Condizioni di Utilizzo IBM (TOU) – Condizioni Specifiche dell'Offerta SaaS

IBM Security Trusteer Fraud Protection

Le Condizioni di Utilizzo ("ToU") sono costituite dalle presenti Condizioni di Utilizzo IBM – Condizioni Specifiche dell'Offerta SaaS ("Condizioni Specifiche dell'Offerta SaaS") e dalle disposizioni contenute nel documento Condizioni di Utilizzo IBM - Condizioni Generali ("Condizioni Generali") disponibile alla seguente pagina web: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

In caso di discordanza, le presenti Condizioni Specifiche dell'Offerta SaaS prevalgono sulle Condizioni Generali. Ordinando, accedendo o utilizzando i servizi IBM SaaS, il Cliente accetta le presenti Condizioni di Utilizzo (ToU).

Le presenti Condizioni di Utilizzo (ToU) sono disciplinate da IBM International Passport Advantage Agreement, IBM International Passport Advantage Express Agreement, o IBM International Agreement per l'offerta dei Servizi IBM SaaS selezionata, quando applicabili ("Accordo"), e complessivamente costituiscono l'accordo completo tra le parti.

1. IBM SaaS

Le presenti Condizioni Specifiche dell'Offerta SaaS si applicano alla seguente offerta di servizi IBM SaaS:

1.1 Offerte Rapport IBM SaaS

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 Offerte Pinpoint IBM SaaS

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile

- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 Offerte Mobile IBM SaaS

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

2. Calcolo dei Corrispettivi

I servizi IBM SaaS sono venduti secondo uno dei seguenti calcoli dei corrispettivi e come specificato nel Documento della Transazione:

a. **Partecipante Eleggibile** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. 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 IBM SaaS. È necessario ottenere titolarità sufficienti per coprire tutti i Partecipanti Eleggibili gestiti o tracciati all'interno dei servizi IBM SaaS durante il periodo di misurazione specificato nel Documento della Transazione del Cliente.

   Ciascun programma per l'erogazione del servizio gestito dall'offerta IBM SaaS, è analizzato separatamente e poi di nuovo aggiunto. Le persone giuridiche o fisiche eleggibili per i programmi di fornitura dei servizi devono ottenere titolarità separate.

   Per queste offerte, il programma di fornitura dei servizi include una singola Applicazione "Business" o "Retail" del Cliente con una pagina di accesso principale e altre pagine correlate per ciascuna Applicazione "Business" o "Retail". Un Partecipante Eleggibile è un utente finale del Cliente che dispone di credenziali di accesso per l'Applicazione "Business" o "Retail".

b. **Dispositivo Client** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. 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 esegua, fornisca dati, utilizzi i servizi forniti da IBM SaaS, o che acceda ai servizi IBM SaaS in qualunque altro modo, durante il periodo di misurazione specificato nel Documento della Transazione del Cliente.

3. Corrispettivi e Fatturazione

L'ammontare da pagare per i servizi IBM SaaS viene specificato nella Documentazione d'Ordine (Documento della Transazione).

3.1 Corrispettivi Mensili Parziali

Un Corrispettivo Mensile Parziale così come specificato nel Documento della Transazione può essere valutato proporzionalmente.

4. Conformità e Verifica

L'accesso alle offerte IBM Security Trusteer Fraud Protection è soggetto ad un numero massimo di Partecipanti Eleggibili o Dispositivi Client come specificato nel Documento della Transazione. Il Cliente ha la responsabilità di garantire che il relativo numero di Partecipanti Eleggibili o Dispositivi Client non superi il numero massimo consentito come specificato nel Documento della Transazione.

Potrebbe essere eseguito un controllo per verificare la conformità al numero massimo consentito di Partecipanti Eleggibili o Dispositivi Client.

5. Opzioni di rinnovo del Periodo di Abbonamento ai servizi IBM SaaS

Il Documento della Transazione del Cliente verrà aggiornato se i servizi IBM SaaS verranno rinnovati alla fine del Periodo di Abbonamento, secondo una delle seguenti opzioni:

5.1 Rinnovo Automatico

Se il Documento della Transazione del Cliente include il rinnovo automatico dei servizi del Cliente, questi può recedere dal Periodo di Abbonamento in scadenza per i servizi IBM SaaS, mediante un preavviso scritto inviato al rappresentante commerciale IBM o al Business Partner IBM almeno novanta (90) giorni prima della scadenza dell'abbonamento indicata nel Documento della Transazione. Se IBM o il relativo Business Partner IBM non riceve alcuna comunicazione di recesso entro la data di scadenza, il Periodo di Abbonamento in scadenza verrà rinnovato automaticamente per la durata di un anno o per la stessa durata del Periodo di Abbonamento originale come stabilito nel Documento della Transazione.

5.2 Fatturazione Continuativa

Se nel Documento della Transazione viene stabilito che il rinnovo dei servizi è continuativo, il Cliente continuerà ad aver accesso ai servizi IBM SaaS e dovrà corrispondere tutti i corrispettivi per l'utilizzo dei servizi IBM SaaS. Per sospendere l'utilizzo dei servizi IBM SaaS e arrestare il processo di fatturazione continuativa, il Cliente deve fornire ad IBM o al Business Partner IBM un preavviso scritto di novanta (90) giorni, richiedendo la cancellazione dell'accesso ai servizi IBM SaaS. In seguito alla cancellazione dell'accesso del Cliente, saranno fatturati al Cliente tutti i corrispettivi riguardanti l'accesso ancora in sospeso fino al mese in cui è stata effettuata la cancellazione.

5.3 Rinnovo Richiesto

Se il Documento della Transazione stabilisce che il tipo di contratto per il Cliente è "a tempo determinato", i servizi IBM SaaS termineranno alla fine del Periodo di Abbonamento e l'accesso del Cliente ai servizi IBM SaaS verrà revocato. Per continuare ad utilizzare i servizi IBM SaaS oltre quella data, il Cliente dovrà effettuare un ordine rivolgendosi al rappresentante IBM o al Business Partner IBM e sottoscrivere un nuovo Periodo di Abbonamento.

6. Supporto tecnico

Il Supporto tecnico per i servizi IBM SaaS è disponibile per il Cliente ed i relativi Partecipanti Eleggibili per assistenza durante l'utilizzo degli stessi.

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

Per ciascuna offerta IBM SaaS, è disponibile ad un costo aggiuntivo un abbonamento per il Supporto Premium, ad eccezione delle offerte IBM Security Trusteer Mobile SDK e IBM Security Trusteer Rapport Mandatory Service.

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 di IBM 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 accedere direttamente al supporto telefonicamente.
- 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 di IBM Software as a Service [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

7. Ulteriori Condizioni dell'Offerta IBM SaaS

7.1 Conformità Safe Harbor

IBM si attiene al U.S. – EU Safe Harbor Framework developed by the U.S. Department of Commerce in coordinamento con la Commissione Europea. I prodotti IBM Security Trusteer sono inclusi nella certificazione 'EU-U.S. Safe Harbor' di IBM. Ulteriori informazioni inerenti alla certificazione 'Safe Harbor' e all'elenco di società 'Safe Harbor' sono disponibili alla pagina web: http://export.gov/safeharbor/.

7.2 Aumento annuale della quota di abbonamento del Client Annuale

IBM si riserva il diritto di adeguare la quota di abbonamento inerente ai servizi IBM SaaS non più di una volta ogni dodici (12) mesi applicando una percentuale determinata da IBM che non superi il 3%. L'adeguamento della quota di abbonamento entrerà in vigore alla scadenza della data del periodo di copertura iniziale. Tale adeguamento della quota non modifica la titolarità del Cliente inerente ai servizi IBM SaaS o il calcolo dei corrispettivi in base al quale sono stati ottenuti i servizi IBM SaaS. I Business Partner IBM sono soggetti indipendenti da IBM e stabiliscono autonomamente i propri prezzi e le condizioni applicabili.

7.3 Supporto Premium

Il Cliente ha diritto al Supporto Premium solo per le offerte IBM SaaS per le quali il Cliente ha sottoscritto l'abbonamento relativo all'offerta associata al Supporto Premium.

7.4 Utilizzo consentito dalla legge e consenso

Autorizzazione per la Raccolta e il Trattamento dei Dati

L'offerta IBM SaaS è stata progettata per aiutare il Cliente a migliorare la sicurezza del proprio ambiente e dei suoi dati. I servizi IBM SaaS raccoglieranno le informazioni dai Partecipanti Eleggibili e dai Dispositivi Client che interagiscono con le Applicazioni "Business" o "Retail" per le quali il Cliente ha sottoscritto l'abbonamento per la copertura delle offerte IBM SaaS. I servizi IBM SaaS raccolgono informazioni che, singolarmente o insieme, possono essere considerate da alcuni ordinamenti come 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 aggiornati per migliorare la funzionalità dei servizi IBM SaaS. 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 l'articolo Trasferimenti oltre confine, nell'articolo Riservatezza dei Dati delle presenti ToU e nell'articolo Riservatezza e Sicurezza dei dati UE delle Condizioni Generali inerenti alle ToU.

Per le offerte IBM Security Trusteer Pinpoint:

I dati raccolti possono includere l'indirizzo IP dell'utente, gli ID utente criptati o in formato hash irreversibile (one-way), i cookies dei domini non filtrati, le visite alle Applicazioni protette e ai siti di phishing e le credenziali inserite nei siti di phishing.

Per le offerte IBM Security Trusteer Mobile SDK offerings e IBM Security Trusteer Mobile Browser:

I dati raccolti possono includere l'indirizzo IP dell'utente, gli ID utente criptati o in formato hash irreversibile (one-way), le sedi geografiche, le visite alle Applicazioni protette, nonché le informazioni della scheda SIM, il nome del dispositivo e le affiliazioni del Cliente.

Per le offerte IBM Security Trusteer Rapport:

I dati raccolti possono includere l'indirizzo IP dell'utente, gli ID utente criptati o in formato hash irreversibile (one-way), gli eventi di sicurezza, i nomi utente e gli indirizzi email forniti allo scopo di contattare IBM per il supporto clienti, le affiliazioni del Cliente, le password criptate utilizzate nei siti protetti, le visite ad Applicazioni protette e ai siti di phishing, i numeri di carte di credito criptati, i file e i dati raccolti in remoto dal personale IBM per indagare su presunti malware, attività dannose o malfunzionamenti.

Consenso informato degli Interessati:

L'utilizzo di questi servizi IBM SaaS può implicare varie leggi o normative. I servizi IBM SaaS possono essere utilizzati solo per scopi legali e nei termini consentiti dalla legge. Il Cliente accetta di utilizzare i servizi IBM SaaS in ottemperanza alle leggi, normative e policy applicabili e se ne assume ogni responsabilità ed obbligazione.

Per le offerte IBM Security Trusteer Pinpoint e IBM Security Trusteer Mobile SDK:

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 servizi IBM SaaS e la raccolta e il trattamento delle informazioni da parte di IBM tramite i servizi IBM SaaS.

Per le offerte IBM Security Trusteer Rapport e & IBM Security Trusteer Mobile Browser:

Il Cliente autorizza IBM ad ottenere consensi completamente informati necessari per consentire l'utilizzo legale dei servizi IBM SaaS, 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 completamente informato, autorizzazione o licenza, necessari per consentire l'utilizzo legale dei servizi IBM SaaS e la raccolta e il trattamento delle informazioni da parte di IBM, quale Responsabile del Trattamento del Cliente, tramite i servizi IBM SaaS.

7.5 Trasferimenti oltre confine

Il Cliente accetta che IBM possa trattare il contenuto, inclusi i Dati Personali, 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.

7.6 Privacy dei Dati

Se il Cliente inserisce Dati personali nei servizi IBM SaaS all'interno degli Stati membri dell'UE, 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 per gli scopi richiesti per l'erogazione dell'offerta IBM SaaS, in conformità alle condizioni contenute nella descrizione dei servizi IBM SaaS pubblicate da IBM; il Cliente, inoltre, accetta che tale trattamento sarà effettuato in conformità con le istruzioni fornite dal Cliente stesso. IBM fornirà un preavviso ragionevole qualora apportasse una modifica materiale alla sede del trattamento o alla modalità di protezione dei Dati Personali come parte integrante dei servizi IBM SaaS. Il Cliente può recedere dal vigente Periodo di Abbonamento per i servizi IBM SaaS in questione, mediante preavviso scritto da inviare ad IBM entro trenta (30) giorni dalla comunicazione da parte di IBM della modifica stessa. Il Cliente accetta che 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 della Transazione
Amazon Web Services LLC	Subincaricato	410 Terry Ave. N Seattle, WA 98109 Stati Uniti

Nome del Responsabile del Trattamento/Subincaricato	Ruolo (Responsabile del Trattamento dei dati o Subincaricato)	Sede*
Connectria Corp.	Subincaricato	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 Stati Uniti
IBM Israel Ltd.	Subincaricato	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israele
IBM Corp	Subincaricato	1 New Orchard Rd. Armonk, NY 10504 Stati Uniti

Il Cliente accetta che IBM possa, ove lo ritenesse necessario e previa notifica, variare l'elenco delle sedi nazionali per la fornitura dell'offerta IBM SaaS.

Il Cliente accetta che per il servizio fornito 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 della Transazione
Amazon Web Services (Germania)	Subincaricato	Monaco, Germania
IBM Israel Ltd.	Subincaricato	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israele

Il Cliente accetta che per il servizio fornito tramite il data center del Giappone, 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 della Transazione
Amazon Web Services (Giappone)	Subincaricato	Tokyo, Giappone
IBM Israel Ltd.	Subincaricato	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israele

* Le sedi identificate nelle tabelle precedenti includono gli indirizzi degli uffici aziendali del Responsabile del Trattamento/Subincaricato. I data center si trovano all'interno dello stesso paese identificato.

Le Parti o le relative consociate possono sottoscrivere separatamente accordi standard non emendati 'EU Model Clause', in conformità alla EC Decision 2010/87/EU con le clausole facoltative rimosse. Qualsiasi controversia o responsabilità derivante da tali Accordi, anche se generata da società consociate, verrà considerata dalle Parti come se la controversia o la responsabilità fosse sorta tra le Parti medesime in base alle condizioni del presente Accordo.

Appendice A

1. Offerte IBM SaaS

IBM offre questi servizi come offerte e servizi autonomi oppure come offerte e servizi aggiuntivi. Le offerte IBM SaaS specifiche ordinate sono indicate nella PoE del Cliente.

1.1 Definizioni di "Business" e "Retail"

I prodotti antifrode IBM Security Trusteer sono concessi in licenza per essere utilizzati con Applicazioni di tipo specifico. Un'Applicazione viene definita da una delle seguenti tipologie: "Retail" o "Business". Sono disponibili offerte separate per le Applicazioni "Retail" o "Business".

- Un'Applicazione "Retail" viene definita come applicazione di online banking, applicazione per dispositivi mobili o applicazione di e-commerce, progettata per assistere gli utenti. Le policy del Cliente possono classificare alcune piccole imprese come eleggibili per l'accesso alle applicazioni "retail".
- Un'Applicazione "Business" viene definita come applicazione di online banking, applicazione per dispositivi mobili o applicazione di e-commerce, progettata per assistere persone giuridiche, istituzioni o soggetti equivalenti, oppure qualsiasi applicazione che non sia classificata come "Retail".

1.2 Offerte per l'Abbonamento base dei servizi IBM SaaS

Offerte "Business":

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

Offerte "Retail":

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

Per ciascuna offerta "Business" e "Retail", è disponibile ad un costo aggiuntivo il prodotto Supporto Premium (Premium Support) associato, ad eccezione delle offerte IBM Security Trusteer Mobile SDK e IBM Security Trusteer Rapport Mandatory Service.

1.3 Ulteriori offerte per l'abbonamento ai servizi IBM SaaS per le offerte IBM Security Trusteer Rapport

Ulteriori offerte disponibili per IBM Security Trusteer Rapport for Business:

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Mandatory Service for Business

Additional offerings available for IBM Security Trusteer Rapport for Retail:

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

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

L'abbonamento a IBM Security Trusteer Rapport for Business o IBM Security Trusteer Rapport for Retail è un prerequisito per le ulteriori offerte di abbonamento ai servizi IBM SaaS associati ed elencate in questo articolo.

1.4 Ulteriori offerte per l'abbonamento ai servizi IBM SaaS per le offerte IBM Security Trusteer Pinpoint Malware Detection

Ulteriori offerte disponibili per IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition o IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Offerte aggiuntive disponibili per IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition o IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

L'abbonamento al prodotto Supporto Premium è disponibile ad un costo aggiuntivo per ciascuna delle offerte aggiuntive IBM SaaS elencate in questo articolo.

L'abbonamento alle offerte IBM Security Trusteer Pinpoint Malware Detection for Business o IBM Security Trusteer Pinpoint Malware Detection for Retail è un prerequisito per le ulteriori offerte di abbonamento ai servizi IBM SaaS associati ed elencate in questo articolo.

1.5 Ulteriori abbonamenti aggiuntivi per i servizi IBM SaaS

Qualsiasi ulteriore abbonamento ai servizi IBM SaaS per le sottoscrizioni di base di cui sopra non elencato nel presente documento, attualmente disponibile o in fase di sviluppo, non è considerato un aggiornamento e deve essere concesso separatamente.

1.6 Definizioni

Titolare del Conto – 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 IBM SaaS.

Software Client del Titolare del Conto – Indica il software di abilitazione client IBM Security Trusteer Rapport, IBM Security Trusteer Mobile Browser oppure qualsiasi altro software di abilitazione client fornito con alcuni abbonamenti ai servizi IBM SaaS per l'installazione sul dispositivo dell'utente finale.

Trusteer Splash – Indica la schermata iniziale (splash) fornita al Cliente in base ai modelli iniziali disponibili.

Pagina di destinazione – Indica la pagina ospitata da IBM fornita al Cliente insieme alle schermate iniziali del Cliente (Client splash) e al Software Client del Titolare del Conto scaricabile.

2. Offerte IBM Security Trusteer Rapport

2.1 IBM Security Trusteer Rapport for Retail e/o IBM Security 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). Grazie ad una rete di oltre dieci milioni di endpoint in tutto il mondo, IBM Security Trusteer Rapport raccoglie informazioni sugli attacchi di phishing e malware perpetrati contro le organizzazioni mondiali. IBM Security Trusteer Rapport applica degli algoritmi comportamentali finalizzati al blocco degli attacchi di phishing e ad impedire l'installazione e le attività dei malware MitB.

Questa offerta IBM SaaS dispone del calcolo dei corrispettivi inerente ai Partecipanti Eleggibili. L'offerta "Business" è venduta in pacchetti di 10 Partecipanti Eleggibili. L'offerta "Retail" è venduta in pacchetti di 100 Partecipanti Eleggibili.

Questa offerta IBM SaaS include:

a. Trusteer Management Application ("TMA"):

   L'applicazione TMA è disponibile nell'ambiente 'cloud-hosted' IBM Security Trusteer, attraverso cui il Cliente (e un numero illimitato di dipendenti autorizzati del Cliente) può: (i) ricevere la repostistica dei dati sugli eventi e le valutazioni dei rischi, (ii) visualizzare, configurare ed impostare le policy relative alla reportistica sui dati degli eventi, e (iii) visualizzare la configurazione del software di abilitazione client con licenza pubblica disciplinata da un accordo di licenza per l'utente finale ("EULA"), 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 del Conto"). Il Cliente potrà solo commercializzare il Software Client del Titolare del Conto mediante Trusteer Splash o Rapport API, e non potrà utilizzare il Software Client del Titolare del Conto per attività aziendali interne o dei propri dipendenti (usi diversi da quelli personali dei dipendenti).

b. Script Web:

   per l'accesso ad un sito web allo scopo di accedere o utilizzare le offerte IBM SaaS.

c. 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 dal Software Client del Titolare del Conto derivanti dalle interazioni online del Titolare del Conto con le proprie Applicazioni "Business" o "Retail" per cui il Cliente ha sottoscritto l'abbonamento per la copertura delle offerte IBM SaaS. I dati sugli eventi saranno ricevuti dal Software Client del Titolare del Conto 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 del Conto per i Partecipanti Eleggibili che accedono alle Applicazioni "Business" e/o "Retail" del Cliente per le quali il Cliente ha sottoscritto l'abbonamento per la copertura delle offerte IBM SaaS. Il Cliente può selezionare tra i Modelli Iniziali disponibili (Splash Templates). I modelli iniziali 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 del Conto o sulle pagine di destinazione ospitate da IBM e sul sito web IBM Security Trusteer. Qualsiasi utilizzo dei marchi, dei loghi o delle icone fornite dal Cliente avverrà in accordo con le policy di IBM in materia di pubblicità ed utilizzo dei marchi.

Il Cliente deve sottoscrivere l'abbonamento all'offerta IBM Security Trusteer Rapport Mandatory Service SaaS qualora desideri avvalersi di qualsiasi tipo di implementazione obbligatoria del Software Client del Titolare del Conto.

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 del Conto.

2.2 Offerte aggiuntive per i servizi IBM SaaS per IBM Security Trusteer Rapport for Business e/o IBM Security Trusteer Rapport for Retail

La sottoscrizione dell'abbonamento alle offerte IBM Security Trusteer Rapport è un prerequisito per l'abbonamento a qualsiasi ulteriore offerta IBM SaaS indicata di seguito. Se per i servizi IBM SaaS è specificato "for Business", anche le offerte IBM SaaS aggiuntive acquistate devono avere la stessa indicazione "for Business". Se per i servizi IBM SaaS è specificato "for Retail", anche le offerte IBM SaaS aggiuntive acquistate devono avere la stessa indicazione "for Retail". Il Cliente riceverà i dati sugli eventi dai Partecipanti Eleggibili che eseguono il Software Client del Titolare del Conto, 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.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business e/o IBM Security Trusteer Rapport Fraud Feeds for Retail

Il Cliente (e un numero illimitato di dipendenti autorizzati del Cliente) può utilizzare TMA per ricevere i dati sugli eventi relativi alle infezioni malware e su altre vulnerabilità dell'endpoint, su un determinato desktop del Titolare del Conto.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business e/o IBM Security Trusteer Rapport Phishing Protection for Retail

Il Cliente (e un numero illimitato di dipendenti autorizzati del Cliente) può utilizzare TMA per ricevere i dati di eventi relativi all'inserimento delle credenziali di accesso del Titolare del Conto in un sito di phishing o potenzialmente fraudolento. Alcune applicazioni online lecite (URL) potrebbero essere state erroneamente contrassegnate come siti di phishing determinando l'invio di un avviso ai Titolari del Conto da parte dei servizi IBM SaaS. 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.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business e/o IBM Security 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 del Conto ai Partecipanti Eleggibili che accedono alle Applicazioni "Business" e/o "Retail" del Cliente, per le quali il Cliente ha sottoscritto l'abbonamento per la copertura dei servizi IBM SaaS.

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

IBM Security 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 Security 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 IBM SaaS.

3. Offerte IBM Security Trusteer Pinpoint

IBM Security Trusteer Pinpoint è un servizio basato su cloud progettato per fornire un ulteriore livello di protezione e che aiuta nel rilevamento e nell'attenuazione degli 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 per la copertura delle offerte IBM SaaS e nei processi di prevenzione delle frodi.

Questa offerta IBM SaaS include:

a. TMA:

   TMA è disponibile nell'ambiente cloud-hosted IBM Security 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. Script Web e/o API:

   per la distribuzione su un sito web allo scopo di accedere o utilizzare l'offerta IBM SaaS.

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

Nel caso in cui le offerte IBM Security Trusteer Pinpoint Malware Detection rilevino un evento di malaware o di 'account takeover' nelle offerte IBM Security Trusteer Pinpoint Criminal Detection, il Cliente dovrà attenersi alla Guida Pinpoint Best Practices. Non utilizzare le offerte IBM Security Trusteer Pinpoint Malware Detection o IBM Security Trusteer Pinpoint Criminal Detection in modo da non interferire sulle attività del Partecipante Eleggibile immediatamente dopo il rilevamento del malware, per evitare che altri colleghino tali azioni all'utilizzo delle offerte Pinpoint Malware Detection (ad es., notifiche, messaggi,

blocco di dispositivi o blocco dell'accesso all'Applicazione "Business" e/o "Retail" immediatamente dopo il rilevamento di un malware o di un 'account takeover').

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business e/o IBM Security 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, rilevamento del phishing e rilevamento del furto di credenziali tramite malware. Le offerte IBM Security Trusteer Pinpoint Criminal Detection forniscono un altro livello di protezione e hanno l'obiettivo di rilevare i tentativi di account takeover e di fornire direttamente al Cliente punteggi per la valutazione del rischio dei browser 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 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 per la copertura dei servizi IBM SaaS oppure il Cliente può ricevere i dati sugli eventi tramite una modalità di distribuzione dell'API di backend.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile e/o IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

Le offerte IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) sono progettate per fornire un ulteriore livello di protezione che mira a proteggere da impossessamenti dell'account e da attività fraudolente, identificando accessi non consentiti agli account e fornendo raccomandazioni per il Cliente. Questa offerta IBM SaaS raccoglie informazioni provenienti dall'Applicazione "Business" e/o "Retail" del Cliente, mediante l'utilizzo delle offerte PPCD Security Mobile API, e dai dispositivi mobili dei Partecipanti Eleggibili. Le offerte IBM Security Trusteer PPCD Mobile sono progettate per mettere in correlazione le informazioni riguardanti i dispositivi mobili dei Partecipanti Eleggibili con altre origini dati come, ad esempio, le infezioni di malware in tempo reale e gli incidenti di phishing, che vengono integrati mediante altre offerte IBM SaaS di IBM Security Trusteer specificate nella presente ToU.

Il Cliente può accedere e utilizzare le offerte IBM Security Trusteer PPCD Mobile nell'ambiente 'cloud-hosted' di IBM Security Trusteer e ricevere i dati relativi alla valutazione dei rischi per i Dispositivi mobili dei Partecipanti Eleggibili derivanti dalle interazioni online di questi dispositivi mobili con le Applicazioni "Business" o "Retail" del Cliente, per le quali il Cliente ha sottoscritto l'abbonamento per la copertura delle offerte IBM SaaS. Per gli scopi di queste offerte, i "dispositivi mobili" includono solo i telefoni cellulari e i tablet supportati e non includono i PC portatili o i MAC.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition e/o IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition e/o IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition e/o IBM Security 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". Le offerte IBM Security Trusteer Pinpoint Malware Detection forniscono un altro livello di protezione e hanno l'obiettivo di consentire alle organizzazioni di dedicarsi allo sviluppo dei processi di prevenzione delle frodi basati sul rischio malware, mediante le valutazione e la segnalazione 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 dati sugli eventi 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 rilevamento 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 implementare che fornisce la funzionalità di base di questa offerta IBM SaaS come descritto nel presente documento.

3.2 Ulteriori offerte opzionali IBM SaaS per IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition e/o IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition e/o IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition e/o IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Per le offerte IBM Security Trusteer Rapport Remediation for Retail, IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition o IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition sono un prerequisito.

Per IBM Security Trusteer Pinpoint Carbon Copy for Retail, IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition o IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition sono un prerequisito. Per IBM Security Trusteer Pinpoint Carbon Copy for Business, IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition o IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition sono un prerequisito.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business e/o IBM Security Trusteer Pinpoint Carbon Copy for Retail

Le offerte IBM Security 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 per la copertura delle offerte IBM SaaS.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail aiuta a ricercare, porre rimedio, bloccare e rimuovere le infezioni malaware di tipo man-in-the-browser (MitB) da dispositivi infetti (PC/MAC) dei Partecipanti Eleggibili che accedono all'Applicazione "Retail" del Cliente in modo appropriato al contesto, dove le infezioni malware MitB sono state rilevate dai dati sugli eventi di IBM Security Trusteer Pinpoint Malware Detection. Il Cliente deve disporre della sottoscrizione ad un abbonamento corrente dell'offerta IBM Security Trusteer Pinpoint Malware Detection al momento in esecuzione sull'Applicazione "Retail" del Cliente. Il Cliente può utilizzare l'offerta IBM SaaS soltanto insieme ai Partecipanti Eleggibili che accedono all'Applicazione "Retail" del Cliente ed esclusivamente come strumento che ha lo scopo di ricercare e correggere un determinato dispositivo infetto (PC/MAC). IBM Security Trusteer Rapport Remediation for Retail deve 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, la presente offerta IBM SaaS non include il diritto di utilizzare Trusteer Splash e/o promuovere il Software Client del Titolare del Conto in qualsiasi altro modo per la totalità dei Partecipanti Eleggibili del Cliente.

4. Offerte IBM Security Trusteer Mobile

4.1 IBM Security Trusteer Mobile Browser for Business e/o IBM Security Trusteer Mobile Browser for Retail

L'offerta IBM Security Trusteer Mobile Browser è progettata per aggiungere un ulteriore livello di protezione e aiuta a 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 per la copertura delle offerte IBM SaaS, la valutazione del rischio dei dispositivi e la protezione dal phishing. Il rilevamento di reti Wi-Fi sicure è disponibile solo sulle piattaforme Android. Per gli scopi della presente offerta IBM SaaS sono inclusi i telefoni cellulari o i tablet e non sono inclusi i PC Laptop e i Mac.

Attraverso l'applicazione TMA, il Cliente (e un numero illimitato di dipendenti autorizzati del Cliente) può ricevere i dati sugli eventi, l'analisi e le informazioni statistiche sui dispositivi su cui i Partecipanti Eleggibili

hanno: (i) scaricato il Software Client del Titolare del Conto, un'applicazione gratuita con licenza pubblica disciplinata da un accordo di licenza per l'utente finale ("EULA"), e disponibile per il download sui dispositivi 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 per la copertura delle offerte IBM SaaS. Il Cliente potrà commercializzare il Software Client del Titolare del Conto solo mediante Trusteer Splash e non potrà utilizzare il Software Client del Titolare del Conto 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" e/o "Retail" del Cliente, per le quali il Cliente ha sottoscritto l'abbonamento per la copertura dei servizi IBM SaaS.

b. Trusteer Splash:

   La piattaforma di marketing Trusteer Splash identifica e commercializza il Software Client del Titolare del Conto per i Partecipanti Eleggibili che accedono alle Applicazioni "Business" e/o "Retail" del Cliente per le quali il Cliente ha sottoscritto l'abbonamento per la copertura delle offerte IBM SaaS. Il Cliente può selezionare tra i modelli iniziali disponibili ("Splash Template"). I modelli iniziali 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 del Conto o sulle pagine di destinazione ospitate da IBM oppure sul sito web IBM Security Trusteer. Qualsiasi utilizzo dei marchi, dei loghi o delle icone fornite dal Cliente avverrà in accordo con le policy di IBM in materia di pubblicità ed utilizzo dei marchi.

4.2 IBM Security Trusteer Mobile SDK for Business e/o IBM Security Trusteer Mobile SDK for Retail

Le offerte IBM Security Trusteer Mobile SDK sono progettate per aggiungere 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 per la copertura dei servizi IBM SaaS, la valutazione del rischio dei dispositivi e la protezione da pharming. Il rilevamento di reti Wi-Fi sicure è disponibile solo sulle piattaforme Android.

Le offerte IBM Security Trusteer Mobile SDK includono un software developer kit ("SDK") di proprietà di Trusteer, un pacchetto software che contiene la documentazione, le librerie del software di programmazione di proprietà ed altri file ed elementi correlati, noto come IBM Security Trusteer mobile library e come "Componente Run-time" o "Ridistribuibile", un codice proprietario generato da IBM Security Trusteer Mobile SDK che può essere incorporato e integrato nelle applicazioni per dispositivi mobili autonome e protette iOS o Android per le quali il Cliente ha sottoscritto l'abbonamento per la copertura delle offerte IBM SaaS ("Applicazioni Mobili Integrate del Cliente").

IBM Security Trusteer Mobile SDK for Retail è disponibile in pacchetti da 100 Partecipanti Eleggibili o pacchetti da 100 Dispositivi Client e IBM Security 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 Security Trusteer Mobile SDK esclusivamente allo scopo di sviluppare le Applicazioni Mobili Integrate del Cliente;

b. integrare il componente Ridistribuibile (esclusivamente in formato di codice a oggetti), 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 delle presenti ToU; 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 engineer o in altro modo convertire o decodificare l'SDK, salvo quanto previsto da norme di legge senza possibilità di deroga contrattuale; (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 forma di codice ad oggetto e conforme con tutte le direttive, istruzioni e specifiche dell'offerta IBM Security 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 di legge senza possibilità di deroga contrattuale. 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 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 dell'offerta IBM SaaS.

IBM ha eseguito il test sulle applicazioni campione create con gli strumenti per dispositivi mobili forniti nell'IBM Security 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.

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 Security Trusteer Mobile SDK da parte del Cliente è conforme alle condizioni delle presenti ToU.

5. Distribuzione delle offerte IBM SaaS Fraud Protection

La sottoscrizione all'abbonamento base del Cliente include le attività di setup e di implementazione iniziali obbligatorie, quali l'avvio iniziale in un'unica soluzione, la configurazione, i Modelli Iniziali (Splash Template), i test e la formazione.

Ulteriori servizi possono essere oggetto di contratto ad un costo aggiuntivo in un accordo separato.

Appendice B

IBM fornisce il seguente Service Level Agreement ("SLA") di disponibilità per i servizi IBM SaaS ed è applicabile se specificato nel Documento della Transazione del Cliente:

Sarà applicata la versione aggiornata di questo SLA in vigore all'inizio o al momento del rinnovo delle condizioni dell'abbonamento del Cliente. Il Cliente riconosce che questo SLA non costituisce una garanzia per il Cliente.

1. Definizioni

a. **Contatto Autorizzato** – indica la persona che il Cliente ha comunicato a IBM come autorizzata ad inoltrare eventuali Richieste di Rimedio di cui al presente SLA.

b. **Credito di Disponibilità** – indica il rimedio che IBM riconoscerà per una Richiesta di Rimedio convalidata. Il Credito di Disponibilità sarà applicato sotto forma di credito o sconto rispetto ad una fattura futura per i costi di abbonamento ai servizi IBM SaaS.

c. **Richiesta di Rimedio** – indica una richiesta inoltrata dal Contatto Autorizzato a IBM, ai sensi di questo SLA relativamente al mancato rispetto di un Livello di Servizio in un Mese Contrattuale.

d. **Mese Contrattuale** – indica ciascun mese completo durante il periodo dell'offerta IBM SaaS calcolato dalle 00:00 GMT del primo giorno del mese fino alle 23:59 GMT dell'ultimo giorno del mese.

e. **Cliente** – indica una persona giuridica che si abbona ai servizi IBM SaaS direttamente da IBM e che non sia inadempiente rispetto alle proprie obbligazioni, compresi gli obblighi di pagamento pattuiti nel suo contratto con IBM per i servizi IBM SaaS.

f. **Tempo di Fermo** – indica un periodo di tempo durante il quale è stata interrotta l'elaborazione del sistema di produzione per il Servizio e tutti gli utenti non sono in grado di utilizzare tutti gli aspetti del Servizio per cui possiedono le opportune autorizzazioni. Il Tempo di Fermo non comprende il periodo di tempo in cui il Servizio non è disponibile in seguito a:

- Tempo di Fermo di sistema pianificato;
- Forza Maggiore;
- problemi con le applicazioni, attrezzature o dati di un Cliente o di terze parti;
- atti oppure omissioni del Cliente o di terze parti (compreso chiunque abbia accesso ai servizi IBM SaaS tramite le password o le apparecchiature del Cliente);
- mancata adesione da parte del Cliente alle configurazioni di sistema richieste e alle piattaforme supportate per accedere all'offerta IBM SaaS; oppure
- la conformità da parte di IBM a qualsiasi progetto, specifiche o istruzioni fornite dal Cliente o da terze parti per conto del Cliente.

g. **Evento** – Indica un avvenimento o una serie di circostanze considerate nel loro complesso, che comportano un mancato rispetto del Livello di Servizio.

h. **Forza Maggiore** – Indica eventi naturali, atti di terrorismo, scioperi, incendi, inondazioni, terremoti, rivolte, guerra, atti, ordini o restrizioni governative, virus ed altri comportamenti dannosi, assenza di connettività di rete e di utilità o qualsiasi altra causa di indisponibilità dell'offerta IBM SaaS fuori dal ragionevole controllo di IBM.

i. **Tempo di Fermo di Sistema Pianificato** – Indica un'interruzione pianificata dell'offerta IBM SaaS a scopo di manutenzione.

j. **Livello di Servizio** – Indica lo standard qui di seguito stabilito con cui IBM valuta il livello di servizio fornito in questo SLA.

2. Crediti di disponibilità

a. Per avere diritto ad inoltrare una Richiesta di Rimedio, il Cliente deve aver aperto un ticket di assistenza per ciascun Evento con l'help desk di supporto dei clienti IBM per l'offerta IBM SaaS applicabile, nel rispetto della procedura IBM relativa alla notifica dei problemi per cui è necessaria un'assistenza di Severità 1. Il Cliente deve fornire nel dettaglio tutte le informazioni necessarie sull'Evento e fornire a IBM ragionevole assistenza nella diagnosi e risoluzione dell'Evento, per

quanto necessario al supporto per i ticket di Severità 1. Tale ticket deve essere registrato entro ventiquattro (24) ore dal momento in cui il Cliente si rende conto che l'Evento ha avuto un impatto negativo sull'utilizzo dei servizi IBM SaaS.

b. Il Contatto Autorizzato del Cliente deve inoltrare la Richiesta di Rimedio per un Credito di Disponibilità non più tardi di tre giorni (3) lavorativi dal termine del Mese Contrattuale oggetto della Richiesta di Rimedio.

c. Il Contatto Autorizzato del Cliente deve fornire a IBM tutti i dettagli che verranno ragionevolmente richiesti per la Richiesta di Rimedio compresi, a titolo esemplificativo ma non esaustivo, le descrizioni dettagliate di tutti gli Eventi coinvolti e il Livello di servizio che si sostiene non essere stato rispettato.

d. IBM valuterà internamente il tempo di fermo totale combinato durante ciascun Mese Contrattuale applicabile al Livello di Servizio corrispondente mostrato nella seguente tabella. I Crediti di Disponibilità si baseranno sulla durata del Tempo di Fermo misurata dal momento in cui il Cliente è stato interessato dal Tempo di Fermo la prima volta. Qualora il Cliente riferisca che si sono verificati contemporaneamente un Evento di un Tempo di Fermo dell'Applicazione e un Evento di Tempo di Fermo dell'elaborazione dei dati in entrata, IBM considererà i periodi di sovrapposizione del Tempo di Fermo come un unico periodo di Tempo di Fermo e non come due periodi separati. Per ciascuna Richiesta di Rimedio valida, IBM applicherà il più elevato Credito di disponibilità applicabile sulla base del Livello di Servizio raggiunto durante ciascun Mese Contrattuale, come mostrato nelle tabelle seguenti. IBM non sarà responsabile per più Crediti di Disponibilità inerenti agli stessi Eventi nello stesso Mese Contrattuale.

e. Per il Servizio in bundle (singoli Servizi confezionati e venduti insieme ad un unico prezzo combinato), il Credito di Disponibilità verrà calcolato sulla base del singolo prezzo mensile combinato per il Servizio in bundle e non del costo di abbonamento mensile per ciascun singolo Servizio IBM SaaS. Il Cliente può inoltrare soltanto Richieste di Rimedio inerenti ad un singolo Servizio IBM SaaS di un bundle in qualsiasi Mese Contrattuale; e IBM, inoltre, non sarà responsabile per Crediti di Disponibilità relativi a più di un'offerta IBM SaaS di un bundle in qualsiasi Mese Contrattuale.

f. Se il Cliente ha acquistato i servizi IBM SaaS da un rivenditore IBM, in una transazione di rivendita in cui IBM conserva la responsabilità principale per l'adempimento degli impegni dei servizi IBM SaaS e degli SLA, allora il Credito di Disponibilità sarà calcolato sul prezzo RSVP (Relationship Suggested Value Price) per i servizi IBM SaaS, applicato in quel momento, per il Servizio in vigore durante il Mese Contrattuale oggetto della Richiesta di Rimedio, scontato del 50%.

g. I Crediti totali di Disponibilità riconosciuti rispetto ad un Mese Contrattuale non supereranno, in qualsiasi caso, il dieci percento (10%) di un dodicesimo (1/12) del costo annuale pagato dal Cliente a IBM per i servizi IBM SaaS.

h. IBM utilizzerà il proprio ragionevole giudizio per convalidare le Richieste di Rimedio sulla base delle informazioni disponibili registrate da IBM, che prevarranno in caso di eventuali discrepanze con i dati in possesso del Cliente.

i. I CREDITI DI DISPONIBILITÀ FORNITI AL CLIENTE NEL RISPETTO DEL PRESENTE SLA SONO L'UNICO ED ESCLUSIVO RIMEDIO RISPETTO A QUALSIASI RICHIESTA DI RELATIVA AI LIVELLI DI SERVIZI.

3. Livelli di Servizio

Disponibilità dei servizi IBM SaaS durante un Mese Contrattuale

Livello di Servizio raggiunto (durante un mese contrattuale)	**Credito di Disponibilità (% del costo dell'Abbonamento Mensile per il Mese Contrattuale oggetto di una Richiesta di Rimedio)**
< 99,5%	2%
< 98,0%	5%
< 96,0%	10%

"Livello di Servizio raggiunto", espresso come percentuale, è calcolato nel seguente modo: (a) il numero totale di minuti in un Mese Contrattuale meno (b) il numero totale di minuti di Tempo di Fermo nel Mese Contrattuale, diviso per (c) il numero totale di minuti in un Mese Contrattuale.

Esempio: 250 minuti totali di Tempo di Fermo in un Mese Contrattuale

43.200 minuti totali in un Mese Contrattuale di 30 giorni - 250 minuti di tempo fermo = 42.950 minuti _____ 43.200 minuti totali	= 2% Credito di Disponibilità per il 99,4% del Livello di Servizio raggiunto in un Mese Contrattuale

3.1 Esclusioni dal Servizio

Il presente SLA è stato reso disponibile per i Clienti IBM. Il presente SLA non si applica nei seguenti casi:

- Servizi beta e di prova.
- Gli ambienti non di produzione, inclusi a titolo esemplificativo ma non esaustivo, gli ambienti di test, disaster recovery, controllo qualità o sviluppo.
- Le richieste di rimedio effettuate dagli utenti, gli ospiti, i partecipanti e gli invitati autorizzati del Cliente IBM relativamente ai servizi IBM SaaS.
- Nel caso di grave inadempimento contrattuale da parte del Cliente relativo ad obbligazioni contenute nelle ToU, comprese, a titolo esemplificativo ma non esaustivo, le violazioni di qualsiasi obbligazione relativa al pagamento.

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: “Opzioni di rinnovo del Periodo di Abbonamento ai servizi IBM SaaS”; “Autorizzazione per la Raccolta e il Trattamento dei Dati”; “IBM Security Trusteer Mobile Browser for Business e/o IBM Security Trusteer Mobile Browser for Retail”; “Crediti di disponibilità”.

_____

Firma e timbro del Cliente

Data: