„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 Sandorio dokumentai.

1. „Cloud Service“

Šis Paslaugos aprašas taikomas šiems „Cloud Services“ pasiūlymams:

„Pinpoint Assure Cloud Services“:

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

„Rapport Cloud Services“:

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

„Pinpoint Cloud Services“:

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

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

„Cloud Services“ mobiliesiems:

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

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

1.1.2 Mažmeninės prekybos „Cloud Services“

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

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 II“

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

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

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 II for Business“ arba „IBM Trusteer Rapport II 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 II“

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

b. Papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail“ arba „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail“:
   - „IBM Trusteer Rapport Remediation for Retail“

- „IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail“

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

1.1.5 Papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Detect Standard“ ir (arba) „IBM Trusteer Pinpoint Detect Premium“, ir (arba) „IBM Trusteer Pinpoint Detect Standard for Retail“, ir (arba) „IBM Trusteer Pinpoint Detect Premium for Retail“, ir (arba) „IBM Trusteer Pinpoint Detect Standard for Business“, ir (arba) „IBM Trusteer Pinpoint Detect Premium for Business“

a. Papildomos „Cloud Services“, skirtos „IBM Trusteer Detect Standard for Business“ ir (arba) „IBM Trusteer Pinpoint Detect Premium for Business“:
   - „IBM Trusteer Pinpoint Detect Standard Additional Applications for Business“
   - „IBM Trusteer Pinpoint Detect Premium Additional Applications for Business“
   - „IBM Trusteer Digital Content Pack for Business“
   - „IBM Trusteer New Account Fraud for Business“

b. Papildomos „Cloud Services“, skirtos „IBM Trusteer Detect Standard for Retail“ ir (arba) „IBM Trusteer Pinpoint Detect Premium for Retail“:
   - „IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail“
   - „IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail“
   - „IBM Trusteer Digital Content Pack for Retail“
   - „IBM Trusteer New Account Fraud for Retail“

c. Papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Detect Standard“ ir (arba) „IBM Trusteer Pinpoint Premium“:
   - „IBM Trusteer Pinpoint Detect Standard Application“
   - „IBM Trusteer Pinpoint Detect Premium Application“

d. Papildomos „Cloud Services“, skirtos „IBM Trusteer Pinpoint Detect Premium“
   - „IBM Trusteer Pinpoint Verify“

„IBM Trusteer Pinpoint Detect Standard“, „IBM Trusteer Pinpoint Detect Premium“, „IBM Trusteer Pinpoint Detect Standard for Retail“, „IBM Trusteer Pinpoint Detect Premium for Retail“, „IBM Trusteer Pinpoint Detect Standard for Business“ arba „IBM Trusteer Pinpoint Detect Premium for Business“ prenumerata yra šiame skyriuje išvardytų susietų papildomų „Cloud Services“ būtina sąlyga.

1.1.6 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 programine įranga – reiškia „IBM Trusteer Rapport“ kliento įgalinimo programinę įrangą arba bet kurio kito kliento įgalinimo programinę įrangą, kuri teikiama su kai kuriomis „Cloud Services“ diegti galutinio vartotojo prietaise.

„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.

1.3 „IBM Trusteer Rapport Cloud Services“

1.3.1 „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 arba kito Kliento Įrenginio mokesčių apskaitos sistemą. Verslo pasiūlymai parduodami paketais po 10 Priskirtų dalyvių arba 10 Kliento Įrenginių. Mažmeninės prekybos pasiūlymai parduodami paketais po 100 Priskirtų dalyvių arba 100 Kliento Įrenginių.

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.

1.3.2 Papildomos pasirinktinės „Cloud Services“, skirtos „IBM Trusteer Rapport II for Business“ ir (arba) „IBM Trusteer Rapport II for Retail“

„IBM Trusteer Rapport II Cloud Services“ prenumerata yra būtina sąlyga norint prenumeruoti bet kurias iš toliau nurodytų 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 arba Kliento Įrenginių, kuriuose veikia Paskyros turėtojo Kliento programinė įranga ir kurie yra sutikę su EULA sąlygomis, bent kartą yra autentifikuoti kaip besinaudojantys Kliento Verslo ir (arba) Mažmeninės prekybos taikomąja (-omis) programa (-omis), o Kliento konfigūracija turi apimti Vartotojo ID rinkinį.

1.3.3 „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.

Šis pasiūlymas taikomas tik pagal Priskirto dalyvio mokesčių apskaitos sistemą.

1.3.4 „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.

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

„Premium“ palaikymą galima įsigyti pagal Priskirto dalyvio mokesčių apskaitos sistemą arba kito Kliento Įrenginio mokesčių apskaitos sistemą. Verslo pasiūlymai parduodami paketais po 10 Priskirtų dalyvių arba 10 Kliento Įrenginių. Mažmeninės prekybos pasiūlymai parduodami paketais po 100 Priskirtų dalyvių arba 100 Kliento Įrenginių.

1.3.5 „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.

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

1.3.6 „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 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.

1.3.7 „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.

1.4 „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“.

1.4.1 „IBM Trusteer Pinpoint Malware Detection“

Aptikus kenkėjiškos įrangos „IBM Trusteer Pinpoint Malware 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 II Cloud Services“ tokiu būdu, kuris paveiktų Priskirto dalyvio patirtį, pvz., kiti galės 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).

1.4.2 „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 ir (arba) Mažmeninės prekybos Standartiniai leidimai yra greitai įdiegiami sprendimai, suteikiantys 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.

1.4.3 Papildomos pasirinktinės „Cloud Services“, skirtos „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail“ ir (arba) „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail“, ir (arba) „IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business“, ir (arba) „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business“

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

1.4.4 „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 „IBM Trusteer Pinpoint Malware Detection II“ prenumeratą, veikiančią Kliento 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.

1.4.5 „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 II“, privalo 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.

„IBM Trusteer Pinpoint Malware Detection Additional Applications“, skirtas „IBM Trusteer Pinpoint Malware Detection II Standard Edition“ arba „IBM Trusteer Pinpoint Malware Detection II Advanced Edition“, diegiant bet kokioje papildomoje Taikomojoje programoje (šalia pirmosios Taikomosios programos), reikalingos „IBM Trusteer Pinpoint Malware Detection Additional Applications“ teisės.

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

- Naudojant „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail“, norint diegti bet kokią papildomą Mažmeninės prekybos programą (šalia pirmosios Taikomosios programos), būtinos „IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail“ teisės.
- Naudojant „IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business“ arba „IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business“, norint diegti bet kokią papildomą Verslo programą (šalia pirmosios Taikomosios programos), būtinos „IBM Trusteer Pinpoint Malware Detection Additional Applications for Business“ teisės.

1.5 „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 Taikomąja (-osiomis) programa (-omis), dėl kurios (-ių) Klientas užsiprenumeravo „Cloud Service“, rezultatą, 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).

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

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 Mažmeninės prekybos arba Verslo taikomosios 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 tiesiogiai Klientui pateikia naršyklių arba mobiliųjų įrenginių (naudojant vietinę naršyklę arba Kliento mobiliąją programą), pasiekiančių Mažmeninės prekybos arba Verslo programą, rizikos vertinimo balus.

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

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

Paslaugą galima įsigyti paketais po 100 Priskirtų dalyvių arba paketais po 100 Ryšių. Jeigu Klientas pasirenka įsigyti paslaugą pagal Ryšius, Papildomos taikomosios programos mokestis taikomas nuo pirmosios taikomosios programos.

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

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 Mažmeninės prekybos arba Verslo taikomosios 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. Paslauga apima iki 200 valandų bendrai naudojamų diegimo paslaugų išteklių kiekvienai taikomajai programai ir 200 valandų bendrai naudojamų saugos analizės išteklių kiekvienai taikomajai programai nustatymo metu. Nuolatinės paslaugos apima 20 valandų diegimo priežiūros per metus kiekvienai taikomajai programai ir 100 valandų kiekvienos taikomosios programos saugos tyrimų per metus. Už visus papildomus darbus taikomas papildomas mokestis.

„Pinpoint Detect“ gali naudoti tiek mobiliųjų, tiek interneto kanalų operacijas. Jei įtraukiamos Mobiliosios operacijos, „Pinpoint“ naudojama pagal Ryšius. 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.

„IBM Trusteer Pinpoint Detect Premium for Retail“ ir „Business“ paslaugas galima įsigyti 100 Priskirtų dalyvių paketais, o „IBM Trusteer Pinpoint Detect Premium“ – 100 Ryšių paketais. Jeigu Klientas pasirenka įsigyti paslaugą pagal Ryšius, Papildomos taikomosios programos mokestis taikomas nuo pirmosios taikomosios programos.

„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.

1.5.3 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“ arba „IBM Trusteer Pinpoint Detect Standard“.

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

- „IBM Trusteer Rapport for Mitigation for Retail“ 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.
- „IBM Trusteer Rapport for Mitigation for Business“ skirtas ištirti, panaikinti, blokuoti ir pašalinti kenkėjišką programinę įrangą iš užkrėstų įrenginių (asmeninių / MAC kompiuterių), priklausančių Kliento Priskirtiems dalyviams, kurie turi prieigą prie Kliento Verslo 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 Verslo programoje. Klientas gali naudoti šias „Cloud Service“ tik pasitelkęs Priskirtus dalyvius, turinčius prieigą prie Kliento Verslo programos, ir naudoti išskirtinai tik kaip įrankį, galintį ištirti ir pataisyti konkretų užkrėstą įrenginį (asmeninį / MAC kompiuterį) specialiąja tvarka. „IBM Trusteer Rapport for Mitigation for Business“ 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 Verslo 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.

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

Paslauga apima iki 200 valandų bendrai naudojamų diegimo paslaugų išteklių kiekvienai taikomajai programai ir 200 valandų bendrai naudojamų saugos analizės išteklių kiekvienai taikomajai programai nustatymo metu. Nuolatinės paslaugos apima 20 valandų diegimo priežiūros per metus kiekvienai taikomajai programai ir 100 valandų kiekvienos taikomosios programos saugos tyrimų per metus.

- „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 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 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.
- „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.

1.5.6 „IBM Trusteer Pinpoint Detect Standard Application“ ir (arba) „IBM Trusteer Pinpoint Detect Premium Application“

Ši paslauga taikoma interneto ir mobiliesiems kanalams.

Paslauga apima iki 200 valandų bendrai naudojamų diegimo paslaugų išteklių kiekvienai taikomajai programai ir 200 valandų bendrai naudojamų saugos analizės išteklių kiekvienai taikomajai programai nustatymo metu. Nuolatinės paslaugos apima 20 valandų diegimo priežiūros per metus kiekvienai taikomajai programai ir 100 valandų kiekvienos taikomosios programos saugos tyrimų per metus.

- Norint diegti „IBM Trusteer Pinpoint Detect Standard“, kiekvienai Taikomajai programai būtinos „IBM Trusteer Pinpoint Detect Standard Application“ teisės.
- Norint diegti „IBM Trusteer Pinpoint Premium“, kiekvienai Taikomajai programai būtinos „IBM Trusteer Pinpoint Detect Premium Application“ teisės.

1.5.7 „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.

1.5.8 „IBM Trusteer Pinpoint Detect Standard for Retail Premium Support“ ir (arba) „IBM Trusteer Pinpoint Detect Standard for Business Premium Support“

Klientai, kurie įsigyja „Pinpoint Detect Standard Cloud Service“, gali įsigyti „Premium Support“ paslaugą. „Premium Support“ paslaugų aprėptis išvardyta 4 skyriuje toliau.

1.5.9 „IBM Trusteer Digital Content Pack for Retail“ ir (arba) „IBM Trusteer Digital Content Pack for Busines“

„IBM Trusteer Digital Content Pack“ suteikia saugos analitikams galimybę integruoti naujus apsaugos nuo sukčiavimo modelius, taip pat palaiko specialių modelių, skirtų reaguoti į tobulėjančias grėsmes, kūrimą ir modifikavimą. Jis apima išsamų taisyklių, įžvalgų ir strategijų rinkinį, kurį galima įsigyti kaip papildomą ir būtinąją sprendimo dalį. „Digital Content Pack“ padeda dar glaudžiau integruoti „Trusteer“ skaitmenines apsaugos nuo sukčiavimo galimybes ir „IBM Safer Payments“ mokėjimo nenaudojant grynųjų pinigų

kanalus. Naudodamas savo integruotas taisykles ir specialią verslo logiką, „Digital Content Pack“ bankams ir kitoms finansinėms įstaigoms suteikia galimybę išplėsti esamas sukčiavimo aptikimo ir prevencijos galimybes.

„IBM Trusteer Digital Content Pack for Retail“ parduodamas paketais po 100 Priskirtų dalyvių. „IBM Trusteer Digital Content Pack for Business“ parduodamas paketais po 10 Priskirtų dalyvių.

Norint „Digital Content Pack“ integruoti su „Pinpoint Detect“ ir „IBM Safer Payments“, taip pat palaikymo paslaugoms, kurioms reikalingas ypatingas dėmesys, būtinos konsultavimo paslaugos. Konsultavimo paslaugos įsigyjamos atskirai pagal atskirą darbų aprašą.

1.5.10 „IBM Trusteer New Account Fraud for Retail“ ir (arba) „IBM Trusteer New Account Fraud for Business“

Ši paslauga, pasiekiama „Pinpoint“ prenumeratoriams, skirta anomalijoms aptikti, įtartinoms veikloms pažymėti ir įspėjimams generuoti iš anksto naujos paskyros kūrimo proceso metu. Paslauga stebi naujas paskyras, kad identifikuotų naują veiklą, susijusią su apgaulingo pašto paskyromis ir naujų paskyrų profiliavimu, ir suteiktų išankstinį įspėjimą, kad nauja paskyra gali būti mulo paskyra arba naudojama apgaulei, naudojant TMA pasiekiamas naudojimo ataskaitas.

„IBM Trusteer New Account Fraud for Retail“ ir „IBM Trusteer New Account Fraud for Business“ siūloma paketais po 10 API iškvietų.

1.5.11 „IBM Trusteer Pinpoint Verify“

Kad galėtų prenumeruoti šią „Cloud Service“, Klientas privalo turėti galiojančią „IBM Trusteer Pinpoint Detect Premium“ prenumeratą.

Ši „Cloud Service“ suteikia galimybę vartotojams, bandantiems pasiekti skaitmeninę paslaugą, taikyti antrą autentifikavimo veiksnį, norint patikrinti jų tapatybę. Ši galimybė suteikiama „Pinpoint Detect Premium“, kad būtų galima taikyti antrąjį autentifikavimo veiksnį apsaugotose taikomosiose programose. Sprendimą, kada reikalauti vartotojų antrojo veiksnio autentifikavimo, nustato apsaugota taikomoji programa ir jis gali būti pagrįstas „Pinpoint Detect Premium“ platformos pateiktomis rekomendacijomis arba bet kuria kita apsaugotos taikomosios programos apibrėžta politika.

1.6 „IBM Trusteer Pinpoint Assure“

Paslauga pažymi įtartinas veiklas ir generuoja įspėjimus kuriant naują paskyrą / registruojantis. Paslauga stebi paskyros registracijos procesą, kad identifikuotų veiklą, susijusią su apgaulėmis, ir iš anksto įspėtų, kad nauja paskyra gali būti mulo paskyra arba naudojama siekiant apgauti, pasitelkus TMA pasiekiamas naudojimo ataskaitas.

„IBM Trusteer Pinpoint Assure“ siūloma paketais po 100 Ryšių.

1.6.1 Pasirinktinės „IBM Trusteer Pinpoint Assure“ paslaugos

1.6.2 „IBM Trusteer Pinpoint Assure Application“

Norint diegti „IBM Trusteer Pinpoint Assure“ bet kurioje Taikomojoje programoje, reikalingos „IBM Trusteer Pinpoint Assure Application“ teisės.

„IBM Trusteer Pinpoint Assure“ siūloma įsigyti pagal taikomąją programą.

1.6.3 „IBM Trusteer Mobile Carrier Intelligence“ ir (arba) „IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect“

Kad galėtų prenumeruoti šią „Cloud Service“, Klientas privalo turėti galiojančią „IBM Trusteer Pinpoint Assure“ arba „IBM Trusteer Pinpoint Detect“ prenumeratą.

Ši „Cloud Service“ papildo „IBM Trusteer Pinpoint Assure“ ir (arba) „IBM Trusteer Pinpoint Detect“ suteikdama papildomos informacijos ir konteksto apie mobiliuosius numerius, pateikiamus į bet kurią iš šių „Cloud Services“, padėdama nustatyti esamo seanso sukčiavimo riziką. Klientas gali pateikti užklausą šiai„Cloud Service“, kad sužinotų pateikto telefono numerio charakteristikas, pvz., su numeriu susieto operatoriaus informaciją.

Šios „Cloud Service“ pateikiamus duomenis apie mobiliuosius numerius („Mobilioji informacija“) galima naudoti tik Kliento vidiniais tikslais ir laikyti ne ilgiau nei trisdešimt (30) dienų. Po šio laikotarpio Klientas privalo pakartotinai pateikti užklausą „Cloud Service“ dėl to paties telefono numerio, kad gautų su šiuo numeriu susijusią Mobiliąją informaciją, ir negali tiesiog pakartotinai naudoti iš ankstesnės užklausos gautos Mobiliosios informacijos. Klientas negali laikyti talpykloje, išskyrus, kaip leidžiama anksčiau,

pakartotinai naudoti arba visos ar dalies Mobiliosios informacijos naudoti kartu su bet kokia duomenų gavyba, taip pat negali archyvuoti jokios Mobiliosios informacijos.

1.7 „IBM Trusteer Remotely Delivered Services“

„IBM Trusteer Remotely Delivered Services“ teikiamos kaip pasirinktinis priedas, skirtas „Pinpoint Detect Premium“ ir „Pinpoint Assure Cloud Services“.

1.7.1 „IBM Trusteer Project Management and Consultancy Services“

Ši paslauga suteikia iki 200 valandų konsultavimo paslaugų, kurias teikdama IBM atliks kelis arba visus iš šių veiksmų:

a. Pradines nustatymo paslaugas: dažnus periodinius susitikimus, projekto valdymo paslaugas

b. Politikos valdymą: nuolatinį palaikymą

Pasiūlymą galima įsigyti pagal Įsipareigojimą.

1.7.2 „IBM Trusteer Security Research Consultancy Services“

Ši konsultavimo paslauga apima iki 200 valandų bendrai naudojamų išteklių saugos analizei, kad suteiktų papildomas paslaugas prie apibrėžto sprendimo ir „Premium“ palaikymo (kai taikoma), ir ji apima:

a. Išplėstinį apgaulių tyrimą: kassavaitinius susitikimus ir mokymą.

b. Aukšto prioriteto Kliento leidimo palaikymą

c. Nuolatinį tinkintų taisyklių tyrimą ir palaikymą

Pasiūlymą galima įsigyti pagal Įsipareigojimą.

1.7.3 „IBM Trusteer Training Services“

Ši konsultavimo paslauga skirta teikti papildomas paslaugas prie apibrėžto sprendimo ir „Premium“ palaikymo (kai taikoma) ir apima Kliento darbuotojų „Trusteer“ portfelio mokymo paslaugas.

Pasiūlymą galima įsigyti pagal Įsipareigojimą.

1.8 „IBM Trusteer Mobile Cloud Services“

1.8.1 „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 arba platintojų pavadinimų arba prekių pavadinimų reklamuodamas Kliento integruotą mobiliąją 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 negarantuoja, kad kokia nors taikomoji programa ar išvestis, sukurta naudojant su „IBM Security Mobile SDK“ pateiktus mobiliuosius įrankius, veiks, veiks bendrai su kitais įrankiais ar bus suderinama su kokia nors konkrečia mobiliąja operacinės sistemos platforma ar mobiliuoju įrenginiu.

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. Šaltinio komponentus ir Pavyzdinę medžiagą IBM teikia be palaikymo įsipareigojimų ir „TOKIĄ, KOKIA YRA“. 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.

2. Turinio ir duomenų apsauga

Duomenų tvarkymo ir Apsaugos duomenų lape (Duomenų lape) pateikiama „Cloud Service“ informacija apie įgalinto tvarkyti Turinio tipą, įtrauktus tvarkymo veiksmus, duomenų apsaugos funkcijas ir Turinio saugojimo bei grąžinimo specifiką. Visa informacija arba paaiškinimai ir sąlygos, įskaitant Kliento įsipareigojimus dėl „Cloud Service“ naudojimo ir duomenų apsaugos funkcijų, jei tokių yra, yra nustatyti šiame skyriuje. Kliento „Cloud Service“ naudojimui, remiantis Kliento pasirinktomis parinktimis, gali būti taikomas daugiau nei vienas Duomenų lapas. Duomenų lapai pasiekiami tik anglų, o ne vietos kalba. Nepaisant vietos įstatymų ar papročių, šalys sutaria, kad supranta anglų kalbą ir tai yra tinkama kalba „Cloud Service“ įsigyti ir naudoti. Toliau pateiktas (-i) Duomenų lapas (-ai) taikomas (-i) „Cloud Service“ ir

pasiekiamoms parinktims. Klientas pripažįsta, kad i) IBM gali retkarčiais modifikuoti Duomenų lapą (-us) savo nuožiūra ir ii) tokios modifikacijos anuliuos ankstesnes versijas. Bet kokio Duomenų lapo (-ų) modifikavimo tikslas yra i) patobulinti arba išaiškinti esamus įsipareigojimus, ii) palaikyti atitiktį šiuo metu taikomiems standartams ir teisės aktams arba iii) pateikti papildomus įsipareigojimus. Joks Duomenų lapo (-ų) pakeitimas reikšmingai nesumažins „Cloud Service“ duomenų saugos.

Taikomo (-ų) Duomenų lapo (-ų) saitas (-ai):

„IBM Trusteer Mobile SDK“

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

„IBM Trusteer Mobile Secure Browser“

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

„IBM Trusteer Pinpoint Assure“

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

„IBM Trusteer Pinpoint Criminal Detect“

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

„IBM Trusteer Pinpoint Detect“

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

„IBM Trusteer Pinpoint Malware Detection“

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

„IBM Trusteer Rapport“

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

„IBM Trusteer Pinpoint Verify“

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

(„IBM Cloud Identity Verify“ duomenų lapas tinka „IBM Trusteer Pinpoint Verify“)

Klientas yra įsipareigojęs imtis reikiamų veiksmų, kad užsakytų, įgalintų arba naudotų pasiekiamas „Cloud Service“ duomenų apsaugos priemones, ir prisiima atsakomybę už „Cloud Service“ naudojimą, jei Klientui nepavyksta imtis tokių veiksmų, įskaitant visų su Turiniu susijusių duomenų apsaugos ar teisinių reikalavimų laikymąsi.

IBM Duomenų tvarkymo priedas (DTP) ir DTP įrodymas (-ai), pateiktas (-i) http://ibm.com/dpa, yra taikomas (-i) ir minimas (-i) kaip Sutarties dalis, jei Turinyje esantiems asmens duomenims taikomas Europos bendrasis duomenų apsaugos reglamentas (ES/2016/679) (BDAR) ir tik tokia apimtimi. Šiai „Cloud Service“ taikomas Duomenų lapas (-ai) bus kaip DTP įrodymas (-ai). Jei taikomas DTP, IBM įsipareigojimas pateikti įspėjimą dėl Papildomų procesorių ir Kliento teisių į objektą pakeitimų bus taikomas, kaip nustatyta DTP.

2.1 EULA ir duomenų subjektų duomenų tvarkymo pagrindas

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

Jei nesutarta kitaip ir remiantis tvarkymo pagrindais, kuriuos Klientas nustatė nepriklausomai, Klientas suteikia IBM teisę teikti Galutinio vartotojo licencijos sutartį, pasiekiamą https://www.trusteer.com/support/end-user-license-agreement, kad IBM galėtų rinkti ir tvarkyti informaciją, būtiną teikiant „Cloud Services“.

2.2 Duomenų naudojimas

IBM nenaudos arba neatskleis Klientui naudojant „Cloud Service“ gautų rezultatų, kurie yra unikalūs jūsų Turinio (Įžvalgų) rezultatai ar kitaip identifikuoja Klientą. Tačiau IBM gali naudoti Turinį ir kitą iš Turinio teikiant „Cloud Service“ gautą informaciją (išskyrus tuomet, kai naudojama „Insights“), iš kurios pašalinami asmens identifikatoriai taip, kad jokių asmens duomenų nebebūtų galima priskirti konkrečiam asmeniui nepanaudojant papildomos informacijos. IBM naudos tokius duomenis tik tyrimų, tikrinimo ir pasiūlymo kūrimo tikslais.

2.3 Duomenų tvarkymas ir laikymas

2.3.1 Papildoma apdorojama vietos informacija

„Trusteer Pinpoint Verify“ paslaugų atveju visos išteklių nuomos ir apdorojimo vietos nurodytos atitinkamame Duomenų lape.

Jei visos kitos paslaugos teikiamos per Vokietijos duomenų centrą, IBM tvarkys Asmens duomenis tik toje šalyje, kurioje yra IBM sutarties juridinis asmuo, ir šiose šalyse: Vokietijoje, Izraelyje, Airijoje, Nyderlanduose, taip pat visose papildomose šalyse, kurios nurodytos atitinkamame IBM trečiųjų šalių antrinių tvarkytojų duomenų lape.

Jei visos kitos paslaugos teikiamos per Japonijos duomenų centrą, IBM tvarkys Asmens duomenis tik toje šalyje, kurioje yra IBM sutarties juridinis asmuo, ir šiose šalyse: Japonijoje, Izraelyje, Airijoje, taip pat visose papildomose šalyse, kurios nurodytos atitinkamame IBM trečiųjų šalių antrinių tvarkytojų duomenų lape.

Jei visos kitos paslaugos teikiamos per JAV duomenų centrą, IBM tvarkys Asmens duomenis tik toje šalyje, kurioje yra IBM sutarties juridinis asmuo, ir šiose šalyse: JAV, Izraelyje, Airijoje, Singapūre, Australijoje, taip pat visose papildomose šalyse, kurios nurodytos atitinkamame IBM trečiųjų šalių antrinių tvarkytojų duomenų lape.

„IBM Trusteer“ palaikymo ir paskyros tvarkymo paslaugos, jei reikia, taip pat gali būti teikiamos, atsižvelgiant į atitinkamo IBM personalo pasiekiamumą, Kliento vietą ir duomenų centrą, kuriame laikomi duomenys.

2.3.2 Paskyros savininko duomenys

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.

2.3.3 Integruoti sprendimai

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

3. Paslaugos lygio sutartis

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

3.1 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 paskelbtos 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 tolesnėje lentelėje. Bendra kompensacijos suma, atsižvelgiant į bet kurį sutartinį mėnesį, negali neviršyti 10 procentų nuo vienos dvyliktosios (1/12) metinio mokesčio už „Cloud Service“ dalies.

3.2 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)**
<99,9 %	2 %
<99,0 %	5 %
< 95,0 %	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 kompensavimo 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

4. Techninė pagalba

„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**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital Content Pack** ir **IBM Trusteer Mobile Carrier Intelligence**. 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 IBM programinės įrangos kaip paslaugos palaikymo vadove, pateiktame https://www.ibm.com/software/support/saas_support_guide.html.
- Klientai gali pasiekti Klientų palaikymo portalą ir gauti pranešimus, dokumentus, atvejų ataskaitas ir DUK apsilankę: http://www-01.ibm.com/software/security/trusteer

„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 ataskaitas ir DUK apsilankę http://www.ibm.com/software/security/trusteer/support/.
- Palaikymo parinktis ir išsamią informaciją rasite IBM programinės įrangos kaip paslaugos palaikymo vadove, apsilankę https://www.ibm.com/software/support/saas_support_guide.html.

5. Teisių suteikimo ir sąskaitų išrašymo informacija

5.1 Mokesčio apskaičiavimas

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

- 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.
- 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.
- 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.

- 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.

  Naudojant šią „Cloud Service“, Taikomoji programa yra viena Kliento Verslo arba Mažmeninės prekybos programa.
- API iškvieta yra matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. API iškvieta – tai „Cloud Service“ iškvieta per programuojamą sąsają. Reikia įsigyti teises, pakankamas bendram API iškvietų skaičiui, suapvalintam iki artimiausios dešimties padengti matavimo laikotarpiu, nurodytu Kliento TSD arba Operacijų dokumente.
- Ryšys yra matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Ryšys – tai duomenų bazės, taikomosios programos, serverio arba kito įrenginio tipo saitas arba sąsaja su „Cloud Service“. Reikia įsigyti teises, pakankamas bendram suteiktų arba suteikiamų Ryšių su „Cloud Service“ skaičiui padengti matavimo laikotarpiu, nurodytu Kliento TSD arba Operacijų dokumente.

  Naudojant šią „Cloud Service“, Ryšys yra atskiras Kliento Taikomosios programos seansas arba srautas.

5.2 Mokesčiai už perviršį

Jei faktinis „Cloud Service“ naudojimas matavimo laikotarpiu viršys TSD nurodytas teises, mokestis už perviršį, pagal Operacijų dokumente nustatytą tarifą, bus taikomas kitą mėnesį po perviršio.

5.3 Sąskaitų išrašymo dažnumas

Atsižvelgiant į atsiskaitymo dažnumą, IBM išrašys Klientui sąskaitą už mokesčius, kurią reikia apmokėti atsiskaitymo dažnumo periodo pradžioje, išskyrus permoką ir naudojimo tipo mokesčius, už kuriuos sąskaita bus išrašoma įsiskolinus.

6. Terminas ir pratęsimo 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.

Atnaujinant automatiškai, jei Klientas nepateikia prašymo neatnaujinti raštu mažiausiai prieš 90 dienų iki termino galiojimo pabaigos datos, „Cloud Service“ automatiškai atnaujinama TSD nurodytam laikotarpiui. Atnaujinimams taikomas kasmetinis kainos padidėjimas, kaip nurodyta pasiūlyme. Jei automatiškai atnaujinama po IBM pranešimo apie „Cloud Service“ atšaukimą, atnaujinimo laikotarpis pasibaigs ne vėliau nei esamas atnaujinimo laikotarpis arba paskelbta atšaukimo data.

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.

7. Papildomos sąlygos

7.1 Bendrosios nuostatos

Klientas sutinka, kad spaudoje ar rinkodaros informacijoje IBM gali Klientą viešai vadinti „Cloud Services“ prenumeratoriumi.

Klientas negali naudoti „Cloud Service“ atskirai ar kartu su kitomis paslaugomis ar produktais bet kuriai iš šių didelės rizikos veiklų palaikyti: branduolinių objektų, masinio vežimo sistemų, oro eismo kontrolės sistemų, automobilių kontrolės sistemų, ginkluotės sistemų, orlaivių navigacijos ar ryšių kūrimo, konstravimo, valdymo arba techninės priežiūros arba bet kurios kitos veiklos, kur „Cloud Service“ gedimas gali kelti mirties arba rimto sužalojimo esminį pavojų.

7.2 Įgalinimo programinė įranga

„Cloud Service“ būtina naudoti įgalinimo programinę įrangą, kurią Klientas atsisiunčia į Kliento sistemas, kad galėtų naudoti „Cloud Service“. Klientas gali naudoti įgalinimo programinę įrangą tik kartu su naudojama „Cloud Service“. Įgalinimo programinė įranga pateikiama „TOKIA, KOKIA YRA“.

7.3 „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.