati ad attività dannose o file correlati a malfunzionamenti insoliti del Programma. IBM non usa il Programma in funzione di file contenenti informazioni personali del Cliente; tuttavia, i file raccolti potrebbero contenere dati personali ottenuti da un malware senza l'autorizzazione del Cliente. IBM dovrà 1) cancellare tempestivamente qualsiasi file non pertinente per tale analisi e 2) conservare i file pertinenti solo per la durata dell'analisi e in nessun caso oltre tre mesi.

5.2 Ulteriori Informazioni sulla Sede del Trattamento

Tutto l'hosting ed il trattamento dei dati personali, compresi da tutti i subresponsabili di terze parti identificati nelle Specifiche Tecniche, sarà condotto in tutte le sedi indicate di seguito:

Per tutti i servizi forniti tramite i data center ubicati in Germania, IBM limiterà l'hosting ed il trattamento dei Dati Personali al paese dell'entità appaltante di IBM ed ai seguenti paesi: Germania, Israele, Irlanda e Paesi Bassi.

Per tutti i servizi forniti tramite i data center ubicati in Giappone, IBM limiterà l'hosting ed il trattamento dei Dati Personali al paese dell'entità appaltante di IBM ed ai seguenti paesi: Giappone, Israele ed Irlanda.

Per tutti i servizi forniti tramite i data center ubicati negli Stati Uniti, IBM limiterà l'hosting ed il trattamento dei Dati Personali al paese dell'entità appaltante di IBM ed ai seguenti paesi: Stati Uniti, Israele, Irlanda, Singapore ed Australia.

Oltre alle sedi riportate in precedenza, per tutti i servizi forniti tramite i data center siti in Germania, Giappone e Stati Uniti, (1) l'hosting ed il trattamento dei dati di supporto potrà essere assicurato in Germania e Francia da Salesforce.Com, in qualità di subresponsabile di terze parti e (2) per i clienti con l'opzione che consente di inviare dati ai provider Mobile Carrier Intelligence, l'hosting ed il trattamento dei Dati Personali potrà avvenire nei paesi dei subresponsabili di terze parti applicabili, come riportato nelle Specifiche Tecniche. Nonostante quanto diversamente indicato nelle Specifiche Tecniche, i subresponsabili di terze parti specificati nella clausola (2) della frase precedente potrebbero non essere conformi a ISO 27001 o SOC2.

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

5.3 Dati del Titolare dell'Account

Per chiarezza, in presenza di più di un cliente IBM affiliato al Software Client del Titolare dell'Account di un determinato Titolare dell'Account (quali i clienti IBM, "Clienti Affiliati") e nel caso in cui i servizi riportati nella presente Descrizione dei Servizi siano erogati da IBM a tali Clienti Affiliati attraverso data center ubicati in regioni diverse, sarà possibile che i dati del Titolare dell'Account vengano trattati in una o tutte le sedi associate al data center in questione, così come specificato nell'Articolo 5.2 precedente.

5.4 Soluzioni integrate

Per chiarezza, le diverse offerte con marchi Trusteer possono costituire una soluzione integrata. Pertanto, se il Cliente recede da uno di questi Servizi Cloud, IBM potrà conservare i dati del Cliente allo scopo di assicurare l'erogazione al Cliente dei rimanenti Servizi Cloud, in base alla presente Descrizione dei Servizi, oltre ad altri servizi Trusteer, ai sensi delle descrizioni dei servizi applicabili a tale altro servizio Trusteer.

5.5 Prerequisiti Software (Software di Abilitazione)

Il Servizio Cloud contiene il seguente Software di Abilitazione:

- Agenti IBM Rapport

5.6 Pinpoint Best Practices

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

5.7 Dati raccolti come parte della distribuzione

La distribuzione del Servizio Cloud può comportare la fornitura a IBM di determinati dati da parte del Cliente. Tali dati non devono includere informazioni che possono identificare o che possono essere attribuite a individui specifici. Ulteriori Linee Guida sui dati forniti a IBM come parte della distribuzione, sono incluse nelle Linee Guida sulla Distribuzione di Trusteer, da fornire al Cliente.

6. Condizioni derogative

6.1 Uso dei Dati

Quanto segue prevale su quanto diversamente riportato nell'Articolo Contenuto e Protezione dei Dati Personali dei termini di base del Servizio Cloud tra le parti: IBM non utilizzerà o divulgherà i risultati derivanti dall'utilizzo da parte del Cliente del Servizio Cloud che sono specifici del Contenuto del Cliente (Approfondimenti) o che altrimenti identifichino il Cliente. IBM tuttavia utilizzerà il Contenuto e altre informazioni derivanti dal Contenuto (ad eccezione degli Approfondimenti), come parte del Servizio Cloud, allo scopo di migliorare il Servizio Cloud. Allo scopo di migliorare il processo di rilevamento delle minacce e la conseguente protezione dalle stesse, IBM potrà decidere di condividere gli identificatori di minacce ed altre informazioni di sicurezza presenti nel Contenuto.

Accettato da:

_____

Firma e timbro del Cliente

Data: .....

Ai sensi e per gli effetti degli articoli 1341 e 1342 del Codice Civile Italiano, il Cliente approva specificamente i seguenti articoli del presente documento: "IBM Trusteer Pinpoint Detect Premium for Retail e/o IBM Trusteer Pinpoint Detect Premium for Business", "Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)", "Service Level Agreement ("SLA")", "EULA e Basi giuridiche per il trattamento dei dati dei Data Subjects ", "Prerequisiti Software (Software di Abilitazione)".

Accettato da:

_____

Firma e timbro del Cliente

Data: .....