„IBM Trusteer Pinpoint Detect“

Šiame paslaugos apraše aprašoma „Cloud Service“. Taikomuose užsakymo dokumentuose pateikiama išsami informacija apie kainą ir papildoma informacija apie Kliento užsakymą.

1. „Cloud Service“

„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. „Trusteer Management Application“ (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. „IBM Trusteer Pinpoint Detect“ ir „IBM Trusteer Pinpoint Verify“ naudojami kaip TMA prisijungimo dalis.

b. Žiniatinklio scenarijus ir (arba) API:

   Diegimas svetainėje norint pasiekti arba naudoti „Cloud Service“.

„Pinpoint“ seanso laikas skaičiuojamas tarp vartotojo sąveikos pradžios ir pabaigos. Seanso pradžia skaičiuojama nuo kredencialų pateikimo arba kitokio kredencialų patvirtinimo kliento prisijungimo puslapyje. Seanso pabaiga užregistruojama įvykus vienam iš šių dalykų:

- Seansas nustatomas iš naujo įprastai atsijungus nuo programos.
- Uždarius naršyklę arba skirtuką.
- Ištrynus slapukus.
- Pasibaigus skirtajam laikui.

1.1 Pasiūlymai

Klientas gali rinktis iš šių pasiūlymų.

1.1.1 „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.

1.1.2 „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.

1.1.3 „IBM Trusteer Pinpoint Detect for Connections“

Ši „Cloud Service“ suteikia apsaugą ir siekia aptikti bandymus perimti paskyras ir pateikia naršyklių ir (arba) mobiliųjų įrenginių, turinčių prieigą prie Verslo arba Mažmeninės prekybos programos, rizikos / pasitikėjimo įvertinimo balus (naudojant vietinę naršyklę arba Kliento mobiliąją programą). Šio sprendimo vartotojai naudoja įvairius rizikos indikatorius, analizuojančius galutinio vartotojo įrenginį, ryšį ir veikimą, ir juos palygina su vartotojo istorija, kad aptiktų įtartiną naudojimą.

„Cloud Service“ gali naudoti tiek mobiliųjų, tiek interneto kanalų ryšius. „IBM Trusteer Pinpoint Detect“ apima teises į „IBM Trusteer Mobile“ SDK, jei tai aktualu.

Šią „Cloud Service“ galima įsigyti 100 Ryšių per metus paketais.

1.2 Pasirinktinės paslaugos

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

1.2.1 „IBM Trusteer Pinpoint Detect Standard Application“

Kliento programa reiškia Žiniatinklio taikomąją programą ir (arba) Mobiliąją taikomąją programą. Žiniatinklio taikomoji programa sugrupuoja visas Kliento Priskirtiems dalyviams keliuose tinklalapiuose arba iš prisijungimo arba identifikavimo ekrano siūlomas funkcijas, kurios kaip viena Taikomoji programa stebimos „Trusteer“ konsolėje („Trusteer Management Application“). Mobilioji taikomoji programa kartu sugrupuoja visas Kliento Priskirtiems dalyviams vienoje programoje, kurią galima atsisiųsti iš programų parduotuvės (parduotuvė), arba iš prisijungimo ar identifikavimo ekrano siūlomas funkcijas, kurios kaip viena Taikomoji programa stebimos „Trusteer“ konsolėje („Trusteer Management Application“).

Norint integruoti „IBM Trusteer Pinpoint“, kiekvienai Taikomajai programai būtinos „IBM Trusteer Pinpoint“ teisės.

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

1.2.2 „IBM Trusteer Pinpoint Detect Premium Application“

Kliento programa reiškia Žiniatinklio taikomąją programą ir (arba) Mobiliąją taikomąją programą. Žiniatinklio taikomoji programa sugrupuoja visas Kliento Priskirtiems dalyviams keliuose tinklalapiuose arba iš prisijungimo arba identifikavimo ekrano siūlomas funkcijas, kurios kaip viena Taikomoji programa stebimos „Trusteer“ konsolėje („Trusteer Management Application“). Mobilioji taikomoji programa kartu sugrupuoja visas Kliento Priskirtiems dalyviams vienoje programoje, kurią galima atsisiųsti iš programų parduotuvės (parduotuvė), arba iš prisijungimo ar identifikavimo ekrano siūlomas funkcijas, kurios kaip viena Taikomoji programa stebimos „Trusteer“ konsolėje („Trusteer Management Application“).

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 Premium“, kiekvienai Taikomajai programai būtinos „IBM Trusteer Pinpoint Detect Premium Application“ teisės.

1.2.3 „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.

1.2.4 „IBM Trusteer Digital Content Pack for Retail“ ir (arba) „IBM Trusteer Digital Content Pack for Business“

„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.

1.2.5 „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).

1.2.6 „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.

1.2.7 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“.

1.2.8 „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. Šio Paslaugos aprašo tikslais 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 Service“ Klientas užsiprenumeravo. Paskyros turėtojo Kliento programinė 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 įrenginyje.

1.2.9 „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.

1.2.10 „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) specialiaja 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.

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

- „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.

1.2.12 „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 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.

1.2.13 „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.

1.2.14 „IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect“

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

Ši „Cloud Service“ papildo „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.

1.3 Akceleravimo paslaugos

1.3.1 „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.

1.3.2 „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.

2. Duomenų tvarkymo ir apsaugos duomenų lapai

Svetainėje http://ibm.com/dpa pateikiamame IBM Duomenų tvarkymo priede (DTP) ir toliau esančiose nuorodose pateikiamame (-uose) Duomenų tvarkymo bei apsaugos duomenų lape (-uose) (vadinamame (-uose) duomenų lapu (-ais) arba DTP įrodymu (-ais) pateikiama papildoma „Cloud Service“ duomenų apsaugos informacija ir jos apsaugos galimybės, susijusios su Turinio, kuris gali būti tvarkomas, tipais, atliekamais tvarkymo veiksmais, duomenų apsaugos funkcijomis ir Turinio saugojimo bei grąžinimo specifika. DTP taikomas asmeniniams duomenims, esantiems turinyje, jei (ir tik tokia apimtimi) taikomas i) Europos bendrasis duomenų apsaugos reglamentas (ES/2016/679) (BDAR) arba ii) kiti duomenų apsaugos teisės aktai, nurodyti http://ibm.com/dpa/dpl.

Paaiškinama, kad Duomenų lapuose paprastai nurodomos visos vietos, kur IBM (įskaitant visus trečiosios šalies antrinius tvarkytojus) laiko ir apdoroja Asmens duomenis neatsižvelgiant į duomenų centrą, iš kur diegiamos paslaugos. Laikymo ir apdorojimo vietų, priklausančių nuo duomenų centro, iš kurio diegiamos paslaugos, sąrašo ieškokite tolesniame 5.2 skyriuje (Papildoma apdorojimo vietų informacija).

„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 Mobile SDK“

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

3. Paslaugos lygiai ir techninis palaikymas

3.1 Paslaugos lygio sutartis

IBM teikia Klientui toliau nurodytus pasiekiamumo paslaugos lygio sutarties (PLS) įsipareigojimus. IBM taikys aukščiausią galimą kompensaciją, pagrįstą „Cloud Service“ kaupiamuoju pasiekiamumu, kaip nurodyta toliau esančioje lentelėje. Pasiekiamumo procentas apskaičiuojamas iš bendro minučių skaičiaus sutartinį mėnesį atėmus bendrą Paslaugos neveikimo minučių skaičių sutartinį mėnesį, gautą rezultatą padalijus iš bendro minučių skaičiaus sutartinį mėnesį. Paslaugos neveikimo apibrėžimas, prašymų pateikimo procesas ir informacija, kaip susisiekti su IBM dėl paslaugos pasiekiamumo problemų, pateikiama „IBM Cloud Service“ palaikymo vadove https://www.ibm.com/software/support/saas_support_overview.html.

Prieinamumas	Kreditas (% mėnesio prenumeratos mokesčio*)
Mažiau nei 99,9 %	2 %
Mažiau nei 99,0 %	5 %
Mažiau nei 95,0 %	10 %

* Prenumeratos mokestis yra teiginyje minimo mėnesio sutartinė kaina.

3.2 Techninė pagalba

„Cloud Service“ techninį palaikymą, įskaitant palaikymo kontaktinę informaciją, sudėtingumo lygius, pasiekiamumo palaikymo valandas, atsakymo laiką ir kitą palaikymo informaciją ir procesus rasite pasirinkę „Cloud Service“ IBM palaikymo vadove svetainėje https://www.ibm.com/support/home/pages/support-guide/.

„Premium Support“:

Už papildomą mokestį galima įsigyti „Cloud Service“ skirtą „Premium Support“ prenumeratą, į kurią įeina:

- 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/.

4. Mokesčiai

4.1 Mokesčio apskaičiavimas

„Cloud Service“ mokesčio apskaičiavimas nurodytas Operacijų dokumente.

Šiai „Cloud Service“ taikomas toliau aprašytas mokesčio apskaičiavimas.

- „Engagement“ yra profesionali arba mokymo paslauga, susijusi su „Cloud Services“.
- Priskirtas dalyvis – tai privatus ar juridinis asmuo, turintis teisę dalyvauti bet kurioje „Cloud Services“ valdomoje arba stebimoje paslaugos teikimo programoje.
- Taikomoji programa – tai programinė įranga unikaliu pavadinimu. Ji sukurta, pasiekiama arba naudojama „Cloud Service“.
- API iškvieta – tai „Cloud Services“ iškvieta per programuojamąją sąsają.
- Ryšys – tai duomenų bazės, taikomosios programos, serverio arba kito įrenginio tipo, kuris yra pasiekiamas „Cloud Service“ arba buvo toks padarytas, saitas arba sąsaja.

4.2 Nuotolinių paslaugų mokesčiai

Nuotolinės paslaugos galiojimas baigsis praėjus 90 dienų nuo įsigijimo dienos, neatsižvelgiant į tai, ar nuotoline paslauga buvo pasinaudota.

5. Papildomos sąlygos

„Cloud Service“ sutartims (arba atitinkamoms debesies technologijomis pagrįstoms sutartims), vykdytoms iki 2019 m. sausio 1 d., taikomos sąlygos, pateikiamos https://www.ibm.com/acs.

5.1 EULA ir duomenų subjektų duomenų tvarkymo pagrindas

Naudojant „IBM Trusteer Rapport Cloud Services“ (įskaitant „Rapport Remediation“ arba „Rapport for Mitigation“, kai įdiegta 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://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA, kad IBM galėtų rinkti ir apdoroti informaciją, būtiną teikiant „Cloud Services“.

Naudojant „IBM Trusteer Rapport Cloud Services,“, Klientas įgalioja IBM, kaip Remiančiosios įmonės duomenų tvarkytoją, naudoti Programą, kad ji galėtų rinkti kenkėjišką programinę įrangą ir kenkėjiškos programinės įrangos artefaktus, tai yra failus, susijusius su kenkėjiška veikla, arba failus, susijusius su neįprastu Programos neveikimu. IBM nenaudoja Programos, kad pasiektų failus su galutinio vartotojo asmenine informacija, tačiau surinktuose failuose gali būti asmens duomenų, kuriuos kenkėjiška programinė įranga surinko be galutinio vartotojo leidimo. IBM 1) greitai pašalins visus failus, nesusijusius su tokia analize, o 2) susijusius failus saugos tik analizės metu ir ne ilgiau nei tris mėnesius.

5.2 Papildoma apdorojama vietos informacija

Bet koks Asmens duomenų laikymas ir apdorojimas, įskaitant vykdomą trečiosios šalies antrinių tvarkytojų, nurodytų Duomenų lape, bus vykdomas toliau nurodytose vietose:

Jei paslaugos teikiamos per Vokietijos duomenų centrą, IBM laikys ir tvarkys Asmens duomenis tik toje šalyje, kurioje yra IBM sutarties juridinis asmuo ir šiose šalyse: Vokietijoje, Izraelyje, Airijoje ir Nyderlanduose.

Jei paslaugos teikiamos per Japonijos duomenų centrą, IBM laikys ir tvarkys Asmens duomenis tik toje šalyje, kurioje yra IBM sutarties juridinis asmuo ir šiose šalyse: Japonijoje, Izraelyje ir Airijoje.

Jei paslaugos teikiamos per JAV duomenų centrą, IBM laikys ir tvarkys Asmens duomenis tik toje šalyje, kurioje yra IBM sutarties juridinis asmuo ir šiose šalyse: JAV, Izraelyje, Airijoje, Singapūre ir Australijoje.

Be anksčiau minėtų vietų, visų per Vokietijos, Japonijos ir JAV duomenų centrus teikiamų paslaugų (1) palaikymo duomenys gali būti laikomi arba apdorojami Vokietijoje ir Prancūzijoje „Salesforce.Com“ kaip IBM trečiosios šalies antrinio tvarkytojo ir (2) klientų, kurie pasirenka siųsti duomenis „Mobile Carrier Intelligence“ teikėjams, Asmens duomenys gali būti laikomi ir apdorojami atitinkamų trečiosios šalies antrinių tvarkytojų šalyse, kaip nurodyta Duomenų lape. Neatsižvelgiant į prieštaraujančias Duomenų lapo sąlygas, iškart prieš tai einančio sakinio (2) punkte nurodyti trečiosios šalies antriniai tvarkytojai gali neatitikti ISO 27001 arba SOC2.

„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.

5.3 Paskyros savininko duomenys

Kad būtų visiškai aišku, jei su konkretaus Paskyros turėtojo Programine įranga yra susijęs daugiau nei vienas IBM klientas (pvz., IBM klientai, „Susiję klientai“) ir paslaugos pagal šį Paslaugų aprašą tokiems Susijusiems klientams IBM teikiamos per duomenų centrus skirtinguose regionuose, tuomet Paskyros turėtojo duomenys gali būti apdorojami bet kurioje ir visose vietose, susijusiose su kiekvienu iš tokių duomenų centrų, kaip nurodyta ankstesniame 5.2 skyriuje.

5.4 Integruoti sprendimai

Kad būtų visiškai aišku, įvairūs „Trusteer“ prekės ženklui priklausantys sprendimai gali sudaryti integruotą sprendimą. Taigi, Klientui nutraukus bet kurią iš šių „Cloud Services“, IBM gali pasilikti Kliento duomenis tam, kad galėtų Klientui teikti likusias „Cloud Services“ pagal šį Paslaugų aprašą, taip pat kitas „Trusteer“ paslaugas, laikantis tokioms „Trusteer“ paslaugoms taikomų paslaugų aprašų.

5.5 Įgalinimo programinė įranga

„Cloud Service“ yra ši įgalinimo programinė įranga:

- „IBM Rapport Agents“

5.6 „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).

5.7 Duomenys renkami kaip diegimo dalis

Dėl „Cloud Service“ diegimo Klientui gali tekti pateikti IBM tam tikrus duomenis. Tokie duomenys negali apimti informacijos, pagal kurią galima identifikuoti konkrečius asmenis arba kurią galima priskirti konkretiems asmenims. Daugiau rekomendacijų dėl duomenų, kurie pateikiami IBM kaip diegimo dalis, pateikta „Trusteer“ diegimo rekomendacijose, kurios pateikiamos Klientui.

6. Atšaukimo sąlygos

6.1 Duomenų naudojimas

Toliau nurodytas teiginys laikomas svarbesniu už bet kuriuos jam prieštaraujančius pagrindinių „Cloud Service“ sąlygų tarp šalių Turinio ir Duomenų apsaugos skyriuose nurodytus teiginius: IBM nenaudos arba neatskleis Klientui naudojant „Cloud Service“ gautų rezultatų, kurie yra unikalūs Kliento Turinio (įžvalgų) rezultatai ar kitaip identifikuoja Klientą. Tačiau IBM naudos Turinį ir kitą iš Turinio, kaip „Cloud Service“ dalies, gautą informaciją, 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.