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 Pinpoint Assure:

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

Usługi Przetwarzania w Chmurze Rapport:

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

Usługi Przetwarzania w Chmurze Pinpoint:

- IBM Trusteer Pinpoint Malware Detection Standard Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business

- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Rapport for Mitigation for Retail
- IBM Trusteer Rapport for Mitigation for Retail Premium Support
- IBM Trusteer Rapport for Mitigation for Business
- IBM Trusteer Rapport for Mitigation for Business Premium Support
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail Premium Support
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Project Management and Consultancy Services
- IBM Trusteer Security Research Consultancy Services
- IBM Trusteer Training Services
- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application
- IBM Trusteer Pinpoint Detect Standard
- IBM Trusteer Pinpoint Detect Premium
- IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect
- IBM Trusteer Pinpoint Verify

Usługi Przetwarzania w Chmurze Mobile:

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

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 II for Business
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer Mobile SDK for Business

1.1.2 Usługi Przetwarzania w Chmurze dla klientów indywidualnych

- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Mobile SDK for Retail

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 II

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

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

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 II for Business lub IBM Trusteer Rapport II for Retail.

1.1.4 Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do oferty IBM Trusteer Pinpoint Malware Detection II

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

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

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 usług 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 dostępne w odniesieniu do ofert IBM Trusteer Pinpoint Detect Standard, IBM Trusteer Pinpoint Detect Premium, IBM Trusteer Pinpoint Detect Standard for Retail, IBM Trusteer Pinpoint Detect Premium for Retail, IBM Trusteer Pinpoint Detect Standard for Business i/lub IBM Trusteer Pinpoint Detect Premium for Business

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:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
   - IBM Trusteer Digital Content Pack for Business
   - IBM Trusteer New Account Fraud for Business

b. 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:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
   - IBM Trusteer Digital Content Pack for Retail
   - IBM Trusteer New Account Fraud for Retail

c. Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do ofert IBM Trusteer Pinpoint Detect Standard i/lub IBM Trusteer Pinpoint Premium:
   - IBM Trusteer Pinpoint Detect Standard Application
   - IBM Trusteer Pinpoint Detect Premium Application

d. Dodatkowe Usługi Przetwarzania w Chmurze dostępne w odniesieniu do oferty IBM Trusteer Pinpoint Detect Premium
   - IBM Trusteer Pinpoint Verify

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

1.1.6 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 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.

1.3 Usługi Przetwarzania w Chmurze IBM Trusteer Rapport

1.3.1 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 lub Urządzenie Klienckie. W przypadku oferty biznesowej sprzedawane są pakiety obejmujące dziesięciu Uprawnionych Uczestników lub dziesięć Urządzeń Klienckich, a w przypadku oferty indywidualnej – stu Uprawnionych Uczestników lub sto Urządzeń Klienckich.

Niniejsza oferta Usług Przetwarzania w Chmurze obejmuje następujące komponenty:

a. Aplikacja 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.

1.3.2 Opcjonalne dodatkowe Usługi Przetwarzania w Chmurze dla ofert 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 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 lub Urządzeń Klienckich korzystających z Oprogramowania Klienckiego Posiadacza Konta, w przypadku których zostały zaakceptowane warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz nastąpiło uwierzytelnienie w jednej lub wielu Aplikacjach Biznesowych i/lub Indywidualnych Klienta, przy czym stosowana przez Klienta konfiguracja musi obejmować gromadzenie identyfikatorów użytkowników.

1.3.3 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.

Jedyną jednostką miary, według której naliczane są opłaty za uprawnienia do niniejszej Usługi, jest Uprawniony Uczestnik.

1.3.4 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.

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

Jednostką miary, według której naliczane są opłaty za usługi wsparcia na poziomie Premium do niniejszej Usługi Przetwarzania w Chmurze, jest Uprawniony Uczestnik lub Urządzenie Klienckie. W przypadku oferty biznesowej sprzedawane są pakiety obejmujące dziesięciu Uprawnionych Uczestników lub dziesięć Urządzeń Klienckich, a w przypadku oferty indywidualnej – stu Uprawnionych Uczestników lub sto Urządzeń Klienckich.

1.3.5 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.

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

1.3.6 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 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.

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

Aby wdrożyć usługę 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 usługę 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.

1.4 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 wchodzą następujące komponenty:

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.

1.4.1 IBM Trusteer Pinpoint Malware Detection

W przypadku wykrycia szkodliwego oprogramowania w ramach Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint Malware Detection II Klient jest zobowiązany postępować zgodnie z Podręcznikiem sprawdzonych procedur Pinpoint. Z Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint Malware 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 (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).

1.4.2 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 Security 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 for Business i/lub Advanced Edition for Retail 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

Wydania Standard Edition for Business i/lub Standard Edition for Retail to przeznaczone do szybkiego wdrożenia rozwiązania, które zapewniają 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.

1.4.3 Opcjonalne dodatkowe Usługi Przetwarzania w Chmurze dla ofert IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail, IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail, IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 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 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 II for Business lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

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

Celem usług IBM Trusteer Rapport Remediation for Retail i IBM Trusteer Rapport Remediation for Business 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 typu MitB 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 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.

1.4.5 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 wdrożonej usłudze 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 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.

IBM Trusteer Pinpoint Malware Detection Additional Applications: Wdrożenie usługi IBM Trusteer Pinpoint Malware Detection II Standard Edition lub IBM Trusteer Pinpoint Malware Detection II Advanced Edition w odniesieniu do dowolnej dodatkowej Aplikacji oprócz pierwszej Aplikacji wymaga nabycia uprawnienia do usługi IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.4.6 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 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.
- 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.

1.5 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 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 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).

1.5.1 IBM Trusteer Pinpoint Detect Standard for Retail i/lub IBM Trusteer Pinpoint Detect Standard for Business

Ta Usługa Przetwarzania w Chmurze łączy usługi IBM Trusteer Pinpoint Criminal Detection oraz IBM Trusteer Pinpoint Malware Detection w ramach jednego skonsolidowanego rozwiązania.

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 w odniesieniu do 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 Pinpoint Standard Premium Support.

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.

Usługa jest sprzedawana w pakietach po 100 Uprawnionych Uczestników lub 100 Połączeń. Jeśli Klient wybierze opcję zakupu według Połączeń, to opłata za Dodatkową Aplikację będzie naliczana począwszy od pierwszej aplikacji.

1.5.2 IBM Trusteer Pinpoint Detect Premium for Retail i/lub IBM Trusteer Pinpoint Detect Premium for Business

Ta Usługa Przetwarzania w Chmurze łączy usługi IBM Trusteer Pinpoint Criminal Detection oraz IBM Trusteer Pinpoint Malware Detection w ramach jednego skonsolidowanego rozwiązania.

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.

Oferta obejmuje rozwiązanie o rozszerzonym zakresie funkcji i usług, takich jak rozszerzone usługi wdrażania i konfigurowania, dostosowane strategie bezpieczeństwa, usługi badania incydentów itp. Klient uzyskuje dostęp do usług wdrażania z wykorzystaniem współużytkowanych zasobów dla każdej aplikacji w wymiarze 200 godzin oraz usług analizy bezpieczeństwa, również z wykorzystaniem współużytkowanych zasobów, w maksymalnym wymiarze 200 godzin dla każdej aplikacji po jej skonfigurowaniu. Usługi bieżące obejmują 20 godzin wdrażania i serwisowania dla każdej aplikacji

rocznie oraz 100 godzin badań w dziedzinie bezpieczeństwa dla każdej aplikacji rocznie. Każda dodatkowa czynność będzie podlegać opłacie.

Usługa Pinpoint Detect może wykorzystywać transakcje zarówno z kanałów mobilnych, jak i kanałów WWW. W przypadku transakcji mobilnych stosowana jest usługa Pinpoint nabywana według Połączeń. 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.

Usługi IBM Trusteer Pinpoint Detect Premium for Retail oraz Business są sprzedawane w pakietach po 100 Uprawnionych Uczestników. Usługa IBM Trusteer Pinpoint Detect Premium jest sprzedawana w pakietach po 100 Połączeń. Jeśli Klient wybierze opcję zakupu według Połączeń, to opłata za Dodatkową Aplikację będzie naliczana począwszy od pierwszej aplikacji.

Pinpoint Detect Policy Manager

Funkcja Policy Manager wchodzi w skład usługi Pinpoint Detect Premium i jest udostępniana w środowisku IBM Trusteer utrzymywanym w chmurze, za pośrednictwem którego Klient (oraz nieograniczona liczba upoważnionych członków personelu) może: (i) projektować, testować i wdrażać w środowisku produkcyjnym logikę wykrywania oszustw; (ii) projektować raporty i panele kontrolne oraz (ii) wyświetlać, konfigurować i ustalać strategie bezpieczeństwa oraz strategie związane z wykrywaniem budzącej podejrzenia aktywności w Aplikacji klienta.

W celu aktywacji funkcji Policy Manager i zaawansowanego wsparcia obowiązkowego niezbędne są usługi konsultacji. Szczegółowe informacje o usługach konsultacji zostaną podane w osobnym zakresie prac.

W przypadku aktywacji funkcji Policy Manager IBM zastrzega sobie prawo do uzyskiwania dostępu do środowiska Klienta w celu świadczenia wsparcia w zakresie dostosowywania strategii Klienta w taki sposób, aby usunąć poważne problemy wynikające ze zmian takich strategii.

Klient zobowiązuje się zapewnić ochronę wszelkich danych udostępnianych za pośrednictwem funkcji Policy Manager przed niewłaściwym użytkowaniem.

Jeśli zostanie aktywowana funkcja Policy Manager, Klient musi wykonywać instrukcje IBM dotyczące konfiguracji reguł zgodnie z opisem podanym w dokumentacji. Klient potwierdza, że IBM nie ponosi odpowiedzialności za sytuacje spowodowane nieprzestrzeganiem tych zaleceń przez Klienta.

Wszelkie problemy polegające na pogorszeniu stabilności lub dostępności usługi, które wynikają z błędnej konfiguracji funkcji Policy Manager przez Klienta, są wyłączone z czasu Przestoju wykorzystywanego w obliczeniach na potrzeby umowy dotyczącej poziomu usług.

1.5.3 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 albo IBM Trusteer Pinpoint Detect Standard.

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

- Usługa IBM Trusteer Rapport for Mitigation for Retail 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.

- Usługa IBM Trusteer Rapport for Mitigation for Business 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 Biznesowej 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 Biznesowej Klienta. Klient może korzystać z niniejszej Usługi Przetwarzania w Chmurze wyłącznie w powiązaniu z Uprawnionymi Uczestnikami uzyskującymi dostęp do Aplikacji Biznesowej 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 Business 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 Biznesowych 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.

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

Oferta obejmuje dostęp do usług wdrażania z wykorzystaniem współużytkowanych zasobów dla każdej aplikacji w wymiarze 200 godzin oraz usług analizy bezpieczeństwa, również z wykorzystaniem współużytkowanych zasobów, w maksymalnym wymiarze 200 godzin dla każdej aplikacji przy jej konfigurowaniu. Usługi bieżące obejmują 20 godzin wdrażania i serwisowania dla każdej aplikacji rocznie oraz 100 godzin badań w dziedzinie bezpieczeństwa dla każdej aplikacji rocznie.

- Aby wdrożyć ofertę IBM Trusteer Pinpoint Detect 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 Detect 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 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.
- 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.

1.5.6 IBM Trusteer Pinpoint Detect Standard Application i/lub IBM Trusteer Pinpoint Detect Premium Application

Ta oferta ma zastosowanie do kanałów WWW i kanałów mobilnych.

Oferta obejmuje dostęp do usług wdrażania z wykorzystaniem współużytkowanych zasobów dla każdej aplikacji w wymiarze 200 godzin oraz usług analizy bezpieczeństwa, również z wykorzystaniem współużytkowanych zasobów, w maksymalnym wymiarze 200 godzin dla każdej aplikacji przy jej

konfigurowaniu. Usługi bieżące obejmują 20 godzin wdrażania i serwisowania dla każdej aplikacji rocznie oraz 100 godzin badań w dziedzinie bezpieczeństwa dla każdej aplikacji rocznie.

- Wdrożenie usługi IBM Trusteer Pinpoint Detect Standard wymaga nabycia uprawnień IBM Trusteer Pinpoint Detect Standard Application w odniesieniu do każdej Aplikacji.
- Wdrożenie usługi IBM Trusteer Pinpoint Premium wymaga nabycia uprawnień IBM Trusteer Pinpoint Detect Premium Application w odniesieniu do każdej Aplikacji.

1.5.7 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 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.

1.5.8 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support i/lub IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Klienci, którzy nabywają Usługę Przetwarzania w Chmurze Pinpoint Detect Standard, mogą również nabyć ofertę Premium Support. Zakres usług Premium Support został określony poniżej w paragrafie 4.

1.5.9 IBM Trusteer Digital Content Pack for Retail i/lub IBM Trusteer Digital Content Pack for Business

Usługa IBM Trusteer Digital Content Pack umożliwia analitykom ds. bezpieczeństwa integrowanie nowych modeli przeciwdziałania oszustwom oraz zapewnia pełne wsparcie podczas tworzenia i modyfikowania doraźnych modeli reagowania na coraz bardziej zaawansowane zagrożenia. Obejmuje obszerny zbiór reguł, danych analitycznych i strategii, które można nabyć jako dodatkową i integralną część rozwiązania. Digital Content Pack pozwala na jeszcze ściślejszą integrację między funkcjami zapobiegania oszustwom cyfrowym oferowanymi przez Trusteer a kanałami płatności bezgotówkowych IBM Safer Payments. Dzięki wykorzystaniu wbudowanych reguł i specyficznej logiki biznesowej usługa Digital Content Pack umożliwia bankom i innym instytucjom finansowym rozszerzanie istniejących funkcji wykrywania oszustw i zapobiegania im.

Usługa IBM Trusteer Digital Content Pack for Retail jest dostępna w pakietach po 100 Uprawnionych Uczestników, a usługa IBM Trusteer Digital Content Pack for Business – w pakietach po 10 Uprawnionych Uczestników.

W przypadku integrowania usługi Digital Content Pack z rozwiązaniami Pinpoint Detect oraz IBM Safer Payments, a także w przypadku usług wymagających szczególnej uwagi niezbędne są usługi konsultacji. Usługi konsultacji nabywa się osobno, na podstawie odrębnego zakresu prac.

1.5.10 IBM Trusteer New Account Fraud for Retail i/lub IBM Trusteer New Account Fraud for Business

Usługa ta, dostępna dla subskrybentów usługi Pinpoint, została zaprojektowana z myślą o wykrywaniu nieprawidłowości, oznaczaniu podejrzanych działań oraz wczesnym generowaniu alertów podczas tworzenia nowych kont. Monitoruje ona nowe konta w celu rozpoznawania nowych działań mogących wskazywać na oszustwa, związanych z tworzeniem profili kont osób młodych oraz operacjami na kontach. Usługa generuje wczesne ostrzeżenia wskazujące, że takie nowe konto może być założone na podstawioną osobę lub wykorzystane w celu dokonywania oszustw, i przekazuje te ostrzeżenia za pośrednictwem raportów dotyczących używania usługi, dostępnych w aplikacji TMA.

Usługi IBM Trusteer New Account Fraud for Retail i IBM Trusteer New Account Fraud for Business można nabywać w pakietach po 10 Wywołań API.

1.5.11 IBM Trusteer Pinpoint Verify

Aby nabyć subskrypcję na tę Usługę Przetwarzania w Chmurze, Klient musi już posiadać subskrypcję usługi IBM Trusteer Pinpoint Detect Premium.

Niniejsza Usługa Przetwarzania w Chmurze umożliwia stosowanie drugiego składnika uwierzytelniania użytkowników w celu weryfikacji ich tożsamości podczas uzyskiwania dostępu do usługi cyfrowej.

Możliwość ta jest dostępna dla konfiguracji Pinpoint Detect Premium i ma na celu wprowadzenie drugiego składnika uwierzytelniania dla chronionych aplikacji. Decyzja o tym, kiedy żądać od użytkowników drugiego składnika uwierzytelniania, jest podejmowana przez chronioną aplikację i może opierać się na zaleceniach zwróconych przez platformę Pinpoint Detect Premium lub na jakichkolwiek innych zasadach zdefiniowanych przez chronioną aplikację.

1.6 IBM Trusteer Pinpoint Assure

Usługa ta oznakowuje podejrzane działania i generuje alerty w trakcie tworzenia lub rejestracji nowych kont. Monitoruje proces rejestracji kont w celu rozpoznania działań mogących wskazywać na oszustwa. Generuje wczesne ostrzeżenia wskazujące, że nowe konto może być założone na podstawioną osobę lub wykorzystane w celu dokonywania oszustw, i przekazuje te ostrzeżenia za pośrednictwem raportów dotyczących używania usługi, dostępnych w aplikacji TMA.

Usługa IBM Trusteer Pinpoint Assure jest sprzedawana w pakietach po 100 Połączeń.

1.6.1 Usługi opcjonalne związane z usługami IBM Trusteer Pinpoint Assure

1.6.2 IBM Trusteer Pinpoint Assure Application

Wdrożenie usługi IBM Trusteer Pinpoint Assure w odniesieniu do każdej Aplikacji wymaga nabycia uprawnienia IBM Trusteer Pinpoint Assure Application.

Usługa IBM Trusteer Pinpoint Assure jest sprzedawana według aplikacji.

1.6.3 IBM Trusteer Mobile Carrier Intelligence i/lub IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Aby nabyć subskrypcję na tę Usługę Przetwarzania w Chmurze, Klient musi już posiadać subskrypcję usługi IBM Trusteer Pinpoint Assure lub IBM Trusteer Pinpoint Detect.

Ta Usługa Przetwarzania w Chmurze rozszerza usługę IBM Trusteer Pinpoint Assure i/lub IBM Trusteer Pinpoint Detect, udostępniając dodatkowe informacje i kontekst w związku z numerami telefonów komórkowych przekazanymi do jednej z tych Usług Przetwarzania w Chmurze. Ułatwia to ocenę ryzyka oszustwa zachodzącego w danej sesji. Klient może wysyłać do Usługi Przetwarzania w Chmurze zapytania dotyczące charakterystyki danego numeru telefonu komórkowego, na przykład informacji o operatorze powiązanych z tym numerem.

Dane dotyczące numerów telefonów komórkowych udostępnione przez tę Usługę Przetwarzania w Chmurze („Analiza Danych Komórkowych”) mogą być wykorzystywane wyłącznie do celów wewnętrznych Klienta i przechowywane nie dłużej niż 30 (trzydzieści) dni. Po upływie tego okresu Klient musi wysłać do Usługi Przetwarzania w Chmurze ponowne zapytanie o ten sam numer telefonu komórkowego, aby uzyskać Analizę Danych Komórkowych na jego temat; niedozwolone jest ponowne wykorzystywanie Analizy Danych Komórkowych uzyskanych w ramach poprzedniego zapytania. Klient nie jest uprawniony do buforowania Analizy Danych Komórkowych w sposób inny niż określony powyżej, a także do jej ponownego wykorzystywania ani używania w całości lub w części w połączeniu z funkcjami eksploracji danych lub w celu archiwizacji jakiejkolwiek jej części.

1.7 IBM Trusteer Remotely Delivered Services

Usługi IBM Trusteer Remotely Delivered Services są dostępne jako opcjonalny moduł dodatkowy do Usług Przetwarzania w Chmurze Pinpoint Detect Premium i Pinpoint Assure.

1.7.1 IBM Trusteer Project Management and Consultancy Services

Ta oferta obejmuje maksymalnie 200 (dwieście) godzin usług konsultacji, w czasie których IBM wykona niektóre lub wszystkie spośród wymienionych poniżej zadań:

a. Usługi początkowego konfigurowania: częste spotkania okresowe, usługi zarządzania projektami.

b. Funkcja Policy Manager: bieżące wsparcie.

Usługi te można nabyć według Przedsięwzięcia.

1.7.2 IBM Trusteer Security Research Consultancy Services

Ta usługa konsultacji obejmuje maksymalnie 200 godzin dostępu do współużytkowanych zasobów na potrzeby analizy bezpieczeństwa. Umożliwia ona skorzystanie z dodatkowych usług, uzupełniających wybrane rozwiązanie oraz wsparcie na poziomie premium, a w jej skład wchodzą następujące elementy:

a. Rozszerzone badania w celu wykrywania oszustw: cotygodniowe spotkania i szkolenia.

b. Priorytetowe wsparcie wersji używanej przez Klienta.

c. Bieżące badania oparte na niestandardowych regułach i wsparcie.

Usługi te można nabyć według Przedsięwzięcia.

1.7.3 IBM Trusteer Training Services

Te usługi konsultacji zostały zaprojektowane z myślą o udostępnieniu dodatkowych usług oprócz zdefiniowanego rozwiązania i wsparcia premium (o ile ma to zastosowanie); obejmują usługi szkoleniowe dla pracowników Klienta w zakresie oferty Trusteer.

Usługi te można nabyć według Przedsięwzięcia.

1.8 Usługi Przetwarzania w Chmurze IBM Trusteer Mobile

1.8.1 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, przy czym 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 następującymi warunkami:

   - 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 lub 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 nie gwarantuje, że aplikacje lub dane wyjściowe wytworzone z użyciem narzędzi mobilnych wchodzących w skład pakietu IBM Security Mobile SDK będą zgodne operacyjnie, kompatybilne lub zdolne funkcjonować w połączeniu z konkretnym systemem operacyjnym platformy mobilnej lub konkretnym urządzeniem mobilnym.

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”). 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.

2. Ochrona Zawartości i danych

Specyfikacja techniczna dotycząca Przetwarzania i Ochrony Danych (zwana dalej „Specyfikacją Techniczną”) określa informacje odnoszące się do konkretnej Usługi Przetwarzania w Chmurze i precyzujące, jakie rodzaje Zawartości mogą być przetwarzane przez daną Usługę, jakie czynności przetwarzania są realizowane, jakie są opcje ochrony danych, a także jakie są szczegółowe zasady przechowywania i zwrotu Zawartości. Wszelkie szczegółowe informacje lub wyjaśnienia i terminy, w tym

obowiązki Klienta, związane z korzystaniem z Usługi Przetwarzania w Chmurze oraz opcjami ochrony danych (jeśli są dostępne) zostaną przedstawione w tym paragrafie. W zależności od opcji wybranych przez Klienta korzystanie z Usługi Przetwarzania w Chmurze może być regulowane przez więcej niż jedną Specyfikację Techniczną. Specyfikacja Techniczna może być dostępna tylko w języku angielskim, bez tłumaczenia na język miejscowy. Strony uzgadniają, bez względu na praktykę prawa miejscowego oraz zwyczaje lokalne, że znają język angielski i że jest to właściwy język w odniesieniu do nabywania Usług Przetwarzania w Chmurze oraz korzystania z nich. Do Usługi Przetwarzania w Chmurze oraz opcji dostępnych w jej ramach mają zastosowanie określone poniżej Specyfikacje Techniczne. Klient potwierdza, że i) IBM może co pewien czas modyfikować Specyfikacje Techniczne według własnego uznania oraz ii) takie modyfikacje zastąpią wcześniejsze wersje. Celem modyfikacji Specyfikacji Technicznych jest i) doprecyzowanie lub lepsze objaśnienie zobowiązań, ii) zapewnienie zgodności z aktualnie obowiązującymi standardami i przepisami prawa lub iii) dodanie nowych zobowiązań. Żadne modyfikacje Specyfikacji Technicznych nie umniejszą w znacznym stopniu ochrony danych w Usłudze Przetwarzania w Chmurze.

Odsyłacze do odpowiednich Specyfikacji Technicznych:

IBM Trusteer Mobile SDK

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

IBM Trusteer Mobile Secure Browser

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492579396

IBM Trusteer Pinpoint Assure

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=CF0C527046E011E8ADCBA344DE8FB657

IBM Trusteer Pinpoint Criminal Detect

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

IBM Trusteer Pinpoint Detect

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

IBM Trusteer Pinpoint Malware Detection

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

IBM Trusteer Rapport

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402483908375

IBM Trusteer Pinpoint Verify

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

(Specyfikacja techniczna usługi IBM Cloud Identity Verify odzwierciedla specyfikację usługi IBM Trusteer Pinpoint Verify).

Klient odpowiada za podjęcie niezbędnych działań w celu zamówienia, aktywacji lub zastosowania dostępnych opcji ochrony danych w odniesieniu do Usługi Przetwarzania w Chmurze. Klient przyjmuje odpowiedzialność za używanie Usług Przetwarzania w Chmurze w przypadku niepodjęcia tych działań, w tym odpowiedzialność związaną z przestrzeganiem przepisów o ochronie danych lub innych przepisów prawa mających zastosowanie do Zawartości.

Jeśli do Zawartości stosuje się ogólne rozporządzenie o ochronie danych (RODO – UE/2016/679), to w zakresie, w jakim przepisy te mają zastosowanie do danych osobowych uwzględnionych w Zawartości, obowiązuje Dodatek dotyczący Przetwarzania Danych IBM (DPD) dostępny pod adresem http://ibm.com/dpa oraz Załączniki szczegółowe do DPD przywołane w niniejszej Umowie jako jej część. Odpowiednie Specyfikacje Techniczne do niniejszej Usługi Przetwarzania w Chmurze będą pełnić rolę

Załączników Szczegółowych do Dodatku dotyczącego Przetwarzania Danych. Jeśli obowiązuje DPD, to obowiązek powiadamiania przez IBM Podwykonawców Podmiotu Przetwarzającego o zmianach oraz prawo Klienta do sprzeciwu wobec takich zmian będą stosowane w sposób określony w DPD.

2.1 Umowa Licencyjna z Użytkownikiem Końcowym i podstawa przetwarzania danych Podmiotów Danych

W przypadku Usług Przetwarzania w Chmurze IBM Trusteer Rapport (w tym Rapport Remediation lub Rapport for Mitigation) wdrażanych w połączeniu z Usługami Przetwarzania w Chmurze Pinpoint:

O ile nie uzgodniono inaczej, zgodnie z podstawą przetwarzania, którą Klient określił w sposób niezależny, Klient upoważnia IBM do udostępniania Umowy Licencyjnej z Użytkownikiem Końcowym dostępnej pod adresem https://www.trusteer.com/support/end-user-license-agreement w celach związanych z gromadzeniem i przetwarzaniem przez IBM informacji niezbędnych do świadczenia Usług Przetwarzania w Chmurze.

2.2 Wykorzystanie danych

IBM nie będzie wykorzystywać ani ujawniać rezultatów używania Usługi Przetwarzania w Chmurze przez Klienta, które występują wyłącznie w Zawartości (Rezultatach) Klienta lub w inny sposób umożliwiają jego identyfikację. IBM może jednak wykorzystywać Zawartość oraz oparte na niej informacje (z wyjątkiem Rezultatów) uzyskane w trakcie świadczenia Usługi Przetwarzania w Chmurze, pod warunkiem że usunie z nich identyfikatory osób, tak aby przypisanie danych osobowych do konkretnych osób bez dodatkowych informacji nie było już możliwe. IBM będzie wykorzystywać takie dane wyłącznie do celów związanych z badaniami, testami i tworzeniem ofert.

2.3 Przetwarzanie i przechowywanie danych

2.3.1 Informacje o dodatkowych miejscach przetwarzania

W przypadku usług Trusteer Pinpoint Verify wszystkie lokalizacje udostępniania usług serwerowych i przetwarzania są wyszczególnione w odpowiedniej Specyfikacji Technicznej.

W przypadku wszystkich pozostałych usług świadczonych za pośrednictwem centrum przetwarzania danych w Niemczech IBM ograniczy przetwarzanie Danych Osobowych do kraju Podmiotu IBM zawierającego Umowę oraz następujących krajów: Niemcy, Izrael, Irlandia, Holandia, a także do pozostałych krajów wymienionych na liście w odpowiedniej specyfikacji technicznej IBM dotyczącej Podwykonawców Podmiotu Przetwarzającego będących osobami trzecimi.

W przypadku wszystkich pozostałych usług świadczonych za pośrednictwem centrum przetwarzania danych w Japonii IBM ograniczy przetwarzanie Danych Osobowych do kraju Podmiotu IBM zawierającego Umowę oraz następujących krajów: Japonia, Izrael, Irlandia, a także do pozostałych krajów wymienionych na liście w odpowiedniej specyfikacji technicznej IBM dotyczącej Podwykonawców Podmiotu Przetwarzającego będących osobami trzecimi.

W przypadku wszystkich pozostałych usług świadczonych za pośrednictwem centrum przetwarzania danych w Stanach Zjednoczonych IBM ograniczy przetwarzanie Danych Osobowych do kraju Podmiotu IBM zawierającego Umowę oraz następujących krajów: Stany Zjednoczone, Izrael, Irlandia, Singapur, Australia, a także do pozostałych krajów wymienionych na liście w odpowiedniej specyfikacji technicznej IBM dotyczącej Podwykonawców Podmiotu Przetwarzającego będących osobami trzecimi.

Usługi wsparcia i serwisowania kont IBM Trusteer mogą być również udostępniane w razie potrzeby, w miarę dostępności odpowiedniego personelu IBM, lokalizacji Klienta oraz centrum przetwarzania danych, w którym przechowywane są odpowiednie dane.

2.3.2 Dane Posiadacza Konta

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.

2.3.3 Zintegrowane rozwiązania

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.

3. 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.

3.1 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.

3.2 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)**
< 99,9%	2%
< 99,0%	5%
< 95,0%	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 usług oraz powiązane z nimi uznania z tytułu wyrównań 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

4. 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 za dodatkową opłatą jest dostępna subskrypcja Wsparcia Premium; wyjątek stanowią **Usługi Przetwarzania w Chmurze IBM Trusteer Mobile SDK** oraz **Usługi Przetwarzania w Chmurze IBM Trusteer Rapport Mandatory Service**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital Content Pack** i **IBM Trusteer Mobile Carrier Intelligence**. Prosimy o kontakt z przedstawicielem handlowym 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)” dostępnym pod adresem https://www.ibm.com/software/support/saas_support_guide.html.
- Klient może uzyskiwać 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

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)”.

- Klient może uzyskiwać dostęp do powiadomień, dokumentów, raportów z wdrożeń i często zadawanych pytań w Portalu Obsługi Klienta pod adresem: http://www.ibm.com/software/security/trusteer/support/.
- Wykaz opcji wsparcia oraz inne szczegółowe informacje można znaleźć w „Podręczniku wsparcia dla usługi IBM Software as a Service (SaaS)" dostępnym pod adresem: https://www.ibm.com/software/support/saas_support_guide.html.

5. Informacje o uprawnieniach i rozliczaniu

5.1 Opłaty rozliczeniowe

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

- Jednostką miary, według której można korzystać z usług, jest Przedsięwzięcie. Przedsięwzięcie obejmuje usługi specjalistyczne i/lub szkoleniowe związane z Usługą Przetwarzania w Chmurze. Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę każdego Przedsięwzięcia.
- 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 podmioty uprawnione do uczestnictwa w wielu programach 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.
- 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.
- 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.
- Jednostką miary, według której można korzystać z Usługi Przetwarzania w Chmurze, jest Wywołanie API. Wywołanie API oznacza odwołanie do Usługi Przetwarzania w Chmurze za pośrednictwem interfejsu programowania. Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę łącznej liczby Wywołań API, zaokrąglonej w górę do dziesięciu, w okresie pomiarowym określonym w dokumencie Proof of Entitlement (PoE) lub w Dokumencie Transakcyjnym.

- Jednostką miary, według której można korzystać z Usługi Przetwarzania w Chmurze, jest Połączenie. Połączenie to łącze lub powiązanie między bazą danych, aplikacją, serwerem lub innym typem urządzenia a Usługą Przetwarzania w Chmurze. Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę łącznej liczby Połączeń nawiązywanych z Usługą Przetwarzania w Chmurze w okresie pomiarowym wyszczególnionym w dokumencie PoE lub Dokumencie Transakcyjnym Klienta.

  Na potrzeby niniejszej Usługi Przetwarzania w Chmurze Połączenie oznacza sesję lub przepływ w Aplikacji Klienta.

5.2 Opłaty za przekroczenie limitu

Jeśli rzeczywiste wykorzystanie Usługi Przetwarzania w Chmurze w okresie pomiarowym przekroczy uprawnienia określone w dokumencie PoE, to w miesiącu następującym po takim przekroczeniu Klientowi zostanie naliczona opłata za przekroczenie limitu zgodnie z postanowieniami Dokumentu Transakcyjnego.

5.3 Częstotliwość rozliczeń

Na początku okresu rozliczeniowego, zgodnie z wybraną częstotliwością rozliczeń IBM będzie wystawiać Klientowi faktury z tytułu należnych opłat, z wyjątkiem opłat za przekroczenie limitu i opłat za faktyczne wykorzystanie, które będą rozliczane z dołu.

6. 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 zostanie określone, czy Usługa Przetwarzania w Chmurze będzie odnawiana automatycznie, kontynuowana na zasadzie nieprzerwanego używania czy zakończona po upływie okresu jej obowiązywania.

W przypadku odnawiania automatycznego Usługa Przetwarzania w Chmurze będzie automatycznie przedłużana na okres wskazany w dokumencie PoE, chyba że Klient złoży pisemny wniosek o jej nieprzedłużanie co najmniej 90 dni przed datą jej wygaśnięcia. Z każdym odnowieniem wiąże się coroczny wzrost ceny, zgodnie z informacjami podanymi w wycenie. W przypadku automatycznego odnowienia po otrzymaniu powiadomienia od IBM o wycofaniu Usługi Przetwarzania w Chmurze, data zakończenia okresu odnowienia będzie przypadać na dzień zakończenia bieżącego okresu odnowienia lub dzień wycofania podany w powiadomieniu, w zależności od tego, która z tych dat przypada wcześniej.

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. Po zakończeniu takiego 90-dniowego okresu wypowiedzenia Usługa Przetwarzania w Chmurze będzie dostępna do końca miesiąca kalendarzowego.

7. Warunki dodatkowe

7.1 Postanowienia ogólne

Klient wyraża zgodę na publikowanie przez IBM w komunikatach reklamowych lub marketingowych informacji o Kliencie jako subskrybencie Usługi Przetwarzania w Chmurze.

Klient nie może używać Usługi Przetwarzania w Chmurze, osobno lub w połączeniu z innymi usługami lub produktami, w celu wykonywania następujących czynności wysokiego ryzyka: projektowanie, konstrukcja, kontrolowanie lub konserwacja obiektów jądrowych, systemów transportu masowego, systemów kontroli lotów, samochodowych systemów kontrolnych, systemów uzbrojenia, nawigacji lotniczej lub lotniczych systemów komunikacyjnych, ani też do wykonywania innych czynności, w przypadku których awaria Usługi Przetwarzania w Chmurze mogłaby spowodować ryzyko śmierci lub poważnego uszczerbku na zdrowiu.

7.2 Oprogramowanie pomocnicze

Usługa Przetwarzania w Chmurze wymaga zastosowania oprogramowania pomocniczego, które Klient pobiera do swoich systemów, aby ułatwić sobie korzystanie z tej usługi. Klient może używać oprogramowania pomocniczego wyłącznie w połączeniu z Usługą Przetwarzania w Chmurze. Oprogramowanie pomocnicze jest dostarczane w stanie, w jakim się znajduje („AS-IS”).

7.3 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.