„IBM Trusteer Fraud Protection“

Šiame Paslaugos apraše apibūdinta „Cloud Service“, kurią IBM pateikia Klientui. Klientas reiškia susitariančiąją šalį, jos įgaliotuosius vartotojus ir „Cloud Service“ gavėjus. Atitinkamas Pasiūlymas ir Teisių suteikimo dokumentas (TSD) pateikiami kaip atskiri Operacijų dokumentai.

1. „Cloud Service“

Šis Paslaugos aprašas taikomas šiems „Cloud Services“ pasiūlymams:

„Rapport Cloud Services“:

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

„Pinpoint Cloud Services“:

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

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

„Cloud Services“ mobiliesiems:

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

- „IBM Trusteer Mobile Browser for Retail Premium Support“

1.1 Verslo ir Mažmeninės prekybos „Cloud Services“

„IBM Trusteer Cloud Services“ suteikiamos naudoti su tam tikrų tipų Taikomosiomis programomis. Programa priskiriama vienam iš iš dviejų tipų: Mažmeninės prekybos arba Verslo. Mažmeninės prekybos ir Verslo programoms taikomi atskiri pasiūlymai.

a. Verslo programa apibrėžiama kaip internetinės bankininkystės programa, mobilioji programa arba el. komercijos programa, sukurta klientams aptarnauti. Kliento politika gali priskirti tam tikras mažas įmones kaip galinčias naudoti mažmeninės prekybos sprendimus.

b. Verslo programa apibrėžiama kaip internetinės bankininkystės programa, mobilioji programa arba el. komercijos programa, sukurta aptarnauti korporacinius, institucinius ar lygiaverčius objektus arba visas programas, kurios nėra priskiriamos Mažmeninei prekybai.

1.1.1 Verslo „Cloud Services“

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

1.1.2 Mažmeninės prekybos „Cloud Services“

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

Visuose Verslo ir Mažmeninės prekybos „Cloud Services“ pasiūlymuose susijęs „Premium Support“ produktas prieinamas už papildomą mokestį, išskyrus „IBM Trusteer Mobile SDK“ „Cloud Services“ pasiūlymus.

1.1.3 Papildomos „Cloud Services“, skirtos „IBM Trusteer Rapport“

a. Papildomos „Cloud Services“, skirtos „IBM Trusteer Rapport for Business“:
   - „IBM Trusteer Rapport Fraud Feeds for Business“
   - „IBM Trusteer Rapport Phishing Protection for Business“
   - „IBM Trusteer Rapport Mandatory Service for Business“
   - „IBM Trusteer Rapport Additional Applications For Business“

b. Papildomos „Cloud Services“, skirtos „IBM Trusteer Rapport for Retail“:
   - „IBM Trusteer Rapport Fraud Feeds for Retail“
   - „IBM Trusteer Rapport Phishing Protection for Retail“
   - „IBM Trusteer Rapport Mandatory Service for Retail“
   - „IBM Trusteer Rapport Additional Applications For Retail“

Visuose „IBM Trusteer Rapport Cloud Services“ Verslo ir Mažmeninės prekybos prieduose, išskyrus „IBM Trusteer Rapport Mandatory Service“ priedus, susijęs „Premium Support“ produktas prieinamas už papildomą mokestį.

„IBM Trusteer Rapport for Business“ arba „IBM Trusteer Rapport for Retail“ prenumerata yra šiame skyriuje išvardytų susietų papildomų „Cloud Services“ būtinoji sąlyga.

1.1.4 Papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Malware Detection“ ir (arba) „IBM Trusteer Pinpoint Malware Detection II“

a. Papildomos „Cloud Services“, galimos „IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition“, „IBM Trusteer Pinpoint Malware Detection for Business Standard Edition“, „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business“ arba „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business“:
   - „IBM Trusteer Pinpoint Carbon Copy for Business“
   - „IBM Trusteer Rapport Remediation for Business“
   - „IBM Trusteer Pinpoint Malware Detection Additional Applications for Business“

b. Papildomos „Cloud Services“ galimos „IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition“, „IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition“, „IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition“ arba „IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition“:
   - „IBM Trusteer Pinpoint Carbon Copy for Retail“
   - „IBM Trusteer Rapport Remediation for Retail“
   - „IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail“

„Premium support“ gali būti teikiamas konkretiems pasiūlymams, kaip nurodyta šiame dokumente. „IBM Trusteer Pinpoint Malware Detection for Business“, „IBM Trusteer Pinpoint Malware Detection for Retail“, „IBM Trusteer Pinpoint Malware Detection II for Business“ arba „IBM Trusteer Pinpoint Malware Detection II for Retail“ prenumerata yra šiame skyriuje išvardytų susietų papildomų „Cloud Services“ būtina sąlyga.

1.1.5 Papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Criminal Detection“ ir (arba) „IBM Trusteer Pinpoint Criminal Detection II“

a. Papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Criminal Detection for Business“ arba „IBM Trusteer Pinpoint Criminal Detection II“
   - „IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business“

b. Papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Criminal Detection for Retail“ ir (arba) „IBM Trusteer Pinpoint Criminal Detection II for Retail“:
   - „IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail“

„Premium support“ yra prieinamas konkretiems pasiūlymams, kaip nurodyta šiame dokumente.

„IBM Trusteer Pinpoint Criminal Detection for Business“, „IBM Trusteer Pinpoint Criminal Detection for Retail“, „IBM Trusteer Pinpoint Criminal Detection II for Business“ arba „IBM Trusteer Pinpoint Criminal Detection II for Retail“ prenumerata yra šiame skyriuje išvardytų susietų papildomų „Cloud Services“ būtina sąlyga.

1.1.6 Papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Detect Standard“, „IBM Trusteer Pinpoint Detect Premium“, „IBM Security Pinpoint Detect Standard with access management integration“ ir (arba) „IBM Security Detect Premium with access management integration“

a. Papildomos „Cloud Services“ galimos „IBM Trusteer Detect Standard for Business“, „IBM Trusteer Pinpoint Detect Premium for Business“, „IBM Security Pinpoint Detect Standard with access management integration for Business“ ir (arba) „IBM Security Detect Premium with access management integration for Business“:

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

b. Papildomos „Cloud Services“ galimos „IBM Trusteer Detect Standard for Retail“, „IBM Trusteer Pinpoint Detect Premium for Retail“, „IBM Security Pinpoint Detect Standard with access management integration for Retail“ ir (arba) „IBM Security Detect Premium with access management integration for Retail“:

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

„IBM Trusteer Detect Standard“, „IBM Trusteer Pinpoint Detect Premium“, „IBM Pinpoint Detect Standard with access management integration“ arba „IBM Security Detect Premium with access management integration“ prenumerata yra šiame skyriuje išvardytų susietų papildomų „Cloud Services“ būtina sąlyga.

1.1.7 Kitos papildomos „Cloud Services“

Visos papildomos prie pagrindinių prenumeratų pridedamos „Cloud Services“ prenumeratos, kurios čia neišvardytos ir yra šiuo metu galimos arba vis dar kuriamos, nėra laikomos naujinimu ir jas reikia suteikti atskirai.

1.2 Apibrėžtys

Terminas **Paskyros turėtojas** reiškia galutinį Kliento vartotoją, kuris įdiegė kliento programinę įrangą, sutiko su galutinio vartotojo licencijos sutartimi (EULA) ir bent kartą yra autentifikuotas kaip besinaudojantis Kliento Mažmeninės prekybos arba Verslo programa, kuriai skirtą „Cloud Services“ Klientas užsiprenumeravo.

Paskyros turėtojo Kliento programinė įranga reiškia „IBM Trusteer Rapport“ kliento programinę įrangą, „IBM Trusteer Mobile Browser“ kliento programinę įrangą arba bet kurią kitą kliento programinę įrangą, pateiktą kartu su kai kuriomis „Cloud Services“, diegiamomis galutinio vartotojo įrenginyje.

„Trusteer“ prisistatymo tinklalapis – tinklalapis, kuris Klientui suteikiamas remiantis galimais Prisistatymo tinklalapių šablonais.

Nukreipimo puslapis yra IBM priglobtas puslapis, kuris pateikiamas Klientui su prisistatymo tinklalapiu ir atsisiunčiama Paskyros turėtojo Kliento programine įranga.

2. „IBM Trusteer Rapport Cloud Services“

2.1 „IBM Trusteer Rapport for Retail“ ir (arba) „IBM Trusteer Rapport for Business“ („Trusteer Rapport“)

„Trusteer Rapport“ suteikia apsaugą nuo sukčiavimo apsimetant ir „Man-in-the-Browser“ („MitB“) kenkėjiškos programinės įrangos atakų. Naudodamas dešimtis milijonų galutinių taškų visame pasaulyje, „IBM Trusteer Rapport“ renka žinias apie aktyvias sukčiavimo apsimetant ir kenkėjiškos programinės įrangos atakas prie viso pasaulio organizacijas. „IBM Trusteer Rapport“ taiko elgsenos algoritmus, kad galėtų blokuoti sukčiavimo apsimetant atakas ir apsaugoti diegimą ir veikimą nuo „MitB“ kenkėjiškos programinės įrangos.

Ši „Cloud Service“ apima Priskirto dalyvio apskaitos sistemą. Verslo pasiūlymai parduodami paketais po 10 Priskirtų dalyvių. Mažmeninės prekybos pasiūlymai parduodami paketais po 100 Priskirtų dalyvių.

Šis „Cloud Service“ pasiūlymas apima:

a. „Trusteer Management Application“ (TMA):

   TMA prieinama „IBM Trusteer“ debesyje laikomoje aplinkoje, kurioje Klientas (ir neribotas įgaliotų darbuotojų skaičius) gali: (i) peržiūrėti ir atsisiųsti tam tikras įvykių duomenų ataskaitas bei rizikos vertinimus ir (ii) peržiūrėti kliento įgalinimo programinės įrangos (dar vadinama „Trusteer Rapport“ programinės įrangos paketu („Paskyros turėtojo Kliento programinė įranga“), nemokamai

licencijuotos Kliento Priskirtiems dalyviams pagal galutinio vartotojo licencijos sutartį (EULA), kurią galima atsisiųsti į Priskirtojo dalyvio kompiuterius ar įrenginius (asmeninius / MAC kompiuterius), konfigūraciją. Klientas gali reklamuoti Paskyros turėtojo Kliento programinę įrangą tik naudodamas „Trusteer“ prisistatymo tinklalapį arba „Rapport“ API, Klientas negali naudoti Paskyros turėtojo Kliento programinės įrangos vidiniams įmonės veiksmams atlikti ar leisti ja naudotis savo darbuotojams (ne darbuotojo asmeninio naudojimo tikslais).

b. Žiniatinklio scenarijus:

   Prieiga svetainėje norint pasiekti arba naudoti „Cloud Service“.

c. Įvykių duomenys:

   Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenis, sugeneruotus iš Paskyros turėtojo Kliento programinės įrangos kaip Paskyros turėtojo internetinės sąveikos su Verslo ar Mažmeninės prekybos programa, kuriai skirtas „Cloud Services“ Klientas užsiprenumeravo. Įvykių duomenys bus gaunami iš Priskirtų dalyvių Paskyros turėtojo Kliento programinės įrangos, veikiančios jų įrenginiuose. Dalyviai turi būti suutikę su EULA, bent kartą autentifikuoti kaip besinaudojantys Kliento Verslo ar Mažmeninės prekybos programa, o Kliento konfigūracijoje turi būti Vartotojo ID rinkinys.

d. „Trusteer“ prisistatymo tinklalapis:

   „Trusteer“ prisistatymo tinklalapio rinkodaros platforma atpažįsta ir reklamuoja Paskyros turėtojo Kliento programinę įrangą Priskirtiems dalyviams, turintiems prieigą prie Kliento Verslo ir (arba) Mažmeninės prekybos programų, kurioms skirtas „Cloud Services“ Klientas užsiprenumeravo. Klientas gali rinktis iš galimų Prisistatymo tinklalapio šablonų. Dėl pasirinktinio prisistatymo tinklalapio gali būti pasirašoma atskira sutartis arba įsipareigojimų aprašymas.

Klientas gali sutikti pateikti prekių ženklus, logotipus ar piktogramas, skirtas naudoti pagal TMA, naudoti tik su „Trusteer“ prisistatymo tinklalapiu, pateikti Paskyros turėtojo Kliento programinėje įrangoje arba IBM globojamuose nukreipimo puslapiuose ir „IBM Trusteer“ svetainėje. Visas pateiktų prekių ženklų, logotipų ar piktogramų naudojimas vykdomas remiantis pagrįsta IBM politika, susijusia su reklamavimu ir prekių ženklų naudojimu.

Klientas privalo užsiprenumeruoti „IBM Trusteer Rapport Mandatory Service Cloud Service“, jei Klientas nori taikyti bet kurio tipo privalomą Paskyros turėtojo Kliento programinės įrangos diegimą.

Paskyros turėtojo Kliento programinė įranga apima (neapsiribojant) visų tipų privalomą diegimą tų mechanizmų ar priemonių, kurios tiesiogiai ar netiesiogiai priverčia Priskirtą dalyvį atsisiųsti Paskyros turėtojo Kliento programinę įrangą, arba kokį nors metodą, įrankį ar procedūrą, sutartį arba mechanizmą, kurio IBM nesukūrė arba nepatvirtino ir kuris skirtas Paskyros turėtojo kliento programinės įrangos privalomo diegimo licencijavimo reikalavimams apeiti.

2.2 „IBM Trusteer Rapport II for Retail“ ir (arba) „IBM Trusteer Rapport II for Business“ („Trusteer Rapport II“)

„Trusteer Rapport II Cloud Service“ yra naujas „IBM Trusteer Rapport“ variantas, skirtas padėti standartizuoti mokesčius, susijusius su kelių Taikomųjų programų apsauga, kuris pakeičia vienkartinius mokesčius įtraukiant Taikomąsias programas.

„Trusteer Rapport II“ suteikia apsaugą nuo sukčiavimo apsimetant ir „Man-in-the-Browser“ („MitB“) kenkėjiškos programinės įrangos atakų. Naudodamas dešimtis milijonų galutinių taškų visame pasaulyje, „IBM Trusteer Rapport“ renka žinias apie aktyvias sukčiavimo apsimetant ir kenkėjiškos programinės įrangos atakas prie viso pasaulio organizacijas. „IBM Trusteer Rapport“ taiko elgsenos algoritmus, kad galėtų blokuoti sukčiavimo apsimetant atakas ir apsaugoti diegimą ir veikimą nuo „MitB“ kenkėjiškos programinės įrangos.

Ši „Cloud Service“ suteikiama pagal Priskirto dalyvio mokesčių apskaitos sistemą. Verslo pasiūlymai parduodami paketais po 10 Priskirtų dalyvių. Mažmeninės prekybos pasiūlymai parduodami paketais po 100 Priskirtų dalyvių.

Šis „Cloud Service“ pasiūlymas apima:

a. „Trusteer Management Application“ (TMA):

   TMA prieinama „IBM Trusteer“ debesyje laikomoje aplinkoje, kurioje Klientas (ir neribotas įgaliotų darbuotojų skaičius) gali: (i) peržiūrėti ir atsisiųsti tam tikras įvykių duomenų ataskaitas bei rizikos vertinimus ir (ii) peržiūrėti kliento įgalinimo programinės įrangos (dar vadinama „Trusteer Rapport“

programinės įrangos paketu („Paskyros turėtojo Kliento programinė įranga“), nemokamai licencijuotos Kliento Priskirtiems dalyviams pagal galutinio vartotojo licencijos sutartį (EULA), kurią galima atsisiųsti į Priskirtojo dalyvio kompiuterius ar įrenginius (asmeninius / MAC kompiuterius), konfigūraciją. Klientas gali reklamuoti Paskyros turėtojo Kliento programinę įrangą tik naudodamas „Trusteer“ prisistatymo tinklalapį arba „Rapport“ API, Klientas negali naudoti Paskyros turėtojo Kliento programinės įrangos vidiniams įmonės veiksmams atlikti ar leisti ja naudotis savo darbuotojams (ne darbuotojo asmeninio naudojimo tikslais).

b. Žiniatinklio scenarijus:

Prieiga svetainėje norint pasiekti arba naudoti „Cloud Service“.

c. Įvykių duomenys:

Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenis, sugeneruotus iš Paskyros turėtojo Kliento programinės įrangos kaip Paskyros turėtojo internetinės sąveikos su Verslo ar Mažmeninės prekybos programa, kuriai skirtas „Cloud Services“ Klientas užsiprenumeravo. Įvykių duomenys bus gaunami iš Priskirtų dalyvių Paskyros turėtojo Kliento programinės įrangos, veikiančios jų įrenginiuose. Dalyviai turi būti suutikę su EULA, bent kartą autentifikuoti kaip besinaudojantys Kliento Verslo ar Mažmeninės prekybos programa, o Kliento konfigūracijoje turi būti Vartotojo ID rinkinys.

d. „Trusteer“ prisistatymo tinklalapis:

„Trusteer“ prisistatymo tinklalapio rinkodaros platforma atpažįsta ir reklamuoja Paskyros turėtojo Kliento programinę įrangą Priskirtiems dalyviams, turintiems prieigą prie Kliento Verslo ir (arba) Mažmeninės prekybos programų, kurioms skirtas „Cloud Services“ Klientas užsiprenumeravo. Klientas gali rinktis iš galimų Prisistatymo tinklalapio šablonų. Dėl pasirinktinio prisistatymo tinklalapio gali būti pasirašoma atskira sutartis arba įsipareigojimų aprašymas.

Klientas gali sutikti pateikti prekių ženklus, logotipus ar piktogramas, skirtas naudoti pagal TMA, naudoti tik su „Trusteer“ prisistatymo tinklalapiu, pateikti Paskyros turėtojo Kliento programinėje įrangoje arba IBM globojamuose nukreipimo puslapiuose ir „IBM Trusteer“ svetainėje. Visas pateiktų prekių ženklų, logotipų ar piktogramų naudojimas vykdomas remiantis pagrįsta IBM politika, susijusia su reklamavimu ir prekių ženklų naudojimu.

Klientas privalo užsiprenumeruoti „IBM Trusteer Rapport Mandatory Service Cloud Service“, jei Klientas nori taikyti bet kurio tipo privalomą Paskyros turėtojo Kliento programinės įrangos diegimą.

Paskyros turėtojo Kliento programinė įranga apima (neapsiribojant) visų tipų privalomą diegimą tų mechanizmų ar priemonių, kurios tiesiogiai ar netiesiogiai priverčia Priskirtą dalyvį atsisiųsti Paskyros turėtojo Kliento programinę įrangą, arba kokį nors metodą, įrankį ar procedūrą, sutartį arba mechanizmą, kurio IBM nesukūrė arba nepatvirtino ir kuris skirtas Paskyros turėtojo kliento programinės įrangos privalomo diegimo licencijavimo reikalavimams apeiti.

„Trusteer Rapport II for Business“ ir (arba) „Trusteer Rapport II for Retail“ kiekvienas apima apsaugą vienai Taikomajai programai. Kiekvienai papildomai Taikomajai programai Klientas turi įsigyti „IBM Trusteer Rapport Additional Applications“ teises.

2.3 Pasirinktinės papildomos „Cloud Services“, skirtos „IBM Trusteer Rapport for Business“ ir (arba) „IBM Trusteer Rapport for Retail“ ir (arba) „IBM Trusteer Rapport II for Business“ ir (arba) „IBM Trusteer Rapport II for Retail“

„IBM Trusteer Rapport Cloud Services“ arba „IBM Trusteer Rapport II Cloud Services“ prenumerata yra būtina sąlyga prenumeruojant bet kurias iš toliau išvardytų papildomų „Cloud Services“. Jei „Cloud Service“ pažymėta kaip „Verslui“, tada papildomos įsigytos „Cloud Services“ taip pat turi būti pažymėtos kaip „Verslui“. Jei „Cloud Service“ pažymėta kaip „Mažmeninei prekybai“, įsigytos papildomos „Cloud Services“ taip pat turi būti pažymėtos kaip „Mažmeninei prekybai“. Klientas gaus įvykių duomenis iš Priskirtų dalyvių, pas kuriuos veikia Paskyros turėtojo Kliento programinė įranga ir kurie yra sutikę EULA, bent kartą yra autentifikuoti kaip besinaudojantys Kliento Verslo ir (arba) Mažmeninės prekybos programa (-omis), o Kliento konfigūracija turi apimti Vartotojo ID rinkinį.

2.3.1 „IBM Trusteer Rapport Fraud Feeds for Business“ ir (arba) „IBM Trusteer Rapport Fraud Feeds for Retail“

Prenumeruodamas šią papildomą „Cloud Service“ Klientas (ir neribotas jo įgaliotųjų darbuotojų skaičius) gali naudoti TMA norėdamas peržiūrėti, prenumeruoti ir konfigūruoti iš „Trusteer Rapport Cloud Service“

sugeneruotų grėsmių informacijos santraukų pristatymą. Informacijos santraukos gali būti siunčiamos priskirtu el. pašto adresu arba per SFTP kaip teksto failai.

2.3.2 „IBM Trusteer Rapport Phishing Protection for Business“ ir (arba) „IBM Trusteer Rapport Phishing Protection for Retail“

Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenų pranešimus, susijusius su Paskyros turėtojo prisijungimo kredencialų pateikimu įtartinoje apsimestinėje arba galimai apgaulingoje svetainėje. Teisėtos interneto programos (URL) per klaidą gali būti pažymėtos kaip apsimestinės svetainės, o „Cloud Service“ gali įspėti Paskyros turėtojus, kad teisėta svetainė yra apsimestinė. Tokiu atveju Klientas privalo pranešti IBM apie tokią klaidą, o IBM ją ištaisys. Tai bus vienitelė Kliento teisių gynybos priemonė šios kaidos atžvilgiu.

2.3.3 „IBM Trusteer Rapport Mandatory Service for Business“ ir (arba) „IBM Trusteer Rapport Mandatory Service for Retail“

Klientas gali naudoti „Trusteer“ prisistatymo tinklalapio rinkodaros platformos egzempliorių norėdamas suteikti teisę atsisiųsti Paskyros turėtojo Kliento programinę įrangą Priskirtiems dalyviams, galintiems pasiekti Kliento Verslo ir (arba) Mažmeninės prekybos programas, kurioms skirtas „Cloud Services“ Klientas užsiprenumeravo.

„IBM Trusteer Rapport Premium Support for Business“ yra būtina „IBM Security Rapport Mandatory Service for Business“ sąlyga.

„IBM Trusteer Rapport Premium Support for Retail“ yra būtina „IBM Security Rapport Mandatory Service for Retail“ sąlyga.

Klientas gali įdiegti „IBM Trusteer Rapport Mandatory Service“ papildomą funkciją tik tada, jei ji buvo užsakyta ir sukonfigūruota naudoti su Kliento Mažmeninės prekybos arba Verslo programa, kuriai skirtas „Cloud Services“ Klientas užsiprenumeravo.

2.3.4 „IBM Trusteer Rapport Large Redeployment“ ir (arba) „IBM Trusteer Rapport Small Redeployment“

Klientai, kurie iš naujo diegia savo internetinės bankininkystės Taikomąsias programas paslaugų naudojimo laikotarpiu ir kuriems dėl to reikia pakeisti savo „IBM Trusteer Rapport“ arba „IBM Trusteer Rapport II“ įdiegtį, privalo įsigyti „IBM Trusteer Rapport Redeployment Cloud Service“.

Jei Klientas pakeičia Taikomosios programos domeną ar pagrindinio kompiuterio URL, pakeičia prisistatymo konfigūraciją arba pereina į naują internetinės bankininkystės platformą, gali reikėti diegti iš naujo.

Diegimo iš naujo 6 mėnesių perėjimo laikotarpiu Klientui suteikiama teisė į papildomas Taikomąsias programas santykiu „vienas su vienu“, veikiančias šalia jau prenumeruojamų Taikomųjų programų.

„IBM Trusteer Rapport Large Redeployment“ taikomas aplinkoms, kuriose yra daugiau nei 20 000 vartotojų, o „IBM Trusteer Rapport Small Redeployment“ taikomas aplinkoms, kuriose yra 20 000 arba mažiau vartotojų.

2.3.5 „IBM Trusteer Rapport Additional Applications for Business“ ir (arba) „IBM Trusteer Rapport Additional Applications for Retail“

„IBM Trusteer Rapport II for Business“ diegiant bet kokioje papildomoje Verslo programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Rapport Additional Applications for Business Cloud Service“ teisės. „IBM Trusteer Rapport II for Retail“ diegiant bet kokioje papildomoje Mažmeninės prekybos programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Rapport Additional Applications for Retail Cloud Service“ teisės.

3. „IBM Trusteer Pinpoint Cloud Services“

„IBM Trusteer Pinpoint“ yra debesyje veikianti paslauga, sukurta suteikti dar vieną apsaugos sluoksnį ir skirta aptikti ir susilpninti kenkėjišką programinę įrangą, sukčiavimo apsimetant ir paskyrų perėmimo atakas. „Trusteer Pinpoint“ galima integruoti į Kliento Verslo ir (arba) Mažmeninės prekybos programas, kurioms skirtas „Cloud Services“ ir procesus, apsaugančius nuo apgaulės, Klientas užsiprenumeravo.

Ši „Cloud Service“ apima:

a. TMA:

   TMA galima rasti „IBM Trusteer“ debesyje laikomoje aplinkoje, kurioje Klientas (ir neribotas jo įgaliotų darbuotojų skaičius) gali: (i) peržiūrėti ir atsisiųsti tam tikras įvykių duomenų ataskaitas bei

rizikos vertinimus ir (ii) peržiūrėti, prenumeruoti ir konfigūruoti grėsmių informacijos santraukų, generuojamų iš „Pinpoint“ pasiūlymų, pristatymą.

b. Žiniatinklio scenarijus ir (arba) API:

Diegimas svetainėje norint pasiekti arba naudoti „Cloud Service“.

3.1 „IBM Trusteer Pinpoint Malware Detection“ ir „IBM Trusteer Pinpoint Criminal Detection“ geriausios praktikos

Aptikus kenkėjišką įrangą „IBM Trusteer Pinpoint Malware Detection Cloud Services“ arba „IBM Trusteer Pinpoint Malware Detection II Cloud Services“ arba paskyros perėmimą „IBM Trusteer Pinpoint Criminal Detection Cloud Services“ arba „IBM Trusteer Pinpoint Criminal Detection II Cloud Services“, Klientas privalo vadovautis „Pinpoint“ geriausios praktikos vadovu. Iš karto, aptikus kenkėjišką programinę įrangą arba paskyros perėmimą, nenaudokite „IBM Trusteer Pinpoint Malware Detection Cloud Services“, „IBM Trusteer Pinpoint Criminal Detection II Cloud Services“, „IBM Trusteer Pinpoint Criminal Detection Cloud Services“ arba „IBM Trusteer Pinpoint Criminal Detection II Cloud Services“ tokiu būdu, kuris paveiktų Priskirto dalyvio patirtį, taip, kad kiti galėtų susieti Kliento veiksmus su „IBM Trusteer Pinpoint Cloud Services“ naudojimu (pvz., perspėjimai, pranešimai, įrenginių blokavimas arba prieigos prie Verslo ir (arba) Mažmeninės prekybos programos blokavimas iš karto po kenkėjiškos programinės įrangos arba paskyros perėmimo aptikimo).

3.2 „IBM Trusteer Pinpoint Criminal Detection for Business“ ir (arba) „IBM Trusteer Pinpoint Criminal Detection for Retail“

Įtartinų paskyrų perėmimas klientui nedalyvaujant, naršyklių veikimas prisijungiant prie Verslo arba Mažmeninės prekybos programos, naudojant įrenginio ID, sukčiavimo apsimetant aptikimas ir kenkėjiškos programos aptikimas, kai bandoma pavogti kredencialus. „IBM Trusteer Pinpoint Criminal Detection Cloud Services“ suteikia dar vieną apsaugos sluoksnį, aptinka bandymus perimti paskyras ir pateikia naršyklių arba mobiliųjų įrenginių rizikos vertinimo balus (naudojant vietinę naršyklę arba Kliento mobiliąją programą), nes Verslo arba Mažmeninės prekybos programą tiesiogiai susieja su Klientu.

a. Įvykių duomenys:

Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenis, sugeneruotus kaip Priskirtų dalyvių internetinės sąveikos su Verslo ar Mažmeninės prekybos programa (-omis), kuriai (-ioms) skirtas „Cloud Services“ Klientas užsiprenumeravo, rezultatas, arba Klientas gali gauti įvykių duomenis naudodamas vidinės API pristatymo režimą.

3.3 „IBM Trusteer Pinpoint Criminal Detection II for Business“ ir (arba) „IBM Trusteer Pinpoint Criminal Detection II for Retail“

„IBM Trusteer Pinpoint Criminal Detection II“ yra naujas „IBM Trusteer Pinpoint Criminal Detection“ variantas, skirtas padėti standartizuoti mokesčius, susijusius su kelių Taikomųjų programų apsauga, kuris pakeičia vienkartinius mokesčius įtraukiant Taikomąsias programas.

Įtartinų paskyrų perėmimas klientui nedalyvaujant, naršyklių veikimas prisijungiant prie Verslo arba Mažmeninės prekybos programos, naudojant įrenginio ID, sukčiavimo apsimetant aptikimas ir kenkėjiškos programos aptikimas, kai bandoma pavogti kredencialus. „IBM Trusteer Pinpoint Criminal Detection II Cloud Services“ suteikia dar vieną apsaugos sluoksnį, aptinka bandymus perimti paskyras ir pateikia naršyklių arba mobiliųjų įrenginių rizikos vertinimo balus (naudojant vietinę naršyklę arba Kliento mobiliąją programą), nes Verslo arba Mažmeninės prekybos programą tiesiogiai susieja su Klientu.

a. Įvykių duomenys:

Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenis, sugeneruotus kaip Priskirtų dalyvių internetinės sąveikos su Verslo ar Mažmeninės prekybos programa (-omis), kuriai (-ioms) skirtas „Cloud Services“ Klientas užsiprenumeravo, rezultatas, arba Klientas gali gauti įvykių duomenis naudodamas vidinės API pristatymo režimą.

Ši „Cloud Service“ apima vienos Taikomosios programos apsaugą. Kiekvienai papildomai Taikomajai programai Klientas turi įsigyti „IBM Trusteer Pinpoint Criminal Detection Additional Applications“ teises.

3.4 „IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition“ ir (arba) „IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition“, ir (arba) „IBM Trusteer Pinpoint Malware Detection for Business Standard Edition“, ir (arba) „IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition“

„Man in the Browser“ („MitB“) į finansus nukreipta kenkėjiška programine įranga apkrėstos naršyklės aptikimas klientui nedalyvaujant, jungiantis prie Verslo ir (arba) Mažmeninės prekybos programos. „IBM Trusteer Pinpoint Malware Detection Cloud Services“ suteikia dar vieną apsaugos sluoksnį ir įgalina organizacijas atkreipti dėmesį į apsaugos nuo apgaulės (pagrįstos kenkėjiška programine įranga) procesus, pateikiant Klientui vertinimus ir įspėjimus apie „MitB“ finansinės kenkėjiškos programinės įrangos buvimą.

a. Įvykių duomenys:

   Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenis, sugeneruotus kaip Priskirtų dalyvių internetinės sąveikos su Verslo ar Mažmeninės prekybos programa (-omis).

b. Papildomas leidimas:

   Verslo ir (arba) Mažmeninės prekybos Papildomi leidimai suteikia papildomą aptikimo ir apsaugos sluoksnį, kuris koreguojamas ir pritaikomas prie Kliento Verslo ir (arba) Mažmeninės prekybos programų struktūros ir srauto. Jį galima pritaikyti prie konkrečios Klientui kylančios grėsmės aplinkos. Jį galima įtraukti į įvairias Kliento Verslo ir (arba) Mažmeninės prekybos programų vietas.

   Papildomas leidimas Klientui siūlomas minimaliais kiekiais: bent 100 000 Mažmeninės prekybos programos Priskirtų dalyvių arba 10 000 Verslo programos Priskirtų dalyvių, tai yra 1 000 paketų po 100 Mažmeninės prekybos programos Priskirtų dalyvių arba 1 000 paketų po 10 Verslo programos Priskirtų dalyvių.

c. Standartinis leidimas:

   Verslo arba Mažmeninės prekybos Standartinis leidimas yra greitai įdiegiamas sprendimas, suteikiantis šios „Cloud Service“ pagrindines funkcines galimybes, kaip aprašyta šiame skyriuje.

3.5 „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business“ ir (arba) „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail“ ir (arba) „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business“ ir (arba) „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail“

„IBM Security Pinpoint Malware Detection II“ yra nauja „IBM Trusteer Pinpoint Malware Detection“ konstrukcija, skirta padėti standartizuoti mokesčius, susijusius su kelių Taikomųjų programų apsauga, kuri pakeičia vienkartinius mokesčius įtraukiant Taikomąsias programas.

„Man in the Browser“ („MitB“) į finansus nukreipta kenkėjiška programine įranga apkrėstos naršyklės aptikimas klientui nedalyvaujant, jungiantis prie Verslo ir (arba) Mažmeninės prekybos programos. „IBM Trusteer Pinpoint Malware Detection Cloud Services“ suteikia dar vieną apsaugos sluoksnį ir įgalina organizacijas atkreipti dėmesį į apsaugos nuo apgaulės (pagrįstos kenkėjiška programine įranga) procesus, pateikiant Klientui vertinimus ir įspėjimus apie „MitB“ finansinės kenkėjiškos programinės įrangos buvimą.

a. Įvykių duomenys:

   Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenis, sugeneruotus kaip Priskirtų dalyvių internetinės sąveikos su Verslo ar Mažmeninės prekybos programa (-omis).

b. Papildomas leidimas:

   Verslo ir (arba) Mažmeninės prekybos Papildomi leidimai suteikia papildomą aptikimo ir apsaugos sluoksnį, kuris koreguojamas ir pritaikomas prie Kliento Verslo ir (arba) Mažmeninės prekybos programų struktūros ir srauto. Jį galima pritaikyti prie konkrečios Klientui kylančios grėsmės aplinkos. Jį galima įtraukti į įvairias Kliento Verslo ir (arba) Mažmeninės prekybos programų vietas.

   Papildomas leidimas Klientui siūlomas minimaliais kiekiais: bent 100 000 Mažmeninės prekybos programos Priskirtų dalyvių arba 10 000 Verslo programos Priskirtų dalyvių, tai yra 1 000 paketų po 100 Mažmeninės prekybos programos Priskirtų dalyvių arba 1 000 paketų po 10 Verslo programos Priskirtų dalyvių.

c. Standartinis leidimas:

Verslo arba Mažmeninės prekybos Standartinis leidimas yra greitai įdiegiamas sprendimas, suteikiantis šios „Cloud Service“ pagrindines funkcines galimybes, kaip aprašyta šiame skyriuje.

Ši „Cloud Service“ apima vienos Taikomosios programos apsaugą. Kiekvienai papildomai Taikomajai programai Klientas turi įsigyti „IBM Trusteer Pinpoint Malware Detection Additional Applications“ teises.

3.6 Pasirinktinės papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition“ ir (arba) „IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition“ ir (arba) „IBM Trusteer Pinpoint Malware Detection for Business Standard Edition“ ir (arba) „IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition“ ir (arba) „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail“ ir (arba) „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business“ ir (arba) „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail“ ir (arba) „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business“

- „IBM Trusteer Rapport Remediation for Retail Cloud Service“ taikoma būtina sąlyga turėti „IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail“ arba „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail“.
- „IBM Trusteer Rapport Remediation for Business Cloud Service“ taikoma būtina sąlyga turėti „IBM Trusteer Pinpoint Malware Detection Standard Edition for Business“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business“ arba „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business“.
- „IBM Trusteer Pinpoint Carbon for Retail“ taikoma būtina sąlyga turėti „IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail“ arba „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail“.
- „IBM Trusteer Pinpoint Carbon Copy for Business“ taikoma būtina sąlyga turėti „IBM Trusteer Pinpoint Malware Detection Standard Edition for Business“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business“ arba „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business“.

3.6.1 „IBM Trusteer Pinpoint Carbon Copy for Business“ ir (arba) „IBM Trusteer Pinpoint Carbon Copy for Retail“

„IBM Trusteer Pinpoint Carbon Copy“ pasiūlymai skirti suteikti dar vieną apsaugos sluoksnį ir stebėjimo paslaugą, galinčią padėti nustatyti, ar Priskirto dalyvio kredencialams kilo pavojus dėl sukčiavimo apsimetant atakų Kliento Verslo arba Mažmeninės prekybos programose, kurioms skirtus „Cloud Services“ pasiūlymus Klientas užsiprenumeravo.

3.6.2 „IBM Trusteer Rapport Remediation for Retail“ ir (arba) „IBM Trusteer Rapport Remediation for Business“

„IBM Trusteer Rapport Remediation for Retail“ ir „IBM Trusteer Rapport Remediation for Business“ yra skirti ištirti, panaikinti, blokuoti ir pašalinti „man-in-the-browser“ („MitB“) tipo kenkėjišką programinę įrangą iš užkrėstų įrenginių (asmeninių / MAC kompiuterių), priklausančių Kliento Priskirtiems dalyviams, kurie turi prieigą prie Kliento Taikomosios programos specialiąja tvarka, kai „MitB“ kenkėjiškos programinės įrangos užkratai aptinkami pagal „IBM Trusteer Pinpoint Malware Detection“ įvykių duomenis. Klientas privalo turėti dabartinę „IBM Trusteer Pinpoint Malware Detection“ arba „IBM Trusteer Pinpoint Malware Detection II“ prenumeratą, faktiškai veikiančią Kliento Taikomojoje programoje. Klientas gali naudoti šį „Cloud Service“ pasiūlymą tik pasitelkęs Priskirtus dalyvius, kurie turi prieigą prie Kliento Taikomosios programos, ir naudoti išskirtinai tik kaip įrankį, galintį ištirti ir pataisyti konkretų užkrėstą įrenginį (asmeninį / MAC kompiuterį) specialiąja tvarka. „IBM Trusteer Rapport Remediation“ turi faktiškai veikti tokiame užkrėstame Priskirto dalyvio įrenginyje (asmeniniame / MAC kompiuteryje), toks Priskirtas dalyvis turi sutikti su EULA sutartimi, bent kartą būti autentifikuotas kaip besinaudojantis Kliento Taikomąja programa (-omis), o į Kliento konfigūraciją turi būti įtrauktas Vartotojo ID rinkinys. Siekiant išvengti abejonių, šis

„Cloud Service“ pasiūlymas neapima teisės naudoti „Trusteer“ prisistatymo tinklalapį ir (arba) reklamuoti Paskyros turėtojo Kliento programinės įrangos kur nors kitur, o ne Kliento bendrojoje Priskirtų dalyvių bendruomenėje.

3.6.3 „IBM Trusteer Pinpoint Malware Detection Redeployment“

Klientai, kurie iš naujo diegia savo internetinės bankininkystės Taikomąsias programas paslaugų naudojimo laikotarpiu ir kuriems dėl to reikia pakeisti savo „IBM Trusteer Pinpoint Malware Detection“ ir (arba) „IBM Trusteer Pinpoint Malware Detection II“ įdiegtį, turi įsigyti „IBM Trusteer Pinpoint Malware Detection Redeployment“.

Jei Klientas pakeičia Taikomosios programos domeną ar pagrindinio kompiuterio URL, internetinę Taikomąją programą konvertuoja į naują technologiją, pereina į naują internetinės bankininkystės platformą arba į esamą Taikomąją programą įtraukia naują prisijungimo srautą, gali reikėti įdiegti iš naujo.

Diegimo iš naujo 6 mėnesių perėjimo laikotarpiu Klientui suteikiama teisė į papildomas Taikomąsias programas santykiu „vienas su vienu“, veikiančias šalia jau prenumeruojamų Taikomųjų programų.

3.6.4 „IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail“ ir (arba) „IBM Trusteer Pinpoint Malware Detection Additional Applications for Business“

„IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business“ diegiant bet kokioje papildomoje Verslo programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Pinpoint Malware Detection Additional Applications for Business“ teisės. „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail“ diegiant bet kokioje papildomoje Mažmeninės prekybos programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail“ teisės.

3.7 Pasirinktinės papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Criminal Detection for Business“ ir (arba) „IBM Trusteer Pinpoint Criminal Detection for Retail“ ir (arba) „IBM Trusteer Pinpoint Criminal Detection II for Business“ ir (arba) „IBM Trusteer Pinpoint Criminal Detection II for Retail“

3.7.1 „IBM Trusteer Pinpoint Criminal Detection Redeployment“

Klientai, kurie iš naujo diegia savo internetinės bankininkystės Taikomąsias programas paslaugų naudojimo laikotarpiu ir kuriems dėl to reikia pakeisti savo „IBM Trusteer Pinpoint Criminal Detection Cloud Service“, privalo įsigyti „IBM Trusteer Pinpoint Criminal Detection Redeployment“.

Jei Klientas pakeičia Taikomosios programos domeną ar pagrindinio kompiuterio URL, internetinę Taikomąją programą konvertuoja į naują technologiją, pereina į naują internetinės bankininkystės platformą arba į esamą Taikomąją programą įtraukia naują prisijungimo srautą, gali reikėti įdiegti iš naujo.

Diegimo iš naujo 6 mėnesių perėjimo laikotarpiu Klientui suteikiama teisė į papildomas Taikomąsias programas santykiu „vienas su vienu“, veikiančias šalia jau prenumeruojamų Taikomųjų programų.

3.7.2 „IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business“ ir (arba) „IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail“

„IBM Trusteer Pinpoint Criminal Detection II for Business“ diegiant bet kokioje papildomoje Verslo programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business“ teisės. „IBM Trusteer Pinpoint Criminal Detection II for Retail“ diegiant bet kokioje papildomoje Mažmeninės prekybos programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail“ teisės.

4. „IBM Trusteer Fraud Protection Suite“

„IBM Trusteer Fraud Protection Suite“ („Suite“) yra debesies technologija grindžiamų paslaugų rinkinys, skirtas apsaugai nuo sukčiavimų užtikrinti, kurį galima integruoti su papildomais IBM produktais ir teikti eksploatavimo ciklo valdymo sprendimą. Į „Suite“ įtrauktos šios debesies technologija grindžiamos paslaugos:

- „IBM Trusteer Pinpoint Detect“ skirta aptikti ir susilpninti kenkėjišką programinę įrangą, sukčiavimo apsimetant ir paskyrų perėmimo atakas. „Trusteer Pinpoint Detect“ galima integruoti į Kliento Verslo ir (arba) Mažmeninės prekybos programas, dėl kurių Klientas užsiprenumeravo „Cloud Service“ ir procesus, apsaugančius nuo apgaulės.

- „IBM Trusteer Rapport for Mitigation“ skirta taisyti ir apsaugoti problematiškus galutinius taškus.

„Cloud Services“ apima:

a. TMA:

   TMA galima rasti „IBM Trusteer“ debesyje laikomoje aplinkoje, kurioje Klientas (ir neribotas įgaliotų darbuotojų skaičius) gali: (i) gauti įvykio duomenų ataskaitas ir rizikos vertinimus ir (ii) peržiūrėti, konfigūruoti ir nustatyti saugos politiką ir politiką, susijusią su įvykių duomenų ataskaitomis.

b. Įvykių duomenys:

   Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenis, sugeneruotus kaip Priskirtų dalyvių internetinės sąveikos su Verslo ar Mažmeninės prekybos programa (-omis), dėl kurios (-ių) Klientas užsiprenumeravo „Cloud Service“, arba Klientas gali gauti įvykių duomenis per galutinio taško API pristatymo režimą.

c. Žiniatinklio scenarijus ir (arba) API:

   Diegimas svetainėje norint pasiekti arba naudoti „Cloud Service“.

„Pinpoint“ gerosios praktikos pavyzdžiai

Aptikus kenkėjišką įrangą arba paskyros perėmimą, Klientas turi vadovautis „Pinpoint“ gerosios praktikos vadovu. Iš karto, aptikus kenkėjišką programinę įrangą arba paskyros perėmimą, nenaudokite „IBM Trusteer Pinpoint Detect Cloud Services“ tokiu būdu, kuris paveiktų Priskirto dalyvio patirtį, pvz., kiti galės susieti Kliento veiksmus su „IBM Trusteer Pinpoint Detect“ pasiūlymų naudojimu (pvz., perspėjimai, pranešimai, įrenginių blokavimas arba prieigos prie Verslo ir (arba) Mažmeninės prekybos programos blokavimas iš karto po kenkėjiškos programinės įrangos arba paskyros perėmimo aptikimo).

4.1 „IBM Trusteer Pinpoint Detect Standard for Business“ ir (arba) „IBM Trusteer Pinpoint Detect Standard for Retail“

Ši „Cloud Service“ apima „IBM Trusteer Pinpoint Criminal Detection“ ir „IBM Trusteer Pinpoint Malware Detection“ ir pateikia vieną bendrą sprendimą.

Sprendimas padeda, nedalyvaujant klientui, aptikti kenkėjišką programinę įrangą ir (arba) nustatyti įtartinus prie Verslo arba Mažmeninės prekybos programos besijungiančių naršyklių paskyrų perėmimo veiksmus, naudojant įrenginio ID, sukčiavimo apsimetant aptikimą ir kenkėjiškos programos aptikimą, kai bandoma pavogti kredencialus. „IBM Trusteer Pinpoint“ pasiūlymai suteikia dar vieną apsaugos sluoksnį, aptinka bandymus perimti paskyras ir pateikia naršyklių arba mobiliųjų įrenginių rizikos vertinimo balus (naudojant vietinę naršyklę arba Kliento mobiliąją programą), nes Verslo arba Mažmeninės prekybos programą tiesiogiai susieja su Klientu.

Į šią „Cloud Service“ įtrauktas Standartinis palaikymas (kaip apibrėžta toliau pateiktame skyriuje „Techninis palaikymas“). Norėdamas gauti „Premium“ palaikymą Klientas privalo įsigyti „Detect Premium“.

Ši „Cloud Service“ apima vienos Taikomosios programos apsaugą. Kiekvienai papildomai Taikomajai programai Klientas turi įsigyti „IBM Trusteer Pinpoint Detect Standard Additional Applications“ teisę.

4.2 „IBM Trusteer Pinpoint Detect Premium for Business“ ir (arba) „IBM Trusteer Pinpoint Detect Premium for Retail“

Ši „Cloud Service“ apima „IBM Trusteer Pinpoint Criminal Detection“ ir „IBM Trusteer Pinpoint Malware Detection“ ir pateikia vieną bendrą, lengvai integruojamą sprendimą.

Sprendimas padeda, nedalyvaujant klientui, aptikti kenkėjišką programinę įrangą ir (arba) nustatyti įtartinus prie Verslo arba Mažmeninės prekybos programos besijungiančių naršyklių paskyrų perėmimo veiksmus, naudojant įrenginio ID, sukčiavimo apsimetant aptikimą ir kenkėjiškos programos aptikimą, kai bandoma pavogti kredencialus. „IBM Trusteer Pinpoint“ pasiūlymai suteikia dar vieną apsaugos sluoksnį, aptinka bandymus perimti paskyras ir pateikia naršyklių arba mobiliųjų įrenginių rizikos vertinimo balus (naudojant vietinę naršyklę arba Kliento mobiliąją programą), nes Verslo arba Mažmeninės prekybos programą tiesiogiai susieja su Klientu.

Paslauga apima išplėstines funkcijas ir paslaugas, įskaitant išplėstines diegimo ir nustatymo paslaugas, pritaikytas saugos strategijas, tyrimo paslaugas ir t. t.

Ši „Cloud Service“ apima vienos Taikomosios programos apsaugą. Kiekvienai papildomai Taikomajai programai Klientas turi įsigyti „IBM Trusteer Pinpoint Detect Premium Additional Applications“ teisę.

Į šią „Cloud Service“ įtrauktas „Premium“ palaikymas.

„Pinpoint Detect Policy Manager“:

„Policy Manager“ įtraukta į „Pinpoint Detect Premium“ paslaugą ir yra pasiekiama „IBM Trusteer“ debesyje laikomoje aplinkoje, kurioje Klientas (ir neribotas skaičius įgaliotojo personalo) gali: (i) kurti, tikrinti ir diegti gamybos aplinkoje logiką, skirtą apgaulingai veiklai aptikti, (ii) kurti ataskaitas ir stebėjimo skydus ir (iii) peržiūrėti, konfigūruoti ir nustatyti saugos strategijas ir strategijas, skirtas įtartinoms veikloms kliento Taikomojoje programoje aptikti.

Norint aktyvinti „Policy Manager“ funkciją ir gauti reikiamą papildomą išsamų palaikymą, reikalingos konsultavimo paslaugos. Išsami konsultavimo paslaugų informacija bus pateikta atskirai darbų aprašyme.

Kai „Policy Manager“ suaktyvinta, IBM pasilieka teisę pasiekti Kliento aplinką palaikymo tikslais, kad galėtų koreguoti Kliento strategijas ir šalinti pagrindines problemas, atsiradusias dėl strategijos pakeitimų.

Klientas įsipareigoja apsaugoti visus duomenis, atskleistus „Policy Manager“ nuo netinkamo naudojimo.

Kai „Policy Manager“ funkcija suaktyvinta, Klientas privalo laikytis taisyklių nustatymo IBM rekomendacijų, apibrėžtų dokumentacijoje. Klientas patvirtina, kad IBM neatsakinga už jokią situaciją, susidariusią Klientui nesilaikant šių rekomendacijų.

Bet kokios stabilumo ir (arba) paslaugos pablogėjimo problemos, kurios gali atsirasti dėl netinkamai Kliento atlikto „Policy Manager“ funkcijos konfigūravimo, nebus laikomos Prastova skaičiuojant PLS.

4.3 „IBM Trusteer Pinpoint Detect Standard with access management integration for Business“ ir (arba) „IBM Trusteer Pinpoint Detect Standard with access management integration for Retail“

„IBM Trusteer Pinpoint Detect Standard with access management integration Cloud Service“ apima „IBM Pinpoint Detect Standard“ funkcijas, kaip apibrėžta ankstesniame 4.1 skyriuje.

„IBM Trusteer Pinpoint Detect Standard with access management integration“ naudojamas įsigijus su prieigos valdymo sistemomis, pvz., „IBM Security Access Management“ (ISAM). Įsigijus su ISAM, turi būti įgalinti abu pasiūlymai. Šis pasiūlymas apima integracijos su prieigos valdymo sistema galimybę. Jis neapima prieigos valdymo sistemos teisių.

Šis pasiūlymas apima vienos Taikomosios programos apsaugą. Kiekvienai papildomai Taikomajai programai Klientas turi įsigyti „IBM Trusteer Pinpoint Detect Standard Additional Applications“ teisę.

Į šią „Cloud Service“ įtrauktas Standartinis palaikymas (kaip apibrėžta skyriuje „Techninis palaikymas“).
„IBM Trusteer Pinpoint Detect Premium with access management integration for Business“ ir (arba) „IBM Trusteer Pinpoint Detect Premium with access management integration for Retail“

IBM Pinpoint Detect Premium with access management integration Cloud Service includes the functionality of IBM Pinpoint Detect Premium as detailed in section 4.2 above, and the integration option with the access management system.

„IBM Trusteer Pinpoint Detect Premium with access management integration“ naudojamas įsigijus su prieigos valdymo sistemomis, pvz., „IBM Security Access Management“ (ISAM). Įsigijus su ISAM, turi būti įgalinti abu pasiūlymai. Ši „Cloud Service“ apima integracijos su prieigos valdymo sistema galimybę. Jis neapima prieigos valdymo sistemos teisių.

Ši „Cloud Service“ apima vienos Taikomosios programos apsaugą. Kiekvienai papildomai Taikomajai programai Klientas turi įsigyti „IBM Trusteer Pinpoint Detect Premium Additional Applications“ teises.

Į šį pasiūlymą įtrauktas „Premium“ palaikymas.

4.4 Pasirinktinės „IBM Trusteer Pinpoint Detect Standard“ ir (arba) „IBM Trusteer Pinpoint Detect Premium“ paslaugos

Norint naudoti šiame skyriuje nurodytas „Cloud Services“, būtina turėti teisę naudoti „IBM Trusteer Pinpoint Detect Premium for Retail“ arba „IBM Trusteer Pinpoint Detect Standard for Retail“.

4.5 „IBM Trusteer Rapport for Mitigation for Retail“ ir (arba) „IBM Trusteer Rapport for Mitigation for Business“

„IBM Trusteer Rapport for Mitigation“ skirtas ištirti, panaikinti, blokuoti ir pašalinti kenkėjišką programinę įrangą iš užkrėstų įrenginių (asmeninių / MAC kompiuterių), priklausančių Kliento Priskirtiems dalyviams, kurie turi prieigą prie Kliento Mažmeninės prekybos programos nustatyta tvarka, kai kenkėjiškos programinės įrangos užkratus aptinka „IBM Trusteer Pinpoint Detect Premium“ arba „IBM Trusteer Pinpoint Detect Standard“ įvykių duomenys. Klientas privalo turėti „IBM Trusteer Pinpoint Detect Premium“ arba „IBM Trusteer Pinpoint Detect Standard“ prenumeratą, veikiančią Kliento Mažmeninės

prekybos programoje. Klientas gali naudoti šias „Cloud Service“ tik pasitelkęs Priskirtus dalyvius, kurie turi prieigą prie Kliento Mažmeninės prekybos programos, ir naudoti išskirtinai tik kaip įrankį, galintį ištirti ir pataisyti konkretų užkrėstą įrenginį (asmeninį / MAC kompiuterį). „IBM Trusteer Rapport for Mitigation for Retail“ turi praktiškai veikti tokiame užkrėstame Priskirto dalyvio įrenginyje (asmeniniame / MAC kompiuteryje), toks Priskirtas dalyvis turi sutikti su EULA sutartimi, bent kartą būti autentifikuotas kaip besinaudojantis Kliento Mažmeninės prekybos programa (-omis), o į Kliento konfigūraciją turi būti įtrauktas Vartotojo ID rinkinys. Siekiant išvengti abejonių, ši „Cloud Service“ neapima teisės naudoti „Trusteer“ prisistatymo tinklalapį ir (arba) reklamuoti Paskyros turėtojo Kliento programinės įrangos kur nors kitur, o ne Kliento bendrojoje Priskirtų dalyvių bendruomenėje.

4.5.1 „IBM Trusteer Pinpoint Detect Standard Additional Applications for Business“ ir (arba) „IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail“ ir (arba) „IBM Trusteer Pinpoint Detect Premium Additional Applications for Business“ ir (arba) „IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail“

„IBM Trusteer Pinpoint Detect Standard for Business“ diegiant bet kokioje papildomoje Verslo programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Pinpoint Detect Standard Additional Applications for Business“ teisės.

„IBM Trusteer Pinpoint Detect Standard for Retail“ diegiant bet kokioje papildomoje Mažmeninės prekybos programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail“ teisės.

„IBM Trusteer Pinpoint Premium for Business“ diegiant bet kokioje papildomoje Verslo programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Pinpoint Detect Premium Additional Applications for Business“ teisės.

„IBM Trusteer Pinpoint Premium for Retail“ diegiant bet kokioje papildomoje Mažmeninės prekybos programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail“ teisės.

4.5.2 „IBM Trusteer Pinpoint Detect Standard Redeployment“ ir (arba) „IBM Trusteer Pinpoint Detect Premium Redeployment“

Klientai, kurie iš naujo diegia savo internetinės bankininkystės Taikomąsias programas paslaugų naudojimo laikotarpiu ir kuriems dėl to reikia pakeisti savo „IBM Trusteer Pinpoint Detect“, turi įsigyti „IBM Trusteer Pinpoint Detect Redeployment“.

Jei Klientas pakeičia Taikomosios programos domeną ar pagrindinio kompiuterio URL, internetinę Taikomąją programą konvertuoja į naują technologiją, pereina į naują internetinės bankininkystės platformą arba į esamą Taikomąją programą įtraukia naują prisijungimo srautą, gali reikėti įdiegti iš naujo.

Diegimo iš naujo 6 mėnesių perėjimo laikotarpiu Klientui suteikiama teisė į papildomas Taikomąsias programas santykiu „vienas su vienu“, veikiančias šalia jau prenumeruojamų Taikomųjų programų.

5. „IBM Trusteer Mobile Cloud Services“

5.1 „IBM Trusteer Mobile Browser for Business“ ir (arba) „IBM Trusteer Mobile Browser for Retail“

„IBM Trusteer Mobile Browser“ sukurtas kaip papildomas apsaugos sluoksnis ir yra skirtas suteikti saugią internetinę Priskirtų dalyvių mobiliųjų įrenginių prieigą prie Kliento Mažmeninės prekybos arba Verslo programų, kurioms skirtas „Cloud Services“ Klientas užsiprenumeravo, mobiliųjų įrenginių rizikos vertinimą ir apsaugą nuo sukčiavimo apsimetant. Saugaus „Wi-Fi“ aptikimas pasiekiamas tik „Android“ platformose. Naudojant šią „Cloud Service“, mobilieji įrenginiai apima mobiliuosius telefonus ar planšetinius kompiuterius, bet neapima nešiojamųjų ir „Mac“ kompiuterių.

Naudodamas TMA, Klientas gali gauti įvykių duomenis, analizę ir statistinę informaciją, susijusią su Įrenginiais, kuriuos turintys Priskirti dalyviai: (i) atsisiuntė Paskyros turėtojo Kliento programinę įrangą, programą, licencijuotą naudoti nemokamai ir viešai pagal galutinio vartotojo licencijos sutartį (EULA), ir padarė atsisiunčiamą į Priskirtų dalyvių mobiliuosius įrenginius, ir (ii) sutiko su EULA sutartimi ir bent kartą buvo autentifikuoti kaip besinaudojantys Kliento Verslo ar Mažmeninės prekybos programomis, kurioms skirtas „Cloud Services“ Klientas užsiprenumeravo. Klientas gali reklamuoti Paskyros turėtojo Kliento programinę įrangą tik naudodamas „Trusteer“ prisistatymo tinklalapį ir negali naudoti Paskyros turėtojo Kliento programinės įrangos vidiniams įmonės veiksmams atlikti.

a. Įvykių duomenys:

   Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenis, sugeneruotus kaip mobiliųjų įrenginių internetinės sąveikos su Verslo ar Mažmeninės prekybos programomis, kurioms skirtas „Cloud Services“ Klientas užsiprenumeravo, rezultatas.

b. „Trusteer“ prisistatymo tinklalapis:

   „Trusteer“ prisistatymo tinklalapio rinkodaros platforma atpažįsta ir reklamuoja Paskyros turėtojo Kliento programinę įrangą Priskirtiems dalyviams, turintiems prieigą prie Kliento Verslo ir (arba) Mažmeninės prekybos programų, kurioms skirtas „Cloud Services“ Klientas užsiprenumeravo. Klientas gali rinktis iš galimų prisistatymo tinklalapio šablonų (Prisistatymo tinklalapio šablonas). Dėl pasirinktinio prisistatymo tinklalapio gali būti pasirašoma atskira sutartis arba įsipareigojimų aprašymas.

Klientas gali sutikti pateikti prekių ženklus, logotipus ar piktogramas, skirtas naudoti pagal TMA, naudoti tik su „Trusteer“ prisistatymo tinklalapiu, pateikti Paskyros turėtojo Kliento programinėje įrangoje, IBM laikomuose nukreipimo puslapiuose arba „IBM Trusteer“ svetainėje. Visas pateiktų prekių ženklų, logotipų ar piktogramų naudojimas vykdomas remiantis pagrįsta IBM politika, susijusia su reklamavimu ir prekių ženklų naudojimu.

5.2 „IBM Trusteer Mobile SDK for Business“ ir (arba) „IBM Trusteer Mobile SDK for Retail“

„IBM Trusteer Mobile SDK Cloud Services“ sukurtos kaip papildomas apsaugos sluoksnis ir yra skirtos suteikti saugią internetinę prieigą prie Kliento Verslo ir (arba) Mažmeninės prekybos programų, kurioms skirtas „Cloud Services“, įrenginių rizikos vertinimą ir apsaugą nuo kibernetinių atakų Klientas užsiprenumeravo. Saugaus „Wi-Fi“ aptikimas pasiekiamas tik „Android“ platformose.

„IBM Trusteer Mobile SDK Cloud Services“ apima nuosavybinės mobiliojo prietaiso programinės įrangos kūrėjo rinkinį (SDK), programinės įrangos paketą su dokumentacija, programavimo nuosavybinės programavimo įrangos bibliotekas ir kitus susijusius failus bei elementus, vadinamus „IBM Trusteer“ mobiliąja biblioteka, taip pat Vykdymo laiko komponentus arba Perskirstymo paketus, nuosavybiniu kodu, kurį sugeneravo „IBM Trusteer Mobile SDK“. Šį pasiūlymą galima įdėti ir integruoti į atskirą, apsaugotą Kliento „iOS“ arba „Android“ mobiliąsias programas, kurioms skirtas „Cloud Services“ Klientas užsiprenumeravo. („Kliento integruota mobilioji programa“).

„IBM Trusteer Mobile SDK for Retail“ galima gauti paketais po 100 Priskirtų dalyvių arba paketais po 100 Kliento įrenginių, o „IBM Trusteer Mobile SDK for Business“ galima gauti paketais po 10 Priskirtų dalyvių arba paketais po 10 Kliento įrenginių.

Naudodamas TMA Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali gauti įvykio duomenų ataskaitą ir rizikos tendencijų įvertinimą. Naudodamas Kliento integruotą mobiliojo programą, Klientas gali gauti rizikos analizės ir mobiliojo prietaiso informaciją, susijusią su Priskirtų dalyvių, kurie atsisiuntė Kliento integruotą mobiliojo programą, mobiliaisiais įrenginiais, kad Klientas galėtų formuluoti kovos su sukčiavimu politiką, kuri realizuotų šias rizikas mažinančius veiksmus. Kiek tai susiję su šiuo pasiūlymu, „mobilieji įrenginiai“ yra tik palaikomi mobilieji telefonai ir planšetiniai kompiuteriai, o ne asmeniniai arba MAC kompiuteriai.

Klientas gali:

a. įmonės viduje naudoti „IBM Trusteer Mobile SDK“ tik kurdamas Kliento integruotą mobiliąją programą;

b. į Kliento integruotą mobiliojo programą įdėti Perskirstymo paketą (tik objekto kodo formatu) integruotu, neatskiriamu būdu. Pagal šią licenciją bet kokiai modifikuotai ar sulietai Perskirstymo paketo daliai taikomas šis Paslaugos aprašas;

c. prekiauti ir paskirstyti Perskirstymo paketą, skirtą atsisiųsti į Priskirtų dalyvių arba Kliento įrangos turėtojo mobiliuosius įrenginius, su sąlyga, kad:

   - Išskyrus, kai aiškiai leidžia šios Sutarties sąlygos, Klientas (1) negali naudoti, kopijuoti, modifikuoti arba platinti SDK, (2) negali išardyti, dekompiliuoti, kitaip versti ar atkurti SDK, nebent tai aiškiai leidžia įstatymai, nenumatant sutartinio atleidimo nuo įsipareigojimų, (3) negali licencijuoti trečiajai šaliai, nuomoti ir išperkamosios nuomos pagrindais suteikti SDK, (4) negali pašalinti jokių Perskirstymo pakete esančių autoriaus teisių arba pastabų failų, (5) negali naudoti tokio paties kelio pavadinimo, koks priskirtas originaliems Perskirstymo paketo failams / moduliams ir (6) negali naudoti IBM, jos licencijų davėjų arb aplatintojų pavadinimų

arba prekių pavadinimų reklamuodamas Kliento integruotą mobiliojo programą be IBM arba atitinkamo licencijos davėjo ar platintojo išankstinio sutikimo raštų.

- Perskirstymo paketas turi likti neatskiriamai integruotas Kliento integruotoje mobiliojo programoje. Perskirtymo paketas turi būti tik objekto kodo forma ir turi atitikti visus SDK ir dokumentacijoje pateiktus nurodymus, instrukcijas ir specifikacijas. Kliento integruotos mobiliojo programos galutinio vartotojo licencijos sutartyje galutinis vartotojas turi būti įspėtas, kad Perskirstymo paketų negalima i) naudoti kitu tikslu, o tik Kliento integruotai mobiliojo programai įgalinti, ii) kopijuoti (išskyrus kuriant atsarginę kopiją), iii) platinti ar perduoti, iv) išardyti, dekompiliuoti ar kitaip versti, išskyrus, jei tai aiškiai leidžia teisės aktai ir nepažeidžiami sutartiniai įsipareigojimai. Kliento licencinė sutartis turi būti sauganti IBM bent tiek, kiek tai apibrėžia šios Sutarties sąlygos.
- SDK galima diegti tik kaip dalį Kliento vidinio kūrimo ir įrenginio tikrinimo Kliento nurodytuose mobiliuosiuose tikrinimo įrenginiuose. Klientas neturi teisės naudoti SDK gamybos darbo krūviams apdoroti, gamybos darbo krūviams modeliuoti arba bet kurio kodo, taikomosios programos arba sistemos pritaikomumui tikrinti. Klientas neturi teisės naudoti bet kurios SDK dalies bet kokiais kitais tikslais.

Tiktai klientas yra atsakingas už Kliento integruotos mobiliojo programos kūrimą, testavimą ir palaikymą. Klientas atsakingas už visą techninę pagalbą, susijusią su Kliento integruota mobiliojo programa, ir už bet kokias Kliento atliktas, šiame dokumente leidžiamas, Perskirstymo paketų modifikacijas.

Klientui suteikiama teisė diegti ir naudoti Perskirstymo paketus ir „IBM Security Mobile SDK“ tik siekiant palaikyti Kliento „Cloud Services“ naudojimą.

IBM atliko kai kurių pavyzdinių taikomųjų programų, sukurtų naudojant „IBM Trusteer Mobile SDK“ pateiktus įrankius mobiliesiems („Įrankiai mobiliesiems“) testavimą, kad nustatytų, ar jos tinkamai veiks tam tikrose „Apple“ („iOS“), „Google“ („Android“) ir kitose (bendrai „OS platformos mobiliesiems“) operacinių sistemų platformų mobiliesiems versijose; vis dėlto OS platformas mobiliesiems teikia trečiosios šalys ir jos nepavaldžios IBM, taigi gali būti pakeitimų apie tai nepranešus IBM. Nepaisant prieštaraujančių sąlygų, IBM negarantuoja, kad bet kokios taikomosios programos ar kitokia išvestis, sukurta naudojant Įrankius mobiliesiems, bus tinkamai vykdoma, sąveikaus ir bus suderinama su bet kuriomis OS platformomis mobiliesiems ar mobiliaisiais įrenginiais.

Šaltinio komponentai ir Pavyzdinė medžiaga – į „IBM Trusteer Mobile SDK“ gali būti įtraukti keli komponentai šaltinio kodo forma („Šaltinio komponentai) ir kita medžiaga, apibrėžiama kaip Pavyzdinė medžiaga. Klientas gali kopijuoti ir modifikuoti Šaltinio komponentus ir Pavyzdinę medžiagą tik naudoti viduje, jei toks naudojimas nepažeidžia šios Sutarties licencijos teisių ir jei Klientas nekeičia ar nenaikina jokios Šaltinio komponentuose ir Pavyzdinėje medžiagoje esančios autoriaus teisių informacijos ar pranešimų. IBM pateikia Šaltinio komponentus ir Pavyzdinę medžiagą be palaikymo įsipareigojimo ir TOKIĄ, KOKIA YRA, NESUTEIKIANT JOKIŲ AIŠKIAI NURODYTŲ AR NENURODYTŲ GARANTIJŲ, ĮSKAITANT NUOSAVYBĖS TEISĖS, NEPAŽEIDŽIAMUMO AR NEĮSIKIŠIMO GARANTIJAS IR NENURODYTAS TINKAMUMO PREKIAUTI IR TAM TIKRAM TIKSLUI GARANTIJAS IR SĄLYGAS. Atminkite, kad Šaltinio komponentai arba Pavyzdinės medžiagos pateikiami tik kaip pavyzdys, kaip Įdedamuosius komponentus įgyvendinti į CIMA, Šaltinio komponentai ar Pavyzdinė medžiaga gali būti nesuderinami su Kliento kūrimo aplinka ir tiktai pats Klientas yra atsakingas už Įdedamųjų komponentų testavimą ir įgyvendinimą į jo CIMA.

Klientas sukurs, saugos ir pateiks IBM bei jos auditoriams tikslias rašytines ataskaitas, sistemos įrankių išvestis ir kitą sistemos informaciją, kuri leistų aiškiai įvertinti, ar Klientas naudoja „IBM Trusteer Mobile SDK“ laikydamasis šio Paslaugos aprašo sąlygų.

6. „Premium Support“

Klientas turi teisę į „Premium Support“ lygio palaikymą, teikiamą tik toms „Cloud Services“, kurioms skirtą „Premium Support“ pasiūlymą Klientas užsiprenumeravo.

7. „IBM Trusteer Fraud Protection“ diegimas

Kiekvienos Kliento prenumeruojamos Taikomosios programos atveju Kliento pagrindinė prenumerata apima reikiamą nustatymą ir pradinio diegimo veiksmus „IBM Trusteer“ debesyje, įskaitant pradinį vienkartinį įjungimą, konfigūravimą, Prisistatymo tinklalapio šablonus, testavimą ir mokymą.

Diegimo veiksmai neapima diegimo veiksmų, kuriuos būtina atlikti Kliento Taikomosiose programose ar sistemose.

Įvairių „Cloud Services“ diegimo etapas turi būti vykdomas laikotarpiais, apibrėžtais atitinkamuose diegimo vadovuose.

Šių įgyvendinimo etapų užbaigimas per paskirtą laikotarpį priklauso nuo visiško Kliento administracijos ir personalo atsidavimo ir dalyvavimo. Klientas turi laiku pateikti reikiamą informaciją. IBM našumas pagrįstas Kliento laiku suteikiama informacija ir priimamais sprendimais, todėl bet kokia delsa gali papildomai pabranginti šias diegimo paslaugas ir (arba) pavėlinti jų užbaigimą.

Kiekvienos Kliento prenumeruojamos Taikomosios programos atveju kliento pagrindinė prenumerata apima reikiamą nustatymą ir pradinio diegimo veiksmus „IBM Trusteer“ debesyje, įskaitant pradinį vienkartinį įjungimą, konfigūravimą, Prisistatymo tinklalapio šablonus, testavimą ir mokymą.

Kliento prenumerata apima tokios Kliento taikomosios programos puslapių, kurie bus pažymėti, atsižvelgiant į pradinio kūrimo metu IBM pateiktas rekomendacijas, palaikymą ir testavimą. IBM nėra atsakinga už: (i) dalinį diegimą, (ii) Kliento pasirinkimą nediegti „IBM Cloud Service“, kaip rekomenduoja IBM, arba (iii) Kliento pasirinkimą atlikti savarankišką diegimą, nustatymą ir testavimą. (IV) dalinio diegimo arba apsaugos rezultatą dėl Kliento pateiktos nepakankamos informacijos. Dėl papildomų paslaugų, įskaitant diegimą po pradinio kūrimo, galima sudaryti atskirą sutartį ir mokėti už jas atskirą mokestį.

8. Duomenų privatumas ir sauga

Šiai „Cloud Service“ taikomi „Cloud Services“ duomenų saugos ir privatumo principai, kurie pasiekiami http://www.ibm.com/cloud/data-security, ir bet kokios kitos šiame skyriuje nurodytos papildomos sąlygos. Jokie IBM duomenų saugos ir privatumo pricipų pakeitimai nesumažins „Cloud Service“ saugos.

Šią „Cloud Service“ galima naudoti apdorojant turinį, kuriame yra asmens duomenų, jei Klientas, kaip duomenų valdytojas, nustato, kad techninės ir organizacinės saugos priemonės yra tinkamos pagal riziką, kuri kyla apdorojant, ir saugotinų duomenų pobūdį. Klientas pripažįsta, kad ši „Cloud Service“ nesiūlo funkcijų, skirtų apsaugoti konfidencialius asmens duomenis, ar duomenų objekto, skirto papildomiems teisiniams reikalavimams.

Ši „Cloud Service“ įtraukiama į IBM Privatumo apsaugos sertifikavimą ir taikoma, kai Klientas pasirenka saugoti „Cloud Service“ JAV esančiame duomenų centre, ir jai taikoma IBM Privatumo apsaugos privatumo politika, kurią rasite apsilankę http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

8.1 Saugos funkcijos ir įsipareigojimai

„Cloud Service“ vykdo šias saugos funkcijas:

„Cloud Service“ šifruoja turinį perduodant duomenis į IBM tinklą ir iš jo bei kai laukiama duomenų perdavimo iš galutinio taško.

8.2 Teisėtas naudojimas ir turinys

Teisėtas naudojimas

Naudojant šias „Cloud Service“, gali būti taikomi įvairūs teisės aktai ir taisyklės. „Cloud Service“ galima naudoti tik teisėtais tikslais ir teisėtu būdu. Klientas sutinka naudoti „Cloud Service“ laikydamasis taikomų teisės aktų, taisyklių ir politikos nuostatų ir prisiima už tai visą atsakomybę.

Įgaliojimas rinkti ir apdoroti duomenis

„Cloud Service“ rinks informaciją iš Priskirtų dalyvių ir Kliento įrenginių, palaikančių ryšį su Verslo arba Mažmeninės prekybos programomis, kurioms skirtas „Cloud Service“ Klientas užsiprenumeravo. „Cloud Service“ renka informaciją, kuri pati savaime arba kartu su kitais duomenimis kai kuriose jurisdikcijose gali būti laikoma Asmens duomenimis. Asmens duomenys – tai bet kokia informacija, pagal kurią galima identifikuoti konkretų asmenį, pavyzdžiui, vardas, el. pašto adresas, namų adresas arba telefono numeris, kuri pateikiama IBM saugoti, tvarkyti arba perduoti Kliento vardu.

Duomenų rinkimo ir apdorojimo praktika gali būti atnaujinama siekiant patobulinti „Cloud Service“ veikimą. Dokumentas su visu duomenų rinkimo ir apdorojimo praktikos aprašu yra atnaujinamas, kai reikia, ir pasiekiamas Klientui paprašius. Klientas įgalioja IBM rinkti šią informaciją ir ją tvarkyti remiantis skyriumi „Tarptautinis perdavimas“ ir Paslaugos aprašo skyriumi „Duomenų privatumas“.

Jei naudojami „IBM Trusteer“ pasiūlymai, į kuriuos įtraukta „Trusteer Management Application“ (TMA):

Programoje „Trusteer Management Application“ (TMA) TMA administratoriams renkami ir saugomi tokie remiančios įmonės duomenys: el. pašto adresas (kaip prisijungimo vardas), užšifruotas slaptažodis, vardas, pavardė, pareigos ir skyrius.

Skirta „IBM Trusteer Pinpoint Cloud Services“:

Surinkti duomenys gali apimti:

- vartotojo arba galinio punkto identifikatorius, pvz., užšifruotą arba iš vienos pusės užšifruotą Vartotojo ID (PUID), Ryšio agento raktą ir Kliento seanso ID;
- duomenis, susijusius su apsaugota programa, pvz., konkrečius atributus / elementus iš klientų internetinės bankininkystės programos, kaip jie atvaizduojami galutinio vartotojo naršyklėje, apsilankymus svetainėje ir naršymo istoriją;
- įdiegtos programinės įrangos aplinkos informaciją, naršyklės ir įrenginio atributus ir parametrus bei naršyklės istorijos ilgį;
- aparatūros informaciją ir laiko žymą;
- naršyklės antraštes ir ryšių protokolo duomenis, pvz., IP adresą, slapukus, persiuntimo antraštę ir kitas HTTP antraštes;
- galutinio vartotojo pele atliktų veiksmų duomenis (pvz., pelės žymiklio koordinates, paspaudimus ir slinkimo ratuko veiksmus (bei jų atitikmenis), taip pat laiko žymą, kai buvo sąveikaujama su Kliento internetinės bankininkystės taikomąja programa;
- apsimestines svetaines ir į jas pateikiamą informaciją; ir
- Kliento nuožiūra, operacinius duomenis (operacijos suma, operacijos valiuta ir paskirties vietos kodai, iš vienos pusės užšifruotos operacijos paskirties banko identifikatorius, iš vienos pusės užšifruotos operacijos paskirties sąskaitos identifikatorius, dvejetainė reikšmė, jei operacija yra naujas mokėtojas, ir operacijos data / laikas) ir pasirinktinį rizikos duomenų balą.
- tik Kliento pasirinkimu – klaviatūros spaudimo ritmus ir grupinių sekų klaviatūroje paspaudimus, kuriuos naudoja galutinis vartotojas, įvesdamas vartotojo vardą, slaptažodį ar kitą tekstą (tačiau ne pačias raides, skaičius ar specialiuosius simbolius ir be galimybės atskirti vartotojo vardą ar slaptažodį);

Kai „Policy Manager“ suaktyvinta, atsakomybę už visus naudojamus išplėstinius duomenis prisiima išskirtinai Klientas. IBM rekomenduoja maišyti arba šifruoti duomenis, kuriuos galima laikyti Asmens identifikatoriais.

Klientas supranta ir sutinka, kad IBM nerinks, nesaugos, nevaldys ir netvarkys oficialių Kliento registrų ir (arba) įrašų.

Kai Klientas užsiprenumeruoja „IBM Trusteer Rapport for Remediation“ pasiūlymą arba tam tikrais „Pinpoint“ palaikymo atvejais, IBM gali rekomenduoti Priskirto dalyvio kompiuteryje įdiegti „Rapport“ paskyros turėtojo kliento programinę įrangą, kad būtų galima analizuoti ir tirti įtariamą užkrėtimą kenkėjiška programine įranga. „Rapport“ pasiūlymų renkami duomenys apibrėžti toliau.

„IBM Trusteer Rapport Cloud Services“ (įskaitant „Rapport for Remediation“ arba „Rapport for Mitigation“, diegiant kartu su „Pinpoint“ pasiūlymais):

Surinkti duomenys gali apimti:

- URL ir interneto protokolo (IP) adresus, priklausančius svetainėms, kurias Paskyros turėtojas aplanko ir kurias IBM laiko potencialiai apgaulingomis, apsimestinėmis ar išnaudojančiomis, taip informaciją apie identifikuotų grėsmių kilmę;
- svetainių, kuriose lankosi Paskyros turėtojas ir kurias kontroliuoja Klientas ir apsaugo „Cloud Service“, pvz., internetinės bankininkystės svetainių, URL ir IP adresus; Paskyros turėtojo IP adresus;
- informaciją apie techninės įrangos identifikavimą, operacines sistemas, taikomųjų programų programinę įrangą, išorinę įrangą, saugos konfigūravimą, sistemų parametrus ir galinio punkto tinklo ryšius, taip pat ID, pavadinimą, naudojimo įpročius ir kitą galinį punktą identifikuojančią informaciją;
- informaciją, susijusią su programos diegimu ir veikimu, programos ID, programos versiją, galinio punkto sugeneruotus saugos įvykius ir informaciją apie programos klaidas;
- naudojimo statistiką ir statistinę informaciją apie programos aptiktas grėsmes; žurnalo failus, kuriuose registruojami naršyklės gedimai, užkrėtimo data ir laikas ir informacija apie identifikuotų grėsmių ar trikčių kilmę;
- Klieno filialą, dar vadinamą Remiančia įmone. Filialas įkuriamas, kai iš Kliento svetainės galutinis vartotojas atsisiunčia „Rapport“, atsisiųsdamas „Rapport“ iš „Trusteer“ palaikymo svetainės

pasirenka konkretų Klientą arba prisijungia prie Kliento bankininkystės programos. Galutinis vartotojas gali turėti daugiau nei vieną Kliento filialą;

- užšifruoto Vartotojo ID, kurį Paskyros turėtojas naudoja sąveikauti su Klientu kopiją (nebūtina);
- užšifruotą kredito kortelės numerio, kurį Paskyros turėtojas įveda į svetainę, kai programa Paskyros turėtoją informuoja, jog programa laiko svetainę rizikinga, kopiją;
- failus ar kitą informaciją iš galinio punkto, kurią IBM saugos specialistai įtaria esant susijus su kenkėjiška programine įranga ar kita piktybine veikla arba esant susijus su bendru programos netinkamu veikimu; ir
- Asmeninę kontaktinę informaciją, įskaitant vardą ir el. paštą, kai galutinis vartotojas kreipiasi į Palaikymo tarnybą.

„IBM Trusteer Mobile SDK“ ir „IBM Trusteer Mobile Browser Cloud Services“:

Surinkti duomenys gali apimti:

- vartotojo identifikatorius, pvz., užšifruotą arba iš vienos pusės užšifruotą Vartotojo ID;
- įrenginio informaciją, pvz., IP adresą, įrenginio ID maišos reikšmę, laiko žymą, įdiegto paketo MD5 vertes ir kitą įrenginio aparatūros bei programinės įrangos informaciją;
- „Mobile SDK“ arba „Mobile Browser“ versiją ir įdiegimo datą;
- informaciją apie apsilankymus apsaugotose taikomosiose programose;
- Kliento priklausomybę; ir
- įrenginio rizikos duomenis (pvz., apie kenkėjiškos programinės įrangos buvimą, šakninius slėptuvus, „Wi-Fi“ šifravimo būseną, apie tai, ar pašalinti įrenginio programinės įrangos apribojimai);
- gedimų ataskaitą (netikėtai nustojus veikti taikomajai programai);
- telefono komponavimo versijos duomenis (pvz., modelis, gamintojas);
- galutinių vartotojų jutiklinio ekrano veiksmus, įskaitant x ir y koordinates, jutiklinio ekrano sritį ir veiksmų tipus (žemyn, aukštyn ir judėjimo);
- judesio jutiklio duomenis, energijos / šaltinių naudojimą, ryšio parametrus, aplinkos jutiklius, pvz., temperatūrą, apšvietimą ir oro slėgį, taip pat bendruosius įrenginio parametrus (garsumą, skambutį, ekrano ryškumą ir kt.).

8.3 Duomenų subjektų sutikimas

Skirta „IBM Trusteer Pinpoint Cloud Services“ ir „IBM Trusteer Mobile SDK Cloud Services“:

Klientas sutinka, kad gavo arba gaus visus išsamius sutikimus, leidimus ir licencijas, reikalingas įgalinti teisėtą „Cloud Service“ naudojimą ir leidžiančias IBM rinkti ir tvarkyti informaciją per „Cloud Service“.

„IBM Trusteer Rapport Cloud Services“ (įskaitant „Rapport for Remediation“ arba „Rapport for Mitigation“, diegiant kartu su „Pinpoint Cloud Services“) ir „IBM Trusteer Mobile Browser Cloud Services“:

Klientas įgalioja IBM gauti išsamius sutikimus, reikalingus įgalinti teisėtą „Cloud Service“ naudojimą, ir rinkti ir apdoroti informaciją, kaip aprašyta Galutinio vartotojo licencijos sutartyje adresu https://www.trusteer.com/support/end-user-license-agreement. Jei Klientas nustato, kad jis (o ne IBM) tvarkys komunikaciją su galutiniais vartotojais dėl jų sutikimo, Klientas sutinka, kad gavo arba gaus visus išsamius sutikimus, leidimus ar licencijas, reikalingas įgalinti teisėtą „Cloud Service“ naudojimą ir leidžiančias IBM, kaip Kliento duomenų apdorotojui, rinkti ir apdoroti informaciją per „Cloud Service“.

8.4 Saugos duomenų naudojimas

Kartu su „Cloud Service“, kuri apima ataskaitų teikimą, IBM parengs ir tvarkys iš „Cloud Service“ surinktą informaciją, iš kurios buvo pašalinti identifikavimo duomenys ir (arba) kuri buvo sukaupta vienoje vietoje („Saugos duomenys“). Saugos duomenys neidentifikuos Kliento, jo Priskirtų dalyvių ar asmens, išskyrus atvejus, nurodytus toliau esančiame d punkte. Klientas sutinka, kad IBM gali nuolatos naudoti ir (arba) kopijuoti Saugos duomenis tik šiais tikslais:

a. publikuojant ir (arba) platinant Saugos duomenis (pvz., su kibernetine sauga susijusiuose rinkiniuose ir (arba) analizėse);

b. kuriant arba tobulinant produktus ar paslaugas;

c. atliekant vidinį tyrimą arba tyrimą su trečiosiomis šalimis;

d. teisėtai bendrinant patvirtintą informaciją apie trečiųjų šalių nusikaltėlius ir

e. „Policy Manager“ taisyklėms, iš kurių pašalinta asmeninė informacija.

8.5 Tarptautiniai perdavimai

Klientas sutinka, kad IBM gali keliose valsybėse tvarkyti turinį, įskaitant visus Asmens duomenis, kaip nurodyta anksčiau pateiktame skyriuje „Teisėtas naudojimas ir sutikimas“, remdamasi atitinkamais įstatymais ir reikalavimais, kartu su tvarkytojais ir antriniais tvarkytojais iš toliau nurodytų šalių, kurios nepriklauso Europos Ekonominei Ervei, ir šalių, kuriose, Europos Komisijos nuomone, užtikrinami adekvatūs saugos lygiai, pvz., JAV.

8.6 Duomenų privatumas

Jei Klientas padaro asmens duomenis prieinamus „Cloud Service“ ES šalyse narėse, Islandijoje, Lichtenšteine, Norvegijoje ar Šveicarijoje arba jei Klientas tose šalyse turi Priskirtų dalyvių ar Kliento įrenginių, tada Klientas (kaip vienintelis valdytojas) nurodo IBM (kaip apdorotojui) apdoroti asmens duomenis (pagal sąlygas, nurodytas ES direktyvoje 95/46/EB). IBM apdoros jūsų asmens duomenis tik tiek, kiek reikalinga norint teikti „Cloud Service“ pasiūlymą pagal IBM paskelbtus „Cloud Services“ aprašus, o Klientas sutinka, kad bet koks toks apdorojimas atitinka Kliento nurodymus. IBM per Klientų portalą pakankamai iš anksto praneš, jei IBM iš esmės keis Asmens duomenų, kaip „Cloud Service“ dalies, apdorojimo vietą arba apsaugos būdą. Klientas gali nutraukti paveiktos „Cloud Service“ esamą prenumeratos laikotarpį pateikęs IBM įspėjimą raštu per trisdešimt (30) dienų nuo IBM pranešimo Klientui apie keitimą.

Šalys arba atitinkamos jų susijusios įmonės gali sudaryti atskiras standartines nemodifikuotas ES tipinių sąlygų sutartis, remdamosi EB sprendimu 2010/87/ES, pašalinusios neprivalomus punktus. Visi ginčai ar atsakomybė, kylanti dėl šių sutarčių, net jei jas sudarė susijusios įmonės, šalių bus sprendžiami taip, tarsi tarp šių šalių kilęs ginčas ar atsakomybė būtų apibrėžti šios Sutarties sąlygose.

a. Klientas sutinka, kad teikiant paslaugas Vokietijos duomenų centre, kaip apibrėžta aprūpinimo proceso metu, IBM gali apdoroti turinį, įskaitant bet kuriuos Asmens duomenis, už šalies ribų kartu su toliau nurodytais apdorotojais ir antriniais apdorotojais:

Apdorotojo / antrinio apdorotojo pavadinimas	Vaidmuo (duomenų apdorotojas arba antrinis apdorotojas)	Vieta
IBM sutartį sudarantis objektas	Apdorototas	Kaip nurodyta Operacijų dokumente
„Amazon Web Services (Germany)“	Antrinis apdorotojas	Vokietija
„IBM Ireland Ltd.“	Apdorototas	Airija
„IBM Israel Ltd.“	Apdorototas	Izraelis

Kai paslaugos teikiamos per Vokietijos duomenų centrą, kai kurias kliento palaikymo paslaugas gali teikti „Trusteer“ darbuotojai, esantys bet kurioje Europos Sąjungos šalyje.

b. Klientas sutinka, kad teikiant paslaugas Japonijos duomenų centre, kaip apibrėžta aprūpinimo proceso metu, IBM gali apdoroti turinį, įskaitant bet kuriuos Asmens duomenis, už šalies ribų kartu su toliau nurodytais apdorotojais ir antriniais apdorotojais:

Apdorotojo / antrinio apdorotojo pavadinimas	Vaidmuo (duomenų apdorotojas arba antrinis apdorotojas)	Vieta
IBM sutartį sudarantis objektas	Apdorototas	Japonija, kaip nurodyta Operacijų dokumente
„Amazon Web Services (Japan)“	Antrinis apdorotojas	Japonija
„IBM Ireland Ltd.“	Apdorototas	Airija
„IBM Israel Ltd.“	Apdorototas	Izraelis

c. Klientas sutinka, kad teikiant paslaugas JAV duomenų centre, IBM gali apdoroti turinį, įskaitant bet kuriuos Asmens duomenis, už šalies ribų kartu su toliau nurodytais apdorotojais ir antriniais apdorotojais:

Apdorotojo / antrinio apdorotojo pavadinimas	Vaidmuo (duomenų apdorotojas arba antrinis apdorotojas)	Vieta
IBM sutartį sudarantis objektas	Apdorototas	Kaip nurodyta Operacijų dokumente
„Amazon Web Services LLC“	Antrinis apdorotojas	Jungtinės Amerikos Valstijos
„IBM Ireland Ltd.“	Apdorototas	Airija
„IBM Israel Ltd.“	Apdorototas	Izraelis
„IBM Corp“	Apdorototas	Jungtinės Amerikos Valstijos

d. Jei paslaugos teikiamos per 8.5.c dalyje virš „JAV duomenų centro“ išvardytus duomenų centrus, IBM taip pat gali apdorojimą atlikti per vieną arba kelis toliau nurodytus tinkamus antrinius apdorotojus, kaip apibrėžta vykstant aprūpinimo procesui:

Apdorotojo / antrinio apdorotojo pavadinimas	Vaidmuo (duomenų apdorotojas arba antrinis apdorotojas)	Vieta
„Amazon Web Services (Australia)“	Antrinis apdorotojas	Australija
„Amazon Web Services (Singapore)“	Antrinis apdorotojas	Singapūras
„Amazon Web Services (Ireland)“	Antrinis apdorotojas	Airija

e. Klientas sutinka, kad, paskelbusi Klientų portale, IBM gali perkelti apdorojimą iš „Amazon Web Services“ į IBM duomenų centrus. Be to, IBM gali, paskelbusi Klientų portale, keisti anksčiau pateiktų antrinių apdorotojų sąrašus.

f. Paskyros turėtojo duomenys bus apdorojami regione, kuriame paskyros turėtojas pirmą kartą įdiegė Paskyros turėtojo Kliento Programinę įrangą. Tai gali reikšti, kad Paskyros turėtojo turinys gali būti apdorojamas ir pradiniame regione, ir regione, dėl kurio buvo susitarta su Klientu.

g. Kliento palaikymo duomenys saugomi Salesforce.com debesies serveryje, kuris yra Airijoje.

h. Siekiant aiškumo „Trusteer Fraud Protection“ yra integruotas sprendimas, todėl, Klientui nutraukus vieną iš šių „Cloud Service“, IBM gali išsaugoti Kliento duomenis norėdama Klientui suteikti likusias „Cloud Service“ pagal šį Paslaugos aprašą.

9. Paslaugos lygio sutartis

IBM užtikrina toliau nurodytus „Cloud Service“ pasiekiamumo paslaugos lygio sutarties (PLS) įsipareigojimus, kaip nurodyta TSD. PLS neteikia garantijų. PLS yra pasiekiama Klientui ir yra skirta naudoti tik gamybos aplinkose.

9.1 Pasiekiamumo kreditai

Sužinojęs, kad įvykis paveikė „Cloud Service“ pasiekiamumą, Klientas turi per 24 valandas IBM techninio palaikymo centre užregistruoti 1 sudėtingumo lygio palaikymo kortelę. Klientas turi, kiek galėdamas, padėti IBM diagnozuoti problemą ir ją išspręsti.

Palaikymo kortelės pretenzija dėl PLS sąlygų nesilaikymo turi būti pateikta per tris darbo dienas nuo sutartinio mėnesio pabaigos. Kompensacija už pagrįstą PLS pretenziją bus suteikta kaip kreditas būsimoje „Cloud Service“ sąskaitoje faktūroje, atsižvelgiant į laikotarpį, per kurį „Cloud Service“ gamybos sistema buvo nepasiekiama („Prastova“). Prastova skaičiuojama nuo tada, kai Klientas praneša apie įvykį, iki tada, kai „Cloud Service“ atkuriama. Ji neapima laiko, susijusio su paslaugos teikimo nutraukimu dėl suplanuotos arba informuotos techninės priežiūros, dėl nuo IBM nepriklausančių priežasčių, problemų, susijusių su Kliento ar trečiosios šalies turiniu, technologijomis, dizainu ar instrukcijomis, nepalaikomų sistemų konfigūracijų ir platformų ar kitų Kliento klaidų arba Kliento sukeltų saugos problemų ar Kliento saugos tikrinimo. IBM taikys aukščiausią galimą kompensaciją, pagrįstą kiekvieno

sutartinio mėnesio „Cloud Service“ kaupiamuoju pasiekiamumu, kaip nurodyta toliau esančioje lentelėje. Bendra kompensacijos suma, atsižvelgiant į bet kurį sutartinį mėnesį, negali neviršyti 10 procentų vienos dvyliktosios (1/12) metinio mokesčio už „Cloud Service“ dalies.

9.2 Paslaugų lygiai

„Cloud Service“ pasiekiamumas per sutartinį mėnesį

Pasiekiamumas per sutartinį mėnesį	**Kompensacija (% mėnesinio prenumeratos mokesčio* už „Audio Conferencing for Connections Meetings“ sutartinį mėnesį, kuris yra pretenzijos dalykas)**
< 99,5 %	2 %
<98,0 %	5 %
< 96,0 %	10 %

* Jei „Cloud Service“ buvo įsigyta iš IBM verslo partnerio, mėnesio prenumeratos mokestis bus apskaičiuojamas, atsižvelgiant į tuo metu galiojančiame kainoraštyje nurodytą „Cloud Service“ kainą, kuri galioja pretenzijoje nurodytą sutartinį mėnesį, pritaikant 50 % nuolaidą. IBM suteiks nuolaidą Klientui tiesiogiai.

Kiekvienos „Cloud Service“ ir kiekvienos Kliento taikomosios programos paslaugų lygiai ir susiję paslaugų kreditai vertinami atskirai.

Pagal Taikomosios programos teises skaičiuojant „Cloud Services“ PLS kreditus, Pasiekiamumas bus vertinamas atsižvelgiant į toliau pateiktas rekomendacijas:

- Kiekviena Taikomoji programa turės priskirtą svertinę dalį pagal suskaičiuotą seansų skaičių sutartą mėnesį.
- Kiekvienos Taikomosios programos „Cloud Service“ prastova sutartinį mėnesį bus kaupiama atskirai.

Toliau pateikiamas pavyzdys, kaip apskaičiuojama vieno mėnesio veikla ir susiję papildomi kreditai. Toliau pateikiamas pavyzdys tik iliustravimo tikslais:

Mažmeninės prekybos taikomosios programos	**Dalis bendro # seansų skaičiaus per nurodytą sutartinį mėnesį**	**Bendras prastovų skaičius per sutartinį mėnesį**	**Papildomos prastovų minutės**
Mažmeninės prekybos taikomoji programa A	40 %	300 min.	40 % x 300 min. = 120 min.
Mažmeninės prekybos taikomoji programa B	20 %	250 min.	20 % x 250 min. = 50 min.
Mažmeninės prekybos taikomoji programa C	40 %	150 min.	40 % x 150 min. = 60 min.
			Bendras papildomų prastovų minučių skaičius = 230

Pasiekiamumas, išreikštas procentine išraiška, apskaičiuojamas iš bendro minučių skaičiaus sutartinį mėnesį atėmus bendrą papildomų Prastovų minučių skaičių sutartinį mėnesį, gautą rezultatą padalijus iš bendro minučių skaičiaus sutartinį mėnesį. Pavyzdyje skaičiuojama atsižvelgiant į anksčiau pateiktą papildomų minučių skaičiaus pavyzdį:

Iš viso sutartinį mėnesį, kurį sudarė 30 dienų, buvo 43 200 min. - papildomų Prastovų minučių = 42 970 min. _____ Iš viso 43 200 minučių	= 2 % Pasiekiamumo kredito už 99,4 % pasiekiamumo per sutartinį mėnesį

10. Techninis palaikymas

„Cloud Services“ techninis palaikymas yra prieinamas Klientui ir jo Priskirtiems dalyviams siekiant padėti jiems naudotis „Cloud Services“.

„Standard Support“ yra įtrauktas į visų pasiūlymų prenumeratą. „Trusteer Rapport Mandatory Service“, kuri yra „Trusteer Rapport“ priedas, taikoma būtina pagrindinės „Trusteer Rapport“ prenumeratos „Premium Support“ sąlyga.

Naudojant bet kurią „Cloud Service“, „Premium Support“ prenumerata pasiekiama už papildomą mokestį, išskyrus „IBM Trusteer Mobile SDK Cloud Services“ ir „IBM Trusteer Rapport Mandatory Service Cloud Services“. Kreipkitės į savo IBM pardavimo atstovą arba IBM verslo partnerį.

„Standard Support“:

- palaikymas 8-17 val. vietos laiku.
- Klientai ir jų Priskirti dalyviai gali pateikti palaikymo korteles elektroniniu būdu, kaip išsamiai nurodyta Programinės įrangos kaip paslaugos [SaaS] palaikymo vadove.
- Klientai gali pasiekti Klientų palaikymo portalą ir gauti pranešimus, dokumentus, atvejų analizes ir DUK apsilankę http://www-01.ibm.com/software/security/trusteer/support/.
- Palaikymo parinktis ir išsamią informaciją apie Programinę įrangą kaip paslaugą [SaaS] rasite palaikymo vadove http://www-01.ibm.com/software/support/handbook.html.

„Premium Support“:

- Visų sudėtingumo lygių palaikymas ištisą parą.
- Klientai gali gauti palaikymą tiesiogiai telefonu ir pateikę užklausą dėl atgalinio skambinimo.
- Klientai ir jų Priskirti dalyviai gali pateikti palaikymo korteles elektroniniu būdu, kaip išsamiai nurodyta Programinės įrangos kaip paslaugos [SaaS] palaikymo vadove.
- Klientai gali pasiekti Klientų palaikymo portalą ir gauti pranešimus, dokumentus, atvejų analizes ir DUK apsilankę http://www-01.ibm.com/software/security/trusteer/support/.
- Palaikymo parinktis ir išsamią informaciją apie Programinę įrangą kaip paslaugą [SaaS] rasite palaikymo vadove http://www-01.ibm.com/software/support/handbook.html.

11. Teisių suteikimo ir sąskaitų išrašymo informacija

11.1 Mokesčio apskaičiavimas

„Cloud Service“ pateikiama pagal mokesčių apskaitos metriką, nurodomą Operacijų dokumente:

a. Priskirtas dalyvis yra matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Kiekvienas asmuo ar objektas, turintis teisę dalyvauti bet kurioje „Cloud Service“ valdomoje arba stebimoje paslaugos teikimo programoje, yra Priskirtas dalyvis. Reikia įsigyti teises, kurių pakaktų visiems „Cloud Service“ valdomiems ar stebimiems Priskirtiems dalyviams matavimo laikotarpiu, nurodytu Kliento Operacijų dokumente.

   Kiekviena paslaugų teikimo programa, kurią valdo „Cloud Service“, analizuojama atskirai, o tada visos sudedamos į vieną. Fiziniai asmenys arba įmonės, turinčios teisę naudoti kelias paslaugų teikimo programas, turi turėti atskiras teises.

   Šių „Cloud Service“ teisių suteikimo tikslais Priskirtas dalyvis yra galutinis Kliento vartotojas, turintis unikalius Kliento Verslo arba Mažmeninės prekybos programos prisijungimo kredencialus.

b. Kliento įrenginys yra matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Kliento įrenginys yra vieno vartotojo kompiuterinis įrenginys, specialiosios paskirties jutiklis arba telemetrijos įrenginys, kuris teikia arba gauna užklausas vykdyti komandų, procedūrų arba taikomųjų programų rinkinį iš kitos, paprastai serverio arba serverio valdomos, kompiuterinės sistemos arba teikia jai duomenis. Keli klientų įrenginiai gali bendrai naudoti prieigą prie bendro serverio. Kliento įrenginyje gali būti kai kurios tvarkymo funkcinės galimybės arba būti programuojamas leisti vartotojui dirbti. Klientas turi įsigyti teises kiekvienam Kliento įrenginiui, kuris veikia, teikia duomenis, naudoja teikiamas paslaugas ar kitokiu būdu naudoja prieigą prie „Cloud Service“ matavimo laikotarpiu, nurodytu Kliento Operacijų dokumente.

c. Taikomoji programa yra matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Taikomoji programa – tai programinė įranga unikaliu pavadinimu. Reikia įsigyti teises, skirtas

kiekvienai Taikomajai programai pasiekti ir naudoti matavimo laikotarpiu, nurodytu Kliento TSD arba Operacijų dokumente.

„Cloud Service“ pasiūlymuose taikomoji programa yra viena Kliento Verslo arba Mažmeninės prekybos programa.

d. Įsipareigojimas yra matavimo vienetas, pagal kurį galima gauti paslaugas. Įsipareigojimas apima specialistų ir (arba) mokymo paslaugas, susijusias su „Cloud Service“. Reikia įsigyti teises, kurių pakaktų kiekvienam Įsipareigojimui padengti.

12. Atitiktis ir auditas

Prieiga prie „IBM Trusteer Fraud Protection Cloud Services“ priklauso nuo maksimalaus Taikomųjų programų, Priskirtų dalyvių arba Kliento įrenginių skaičiaus, nurodyto Operacijų dokumente. Klientas yra atsakingas už tai, kad Taikomųjų programų, Priskirtų dalyvių ir (arba) Kliento įrenginių skaičius neviršytų maksimalaus Sandorio dokumente nurodyto kiekio.

Norėdama patikrinti, ar maksimalus Taikomųjų programų, Priskirtų dalyvių ir (arba) Kliento įrenginių skaičius atitinka, IBM gal atlikti auditą.

13. Terminas ir atnaujinimo galimybės

„Cloud Service“ naudojimo terminas prasideda nuo dienos, kai IBM praneša Klientui, kad jis turi prieigą prie „Cloud Service“, kaip aprašyta TSD. TSD bus nurodyta, ar „Cloud Service“ bus atnaujinama automatiškai, naudojama nepertraukiamo naudojimo pagrindu ar nutraukiama laikotarpio pabaigoje.

Taikant automatinį atnaujinimą, jei Klientas mažiausiai prieš 90 dienų iki termino galiojimo pabaigos nepateikė prašymo raštu nebeatnaujinti, „Cloud Service“ bus automatiškai atnaujinta TSD nurodytam laikotarpiui.

Naudojant nuolat, „Cloud Service“ pasiekiamumas pratęsiamas kiekvieną mėnesį, kol Klientas prieš 90 dienų iki nutraukimo raštu pateiks prašymą nutraukti. Praėjus 90 dienų laikotarpiui, „Cloud Service“ bus pasiekiama iki kalendorinio mėnesio pabaigos.

14. Papildomos sąlygos

14.1 Įgalinimo programinė įranga

Ši „Cloud Service“ apima įgalinimo programinę įrangą, kurią galima naudoti tik kartu su Kliento naudojama „Cloud Service“ ir tik „Cloud Service“ naudojimo laikotarpiu.

14.2 „IBM Trusteer“ metinio prenumeratos mokesčio didėjimas

IBM pasilieka teisę koreguoti „Cloud Service“ prenumeratos mokestį. Prenumeratos mokesčio koregavimas atsispindės kainose, nurodytose Pasiūlyme ir taikomose Pasiūlymo laikotarpiu. Papildomi prenumeratos mokesčio koregavimai, kurie bus taikomi ne dažniau nei kartą per dvylika (12) mėnesių IBM nustatyta procentine dalimi, neviršijančia 3 %, gali būti taikomi, kai „Cloud Services“ laikotarpis yra pratęsiamas dėl automatinio atnaujinimo arba nuolatinio naudojimo. Šie mokesčių koregavimai nekeičia Kliento teisių į „Cloud Service“ ar mokesčio apskaitos sistemos, pagal kurią įsigyjamos „Cloud Service“. IBM verslo partneriai yra nepriklausomi nuo IBM ir vienašališkai nustato savo kainas ir sąlygas.