

„IBM Security Trusteer Fraud Protection“

Naudojimo sąlygas (NS) sudaro šios IBM naudojimo sąlygos – su „SaaS“ susijusios pasiūlymo sąlygos („Su „SaaS“ susijusios pasiūlymo sąlygos“) ir dokumentas „IBM naudojimo sąlygos – bendrosios sąlygos“ („Bendrosios sąlygos“), pasiekiamos šiuo URL: <http://www.ibm.com/software/sla/slabd.nsf/sla/tou-gen-terms/>.

Atsiradus prieštaravimams, su „SaaS“ susijusios pasiūlymo sąlygos laikomos viršesnėmis už Bendrąsias sąlygas. Klientas sutinka su šiomis NS, jeigu užsako, pasiekia ar naudoja „IBM SaaS“.

NS nustato IBM tarptautinės „Passport Advantage“ sutarties, IBM tarptautinės „Passport Advantage Express“ sutarties arba IBM tarptautinės pasirinktų „IBM SaaS“ pasiūlymų sutarties sąlygos, kiek jos taikomos, („Sutartis“) ir kartu su NS sudaro visą sutartį.

1. „IBM SaaS“

Šiems „IBM SaaS“ pasiūlymams taikomos šios Su „SaaS“ susijusios pasiūlymo sąlygos:

1.1 „Rapport IBM SaaS“ pasiūlymai

- „IBM Security Trusteer Rapport for Business“
- „IBM Security Trusteer Rapport for Business Premium Support“
- „IBM Security Trusteer Rapport for Retail“
- „IBM Security Trusteer Rapport for Retail Premium Support“
- „IBM Security Trusteer Rapport Fraud Feeds for Business“
- „IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support“
- „IBM Security Trusteer Rapport Fraud Feeds for Retail“
- „IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support“
- „IBM Security Trusteer Rapport Phishing Protection for Business“
- „IBM Security Trusteer Rapport Phishing Protection for Business Premium Support“
- „IBM Security Trusteer Rapport Phishing Protection for Retail“
- „IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support“
- „IBM Security Trusteer Rapport Mandatory Service for Business“
- „IBM Security Trusteer Rapport Mandatory Service for Retail“

1.2 „Pinpoint IBM SaaS“ pasiūlymai

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

- „IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile“
- „IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support“
- „IBM Security Trusteer Pinpoint Carbon Copy for Business“
- „IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support“
- „IBM Security Trusteer Pinpoint Carbon Copy for Retail“
- „IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support“
- „IBM Security Trusteer Rapport Remediation for Retail“
- „IBM Security Trusteer Rapport Remediation for Retail Premium Support“

1.3 Mobilieji IBM SaaS“ pasiūlymai

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

2. Mokesčio apskaičiavimas

„IBM SaaS“ parduodamas pagal vieną iš toliau nurodytų mokesčių apskaičiavimo schemų, pateiktų Sandorio dokumente:

- a. **Priskirtas dalyvis** yra matavimo vienetas, kuriuo remiantis galima gauti „IBM SaaS“. Kiekvienas privatus ar juridinis asmuo, turintis teisę dalyvauti bet kurioje „IBM SaaS“ valdomoje arba stebimoje paslaugos teikimo programoje, yra Priskirtas dalyvis. Reikia įsigyti teises, kurių pakaktų visiems „IBM SaaS“ valdomiems ar stebimiems Priskirtiems dalyviams matavimo laikotarpiu, nurodytu Kliento Sandorio dokumente.

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

Taikant šiuos pasiūlymus, paslaugos teikimo programa apima vieną Kliento Verslo arba Mažmeninės prekybos programą su pagrindiniu prisijungimo puslapiu ir susijusiais kiekvienos Verslo arba Mažmeninės prekybos programos puslapiais. Priskirtas dalyvis yra galutinis Kliento vartotojas, turintis Verslo arba Mažmeninės prekybos programos prisijungimo kredencialus.

- b. **Kliento įrenginys** yra matavimo vienetas, kuriuo remiantis galima gauti „IBM SaaS“. 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 „IBM SaaS“ matavimo laikotarpiu, nurodytu Kliento Sandorio dokumente.

3. Mokesčiai ir sąskaitų išrašymas

Už „IBM SaaS“ mokėtina suma nurodyta Sandorio dokumente.

3.1 Daliniai mėnesio mokesčiai

Dalinis mėnesio mokestis, kaip nurodyta Sandorio dokumente, gali būti nustatomas proporcingai.

4. Atitiktis ir auditas

Prieiga prie „IBM Security Trusteer Fraud Protection“ pasiūlymų priklauso nuo maksimalaus Priskirtų dalyvių arba Kliento įrenginių skaičiaus, nurodyto Sandorio dokumente. Klientas yra atsakingas už tai, kad Priskirtų dalyvių arba Kliento įrenginių skaičius neviršytų maksimalaus Sandorio dokumente nurodyto kiekio.

Norint patikrinti, ar maksimalus Priskirtų dalyvių arba Kliento įrenginių skaičius atitinka, gali būti atliktas auditas.

5. „IBM SaaS“ prenumeratos laikotarpio naujinimo parinktys

Kliento Sandorio dokumente bus nustatyta, ar Prenumeratos laikotarpio pabaigoje „IBM SaaS“ naudojimas bus atnaujintas, nurodant vieną iš toliau pateiktų terminų:

5.1 Automatinis atnaujinimas

Jeigu Kliento Sandorio dokumente nurodyta, kad Kliento atnaujinimas yra automatinis, Klientas gali nutraukti besibaigiantį „IBM SaaS“ Prenumeratos laikotarpį pateikęs prašymą raštu Kliento IBM pardavimo atstovui arba IBM Verslo partneriui mažiausiai prieš devyniasdešimt (90) dienų iki galiojimo pabaigos, kuri nurodyta Sandorio dokumente. Jeigu IBM arba IBM Verslo partneris negauna tokio pranešimo apie nutraukimą iki galiojimo pabaigos datos, bebaigiantis galioti Prenumeratos laikotarpis bus automatiškai atnaujintas vieniams metams arba tokiam pačiam Prenumeratos laikotarpiui, koks pradžioje buvo nurodytas Sandorio dokumente.

5.2 Nepertraukiamas sąskaitų išrašymas

Kai Sandorio dokumente nurodyta, kad Kliento atnaujinimas yra nepertraukiamas, Klientas ir toliau turės prieigą prie „IBM SaaS“ ir už „IBM SaaS“ naudojimą jam nepertraukiamai bus išrašomos sąskaitos. Norėdamas nutraukti „IBM SaaS“ naudojimą ir sustabdyti nepertraukiamo sąskaitų išrašymo procesą, Klientas turės prieš devyniasdešimt (90) dienų raštu pateikti IBM arba IBM verslo partneriui prašymą atšaukti Kliento „IBM SaaS“. Atšaukus Kliento prieigą, Klientui bus išrašyta sąskaita už atšaukimo įsigaliojimo mėnesio nesumokėtus prieigos mokesčius.

5.3 Reikalingas atnaujinimas

Kai Sandorio dokumente nurodyta, kad Kliento atnaujinimo tipas yra „terminuotas“, pasibaigus Prenumeratos laikotarpiui „IBM SaaS“ paslaugos teikimas pasibaigs ir bus pašalinta Kliento prieiga prie „IBM SaaS“. Norėdamas ir toliau naudoti „IBM SaaS“ pasibaigus terminui, Klientas turės pateikti užsakymą Kliento IBM pardavimo atstovui arba IBM verslo partneriui ir įsigyti naują Prenumeratos laikotarpį.

6. Techninis palaikymas

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

„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.

Visiems „IBM SaaS“ pasiūlymams: „Premium Support“ prenumerata pasiekama už papildomą mokestį, išskyrus „IBM Security Trusteer Mobile SDK“ ir „IBM Security Trusteer Rapport Mandatory Service“ pasiūlymus.

„Standard Support“:

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

„Premium Support“:

- Visų sudėtingumo lygių palaikymas ištisą parą.
- Klientai gali gauti palaikymą telefonu.
- Klientai ir jų Priskirti dalyviai gali pateikti palaikymo korteles elektroniniu būdu, kaip išsamiai nurodyta Programinės įrangos kaip paslaugos [SaaS] palaikymo vadove.
- Klientai gali pasiekti Klientų palaikymo portalą ir gauti pranešimus, dokumentus, atvejų analizes ir DUK apsilankę <http://www-01.ibm.com/software/security/trusteer/support/>.

- Palaikymo parinktis ir išsamią informaciją apie IBM programinę įrangą kaip paslaugą [SaaS] rasite palaikymo vadove <http://www-01.ibm.com/software/support/handbook.html>.

7. „IBM SaaS“ pasiūlymo papildomos sąlygos

7.1 „Saugaus uosto“ nuostatų laikymasis

IBM laikosi JAV komercijos departamento, derinant su Europos Komisija, nustatytų JAV–ES „saugaus uosto“ principų. „IBM Security Trusteer“ produktai įtraukti į IBM ES–JAV „saugaus uosto“ sistemos liudijimą. Daugiau informacijos apie „saugaus uosto“ sistemą ir „saugaus uosto“ įmonių sąrašą rasite čia: <http://export.gov/safeharbor/>.

7.2 Kliento metinio prenumeratos mokesčio didėjimas

IBM pasilieka teisę koreguoti „IBM SaaS“ prenumeratos mokesť ne dažniau nei kartą per dvylika (12) mėnesių IBM nustatyta procentine dalimi, neviršijančia 3 %. Prenumeratos mokesčio koregavimas įsigalios nuo paslaugos teikimo laikotarpio pradžios sukakties datos. Šio mokesčio pakeitimai nekeičia Kliento įsipareigojimo dėl „IBM SaaS“ ar mokesčio apskaitos sistemos, pagal kurią įsigyjama „IBM SaaS“. IBM verslo partneriai yra nepriklausomi nuo IBM ir vienašališkai nustato savo kainas ir sąlygas.

7.3 „Premium Support“

Klientas turi teisę į aukščiausio lygio palaikymą, skirtą tik „IBM SaaS“ pasiūlymams, kuriuos užsiprenumeravo pagal susijusį „Premium Support“ pasiūlymą.

7.4 Teisėtas naudojimas ir turinys

Įgaliojimas rinkti ir apdoroti duomenis

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

Duomenų rinkimo ir apdorojimo praktika gali būti atnaujinama siekiant patobulinti „IBM SaaS“ veikimą. Dokumentas su visu duomenų rinkimo ir apdorojimo praktikos aprašu yra atnaujinamas, kai reikia, ir pasiekiamas Klientui paprašius. Klientas įgalioja IBM rinkti šią informaciją ir ją apdoroti remiantis šių „Naudojimo sąlygų“ skyriais „Tarptautinis perdavimas“ ir „Duomenų privatumas“ bei dokumento „Naudojimo sąlygos. Bendrosios sąlygos“ skyriumi „Duomenų privatumas ir sauga“.

„IBM Security Trusteer Pinpoint“ pasiūlyme:

Renkami duomenys gali būti vartotojo IP adresas, užšifruotas arba iš vienos pusės užšifruotas vartotojo ID, domeno slapukai (jei nefiltruojami), apsilankymai apsaugotose programose ir apsimestinėse svetainėse, geografinės vietos bei šiose svetainėse įvedami kredencialai.

„IBM Security Trusteer Mobile SDK“ ir „IBM Security Trusteer Mobile Browser“ pasiūlymuose:

Renkami duomenys gali būti vartotojo IP adresas, užšifruotas arba iš vienos pusės užšifruotas vartotojo ID, geografinės vietos, apsilankymai apsaugotose programose, SIM kortelės informacija, įrenginio pavadinimas ir Klientų filialai.

„IBM Security Trusteer Rapport“ pasiūlymuose:

Renkami duomenys gali būti vartotojo IP adresas, užšifruotas arba iš vienos pusės užšifruotas vartotojo ID, saugos įvykiai, vartotojo vardas ir el. pašto adresas, kuriuo IBM susisiekiama su klientais palaikymo tikslais, Klientų filialai, apsaugotose svetainėse įvestas šifruotas slaptažodis, apsilankymai apsaugotose programose ir apsimestinėse svetainėse, šifruotas mokėjimo kortelės numeris, failai ir duomenys, kuriuos surinko IBM darbuotojai, kad patikrintų įtartiną kenkėjišką programinę įrangą, kenkėjišką veiklą ar triktis.

Informuotas duomenų subjektų sutikimas:

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

„IBM Security Trusteer Pinpoint“ ir „IBM Security Trusteer Mobile SDK“ pasiūlymuose:

Klientas sutinka, kad gavo arba gaus visus išsamius sutikimus, leidimus ir licencijas, reikalingas įgalinant teisėtą „IBM SaaS“ naudojimą ir leidžiančias IBM rinkti ir apdoroti informaciją per „IBM SaaS“.

„IBM Security Trusteer Rapport“ ir „IBM Security Trusteer Mobile Browser“ pasiūlymuose:

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

7.5 Tarptautiniai perdavimai

Klientas sutinka, kad IBM gali apdoroti turinį, įskaitant visus Asmens duomenis, remdamasi atitinkamais tarptautiniais įstatymais ir reikalavimais, kartu su apdorotojais ir antriniais apdorotojais iš toliau nurodytų šalių, kurios nepriklauso Europos ekonominei zonai, ir šalių, kuriose, Europos Komisijos nuomone, užtikrinami adekvatūs saugos lygiai, pvz., JAV.

7.6 Duomenų privatumas

Jei Klientas padaro Asmens duomenis prieinamus „IBM SaaS“ ES šalyse narėse, Islandijoje, Lichtenšteine, Norvegijoje ar Šveicarijoje arba jei Klientas tose šalyse turi Priskirtų dalyvių ar Kliento įrenginių, tada Klientas (kaip vienintelis valdytojas) nurodo IBM (kaip apdorotojui) apdoroti Asmens duomenis (pagal sąlygas, nurodytas ES direktyvoje 95/46/EK). IBM apdoros jūsų Asmens duomenis tik tiek, kiek reikalinga norint teikti „IBM SaaS“ pasiūlymą pagal IBM paskelbtus „IBM SaaS“ aprašus, o Klientas sutinka, kad bet koks toks apdorojimas atitinka Kliento nurodymus. IBM prieš protingą laiko tarpą praneš, jei IBM iš esmės keis Asmens duomenų, kaip „IBM SaaS“ dalies, apdorojimo vietą arba apsaugos būdą. Klientas gali nutraukti paveikto „IBM SaaS“ esamą Prenumeratos laikotarpį pateikęs IBM įspėjimą raštu per trisdešimt (30) dienų nuo IBM pranešimo Klientui apie keitimą. Klientas sutinka, kad IBM gali apdoroti turinį, įskaitant bet kokius Asmens duomenis, už šalies ribų šiose šalyse (su apdorotojais ir antriniais apdorotojais):

Apdorotojo / antrinio apdorotojo pavadinimas	Vaidmuo (duomenų apdorotojas arba antrinis apdorotojas)	Vieta*
IBM sutartį sudarantis objektas	Apdorototas	Kaip nurodyta Sandorio dokumente
„Amazon Web Services LLC“	Antrinis tvarkytojas	410 Terry Ave. N Seattle, WA 98109 Jungtinės Amerikos Valstijos
Connectria Corp.	Antrinis tvarkytojas	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 Jungtinės Amerikos Valstijos
„IBM Israel Ltd.“	Antrinis tvarkytojas	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izraelis
„IBM Corp“	Antrinis tvarkytojas	1 New Orchard Rd. Armonk, NY 10504 Jungtinės Amerikos Valstijos

Klientas sutinka, kad IBM pranešusi gali keisti šį šalių sąrašą, pagrįstai nustačius, kad tai būtina teikiant „IBM SaaS“.

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

Apdorotojo / antrinio apdorotojo pavadinimas	Vaidmuo (duomenų apdorotojas arba antrinis apdorotojas)	Vieta*
IBM sutartį sudarantis objektas	Apdorototas	Kaip nurodyta Sandorio dokumente
„Amazon Web Services (Germany)“	Antrinis tvarkytojas	Miunchenas, Vokietija

Apdorotojo / antrinio apdorotojo pavadinimas	Vaidmuo (duomenų apdorotojas arba antrinis apdorotojas)	Vieta*
„IBM Israel Ltd.“	Antrinis tvarkytojas	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izraelis

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

Apdorotojo / antrinio apdorotojo pavadinimas	Vaidmuo (duomenų apdorotojas arba antrinis apdorotojas)	Vieta*
IBM sutartį sudarantis objektas	Apdorototas	Kaip nurodyta Sandorio dokumente
„Amazon Web Services (Japan)“	Antrinis tvarkytojas	Tokijas, Japonija
„IBM Israel Ltd.“	Antrinis tvarkytojas	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izraelis

* Anksčiau pateiktose lentelėse nurodytos vietos yra Apdorotojo arba Antrinio apdorotojo įmonės biuro adresai. Duomenų centrai yra toje pačioje šalyje.

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

A priedas

1. „IBM SaaS“ pasiūlymai

IBM siūlo šias paslaugas kaip atskiras paslaugas ir pasiūlymus arba kaip papildomas paslaugas ir pasiūlymus. Konkretūs užsakyti „IBM SaaS“ pasiūlymai nurodomi Kliento TSD.

1.1 Verslo ir Mažmeninės prekybos apibrėžimai

„IBM Security Trusteer“ apsaugos nuo sukčiavimo produktai licencijuojami naudoti su konkrečiais programų tipais. Programa priskiriama vienam iš dviejų tipų: Mažmeninės prekybos arba Verslo. Mažmeninės prekybos ir Verslo programoms taikomi atskiri pasiūlymai.

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

1.2 „IBM SaaS“ pagrindinės prenumeratos pasiūlymai

Verslo pasiūlymai:

- „IBM Security Trusteer Rapport for Business“
- „IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition“
- „IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition“
- „IBM Security Trusteer Pinpoint Criminal Detection for Business“
- „IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile“
- „IBM Security Trusteer Mobile SDK for Business“
- „IBM Security Trusteer Mobile Browser for Business“

Mažmeninės prekybos pasiūlymai:

- „IBM Security Trusteer Rapport for Retail“
- „IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition“
- „IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition“
- „IBM Security Trusteer Pinpoint Criminal Detection for Retail“
- „IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile“
- „IBM Security Trusteer Mobile SDK for Retail“
- „IBM Security Trusteer Mobile Browser for Retail“

Visuose Verslo ir Mažmeninės prekybos pasiūlymuose „Premium Support“ prenumerata pasiekama už papildomą mokestį, išskyrus „IBM Security Trusteer Mobile SDK“ pasiūlymus.

1.3 Papildomi „IBM SaaS“ prenumeratos pasiūlymai, skirti „IBM Security Trusteer Rapport“ pasiūlymams

Papildomi „IBM Security Trusteer Rapport for Business“ pasiūlymai:

- „IBM Security Trusteer Rapport Fraud Feeds for Business“
- „IBM Security Trusteer Rapport Phishing Protection for Business“
- „IBM Security Trusteer Rapport Mandatory Service for Business“

Papildomi pasiūlymai, skirti „IBM Security Trusteer Rapport for Retail“:

- „IBM Security Trusteer Rapport Fraud Feeds for Retail“
- „IBM Security Trusteer Rapport Phishing Protection for Retail“
- „IBM Security Trusteer Rapport Mandatory Service for Retail“

Visuose „IBM Security Trusteer Rapport“ pasiūlymų Verslo ir Mažmeninės prekybos prieduose, išskyrus „IBM Security Trusteer Rapport Mandatory Service“ priedus, „Premium Support“ prenumerata pasiekama už papildomą mokestį.

„IBM Security Trusteer Rapport for Business“ arba „IBM Security Trusteer Rapport for Retail“ prenumerata yra šiame skyriuje išvardytų susietų papildomų „IBM SaaS“ prenumeratos pasiūlymų būtina sąlyga.

1.4 **Papildomi „IBM SaaS“ pasiūlymai, skirti „IBM Security Trusteer Pinpoint Malware Detection“ pasiūlymams**

Papildomi „IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition“ arba „IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition“ pasiūlymai:

- „IBM Security Trusteer Pinpoint Carbon Copy for Business“

Papildomi „IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition“ arba „IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition“ pasiūlymai:

- „IBM Security Trusteer Pinpoint Carbon Copy for Retail“
- „IBM Security Trusteer Rapport Remediation for Retail“

„Premium Support“ prenumerata pasiekama už papildomą mokestį, mokamą už kiekvieną papildomą „IBM SaaS“ pasiūlymą, išvardytą šiame skyriuje.

„IBM Security Trusteer Pinpoint Malware Detection for Business“ arba „IBM Security Trusteer Pinpoint Malware Detection for Retail“ pasiūlymų prenumerata yra šiame skyriuje išvardytų susietų papildomų „IBM SaaS“ prenumeratos pasiūlymų būtina sąlyga.

1.5 **Kitos papildomos „IBM SaaS“ prenumeratos**

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

1.6 **Apibrėžtys**

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, kurią Klientas užsiprenumeravo kaip įeinančią į „IBM SaaS Services“.

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

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

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

2. **„IBM Security Trusteer Rapport“ pasiūlymai**

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

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

Šis „IBM SaaS“ pasiūlymas apima Priskirto dalyvio apskaitos sistemą. Verslo pasiūlymai parduodami paketais po 10 Priskirtų dalyvių. Mažmeninės prekybos pasiūlymai parduodami paketais po 100 Priskirtų dalyvių.

Šis „IBM SaaS“ pasiūlymas apima:

- a. „Trusteer Management Application“ (TMA):

TMA galima rasti „IBM Security Trusteer“ debesyje laikomoje aplinkoje, kurioje Klientas (ir neribotas įgaliotų darbuotojų skaičius) gali: (i) gauti įvykių duomenų ataskaitas ir rizikos vertinimus, (ii) peržiūrėti, konfigūruoti ir nustatyti politiką, susijusią su įvykių duomenų ataskaitomis, ir (iii) peržiūrėti konfigūraciją kliento programinės įrangos, licencijuotos veikti viešai ir nemokamai pagal galutinio vartotojo licencijos sutartį (EULA), kurią galima atsisiųsti į Priskirto dalyvio kompiuterį ar įrenginius (asmeninius kompiuterius / MAC). Ta aplinka dar vadinama „Trusteer Rapport“ programinės įrangos paketu („Paskyros turėtojo Kliento programinė įranga“). 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 veiksams atlikti ar leisti ja naudotis savo darbuotojams (ne darbuotojo asmeninio naudojimo tikslais).
- b. Žiniatinklio scenarijus:

Prieiga svetainėje norint pasiekti arba naudoti „IBM SaaS“ pasiūlymus.
- 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, dėl kurios Klientas užsiprenumeravo „IBM SaaS“ pasiūlymus. 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, dėl kurių Klientas užsiprenumeravo „IBM SaaS“ pasiūlymus. 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 Security 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 Security Trusteer Rapport Mandatory Service“ „SaaS“ pasiūlymą, jei Klientas nori taikyti bet kurio tipo privalomą Paskyros turėtojo Kliento programinės įrangos diegimą.

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

2.2 „IBM SaaS Offerings for IBM Security Trusteer Rapport for Business“ ir (arba) „IBM Security Trusteer Rapport for Retail“ pasirenkami papildomi pasiūlymai

„IBM Security Trusteer Rapport“ pasiūlymų prenumerata yra būtina sąlyga prenumeruojant bet kuriuos toliau išvardytus papildomus „IBM SaaS“ pasiūlymus. Jei „IBM SaaS“ pažymėtas kaip „Verslui“, įsigytas papildomas „IBM SaaS“ pasiūlymas taip pat turi būti pažymėtas „Verslui“. Jei „IBM SaaS“ pažymėtas kaip „Mažmeninei prekybai“, įsigytas papildomas „IBM SaaS“ pasiūlymas taip pat turi būti pažymėtas „Mažmeninei prekybai“. Klientas gaus įvykių duomenis iš Priskirtų dalyvių, pas kuriuos veikia Paskyros turėtojo Kliento programinė įranga ir kurie yra sutikę EULA, bent kartą yra autentifikuoti kaip besinaudojantys Kliento Verslo ir (arba) Mažmeninės prekybos programa (-omis), o Kliento konfigūracija turi apimti Vartotojo ID rinkinį.

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

Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenis, susijusius su kenkėjiškos programinės įrangos užkrėtimo atvejais ir kitais galutinio taško pažeidžiamumais konkrečiame Paskyros turėtojo kompiuteryje.

2.2.2 „IBM Security Trusteer Rapport Phishing Protection for Business“ ir (arba) „IBM Security 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 „IBM SaaS“ gali įspėti Paskyros turėtojus, kad teisėta svetainė yra apsimestinė. Tokiu atveju Klientas privalo pranešti IBM apie tokią klaidą, o IBM ją ištaisys. Tai bus vienintelė Kliento teisių gynbos priemonė šios kaidos atžvilgiu.

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

Klientas gali naudoti „Trusteer“ prisistatymo tinklalapio rinkodaros platformos egzempliorių norėdamas įgalioti atsisiųsti Paskyros turėtojo Kliento programinę įrangą Priskirtiems dalyviams, galintiems pasiekti Kliento Verslo ir (arba) Mažmeninės prekybos programas, dėl kurių Klientas užsiprenumeravo „IBM SaaS“ pasiūlymą.

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

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

Klientas gali įdiegti „IBM Security Trusteer Rapport Mandatory Service“ papildomą funkciją tik tada, jei ji buvo užsakyta ir sukonfigūruota naudoti su Kliento Mažmeninės prekybos arba Verslo programa, dėl kurios Klientas užsiprenumeravo „IBM SaaS“ pasiūlymus.

3. „IBM Security Trusteer Pinpoint“ pasiūlymai

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

Šis „IBM SaaS“ pasiūlymas apima:

a. TMA:

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

b. Žiniatinklio scenarijus ir (arba) API:

Diegimas svetainėje norint pasiekti arba naudoti „IBM SaaS“.

3.1 „IBM Security Trusteer Pinpoint Malware Detection“ ir „IBM Security Trusteer Pinpoint Criminal Detection“

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

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

Įtartinų paskyrų perėmimas klientui nedalyvaujant, naršyklių veikimas prisijungiant prie Verslo arba Mažmeninės prekybos programos, naudojant įrenginio ID, sukčiavimo apsimetant aptikimas ir kenkėjiškos programos aptikimas, kai bandoma pavogti kredencialus. „IBM Security Trusteer Pinpoint Criminal Detection“ 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.

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), dėl kurios (-ių) Klientas užsiprenumeravo „IBM SaaS“ pasiūlymus, arba Klientas gali gauti įvykių duomenis per galutinio taško API pristatymo režimą.

3.1.2 „IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile“ ir (arba) „IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile“

„IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile)“ pasiūlymai sukurti, kad suteiktų dar vieną apsaugos sluoksnį ir apsaugotų nuo paskyros perėmimo bei apgaulingos veiklos. Jie atpažįsta neteisėtą paskyros prieigą ir teikia Klientui rekomendaciją. Šis „IBM SaaS“ pasiūlymas renka informaciją tiek iš Kliento Verslo ir (arba) Mažmeninės prekybos programų, kuriose naudojami „PPCD Mobile“, ir iš Priskirtų dalyvių mobiliųjų įrenginių. „IBM Security Trusteer PPCD Mobile“ pasiūlymai skirti susieti tarpusavyje sudėtinę informaciją, susijusią su Priskirtų dalyvių mobiliaisiais įrenginiais, su kitais duomenų šaltiniais, pvz., kenkėjiškos programinės įrangos užkrėtimais realiuoju laiku ir sukčiavimo apsimetant incidentais. Šie šaltiniai yra integruoti per kitus „IBM Security Trusteer“ „IBM SaaS“ pasiūlymus, nurodytus šiose NS.

Klientas gali naudoti „IBM Security Trusteer PPCD Mobile“ pasiūlymus, esančius „IBM Security Trusteer“ debesų kompiuterijos aplinkoje, kad gautų rizikos vertinimo duomenis iš Priskirtų dalyvių mobiliųjų įrenginių. Duomenys bus sugeneruojami atsižvelgiant į šių mobiliųjų įrenginių internetinę sąveiką su Kliento Verslo ar Mažmeninės prekybos programa, dėl kurios Klientas užsiprenumeravo „IBM SaaS“ pasiūlymus. Kiek tai susiję su šiais pasiūlymais, „mobilieji įrenginiai“ yra tik palaikomi mobilieji telefonai ir planšetiniai kompiuteriai, bet ne asmeniniai arba MAC kompiuteriai.

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

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

a. Įvykių duomenys:

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

b. Papildomas leidimas:

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

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

c. Standartinis leidimas:

Verslo arba Mažmeninės prekybos standartinis leidimas yra greitai įdiegiamas sprendimas, suteikiantis šiam „IBM SaaS“ pasiūlymui pagrindines funkcijas, kaip aprašyta šiame skyriuje.

3.2 Pasirinktinis papildomas „IBM SaaS Offerings for IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition“ ir (arba) „IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition“, ir (arba) „IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition“ ir (arba) „IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition“

Naudojant „IBM Security Trusteer Rapport Remediation for Retail“ pasiūlymus, taikoma būtina „IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition“ arba „IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition“ sąlyga.

Naudojant „IBM Security Trusteer Pinpoint Carbon Copy for Retail“, taikoma būtina „IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition“ arba „IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition“ sąlyga. Naudojant „IBM Security Trusteer Pinpoint Carbon Copy for Business“, taikoma būtina „IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition“ arba „IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition“ sąlyga.

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

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

3.2.2 „IBM Security Trusteer Rapport Remediation for Retail“

„IBM Security Trusteer Rapport Remediation for Retail“ pasiūlymas yra skirtas 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 Mažmeninės prekybos programos ad-hoc tvarka, kai „MitB“ kenkėjiškos programinės įrangos užkratus aptinka „IBM Security Trusteer Pinpoint Malware Detection“ įvykių duomenys. Klientas privalo turėti „IBM Security Trusteer Pinpoint Malware Detection“ prenumeratą, veikiančią Kliento Mažmeninės prekybos programoje. Klientas gali naudoti šį „IBM SaaS“ pasiūlymą 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 Security Trusteer Rapport Remediation for Retail“ turi praktiškai veikti tokiaame 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, šis „IBM SaaS“ 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.

4. „IBM Security Trusteer Mobile“ pasiūlymai

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

„IBM Security Trusteer Mobile Browser“ sukurtas kaip papildomas apsaugos sluoksnis ir yra skirtas suteikti saugią internetinę Priskirtų dalyvių mobiliųjų įrenginių prieigą prie Kliento Mažmeninės prekybos arba Verslo programų, dėl kurių Klientas užsiprenumeravo „IBM SaaS“ pasiūlymus, mobiliųjų įrenginių rizikos vertinimą ir apsaugą nuo sukčiavimo apsimitant. Saugaus „Wi-Fi“ aptikimas pasiekiamas tik „Android“ platformose. Šio „IBM SaaS“ pasiūlymo tikslas – įtraukti mobiliuosius įrenginius, tai yra mobiliuosius telefonus ar planšetinius kompiuterius, bet neįtraukti nešiojamųjų kompiuterių ir „Mac“.

Naudodamas TMA, Klientas (ir neribotas įgaliotų darbuotojų skaičius) gali gauti įvykių duomenis, analizę ir statistinę informaciją, susijusią su įrenginiais, kuriuos turintys Priskirti dalyviai: (i) atsisiuntė Paskyros turėtojo Kliento programinę įrangą, programą, licencijuotą naudoti nemokamai ir viešai pagal galutinio vartotojo licencijos sutartį (EULA), ir padarė atsisiunčiamą į Priskirtų dalyvių mobiliuosius įrenginius, ir (ii) sutiko su EULA sutartimi ir bent kartą yra autentifikuoti kaip besinaudojantys Kliento Verslo ar Mažmeninės prekybos programomis, dėl kurių Klientas užsiprenumeravo „IBM SaaS“. Klientas gali

reklamuoti Paskyros turėtojo Kliento programinę įrangą tik naudodamas „Trusteer“ prisistatymo tinklalapį ir negali naudoti Paskyros turėtojo Kliento programinės įrangos vidiniams įmonės veiksmams atlikti.

a. Įvykių duomenys:

Klientas (ir neribotas skaičius jo įgaliotųjų darbuotojų) gali naudoti TMA, kad gautų įvykių duomenis, sugeneruotus kaip mobiliųjų įrenginių internetinės sąveikos su Verslo ar Mažmeninės prekybos programomis, dėl kurių Klientas užsiprenumeravo „IBM SaaS“ pasiūlymus.

b. „Trusteer“ prisistatymo tinklalapis:

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

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

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

„IBM Security Trusteer Mobile SDK“ pasiūlymai sukurti dar vieną papildomą apsaugos sluoksnį ir yra skirti suteikti saugią internetinę prieigą prie Kliento Verslo ir (arba) Mažmeninės prekybos programų, dėl kurių Klientas užsiprenumeravo „IBM SaaS“ pasiūlymus, įrenginių rizikos vertinimą ir apsaugą nuo kibernetinių atakų. Saugaus „Wi-Fi“ aptikimas pasiekiamas tik „Android“ platformose.

„IBM Security Trusteer Mobile SDK“ pasiūlymai 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, žinomus kaip „IBM Security Trusteer“ mobilioji biblioteka, taip pat Vykdomo laiko komponentas arba Perskirstymo paketas, nuosavybinis kodas, kurį sugeneravo „IBM Security Trusteer Mobile SDK“. Šį pasiūlymą galima įdėti ir integruoti į atskirą, apsaugotą Kliento „iOS“ arba „Android“ mobiliąsias programas, dėl kurių Klientas užsiprenumeravo „IBM SaaS“ pasiūlymus („Kliento integruota mobiliojo programa“).

„IBM Security Trusteer Mobile SDK for Retail“ galima gauti paketais po 100 Priskirtų dalyvių arba paketais po 100 Kliento įrenginių, o „IBM Security 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 įvykių 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 Security Trusteer Mobile SDK“ tik kurdamas Kliento integruotą mobiliojo 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 taikomos šios NS;
- c. prekiauti ir platinti 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, be galimybės atsisakyti to sutartimi, 3) negali licencijuoti trečiajai šaliai, nuomoti ir išperkamosios nuomos pagrindais suteikti SDK, (4) negali pašalinti jokių Perskirstymo pakete esančių autoriaus teisių arba įspėjamųjų 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 mobiliojo programą be IBM arba atitinkamo licencijos davėjo ar platintojo išankstinio sutikimo raštu.

- Perskirstymo paketas turi likti neatskiriama integruotas Kliento integruotoje mobiliojo programoje. Perskirstymo 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, be galimybės atsisakyti to sutartimi. 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.

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 „IBM SaaS“ pasiūlymo naudojimą.

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

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

5. „IBM SaaS Fraud Protection“ pasiūlymų diegimas

Kliento pagrindinė prenumerata apima reikiamą nustatymą ir pradinio diegimo veiksmus, įskaitant pradinį vienkartinį įjungimą, konfigūravimą, Prisistatymo tinklalapio šablonus, testavimą ir mokymą.

Dėl papildomų paslaugų galima sudaryti atskirą sutartį ir mokėti už jas atskirą mokestį.

B priedas

IBM teikia toliau nurodytą pasiekiamumo paslaugos lygio susitarimą (PLS), kuris yra skirtas „IBM SaaS“ ir taikomas, jei nurodyta Kliento Sandorio dokumente:

Taikoma ta PLS versija, kuri galioja pradėjus vykdyti Kliento prenumeratą arba atnaujinus prenumeratos sąlygas. Klientas supranta, kad PLS nesuteikia garantijos.

1. Apibrėžtys

- a. **Įgaliotasis kontaktinis asmuo** – tai asmuo, kurį Klientas nurodė IBM kaip turintį teisę teikti Pretenzijas pagal šią PLS.
- b. **Pasiekiamumo kreditas** – tai IBM suteikiama teisių gynimo priemonė (kompensacija) už patvirtintą Pretenziją. Pasiekiamumo kreditas bus pritaikytas kredito arba nuolaidos forma kitoje sąskaitoje už „IBM SaaS“ prenumeratą.
- c. **Pretenzija** – tai Kliento Įgaliotojo kontaktinio asmens pagal šią PLS pateikta pretenzija IBM dėl nepasiekto Paslaugų lygio per Sutartinį mėnesį.
- d. **Sutartinis mėnuo** – tai kiekvienas visas „IBM SaaS“ teikimo laikotarpio mėnuo, skaičiuojamas nuo 00:00 GMT pirmąją mėnesio dieną iki 23:59 GMT paskutinę mėnesio dieną.
- e. **Klientas** – tai subjektas, prenumeruojantis „IBM SaaS“ tiesiai iš IBM ir neturintis jokių neįvykdytų materialinių įsipareigojimų, įskaitant mokestinius įsipareigojimus, pagal šią „IBM SaaS“ sutartį su IBM.
- f. **Prastovos** – tai laikotarpis, per kurį Paslaugos gamybos sistema nustojo veikti ir visi jūsų vartotojai negalėjo naudoti visų Paslaugos aspektų, kurių teises jie turi. Į Prastovos laiką neįtraukiamas laikotarpis, kai Paslauga nepasiekama dėl:
 - suplanuotų sistemos prastovų;
 - „Force Majeure“;
 - problemos, susijusios su Kliento arba trečiosios šalies taikomosiomis programomis, įranga arba duomenimis;
 - Kliento ar trečiųjų šalių veiksmų ar jų neatlikimo (įskaitant visus atvejus, kai prieiga prie „IBM SaaS“ gaunama, pasinaudojus Kliento slaptažodžiais ar įranga);
 - privalomų sistemos konfigūracijų ir palaikomų platformų nesilaikymo naudojant „IBM SaaS“;
 - kliento arba Kliento vardu trečiosios šalies pateiktų planų, specifikacijų arba instrukcijų IBM laikymosi.
- g. **Įvykis** – tai aplinkybė ar aplinkybių rinkinys, dėl kurio Paslaugų lygis nebuvo pasiektas.
- h. **„Force Majeure“** – tai nenugalima jėga, teroristinis išpuolis, streikas, gaisras, potvynis, žemės drebėjimas, riaušės, karas, vyriausybės veiksmai, įsakymai ar apribojimai, virusai, paslaugų neteikimo atakos ir kiti kenkėjiški veiksmai, komunalinių paslaugų sutrikimai ir tinklo ryšių gedimai ar bet kokia kita priežastis, dėl kurios „IBM SaaS“ tapo nepasiekiamas ir kurios IBM pagrįstai negalėjo kontroliuoti.
- i. **Suplanuotos sistemos prastovos** – tai suplanuotas „IBM SaaS“ teikimo nutraukimas, siekiant atlikti techninę priežiūrą.
- j. **Paslaugos lygis** – tai toliau nustatytas standartas, pagal kurį IBM vertina paslaugos, kurią teikia pagal šią PLS, lygį.

2. Pasiekiamumo kreditai

- a. Norėdamas pateikti Pretenziją, Klientas IBM klientų palaikymo centre turi užregistruoti kiekvieno atitinkamos „IBM SaaS“ Įvykio palaikymo kortelę, vykdydamas IBM procedūrą, skirtą pranešti apie 1 sudėtingumo problemas. Klientas turi pateikti visą reikiamą ir išsamią informaciją apie Įvykį bei padėti IBM jį įvertinti ir išspręsti tokiu lygmeniu, koks numatytas 1 sudėtingumo palaikymo kortelėje. Tokia kortelė turi būti užregistruota per dvidešimt keturias (24) valandas, Klientui sužinojus, kad Įvykis paveikė Kliento „IBM SaaS“ naudojimą.

- b. Kliento Įgaliotasis kontaktinis asmuo Kliento Pretenziją dėl Pasiekiamumo kredito turi pateikti ne vėliau kaip per tris (3) darbo dienas nuo Sutartinio mėnesio, per kurį atsitiko Įvykis, pabaigos.
- c. Kliento Įgaliotasis kontaktinis asmuo turi IBM pateikti visą pagrįstą išsamią su Pretenzija susijusią informaciją, įskaitant, bet neapsiribojant, išsamius visų atitinkamų Įvykių aprašymus, ir nurodyti nepasiektą Paslaugos lygį.
- d. IBM įvertins kiekvieno Sutartinio mėnesio bendrą Prastovos laiką, taikomą atitinkamam Paslaugos lygiui, nurodytam toliau esančioje lentelėje. Pasiekiamumo kreditai bus pagrįsti Prastovos laiko trukme, skaičiuojama nuo pirmojo Kliento pranešimo apie Klientą paveikusį Prastovos laiką. Jei Klientas praneša apie vienu metu įvykusius Taikomosios programos prastovos laiko Įvykį ir Gaunamų duomenų tvarkymo prastovos laiko Įvykį, persidengiančius laikotarpius IBM laikys vienu Prastovos laiko laikotarpiu, bet ne dviem atskirais Prastovos laiko laikotarpiais. Kiekvienos galiojančios Pretenzijos atveju IBM taikys aukščiausią galimą Pasiekiamumo kreditą, pagrįstą kiekvieną Sutartinį mėnesį pasiektu Paslaugos lygiu, kaip nurodyta toliau esančiose lentelėse. IBM neįsipareigoja teikti kelių Pasiekiamumo kreditų už tą patį Įvykį (-ius) per tą patį Sutartinį mėnesį.
- e. Jei naudojamas Paslaugų paketas (atskiri „IBM SaaS“ supakuoti ir parduodami kartu už vieną sudėtinę kainą), Pasiekiamumo kreditas bus apskaičiuojamas, atsižvelgiant į vieną sudėtinę mėnesio kainą už Paslaugų paketą, o ne į mėnesinį prenumeratos mokestį už kiekvieną „IBM SaaS“ atskirai. Klientas gali pateikti tik tokias Pretenzijas, kurios yra susijusios su vienu paketo „IBM SaaS“ per bet kurį Sutartinį mėnesį. IBM neįsipareigoja suteikti Pasiekiamumo kreditų daugiau nei vienam paketo „IBM SaaS“ bet kurį Sutartinį mėnesį.
- f. Jei Klientas įsigijo „IBM SaaS“ iš teisėto IBM pardavėjo perpardavimo būdu, kai IBM išlaiko pirminę atsakomybę už „IBM SaaS“ atlikimą ir PLS įsipareigojimus, Pasiekiamumo kreditas suteikiamas, atsižvelgiant į tuo metu galiojančią Santykiais pagrįstą vertės kainą (RSVP) už „IBM SaaS“, kuri galioja Pretenzijoje nurodytą Sutartinį mėnesį, pritaikant jam 50 % nuolaidą.
- g. Bendra suteikiamų Pasiekiamumo kreditų suma, atsižvelgiant į bet kurį Sutartinį mėnesį, jokių atvejų neviršys dešimties procentų (10 %) vienos dvyliktosios (1/12) Kliento metinio mokesčio IBM už „IBM SaaS“.
- h. IBM savo pagrįstu sprendimu patvirtins Pretenzijas, remdamasi IBM įrašuose turima informacija, kuri, kilus prieštaravimui, bus laikoma viršesne už Kliento įrašuose esančius duomenis.
- i. PAGAL ŠIĄ PLS KLIENTUI SUTEIKIAMI PASIEKIAMUMO KREDITAI YRA VIENINTELĖ IR IŠIMTINĖ TEISIŲ GYNIMO PRIEMONĖ ESANT BET KOKIAI PRETENZIJAI.

3. Paslaugų lygiai

„IBM SaaS“ pasiekiamumas per Sutartinį mėnesį

Pasiektas paslaugos lygis (per Sutartinį mėnesį)	Pasiekiamumo kreditas (Mėnesinio prenumeratos mokesčio už Sutartinį mėnesį, per kurį iškelta Pretenzija, %)
< 99,5 %	2 %
<98,0 %	5 %
< 96,0 %	10 %

Pasiektas Paslaugos lygis, išreikštas procentine išraiška, apskaičiuojamas (a) iš bendro minučių skaičiaus Sutartinį mėnesį atėmus (b) bendrą Prastovų minučių skaičių Sutartinį mėnesį, gautą rezultatą padalijus iš (c) bendro minučių skaičiaus Sutartinį mėnesį.

Pavyzdžiui, Sutartinį mėnesį iš viso buvo 250 Prastovos minučių

Iš viso Sutartinį mėnesį, kurį sudarė 30 dienų, buvo 43 200 min. - 250 minučių Prastovų = 42 950 minučių <hr/> Iš viso 43 200 minučių	= 2 % Pasiekiamumo kredito už 99,4 % pasiekto Paslaugos lygio per Sutartinį mėnesį
--	---

3.1 Išimtys

Ši PLS skirta tik IBM Klientams. Ši PLS netaikoma:

- beta ir bandomosioms Paslaugoms;
- ne gamybos aplinkoms, įskaitant, bet neapsiribojant, tikrinimo, avarinio atkūrimo, kokybės užtikrinimo arba kūrimo;
- Pretenzijų, kurias iškelė IBM Kliento „IBM SaaS“ vartotojai, svečiai, dalyviai ir leistini kviestiniai.
- Jei Klientas pažeidė bet kokius esminius įsipareigojimus, nurodytus Naudojimo sąlygose, įskaitant, bet neapsiribojant, bet kokių mokestinių įsipareigojimų pažeidimą.