# IBM Trusteer Fraud Protection

Ta opis storitve opisuje storitve v oblaku, ki jih IBM zagotavlja naročniku. Naročnik pomeni pogodbeno stranko in njene pooblaščene uporabnike ter prejemnike storitev v oblaku. Veljavna ponudba in dokazilo o upravičenosti sta zagotovljena v obliki ločenih transakcijskih dokumentov.

## 1. Storitev v oblaku

Ta opis storitev velja za naslednje storitve v oblaku:

**Storitve v oblaku Pinpoint Assure:**

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

**Storitve v oblaku Rapport:**

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

**Storitve v oblaku Pinpoint:**

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

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

**Storitve v oblaku Mobile:**

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

## 1.1 Poslovne in prodajne storitve v oblaku

Storitve v oblaku IBM Trusteer so odobrene za uporabo z določenimi vrstami aplikacij. Aplikacija je opredeljena kot ena od naslednjih vrst: prodajna ali poslovna. Za prodajne in poslovne aplikacije so na voljo ločene ponudbe.

a. Prodajna aplikacija je opredeljena kot aplikacija za spletno bančništvo, mobilna aplikacija ali aplikacija za e-trgovino, ki je zasnovana za uporabo s strani potrošnikov. Naročnikov pravilnik lahko klasificira določena mala podjetja kot primerna za prodajni dostop.

b. Poslovna aplikacija je opredeljena kot aplikacija za spletno bančništvo, mobilna aplikacija ali aplikacija za e-trgovino, ki je zasnovana za uporabo s strani podjetij, ustanov ali enakovrednih entitet, oz. katerakoli aplikacija, ki ni opredeljena kot prodajna.

### 1.1.1 Poslovne storitve v oblaku

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

### 1.1.2 Prodajne storitve v oblaku

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

Za vsako poslovno (Business) in prodajno (Retail) storitev v oblaku je za dodatno plačilo na voljo povezani produkt Premium Support, razen za storitve v oblaku IBM Trusteer Mobile SDK.

### 1.1.3 Dodatne storitve v oblaku za IBM Trusteer Rapport II

a. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Rapport II for Business:
   - IBM Trusteer Rapport Fraud Feeds for Business
   - IBM Trusteer Rapport Phishing Protection for Business
   - IBM Trusteer Rapport Mandatory Service for Business
   - IBM Trusteer Rapport Additional Applications for Business

b. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Rapport II for Retail:
   - IBM Trusteer Rapport Fraud Feeds for Retail
   - IBM Trusteer Rapport Phishing Protection for Retail
   - IBM Trusteer Rapport Mandatory Service for Retail
   - IBM Trusteer Rapport Additional Applications For Retail

Za vse dodatke k storitvam v oblaku IBM Trusteer Rapport, tako za poslovanje (Business) kot za prodajo (Retail), razen za dodatke IBM Trusteer Rapport Mandatory Service, je za dodatno plačilo na voljo povezani produkt Premium Support.

Naročnina na storitev IBM Trusteer Rapport II for Business ali IBM Trusteer Rapport II for Retail je predpogoj za povezane dodatne storitve v oblaku, ki so navedene v tem razdelku.

### 1.1.4 Dodatne storitve v oblaku za IBM Trusteer Pinpoint Malware Detection II

a. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business:
   - IBM Trusteer Rapport Remediation for Business
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail:
   - IBM Trusteer Rapport Remediation for Retail
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

Podpora Premium je na voljo za posebne ponudbe, kot je navedeno v tem dokumentu. Naročnina na IBM Trusteer Pinpoint Malware Detection II for Business ali IBM Trusteer Pinpoint Malware Detection II for Retail je predpogoj za povezane dodatne storitve v oblaku, navedene v tem razdelku.

#### 1.1.5 Dodatne storitve v oblaku za IBM Trusteer Pinpoint Detect Standard in/ali IBM Trusteer Pinpoint Detect Premium in/ali IBM Trusteer Pinpoint Detect Standard for Retail in/ali IBM Trusteer Pinpoint Detect Premium for Retail in/ali IBM Trusteer Pinpoint Detect Standard for Business in/ali IBM Trusteer Pinpoint Detect Premium for Business

a. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Detect Standard for Business in/ali IBM Trusteer Pinpoint Detect Premium for Business:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
   - IBM Trusteer Digital Content Pack for Business
   - IBM Trusteer New Account Fraud for Business

b. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Detect Standard for Retail in/ali IBM Trusteer Pinpoint Detect Premium for Retail:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
   - IBM Trusteer Digital Content Pack for Retail
   - IBM Trusteer New Account Fraud for Retail

c. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Pinpoint Detect Standard in/ali IBM Trusteer Pinpoint Premium:
   - IBM Trusteer Pinpoint Detect Standard Application
   - IBM Trusteer Pinpoint Detect Premium Application

d. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Pinpoint Detect Premium
   - IBM Trusteer Pinpoint Verify

Naročnina na IBM Trusteer Pinpoint Detect Standard ali IBM Trusteer Pinpoint Detect Premium ali IBM Trusteer Pinpoint Detect Standard for Retail ali IBM Trusteer Pinpoint Detect Premium for Retail ali IBM Trusteer Pinpoint Detect Standard for Business ali IBM Trusteer Pinpoint Detect Premium for Business je predpogoj za povezane dodatne storitve v oblaku, ki so navedene v tem razdelku.

#### 1.1.6 Druge dodatne storitve v oblaku

Morebitne dodatne naročnine za storitve v oblaku za zgornje osnovne naročnine, ki niso navedene v tem dokumentu, in so bodisi trenutno na voljo ali še v razvoju, se ne štejejo kot posodobitev in jih je treba odobriti ločeno.

### 1.2 Opredelitev pojmov

**Imetnik računa** – je naročnikov končni uporabnik, ki je namestil programsko opremo za aktiviranje odjemalca, sprejel licenčno pogodbo za končne uporabnike ("EULA") in se je vsaj enkrat overil v naročnikovi prodajni ali poslovni aplikaciji, za katero ima naročnik naročnino za storitve v oblaku.

**Odjemalska programska oprema imetnika računa** – je programska oprema za aktiviranje odjemalca IBM Trusteer Rapport ali katerakoli druga programska oprema za aktiviranje odjemalca, ki je zagotovljena v nekaterih storitvah v oblaku za namestitev v napravo končnega uporabnika.

**Trusteer Splash** se nanaša na pozdravno okno, ki se naročniku zagotovi na podlagi razpoložljivih pozdravnih predlog.

**Pristajalna stran** se nanaša na stran, ki jo gosti IBM ter se naročniku zagotovi skupaj s pozdravnim oknom za naročnike in odjemalsko programsko opremo imetnika računa, ki jo je mogoče prenesti.

## 1.3 IBM Trusteer Rapport Cloud Services

### 1.3.1 IBM Trusteer Rapport II for Retail and/or IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Trusteer Rapport II Cloud Service je nova izgradnja storitve IBM Trusteer Rapport za lažjo standardizacijo stroškov, povezanih z zaščito več aplikacij, in se uporablja namesto enkratnih stroškov pri dodajanju aplikacij.

Trusteer Rapport II zagotavlja plast zaščite proti lažnemu predstavljanju in napadom zlonamerne programske opreme Man-in-the-Browser (MitB). Z omrežjem, ki vključuje na desetine milijonov končnih točk po svetu, IBM Trusteer Rapport zbira podatke o dejavnem lažnem predstavljanju in zlonamernih napadih na organizacije po vsem svetu. IBM Trusteer Rapport uporablja vedenjske algoritme, ki blokirajo napade lažnega predstavljanja ter preprečijo namestitev in delovanje zlonamerne programske opreme MitB.

Upravičenost do te storitve v oblaku temelji na metriki zaračunavanja z upravičenimi udeleženci ali metriki zaračunavanja z odjemalskimi napravami. Poslovna ponudba je naprodaj v paketih po 10 upravičenih udeležencev ali po 10 odjemalskih naprav. Prodajna ponudba je naprodaj v paketih po 100 upravičenih udeležencev ali po 100 odjemalskih naprav.

Ta ponudba storitev v oblaku vključuje:

a. Trusteer Management Application ("TMA"):

   Aplikacija TMA je na voljo v okolju IBM Trusteer, ki gostuje v oblaku, prek katerega lahko naročnik (in neomejeno število njegovih pooblaščencev): (i) pregleduje in prenaša poročila o nekaterih podatkih o dogodkih in ocene tveganja ter (ii) pregleduje konfiguracijo programske opreme za aktiviranje odjemalca, ki je brezplačno licencirana za naročnikove upravičene udeležence na podlagi licenčne pogodbe za končne uporabnike ("EULA"), pri čemer je na voljo za prenos na namizja ali v naprave (PC/Mac) upravičenega udeleženca - z drugim imenom zbirka programske opreme Trusteer Rapport ("odjemalska programska oprema imetnika računa"). Naročnik lahko odjemalsko programsko opremo imetnika računa trži samo prek platforme Trusteer Splash ali Rapport API in je ne sme uporabljati za notranje poslovanje ali uporabo s strani zaposlenih (razen za njihovo osebno uporabo).

b. Spletni skript:

   Za dostop na spletnem mestu za namene dostopa ali uporabe storitve v oblaku.

c. Podatki o dogodkih:

   Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporablja aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih z odjemalsko programsko opremo imetnika računa na podlagi spletnih interakcij imetnikov računov z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami, za katere ima naročnik naročnino za storitve v oblaku. Podatki o dogodkih bodo prejeti iz odjemalske programske opreme imetnika računa, ki se izvaja v napravah upravičenih udeležencev, ki so sprejeli pogodbo EULA in se vsaj enkrat overili v naročnikovi poslovni ali prodajni aplikaciji, pri čemer mora naročnikova konfiguracija vključevati zbirko ID-jev uporabnikov.

d. Trusteer Splash:

   Platforma za trženje Trusteer Splash predstavi in trži odjemalsko programsko opremo imetnika računa upravičenim udeležencem, ki dostopajo do naročnikovih poslovnih in/ali prodajnih aplikacij, za katere ima naročnik naročnino za storitve v oblaku. Naročnik lahko izbira med razpoložljivimi pozdravnimi predlogami. Pozdravno okno po meri se lahko pogodbeno določi na podlagi ločene pogodbe ali dogovora o obsegu del.

Naročnik lahko soglaša, da svoje blagovne znamke, logotipe ali ikone ponudi v uporabo v povezavi z aplikacijo TMA in samo za uporabo s platformo Trusteer Splash ter za prikaz v odjemalski programski opremi imetnika računa ali na pristajalnih straneh, ki jih gostita IBM in spletna stran IBM Trusteer. Vsaka uporaba naročnikovih blagovnih znamk, logotipov ali ikon bo v skladu z IBM-ovimi razumnimi načeli glede oglaševanja in uporabe blagovnih znamk.

Naročnik mora skleniti naročnino za IBM Trusteer Rapport Mandatory Service, če želi izvesti katerokoli vrsto obvezne razmestitve odjemalske programske opreme imetnika računa.

Obvezna razmestitev odjemalske programske opreme imetnika računa med drugim vključuje katerokoli vrsto obvezne razmestitve na podlagi kateregakoli mehanizma ali sredstva, ki od upravičenega

udeleženca neposredno ali posredno zahteva prenos odjemalske programske opreme imetnika računa, ali katerokoli metodo, orodje, postopek, pogodbo ali mehanizem, ki ga IBM ni ustvaril ali odobril in je ustvarjen za to, da obide zahteve za licenciranje v okviru te obvezne razmestitve odjemalske programske opreme imetnika računa.

Posamezna ponudba Trusteer Rapport II for Business in/ali Trusteer Rapport II for Retail vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Rapport Additional Applications.

### 1.3.2 Neobvezne dodatne storitve v oblaku za IBM Trusteer Rapport II for Business in/ali IBM Trusteer Rapport II for Retail

Naročnina na storitve v oblaku IBM Trusteer Rapport II je predpogoj za naročnino na katero koli od dodatnih storitev v oblaku, navedenih v nadaljevanju. Če je storitev v oblaku označena za poslovanje ("for Business"), mora biti tudi dodatna pridobljena storitev v oblaku označena za poslovanje ("for Business"). Če je storitev v oblaku označena za prodajo ("for Retail"), mora biti tudi dodatna pridobljena storitev v oblaku označena za prodajo ("for Retail"). Naročnik bo prejel podatke o dogodkih bodisi od upravičenih udeležencev, ki so sprejeli pogodbo EULA in se vsaj enkrat overili v naročnikovi poslovni in/ali prodajni aplikaciji, pri čemer mora naročnikova konfiguracija vključevati zbirko ID-jev uporabnikov ali odjemalskih naprav, ki izvajajo odjemalsko programsko opremo imetnika računa.

### 1.3.3 IBM Trusteer Rapport Fraud Feeds for Business and/or IBM Trusteer Rapport Fraud Feeds for Retail

Ko naročnik (in neomejeno število njegovih pooblaščencev) sklene naročnino za ta dodatek storitve v oblaku, lahko uporablja aplikacijo TMA za ogledovanje, konfiguriranje in naročanje na dostavo virov groženj, ki jih ustvari storitev v oblaku Trusteer Rapport. Viri so lahko poslani prek e-pošte na podan e-poštni naslov ali prek protokola SFTP v obliki besedilnih datotek.

Ta ponudba je veljavna samo na osnovi metrike zaračunavanja z upravičenimi udeleženci.

### 1.3.4 IBM Trusteer Rapport Phishing Protection for Business and/or IBM Trusteer Rapport Phishing Protection for Retail

Naročnik (in neomejeno število njegovih pooblaščencev) lahko z aplikacijo TMA prejema obvestila s podatki o dogodkih, povezanih s predložitvijo prijavnih poverilnic imetnika računa na domnevnem spletnem mestu za lažno predstavljanje ali goljufivem spletnem mestu. Zakonite spletne aplikacije (URL-ji) so lahko zmotno označene kot spletna mesta za lažno predstavljanje in storitev v oblaku lahko opozori imetnike računov, da je zakonito spletno mesto spletno mesto za lažno predstavljanje. V tem primeru mora naročnik o taki napaki obvestiti IBM, ki bo napako odpravil. To je naročnikovo edino pravno sredstvo v zvezi s tako napako.

Upravičenost do te storitve v oblaku temelji na metriki zaračunavanja z upravičenimi udeleženci ali metriki zaračunavanja z odjemalskimi napravami. Poslovna ponudba je naprodaj v paketih po 10 upravičenih udeležencev ali po 10 odjemalskih naprav. Prodajna ponudba je naprodaj v paketih po 100 upravičenih udeležencev ali po 100 odjemalskih naprav.

Podporo Premium je mogoče za te storitve v oblaku pridobiti na osnovi metrike zaračunavanja z upravičenimi udeleženci ali metrike zaračunavanja z odjemalskimi napravami. Poslovna ponudba je naprodaj v paketih po 10 upravičenih udeležencev ali po 10 odjemalskih naprav. Prodajna ponudba je naprodaj v paketih po 100 upravičenih udeležencev ali po 100 odjemalskih naprav.

### 1.3.5 IBM Trusteer Rapport Mandatory Service for Business and/or IBM Trusteer Rapport Mandatory Service for Retail

Naročnik lahko uporabi primerek platforme za trženje Trusteer Splash za pooblastitev prenosa odjemalske programske opreme imetnika računa za upravičene udeležence, ki dostopajo do naročnikovih poslovnih in/ali prodajnih aplikacij, za katere ima naročnik naročnino za storitve v oblaku.

IBM Trusteer Rapport Premium Support for Business je predpogoj za IBM Security Rapport Mandatory Service for Business.

IBM Trusteer Rapport Premium Support for Retail je predpogoj za IBM Security Rapport Mandatory Service for Retail.

Naročnik lahko uvede dodatno funkcionalnost storitve IBM Trusteer Rapport Mandatory Service, samo če je bila ta storitev naročena in konfigurirana za uporabo z naročnikovo prodajno ali poslovno aplikacijo, za katero ima naročnik naročnino za storitve v oblaku.

Upravičenost do te storitve v oblaku temelji na metriki zaračunavanja z upravičenimi udeleženci. Poslovna ponudba je naprodaj v paketih po 10. Prodajna ponudba je naprodaj v paketih po 100 upravičenih udeležencev.

### 1.3.6 IBM Trusteer Rapport Large Redeployment and/or IBM Trusteer Rapport Small Redeployment

Odjemalci, ki želijo znova namestiti aplikacije za spletno bančništvo med obdobjem storitve, kar posledično zahteva spremembe pri razmestitvi storitve IBM Trusteer Rapport II, naj kupijo storitev v oblaku IBM Trusteer Rapport Redeployment.

Razmestitev je lahko potrebna, ker je naročnik spremenil domeno ali URL gostitelja aplikacije, spremenil konfiguracijo pozdravnega okna ali se preselil na novo platformo spletnega bančništva.

V šestmesečnem obdobju prehoda na razmestitev je naročnik upravičen do dodatnih aplikacij, ki se izvajajo nad obstoječimi naročenimi aplikacijami na podlagi "ena proti ena".

IBM Trusteer Rapport Large Redeployment velja za okolja z več kot 20.000 uporabniki, IBM Trusteer Rapport Small Redeployment pa velja za okolja z manj ali enako kot 20.000 uporabniki.

### 1.3.7 IBM Trusteer Rapport Additional Applications for Business in/ali IBM Trusteer Rapport Additional Applications for Retail

Za IBM Trusteer Rapport II for Business se za razmestitev v vse dodatne poslovne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za storitev v oblaku IBM Trusteer Rapport Additional Applications for Business. Za IBM Trusteer Rapport II for Retail se za razmestitev v vse dodatne prodajne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za storitev v oblaku IBM Trusteer Rapport Additional Applications for Retail.

## 1.4 Storitve v oblaku IBM Trusteer Pinpoint

IBM Trusteer Pinpoint je storitev v oblaku, ki je zasnovana tako, da zagotavlja dodatno plast zaščite ter zaznava in blaži napade zlonamerne programske opreme, lažno predstavljanje in zlorabe računov. Trusteer Pinpoint lahko naročnik integrira v svoje poslovne in/ali prodajne aplikacije, za katere ima naročnik naročnino za storitve v oblaku, in so vključene v postopke za preprečevanje prevar.

Te storitve v oblaku vključujejo:

a. TMA:

   Aplikacija TMA je na voljo v okolju IBM Trusteer, ki ga gosti oblak in prek katerega lahko naročnik (in neomejeno število njegovih pooblaščencev): (i) pregleduje poročila o podatkih dogodkov in ocene tveganja ter (ii) ogleduje, se naroča na in konfigurira dostavo virov groženj, ki se ustvarijo s ponudbami Pinpoint.

b. Spletni skript in/ali API-ji:

   Za razmestitev na spletnem mestu za namene dostopa do storitve v oblaku ali njene uporabe.

### 1.4.1 IBM Trusteer Pinpoint Malware Detection

V primeru zaznavanja zlonamerne programske opreme v storitvah v oblaku IBM Trusteer Pinpoint Malware Detection II Cloud Services mora odjemalec upoštevati navodila v vodiču za storitev Pinpoint za določitev najboljših praks. Storitev v oblaku IBM Trusteer Pinpoint Malware ni dovoljeno uporabljati na načine, ki bi vplivali na izkušnjo upravičenega udeleženca neposredno po primeru zaznavanja zlonamerne programske opreme ali zlorabe računa in bi drugim osebam omogočali povezavo naročnikovih dejanj z uporabo storitev IBM Trusteer Pinpoint Cloud (npr. obvestila, sporočila, blokiranje naprav ali dostop do poslovne in/ali prodajne aplikacije neposredno po primeru zaznavanja zlonamerne programske opreme ali zlorabe računa).

### 1.4.2 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business in/ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail in/ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business in/ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II je nova izgradnja storitve IBM Trusteer Pinpoint Malware Detection za lažjo standardizacijo stroškov, povezanih z zaščito več aplikacij, in se uporablja namesto enkratnih stroškov pri dodajanju aplikacij.

Brez-odjemalsko zaznavanje finančnih brskalnikov, okuženih z zlonamerno programsko opremo (Man-in-the-Browser – MitB) pri povezovanju s poslovno ali prodajno aplikacijo. Storitve v oblaku IBM Trusteer

Pinpoint Malware Detection zagotavljajo dodatno plast zaščite ter organizacijam omogočajo, da se osredotočijo na postopke preprečevanja prevar na podlagi tveganja okužbe z zlonamerno programsko opremo, ki temelji na ocenah in opozorilih o prisotnosti zlonamerne programske opreme MitB, usmerjene proti finančnim aplikacijam.

a. Podatki o dogodkih:

   Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporablja aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih na podlagi spletnih interakcij upravičenih udeležencev z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami.

b. Napredna izdaja (Advanced Edition):

   Napredne izdaje Advanced Editions for Business in/ali Retail ponujajo dodatno raven zaznavanja in zaščite, ki je prilagojena strukturi in poteku odjemalčevih poslovnih (Business) in/ali prodajnih (Retail) aplikacij in se lahko prilagodi tudi določenemu področju groženj, ki cilja na odjemalca. . To plast je mogoče umestiti na različne lokacije v naročnikovih poslovnih in/ali prodajnih aplikacijah.

   Napredna izdaja (Advanced Edition) je odjemalcu ponujena pri najmanj 100K upravičenih udeležencih za Retail ali 10K upravičenih udeležencih za Business, in sicer 1000 paketov 100 upravičenih udeležencev za Retail ali 1000 paketov 10 upravičenih udeležencev za Business.

c. Standardna izdaja (Standard Edition):

   Standardne izdaje Standard Editions for Business in/ali Retail so rešitve za hitro razmestitev, ki ponujajo osrednjo funkcionalnost te storitve v oblaku, kot je opisana tukaj.

Ta storitev v oblaku vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Pinpoint Malware Detection Additional Applications.

### 1.4.3 Izbirne dodatne storitve v oblaku za IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail in/ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail in/ali IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business in/ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- Za storitev v oblaku IBM Trusteer Rapport Remediation for Retail je predpogoj storitev IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Za storitev v oblaku IBM Trusteer Rapport Remediation for Business Cloud Service je predpogoj storitev IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

### 1.4.4 IBM Trusteer Rapport Remediation for Retail in/ali IBM Trusteer Rapport Remediation for Business

Namen storitev IBM Trusteer Rapport Remediation Retail in IBM Trusteer Rapport Remediation for Business je raziskati, sanirati, blokirati in odstraniti okužbe zlonamerne programske opreme man-in-the-browser (MitB) iz okuženih naprav (PC/Mac) naročnikovih upravičenih udeležencev, ki na ravni ad-hoc dostopajo do odjemalčeve aplikacije, in sicer, kjer so okužbe zlonamerne programske opreme MitB zaznali podatki dogodka IBM Trusteer Pinpoint Malware Detection. Odjemalec mora imeti veljavno naročnino na IBM Trusteer Pinpoint Malware Detection II, ki se dejansko izvaja v odjemalčevi aplikaciji. Naročnik lahko uporablja to ponudbo storitve v oblaku izključno v povezavi z upravičenimi udeleženci, ki dostopajo do naročnikove aplikacije, in izključno kot orodje, ki omogoča preiskovanje in popravilo določene okužene naprave (PC/Mac) na ad-hoc osnovi. Storitev IBM Security Trusteer Rapport Remediation se mora dejansko izvajati v taki okuženi napravi (PC/Mac) upravičenega udeleženca, ki mora soglašati s pogoji pogodbe za končnega uporabnika (EULA) in vsaj enkrat izvesti overjanje v povezavi z naročnikovimi aplikacijami, pri čemer mora naročnikova konfiguracija vključevati zbirko ID-jev uporabnikov. V izogib dvoumnosti: ta ponudba storitve v oblaku ne vključuje pravice do uporabe platforme Trusteer Splash in/ali promocije odjemalske programske opreme imetnika računa naročnikovim splošnim upravičenim udeležencem na kakršenkoli drug način.

### 1.4.5 IBM Trusteer Pinpoint Malware Detection Redeployment

Odjemalci, ki želijo ponovno razmestiti aplikacije za spletno bančništvo med obdobjem storitve, kar posledično zahteva spremembe pri razmestitvi storitve IBM Trusteer Pinpoint Malware Detection II, naj kupijo IBM Trusteer Pinpoint Malware Detection Redeployment.

Razmestitev je lahko potrebna, ker je naročnik spremenil domeno ali URL gostitelja aplikacije, pretvoril spletno aplikacijo v novo tehnologijo, se preselil na novo platformo spletnega bančništva ali dodal nov potek za prijavo v obstoječo aplikacijo.

V šestmesečnem obdobju prehoda na razmestitev je naročnik upravičen do dodatnih aplikacij, ki se izvajajo nad obstoječimi naročenimi aplikacijami na podlagi "ena proti ena".

Razmestitev IBM Trusteer Pinpoint Malware Detection Additional Applications For IBM Trusteer Pinpoint Malware Detection II Standard Edition ali IBM Trusteer Pinpoint Malware Detection II Advanced Edition v katerokoli dodatno aplikacijo poleg prve zahteva pooblastilo za IBM Trusteer Pinpoint Malware Detection Additional Applications.

### 1.4.6 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail in/ali IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- Za IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail se za razmestitev v vse dodatne prodajne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.
- Za IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business se za razmestitev v vse dodatne poslovne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za IBM Trusteer Pinpoint Malware Detection Additional Applications for Business.

## 1.5 IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Suite") je zbirka storitev v oblaku, ki je zasnovana za zagotavljanje plasti zaščite pred prevarami in jo je mogoče integrirati z dodatnimi IBM-ovimi produkti, s čimer se zagotovi rešitev za upravljanje življenjskega cikla. Suite vključuje naslednje storitve v oblaku:

- IBM Trusteer Pinpoint Detect, ki zaznava in blaži napade zlonamerne programske opreme, lažno predstavljanje in zlorabe računov. Storitev Trusteer Pinpoint Detect lahko naročnik integrira v svoje poslovne in/ali prodajne aplikacije, za katere ima naročnik naročnino za storitve v oblaku, in so vključene v postopke za preprečevanje prevar.
- IBM Trusteer Rapport for Mitigation, ki odpravlja in ščiti okužene končne točke.

Storitve v oblaku vključujejo:

a. TMA:

   Aplikacija TMA je na voljo v okolju IBM Trusteer, ki gostuje v oblaku, prek katerega lahko naročnik (in neomejeno število njegovih pooblaščencev): (i) prejema poročila o podatkih dogodkov in ocene tveganja ter (ii) pregleduje, konfigurira in nastavlja varnostne pravilnike in pravilnike v zvezi s poročanjem o podatkih dogodkov.

b. Podatki o dogodkih:

   Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporabljajo aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih na podlagi spletnih interakcij upravičenih udeležencev z naročnikovimi aplikacijami, za katere ima naročnik naročnino za storitev v oblaku, ali prejema podatke o dogodkih v načinu dostave prek zalednega API-ja.

c. Spletni skript in/ali API-ji:

   Za razmestitev na spletnem mestu za namene dostopa do storitve v oblaku ali njene uporabe.

**Dobre prakse Pinpoint**

V primeru zaznavanja zlonamerne programske opreme ali zlorabe računa mora naročnik upoštevati navodila v Vodiču za določitev najboljših praks. Storitev v oblaku IBM Trusteer Pinpoint Detect ni dovoljeno uporabljati na načine, ki bi vplivali na izkušnjo upravičenega udeleženca neposredno po primeru zaznavanja zlonamerne programske opreme ali zlorabe računa in bi drugim osebam omogočali povezavo naročnikovih dejanj z uporabo storitev IBM Trusteer Pinpoint Detect (npr. obvestila, sporočila, blokiranje naprav ali dostop do poslovne in/ali prodajne aplikacije neposredno po primeru zaznavanja zlonamerne programske opreme ali zlorabe računa).

### 1.5.1 IBM Trusteer Pinpoint Detect Standard for in/ali IBM Trusteer Pinpoint Detect Standard for Business

Ta storitev v oblaku združuje storitvi v oblaku IBM Trusteer Pinpoint Criminal Detection in IBM Trusteer Pinpoint Malware Detection, kar zagotavlja enotno rešitev.

Rešitev pomaga pri zaznavi zlonamerne programske opreme, ki je ne zazna odjemalec, in/ali pri sumljivi dejavnosti zlorabe računa, ko se brskalniki povežejo s prodajnimi ali poslovnimi aplikacijami, uporabijo identifikacijsko številko naprave,pri zaznavi ribarjenja in zaznavi kraje poverilnic zlonamerne programske opreme. Ponudbe IBM Trusteer Pinpoint zagotavljajo dodatno plast zaščite, zaznavajo poskuse zlorabe računov in odjemalcu posredujejo ocene tveganja brskalnikov ali mobilnih naprav (prek izvirnega brskalnika ali odjemalčeve mobilne aplikacije), ki dostopajo do poslovne ali prodajne aplikacije.

V to storitev v oblaku je vključena standardna podpora (kot je opredeljena spodaj v razdelku o tehnični podpori). Za najvišjo stopnjo podpore mora naročnik kupiti Pinpoint Standard Premium Support.

Ta storitev v oblaku vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Pinpoint Detect Standard Additional Applications.

Storitev je mogoče kupiti v paketih 100 upravičenih udeležencev ali v paketih 100 povezav. Če se naročnik odloči za nakup storitve po povezavah, velja strošek za dodatne aplikacije poleg prve.

### 1.5.2 IBM Trusteer Pinpoint Detect Premium for Retail in/ali IBM Trusteer Pinpoint Detect Premium for Business

Ta storitev v oblaku združuje storitvi v oblaku IBM Trusteer Pinpoint Criminal Detection in IBM Trusteer Pinpoint Malware Detection, kar zagotavlja enotno rešitev, ki je preprosta za integracijo.

Rešitev pomaga pri zaznavi zlonamerne programske opreme, ki je ne zazna odjemalec, in/ali pri sumljivi dejavnosti zlorabe računa, ko se brskalniki povežejo s prodajnimi ali poslovnimi aplikacijami, uporabijo identifikacijsko številko naprave,pri zaznavi ribarjenja in zaznavi kraje poverilnic zlonamerne programske opreme. Ponudbe IBM Trusteer Pinpoint zagotavljajo dodatno plast zaščite, zaznavajo poskuse zlorabe računov in naročniku posredujejo ocene tveganja brskalnikov ali mobilnih naprav (prek izvirnega brskalnika ali naročnikove mobilne aplikacije), ki dostopajo do poslovne ali prodajne aplikacije.

Ta storitev vključuje izboljšano delovanje in storitve, vključno z razširjenimi storitvami razmestitve in nastavitve, prilagojenimi varnostnimi pravilniki, storitvami pregledovanja itd. Storitev vključuje do 200 ur virov v skupni rabi za storitve razmestitve na aplikacijo in 200 ur virov v skupni rabi za analizo varnosti na aplikacijo ob nastavitvi. Trajne storitve vključujejo 20 ur vzdrževanja razmestitve za aplikacijo na leto in 100 ur raziskovanja varnosti za aplikacijo na leto. Katerokoli dodatno delo zahteva dodatno plačilo.

Pinpoint Detect lahko uporablja transakcije iz mobilnih in spletnih kanalov. Če so vključene mobilne transakcije, velja Pinpoint by Connection. Ta storitev v oblaku vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Pinpoint Detect Premium Additional Applications.

V to storitev v oblaku je vključena najvišja stopnja podpore.

Storitve IBM Trusteer Pinpoint Detect Premium for Retail and Business je mogoče kupiti v paketih 100 upravičenih udeležencev ali v paketih 100 povezav. Če se naročnik odloči za nakup storitve po povezavah, velja strošek za dodatne aplikacije poleg prve.

**Pinpoint Detect Policy Manager:**

Aplikacija Policy Manager je vključena v storitev Pinpoint Detect Premium in je na voljo v okolju IBM Trusteer, ki gostuje v oblaku, prek katerega lahko naročnik (in neomejeno število njegovih pooblaščencev): (i) načrtuje, preizkuša in v produkcijsko okolje uvaja logiko za odkrivanje goljufive dejavnosti, (ii) načrtuje poročila in nadzorne plošče ter (iii) pregleduje, konfigurira in nastavlja varnostne pravilnike in pravilnike za odkrivanje sumljive dejavnosti v aplikaciji naročnika.

Za aktiviranje funkcije Policy Manager in za podporo za dodatno poglobljeno obravnavo so zahtevane svetovalne storitve. Podrobnosti o svetovalnih storitvah bodo podane ločeno v dogovoru o obsegu del.

Ko je funkcija Policy Manager aktivirana, si IBM pridržuje pravico do dostopa do naročnikovega okolja za namene podpore, da se naročnikovi pravilniki prilagodijo za odpravljanje večjih težav, ki izhajajo iz sprememb pravilnika.

Naročnik se zavezuje, da bo pred zlorabo varoval katere koli podatke, izpostavljene prek funkcije Policy Manager.

Ko je funkcija Policy Manager aktivirana, mora naročnik upoštevati IBM-ove smernice za določanje pravil, kot je navedeno v dokumentaciji. Naročnik potrjuje, da IBM ni odgovoren za nobeno situacijo, ki bi lahko izhajala iz naročnikovega neupoštevanja teh priporočil.

Kakršne koli težave s stabilnostjo in/ali poslabšanjem kakovosti storitve, ki bi lahko nastale zaradi naročnikove napačne konfiguracije funkcije Policy Manager, se ne bodo obravnavale kot čas nedelovanja za izračun v okviru pogodbe o ravni storitve.

### 1.5.3 Izbirne storitve za IBM Trusteer Pinpoint Detect Standard in/ali IBM Trusteer Pinpoint Detect Premium

Predpogoj za storitve v oblaku iz tega razdelka je pooblastilo za IBM Trusteer Pinpoint Detect Premium ali IBM Trusteer Pinpoint Detect Standard.

### 1.5.4 IBM Trusteer Rapport for Mitigation for Retail in/ali IBM Trusteer Rapport for Mitigation for Business

- Namen storitve IBM Trusteer Rapport for Mitigation for Retail je raziskati, sanirati, blokirati in odstraniti okužbe zlonamerne programske opreme iz okuženih naprav (PC/Mac) naročnikovih upravičenih udeležencev, ki na ravni ad-hoc dostopajo do naročnikove prodajne aplikacije, in sicer, kjer so okužbe zlonamerne programske opreme zaznali podatki dogodkov IBM Trusteer Pinpoint Detect Premium ali IBM Trusteer Pinpoint Detect Standard. Naročnik mora imeti veljavno naročnino na ponudbo IBM Trusteer Pinpoint Detect Premium ali IBM Trusteer Pinpoint Detect Standard, ki se dejansko izvajata v naročnikovi prodajni aplikaciji. Naročnik lahko uporablja to storitev v oblaku izključno v povezavi z upravičenimi udeleženci, ki dostopajo do naročnikove prodajne aplikacije, in izključno kot orodje, ki omogoča preiskovanje in popravilo določene okužene naprave (PC/Mac) na ad-hoc osnovi. Storitev IBM Trusteer Rapport for Mitigation for Retail se mora dejansko izvajati v taki okuženi napravi (PC/Mac) upravičenega udeleženca, ki mora soglašati s pogoji pogodbe EULA in vsaj enkrat izvesti overjanje v povezavi z naročnikovimi prodajnimi aplikacijami, pri čemer mora naročnikova konfiguracija vključevati zbirko ID-jev uporabnikov. V izogib dvoumnosti: ta storitev v oblaku ne vključuje pravice do uporabe platforme Trusteer Splash in/ali promocije odjemalske programske opreme imetnika računa naročnikovim splošnim upravičenim udeležencem na kakršenkoli drug način.
- Namen storitve IBM Trusteer Rapport for Mitigation for Business je raziskati, sanirati, blokirati in odstraniti okužbe zlonamerne programske opreme iz okuženih naprav (PC/Mac) naročnikovih upravičenih udeležencev, ki na ravni ad-hoc dostopajo do naročnikove poslovne aplikacije, in sicer, kjer so okužbe zlonamerne programske opreme zaznali podatki dogodkov IBM Trusteer Pinpoint Detect Premium ali IBM Trusteer Pinpoint Detect Standard. Odjemalec mora imeti veljavno naročnino na IBM Trusteer Pinpoint Detect Premium ali IBM Trsuteer Pinpoint Detect Standard, ki se dejansko izvaja v odjemalčevi aplikaciji. Naročnik lahko uporablja to storitev v oblaku izključno v povezavi z upravičenimi udeleženci, ki dostopajo do naročnikove poslovne aplikacije, in izključno kot orodje, ki omogoča preiskovanje in popravilo določene okužene naprave (PC/Mac) na ad-hoc osnovi. Storitev IBM Trusteer Rapport for Mitigation for Business se mora dejansko izvajati v taki okuženi napravi (PC/Mac) upravičenega udeleženca, ki mora soglašati s pogoji pogodbe EULA in vsaj enkrat izvesti overjanje v povezavi z naročnikovimi prodajnimi aplikacijami, pri čemer mora naročnikova konfiguracija vključevati zbirko ID-jev uporabnikov. V izogib dvoumnosti: ta storitev v oblaku ne vključuje pravice do uporabe platforme Trusteer Splash in/ali promocije odjemalske programske opreme imetnika računa naročnikovim splošnim upravičenim udeležencem na kakršenkoli drug način.

### 1.5.5 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail in/ali IBM Trusteer Pinpoint Detect Standard Additional Applications for Business in/ali IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail in/ali IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

Storitev vključuje do 200 ur virov v skupni rabi za storitve razmestitve na aplikacijo in 200 ur virov v skupni rabi za analizo varnosti na aplikacijo ob nastavitvi. Trajne storitve vključujejo 20 ur vzdrževanja razmestitve za aplikacijo na leto in 100 ur raziskovanja varnosti za aplikacijo na leto.

- Za IBM Trusteer Pinpoint Detect Standard for Retail se za razmestitev v vse dodatne prodajne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.

- Za IBM Trusteer Pinpoint Detect Standard for Business se za razmestitev v vse dodatne poslovne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.
- Za IBM Trusteer Pinpoint Premium for Retail se za razmestitev v vse dodatne prodajne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.
- Za IBM Trusteer Pinpoint Premium for Business se za razmestitev v vse dodatne poslovne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

### 1.5.6 IBM Trusteer Pinpoint Detect Standard Application in/ali IBM Trusteer Pinpoint Detect Premium Application

Ta storitev se lahko uporablja na spletnih in mobilnih kanalih.

Storitev vključuje do 200 ur virov v skupni rabi za storitve razmestitve na aplikacijo in 200 ur virov v skupni rabi za analizo varnosti na aplikacijo ob nastavitvi. Trajne storitve vključujejo 20 ur vzdrževanja razmestitve za aplikacijo na leto in 100 ur raziskovanja varnosti za aplikacijo na leto.

- Razmestitev storitve IBM Trusteer Pinpoint Detect Standard zahteva pooblastilo za IBM Trusteer Pinpoint Detect Standard Application za vsako aplikacijo.
- Razmestitev storitve IBM Trusteer Pinpoint Premium zahteva pooblastilo za IBM Trusteer Pinpoint Detect Premium Application za vsako aplikacijo.

### 1.5.7 IBM Trusteer Pinpoint Detect Standard Redeployment in/ali IBM Trusteer Pinpoint Detect Premium Redeployment

Naročniki, ki želijo ponovno razmestiti aplikacije za spletno bančništvo med obdobjem storitve, kar posledično zahteva spremembe pri razmestitvi storitve IBM Trusteer Pinpoint Detect, naj kupijo IBM Trusteer Pinpoint Detect Redeployment.

Razmestitev je lahko potrebna, ker je naročnik spremenil domeno ali URL gostitelja aplikacije, pretvoril spletno aplikacijo v novo tehnologijo, se preselil na novo platformo spletnega bančništva ali dodal nov potek za prijavo v obstoječo aplikacijo.

V šestmesečnem obdobju prehoda na razmestitev je naročnik upravičen do dodatnih aplikacij, ki se izvajajo nad obstoječimi naročenimi aplikacijami na podlagi "ena proti ena".

### 1.5.8 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support in/ali IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Naročniki, ki kupijo storitev Pinpoint Detect Standard Cloud Service, lahko kupijo storitev Premium Support. Obseg storitev Premium Support je naveden v 4. razdelku spodaj.

### 1.5.9 IBM Trusteer Digital Content Pack for Retail in/ali IBM Trusteer Digital Content Pack for Business

IBM Trusteer Digital Content Pack varnostnim analitikom omogoča integracijo novih modelov prevar, ob tem pa v celoti podpira ustvarjanje in spreminjanje ad hoc modelov, s katerimi se je mogoče odzvati na nastajajoče grožnje. Obsega obširen sklop pravil, vpogledov in pravilnikov, ki jih je mogoče kupiti kot dodaten in sestavni del te rešitve. Digital Content Pack omogoča še tesnejšo povezavo med zmožnostmi preprečevanja digitalnih prevar v okviru rešitve Trusteer in kanali brezgotovinskega plačevanja v okviru rešitve IBM Safer Payments. Z uporabo vgrajenih pravil in specifične poslovne logike Digital Content Pack omogoča bankam in drugim finančnim ustanovam, da še dodatno izboljšajo obstoječe zmožnosti zaznavanja in preprečevanja prevar.

IBM Trusteer Digital Content Pack for Retail je na voljo v paketih s po 100 upravičenimi udeleženci. IBM Trusteer Digital Content Pack for Business pa je na voljo v paketih s po 10 upravičenimi udeleženci.

Za integracijo Digital Content Pack s Pinpoint Detect in IBM Safer Payments so potrebne svetovalne storitve, ki so potrebne tudi za storitve podpore, ki se jim je treba temeljiteje posvetiti. Svetovalne storitve je mogoče pridobiti ločeno v skladu z ločenim dogovorom o obsegu del.

### 1.5.10 IBM Trusteer New Account Fraud for Retail in/ali IBM Trusteer New Account Fraud for Business

Ta storitev, ki je na voljo naročnikom na Pinpoint, je zasnovana za zaznavanje nepravilnosti, označevanje sumljivih dejavnosti in ustvarjanje opozoril že v začetku postopka ustvarjanja novega računa. Storitev nadzoruje nove račune, da lahko identificira nove dejavnosti, povezane s profiliranjem prevar po

ustvarjanju računa in profiliranjem mladih računov, in tako zagotavlja zgodnja opozorila, da je nov račun lahko račun mule ali da se uporablja za prevare, prek poročil o uporabi v aplikaciji TMA.

IBM Trusteer New Account Fraud for Retail in IBM Trusteer New Account Fraud for Business sta na voljo v paketih po 10 klicev API-ja.

#### 1.5.11 IBM Trusteer Pinpoint Verify

Naročnik mora imeti veljavno naročnino na IBM Trusteer Pinpoint Detect Premium, preden se naroči na to storitev v oblaku.

Ta storitev v oblaku zagotavlja zmožnosti, v okviru katerih se od uporabnikov zahteva dodaten način overjanja, da se preveri njihova identiteta ob dostopanju do digitalne storitve. Na voljo je za Pinpoint Detect Premium, da zagotavlja dodaten dejavnik za preverjanje pristnosti za zaščitene aplikacije. Odločitev o tem, kdaj pozvati uporabnike k preverjanju pristnosti z dodatnim dejavnikom, izvira iz zaščitene aplikacije in lahko temelji na priporočilih, ki jih vrne platforma Pinpoint Detect Premium ali katerikoli drugi pravilniki, ki jih določi zaščitena aplikacija.

### 1.6 IBM Trusteer Pinpoint Assure

Ta storitev označi sumljive dejavnosti in ustvari opozorila v postopku ustvarjanja/registriranja novega računa. Storitev nadzoruje postopek registracije računa in v poročilih o uporabi, ki so na voljo v aplikaciji TMA, določa dejavnosti, povezane z goljufijo, s čimer vnaprej opozarja, da je novi račun lahko račun mule ali se uporablja za prevare.

IBM Trusteer Pinpoint Assure je na voljo v paketih po 100 povezav.

#### 1.6.1 Dodatne storitve za IBM Trusteer Pinpoint Assure

#### 1.6.2 IBM Trusteer Pinpoint Assure Application

Razmestitev storitve IBM Trusteer Pinpoint Assure zahteva pooblastilo za IBM Trusteer Pinpoint Assure Application za vsako aplikacijo.

IBM Trusteer Pinpoint Assure je na voljo za nakup po aplikaciji.

#### 1.6.3 IBM Trusteer Mobile Carrier Intelligence in/ali IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Naročnik mora imeti veljavno naročnino na IBM Trusteer Pinpoint Assure ali IBM Trusteer Pinpoint Detect, preden se naroči na to storitev v oblaku.

Ta storitev v oblaku izboljša IBM Trusteer Pinpoint Assure in/ali IBM Trusteer Pinpoint Detect z dodatnimi informacijami in kontekstom o telefonskih številkah, ki so posredovane kateri koli od omenjenih storitev v oblaku, s tem pa pomaga določiti tveganje za prevaro dane seje. Naročnik lahko poizveduje o storitvi v oblaku, da pridobi informacije o značilnostih telefonske številke, na primer informacije o nosilcu številke.

Podatki, povezani s telefonskimi številkami (mobilno obveščanje), ki jih posreduje ta storitev v oblaku, lahko naročnik uporablja le za zasebne namene in jih lahko zadrži le trideset (30) dni. Naročnik mora poizvedeti o storitvi v oblaku v povezavi z isto telefonsko številko po določenem obdobju, da ohrani mobilno obveščanje za to številko in ne more ponovno uporabiti mobilnega obveščanja prejšnje poizvedbe. Naročnik ne sme pridobivati, razen kot je dovoljeno zgoraj, ponovno uporabiti ali delno ali v celoti uporabiti skupaj z izkopavanjem podatkov ali arhivirati podatkov mobilnega obveščanja.

### 1.7 IBM Trusteer Remotely Delivered Services

Storitve IBM Trusteer Remotely Delivered Services so na voljo kot izbirni dodatek za Pinpoint Detect Premium in Pinpoint Assure Cloud Services.

#### 1.7.1 IBM Trusteer Project Management and Consultancy Services

Ta storitev zagotavlja do 200 ur svetovalnih storitev (consultancy services), med katerimi bo IBM izvedel nekaj ali vse od spodaj naštetega:

a. Storitve začetne nastavitve: pogoste občasne sestanke, storitve upravljanja projektov

b. Policy Manager: neprekinjena podpora

Ponudba je na voljo za nakup po sodelovanju.

### 1.7.2 IBM Trusteer Security Research Consultancy Services

Ta svetovalna storitev vključuje do 200 ur virov s kupni rabi za analizo varnosti, s čimer zagotavlja dodatne storitve, definirane rešitve ter podporo Premium (kadar je primerna), ter vključuje:

a. Razširjeno raziskavo goljufij: tedenske sestanke in usposabljanja.

b. Podporo za naročnikovo izdajo z visoko prioriteto

c. Trajno preiskovanje in podporo za pravila po meri

Ponudba je na voljo za nakup po sodelovanju.

### 1.7.3 IBM Trusteer Training Services

Ta svetovalna storitev je zasnovana tako, da poleg definirane rešitve in podpore Premium (ko je ustrezno) zagotavlja še dodatne storitve in vključuje storitve usposabljanja naročnikovih zaposlenih za portfelj Trusteer.

Ponudba je na voljo za nakup po sodelovanju.

## 1.8 Storitve v oblaku IBM Trusteer Mobile

### 1.8.1 IBM Trusteer Mobile SDK for Business in/ali IBM Trusteer Mobile SDK for Retail

Storitve v oblaku IBM Trusteer Mobile SDK so zasnovane tako, da zagotavljajo dodatno plast zaščite in varen spletni dostop do naročnikovih prodajnih ali poslovnih aplikacij, za katere ima naročnik naročnino za storitve v oblaku, oceno tveganja naprav in zaščito pred lažnim predstavljanjem. Zaznavanje varne povezave Wi-Fi je na voljo samo za platforme sistema Android.

Storitve v oblaku IBM Trusteer Mobile SDK vključujejo lastniški mobilni komplet razvijalca programske opreme ("SDK"), paket programske opreme, ki vključuje dokumentacijo, lastniške knjižnice s programsko opremo za programiranje in druge povezane datoteke in elemente (z drugim imenom mobilna knjižnica IBM Trusteer) ter "komponento za izvajalno okolje" oz. "kodo za vnovično razpošiljanje", ki je lastniška programska koda, generirana s kompletom IBM Trusteer Mobile SDK, katero je mogoče vdelati ali integrirati v naročnikove zaščitene samostojne mobilne aplikacije za sistem iOS ali Android, za katere ima naročnik naročnino za storitve v oblaku ("naročniško integrirana mobilna aplikacija").

IBM Trusteer Mobile SDK for Retail je na voljo v paketih po 100 upravičenih udeležencev ali 100 odjemalskih naprav, IBM Trusteer Mobile SDK for Business pa je na voljo v paketih po 10 upravičenih udeležencev ali 10 odjemalskih naprav.

Naročnik (in neomejeno število njegovih pooblaščencev) lahko prek aplikacije TMA prejme podatke o dogodku, ki poročajo o trendih tveganj in takšna tveganja tudi ocenjujejo. Naročnik lahko prek naročniško integrirane mobilne aplikacije prejema podatke o analizi tveganj in podatke o mobilnih napravah upravičenih udeležencev, ki so prenesli naročniško integrirano mobilno aplikacijo, s čimer se naročniku omogoči oblikovanje pravilnika za preprečevanje goljufij, na podlagi katerega je mogoče uvesti ukrepe za zmanjševanje teh tveganj. "Mobilne naprave" v okviru te ponudbe vključujejo samo mobilne telefone in tablične računalnike ter ne vključujejo prenosnih računalnikov (PC/Mac).

Naročnik lahko:

a. interno uporablja IBM Trusteer Mobile SDK izključno za namene razvijanja naročniško integrirane mobilne aplikacije;

b. vdela lastniško kodo za vnovično razpošiljanje (samo v obliki objektne kode) na združen, neločljiv način v naročniško integrirano mobilno aplikacijo Vsakršen spremenjeni ali spojeni del kode za vnovično razpošiljanje v okviru določil te licence bo predmet pogojev tega opisa storitev; ter

c. trži in razpošilja lastniško kodo za vnovično razpošiljanje za prenos v mobilne naprave upravičenih udeležencev ali odjemalsko napravo imetnika računa, pod pogojem, da:

   - Razen če je izrecno dovoljeno v tej pogodbi, naročnik ne sme (1) uporabljati, kopirati, spreminjati ali razširjati kompleta SDK; (2) obratno sestaviti, obratno prevesti ali drugače prevesti ali izvesti obratni inženiring kompleta SDK, razen v obsegu, ki je zakonsko izrecno dovoljen brez možnosti pogodbene odpovedi; (3) izdajati podlicenc, izposojati ali dajati v najem kompleta SDK; (4) odstraniti nobene datoteke o avtorskih pravicah ali datoteke z obvestili, shranjene v paketu za vnovično razpošiljanje; (5) uporabiti istega imena poti kot je uporabljeno za izvorne datoteke/module za vnovično razpošiljanje; in (6) brez predhodnega pisnega soglasja IBM-a ali zadevnega dajalca licence oz. distributerja uporabiti imen ali

blagovnih znamk IBM-a, njegovih dajalcev licenc ali distributerjev v povezavi s trženjem naročniško integrirane mobilne aplikacije.

- Lastniška koda za vnovično razpošiljanje mora biti v naročniško integrirani mobilni aplikaciji integrirana na neločljiv način. Lastniška koda za vnovično razpošiljanje je lahko samo v obliki objektne kode ter mora biti v skladu z vsemi smernicami, navodili in specifikacijami v kompletu SDK in njegovi dokumentaciji. Naročnikova licenčna pogodba za končnega uporabnika za naročniško integrirano mobilno napravo mora končnega uporabnika obveščati o tem, da se lastniške kode za vnovično razpošiljanje ne sme i) uporabljati za noben drug namen kot omogočanje naročniško integrirane mobilne aplikacije, ii) kopirati (razen za namene varnostnega kopiranja), iii) nadalje razpošiljati ali prenesti, iv) obratno sestaviti, obratno prevesti ali kako drugače prevesti, razen v obsegu, ki je zakonsko izrecno dovoljen brez možnosti pogodbene odpovedi. IBM mora biti v naročnikovi licenčni pogodbi zaščiten vsaj v tolikšni meri kot z določili te pogodbe.
- Komplet SDK se sme namestiti le kot del naročnikovega notranjega razvoja in preizkušanja enot, in sicer v mobilne naprave za preizkušanje, ki jih določi naročnik. Naročnik nima pooblastila za uporabo kompleta SDK za obdelavo produkcijskih delovnih obremenitev, simulacije produkcijskih delovnih obremenitev ali preizkušanja razširljivosti katerekoli kode, aplikacije ali sistema. Naročnik ni pooblaščen za uporabo kateregakoli dela kompleta SDK za katerikoli drug namen.

Naročnik je sam izključno odgovoren za razvoj, preizkušanje in podporo naročniško integrirane mobilne aplikacije. Naročnik je odgovoren za vso tehnično podporo v zvezi z naročniško integrirano mobilno aplikacijo in vse spremembe lastniških kod za vnovično razpošiljanje, ki jih izvede naročnik, in so dovoljene s to pogodbo.

Naročnik je pooblaščen za namestitev in uporabo kod za vnovično razpošiljanje in kompleta IBM Security Mobile SDK samo za namene podpore naročnikove uporabe storitev v oblaku.

IBM ne zagotavlja, da bo vsaka aplikacija ali izhodno ustvarjanje z uporabo mobilnih orodji, vključenih v IBM Security Mobile SDK, funkcionirala, vzajemno delovala ali bo združljiva s katero koli platformo mobilnega operacijskega sistema ali mobilno napravo.

Komponente v izvorni kodi in vzorčno gradivo - IBM Security Trusteer Mobile SDK lahko vključuje nekatere komponente v obliki izvorne kode ("komponente v izvorni kodi") in drugo gradivo, označeno kot vzorčno gradivo. Naročnik lahko kopira in spreminja komponente v izvorni kodi in vzorčno gradivo samo za notranjo uporabo v skladu z omejitvami licenčnih pravic iz te pogodbe, vendar ne sme spremeniti ali izbrisati katerihkoli informacij o avtorskih pravicah ali obvestil, ki jih vsebujejo komponente v izvorni kodi ali vzorčno gradivo. IBM zagotavlja izvorno komponento in vzorčne materiale brez obveznosti podpore in "AS IS". Naročnik naj upošteva, da so komponente v izvorni kodi ali vzorčno gradivo zagotovljeni samo kot primer načina uvedbe elementov, ki jih je mogoče vdelati v naročniško integrirano mobilno aplikacijo, da komponente v izvorni kodi ali vzorčna gradiva morda ne bodo združljivi z naročnikovim razvojnim okoljem, in da je naročnik sam odgovoren za preizkušanje in uvedbo elementov, ki jih je mogoče vdelati, v svojo naročniško integrirano mobilno aplikacijo.

## 2. Vsebina in varstvo podatkov

Podatkovni list za obdelavo in varstvo podatkov (podatkovni list) podaja informacije, specifične za storitev v oblaku, glede vrste vsebine, ki jo bo mogoče obdelovati, vključenih aktivnosti obdelave, funkcij varstva podatkov in podrobnosti glede hrambe in vračila vsebine. V tem razdelku so določene podrobnosti ali pojasnila ter določbe, vključno z odgovornostmi naročnika, povezanimi z uporabo storitve v oblaku, in morebitne funkcije varstva podatkov. Glede na možnosti, ki jih je izbral naročnik, se lahko za naročnikovo uporabo storitev v oblaku uporablja več podatkovnih listov. Podatkovni list je lahko na voljo samo v angleščini, medtem ko v lokalnem jeziku ni na voljo. Navkljub morebitnim lokalnim zakonodajnim praksam ali običajem stranki soglašata, da razumeta angleščino in da je angleščina ustrezen jezik za pridobitev in uporabo storitev v oblaku. Za storitve v oblaku in možnosti, ki so na voljo, se uporablja(jo) naslednji podatkovni list(i). Naročnik potrjuje, da i) lahko IBM občasno spremeni podatkovne liste po lastni presoji in da ii) bodo takšne spremembe nadomestile predhodne različice. Namen morebitne spremembe podatkovnih listov bo i) izboljšanje ali razjasnitev obstoječih obvez, ii) ohranjanje usklajenosti s trenutno sprejetimi standardi in veljavno zakonodajo ali iii) določanje dodatnih obveznosti. Nobena sprememba podatkovnih listov ne bo bistveno poslabšala varstva podatkov storitev v oblaku.

Povezave do ustreznih podatkovnih listov:

**IBM Trusteer Mobile SDK**

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

**IBM Trusteer Mobile Secure Browser**

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

**IBM Trusteer Pinpoint Assure**

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

**IBM Trusteer Pinpoint Criminal Detect**

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

**IBM Trusteer Pinpoint Detect**

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

**IBM Trusteer Pinpoint Malware Detection**

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

**IBM Trusteer Rapport**

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

**IBM Trusteer Pinpoint Verify**

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

(Podatkovni list za IBM Cloud Identity Verify odraža IBM Trusteer Pinpoint Verify)

Naročnik mora sprejeti potrebne ukrepe za naročanje, omogočanje ali uporabo razpoložljivih funkcij za varstvo podatkov za storitev v oblaku, ter prevzema odgovornost za uporabo storitev v oblaku, če takšnih ukrepov ne sprejme, vključno z izpolnjevanjem morebitnih zahtev s področja varstva podatkov ali drugih zakonskih zahtev, povezanih z vsebino.

Velja IBM-ov dodatek o obdelavi podatkov (DPA – Data Processing Addendum), ki je na voljo na naslovu http://ibm.com/dpa, ter specifikacijski listi k DPA, ki so s sklicem vključeni v pogodbo, in sicer v obsegu, v katerem za osebne podatke, vključene v vsebino, velja Splošna uredba (EU) 2016/679 o varstvu podatkov (GDPR). Veljavni podatkovni listi za to storitev v oblaku se bodo uporabljali kot specifikacijski listi k DPA. Če velja DPA, velja IBM-ova obveznost zagotavljanja obvestila o spremembah podobdelovalcem in naročnikova pravica do ugovora takšnim spremembam, kot je določeno v DPA.

## 2.1 Pogodba EULA in podlaga za obdelavo podatkov podatkovnih subjektov

**Za storitve v oblaku IBM Trusteer Rapport (vključno z Rapport Remediation ali Rapport for Mitigation pri razmestitvi v povezavi s storitvami v oblaku Pinpoint):**

Razen če je dogovorjeno drugače in skladno s podlago za obdelovanje, ki jo je naročnik vzpostavil neodvisno, naročnik pooblašča IBM za to, da zagotovi licenčno pogodbo za končne uporabnike, ki je na voljo na spletni strani https://www.trusteer.com/support/end-user-license-agreement in ki bo IBM-u omogočila zbiranje in obdelavo podatkov, potrebnih za zagotavljanja storitev v oblaku.

## 2.2 Uporaba podatkov

IBM ne bo uporabil ali razkril rezultatov, ki izhajajo iz naročnikove uporabe storitve v oblaku in so edinstveni za naročnikovo vsebino (vpogledi) oziroma na kak drug način identificirajo naročnika. IBM pa lahko uporablja vsebino in druge informacije (razen vpogledov), ki izhajajo iz vsebine med nudenjem storitve v oblaku, pod pogojem, da so odstranjeni osebni identifikatorji, tako da osebnih podatkov ni več

mogoče pripisati določenemu posamezniku brez uporabe dodatnih informacij. IBM bo takšne podatke uporabil samo za raziskave, preizkušanje in razvoj ponudb.

## 2.3 Obdelava in shranjevanje podatkov

### 2.3.1 Dodatne informacije o lokaciji obdelave

Za storitve Trusteer Pinpoint Verify so vse lokacije gostovanja in obdelave navedene na ustreznem podatkovnem listu.

Za vse druge storitve, ki se zagotavljajo prek nemškega podatkovnega centra, bo IBM omejil obdelavo osebnih podatkov na državo IBM-ove pogodbene entitete in na naslednje države: Nemčijo, Izrael, Irsko, Nizozemsko in vse dodatne države, navedene na veljavnem podatkovnem listu za IBM-ove zunanje podobdelovalce.

Za vse druge storitve, ki se zagotavljajo prek japonskega podatkovnega centra, bo IBM omejil obdelavo osebnih podatkov na državo IBM-ove pogodbene entitete in na naslednje države: Japonsko, Izrael, Irsko in vse dodatne države, navedene na veljavnem podatkovnem listu za IBM-ove zunanje podobdelovalce.

Za vse druge storitve, ki se zagotavljajo prek ameriškega podatkovnega centra, bo IBM omejil obdelavo osebnih podatkov na državo IBM-ove pogodbene entitete in na naslednje države: ZDA, Izrael, Irsko, Singapur, Avstralijo in vse dodatne države, navedene na veljavnem podatkovnem listu za IBM-ove zunanje podobdelovalce.

Storitve podpore in vzdrževanja računa za IBM Trusteer so lahko zagotovljene tudi po potrebi in glede na razpoložljivost ustreznega IBM-ovega osebja, lokacijo naročnika in podatkovni center, ki gosti podatke.

### 2.3.2 Podatki imetnika računa

Podatki imetnika računa bodo obdelani v regiji, v kateri je imetnik računa prvotno namestil svojo odjemalsko programsko opremo. To lahko pomeni, da je vsebina imetnika računa lahko obdelana v dveh regijah, in sicer v prvotni regiji in regiji, s katero soglaša naročnik.

### 2.3.3 Integrirane rešitve

Zaradi jasnosti: ker je Trusteer Fraud Protection integrirana rešitev; če naročnik odpove eno od teh storitev v oblaku, lahko IBM ohrani naročnikove podatke za namene zagotavljanja preostalih storitev v oblaku naročniku v skladu s tem opisom storitev.

# 3. Pogodba o ravni storitev

IBM za storitev v oblaku zagotavlja naslednjo pogodbo o ravni storitev za razpoložljivost ("SLA"), kot je navedeno v dokazilu o upravičenosti. Pogodba o ravni storitev ne zagotavlja jamstva/garancije. Pogodba o ravni storitev je na voljo samo naročniku in velja samo za uporabo v produkcijskih okoljih.

## 3.1 Dobropisi za razpoložljivost

Naročnik mora pri IBM-ovi službi za tehnično podporo vložiti prijavo za podporo ravni resnosti 1, in sicer v 24 urah od trenutka, ko ugotovi, da je dogodek vplival na razpoložljivost storitve v oblaku. Naročnik mora razumno pomagati IBM-u pri diagnosticiranju in razreševanju težav.

Naročnik mora predložiti zahtevek za podporo na podlagi prijave zaradi neizpolnjevanja pogodbe o ravni storitev v treh delovnih dneh po koncu pogodbenega meseca. Nadomestilo za upravičen zahtevek na podlagi pogodbe o ravni storitev (SLA) bo priznano kot dobropis pri naslednjem računu za storitev v oblaku na podlagi seštevka minut za vsako zahtevo za povezavo s primerkom baze podatkov, ki ni uspešna v minuti ure ("nerazpoložljivost"). Nerazpoložljivost se meri od trenutka, ko je naročnik poročal o dogodku, do trenutka, ko je bilo obnovljeno delovanje storitve v oblaku, in ne vključuje časa, ki je povezan z izpadom zaradi načrtovanega ali napovedanega vzdrževanja; zaradi vzrokov, ki so zunaj IBM-ovega nadzora; zaradi težav z vsebino, tehnologijo, zasnovo ali navodili naročnika ali tretje osebe; zaradi nepodprtih sistemskih konfiguracij in platform ali zaradi drugih napak naročnika; ali zaradi varnostnega incidenta, ki ga je povzročil naročnik ali naročnikovo preizkušanje varnosti. IBM bo priznal najvišje veljavno nadomestilo na podlagi zbirne razpoložljivosti storitve v oblaku v vsakem pogodbenem mesecu, kot je prikazano v spodnji tabeli. Celotno nadomestilo za posamezni pogodbeni mesec ne sme presegati 10 odstotkov ene dvanajstine (1/12) letnih stroškov za storitev v oblaku.

## 3.2 Ravni storitev

Razpoložljivost storitve v oblaku v pogodbenem mesecu

| Razpoložljivost v pogodbenem mesecu | Nadomestilo (odstotek mesečne naročnine* za pogodbeni mesec, na katerega se nanaša zahtevek) |
|---|---|
| < 99,9 % | 2 % |
| < 99,0 % | 5 % |
| < 95,0 % | 10 % |

* Če je naročnik storitev v oblaku pridobil od IBM-ovega poslovnega partnerja, se mesečna naročnina izračuna na podlagi takrat veljavne cene za storitev v oblaku, ki velja za pogodbeni mesec, na katerega se nanaša zahtevek, pri čemer bo upoštevan 50-odstotni popust. IBM bo rabat omogočil neposredno naročniku.

Dobropisi za ravni storitve in sorodni dobropisi za nadomestilo se merijo ločeno na storitev v oblaku in na odjemalsko aplikacijo.

Pri izračunavanju dobropisov za raven storitve za storitve v oblaku na podlagi pooblastil za aplikacijo, se razpoložljivost izračuna na podlagi naslednjih smernic:

- Vsaki aplikaciji se dodeli utežen delež glede na prešteto število sej tekom pogodbenega meseca.
- Čas nerazpoložljivosti vsake storitve v oblaku na aplikacijo se akumulira ločeno za pogodbeni mesec.

V nadaljevanju je predstavljen primer izračuna za en mesec dejavnosti ter s tem povezano uteževanje. Namenjen je le ponazoritvi:

| Prodajne aplikacije | Delež skupnega št. sej v danem pogodbenem mesecu | Skupni čas nerazpoložljivosti tekom pogodbenega meseca | Utežene minute časa nerazpoložljivosti |
|---|---|---|---|
| Prodajna aplikacija A | 40 % | 300 minut | 40 % x. 300 minut = 120 minut |
| Prodajna aplikacija B | 20 % | 250 minut | 20 % x 250 minut = 50 minut |
| Prodajna aplikacija C | 40 % | 150 minut | 40 % x 150 minut = 60 |
| | | | Skupno uteženih minut časa nerazpoložljivosti = 230 |

Razpoložljivost, izražena v odstotkih, se izračuna kot: skupno število minut v pogodbenem mesecu, zmanjšano za skupno število uteženih minut nerazpoložljivosti v pogodbenem mesecu, deljeno s skupnim številom minut v pogodbenem mesecu. Vzorčni izračun na podlagi zgornjega uteženega primera je naslednji:

$$\frac{\text{Skupaj 43.200 minut v 30-dnevnem pogodbenem mesecu} - \text{230 minut uteženega časa nerazpoložljivosti} = \text{42.970 minut}}{\text{Skupaj 43.200 minut}} = \text{2-odstotni dobropis za razpoložljivost za 99,4-odstotno razpoložljivost v pogodbenem mesecu}$$

# 4. Tehnična podpora

Naročniku in njegovim upravičenim udeležencem je kot pomoč pri uporabi storitev v oblaku na voljo tehnična podpora.

Standardna podpora je vključena v naročnino za vse ponudbe. Trusteer Rapport Mandatory Service, ki je dodatek k produktu Trusteer Rapport, zahteva podporo Premium za osnovne naročnine Trusteer Rapport.

Za vsako storitev v oblaku je za dodatno plačilo na voljo naročnina na podporo Premium, z izjemo **storitev v oblaku IBM Trusteer Mobile SDK** in **storitev v oblaku IBM Trusteer Rapport Mandatory Service**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital**

**Content Pack** in **IBM Trusteer Mobile Carrier Intelligence**. Obrnite se na IBM-ovega prodajnega predstavnika ali IBM-ovega poslovnega partnerja.

**Standardna podpora:**

- Podpora od 8.00 do 17.00 po lokalnem času.
- Naročniki in njihovi upravičeni udeleženci lahko vložijo elektronske prijave za podporo, kot je podrobno navedeno v vodiču po IBM-ovi programski opremi kot storitvi, ki je na voljo na spletni strani https://www.ibm.com/software/support/saas_support_guide.html.
- Naročniki lahko dostopajo do portala za podporo naročnikom, na katerem so na voljo obvestila, dokumenti, poročila o primerih in pogosta vprašanj, na spletni strani http://www-01.ibm.com/software/security/trusteer.

**Podpora Premium:**

- Neprekinjena podpora za vse ravni resnosti.
- Naročniki se lahko obrnejo na podporo neposredno po telefonu ali z zahtevo po povratnem klicu.
- Naročniki in njihovi upravičeni udeleženci lahko vložijo elektronske prijave za podporo, kot je podrobno navedeno v priročniku za podporo programske opreme kot storitve [SaaS].
- Naročniki lahko dostopajo do portala za podporo naročnikov, na katerem so na voljo obvestila, dokumenti, poročila o primerih in pogosta vprašanja na spletni strani http://www.ibm.com/software/security/trusteer/support/.
- Za možnosti podpore in podrobnosti si oglejte vodič po IBM-ovi programski opremi kot storitvi, ki je na voljo na spletni strani https://www.ibm.com/software/support/saas_support_guide.html.

# 5. Pooblastila in zaračunavanje

## 5.1 Metrike zaračunavanja

Storitve v oblaku so na voljo na podlagi naslednje metrike zaračunavanja, ki je določena v transakcijskem dokumentu:

- Sodelovanje je merska enota, na podlagi katere je mogoče pridobiti storitve. Sodelovanje sestavljajo strokovne storitve in/ali storitve usposabljanja, povezane s storitvami v oblaku. Naročnik mora pridobiti zadostno število pooblastil za pokritje vseh sodelovanj.
- Upravičeni udeleženec je merska enota, na podlagi katere je mogoče pridobiti storitev v oblaku. Upravičeni udeleženec je vsak posameznik ali subjekt, ki lahko sodeluje v kateremkoli programu za dobavo storitev, ki ga upravlja ali mu sledi storitev v oblaku. Naročnik mora pridobiti zadostna pooblastila za kritje vseh upravičenih udeležencev, ki jih upravlja ali sledi storitev v oblaku med meritvenim obdobjem, navedenim v naročnikovem transakcijskem dokumentu.

  Vsak program za dobavo storitev, ki ga upravlja storitev v oblaku, se analizira ločeno in nato prišteje k drugim. Posamezniki ali subjekti, ki lahko uporabljajo več programov za dobavo storitev, morajo pridobiti ločena pooblastila.

  Za namene pooblaščanja v okviru teh storitev v oblaku je upravičeni udeleženec naročnikov končni uporabnik, ki ima unikatne prijavne poverilnice za naročnikovo poslovno ali prodajno aplikacijo.
- Odjemalska naprava je merska enota, na podlagi katere je mogoče pridobiti storitev v oblaku. Odjemalska naprava je posamezna uporabniška računalniška naprava ali senzorska ali telemetrična naprava s posebnim namenom, ki zahteva izvajanje ali prejme v izvajanje niz ukazov, procedur ali aplikacij iz drugega računalniškega sistema ali ki posreduje podatke v drug računalniški sistem, ki ga običajno imenujemo strežnik ali ga kako drugače upravlja strežnik. Več odjemalskih naprav lahko souporablja dostop do skupnega strežnika. Odjemalska naprava ima lahko zmožnosti za obdelavo ali jo je mogoče programirati tako, da uporabniku omogoča opravljanje dela. Naročnik mora pridobiti pooblastilo za vsako odjemalsko napravo, ki izvaja storitev v oblaku, ji posreduje podatke, uporablja njene storitve ali do nje kako drugače dostopa med meritvenim obdobjem, navedenim v naročnikovem transakcijskem dokumentu.
- Aplikacija je merska enota, na podlagi katere je mogoče pridobiti storitev v oblaku. Aplikacija je unikatno določen program programske opreme. Naročnik mora pridobiti zadostna pooblastila za vsako aplikacijo, do katere je mogoče dostopati in jo uporabljati v meritvenem obdobju, navedenem v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.

Za namene te storitve v oblaku je aplikacija ena poslovna ali prodajna aplikacija naročnika.

- Klic API-ja je merska enota, na podlagi katere je mogoče pridobiti storitve v oblaku. Klic API-ja je priklic storitve v oblaku prek programirljivega vmesnika. Naročnik mora pridobiti zadostna pooblastila, da z njimi pokrije skupno število klicev API-ja, zaokroženo na najbližjo desetico, med meritvenim obdobjem, navedenim v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.
- Povezava je merska enota, na podlagi katere je mogoče pridobiti storitev v oblaku. Povezava je povezava ali povezanost baze podatkov, aplikacije, strežnika ali katerekoli druge vrste naprave s storitvijo v oblaku. Naročnik mora pridobiti zadostna pooblastila, da z njimi pokrije skupno število povezav, ki so bile vzpostavljene ali so vzpostavljene s storitvijo v oblaku med meritvenim obdobjem, navedenim v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.

  Za namene te storitve v oblaku je povezava seja ali potek v naročnikovi aplikaciji.

### 5.2 Zaračunavanje presežkov

Če naročnikova dejanska uporaba storitev v oblaku med meritvenim obdobjem presega pooblastila, navedena v dokazilu o upravičenosti, bo v naslednjem mesecu zaračunan presežek po ceni, navedeni v transakcijskem dokumentu.

### 5.3 Pogostost zaračunavanja

IBM bo na podlagi izbrane pogostosti obračunavanja naročniku izdajal račune za zapadle obveznosti na začetku posameznega obračunskega obdobja, z izjemo stroškov za presežke in vrste uporabe, ki se zaračunavajo za nazaj.

## 6. Obdobje trajanja in možnosti podaljšanja

Obdobje trajanja storitev v oblaku se začne z dnem, ko IBM naročnika obvesti, da ima dostop do storitev v oblaku, navedenih v dokazilu o upravičenosti. V dokazilu o upravičenosti bo navedeno, ali se storitve v oblaku podaljšajo samodejno, se nadaljujejo na podlagi neprekinjene uporabe ali se končajo ob izteku naročniškega obdobja.

Na podlagi samodejnega podaljšanja se bo naročnina na storitve v oblaku samodejno podaljševala v okviru naročniškega obdobja, navedenega v dokazilu o upravičenosti, razen če naročnik posreduje pisno obvestilo o prenehanju podaljšanja najmanj 90 dni pred iztekom naročniškega obdobja. V primeru podaljšanja se cene letno povišajo v skladu z določili ponudbe. Če do samodejnega podaljšanja naročnine pride po IBM-ovem prejemu obvestila o odpovedi storitve v oblaku, bo obdobje podaljšanja končano ob koncu trenutnega obdobja podaljšanja ali na datum napovedanega odstopa, karkoli je prej.

Na podlagi neprekinjene uporabe bodo storitve v oblaku neprestano na voljo iz meseca v mesec, dokler naročnik ne posreduje pisnega obvestila o odpovedi z 90-dnevnim odpovednim rokom. Po izteku takega 90-dnevnega roka bo storitev v oblaku na voljo še do konca koledarskega meseca.

## 7. Dodatna določila

### 7.1 Splošno

Naročnik soglaša, da ga lahko IBM v javnih ali tržnih komunikacijah imenuje kot naročnika storitev v oblaku.

Naročnik ne sme uporabiti storitev v oblaku, niti samostojno niti v kombinaciji z drugimi storitvami ali produkti, za podporo katere koli od naslednjih dejavnosti z visokim tveganjem: načrtovanje, izgradnja, nadzor ali vzdrževanje jedrskih objektov, sistemov za množični transport, nadzornih sistemov za zračni promet, avtomobilskih nadzornih sistemov, oborožitvenih sistemov ali navigacije oziroma komunikacije za zračna plovila ali katerih koli drugih dejavnosti, pri katerih bi lahko odpoved storitve privedla do resne nevarnosti za smrt ali hude telesne poškodbe.

### 7.2 Podporna programska oprema

Storitve v oblaku zahtevajo uporabo podporne programske opreme, ki jo naročnik prenese v svoje sisteme, da omogoči uporabo storitev v oblaku. Naročnik lahko podporno programsko opremo uporablja samo v povezavi z uporabo storitve v oblaku. Podporna programska oprema je zagotovljena "TAKŠNA, KOT JE".

## 7.3 Razmestitev produkta IBM Trusteer Fraud Protection

Za vsako aplikacijo, na katero se naročnik naroči, osnovna naročnina vključuje potrebna dejanja nastavitve in začetne razmestitve v oblak IBM Trusteer, vključno z začetnim enkratnim zagonom, konfiguracijo, pozdravno predlogo, preizkušanjem in usposabljanjem.

Dejanja razmestitve ne vključujejo dejanj uvedbe, ki so potrebna pri naročnikovih aplikacijah ali sistemih.

Faza uvedbe različnih storitev v oblaku je zasnovana za uvedbo znotraj časovnih okvirov, kot je opisano v ustreznih vodičih o razmestitvi.

Dokončanje teh faz uvedbe v dodeljenem časovnem okviru je odvisno od polne zavezanosti in sodelovanja naročnikovega vodstva in osebja. Naročnik mora pravočasno zagotoviti zahtevane podatke. IBM-ova učinkovitost temelji na naročnikovih pravočasnih informacijah in odločitvah, morebitne zamude pa lahko povzročijo dodatne stroške in/ali zamudo pri dokončanju teh storitev uvedbe.

Za vsako aplikacijo, na katero se naročnik naroči, osnovna naročnina vključuje potrebna dejanja nastavitve in začetne razmestitve v oblak IBM Trusteer, vključno z začetnim enkratnim zagonom, konfiguracijo, pozdravno predlogo, preizkušanjem in usposabljanjem.

Naročnikova naročnina vključuje podporo in preizkušanje strani v naročnikovih aplikacijah, ki jih bo IBM pri začetni razmestitvi označil kot priporočljive. IBM ni odgovoren za: (i) delno razmestitev, (ii) naročnikovo izbiro, da ne bo razmestil IBM-ovih storitev tako, kot priporoča IBM, ali (ii) naročnikovo izbiro, da bo razmestitev, nastavitev in preizkušanje izvedel sam, (iv) delno razmestitev ali rezultate zaščite zaradi neustreznih informacij naročnika. Za dodatne storitve, vključno z dodatnimi razmestitvami poleg začetne razmestitve, se lahko sklene ločena pogodba, ki zajema dodatne stroške.