IBM Trusteer Pinpoint Detect

Ta opis storitve opisuje storitev v oblaku. Ustrezni dokumenti o naročilu nudijo cene in dodatne podrobnosti o naročnikovem naročilu.

1. Storitev v oblaku

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.

Ta storitev v oblaku vključuje naslednje:

a. Trusteer Management Application (TMA) in Trustboard:

   TMA je tradicionalna aplikacija upravljanja družbe Trusteer, ki naročnikom omogoča ocenjevanje in klasificiranje opozoril. Trustboard je novejša aplikacija upravljanja, ki se primarno uporablja za raziskovanje. Naročniki se lahko kadar koli odločijo, ali bodo uporabljali TMA ali Trustboard. Aplikaciji TMA in Trustboard sta obe na voljo v okolju IBM Trusteer, ki gostuje v oblaku in prek katerega lahko naročnik (in neomejeno število članov njegovega pooblaščenega osebja): (i) pregleduje in prenaša nekatera poročila o podatkih dogodkov in ocene tveganja ter (ii) pregleduje, naroča in konfigurira dostavo virov o grožnjah, izdelanih iz ponudb Pinpoint. IBM Trusteer Pinpoint Detect in IBM Trusteer Pinpoint Verify se uporabljata kot del prijave v TMA in Trustboard.

b. Spletni skript in/ali API-ji:

   Za razmestitev na spletnem mestu za namene dostopanja do, preizkušanja ali uporabljanja storitve v oblaku.

"Seja" je interakcija med naročnikovo aplikacijo (spletno ali mobilno) in storitvijo v oblaku, ki generira eno ali več ocen tveganja v realnem času. Seja se meri od časa začetka interakcije do konca interakcije. Konec interakcije se zabeleži, ko se zgodi eden od naslednjih dogodkov:

- Interakcija se ponastavi na običajen način z odjavo iz aplikacije.
- Brskalnik, aplikacija ali zavihek se zapre.
- Piškotki so izbrisani.
- Časovna omejitev.

Seja lahko vključuje poljubno število dejavnosti, kot so: prijava, brskanje, odjava, nastavitev plačila in druge dejavnosti, kot jih določi naročnikova aplikacija. V pojasnilo je za namene te storitve v oblaku ena povezava (kot je definirano spodaj) tudi ena seja.

1.1 Ponudbe

Naročnik lahko izbira med naslednjimi razpoložljivimi ponudbami.

1.1.1 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. Ta storitev se lahko uporablja tudi za oddaljeni dostop delovne sile za namene ocenjevanja tveganja in upravljanih ali neupravljanih naprav.

V to storitev v oblaku je vključena najvišja stopnja podpore (kot je definirano v spodnjem odseku "Tehnična podpora").

Storitev je mogoče kupiti v paketih 100 upravičenih udeležencev ali v paketih 100 povezav.

1.1.2 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.

1.1.3 IBM Trusteer Pinpoint Detect for Connections

Ta storitev v oblaku zagotavlja zaščito, zaznava poskuse zlorabe računov in naročniku posreduje ocene tveganja/zaupanja brskalnikov in/ali mobilnih naprav (prek izvirnega brskalnika naročnikove mobilne aplikacije), ki dostopajo do poslovne ali prodajne aplikacije. Rešitev uporablja različne indikatorje tveganja, s katerimi analizira napravo, povezavo in vedenje končnega uporabnika ter jih primerja z zgodovino uporabnika, da bi odkrila sumljivo uporabo.

Storitev v oblaku lahko uporablja povezave iz mobilnih in spletnih kanalov. IBM Trusteer Pinpoint Detect zajema pooblastilo za IBM Trusteer Mobile SDK, če je ustrezno.

Storitev v oblaku je mogoče kupiti v paketih po 100 povezav na leto.

1.2 Izbirne storitve

Za storitve v oblaku iz tega razdelka je predpogoj pooblastilo za IBM Trusteer Pinpoint Detect Premium, IBM Trusteer Pinpoint Detect Standard ali IBM Trusteer Pinpoint for Connections.

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

Odjemalska aplikacija se nanaša na spletno in/ali mobilno aplikacijo. Spletna aplikacija zajema skupino vseh funkcij, ki so ponujene upravičenim udeležencem naročnika prek več spletnih strani, z zaslona za prijavo ali identifikacijo, v konzoli Trusteer (Trusteer Management Application) pa se nadzira kot ena aplikacija. Mobilna aplikacija zajema skupino vseh funkcij, ki so ponujene upravičenim udeležencem naročnika prek enega programa, ki ga je mogoče prenesti iz trgovine z aplikacijami (trgovina), z zaslona za prijavo ali identifikacijo, v konzoli Trusteer (Trusteer Management Application) pa se nadzira kot ena aplikacija.

Integracija aplikacije IBM Trusteer Pinpoint za vsako aplikacijo zahteva pooblastilo za IBM Trusteer Pinpoint Application.

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

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

Odjemalska aplikacija se nanaša na spletno in/ali mobilno aplikacijo. Spletna aplikacija zajema skupino vseh funkcij, ki so ponujene upravičenim udeležencem naročnika prek več spletnih strani, z zaslona za prijavo ali identifikacijo, v konzoli Trusteer (Trusteer Management Application) pa se nadzira kot ena aplikacija. Mobilna aplikacija zajema skupino vseh funkcij, ki so ponujene upravičenim udeležencem naročnika prek enega programa, ki ga je mogoče prenesti iz trgovine z aplikacijami (trgovina), z zaslona za prijavo ali identifikacijo, v konzoli Trusteer (Trusteer Management Application) pa se nadzira kot ena aplikacija.

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 Premium zahteva pooblastilo za IBM Trusteer Pinpoint Detect Premium Application za vsako aplikacijo.

1.2.3 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.

1.2.4 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.

1.2.5 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).

1.2.6 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.

Zaznavanje finančnih brskalnikov, okuženih z zlonamerno programsko opremo (Man-in-the-Browser – MitB) pri povezovanju s poslovno ali prodajno aplikacijo brez sodelovanja naročnika. 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.

1.2.7 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.

1.2.8 IBM Trusteer Pinpoint Criminal Detection for Business in/ali IBM Trusteer Pinpoint Criminal Detection for Retail

Brez-odjemalsko zaznavanje sumljive dejavnosti zlorabe računa v brskalniku pri povezovanju s poslovno ali prodajno aplikacijo na podlagi ID-ja naprave, zaznavanja lažnega predstavljanja in zaznavanja kraje

poverilnic, ki jo omogoča zlonamerna programska oprema. Storitve v oblaku IBM Trusteer Pinpoint Criminal Detection 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.

a. Podatki o dogodkih:

   Naročniki se lahko kadar koli odločijo, ali bodo uporabljali TMA ali Trustboard. 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, za katere je naročnik naročil kritje storitev v oblaku, lahko pa naročnik podatke o dogodkih prejema prek načina dostave z ozadnim API-jem.

1.2.9 IBM Trusteer Pinpoint Criminal Detection II for Business in/ali IBM Trusteer Pinpoint Criminal Detection II for Retail

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

Brez-odjemalsko zaznavanje sumljive dejavnosti zlorabe računa v brskalniku pri povezovanju s poslovno ali prodajno aplikacijo na podlagi ID-ja naprave, zaznavanja lažnega predstavljanja in zaznavanja kraje poverilnic, ki jo omogoča zlonamerna programska oprema. Storitve v oblaku IBM Trusteer Pinpoint Criminal Detection II 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.

a. Podatki o dogodkih:

   Naročniki se lahko kadar koli odločijo, ali bodo uporabljali TMA ali Trustboard. Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporablja aplikacijo TMA ali Trustboard za prejemanje podatkov o dogodkih, ustvarjenih na podlagi spletnih interakcij upravičenih udeležencev z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami, za katere je naročnik naročil kritje storitev v oblaku, lahko pa naročnik podatke o dogodkih prejema prek načina dostave z ozadnim API-jem.

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

1.2.10 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 ponudbo te 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. Za namen tega opisa storitve imetnik računa – pomeni končnega uporabnika naročnika, ki je namestil programsko opremo, ki omogoča odjemalca, sprejel licenčno pogodbo s končnim uporabnikom ("EULA") in se je vsaj enkrat overil v naročnikovi prodajni ali poslovni aplikaciji, za katero ima naročnik naročnino za pokritje storitev v oblaku. Odjemalska programska oprema imetnika računa – pomeni programsko opremo IBM Trusteer Rapport, ki omogoča odjemalca, ali katerokoli drugo programsko opremo, ki omogoča odjemalca in ki je priložena nekaterim storitvam v oblaku za namestitev na napravi končnega uporabnika.

1.2.11 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.

1.2.12 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 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 Trusteer 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.

1.2.13 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail in/ali IBM Trusteer Pinpoint Detect Standard Additional Applications for Business

- 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.

1.2.14 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 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.

1.2.15 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.

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Pred naročilom te storitve v oblaku mora imeti naročnik veljavno naročnino na IBM Trusteer Pinpoint Detect.

Ta storitev v oblaku izboljša storitev IBM Trusteer Pinpoint Detect tako, da zagotovi dodatne informacije in kontekst glede mobilnih številk, ki so bile posredovane kateri koli od teh storitev v oblaku, in pomaga določiti tveganje za prevaro pri dani seji. 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.

1.3 Pospeševalne storitve

1.3.1 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".

1.3.2 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".

IBM Trusteer Pinpoint Malware Detection Additional Applications za IBM Trusteer Pinpoint Malware Detection II Standard Edition ali IBM Trusteer Pinpoint Malware Detection II Advanced Edition; za

razmestitev v katero koli dodatno aplikacijo poleg prve aplikacije je potrebno pooblastilo za IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.3.3 IBM Trusteer Pinpoint Criminal Detection Redeployment

Naročniki, ki želijo ponovno razmestiti aplikacije za spletno bančništvo med obdobjem storitve, kar posledično zahteva spremembe pri razmestitvi storitve IBM Trusteer Pinpoint Criminal Detection Cloud Service, naj kupijo IBM Trusteer Pinpoint Criminal 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".

2. Podatkovni listi za obdelavo in varstvo podatkov

IBM-ov dodatek k obdelavi podatkov http://ibm.com/dpa (DPA) in podatkovni list za obdelavo in varstvo podatkov (podatkovni list) podajata dodatne informacije o varstvu podatkov za storitve v oblaku in možnosti v zvezi z vrstami vsebine, ki se lahko obdeluje, vključene dejavnosti obdelave, funkcije varstva podatkov in podrobnosti glede hrambe in vračila vsebine. DPA velja za osebne podatke, ki jih zajema vsebina, če in v obsegu, v katerem veljajo i) Splošna uredba EU o varstvu podatkov (EU/2016/679) (GDPR); ali ii) drugi zakoni o varstvu podatkov, navedeni na spletni strani http://ibm.com/dpa/dpl.

Pojasnjeno je, da podatkovni listi na splošno navajajo vse lokacije, na katerih IBM (vključno z morebitnimi zunanjimi podobdelovalci) gosti in obdeluje osebne podatke, ne glede na podatkovni center, iz katerega se storitve razmeščajo. Za seznam lokacij, ki izvajajo gostovanje in obdelavo ter so značilne za podatkovni center, iz katerega se razmeščajo storitve, glejte spodnji razdelek 5.2 (Dodatne informacije o lokaciji obdelave).

IBM Trusteer Pinpoint Criminal Detect

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

IBM Trusteer Pinpoint Detect

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

IBM Trusteer Pinpoint Malware Detection

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

IBM Trusteer Mobile SDK

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

3. Ravni storitve in tehnična podpora

3.1 Pogodba o ravni storitev

IBM naročniku zagotavlja naslednjo pogodbo o ravni storitev za razpoložljivost (SLA). IBM bo priznal najvišje veljavno nadomestilo na podlagi zbirne razpoložljivosti storitve v oblaku, kot je prikazano v spodnji tabeli. Razpoložljivost, izražena v odstotkih, se izračuna kot skupno število minut v pogodbenem mesecu, zmanjšano za skupno število minut nerazpoložljivosti v pogodbenem mesecu, deljeno s skupnim številom minut v pogodbenem mesecu. Definicija nerazpoložljivosti storitve, postopek pritožbe in kako kontaktirati IBM v zvezi z razpoložljivostjo storitve, so v IBM-ovem pregledu podpore za storitev v oblaku na naslovu https://www.ibm.com/software/support/saas_support_overview.html.

Razpoložljivost	Dobropis (% mesečne naročnine*)
Manj kot 99,9 %	2 %
Manj kot 99,0 %	5 %
Manj kot 95,0 %	10 %

* Naročnina je pogodbena cena za mesec, na katerega se nanaša zahtevek.

3.2 Tehnična podpora

Tehnično podporo za storitev v oblaku, vključno s kontaktnimi podatki podpore, stopnjami resnosti, časom razpoložljivosti podpore, odzivnim časom in drugimi informacijami ter procesi naročnik najde tako, da izbere storitev v oblaku v storitvi IBM Support, ki je na voljo na https://www.ibm.com/support/home/pages/support-guide/.

Podpora Premium:

Za dodatno plačilo je za storitev v oblaku na voljo naročnina na podporo Premium, ki zajema naslednje:

- 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/.

4. Stroški

4.1 Metrike zaračunavanja

Metrike zaračunavanja za storitev v oblaku so podane v transakcijskem dokumentu.

Za to storitev v oblaku se uporabljajo naslednje metrike zaračunavanja:

- Engagement je profesionalna ali izobraževalna storitev, povezana s storitvijo v oblaku.
- Upravičeni udeleženec je posameznik ali subjekt, upravičen do sodelovanja v katerem koli programu za dobavo storitev, ki ga upravljajo ali mu sledijo storitve v oblaku.
- Aplikacija je unikatno določen program programske opreme, razvite prek storitve v oblaku ali do katere lahko dostopajo ali jo uporabljajo storitve v oblaku.
- Klic API-ja je poziv storitve v oblaku prek vmesnika, ki se lahko programira.
- Povezava je povezava ali povezanost baze podatkov, aplikacije, strežnika ali katerekoli druge vrste naprave, so bile ali so na voljo storitvam v oblaku.

4.2 Stroški oddaljenih storitev

Oddaljena storitev bo potekla 90 dni po dnevu nakupa, ne glede na to, ali je bila porabljena.

5. Dodatna določila

Za pogodbe o storitvi v oblaku (ali enakovredne osnovne pogodbe), podpisane pred 1. januarjem 2019, veljajo pogoji, ki so na voljo na https://www.ibm.com/acs.

5.1 Pogodba EULA in podlaga za obdelavo podatkov podatkovnih subjektov

Za storitve v oblaku IBM Trusteer Rapport (vključno s storitvijo Rapport Remediation ali Rapport for Mitigation, kadar je razmeščena v povezavi s storitvami v oblaku Pinpoint): če ni dogovorjeno drugače in v skladu s podlago za obdelavo, ki jo je naročnik uredil ločeno, naročnik pooblašča IBM, da zagotovi licenčno pogodbo za končnega porabnika, ki je na voljo na spletni strani https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA, s čimer IBM-u omogoči zbiranje in obdelavo informacij, potrebnih za zagotavljanje storitev v oblaku.

Za storitve v oblaku IBM Trusteer Rapport naročnik pooblašča IBM, kot obdelovalca podatkov sponzorskega podjetja, za uporabo programa za zbiranje zlonamerne programske opreme in artefaktov zlonamerne programske opreme, t.j. datotek, povezanih z zlonamerno dejavnostjo, ali datotek, povezanih z neobičajnimi napakami programa. IBM programa ne uporablja za ciljanje na datoteke z osebnimi podatki končnega uporabnika; vendar pa se lahko zgodi, da zbrane datoteke vsebujejo osebne podatke, ki jih je brez dovoljenja končnega uporabnika pridobila zlonamerna programska oprema. IBM bo 1) takoj izbrisal vse datoteke, ki niso pomembne za tako analizo, in 2) ohranil ustrezne datoteke samo za obdobje trajanja analize in nikakor za obdobje, daljše od treh mesecev.

5.2 Dodatne informacije o lokaciji obdelave

Vso gostovanje in obdelovanje osebnih podatkov, vključno tistim, ki ga izvajajo morebitni zunanji podobdelovalci, identificirani na podatkovnem listu, se bo izvajalo na spodaj navedenih lokacijah:

Za vse storitve, ki se zagotavljajo prek podatkovnega centra v Nemčiji, bo IBM omejil gostovanje in obdelavo osebnih podatkov na državo IBM-ovega pogodbenega subjekta ter na naslednje države: Nemčija, Izrael, Irska in Nizozemska.

Za vse storitve, ki se zagotavljajo prek podatkovnega centra na Japonskem, bo IBM omejil gostovanje in obdelavo osebnih podatkov na državo IBM-ovega pogodbenega subjekta ter na naslednje države: Japonska, Izrael in Irska.

Za vse storitve, ki se zagotavljajo prek podatkovnega centra v ZDA, bo IBM omejil gostovanje in obdelavo osebnih podatkov na državo IBM-ovega pogodbenega subjekta ter na naslednje države: ZDA, Izrael, Irska, Singapur in Avstralija.

Dodatno k zgoraj navedenim lokacijam lahko za vse storitve, ki se zagotavljajo prek podatkovnih centrov v Nemčiji, na Japonskem in v ZDA, (1) Salesforce.Com, kot IBM-ov zunanji podobdelovalec, gosti ali obdeluje podporne podatke v Nemčiji in Franciji ter (2) za naročnike, ki izberejo pošiljanje podatkov ponudnikov storitve Mobile Carrier Intelligence, se lahko osebni podatki gostijo in obdelujejo v državah ustreznih zunanjih podobdelovalcev, kot je navedeno na podatkovnem listu. Ne glede na kakršne koli morebitne nasprotujoče podatke na podatkovnem listu, zunanji podobdelovalci, navedeni v členu (2) prejšnjega stavka, morda niso skladni z ISO 27001 ali SOC2.

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.

5.3 Podatki imetnika računa

Za večjo jasnost: če je z odjemalsko programsko opremo določenega imetnika računa povezana več kot ena IBM-ova stranka (kot so IBM-ove stranke, "povezane stranke") in IBM storitve v skladu s tem opisom storitve zagotavlja takim povezanim strankam prek podatkovnih centrov v različnih regijah, potem se lahko podatki imetnika računa obdelujejo na kateri koli in na vseh lokacijah, povezanih z vsakim takim podatkovnim centrom, kot je navedeno v razdelku 5.2 zgoraj.

5.4 Integrirane rešitve

Za večjo jasnost: različne ponudbe v okviru blagovne znamke Trusteer lahko predstavljajo integrirano rešitev. Zato velja naslednje: če naročnik odpove katero koli od teh storitev v oblaku, lahko IBM obdrži naročnikove podatke, da lahko naročniku zagotavlja preostale storitve v oblaku iz tega opisa storitve ter tudi druge storitve Trusteer v skladu z opisi storitev, ki veljajo za take druge storitve Trusteer.

5.5 Podporna programska oprema

Storitev v oblaku vsebuje naslednjo podporno programsko opremo:

- IBM Rapport Agents

5.6 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).

5.7 Podatki, zbrani kot del razmestitve

Razmestitev storitve v oblaku lahko zajema posredovanje določenih naročnikovih podatkov IBM-u. Taki podatki ne smejo vključevati informacij, ki lahko identificirajo določene posameznike ali jim jih je mogoče pripisati. Dodatne smernice glede podatkov, ki se posredujejo IBM-u kot del razmestitve, so vključene v smernice za razmestitev storitve Trusteer, ki se zagotovijo naročniku.

6. Prevladujoče določbe

6.1 Uporaba podatkov

Naslednje prevlada pri morebitnih nasprotnih določbah v razdelku o vsebini in varstvu podatkov osnovnih pogojev za storitev v oblaku med pogodbenima strankama: 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 bo vsebino in druge informacije, ki izhajajo iz vsebine (razen za vpoglede), uporabil kot del storitve v oblaku za namen izboljšanja storitve v oblaku. Prav tako lahko IBM deli identifikatorje groženj in druge varnostne podatke, vdelane v vsebino, za namene zaznavanja groženj in varovanja.