IBM Trusteer Fraud Protection

Niniejszy opis dotyczy Usługi Przetwarzania w Chmurze, którą IBM oferuje Klientowi. „Klient” oznacza tu podmiot zawierający umowę wraz z jego autoryzowanymi użytkownikami i odbiorcami Usługi Przetwarzania w Chmurze. Odpowiednia Oferta Cenowa i dokument Proof of Entitlement (PoE) są dostarczane jako odrębne Dokumenty Transakcyjne.

1. Usługa Przetwarzania w Chmurze

Niniejszy Opis Usług obejmuje następujące Usługi Przetwarzania w Chmurze:

Usługi Przetwarzania w Chmurze Rapport:

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

Usługi Przetwarzania w Chmurze Pinpoint:

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

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

Usługi Przetwarzania w Chmurze Mobile:

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

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

1.1 Usługi przetwarzania w chmurze przeznaczone dla klientów biznesowych i indywidualnych

Usługi Przetwarzania w Chmurze IBM Trusteer są przeznaczone do używania w połączeniu z określonymi rodzajami Aplikacji. Zdefiniowane zostały dwa rodzaje Aplikacji: Aplikacja Indywidualna oraz Aplikacja Biznesowa. Dla każdego z tych rodzajów Aplikacji dostępne są odrębne oferty.

a. Aplikacja Indywidualna oznacza aplikację bankowości elektronicznej, aplikację dla urządzeń mobilnych lub aplikację do handlu elektronicznego zaprojektowaną z myślą o obsłudze konsumenta. Zgodnie ze strategią Klienta niektórym małym przedsiębiorstwom może przysługiwać dostęp do oferty dla odbiorców indywidualnych.

b. Aplikacja Biznesowa oznacza aplikację bankowości elektronicznej, aplikację dla urządzeń mobilnych lub aplikację do handlu elektronicznego zaprojektowaną z myślą o obsłudze przedsiębiorstw, instytucji i podmiotów o równoważnej kategorii, a także dowolną aplikację, która nie została sklasyfikowana jako Aplikacja Indywidualna.

1.1.1 Usługi Przetwarzania w Chmurze dla klientów biznesowych

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

1.1.2 Usługi Przetwarzania w Chmurze dla klientów indywidualnych

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

W przypadku każdej oferty Usług Przetwarzania w Chmurze dla klientów biznesowych i indywidualnych dostępne jest powiązane Wsparcie Premium za dodatkową opłatą. Wyjątek stanowią oferty Usług Przetwarzania w Chmurze IBM Trusteer Mobile SDK.

1.1.3 Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do oferty IBM Trusteer Rapport

a. Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do oferty IBM Trusteer Rapport for Business:
   - IBM Trusteer Rapport Fraud Feeds for Business
   - IBM Trusteer Rapport Phishing Protection for Business
   - IBM Trusteer Rapport Mandatory Service for Business
   - IBM Trusteer Rapport Additional Applications For Business

b. Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do oferty IBM Trusteer Rapport for Retail:
   - IBM Trusteer Rapport Fraud Feeds for Retail
   - IBM Trusteer Rapport Phishing Protection for Retail
   - IBM Trusteer Rapport Mandatory Service for Retail
   - IBM Trusteer Rapport Additional Applications For Retail

W przypadku każdego biznesowego lub indywidualnego programu dodatkowego do Usług Przetwarzania w Chmurze IBM Trusteer Rapport dostępne jest powiązane Wsparcie Premium za dodatkową opłatą. Wyjątek stanowią programy dodatkowe IBM Trusteer Rapport Mandatory Service.

W przypadku dodatkowych powiązanych Usług Przetwarzania w Chmurze wymienionych w niniejszym paragrafie wymaganiem wstępnym jest posiadanie subskrypcji usług IBM Trusteer Rapport for Business lub IBM Trusteer Rapport for Retail.

1.1.4 Dodatkowe Usługi Przetwarzania w Chmurze w odniesieniu do ofert IBM Trusteer Pinpoint Malware Detection i/lub IBM Trusteer Pinpoint Malware Detection II

a. Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do ofert IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition lub IBM Trusteer Pinpoint Malware Detection for Business Standard Edition lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business:
   - IBM Trusteer Pinpoint Carbon Copy for Business
   - IBM Trusteer Rapport Remediation for Business
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do ofert IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition lub IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition lub IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition lub IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition:
   - IBM Trusteer Pinpoint Carbon Copy for Retail
   - IBM Trusteer Rapport Remediation for Retail
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

Wsparcie premium jest dostępne dla konkretnych ofert określonych w niniejszym dokumencie. W przypadku dodatkowych powiązanych Usług Przetwarzania w Chmurze wymienionych w niniejszym paragrafie wymaganiem wstępnym jest posiadanie subskrypcji oferty IBM Trusteer Pinpoint Malware Detection for Business lub IBM Trusteer Pinpoint Malware Detection for Retail lub IBM Trusteer Pinpoint Malware Detection II for Business lub IBM Trusteer Pinpoint Malware Detection II for Retail.

1.1.5 Dodatkowe Usługi Przetwarzania w Chmurze dla ofert IBM Trusteer Pinpoint Criminal Detection i/lub IBM Trusteer Pinpoint Criminal Detection II

a. Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do ofert IBM Trusteer Pinpoint Criminal Detection for Business lub IBM Trusteer Pinpoint Criminal Detection II:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do ofert IBM Trusteer Pinpoint Criminal Detection for Retail i/lub IBM Trusteer Pinpoint Criminal Detection II for Retail:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Wsparcie premium jest dostępne dla konkretnych ofert określonych w niniejszym dokumencie.

W przypadku dodatkowych powiązanych Usług Przetwarzania w Chmurze wymienionych w niniejszym paragrafie wymaganiem wstępnym jest posiadanie subskrypcji oferty IBM Trusteer Pinpoint Criminal Detection for Business lub IBM Trusteer Pinpoint Criminal Detection for Retail lub IBM Trusteer Pinpoint Criminal Detection II for Business lub IBM Trusteer Pinpoint Criminal Detection II for Retail.

1.1.6 Dodatkowe Usługi Przetwarzania w Chmurze dla ofert IBM Trusteer Pinpoint Detect Standard i/lub IBM Trusteer Pinpoint Detect Premium i/lub IBM Security Pinpoint Detect Standard with access management integration i/lub IBM Security Detect Premium with access management integration

a. Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do ofert IBM Trusteer Detect Standard for Business i/lub IBM Trusteer Pinpoint Detect Premium for Business i/lub IBM Security Pinpoint Detect Standard with access management integration for Business i/lub IBM Security Detect Premium with access management integration for Business:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

b. Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do ofert IBM Trusteer Detect Standard for Retail i/lub IBM Trusteer Pinpoint Detect Premium for Retail i/lub IBM Security Pinpoint Detect Standard with access management integration for Retail i/lub IBM Security Detect Premium with access management integration for Retail:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

W przypadku dodatkowych powiązanych Usług Przetwarzania w Chmurze wymienionych w niniejszym paragrafie wymaganiem wstępnym jest posiadanie subskrypcji oferty IBM Trusteer Detect Standard lub IBM Trusteer Pinpoint Detect Premium lub IBM Security Pinpoint Detect Standard with access management integration lub IBM Security Detect Premium with access management integration.

1.1.7 Pozostałe dodatkowe Usługi Przetwarzania w Chmurze

Wszelkie dodatkowe subskrypcje Usług Przetwarzania w Chmurze, które dotyczą wymienionych powyżej subskrypcji podstawowych, lecz nie zostały wymienione w niniejszym dokumencie, nie stanowią aktualizacji i muszą zostać nabyte oddzielnie (bez względu na to, czy są obecnie dostępne, czy też znajdują się na etapie opracowywania).

1.2 Definicje

Posiadacz Konta – użytkownik końcowy z firmy Klienta, który zainstalował klienckie oprogramowanie pomocnicze, zaakceptował Umowę Licencyjną z Użytkownikiem Końcowym oraz co najmniej raz uwierzytelnił się w posiadanej przez Klienta Aplikacji Indywidualnej lub Biznesowej, w odniesieniu do której Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze.

Oprogramowanie Klienckie Posiadacza Konta – klienckie oprogramowanie pomocnicze IBM Trusteer Rapport lub klienckie oprogramowanie pomocnicze IBM Trusteer Mobile Browser lub dowolne inne klienckie oprogramowanie pomocnicze dostarczane w ramach subskrypcji niektórych Usług Przetwarzania w Chmurze i przeznaczone do zainstalowania na urządzeniu użytkownika końcowego.

Ekran powitalny Trusteer – ekran powitalny dostarczany Klientowi zależnie od dostępnych szablonów.

Strona Docelowa – strona udostępniana Klientowi przez IBM wraz ekranem powitalnym Klienta oraz Oprogramowaniem Klienckim Posiadacza Konta do pobrania.

2. Usługi Przetwarzania w Chmurze IBM Trusteer Rapport

2.1 Oferta IBM Trusteer Rapport for Retail i/lub IBM Trusteer Rapport for Business („Trusteer Rapport")

Oferta Trusteer Rapport zapewnia warstwę ochrony przed wyłudzaniem informacji i przed szkodliwym oprogramowaniem typu MitB (ang. Man in the Browser). Usługa ta wykorzystuje sieć kilkudziesięciu milionów punktów końcowych rozmieszczonych na wszystkich kontynentach, aby gromadzić dane analityczne o aktywnych atakach skierowanych przeciwko organizacjom z całego świata, a polegających na wyłudzaniu informacji lub posługiwaniu się szkodliwym oprogramowaniem. W usłudze IBM Trusteer Rapport zastosowano algorytmy analizy zachowania, których celem jest blokowanie ataków związanych z wyłudzaniem informacji oraz zapobieganie instalowaniu i działaniu poszczególnych odmian szkodliwego oprogramowania typu MitB.

Jednostką miary, według której nalicza się opłaty za niniejszą Usługę Przetwarzania w Chmurze, jest Uprawniony Uczestnik. W przypadku oferty biznesowej sprzedawane są pakiety obejmujące dziesięciu Uprawnionych Uczestników, a w przypadku oferty indywidualnej – stu Uprawnionych Uczestników.

Niniejsza oferta Usług Przetwarzania w Chmurze obejmuje:

a. Aplikację Trusteer Management Application („TMA”):

   Aplikacja TMA jest udostępniana w środowisku IBM Trusteer utrzymywanym w chmurze, za pośrednictwem którego Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może: (i) wyświetlać i pobierać niektóre raporty z danymi o zdarzeniach i oceny ryzyka oraz (ii) wyświetlać konfigurację klienckiego oprogramowania pomocniczego, które podlega bezpłatnej licencji udzielonej Uprawnionym Uczestnikom w firmie Klienta na warunkach Umowy Licencyjnej z Użytkownikiem Końcowym, jest udostępnione do pobrania na komputery desktop i inne urządzenia (komputery PC/MAC) Uprawnionych Uczestników i jest znane również pod nazwą pakiet oprogramowania Trusteer Rapport („Oprogramowanie Klienckie Posiadacza Konta”). Klient może prowadzić sprzedaż Oprogramowania Klienckiego Posiadacza Konta wyłącznie przy użyciu ekranu powitalnego Trusteer lub interfejsu API Rapport. Ponadto Klientowi nie wolno wykorzystywać Oprogramowania Klienckiego Posiadacza Konta do wewnętrznej działalności swojego przedsiębiorstwa ani na potrzeby użytkowania przez pracowników Klienta (z wyjątkiem użytku osobistego przez pracowników).

b. Skrypt WWW:

   Skrypt, który umożliwia dostęp do serwisu WWW w celu uzyskania dostępu do Usługi Przetwarzania w Chmurze lub korzystania z niej.

c. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane przez Oprogramowanie Klienckie Posiadacza Konta w wyniku elektronicznych interakcji Posiadacza Konta z Aplikacją Biznesową lub Indywidualną, w odniesieniu do której Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze. Otrzymane dane o zdarzeniach będą pochodziły z Oprogramowania Klienckiego Posiadacza Konta działającego na urządzeniach Uprawnionych Uczestników, którzy zaakceptowali warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnili się w Aplikacji Biznesowej lub Indywidualnej Klienta, przy czym stosowana przez Klienta konfiguracja musi obejmować gromadzenie ID użytkowników.

d. Ekran Powitalny Trusteer:

   Ekran Powitalny Trusteer to platforma marketingowa pozwalająca prezentować i sprzedawać Oprogramowanie Klienckie Posiadacza Konta Uprawnionym Uczestnikom uzyskującym dostęp do Aplikacji Biznesowych i/lub Indywidualnych, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze. Klient może dokonać wyboru spośród dostępnych szablonów Ekranu Powitalnego Trusteer. W ramach odrębnej umowy lub odrębnego zakresu prac można zlecić wykonanie ekranu powitalnego dostosowanego do określonych potrzeb.

Klient może zgodzić się na udostępnienie swoich znaków towarowych, logo lub ikon przeznaczonych do użytku w powiązaniu z Aplikacją TMA. Materiały te będą przeznaczone wyłącznie do używania wraz z Ekranem Powitalnym Trusteer oraz do wyświetlania w Oprogramowaniu Klienckim Posiadacza Konta lub na stronach docelowych udostępnianych przez IBM i w serwisie WWW IBM Trusteer. Każde użycie dostarczonych znaków towarowych, logo lub ikon będzie zgodne z uzasadnioną strategią IBM dotyczącą używania materiałów reklamowych i znaków towarowych.

Klient musi dokonać subskrypcji Usługi Przetwarzania w Chmurze IBM Trusteer Rapport Mandatory Service, jeśli chce zastosować dowolny rodzaj obowiązkowego instalowania Oprogramowania Klienckiego Posiadacza Konta.

Obowiązek zainstalowania Oprogramowania Klienckiego Posiadacza Konta zachodzi w szczególności w przypadku dowolnego rodzaju obowiązku zainstalowania realizowanego za pomocą jakichkolwiek mechanizmów lub środków, które bezpośrednio lub pośrednio zmuszają Uprawnionego Uczestnika do pobrania Oprogramowania Klienckiego Posiadacza Konta, lub w przypadku zastosowania metody, narzędzia, procedury, umowy lub mechanizmu, które nie zostały utworzone ani zatwierdzone przez IBM, a powstały w celu obejścia wymagań licencyjnych w stosunku do obowiązkowego instalowania Oprogramowania Klienckiego Posiadacza Konta.

2.2 Oferta IBM Trusteer Rapport II for Retail i/lub IBM Trusteer Rapport II for Business („Trusteer Rapport II")

Oparta na ofercie IBM Trusteer Rapport nowa Usługa Przetwarzania w Chmurze Trusteer Rapport II ułatwia standaryzowanie opłat związanych z ochroną wielu Aplikacji i zastępuje opłaty jednorazowe przy dodawaniu Aplikacji.

Oferta Trusteer Rapport II zapewnia warstwę ochrony przed wyłudzaniem informacji i przed szkodliwym oprogramowaniem typu MitB (ang. Man in the Browser). Usługa ta wykorzystuje sieć kilkudziesięciu milionów punktów końcowych rozmieszczonych na wszystkich kontynentach, aby gromadzić dane analityczne o aktywnych atakach skierowanych przeciwko organizacjom z całego świata, a polegających na wyłudzaniu informacji lub posługiwaniu się szkodliwym oprogramowaniem. W usłudze IBM Trusteer Rapport zastosowano algorytmy analizy zachowania, których celem jest blokowanie ataków związanych z wyłudzaniem informacji oraz zapobieganie instalowaniu i działaniu poszczególnych odmian szkodliwego oprogramowania typu MitB.

Jednostką miary, według której nalicza się opłaty za uprawnienia do niniejszej Usługi Przetwarzania w Chmurze, jest Uprawniony Uczestnik. W przypadku oferty biznesowej sprzedawane są pakiety obejmujące dziesięciu Uprawnionych Uczestników, a w przypadku oferty indywidualnej – stu Uprawnionych Uczestników.

Niniejsza oferta Usług Przetwarzania w Chmurze obejmuje:

a. Aplikację Trusteer Management Application („TMA"):

   Aplikacja TMA jest udostępniana w środowisku IBM Trusteer utrzymywanym w chmurze, za pośrednictwem którego Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może: (i) wyświetlać i pobierać niektóre raporty z danymi o zdarzeniach i oceny ryzyka oraz (ii) wyświetlać konfigurację klienckiego oprogramowania pomocniczego, które podlega bezpłatnej licencji udzielonej Uprawnionym Uczestnikom w firmie Klienta na warunkach Umowy Licencyjnej z Użytkownikiem Końcowym, jest udostępnione do pobrania na komputery desktop i inne urządzenia (komputery PC/MAC) Uprawnionych Uczestników i jest znane również pod nazwą pakiet oprogramowania Trusteer Rapport („Oprogramowanie Klienckie Posiadacza Konta"). Klient może prowadzić sprzedaż Oprogramowania Klienckiego Posiadacza Konta wyłącznie przy użyciu ekranu powitalnego Trusteer lub interfejsu API Rapport. Ponadto Klientowi nie wolno wykorzystywać Oprogramowania Klienckiego Posiadacza Konta do wewnętrznej działalności swojego przedsiębiorstwa ani na potrzeby użytkowania przez pracowników Klienta (z wyjątkiem użytku osobistego przez pracowników).

b. Skrypt WWW:

   Skrypt, który umożliwia dostęp do serwisu WWW w celu uzyskania dostępu do Usługi Przetwarzania w Chmurze lub korzystania z niej.

c. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane przez Oprogramowanie Klienckie Posiadacza Konta w wyniku elektronicznych interakcji Posiadacza Konta z Aplikacją Biznesową lub Indywidualną, w odniesieniu do której Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze. Otrzymane dane o zdarzeniach będą pochodziły z Oprogramowania Klienckiego Posiadacza Konta działającego na urządzeniach Uprawnionych Uczestników, którzy zaakceptowali warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnili się w Aplikacji Biznesowej lub Indywidualnej Klienta, przy czym stosowana przez Klienta konfiguracja musi obejmować gromadzenie ID użytkowników.

d. Ekran Powitalny Trusteer:

   Ekran Powitalny Trusteer to platforma marketingowa pozwalająca prezentować i sprzedawać Oprogramowanie Klienckie Posiadacza Konta Uprawnionym Uczestnikom uzyskującym dostęp do Aplikacji Biznesowych i/lub Indywidualnych, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze. Klient może dokonać wyboru spośród dostępnych szablonów Ekranu Powitalnego Trusteer. W ramach odrębnej umowy lub odrębnego zakresu prac można zlecić wykonanie ekranu powitalnego dostosowanego do określonych potrzeb.

Klient może zgodzić się na udostępnienie swoich znaków towarowych, logo lub ikon przeznaczonych do użytku w powiązaniu z Aplikacją TMA. Materiały te będą przeznaczone wyłącznie do używania wraz z Ekranem Powitalnym Trusteer oraz do wyświetlania w Oprogramowaniu Klienckim Posiadacza Konta lub na stronach docelowych udostępnianych przez IBM i w serwisie WWW IBM Trusteer. Każde użycie dostarczonych znaków towarowych, logo lub ikon będzie zgodne z uzasadnioną strategią IBM dotyczącą używania materiałów reklamowych i znaków towarowych.

Klient musi dokonać subskrypcji Usługi Przetwarzania w Chmurze IBM Trusteer Rapport Mandatory Service, jeśli chce zastosować dowolny rodzaj obowiązkowego instalowania Oprogramowania Klienckiego Posiadacza Konta.

Obowiązek zainstalowania Oprogramowania Klienckiego Posiadacza Konta zachodzi w szczególności w przypadku dowolnego rodzaju obowiązku zainstalowania realizowanego za pomocą jakichkolwiek mechanizmów lub środków, które bezpośrednio lub pośrednio zmuszają Uprawnionego Uczestnika do pobrania Oprogramowania Klienckiego Posiadacza Konta, lub w przypadku zastosowania metody, narzędzia, procedury, umowy lub mechanizmu, które nie zostały utworzone ani zatwierdzone przez IBM, a powstały w celu obejścia wymagań licencyjnych w stosunku do obowiązkowego instalowania Oprogramowania Klienckiego Posiadacza Konta.

Każda z ofert Trusteer Rapport II for Business i/lub Trusteer Rapport II for Retail obejmuje ochronę jednej Aplikacji. W odniesieniu do każdej kolejnej Aplikacji Klient powinien uzyskać uprawnienia objęte opcją IBM Trusteer Rapport Additional Applications.

2.3 Opcjonalne dodatkowe Usługi Przetwarzania w Chmurze dla ofert IBM Trusteer Rapport for Business i/lub IBM Trusteer Rapport for Retail i/lub IBM Trusteer Rapport II for Business i/lub IBM Trusteer Rapport II for Retail

W przypadku subskrypcji każdej z poniższych dodatkowych Usług Przetwarzania w Chmurze wymaganiem wstępnym jest subskrypcja Usług Przetwarzania w Chmurze IBM Trusteer Rapport lub IBM Trusteer Rapport II. Jeśli w nazwie Usługi Przetwarzania w Chmurze występuje określenie „for Business", to dodatkowe nabywane Usługi Przetwarzania w Chmurze również muszą być określone w ten sposób. Jeśli w nazwie Usługi Przetwarzania w Chmurze występuje określenie „for Retail", to dodatkowe nabywane Usługi Przetwarzania w Chmurze również muszą być określone w ten sposób. Klient będzie otrzymywać dane o zdarzeniach od Uprawnionych Uczestników korzystających z Oprogramowania Klienckiego Posiadacza Konta, którzy zaakceptowali warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnili się w jednej lub wielu Aplikacjach Biznesowych i/lub Indywidualnych Klienta, przy czym stosowana przez Klienta konfiguracja musi obejmować gromadzenie ID użytkowników.

2.3.1 Oferty IBM Trusteer Rapport Fraud Feeds for Business i/lub IBM Trusteer Rapport Fraud Feeds for Retail

W przypadku zasubskrybowania niniejszej dodatkowej Usługi Przetwarzania w Chmurze Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby wyświetlać, subskrybować i konfigurować dostarczanie generowanych przez Usługę Przetwarzania w Chmurze Trusteer Rapport kanałów informacyjnych na temat zagrożeń. Dane z kanałów informacyjnych mogą być przesyłane pocztą elektroniczną na określone adresy e-mail lub za pomocą protokołu SFTP jako pliki tekstowe.

2.3.2 Oferty IBM Trusteer Rapport Phishing Protection for Business i/lub IBM Trusteer Rapport Phishing Protection for Retail

Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach dotyczących wprowadzania danych uwierzytelniających w serwisach, które mogą być wykorzystywane przez oszustów lub co do których zachodzi podejrzenie, że służą one do wyłudzania informacji. Działające zgodnie z prawem aplikacje online (adresy URL) mogą być pomyłkowo oznaczane jako serwisy służące do wyłudzania informacji. Ponadto Usługa Przetwarzania w Chmurze może przesyłać Posiadaczom Konta alerty, w których serwis działający zgodnie z prawem jest określany jako serwis służący do wyłudzania informacji. W takich przypadkach Klient musi powiadamiać IBM o błędach, a IBM zobowiązuje się je naprawiać, przy czym jest to jedyne zadośćuczynienie, jakie przysługuje Klientowi z tytułu zgłoszonego błędu.

2.3.3 Oferty IBM Trusteer Rapport Mandatory Service for Business i/lub IBM Trusteer Rapport Mandatory Service for Retail

Klient może użyć instancji Ekranu Powitalnego Trusteer stanowiącego platformę marketingową, aby zlecić pobranie Oprogramowania Klienckiego Posiadacza Konta Uprawnionym Uczestnikom uzyskującym dostęp do Aplikacji Biznesowych i/lub Indywidualnych Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze.

W przypadku usługi IBM Security Rapport Mandatory Service for Business wymaganiem wstępnym jest posiadanie usługi IBM Trusteer Rapport Premium Support for Business.

W przypadku usługi IBM Security Rapport Mandatory Service for Retail wymaganiem wstępnym jest posiadanie usługi IBM Trusteer Rapport Premium Support for Retail.

Klient może zaimplementować dodatkową funkcjonalność usługi IBM Trusteer Rapport Mandatory Service tylko pod warunkiem, że została ona zamówiona i skonfigurowana pod kątem używania z Aplikacją Indywidualną lub Biznesową Klienta, w odniesieniu do której Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze.

2.3.4 Oferty IBM Trusteer Rapport Large Redeployment i/lub IBM Trusteer Rapport Small Redeployment

Klienci, którzy przydzielają Aplikacje bankowości elektronicznej do innych zadań w okresie świadczenia usługi i na skutek tego wymagają wprowadzenia zmian we wdrożonych usługach IBM Trusteer Rapport lub IBM Trusteer Rapport II, powinni nabyć Usługę Przetwarzania w Chmurze IBM Trusteer Rapport Redeployment.

Przyczyną przydzielenia do innych zadań może być zmiana domeny Aplikacji lub adresu URL hosta, wprowadzenie zmian do konfiguracji ekranu powitalnego lub przejście na nową platformę bankowości elektronicznej.

W sześciomiesięcznym okresie przejściowym związanym z przydzieleniem do innych zadań Klient jest uprawniony do używania dodatkowych Aplikacji, z których każda przypada na jedną wcześniej zasubskrybowaną Aplikację i działa niezależnie od niej.

Oferta IBM Trusteer Rapport Large Redeployment dotyczy środowisk obejmujących ponad 20 tys. użytkowników, natomiast oferta IBM Trusteer Rapport Small Redeployment dotyczy środowisk obejmujących 20 tys. lub mniej użytkowników.

2.3.5 Oferty IBM Trusteer Rapport Additional Applications for Business i/lub IBM Trusteer Rapport Additional Applications for Retail

Aby wdrożyć ofertę IBM Trusteer Rapport II for Business w odniesieniu do dowolnej dodatkowej Aplikacji Biznesowej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do Usługi Przetwarzania w Chmurze IBM Trusteer Rapport Additional Applications for Business. Aby wdrożyć ofertę IBM Trusteer Rapport II for Retail w odniesieniu do dowolnej dodatkowej Aplikacji Indywidualnej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do Usługi Przetwarzania w Chmurze IBM Trusteer Rapport Additional Applications for Retail.

3. Usługi Przetwarzania w Chmurze IBM Trusteer Pinpoint

IBM Trusteer Pinpoint to usługa przetwarzania w chmurze zaprojektowana z myślą o zapewnieniu kolejnej warstwy ochrony. Celem tej usługi jest wykrywanie szkodliwego oprogramowania, przypadków wyłudzania informacji i ataków polegających na przejęciu kontroli nad urządzeniem oraz ograniczanie skutków takich działań. Usługę Trusteer Pinpoint można zintegrować z Biznesowymi i/lub Indywidualnymi Aplikacjami Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony i procesów zapobiegania oszustwom dostępnych w ramach Usług Przetwarzania w Chmurze.

W skład niniejszej Usługi Przetwarzania w Chmurze wchodzi:

a. Aplikacja TMA:

   Aplikacja TMA jest udostępniania w środowisku IBM Trusteer utrzymywanym w chmurze, za pośrednictwem którego Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może: (i) wyświetlać i pobierać niektóre raporty z danymi o zdarzeniach i oceny ryzyka oraz (ii) wyświetlać, subskrybować i konfigurować dostarczanie generowanych w ramach usługi Pinpoint kanałów informacyjnych na temat zagrożeń.

b. Skrypt WWW i/lub interfejsy API:

   Narzędzia do zainstalowania w serwisie WWW w celu uzyskania dostępu do Usługi Przetwarzania w Chmurze lub korzystania z niej.

3.1 IBM Trusteer Pinpoint Malware Detection i IBM Trusteer Pinpoint Criminal Detection

W przypadku wykrycia szkodliwego oprogramowania w ramach Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint Malware Detection lub IBM Trusteer Pinpoint Malware Detection II bądź wykrycia przejęcia konta w ramach Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint Criminal Detection lub IBM Trusteer Pinpoint Criminal Detection II Klient jest zobowiązany postępować zgodnie z Podręcznikiem sprawdzonych procedur Pinpoint. Z Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint Malware Detection lub IBM Trusteer Pinpoint Malware Detection II lub IBM Trusteer Pinpoint Criminal Detection lub IBM Trusteer Pinpoint Criminal Detection II należy korzystać w taki sposób, aby nie wpływać na zachowanie Uprawnionych Uczestników tuż po wykryciu szkodliwego oprogramowania lub przejęcia konta, gdyż mogłoby to umożliwić innym osobom powiązanie czynności wykonanych przez Klienta z użyciem Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint (np. powiadomienia, komunikaty, blokowanie urządzeń lub blokowanie dostępu do Aplikacji Biznesowej i/lub Indywidualnej tuż po wykryciu szkodliwego oprogramowania lub przejęcia konta).

3.2 Oferty IBM Trusteer Pinpoint Criminal Detection for Business i/lub IBM Trusteer Pinpoint Criminal Detection for Retail

Wykrywanie podejrzanych działań polegających na przejmowaniu konta przez przeglądarki, które łączą się z Aplikacją Biznesową lub Indywidualną. Usługa ta działa bez oprogramowania klienckiego i wykorzystuje mechanizmy pozwalające wykryć identyfikator urządzenia, przypadki wyłudzania informacji oraz kradzież referencji dokonywaną przy użyciu szkodliwego oprogramowania. Usługi Przetwarzania w Chmurze IBM Trusteer Pinpoint Criminal Detection zapewniają kolejną warstwę ochrony, a ich celem jest wykrywanie prób przejęcia konta. Ponadto dostarczają one bezpośrednio Klientowi (za pośrednictwem przeglądarki rodzimej lub aplikacji Klienta dla urządzeń mobilnych) wyniki oceny ryzyka, jakiemu podlegają przeglądarki i urządzenia mobilne uzyskujące dostęp do Aplikacji Biznesowej lub Indywidualnej.

a. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji Uprawnionych Uczestników z jedną bądź wieloma Aplikacjami Biznesowymi i/lub Indywidualnymi Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze. Alternatywnie Klient ma do dyspozycji tryb dostarczania danych o zdarzeniach z wykorzystaniem interfejsu API zaplecza.

3.3 Oferty IBM Trusteer Pinpoint Criminal Detection II for Business i/lub IBM Trusteer Pinpoint Criminal Detection II for Retail

Oparta na ofercie IBM Trusteer Pinpoint Criminal Detection nowa oferta IBM Security Pinpoint Criminal Detection II ułatwia standaryzowanie opłat związanych z ochroną wielu Aplikacji i zastępuje opłaty jednorazowe przy dodawaniu Aplikacji.

Wykrywanie podejrzanych działań polegających na przejmowaniu konta przez przeglądarki, które łączą się z Aplikacją Biznesową lub Indywidualną. Usługa ta działa bez oprogramowania klienckiego i wykorzystuje mechanizmy pozwalające wykryć identyfikator urządzenia, przypadki wyłudzania informacji oraz kradzież referencji dokonywaną przy użyciu szkodliwego oprogramowania. Usługi Przetwarzania w Chmurze IBM Trusteer Pinpoint Criminal Detection II zapewniają kolejną warstwę ochrony, a ich celem jest wykrywanie prób przejęcia konta. Ponadto dostarczają one bezpośrednio Klientowi (za pośrednictwem przeglądarki rodzimej lub aplikacji Klienta dla urządzeń mobilnych) wyniki oceny ryzyka, jakiemu podlegają przeglądarki i urządzenia mobilne uzyskujące dostęp do Aplikacji Biznesowej lub Indywidualnej.

a. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji Uprawnionych Uczestników z jedną bądź wieloma Aplikacjami Biznesowymi i/lub Indywidualnymi Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze. Alternatywnie Klient ma do dyspozycji tryb dostarczania danych o zdarzeniach z wykorzystaniem interfejsu API zaplecza.

   Niniejsza Usługa Przetwarzania w Chmurze obejmuje ochronę jednej Aplikacji. W odniesieniu do każdej kolejnej Aplikacji Klient powinien uzyskać uprawnienia objęte opcją IBM Trusteer Pinpoint Criminal Detection Additional Applications.

3.4 Oferty IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition i/lub IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition i/lub IBM Trusteer Pinpoint Malware Detection for Business Standard Edition i/lub IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition

Wykrywanie przeglądarek łączących się z Aplikacją Biznesową i/lub Indywidualną, które są zawirusowane szkodliwym oprogramowaniem typu MitB ukierunkowanym na transakcje finansowe (mechanizm ten działa bez oprogramowania klienckiego). Usługi Przetwarzania w Chmurze IBM Trusteer Pinpoint Malware Detection zapewniają dodatkową warstwę ochrony, a ich celem jest wyposażenie organizacji w narzędzia, które pozwalają koncentrować się na procesach zapobiegania oszustwom opartym na szkodliwym oprogramowaniu. Jest to możliwe dzięki dostarczaniu Klientowi ocen i alertów dotyczących obecności szkodliwego oprogramowania typu MitB ukierunkowanego na transakcje finansowe.

a. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji Uprawnionych Uczestników z jedną bądź wieloma Aplikacjami Biznesowymi i/lub Indywidualnymi Klienta.

b. Wydanie Advanced Edition:

   Wydania Advanced Edition dla wersji Biznesowej i/lub Indywidualnej oferują dodatkową warstwę ochrony i wykrywania dostosowaną i skorygowaną pod kątem struktury Aplikacji Biznesowych i/lub Indywidualnych Klienta oraz przepływów między nimi. Ponadto wydania te można dostosowywać do konkretnych schematów zagrożeń, jakim podlega Klient, oraz wbudowywać w różne obszary Aplikacji Biznesowych i/lub Indywidualnych Klienta.

   Wydanie Advanced Edition jest oferowane Klientowi przy minimalnej wielkości zamówienia obejmującej 100 tys. Uprawnionych Uczestników wersji Indywidualnej lub 10 tys. Uprawnionych Uczestników wersji Biznesowej, czyli 1000 pakietów po 100 Uprawnionych Uczestników wersji Indywidualnej lub 1000 pakietów po 10 Uprawnionych Uczestników wersji Biznesowej.

c. Wydanie Standard Edition:

   Wydanie Standard Edition dla wersji Biznesowej lub wersji Indywidualnej to przeznaczone do szybkiego wdrożenia rozwiązanie, które zapewnia podstawową funkcjonalność Usługi Przetwarzania w Chmurze opisanej w niniejszym dokumencie.

3.5 Oferty IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business i/lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail i/lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business i/lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

Oparta na ofercie IBM Trusteer Pinpoint Malware Detection nowa oferta IBM Pinpoint Malware Detection II ułatwia standaryzowanie opłat związanych z ochroną wielu Aplikacji i zastępuje opłaty jednorazowe przy dodawaniu Aplikacji.

Wykrywanie przeglądarek łączących się z Aplikacją Biznesową i/lub Indywidualną, które są zawirusowane szkodliwym oprogramowaniem typu MitB ukierunkowanym na transakcje finansowe (mechanizm ten działa bez oprogramowania klienckiego). Usługi Przetwarzania w Chmurze IBM Trusteer Pinpoint Malware Detection zapewniają dodatkową warstwę ochrony, a ich celem jest wyposażenie organizacji w narzędzia, które pozwalają koncentrować się na procesach zapobiegania oszustwom opartym na szkodliwym oprogramowaniu. Jest to możliwe dzięki dostarczaniu Klientowi ocen i alertów dotyczących obecności szkodliwego oprogramowania typu MitB ukierunkowanego na transakcje finansowe.

a. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji Uprawnionych Uczestników z jedną bądź wieloma Aplikacjami Biznesowymi i/lub Indywidualnymi Klienta.

b. Wydanie Advanced Edition:

   Wydania Advanced Edition dla wersji Biznesowej i/lub Indywidualnej oferują dodatkową warstwę ochrony i wykrywania dostosowaną i skorygowaną pod kątem struktury Aplikacji Biznesowych i/lub Indywidualnych Klienta oraz przepływów między nimi. Ponadto wydania te można dostosowywać do

konkretnych schematów zagrożeń, jakim podlega Klient, oraz wbudowywać w różne obszary Aplikacji Biznesowych i/lub Indywidualnych Klienta.

Wydanie Advanced Edition jest oferowane Klientowi przy minimalnej wielkości zamówienia obejmującej 100 tys. Uprawnionych Uczestników wersji Indywidualnej lub 10 tys. Uprawnionych Uczestników wersji Biznesowej, czyli 1000 pakietów po 100 Uprawnionych Uczestników wersji Indywidualnej lub 1000 pakietów po 10 Uprawnionych Uczestników wersji Biznesowej.

c. Wydanie Standard Edition:

Wydanie Standard Edition dla wersji Biznesowej lub wersji Indywidualnej to przeznaczone do szybkiego wdrożenia rozwiązanie, które zapewnia podstawową funkcjonalność Usługi Przetwarzania w Chmurze opisanej w niniejszym dokumencie.

Niniejsza Usługa Przetwarzania w Chmurze obejmuje ochronę jednej Aplikacji. W odniesieniu do każdej kolejnej Aplikacji Klient musi uzyskać uprawnienia objęte opcją IBM Trusteer Pinpoint Malware Detection Additional Applications.

3.6 Opcjonalne dodatkowe Usługi Przetwarzania w Chmurze dla usług IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition i/lub IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition i/lub IBM Trusteer Pinpoint Malware Detection for Business Standard Edition i/lub IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition i/lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail i/lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business i/lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail i/lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- W przypadku Usługi Przetwarzania w Chmurze IBM Trusteer Rapport Remediation for Retail wymaganiem wstępnym jest subskrypcja oferty IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail lub IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- W przypadku Usługi Przetwarzania w Chmurze IBM Trusteer Rapport Remediation for Business wymaganiem wstępnym jest subskrypcja oferty IBM Trusteer Pinpoint Malware Detection Standard Edition for Business lub IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.
- W przypadku oferty IBM Trusteer Pinpoint Carbon Copy for Retail wymaganiem wstępnym jest subskrypcja oferty IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail lub IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- W przypadku oferty IBM Trusteer Pinpoint Carbon Copy for Business wymaganiem wstępnym jest subskrypcja oferty IBM Trusteer Pinpoint Malware Detection Standard Edition for Business lub IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

3.6.1 Oferty IBM Trusteer Pinpoint Carbon Copy for Business i/lub IBM Trusteer Pinpoint Carbon Copy for Retail

Oferty IBM Trusteer Pinpoint Carbon Copy zostały zaprojektowane z myślą o zapewnieniu kolejnej warstwy ochrony oraz usługi monitorowania. Takie rozwiązanie pomaga ustalić, czy bezpieczeństwo referencji Uprawnionego Uczestnika zostało naruszone poprzez ataki mające na celu wyłudzanie informacji w Aplikacjach Indywidualnych lub Biznesowych Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach ofert Usług Przetwarzania w Chmurze.

3.6.2 Oferty IBM Trusteer Rapport Remediation for Retail i/lub IBM Trusteer Rapport Remediation for Business

Celem usługi IBM Trusteer Rapport Remediation for Retail jest zbadanie, zneutralizowanie, zablokowanie i usunięcie szkodliwego oprogramowania typu MitB z zawirusowanych urządzeń (komputerów PC/MAC) Uprawnionych Uczestników w firmie Klienta, którzy doraźnie uzyskują dostęp do Aplikacji Klienta. Wykryte przypadki zawirusowania szkodliwym oprogramowaniem są uwzględniane w danych o

zdarzeniach dostarczanych przez usługę IBM Trusteer Pinpoint Malware Detection. Klient musi posiadać aktualną subskrypcję usługi IBM Trusteer Pinpoint Malware Detection lub IBM Trusteer Pinpoint Malware Detection II faktycznie uruchomionej w ramach Aplikacji Klienta. Klient może korzystać z niniejszej oferty Usług Przetwarzania w Chmurze wyłącznie w powiązaniu z Uprawnionymi Uczestnikami uzyskującymi dostęp do Aplikacji Klienta. Ponadto niniejsza Usługa Przetwarzania w Chmurze może być używana tylko jako narzędzie, którego celem jest doraźne zbadanie i naprawienie konkretnego zawirusowanego urządzenia (komputera PC/MAC). Usługa IBM Trusteer Rapport Remediation musi działać na urządzeniu Uprawnionego Uczestnika (komputerze PC/MAC), którego dotyczy zagrożenie. Ponadto Uprawniony Uczestnik, którego dotyczy zagrożenie, musi zaakceptować warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnić się w jednej lub wielu Aplikacjach Klienta, przy czym stosowana przez Klienta konfiguracja musi obejmować gromadzenie ID użytkowników. W celu uniknięcia wątpliwości zaznacza się, że niniejsza oferta Usług Przetwarzania w Chmurze nie obejmuje prawa do używania Ekranu Powitalnego Trusteer i/lub do promowania Oprogramowania Klienckiego Posiadacza Konta jakimikolwiek innymi metodami w całej grupie Uprawnionych Uczestników z firmy Klienta.

3.6.3 IBM Trusteer Pinpoint Malware Detection Redeployment

Klienci, którzy przydzielają Aplikacje bankowości elektronicznej do innych zadań w okresie świadczenia usługi i na skutek tego wymagają wprowadzenia zmian we wdrożonych usługach IBM Trusteer Pinpoint Malware Detection i/lub IBM Trusteer Pinpoint Malware Detection II, powinni nabyć usługę IBM Trusteer Pinpoint Malware Detection Redeployment.

Przyczyną przydzielenia do innych zadań może być zmiana domeny Aplikacji lub adresu URL hosta, przekształcanie Aplikacji obsługi elektronicznej pod kątem nowej technologii, przejście na nową platformę bankowości elektronicznej lub dodanie nowego strumienia logowania do istniejącej Aplikacji.

W sześciomiesięcznym okresie przejściowym związanym z przydzieleniem do innych zadań Klient jest uprawniony do używania dodatkowych Aplikacji, z których każda przypada na jedną wcześniej zasubskrybowaną Aplikację i działa niezależnie od niej.

3.6.4 Oferty IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail i/lub IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

Aby wdrożyć ofertę IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business w odniesieniu do dowolnej dodatkowej Aplikacji Biznesowej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Malware Detection Additional Applications for Business. Aby wdrożyć ofertę IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail w odniesieniu do dowolnej dodatkowej Aplikacji Indywidualnej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.

3.7 Opcjonalne dodatkowe Usługi Przetwarzania w Chmurze dla usług IBM Trusteer Pinpoint Criminal Detection for Business i/lub IBM Trusteer Pinpoint Criminal Detection for Retail i/lub for IBM Trusteer Pinpoint Criminal Detection II for Business i/lub IBM Trusteer Pinpoint Criminal Detection II for Retail

3.7.1 IBM Trusteer Pinpoint Criminal Detection Redeployment

Klienci, którzy przydzielają Aplikacje bankowości elektronicznej do innych zadań w okresie świadczenia usługi i na skutek tego wymagają wprowadzenia zmian we wdrożonej Usłudze Przetwarzania w Chmurze IBM Trusteer Pinpoint Criminal Detection, powinni nabyć usługę IBM Trusteer Pinpoint Criminal Detection Redeployment.

Przyczyną przydzielenia do innych zadań może być zmiana domeny Aplikacji lub adresu URL hosta, przekształcanie Aplikacji obsługi elektronicznej pod kątem nowej technologii, przejście na nową platformę bankowości elektronicznej lub dodanie nowego strumienia logowania do istniejącej Aplikacji.

W sześciomiesięcznym okresie przejściowym związanym z przydzieleniem do innych zadań Klient jest uprawniony do używania dodatkowych Aplikacji, z których każda przypada na jedną wcześniej zasubskrybowaną Aplikację i działa niezależnie od niej.

3.7.2 Oferty IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business i/lub IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Aby wdrożyć ofertę IBM Trusteer Pinpoint Criminal Detection II for Business w odniesieniu do dowolnej dodatkowej Aplikacji Biznesowej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM

Trusteer Pinpoint Criminal Detection Additional Applications for Business. Aby wdrożyć ofertę IBM Trusteer Pinpoint Criminal Detection II for Retail w odniesieniu do dowolnej dodatkowej Aplikacji Indywidualnej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail.

4. IBM Trusteer Fraud Protection Suite

Pakiet IBM Trusteer Fraud Protection („Pakiet") to kolekcja usług przetwarzania w chmurze, które zapewniają warstwę ochrony przed oszustwami. Można je zintegrować z dodatkowymi produktami IBM, aby uzyskać rozwiązanie do zarządzania całym cyklem życia. W ramach Pakietu dostępne są następujące usługi przetwarzania w chmurze:

- Usługa IBM Trusteer Pinpoint Detect, która umożliwia wykrywanie szkodliwego oprogramowania, przypadków wyłudzania informacji i ataków polegających na przejęciu kontroli nad urządzeniem oraz ograniczanie skutków takich działań. Usługę Trusteer Pinpoint Detect można zintegrować z Biznesowymi i/lub Indywidualnymi Aplikacjami Klienta, w odniesieniu do których Klient dokonał subskrypcji Usługi Przetwarzania w Chmurze i procesów zapobiegania oszustwom.
- Usługa IBM Trusteer Rapport for Mitigation, która umożliwia naprawę i ochronę zainfekowanych punktów końcowych.

W skład niniejszej Usługi Przetwarzania w Chmurze wchodzą następujące elementy:

a. Aplikacja TMA:

   Aplikacja TMA jest udostępniania w środowisku IBM Trusteer utrzymywanym w chmurze, za pośrednictwem którego Klient (oraz nieograniczona liczba upoważnionych członków personelu) może: (i) otrzymywać raporty z danymi o zdarzeniach i oceny ryzyka oraz (ii) wyświetlać, konfigurować i ustalać strategie bezpieczeństwa oraz strategie związane z raportowaniem danych o zdarzeniach.

b. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji Uprawnionych Uczestników z jedną bądź wieloma Aplikacjami Biznesowymi i/lub Indywidualnymi Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usługi Przetwarzania w Chmurze. Alternatywnie Klient ma do dyspozycji tryb dostarczania danych o zdarzeniach z wykorzystaniem interfejsu API zaplecza.

c. Skrypt WWW i/lub interfejsy API:

   Narzędzia do zainstalowania w serwisie WWW w celu uzyskania dostępu do Usługi Przetwarzania w Chmurze lub korzystania z niej.

Sprawdzone procedury dotyczące rozwiązań Pinpoint

W przypadku wykrycia szkodliwego oprogramowania lub wykrycia przypadku przejęcia konta Klient jest zobowiązany postępować zgodnie z „Podręcznikiem sprawdzonych procedur dotyczących rozwiązań Pinpoint". Z Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint Detect należy korzystać w taki sposób, aby nie wpływać w żaden sposób na zachowanie Uprawnionych Uczestników tuż po wykryciu szkodliwego oprogramowania lub przejęcia konta, gdyż mogłoby to umożliwić innym osobom powiązanie czynności wykonanych przez Klienta z użyciem usług IBM Trusteer Pinpoint (dotyczy to np. powiadomień, komunikatów, blokowania urządzeń lub blokowania dostępu do Aplikacji Biznesowej i/lub Aplikacji Indywidualnej tuż po wykryciu szkodliwego oprogramowania lub przejęcia konta).

4.1 Oferty IBM Trusteer Pinpoint Detect Standard for Business i/lub IBM Trusteer Pinpoint Detect Standard for Retail

Ta Usługa Przetwarzania w Chmurze łączy usługi IBM Trusteer Pinpoint Criminal Detection oraz IBM Trusteer Pinpoint Malware Detection, oferując jedno, skonsolidowane rozwiązanie.

Rozwiązanie to umożliwia wykrywanie szkodliwego oprogramowania i/lub podejrzanych działań związanych z przejmowaniem kont w przeglądarkach, które łączą się z Aplikacją Biznesową lub Aplikacją Indywidualną. Wykrywanie odbywa się bez użycia oprogramowania klienckiego, z wykorzystaniem mechanizmów pozwalających wykryć identyfikator urządzenia oraz przypadki wyłudzania informacji i kradzieży danych uwierzytelniających przez szkodliwe oprogramowanie. Usługi IBM Trusteer Pinpoint zapewniają kolejną warstwę ochrony. Ich celem jest wykrywanie prób przejęcia konta oraz dostarczanie bezpośrednio Klientowi (za pośrednictwem rodzimej przeglądarki lub aplikacji Klienta dla urządzeń

mobilnych) wyników analizy ryzyka dotyczącej przeglądarek i urządzeń mobilnych uzyskujących dostęp do Aplikacji Biznesowej lub Aplikacji Indywidualnej.

W ramach tej Usługi Przetwarzania w Chmurze jest świadczone wsparcie standardowe (zgodnie z definicją podaną poniżej w paragrafie Wsparcie techniczne). Aby uzyskać wsparcie na poziomie Premium, Klient musi nabyć usługę Detect Premium.

Niniejsza Usługa Przetwarzania w Chmurze obejmuje ochronę jednej Aplikacji. W odniesieniu do każdej kolejnej Aplikacji Klient powinien uzyskać uprawnienia objęte opcją IBM Trusteer Pinpoint Detect Standard Additional Applications.

4.2 Oferty IBM Trusteer Pinpoint Detect Premium for Business i/lub IBM Trusteer Pinpoint Detect Premium for Retail

Niniejsza Usługa Przetwarzania w Chmurze łączy usługi IBM Trusteer Pinpoint Criminal Detection oraz IBM Trusteer Pinpoint Malware Detection, oferując pojedyncze, łatwe w integracji, skonsolidowane rozwiązanie o rozszerzonym zakresie funkcji i usług, takich jak rozszerzone usługi wdrażania i konfigurowania, dostosowane strategie bezpieczeństwa, usługi badania incydentów itp.

Niniejsza Usługa Przetwarzania w Chmurze obejmuje ochronę jednej Aplikacji. W odniesieniu do każdej kolejnej Aplikacji Klient powinien uzyskać uprawnienia objęte opcją IBM Trusteer Pinpoint Detect Premium Additional Applications.

Ta Usługa Przetwarzania w Chmurze obejmuje wsparcie na poziomie Premium.

4.3 Oferty IBM Trusteer Pinpoint Detect Standard with access management integration for Business i/lub IBM Trusteer Pinpoint Detect Standard with access management integration for Retail

Usługa Przetwarzania w Chmurze IBM Trusteer Pinpoint Detect Standard with access management integration zawiera funkcjonalność usługi IBM Security Pinpoint Detect Standard opisanej szczegółowo w punkcie 4.1 powyżej.

Z usługi IBM Trusteer Pinpoint Detect Standard with access management integration można korzystać, jeśli została ona nabyta wraz z systemami zarządzania dostępem, takimi jak IBM Security Access Management („ISAM”). W przypadku zakupu z systemem ISAM obie oferty muszą zostać aktywowane. Niniejsza oferta obejmuje opcję integracji z systemem zarządzania dostępem, natomiast nie obejmuje uprawnień do tego systemu.

Usługa obejmuje ochronę jednej Aplikacji. W odniesieniu do każdej kolejnej Aplikacji Klient powinien uzyskać uprawnienia objęte opcją IBM Trusteer Pinpoint Detect Standard Additional Applications.

W ramach tej Usługi Przetwarzania w Chmurze jest świadczone wsparcie standardowe (zgodnie z definicją podaną w paragrafie Wsparcie techniczne). Oferty IBM Trusteer Pinpoint Detect Premium with access management integration for Business i/lub IBM Trusteer Pinpoint Detect Premium with access management integration for Retail

Usługa Przetwarzania w Chmurze IBM Trusteer Pinpoint Detect Premium with access management integration zawiera funkcjonalność usługi IBM Security Pinpoint Detect Premium opisanej szczegółowo w punkcie 4.2 powyżej oraz opcję integracji z systemem zarządzania dostępem.

Z usługi Trusteer Pinpoint Detect Premium with access management integration można korzystać, jeśli została ona nabyta wraz z systemami zarządzania dostępem, takimi jak IBM Security Access Management („ISAM”). W przypadku zakupu z systemem ISAM obie oferty muszą zostać aktywowane. Niniejsza Usługa Przetwarzania w Chmurze obejmuje opcję integracji z systemem zarządzania dostępem, natomiast nie obejmuje uprawnień do tego systemu.

Niniejsza Usługa Przetwarzania w Chmurze obejmuje ochronę jednej Aplikacji. W odniesieniu do każdej kolejnej Aplikacji Klient powinien uzyskać uprawnienia objęte opcją IBM Trusteer Pinpoint Detect Premium Additional Applications.

Usługa obejmuje wsparcie Premium.

4.4 Usługi opcjonalne związane z usługami IBM Trusteer Pinpoint Detect Standard i/lub IBM Trusteer Pinpoint Detect Premium

W przypadku Usług Przetwarzania w Chmurze wymienionych w tym paragrafie wymaganiem wstępnym jest uzyskanie uprawnienia do usługi IBM Trusteer Pinpoint Detect Premium for Retail albo IBM Trusteer Pinpoint Detect Standard for Retail.

4.5 Oferty IBM Trusteer Rapport for Mitigation for Retail i/lub IBM Trusteer Rapport for Mitigation for Business

Usługa IBM Trusteer Rapport for Mitigation służy do badania, neutralizowania, blokowania i usuwania szkodliwego oprogramowania z zainfekowanych urządzeń (komputerów PC/MAC) Uprawnionych Uczestników w firmie Klienta, którzy uzyskują doraźnie dostęp do Aplikacji Indywidualnej Klienta. Dotyczy to przypadków zainfekowania szkodliwym oprogramowaniem wykrywanych na podstawie danych o zdarzeniach dostarczanych przez usługę IBM Trusteer Pinpoint Detect Premium lub IBM Trusteer Pinpoint Detect Standard. Klient musi posiadać bieżącą subskrypcję usługi IBM Trusteer Pinpoint Detect Premium lub IBM Trusteer Pinpoint Detect Standard, działającą w danym momencie w ramach Aplikacji Indywidualnej Klienta. Klient może korzystać z niniejszej Usługi Przetwarzania w Chmurze wyłącznie w powiązaniu z Uprawnionymi Uczestnikami uzyskującymi dostęp do Aplikacji Indywidualnej Klienta. Ponadto niniejsza Usługa Przetwarzania w Chmurze może być używana tylko jako narzędzie, którego celem jest doraźne zbadanie i naprawienie konkretnego zawirusowanego urządzenia (komputera PC/MAC). Usługa IBM Trusteer Rapport for Mitigation for Retail musi być faktycznie uruchomiona na urządzeniu Uprawnionego Uczestnika (komputerze PC/MAC), którego dotyczy zagrożenie. Ponadto Uprawniony Uczestnik, którego dotyczy zagrożenie, musi zaakceptować warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnić się w jednej lub kilku Aplikacjach Indywidualnych Klienta, a stosowana przez Klienta konfiguracja musi obejmować gromadzenie identyfikatorów użytkowników. W celu uniknięcia wątpliwości zaznacza się, że niniejsza Usługa Przetwarzania w Chmurze nie obejmuje prawa do używania Ekranu Powitalnego Trusteer i/lub do promowania Oprogramowania Klienckiego Posiadacza Konta jakimikolwiek innymi metodami w całej grupie Uprawnionych Uczestników z firmy Klienta.

4.5.1 Oferty IBM Trusteer Pinpoint Detect Standard Additional Applications for Business i/lub IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail i/lub IBM Trusteer Pinpoint Detect Premium Additional Applications for Business i/lub IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

Aby wdrożyć ofertę IBM Trusteer Pinpoint Standard for Business w odniesieniu do dowolnej dodatkowej Aplikacji Biznesowej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

Aby wdrożyć ofertę IBM Trusteer Pinpoint Standard for Retail w odniesieniu do dowolnej dodatkowej Aplikacji Indywidualnej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.

Aby wdrożyć ofertę IBM Trusteer Pinpoint Premium for Business w odniesieniu do dowolnej dodatkowej Aplikacji Biznesowej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

Aby wdrożyć ofertę IBM Trusteer Pinpoint Premium for Retail w odniesieniu do dowolnej dodatkowej Aplikacji Indywidualnej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.

4.5.2 Oferty IBM Trusteer Pinpoint Detect Standard Redeployment i/lub IBM Trusteer Pinpoint Detect Premium Redeployment

Klienci, którzy przydzielają Aplikacje bankowości elektronicznej do innych zadań w okresie świadczenia usługi i na skutek tego wymagają wprowadzenia zmian we wdrożonych usługach IBM Trusteer Pinpoint Detect, powinni nabyć usługę IBM Trusteer Pinpoint Detect Redeployment.

Przyczyną przydzielenia do innych zadań może być zmiana domeny Aplikacji lub adresu URL hosta, przekształcanie Aplikacji obsługi elektronicznej pod kątem nowej technologii, przejście na nową platformę bankowości elektronicznej lub dodanie nowego strumienia logowania do istniejącej Aplikacji.

W sześciomiesięcznym okresie przejściowym związanym z przydzieleniem do innych zadań Klient jest uprawniony do używania dodatkowych Aplikacji, z których każda przypada na jedną wcześniej zasubskrybowaną Aplikację i działa niezależnie od niej.

5. Usługi Przetwarzania w Chmurze IBM Trusteer Mobile

5.1 Oferty IBM Trusteer Mobile Browser for Business i/lub IBM Trusteer Mobile Browser for Retail

Oferta IBM Trusteer Mobile Browser została zaprojektowana z myślą o wprowadzeniu kolejnej warstwy ochrony, a jej celem jest zapewnienie bezpieczeństwa podczas dostępu uzyskiwanego za pośrednictwem

mobilnych urządzeń Uprawnionych Uczestników do Aplikacji Indywidualnych lub Biznesowych Klienta, w odniesieniu do których Klient dokonał subskrypcji Usług Przetwarzania w Chmurze w zakresie ochrony, oceny ryzyka dotyczącego urządzeń mobilnych oraz zabezpieczenia przed wyłudzaniem informacji. Mechanizm wykrywania bezpiecznych sieci Wi-Fi jest dostępny tylko dla platform z systemem operacyjnym Android. Niniejsza Usługa Przetwarzania w Chmurze dla urządzeń mobilnych obejmuje telefony komórkowe i tablety, lecz nie obejmuje laptopów typu PC i Mac.

Dzięki Aplikacji TMA Klient może otrzymywać dane o zdarzeniach, analizy i informacje statystyczne dotyczące Urządzeń będących w posiadaniu Uprawnionych Uczestników, którzy: (i) pobrali Oprogramowanie Klienckie Posiadacza Konta, czyli aplikację podlegającą bezpłatnej publicznej licencji na warunkach Umowy Licencyjnej z Użytkownikiem Końcowym, udostępnianą do pobrania na urządzenia mobilne Uprawnionych Uczestników, oraz (ii) zaakceptowali Umowę Licencyjną z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnili się w Aplikacjach Indywidualnych lub Biznesowych Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze. Klient może prowadzić sprzedaż Oprogramowania Klienckiego Posiadacza Konta wyłącznie przy użyciu Ekranu Powitalnego Trusteer. Ponadto Klientowi nie wolno wykorzystywać Oprogramowania Klienckiego Posiadacza Konta do wewnętrznej działalności swojego przedsiębiorstwa.

a. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji urządzeń mobilnych z Aplikacjami Indywidualnymi lub Biznesowymi Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze.

b. Ekran Powitalny Trusteer:

   Ekran Powitalny Trusteer to platforma marketingowa pozwalająca prezentować i sprzedawać Oprogramowanie Klienckie Posiadacza Konta Uprawnionym Uczestnikom uzyskującym dostęp do Aplikacji Biznesowych i/lub Indywidualnych, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze. Klient może dokonać wyboru spośród dostępnych szablonów Ekranu Powitalnego Trusteer („Szablon Ekranu Powitalnego”). W ramach odrębnej umowy lub odrębnego zakresu prac można zlecić wykonanie ekranu powitalnego dostosowanego do określonych potrzeb.

Klient może zgodzić się na udostępnienie swoich znaków towarowych, logo lub ikon przeznaczonych do użytku w powiązaniu z Aplikacją TMA. Materiały te będą przeznaczone wyłącznie do używania wraz z Ekranem Powitalnym Trusteer oraz do wyświetlania w Oprogramowaniu Klienckim Posiadacza Konta, na stronach docelowych udostępnianych przez IBM, albo w serwisie WWW IBM Trusteer. Każde użycie dostarczonych znaków towarowych, logo lub ikon będzie zgodne z uzasadnioną strategią IBM dotyczącą używania materiałów reklamowych i znaków towarowych.

5.2 Oferty IBM Trusteer Mobile SDK for Business i/lub IBM Trusteer Mobile SDK for Retail

Usługi Przetwarzania w Chmurze IBM Trusteer Mobile SDK zostały zaprojektowane z myślą o wprowadzeniu kolejnej warstwy ochrony, tak aby zapewnić bezpieczny dostęp w sieci WWW do Aplikacji Biznesowych i/lub Indywidualnych Klienta, w odniesieniu do których Klient dokonał subskrypcji Usług Przetwarzania w Chmurze w zakresie ochrony, oceny ryzyka dotyczącego urządzeń mobilnych oraz zabezpieczenia przed wyłudzaniem informacji metodą pharming. Mechanizm wykrywania bezpiecznych sieci Wi-Fi jest dostępny tylko dla platform z systemem operacyjnym Android.

Usługi Przetwarzania w Chmurze IBM Trusteer Mobile SDK zawierają prawnie zastrzeżony pakiet narzędzi do tworzenia oprogramowania dla urządzeń mobilnych („SDK”). Jest to pakiet oprogramowania zawierający dokumentację, prawnie zastrzeżone biblioteki programistyczne oraz inne powiązane pliki i elementy określane nazwą „biblioteka IBM Trusteer dla urządzeń mobilnych”, a także „komponent środowiska wykonawczego” lub „Element Podlegający Redystrybucji”, czyli prawnie zastrzeżony kod wygenerowany przez pakiet IBM Trusteer Mobile SDK, który można osadzać w autonomicznych, chronionych aplikacjach Klienta dla urządzeń mobilnych z systemem operacyjnym iOS lub Android (oraz integrować z takimi aplikacjami), w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze („Zintegrowana przez Klienta Aplikacja dla Urządzeń Mobilnych”).

Oferta IBM Trusteer Mobile SDK for Retail jest dostępna w pakietach po 100 Uprawnionych Uczestników lub w pakietach po 100 Urządzeń Klienckich, natomiast oferta IBM Trusteer Mobile SDK for Business jest dostępna w pakietach po 10 Uprawnionych Uczestników lub w pakietach po 10 Urządzeń Klienckich.

Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może uzyskiwać za pośrednictwem aplikacji TMA dane o zdarzeniach i oceny trendów ryzyka. Klient może odbierać za pośrednictwem Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych informacje dotyczące analizy ryzyka i urządzeń mobilnych w odniesieniu do urządzeń Uprawnionych Uczestników, którzy pobrali Zintegrowaną przez Klienta Aplikację dla Urządzeń Mobilnych. Pozwala to Klientowi opracować strategię zapobiegania oszustwom w celu egzekwowania działań zmierzających do ograniczenia skutków takiego ryzyka. Na potrzeby niniejszej oferty pojęcie „urządzenia mobilne" obejmuje wyłącznie obsługiwane telefony komórkowe i tablety, natomiast nie obejmuje komputerów typu PC lub MAC.

Klient może:

a. wykorzystywać pakiet IBM Trusteer Mobile SDK do użytku wewnętrznego, wyłącznie na potrzeby opracowywania Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych;

b. osadzić Element Podlegający Redystrybucji (wyłącznie w postaci kodu wynikowego) w Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych, tak aby stanowił on integralną, nieodłączną część tej aplikacji. Każdy fragment Elementu Podlegającego Redystrybucji zmodyfikowany lub wbudowany zgodnie z niniejszą licencją będzie podlegał niniejszemu Opisowi Usług;

c. prowadzić sprzedaż i dystrybucję Elementu Podlegającego Redystrybucji przeznaczonego do pobrania na urządzenia mobilne Uprawnionych Uczestników lub do pobrania przez posiadacza Urządzenia Klienckiego, pod warunkiem że:

   - Z wyjątkiem przypadków wyraźnie dozwolonych w niniejszej Umowie, Klient nie ma prawa (1) używać, kopiować, modyfikować ani dystrybuować pakietu SDK; (2) deasemblować, dekompilować ani przeprowadzać translacji pakietu SDK innymi metodami (z wyjątkiem przypadków wyraźnie dozwolonych przez przepisy prawa bez możliwości ich wyłączenia w ramach umowy); (3) udzielać dalszych licencji, wypożyczać ani wydzierżawiać pakietu SDK; (4) usuwać żadnych plików z informacjami o prawach autorskich ani plików informacyjnych zawartych w Elemencie Podlegającym Redystrybucji; (5) używać tej samej nazwy ścieżki, która została użyta w oryginalnych plikach/modułach Elementu Podlegającego Redystrybucji; (6) używać nazw ani znaków towarowych IBM oraz jego licencjodawców i dystrybutorów w powiązaniu ze sprzedażą Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych bez uprzedniej pisemnej zgody IBM lub odpowiedniego licencjodawcy bądź dystrybutora.
   - Element Podlegający Redystrybucji musi pozostać nierozłącznie zintegrowany ze Zintegrowaną przez Klienta Aplikacją dla Urządzeń Mobilnych; ponadto musi mieć wyłącznie postać kodu wynikowego i spełniać wszystkie wytyczne, instrukcje i specyfikacje zawarte w pakiecie SDK i jego dokumentacji. Umowa licencyjna z użytkownikiem końcowym Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych musi zawierać zapis informujący użytkownika końcowego, że Elementu Podlegającego Redystrybucji nie wolno i) używać do jakichkolwiek innych celów niż umożliwienie działania Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych, ii) kopiować (z wyjątkiem tworzenia kopii zapasowej), iii) przeznaczać do dalszej dystrybucji lub przekazywać, iv) deasemblować, dekompilować ani w inny sposób poddawać translacji, o ile nie zezwalają na to przepisy prawa bez możliwości ich wyłączenia w ramach umowy. Umowa licencyjna zawarta przez Klienta musi chronić prawa IBM w stopniu co najmniej równoważnym warunkom niniejszej Umowy.
   - Pakiet SDK może być wdrażany tylko w ramach wewnętrznych testów programistycznych i jednostkowych prowadzonych przez Klienta na urządzeniach mobilnych określonych przez Klienta jako testowe. Klient nie jest upoważniony do używania pakietu SDK w celu przetwarzania lub symulowania obciążeń produkcyjnych ani testowania skalowalności jakiegokolwiek kodu, programu lub systemu. Klient nie jest uprawniony do używania jakiejkolwiek części pakietu SDK do innych celów.

Klient ponosi wyłączną odpowiedzialność za tworzenie i testowanie Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych oraz za świadczenie wsparcia dla niej. Klient odpowiada za świadczenie pełnego zakresu usług pomocy technicznej w odniesieniu do Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych oraz wszelkich modyfikacji w Elemencie Podlegającym Redystrybucji, wprowadzonych przez Klienta w sposób dozwolony w niniejszym dokumencie.

Klient może zainstalować Elementy Podlegające Redystrybucji oraz pakiet IBM Security Mobile SDK oraz używać ich wyłącznie po to, aby ułatwić sobie korzystanie z Usług Przetwarzania w Chmurze.

IBM przetestował przykładowe aplikacje utworzone za pomocą narzędzi mobilnych udostępnionych w pakiecie IBM Trusteer Mobile SDK („Narzędzia Mobilne"), aby ustalić, czy aplikacje te będą się poprawnie uruchamiały na niektórych wersjach mobilnych platform systemów operacyjnych firm Apple (iOS), Google (Android) oraz innych dostawców (zwanych łącznie „Mobilnymi Platformami Systemów Operacyjnych"). Mobilne Platformy Systemów Operacyjnych są jednak udostępniane przez osoby trzecie, nie podlegają kontroli IBM i mogą ulec zmianie bez powiadamiania IBM. Dlatego bez względu na stanowiące inaczej warunki IBM nie gwarantuje, że jakiekolwiek aplikacje lub inne produkty utworzone za pomocą Narzędzi Mobilnych będą się poprawnie uruchamiać na jakichkolwiek Mobilnych Platformach Systemów Operacyjnych lub urządzeniach mobilnych, ani też że będą z nimi współdziałać lub że będą z nimi zgodne.

Komponenty Źródłowe i Materiały Przykładowe – usługa IBM Trusteer Mobile SDK może zawierać pewne komponenty w formie kodu źródłowego (zwane dalej „Komponentami Źródłowymi") i inne materiały określane jako Materiały Przykładowe. Klient ma prawo kopiować i modyfikować Komponenty Źródłowe i Materiały Przykładowe wyłącznie do użytku wewnętrznego pod warunkiem, że takie użycie materiałów jest objęte uprawnieniami licencyjnymi określonymi niniejszą Umową, jednak z zastrzeżeniem, że Klient nie może zmieniać ani usuwać jakichkolwiek informacji i uwag dotyczących praw autorskich zawartych w Komponentach Źródłowych lub Materiałach Przykładowych. IBM udostępnia Komponenty Źródłowe i Materiały Przykładowe bez zobowiązania do wsparcia oraz W STANIE, W JAKIM SIĘ ZNAJDUJĄ („AS IS"), BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (RĘKOJMIA JEST NINIEJSZYM RÓWNIEŻ WYŁĄCZONA), WYRAŹNYCH LUB DOMNIEMANYCH, W TYM GWARANCJI PRAWA WŁASNOŚCI I NIENARUSZANIA PRAW, A TAKŻE DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ I PRZYDATNOŚCI DO OKREŚLONEGO CELU. Zastrzeżenie: Komponenty Źródłowe i Materiały Przykładowe są dostarczane wyłącznie jako przykład sposobu wdrażania Produktu Osadzanego w rozwiązaniu CIMA. Komponenty Źródłowe i Materiały Przykładowe mogą być niezgodne ze środowiskiem programistycznym Klienta. Ponadto Klient ponosi wyłączną odpowiedzialność za testowanie i wdrażanie Produktu Osadzanego w rozwiązaniu CIMA.

Klient zobowiązuje się utworzyć, przechowywać i udostępnić IBM oraz jego rewidentom dokładne rejestry pisemne, dane wyjściowe narzędzi systemowych oraz inne informacje systemowe, wystarczające do stwierdzenia, że korzystanie przez Klienta z pakietu IBM Trusteer Mobile SDK odbywa się zgodnie z niniejszym Opisem Usług.

6. Wsparcie Premium

Klient ma uprawnienia do Wsparcia Premium wyłącznie dla tych Usług Przetwarzania w Chmurze, w odniesieniu do których Klient dokonał subskrypcji powiązanej oferty Wsparcia Premium.

7. Wdrażanie usług IBM Trusteer Fraud Protection

W przypadku każdej Aplikacji subskrybowanej przez Klienta podstawowa subskrypcja Klienta obejmuje wymagane czynności z zakresu konfigurowania i początkowego instalowania Usługi Przetwarzania w Chmurze IBM Trusteer, w tym jednorazowe początkowe uruchamianie, konfigurowanie, dostarczanie Szablonu Ekranu Powitalnego, testowanie i szkolenie.

Czynności wdrożeniowe nie obejmują zakresu wymaganego do implementowania aplikacji lub systemów Klienta.

Usługi Przetwarzania w Chmurze zostały zaprojektowane z myślą o ich wdrażaniu w przedziałach czasowych określonych szczegółowo w odpowiednich podręcznikach dotyczących wdrażania.

Zakończenie faz wdrożenia w wyznaczonym przedziale czasowym zależy od pełnego zaangażowania i udziału ze strony kierownictwa i personelu w przedsiębiorstwie Klienta. Klient powinien terminowo dostarczać potrzebne informacje. Działania IBM zależą od terminowego przekazywania informacji i podejmowania decyzji przez Klienta, a wszelkie opóźnienia mogą skutkować dodatkowymi kosztami i/lub przesunięciem terminu wykonania usług wdrożeniowych.

W przypadku każdej Aplikacji subskrybowanej przez Klienta podstawowa subskrypcja Klienta obejmuje wymagane czynności z zakresu konfigurowania i początkowego instalowania Usługi Przetwarzania w Chmurze IBM Trusteer, w tym jednorazowe początkowe uruchamianie, konfigurowanie, dostarczanie Szablonu Ekranu Powitalnego, testowanie i szkolenie.

Subskrypcja Klienta obejmuje wsparcie i testowanie stron znajdujących się w Aplikacji Klienta, które zostaną oznakowane jako zalecane przez IBM w ramach początkowego wdrożenia. IBM nie odpowiada za: (i) częściowe wdrożenie, (ii) decyzję Klienta o niewdrożeniu Usług Przetwarzania w Chmurze IBM w sposób zalecany przez IBM, (iii) decyzję Klienta o przeprowadzeniu wdrożenia, konfigurowania i testowania we własnym zakresie, (iv) przeprowadzenie częściowego wdrożenia lub zapewnienie częściowej ochrony na skutek dostarczenia niewłaściwych informacji przez Klienta. Dodatkowe usługi (w tym czynności wdrożeniowe wykraczające poza zakres początkowego wdrożenia) mogą zostać zlecone za dopłatą w ramach odrębnej umowy.

8. Ochrona danych i prywatności

W odniesieniu do niniejszej Usługi Przetwarzania w Chmurze stosowane są zasady ochrony danych i prywatności IBM dla usług IBM SaaS, dostępne pod adresem http://www.ibm.com/cloud/data-security, a także ewentualne dodatkowe zasady określone w niniejszym paragrafie. Żadna zmiana strategii bezpieczeństwa i ochrony danych IBM nie zmniejszy bezpieczeństwa Usługi Przetwarzania w Chmurze.

Niniejsza Usługa Przetwarzania w Chmurze może być używana do przetwarzania zawartości zawierającej dane osobowe, jeśli Klient jako administrator danych stwierdzi, że techniczne i organizacyjne środki bezpieczeństwa są odpowiednie do czynników ryzyka związanych z przetwarzaniem i rodzajem danych podlegających ochronie. Klient przyjmuje do wiadomości, że niniejsza Usługa Przetwarzania w Chmurze nie oferuje funkcji ochrony danych osobowych objętych szczególną ochroną oraz danych podlegających dodatkowym wymaganiom prawnym.

Niniejsza Usługa Przetwarzania w Chmurze jest objęta certyfikatem IBM Privacy Shield, który ma zastosowanie, jeśli Klient wybierze opcję udostępniania Usługi Przetwarzania w Chmurze w centrum przetwarzania danych znajdującym się w Stanach Zjednoczonych. Usługa podlega Strategii ochrony prywatności IBM Privacy Shield dostępnej pod adresem http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

8.1 Opcje zabezpieczające i obowiązki związane z bezpieczeństwem

W Usłudze Przetwarzania w Chmurze zaimplementowano następujące opcje zabezpieczające:

Ta Usługa Przetwarzania w Chmurze szyfruje zawartość w trakcie transmisji danych do i z sieci IBM oraz dane oczekujące na transmisję z punktu końcowego.

8.2 Legalne używanie i wyrażenie zgody

Używanie zgodnie z prawem

Korzystanie z niniejszej Usługi Przetwarzania w Chmurze może podlegać różnym przepisom i regulacjom. Z Usługi Przetwarzania w Chmurze można korzystać wyłącznie do celów zgodnych z prawem oraz w sposób zgodny z prawem. Klient zgadza się korzystać z Usługi Przetwarzania w Chmurze w sposób zgodny z odpowiednimi przepisami, regulacjami i strategiami oraz przyjąć pełną odpowiedzialność za przestrzeganie takich przepisów, regulacji i strategii.

Zgoda na gromadzenie i przetwarzanie danych

Usługa Przetwarzania w Chmurze będzie gromadzić informacje pochodzące od Uprawnionych Uczestników i Urządzeń Klienckich komunikujących się z Aplikacjami Biznesowymi lub Aplikacjami Indywidualnymi, które są objęte Usługami Przetwarzania w Chmurze IBM zasubskrybowanymi przez Klienta. Usługa Przetwarzania w Chmurze gromadzi informacje, które same w sobie lub w pewnych kombinacjach mogą być uznawane za Dane Osobowe według ustawodawstwa niektórych krajów. Dane Osobowe oznaczają wszelkie informacje, które mogą posłużyć do zidentyfikowania konkretnej osoby (takie jak imię i nazwisko, adres e-mail, adres zamieszkania lub numer telefonu), udostępniane IBM w celu przechowywania, przetwarzania lub przekazywania w imieniu Klienta.

Procedury gromadzenia i przetwarzania danych mogą być aktualizowane w celu poprawienia funkcjonalności Usługi Przetwarzania w Chmurze. Dokument z pełnym opisem procedur gromadzenia i przetwarzania danych podlega aktualizacji zależnie od potrzeb i jest udostępniany Klientowi na żądanie. Klient upoważnia IBM do gromadzenia powyższych danych i przetwarzania ich zgodnie z postanowieniami paragrafów „Przekazywanie danych za granicę” i „Ochrona danych” w niniejszym Opisie Usług.

W przypadku ofert IBM Trusteer, które obejmują produkt TMA (Trusteer Management Application):

W aplikacji TMA (Trusteer Management Application), przeznaczonej dla administratorów z przedsiębiorstwa sponsorującego, są gromadzone i zapisywane następujące informacje: adres e-mail (jako identyfikator logowania), hasło zakodowane, imię i nazwisko, stanowisko, dział.

W przypadku Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint:

Pobrane dane mogą obejmować:

- identyfikatory użytkownika lub punktu końcowego, takie jak ID użytkownika w postaci zaszyfrowanej lub przetworzonej przez jednokierunkową funkcję mieszającą, trwałe ID użytkownika (PUID), klucz Rapport Agent Key oraz identyfikator sesji użytkownika;
- dane związane z chronioną aplikacją, takie jak konkretne atrybuty/elementy aplikacji klientów do obsługi bankowości elektronicznej w postaci, w jakiej są one wyświetlane w przeglądarce użytkownika, liczbę odwiedzin serwisu WWW oraz historię przeglądania;
- informacje o zainstalowanym środowisku oprogramowania, atrybutach i ustawieniach przeglądarki i urządzenia oraz o zakresie czasowym historii w przeglądarce;
- informacje o sprzęcie i znacznik czasu;
- nagłówki przeglądarek i dane dotyczące protokołu komunikacyjnego, takie jak adres IP użytkownika, informacje cookie, nagłówek strony odsyłającej oraz inne nagłówki protokołu HTTP;
- dane o ruchach myszą wykonywanych przez użytkownika końcowego podczas interakcji z aplikacją bankowości elektronicznej Klienta, takie jak współrzędne wskaźnika myszy, kliknięcia i poruszenia kółka przewijającego (a także ich odpowiedniki) wraz ze znacznikami czasu tych zdarzeń;
- dane o serwisach do wyłudzania informacji oraz informacje wysłane do takich serwisów;
- według uznania Klienta – dane transakcyjne (kwota transakcji, kody waluty transakcji i lokalizacji docelowej, identyfikator banku docelowego przetworzony przez jednokierunkową funkcję mieszającą, identyfikator docelowego rachunku transakcji przetworzony przez jednokierunkową funkcję mieszającą, wartość binarna, jeśli w transakcji występuje nowy odbiorca płatności, a także data i godzina transakcji) oraz opcjonalną ocenę danych o ryzyku.
- wyłącznie według decyzji Klienta – rytm pisania na klawiaturze i sekwencje poszczególnych rodzin klawiszy używanych przez użytkownika końcowego przy wprowadzaniu nazwy konta, hasła i innego tekstu (co nie obejmuje jednak konkretnych liter, cyfr i znaków specjalnych i nie umożliwia uzyskania nazwy konta i hasła);

Klient uznaje i potwierdza, że IBM nie gromadzi i nie prowadzi oficjalnych ksiąg rachunkowych i/lub dokumentacji rachunkowej Klienta ani nie zarządza nimi i nie przechowuje ich.

W przypadku zasubskrybowania przez Klienta usługi IBM Trusteer Rapport for Remediation oraz w określonych przypadkach związanych z korzystaniem ze wsparcia dotyczącego rozwiązań Pinpoint IBM może zalecić zainstalowanie na komputerze Uprawnionego Uczestnika Oprogramowania Klienckiego Posiadacza Konta (wchodzącego w skład oferty Rapport). Oprogramowanie to jest instalowane w celu zbadania domniemanego przypadku zainfekowania systemu przez szkodliwe oprogramowanie. Dane pobierane w ramach ofert Rapport zostały wyszczególnione poniżej.

W przypadku Usług Przetwarzania w Chmurze IBM Trusteer Rapport (w tym ofert Rapport for Remediation lub Rapport for Mitigation, jeśli są one wdrażane w powiązaniu z ofertami Pinpoint):

Pobrane dane mogą obejmować:

- adresy URL i adresy IP odwiedzanych przez Posiadacza Konta serwisów WWW, które w opinii IBM mogą służyć do oszustw, wyłudzania informacji lub wykorzystywania słabych punktów systemu, wraz z informacjami o charakterze zidentyfikowanych zagrożeń;
- adresy URL i adresy IP odwiedzanych przez Posiadacza Konta serwisów WWW, które znajdują się pod kontrolą Klienta i są chronione przez Usługę Przetwarzania w Chmurze, takie jak serwisy bankowości elektronicznej, a także adresy IP Posiadacza Konta;
- informacje o identyfikacji sprzętu, systemach operacyjnych, oprogramowaniu aplikacyjnym, sprzęcie peryferyjnym, konfiguracji zabezpieczeń, ustawieniach systemu i połączeniach sieciowych punktu końcowego, a także identyfikator, nazwę oraz inne informacje umożliwiające zidentyfikowanie punktu końcowego i dane o wzorcach jego używania;

- informacje związane z instalacją i działaniem programu, identyfikator programu, oznaczenie wersji programu, informacje o zdarzeniach dotyczących bezpieczeństwa generowane przez punkt końcowy oraz informacje o błędach w programie;
- statystyki używania oraz informacje statystyczne o zagrożeniach wykrytych przez program; pliki dziennika zawierające informacje o awariach przeglądarki, datę i godzinę zainfekowania oraz informacje o charakterze zidentyfikowanych zagrożeń lub przypadków wadliwego działania;
- informacje o afiliacji Klienta (inna nazwa tego pojęcia to „Przedsiębiorstwo Sponsorujące"); afiliacja zostaje ustanowiona w momencie, gdy użytkownik końcowy pobiera zawartość Rapport z serwisu WWW Klienta, wybiera określonego Klienta podczas pobierania zawartości Rapport z serwisu wsparcia Trusteer lub loguje się w aplikacji bankowości elektronicznej Klienta, przy czym jeden użytkownik końcowy może mieć wiele afiliacji z Klientami;
- kopię zaszyfrowanego ID użytkownika, z którego korzysta Posiadacz Konta, aby prowadzić interakcję z Klientem (opcjonalnie);
- zaszyfrowaną kopię numeru karty kredytowej wpisanego przez Posiadacza Konta w określonym serwisie, jeśli program poinformuje Posiadacza Konta, że serwis ten został uznany za niebezpieczny;
- pliki i inne informacje z punktu końcowego, które w opinii specjalistów IBM ds. bezpieczeństwa mogą być związane ze szkodliwym oprogramowaniem lub innymi szkodliwymi czynnościami bądź mogą mieć związek z ogólnym wadliwym działaniem programu;
- osobiste informacje kontaktowe, w tym imię, nazwisko i adres e-mail (pobierane, gdy użytkownik kontaktuje się z Działem Wsparcia).

W przypadku ofert IBM Trusteer Mobile SDK oraz Usług Przetwarzania w Chmurze IBM Trusteer Mobile Browser:

Pobrane dane mogą obejmować:

- identyfikatory użytkownika, takie jak ID użytkownika w postaci zaszyfrowanej lub przetworzonej przez jednokierunkową funkcję mieszającą;
- informacje o urządzeniu, takie jak adres IP, identyfikator urządzenia przetworzony przez funkcję mieszającą, znacznik czasu, wartości funkcji MD5 dotyczące zainstalowanego pakietu oraz inne informacje o sprzęcie i oprogramowaniu urządzenia;
- oznaczenie wersji mobilnego pakietu SDK lub przeglądarki mobilnej oraz data instalacji;
- odwiedziny chronionych aplikacji;
- informacje o przynależności Klienta do organizacji;
- dane dotyczące ryzyka urządzenia (np. obecności szkodliwego oprogramowania, mechanizmów ukrywających roota, statusu szyfrowania połączeń Wi-Fi czy ewentualnego usunięcia ograniczeń);
- śledzenie stosu w przypadku awarii (nieoczekiwanego zamknięcia aplikacji);
- dane dotyczące budowy telefonu (np. modelu czy producenta);
- interakcje użytkownika końcowego z ekranem dotykowym, w tym współrzędne x i y, obszar dotykania i typ działania (przesunięcie w dół, przesunięcie w górę lub gest);
- dane z czujników ruchu, zużycie energii/zasobów, ustawienia łączności, czujniki środowiskowe (temperatury, światła i ciśnienia) oraz ogólne ustawienia urządzenia (głośność, dzwonek, jasność ekranu itp.).

8.3 Świadoma zgoda właścicieli danych

W przypadku Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint oraz IBM Trusteer Mobile SDK:

Klient potwierdza, że uzyskał lub uzyska wszelkie w pełni świadome zgody, uprawnienia lub licencje, które są niezbędne, aby umożliwić zgodne z prawem korzystanie z Usługi Przetwarzania w Chmurze oraz aby zezwolić IBM na gromadzenie i przetwarzanie informacji za pośrednictwem Usługi Przetwarzania w Chmurze.

W przypadku Usług Przetwarzania w Chmurze IBM Trusteer Rapport (w tym ofert Rapport Remediation lub Rapport for Mitigation, jeśli są one wdrażane w powiązaniu z Usługami Przetwarzania w Chmurze Pinpoint) oraz IBM Trusteer Mobile Browser:

Klient upoważnia IBM do uzyskania w pełni świadomej zgody, która jest niezbędna, aby umożliwić zgodne z prawem korzystanie z Usługi Przetwarzania w Chmurze oraz aby gromadzić i przetwarzać informacje na zasadach opisanych w Umowie Licencyjnej z Użytkownikiem Końcowym dostępnej pod adresem https://www.trusteer.com/support/end-user-license-agreement. Jeśli Klient ustalił, że to Klient (a nie IBM) będzie kontaktować się z użytkownikami końcowymi w celu uzyskania ich zgody, wówczas Klient potwierdza, że uzyskał lub uzyska wszelkie w pełni świadome zgody, uprawnienia lub licencje, które są niezbędne, aby umożliwić zgodne z prawem korzystanie z Usługi Przetwarzania w Chmurze oraz aby zezwolić IBM – jako podmiotowi przetwarzającemu dane na rzecz Klienta – na gromadzenie i przetwarzanie informacji za pośrednictwem Usługi Przetwarzania w Chmurze.

8.4 Korzystanie z Danych dotyczących Bezpieczeństwa

W ramach Usługi Przetwarzania w Chmurze, która obejmuje czynności z zakresu raportowania, IBM będzie przygotowywać i utrzymywać informacje pozbawione danych identyfikacyjnych oraz informacje zagregowane, pochodzące z Usługi Przetwarzania w Chmurze („Dane dotyczące Bezpieczeństwa"). Dane dotyczące Bezpieczeństwa nie mogą umożliwiać zidentyfikowania Klienta, Uprawnionych Uczestników ani innych osób fizycznych z zastrzeżeniem postanowień punktu (d) poniżej. Klient zezwala IBM na bezterminowe wykorzystywanie i/lub kopiowanie Danych dotyczących Bezpieczeństwa wyłącznie w celu:

a. publikowania i/lub dystrybuowania Danych dotyczących Bezpieczeństwa (np. w opracowaniach i/lub analizach związanych z cyberbezpieczeństwem),

b. opracowywania i udoskonalania produktów i usług,

c. prowadzenia badań we własnym zakresie i z udziałem osób trzecich,

d. udostępniania zgodnie z prawem potwierdzonych informacji na temat sprawcy będącego osobą trzecią.

8.5 Przekazywanie danych za granicę

Klient wyraża zgodę na przetwarzanie przez IBM zawartości (w tym wszelkich Danych Osobowych określonych w rozdziale: „Legalne używanie i wyrażenie zgody") poza granicami kraju w sposób zgodny z odpowiednimi przepisami i wymaganiami za pośrednictwem podmiotów przetwarzających i podwykonawców przetwarzania w następujących krajach spoza Europejskiego Obszaru Gospodarczego oraz w krajach, które zdaniem Komisji Europejskiej zapewniają należyty poziom bezpieczeństwa: Stany Zjednoczone.

8.6 Ochrona danych

Jeśli Klient udostępnia Dane Osobowe w ramach Usługi Przetwarzania w Chmurze w krajach członkowskich Unii Europejskiej, w Islandii, Liechtensteinie, Norwegii lub Szwajcarii, bądź jeśli w krajach tych znajdują się Uprawnieni Uczestnicy bądź Urządzenia Klienckie z firmy Klienta, wówczas Klient, jako wyłączny administrator takich danych, mianuje IBM podmiotem przetwarzającym Dane Osobowe (zgodnie z definicją tych terminów w dyrektywie 95/46/WE). IBM będzie przetwarzać takie Dane Osobowe tylko w zakresie wymaganym do udostępnienia Usługi Przetwarzania w Chmurze zgodnie z opublikowanymi przez IBM opisami Usług Przetwarzania w Chmurze, a Klient potwierdza, że przetwarzanie to jest zawsze zgodne z jego instrukcjami. IBM poinformuje Klienta z należytym wyprzedzeniem za pośrednictwem portalu dla klientów w przypadku wprowadzenia istotnych zmian w lokalizacji przetwarzania lub metodach ochrony Danych Osobowych w ramach Usługi Przetwarzania w Chmurze. Klient może zakończyć bieżący okres subskrypcji Usługi Przetwarzania w Chmurze objętej taką zmianą, przekazując IBM pisemne wypowiedzenie w terminie 30 (trzydziestu) dni od otrzymania od IBM powiadomienia o zmianie.

Strony lub ich odpowiednie przedsiębiorstwa afiliowane mogą zawrzeć oddzielne umowy sporządzone na podstawie standardowych, niezmodyfikowanych dokumentów wzorcowych UE (stosownie do ról poszczególnych podmiotów) zgodnie z Decyzją KE nr 2010/87/UE, z pominięciem klauzul opcjonalnych. Wszelkie spory i zobowiązania wynikające z powyższych umów (nawet jeśli umowy te zostaną zawarte przez przedsiębiorstwa afiliowane) będą traktowane jako spory i zobowiązania powstałe między Stronami zgodnie z warunkami niniejszej Umowy.

a. W odniesieniu do usług świadczonych za pośrednictwem centrum przetwarzania danych w Niemczech (co zostanie wskazane podczas udostępniania usługi) Klient wyraża zgodę na przetwarzanie przez IBM zawartości, w tym wszelkich Danych Osobowych, poza granicami kraju za pośrednictwem następujących podmiotów przetwarzających i podwykonawców przetwarzania:

Nazwa podmiotu przetwarzającego/podwykonawcy przetwarzania	Rola (przetwarzający lub podwykonawca przetwarzania)	Lokalizacja
Jednostka zlecająca IBM	Podmiot przetwarzający	Zgodnie z wyszczególnieniem w Dokumencie Transakcyjnym
Amazon Web Services (Niemcy)	Podwykonawca przetwarzania	Niemcy
IBM Ireland Ltd.	Podmiot przetwarzający	Irlandia
IBM Israel Ltd.	Podmiot przetwarzający	Izrael

W przypadku usług świadczonych za pośrednictwem centrum przetwarzania danych w Niemczech część usług wsparcia klienta może być realizowana przez pracowników Trusteer zlokalizowanych w jednym z krajów Unii Europejskiej.

b. W odniesieniu do usług świadczonych za pośrednictwem centrum przetwarzania danych w Japonii (co zostanie wskazane podczas udostępniania usługi) Klient wyraża zgodę na przetwarzanie przez IBM zawartości, w tym wszelkich Danych Osobowych, poza granicami kraju za pośrednictwem następujących podmiotów przetwarzających i podwykonawców przetwarzania:

Nazwa podmiotu przetwarzającego/podwykonawcy przetwarzania	Rola (przetwarzający lub podwykonawca przetwarzania)	Lokalizacja
Jednostka zlecająca IBM	Podmiot przetwarzający	Japonia, zgodnie z wyszczególnieniem w Dokumencie Transakcyjnym
Amazon Web Services (Japonia)	Podwykonawca przetwarzania	Japonia
IBM Ireland Ltd.	Podmiot przetwarzający	Irlandia
IBM Israel Ltd.	Podmiot przetwarzający	Izrael

c. W odniesieniu do usług świadczonych za pośrednictwem centrum przetwarzania danych w Stanach Zjednoczonych Klient wyraża zgodę na przetwarzanie przez IBM zawartości, w tym wszelkich Danych Osobowych, poza granicami kraju za pośrednictwem następujących podmiotów przetwarzających i podwykonawców przetwarzania:

Nazwa podmiotu przetwarzającego/podwykonawcy przetwarzania	Rola (przetwarzający lub podwykonawca przetwarzania)	Lokalizacja
Jednostka zlecająca IBM	Podmiot przetwarzający	Zgodnie z wyszczególnieniem w Dokumencie Transakcyjnym
Amazon Web Services LLC	Podwykonawca przetwarzania	Stany Zjednoczone
IBM Ireland Ltd.	Podmiot przetwarzający	Irlandia
IBM Israel Ltd.	Podmiot przetwarzający	Izrael
IBM Corp	Podmiot przetwarzający	Stany Zjednoczone

d. W przypadku usług świadczonych za pośrednictwem centrów przetwarzania danych, o których mowa w punkcie 8.5.c powyżej („centrów przetwarzania danych w Stanach Zjednoczonych”), IBM może również przetwarzać dane z udziałem jednego lub większej liczby wymienionych poniżej podwykonawców przetwarzania, co zostanie określone podczas procesu udostępniania usługi:

Nazwa podmiotu przetwarzającego/podwykonawcy przetwarzania	Rola (przetwarzający lub podwykonawca przetwarzania)	Lokalizacja
Amazon Web Services (Australia)	Podwykonawca przetwarzania	Australia

Nazwa podmiotu przetwarzającego/podwykonawcy przetwarzania	Rola (przetwarzający lub podwykonawca przetwarzania)	Lokalizacja
Amazon Web Services (Singapur)	Podwykonawca przetwarzania	Singapur
Amazon Web Services (Irlandia)	Podwykonawca przetwarzania	Irlandia

e. Klient przyjmuje do wiadomości, że IBM może (pod warunkiem przekazania stosownego powiadomienia za pośrednictwem portalu dla klientów) przenieść przetwarzanie z placówek Amazon Web Services do centrów przetwarzania danych IBM, i wyraża zgodę na takie ewentualne przeniesienie. Ponadto IBM może (pod warunkiem przekazania stosownego powiadomienia za pośrednictwem portalu dla klientów) zmieniać powyższe listy podwykonawców przetwarzania.

f. Dane Posiadacza Konta będą przetwarzane w regionie, z którego Posiadacz Konta pierwotnie zainstalował Oprogramowanie Klienckie Posiadacza Konta. Zawartość Posiadacza Konta może zatem być przetwarzana zarówno w regionie pochodzenia, jak i w regionie uzgodnionym z Klientem.

g. Dane wsparcia Klienta są przechowywane na serwerze Salesforce.com w chmurze, który jest zlokalizowany w Irlandii.

h. Ponieważ Trusteer Fraud Protection jest rozwiązaniem zintegrowanym, dodatkowo precyzuje się, że jeśli Klient zrezygnuje z jednej z tych Usług Przetwarzania w Chmurze, IBM może zatrzymać dane Klienta w celu świadczenia mu pozostałych Usług Przetwarzania w Chmurze zgodnie z niniejszym Opisem Usługi.

9. Umowa dotycząca Poziomu Usług

IBM udostępnia przedstawioną poniżej Umowę dotyczącą Poziomu Usług („SLA”) w odniesieniu do niniejszej Usługi Przetwarzania w Chmurze zgodnie z dokumentem PoE. Umowa dotycząca Poziomu Usług nie stanowi gwarancji (rękojmia jest również wyłączona). Umowa dotycząca Poziomu Usług jest dostępna tylko dla Klienta i ma zastosowanie wyłącznie w środowiskach produkcyjnych.

9.1 Uznania z tytułu Dostępności

Klient musi zarejestrować w dziale wsparcia technicznego IBM zgłoszenie problemu o Poziomie istotności 1 w ciągu 24 godzin od momentu uzyskania informacji o tym, że dane zdarzenie wpłynęło na dostępność Usługi Przetwarzania w Chmurze. Klient udzieli IBM uzasadnionej pomocy podczas diagnozowania i rozwiązywania problemu.

Reklamację dotyczącą zgłoszenia problemu z powodu niedotrzymania Umowy dotyczącej Poziomu Usług należy złożyć w ciągu trzech dni roboczych od końca miesiąca obowiązywania Umowy. Wyrównanie z tytułu uzasadnionej reklamacji w sprawie niedotrzymania Umowy dotyczącej Poziomu Usług będzie mieć postać uznania na poczet przyszłej faktury z tytułu opłat za Usługę Przetwarzania w Chmurze, a jego kwota będzie uzależniona od czasu, w którym procesy przetwarzania dla Usługi Przetwarzania w Chmurze w systemie produkcyjnym były niedostępne (zwanego dalej „Przestojem”). Przestój jest mierzony od chwili zgłoszenia zdarzenia przez Klienta do chwili przywrócenia Usługi Przetwarzania w Chmurze. Nie obejmuje zaplanowanych lub zapowiedzianych wyłączeń systemu w celu przeprowadzenia prac serwisowych, jak również przerw w pracy systemu spowodowanych przyczynami, na które IBM nie ma wpływu, problemami z zawartością, technologią, projektami lub instrukcjami Klienta bądź osoby trzeciej, zastosowaniem nieobsługiwanych konfiguracji systemu lub platform, innymi błędami Klienta, spowodowanym przez Klienta incydentem dotyczącym bezpieczeństwa lub testowaniem zabezpieczeń Klienta. IBM naliczy najwyższe obowiązujące wyrównanie na podstawie łącznej dostępności Usługi Przetwarzania w Chmurze osiągniętej w danym miesiącu obowiązywania umowy, zgodnie z poniższą tabelą. Łączna kwota wyrównań przyznanych za dowolny miesiąc obowiązywania umowy nie może w żadnym razie przekroczyć 10% kwoty równej 1/12 (jednej dwunastej) rocznej opłaty za Usługę Przetwarzania w Chmurze.

9.2 Poziomy usług

Dostępność Usługi Przetwarzania w Chmurze w Miesiącu Obowiązywania Umowy

Dostępność w miesiącu obowiązywania umowy	Wyrównanie (procent miesięcznej opłaty za subskrypcję* za miesiąc obowiązywania umowy, którego dotyczy reklamacja)
< 99,5%	2%
< 98,0%	5%
< 96,0%	10%

* Jeśli Klient nabył Usługę Przetwarzania w Chmurze od Partnera Handlowego IBM, to miesięczna opłata za subskrypcję zostanie obliczona na podstawie aktualnej ceny katalogowej Usługi Przetwarzania w Chmurze obowiązującej w miesiącu obowiązywania umowy, którego dotyczy reklamacja, objętej upustem w wysokości 50%. IBM udostępni rabat bezpośrednio Klientowi.

Poziomy Usługi oraz powiązane z nimi Uznania z tytułu Usługi są mierzone oddzielnie dla każdej Usługi Przetwarzania w Chmurze oraz Aplikacji Klienckiej.

Przy naliczaniu uznania z tytułu poziomu usług za Usługi Przetwarzania w Chmurze na podstawie uprawnień do Aplikacji obliczanie Dostępności będzie się odbywać zgodnie z następującymi wytycznymi:

- Każda Aplikacja będzie mieć przypisany udział ważony, oparty na liczbie sesji naliczonej w miesiącu obowiązywania umowy.
- Przestój każdej Usługi Przetwarzania w Chmurze w podziale na Aplikacje w miesiącu obowiązywania umowy będzie kumulowany oddzielnie.

Poniżej przedstawiono przykład obliczeń dla aktywności za jeden miesiąc wraz z odpowiednimi wagami. Przykład ma charakter wyłącznie informacyjny:

Aplikacje Indywidualne	Udział w łącznej liczbie sesji w danym miesiącu obowiązywania umowy	Łączny czas trwania Przestojów w miesiącu obowiązywania umowy	Ważona liczba minut Przestojów
Aplikacja Indywidualna A	40%	300 minut	40% x 300 minut = 120 minut
Aplikacja Indywidualna B	20%	250 minut	20% x 250 minut = 50 minut
Aplikacja Indywidualna C	40%	150 minut	40% x 150 minut = 60
			Łączna ważona liczba minut Przestojów = 230

Dostępność wyrażona procentowo jest równa ilorazowi łącznej liczby minut w danym miesiącu obowiązywania umowy pomniejszonej o łączny ważony czas trwania Przestojów w minutach w danym miesiącu obowiązywania umowy oraz łącznej liczby minut w danym miesiącu obowiązywania umowy. Poniżej podano przykładowe wyliczenie oparte na omówionym wcześniej przykładzie przypisywania wag:

43 200 minut w 30-dniowym miesiącu obowiązywania umowy - 230 minut ważonych Przestojów = 42 970 minut łącznie 43 200 minut	= 2% Uznanie z tytułu Dostępności za dostępność na poziomie 99,4% w miesiącu obowiązywania umowy

10. Wsparcie Techniczne

Klientowi i Uprawnionym Uczestnikom udostępniane jest wsparcie techniczne do Usług Przetwarzania w Chmurze, aby pomagać im w korzystaniu z tych Usług.

Wsparcie standardowe jest uwzględnione w subskrypcji każdej oferowanej usługi. W przypadku usługi Trusteer Rapport Mandatory Service, stanowiącej dodatek do usługi Trusteer Rapport, wymaganiem wstępnym jest posiadanie Wsparcia Premium w odniesieniu do podstawowej subskrypcji usługi Trusteer Rapport.

W przypadku każdej Usługi Przetwarzania w Chmurze subskrypcja Wsparcia Premium jest dostępna za dodatkową opłatą. Wyjątek stanowią Usługi Przetwarzania w Chmurze IBM Trusteer Mobile SDK oraz IBM Trusteer Rapport Mandatory Service. Prosimy o kontakt z przedstawicielem lub partnerem handlowym IBM.

Wsparcie standardowe:

- Wsparcie jest świadczone w godzinach od 8:00 do 17:00 czasu miejscowego.
- Klienci i Uprawnieni Uczestnicy mogą wprowadzać zgłoszenia problemów w postaci elektronicznej zgodnie ze szczegółowym opisem w Podręczniku wsparcia dla usługi IBM Software as a Service (SaaS).
- Klienci mogą uzyskać dostęp do powiadomień, dokumentów, raportów z wdrożeń i często zadawanych pytań w Portalu Obsługi Klienta pod adresem http://www-01.ibm.com/software/security/trusteer/support/.
- Wykaz opcji wsparcia oraz inne szczegółowe informacje na temat wsparcia można znaleźć w Podręczniku Wsparcia SaaS pod adresem http://www-01.ibm.com/software/support/handbook.html.

Wsparcie Premium:

- Wsparcie jest świadczone przez całą dobę we wszystkie dni tygodnia bez względu na poziom istotności.
- Klienci mogą kontaktować się bezpośrednio ze wsparciem drogą telefoniczną lub zamawiając oddzwonienie.
- Klienci i Uprawnieni Uczestnicy mogą wprowadzać zgłoszenia problemów w postaci elektronicznej zgodnie ze szczegółowym opisem w Podręczniku wsparcia dla usługi IBM Software as a Service (SaaS).
- Klienci mogą uzyskać dostęp do powiadomień, dokumentów, raportów z wdrożeń i często zadawanych pytań w Portalu Obsługi Klienta pod adresem http://www-01.ibm.com/software/security/trusteer/support/.
- Wykaz opcji wsparcia oraz inne szczegółowe informacje na temat wsparcia można znaleźć w Podręczniku Wsparcia SaaS pod adresem http://www-01.ibm.com/software/support/handbook.html.

11. Informacje o uprawnieniach i rozliczaniu

11.1 Opłaty rozliczeniowe

Przy sprzedaży Usługi Przetwarzania w Chmurze wysokość opłat rozliczeniowych jest ustalana na podstawie następujących miar, zgodnie z Dokumentem Transakcyjnym:

a. Jednostką miary, według której można korzystać z Usługi Przetwarzania w Chmurze, jest **Uprawniony Uczestnik**. Uprawnionym Uczestnikiem jest każda osoba oraz każdy podmiot uprawniony do uczestnictwa w dowolnym programie świadczenia usługi zarządzanym lub monitorowanym za pomocą Usługi Przetwarzania w Chmurze. Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę wszystkich Uprawnionych Uczestników objętych zarządzaniem lub śledzeniem w ramach Usługi Przetwarzania w Chmurze w okresie pomiarowym określonym w Dokumencie Transakcyjnym Klienta.

   Każdy program świadczenia usług zarządzany za pomocą Usługi Przetwarzania w Chmurze podlega odrębnej analizie, a następnie jest rozpatrywany łącznie z pozostałymi programami. Osoby fizyczne lub jednostki zakwalifikowane do wielu programów świadczenia usług muszą uzyskać odrębne uprawnienia.

   W kontekście uprawnień do tych Usług Przetwarzania w Chmurze termin „Uprawniony Uczestnik” oznacza użytkownika końcowego w przedsiębiorstwie Klienta, który dysponuje unikalnymi danymi

uwierzytelniającymi umożliwiającymi zalogowanie się w Aplikacji Biznesowej lub Indywidualnej Klienta.

b. Jednostką miary, według której można korzystać z Usługi Przetwarzania w Chmurze, jest **Urządzenie Klienckie**. Urządzenie Klienckie to pojedyncze urządzenie komputerowe lub telemetryczne bądź pojedyncze urządzenie w postaci czujnika specjalnego przeznaczenia, które żąda wykonania lub otrzymuje do wykonania zestaw komend, procedur lub aplikacji z innego systemu komputerowego bądź też dostarcza dane do takiego systemu, zazwyczaj określanego jako serwer lub zarządzanego w inny sposób przez serwer. Wiele Urządzeń Klienckich może współużytkować dostęp do jednego serwera. Aby umożliwić użytkownikowi wykonywanie pracy, Urządzenie Klienckie może być programowalne lub wyposażone w funkcje przetwarzania. Klient musi uzyskać uprawnienia dla każdego Urządzenia Klienckiego, które uruchamia Usługę Przetwarzania w Chmurze, dostarcza do niej dane, korzysta z udostępnianych przez nią usług lub w inny sposób uzyskuje do niej dostęp w okresie pomiarowym wyszczególnionym w Dokumencie Transakcyjnym Klienta.

c. Jednostką miary, według której można korzystać z Usługi Przetwarzania w Chmurze, jest **Aplikacja**. Aplikacja to jednoznacznie nazwany program. W przypadku każdej udostępnionej Aplikacji Klient musi uzyskać odpowiednie uprawnienia umożliwiające mu uzyskiwanie do niej dostępu i jej używanie w okresie pomiarowym określonym w dokumencie PoE lub Dokumencie Transakcyjnym Klienta.

   W kontekście tej Usługi Przetwarzania w Chmurze termin „Aplikacja” oznacza pojedynczą Aplikację Biznesową lub Aplikację Indywidualną Klienta.

d. Jednostką miary, według której można korzystać z usług, jest **Przedsięwzięcie**. Przedsięwzięcie obejmuje usługi specjalistyczne i/lub szkoleniowe związane z Usługami Przetwarzania w Chmurze. Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę wszystkich Przedsięwzięć.

11.2 Opłaty za niepełne miesiące

Opłata za niepełny miesiąc, zgodnie z treścią Dokumentu Transakcyjnego, może być naliczana w ujęciu proporcjonalnym.

12. Zachowanie zgodności i kontrola

Dostęp do Usług Przetwarzania w Chmurze IBM Trusteer Fraud Protection jest ograniczony maksymalną liczbą Aplikacji, Uprawnionych Uczestników i/lub Urządzeń Klienckich, zgodnie z wyszczególnieniem w Dokumencie Transakcyjnym. Klient zobowiązuje się dopilnować, aby liczba Aplikacji, Uprawnionych Uczestników i/lub Urządzeń Klienckich nie przekraczała wartości maksymalnej określonej w Dokumencie Transakcyjnym.

IBM może przeprowadzić kontrolę w celu sprawdzenia zgodności z maksymalną liczbą Aplikacji, Uprawnionych Uczestników i/lub Urządzeń Klienckich.

13. Okres obowiązywania i możliwości odnowienia

Okres obowiązywania Usługi Przetwarzania w Chmurze rozpoczyna się z datą powiadomienia Klienta przez IBM o udostępnieniu mu tej usługi zgodnie z dokumentem PoE. W dokumencie PoE określono, czy okres obowiązywania Usługi Przetwarzania w Chmurze jest automatycznie odnawiany, czy też usługa ta podlega kontynuacji na zasadzie nieprzerwanego używania lub jej świadczenie kończy się wraz z zakończeniem okresu obowiązywania.

Automatyczne odnawianie okresu obowiązywania Usługi Przetwarzania w Chmurze oznacza, że jest on automatycznie przedłużany na czas określony w dokumencie PoE, chyba że Klient złoży pisemne wypowiedzenie Usługi Przetwarzania w Chmurze co najmniej 90 dni przed datą wygaśnięcia okresu obowiązywania.

W przypadku kontynuacji na zasadzie nieprzerwanego używania dostępność Usługi Przetwarzania w Chmurze będzie przedłużana z miesiąca na miesiąc, chyba że Klient wypowie ją pisemnie z wyprzedzeniem co najmniej 90 dni. Usługa IBM SaaS pozostanie dostępna do końca miesiąca kalendarzowego przypadającego po upływie 90-dniowego okresu wypowiedzenia.

14. Oprogramowanie Pomocnicze

Ta Usługa Przetwarzania w Chmurze obejmuje oprogramowanie pomocnicze, z którego Klient może korzystać tylko w powiązaniu z tą usługą w okresie jej obowiązywania.

15. Coroczna podwyżka opłaty za subskrypcję IBM Trusteer

IBM zastrzega sobie prawo do korygowania opłaty za subskrypcję Usług Przetwarzania w Chmurze. Korekta opłaty za subskrypcję zostanie uwzględniona w cenach wykazanych w odpowiedniej Ofercie Cenowej za okres objęty tą Ofertą. Jeśli okres obowiązywania Usługi Przetwarzania w Chmurze zostanie przedłużony w ramach automatycznego odnowienia lub kontynuacji używania, mogą mieć zastosowanie również dodatkowe korekty opłaty za subskrypcję, wprowadzane nie częściej niż raz na 12 (dwanaście) miesięcy w wysokości ustalonej przez IBM, przy czym wartość procentowa takiej korekty nie może przekroczyć 3%. Taka korekta opłat nie wpływa na uprawnienia Klienta dotyczące Usług Przetwarzania w Chmurze ani na jednostkę miary służącą do obliczania opłat rozliczeniowych, według której można korzystać z Usługi Przetwarzania w Chmurze. Partnerzy Handlowi IBM są niezależni od IBM i jednostronnie ustalają swoje ceny i warunki.