IBM Podmínky užívání – Podmínky specifické pro nabídku IBM SaaS

IBM Security Trusteer Fraud Protection

Podmínky užívání ("ToU") sestávají z těchto dokumentů IBM: Podmínek užívání – Podmínek specifických pro nabídku IBM SaaS ("Podmínky specifické pro nabídku IBM SaaS") a z dokumentu nazvaného IBM podmínky užívání – Všeobecné podmínky ("Všeobecné podmínky"), které jsou dostupné na této adrese URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

V případě rozporu mají Podmínky specifické pro nabídku IBM SaaS přednost před Všeobecnými podmínkami. Objednáním, přístupem nebo užíváním IBM SaaS vyjadřuje Zákazník IBM SaaS svůj souhlas s těmito Podmínkami užívání.

Podmínky užívání se řídí podmínkami Mezinárodní smlouvy IBM Passport Advantage, Mezinárodní smlouvy IBM Passport Advantage Express nebo Mezinárodní smlouvy IBM pro vybrané nabídky IBM SaaS, podle toho, co je relevantní ("Smlouva"), a spolu s Podmínkami užívání tvoří úplnou smlouvu.

1. IBM SaaS

Tyto Podmínky specifické pro nabídku IBM SaaS se vztahují na následující nabídky IBM SaaS:

1.1 Nabídky Rapport IBM SaaS

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

1.2 Nabídky Pinpoint IBM SaaS

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

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

1.3 Nabídky Mobile IBM SaaS

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

2. Metriky poplatků

IBM SaaS je prodávána na základě níže uvedených metrik poplatků, jak je uvedeno v Transakčním dokumentu:

a. **Vybraný účastník** – je měrnou jednotkou, na jejímž základě lze získat IBM SaaS. Vybraným účastníkem je každá fyzická nebo právnická osoba, která je způsobilá k účasti v jakémkoli programu poskytování služeb spravovaném nebo sledovaném prostřednictvím IBM SaaS. Je nutno získat dostatečný počet oprávnění, který bude pokrývat všechny Vybrané účastníky spravované nebo sledované v rámci IBM SaaS během období měření specifikovaného v Zákazníkově Transakčním dokumentu.

   Všechny programy poskytování služeb spravované IBM SaaS jsou analyzovány samostatně a následně sloučeny. Fyzické nebo právnické osoby, které jsou oprávněny využívat více programů poskytování služeb, vyžadují samostatné nároky.

   V případě těchto nabídek program poskytování služeb zahrnuje jednu Obchodní nebo Maloobchodní aplikaci Zákazníka s hlavní přihlašovací stránkou a souvisejícími stránkami pro každou takovou aplikaci. Vybraný účastník je koncový uživatel Zákazníka s přihlašovacími pověřeními k Obchodní nebo Maloobchodní aplikaci.

b. **Zařízení Zákazníka** – je měrnou jednotkou, na jejímž základě lze získat IBM SaaS. Zařízení Zákazníka je výpočetní zařízení pro jednoho uživatele nebo senzor či telemetrické zařízení sloužící ke speciálnímu účelu, které vyžaduje spuštění nebo přijímá pro spuštění sadu příkazů, postupů nebo aplikací z jiného počítačového systému nebo poskytuje data do jiného počítačového systému, který je typicky označován jako server nebo je jinak řízen serverem. Více Zařízení Zákazníka může sdílet přístup ke společnému serveru. Zařízení Zákazníka může mít určité funkce pro zpracování nebo může být naprogramováno tak, aby umožnilo uživateli pracovat. Pro každé Zařízení Zákazníka, které používá, kterému poskytuje data a jehož služby využívá nebo s jehož využitím přistupuje ke službě IBM SaaS během období měření určeného v Transakčním dokumentu, musí Zákazník získat oprávnění.

3. Poplatky a fakturace

Výše platby za IBM SaaS je specifikována v Transakčním dokumentu.

3.1 Poplatky za neúplný měsíc

Poplatek za neúplný měsíc uvedený v Transakčním dokumentu může být posouzen na poměrném základě.

4. Dodržování předpisů a audity

Přístup k nabídkám IBM Security Trusteer Fraud Protection podléhá maximálnímu množství Vybraných účastníků nebo Zařízení Zákazníka určenému v Transakčním dokumentu. Zákazník nese odpovědnost za zajištění, že jeho počet Vybraných účastníků nebo Zařízení Zákazníka nepřekročí maximální množství uvedené v Objednávce.

Za účelem ověření dodržení maximálního počtu Vybraných účastníků nebo Zařízení Zákazníka lze vykonat audit.

5. Volby prodloužení Období registrace IBM SaaS

Transakční dokument Zákazníka stanoví, zda se IBM SaaS obnoví na konci období registrace, a to určením jedné z následujících možností:

5.1 Automatické prodloužení

Jestliže je v Zákazníkově Transakčním dokumentu uvedeno automatické prodloužení, je Zákazník oprávněn vypovědět končící Období registrace IBM SaaS prostřednictvím písemné žádosti zaslané obchodnímu zástupci IBM nebo Obchodnímu partnerovi IBM Zákazníka, a to přinejmenším devadesát (90) dní před datem uplynutí smluvního období, které je uvedeno v Transakčním dokumentu. Neobdrží-li IBM nebo její Obchodní partner IBM takové oznámení o ukončení do data uplynutí smluvního období, bude končící období registrace automaticky prodlouženo buď o jeden rok, nebo o období rovnající se původnímu období registrace uvedenému v Transakčním dokumentu.

5.2 Pokračující fakturace

Je-li v Zákazníkově Transakčním dokumentu uvedeno pokračující obnovení, bude mít Zákazník i nadále přístup k IBM SaaS a bude mu fakturováno užívání IBM SaaS na pokračující bázi. Chce-li Zákazník ukončit užívání IBM SaaS a zastavit proces pokračující fakturace, musí zaslat IBM nebo jejímu Obchodnímu partnerovi IBM devadesát (90) dní předem písemnou žádost o zrušení IBM SaaS. Poté, co bude zrušen přístup Zákazníka, budou Zákazníkovi vyfakturovány jakékoli nesplacené poplatky za přístup až do měsíce, v němž zrušení nabylo účinnosti.

5.3 Požadavek prodloužení

Je-li v Zákazníkově Transakčním dokumentu uvedena volba obnovení "ukončení", znamená to, že IBM SaaS k datu ukončení období registrace skončí a přístup Zákazníka k IBM SaaS bude odebrán. Chce-li Zákazník pokračovat v užívání IBM SaaS i po datu ukončení, musí zaslat svému obchodnímu zástupci IBM nebo Obchodnímu partnerovi IBM objednávku za účelem zakoupení nového Období registrace.

6. Technická podpora

Technická podpora pro IBM SaaS je Zákazníkovi a jeho Vybraným účastníkům poskytována s cílem poskytnout jim asistenci při používání IBM SaaS.

Registrace všech nabídek zahrnuje Standardní podporu. Předpokladem pro podporu Premium pro základní registraci Trusteer Rapport je služba Trusteer Rapport Mandatory Service, což je doplněk služby Trusteer Rapport.

Pro každou nabídku IBM SaaS je za dodatečný poplatek k dispozici registrace Premium, a to s výjimkou nabídek IBM Security Trusteer Mobile SDK a IBM Security Trusteer Rapport Mandatory Service.

Standardní podpora:

- Podpora poskytovaná od 8:00 do 17:00 místního času.
- Zákazníci a jejich Vybraní účastníci mohou odesílat záznamy požadavku podpory elektronicky podle popisu v příručce podpory Software as a Service [SaaS].
- Zákazníci naleznou oznámení, dokumenty, reporty jednotlivých případů a časté dotazy na portálu zákaznické podpory na adrese: http://www-01.ibm.com/software/security/trusteer/support/.
- Volby a podrobnosti podpory naleznete v příručce podpory IBM Software as a Service [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

Podpora Premium:

- Nepřetržitá podpora pro všechny úrovně závažnosti.
- Zákazníci mohou podporu kontaktovat přímo telefonicky.
- Zákazníci a jejich Vybraní účastníci mohou odesílat záznamy požadavku podpory elektronicky podle popisu v příručce podpory Software as a Service [SaaS].
- Zákazníci naleznou oznámení, dokumenty, reporty jednotlivých případů a časté dotazy na portálu zákaznické podpory na adrese: http://www-01.ibm.com/software/security/trusteer/support/.
- Volby a podrobnosti podpory naleznete v příručce podpory IBM Software as a Service [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

7. Dodatečné podmínky pro nabídky IBM SaaS

7.1 Soulad s Pravidly Safe Harbor

IBM je vázána dokumentem U.S. - EU Safe Harbor Framework, který vydalo Ministerstvo obchodu USA ve spolupráci s Evropskou Komisí. Produkty IBM Security Trusteer jsou zahrnuty do certifikace EU-U.S. Safe Harbor IBM. Další informace o rámci Safe Harbor a seznam zahrnutých společností naleznete na adrese: http://export.gov/safeharbor/.

7.2 Navýšení poplatku za roční registraci Zákazníka

IBM si vyhrazuje právo upravit poplatek za registraci služby IBM SaaS maximálně jednou za dvanáct (12) měsíců, a to o procento, které určí IBM a které nepřekročí hodnotu 3 %. Úprava poplatku za registraci vstoupí v platnost k výročnímu datu začátku počátečního období pokrytí. Tato úprava poplatku nezmění nárok Zákazníka na IBM SaaS ani metriku poplatků, na základě které je služba IBM SaaS získávána. Obchodní partneři IBM jsou nezávislí na IBM a sami si určují své ceny a podmínky.

7.3 Podpora Premium

Zákazník má nárok na podporu Premium pouze v případě nabídek IBM SaaS, ke kterým si zajistil registraci související nabídky podpory Premium.

7.4 Použití v souladu s právními předpisy a souhlas

Oprávnění ke shromažďování a zpracování dat

Účelem IBM SaaS je pomoct Zákazníkovi zlepšit jeho prostředí a data zabezpečení. IBM SaaS bude shromažďovat informace od Vybraných účastníků a Zařízení Zákazníka, která spolupracují s Obchodními nebo Maloobchodními aplikacemi, pro které si Zákazník zaregistroval pokrytí nabídek IBM SaaS. IBM SaaS shromažďuje informace, které mohou být samostatně nebo v kombinaci v určitých jurisdikcích považovány za Osobní údaje. Osobní údaje jsou jakékoli informace, které mohou být použity k identifikaci určité osoby (například jméno, e-mailová adresa, adresa bydliště nebo telefonní číslo) a které byly poskytnuty IBM pro účely uložení, zpracování nebo přenosu jménem Zákazníka.

Postupy shromažďování a zpracování dat mohou být aktualizovány za účelem zlepšení funkcí služby IBM SaaS. Zákazníkovi je na vyžádání k dispozici dokument s kompletním popisem postupů shromažďování a zpracování dat, který je podle potřeby aktualizován. Zákazník opravňuje IBM ke shromažďování těchto informací a jejich zpracování v souladu s oddíly Přenosy přes hranice a Ochrana osobních údajů těchto Podmínek užívání a Ochrana a zabezpečení dat ve Všeobecných podmínkách Podmínek užívání.

Pro nabídky IBM Security Trusteer Pinpoint:

Shromažďovaná data mohou zahrnovat adresy IP, šifrovaná nebo jednosměrně hašovaná ID uživatele, soubory cookie domény, pokud nejsou filtrovány, návštěvy chráněných Aplikací a phishingových webů a geografická umístění a pověření zadané na phishingových webech.

Pro nabídky IBM Security Trusteer Mobile SDK a IBM Security Trusteer Mobile Browser:

Shromažďovaná data mohou zahrnovat adresy IP, šifrovaná nebo jednosměrně hašovaná ID uživatele, geografické umístění a návštěvy chráněných Aplikací, informace o kartě SIM, název zařízení a přidružené jednotky Zákazníka.

Pro nabídky IBM Security Trusteer Rapport:

Shromažďovaná data mohou zahrnovat adresy IP, šifrovaná nebo jednosměrně hašovaná ID uživatele, události zabezpečení, uživatelské jméno a e-mailovou adresu poskytnuté pro účely kontaktování IBM s žádostí o zákaznickou podporu, Přidružené jednotky Zákazníka, šifrované heslo zadané na chráněných webech, návštěvy chráněných Aplikací a phishingových webů, šifrovaná čísla platebních karet a soubory a data shromažďovaná vzdáleně zaměstnanci IBM za účelem kontroly podezřelého malwaru, škodlivých aktivit nebo selhání.

Informovaný souhlas od Datových subjektů:

Použití této služby IBM SaaS může implikovat různé právní předpisy. IBM SaaS lze používat pouze pro účely, které jsou v souladu s požadavky právních předpisů, a zákonným způsobem. Zákazník vyjadřuje souhlas s tím, že IBM SaaS bude používat v souladu s platnými právními předpisy a zásadami a v této souvislosti přebírá veškerou odpovědnost.

Pro nabídky IBM Security Trusteer Pinpoint offerings a IBM Security Trusteer Mobile SDK:

Zákazník vyjadřuje souhlas, že získal nebo získá plně informované souhlasy, oprávnění nebo licence nutné k používání IBM SaaS v souladu s právními předpisy a k povolení shromažďování a zpracování informací společností IBM prostřednictvím IBM SaaS.

Pro nabídky IBM Security Trusteer Rapport a & IBM Security Trusteer Mobile Browser:

Zákazník opravňuje IBM k získání plně informovaných souhlasů nutných k používání IBM SaaS v souladu s právními předpisy a ke shromažďování a zpracování informací podle popisu v Licenční smlouvě s koncovým uživatelem na adrese https://www.trusteer.com/support/end-user-license-agreement. Pokud Zákazník určí, že on (a nikoli IBM) bude mít na starosti komunikaci s koncovými uživateli týkající se získání souhlasu, vyjadřuje souhlas s tím, že získal nebo získá plně informované souhlasy, oprávnění nebo licence nutné k používání IBM SaaS v souladu se zákony a k povolení shromažďování a zpracování informací společností IBM prostřednictvím IBM SaaS.

7.5 Přenosy přes hranice

Zákazník vyjadřuje souhlas s tím, že IBM může zpracovat obsah, včetně jakýchkoli Osobních údajů, v souladu s relevantními právními předpisy a požadavky přes státní hranice zpracovatelům a dílčím zpracovatelům v následujících zemích mimo Evropský hospodářský prostor a zemích, které mají podle Evropské Komise odpovídající úrovně zabezpečení: USA.

7.6 Ochrana osobních údajů

Pokud Zákazník poskytuje IBM SaaS Osobní údaje v členských státech EU, na Islandu, v Lichtenštejnsku, Norsku nebo Švýcarsku nebo pokud má Zákazník v těchto zemích Vybrané účastníky nebo Zařízení Zákazníka, Zákazník jako výhradní kontrolor určí IBM jako zpracovatele ke zpracování (tyto pojmy jsou definovány ve směrnici EU 95/46/ES) Osobních údajů. IBM bude takové Osobní údaje zpracovávat pouze v rozsahu požadovaném ke zpřístupnění nabídky IBM SaaS v souladu s publikovanými popisy IBM služby IBM SaaS a Zákazník vyjadřuje souhlas s tím, že takové zpracování je v souladu s pokyny Zákazníka. IBM poskytne oznámení přiměřeně předem, pokud provede podstatnou změnu umístění zpracování nebo způsobu, jakým zabezpečuje Osobní údaje v rámci IBM SaaS. Zákazník smí aktuální Období registrace pro dotčenou nabídku IBM SaaS ukončit, a to na základě písemné výpovědi poskytnuté IBM do třiceti (30) dní od okamžiku, kdy IBM změnu Zákazníkovi oznámila. Zákazník vyjadřuje souhlas, že IBM smí zpracovávat obsah včetně jakýchkoli Osobních údajů přes hranice, a to ve vztahu s následujícími zpracovateli a dílčími zpracovateli:

Název zpracovatele / dílčího zpracovatele	Role (zpracovatel nebo dílčí zpracovatel dat)	Lokalita*
Smluvní partner IBM	Zpracovatel	Tak, jak je uvedeno v Transakčním dokumentu
Amazon Web Services LLC	Dílčí zpracovatel	410 Terry Ave. N Seattle, WA 98109 USA
Connectria Corp.	Dílčí zpracovatel	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 USA

Název zpracovatele / dílčího zpracovatele	Role (zpracovatel nebo dílčí zpracovatel dat)	Lokalita*
IBM Israel Ltd.	Dílčí zpracovatel	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izrael
IBM Corp	Dílčí zpracovatel	1 New Orchard Rd. Armonk, NY 10504 USA

Zákazník souhlasí s tím, že IBM smí prostřednictvím oznámení změnit tento seznam států, pokud důvodně usoudí, že je to nezbytné pro poskytování IBM SaaS.

Zákazník vyjadřuje souhlas s tím, že pro služby poskytované prostřednictvím německého datového střediska smí IBM zpracovávat obsah včetně jakýchkoli Osobních údajů přes hranice, a to ve vztahu s následujícími zpracovateli a dílčími zpracovateli:

Název zpracovatele / dílčího zpracovatele	Role (zpracovatel nebo dílčí zpracovatel dat)	Lokalita*
Smluvní entita IBM	Zpracovatel	Tak, jak je uvedeno v Transakčním dokumentu
Amazon Web Services (Německo)	Dílčí zpracovatel	Mnichov, Německo
IBM Israel Ltd.	Dílčí zpracovatel	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izrael

Zákazník vyjadřuje souhlas s tím, že pro služby poskytované prostřednictvím japonského datového střediska smí IBM zpracovávat obsah včetně jakýchkoli Osobních údajů přes hranice, a to ve vztahu s následujícími zpracovateli a dílčími zpracovateli:

Název zpracovatele / dílčího zpracovatele	Role (zpracovatel nebo dílčí zpracovatel dat)	Lokalita*
Smluvní entita IBM	Zpracovatel	Tak, jak je uvedeno v Transakčním dokumentu
Amazon Web Services (Japonsko)	Dílčí zpracovatel	Tokio, Japonsko
IBM Israel Ltd.	Dílčí zpracovatel	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izrael

* Lokality uvedené v tabulkách výše zahrnují adresy podnikových pracovišť Zpracovatele a Dílčího zpracovatele. Datová střediska se nacházejí ve stejné uvedené zemi.

Strany nebo jejich relevantní příbuzné společnosti mohou uzavřít samostatné standardní a nezměněné smlouvy k Modelovým ustanovením EU z titulu jejich příslušného postavení, a to v souladu s Rozhodnutím EU 2010/87/EU a s odebranými volitelnými klauzulemi. Jakékoli spory nebo nároky vzniklé na základě těchto smluv, a to i v případě, že byly uzavřeny příbuznými společnostmi, budou posuzovány tak, jako by tento spor nebo odpovědnost vznikly mezi nimi podle této smlouvy.

Příloha A

1. Nabídky IBM SaaS

IBM nabízí tyto služby jako samostatné služby a nabídky nebo jako dodatečné služby a nabídky. Konkrétní objednané nabídky IBM SaaS jsou uvedeny v Zákazníkově dokumentu o oprávnění (Proof of Entitlement).

1.1 Definice Obchodních a Maloobchodních aplikací

Produkty IBM Security Trusteer Fraud jsou licencovány k použití s konkrétními typy Aplikací. Aplikace je definována jako jeden z následujících typů: Maloobchodní nebo Obchodní. Pro Maloobchodní a Obchodní aplikace jsou k dispozici oddělené nabídky.

- Maloobchodní aplikace je definována jako aplikace online bankovnictví, mobilní aplikace nebo aplikace e-commerce určená pro zákazníky služby. Zásady týkající se zákazníků mohou klasifikovat určité malé aplikace jako odpovídající pro maloobchodní přístup.
- Obchodní aplikace je definována jako aplikace online bankovnictví, mobilní aplikace nebo aplikace e-commerce určená pro podnikové, institucionální nebo ekvivalentní entity nebo jakákoli aplikace, která není kategorizována jako Maloobchodní.

1.2 Nabídky základní registrace IBM SaaS

Obchodní nabídky:

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

Maloobchodní nabídky:

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

Pro každou nabídku Obchodní nebo Maloobchodní aplikace je za další poplatek k dispozici související podpora Premium, a to s výjimkou nabídek IBM Security Trusteer Mobile SDK.

1.3 Další nabídky registrace IBM SaaS pro nabídky IBM Security Trusteer Rapport

Další nabídky dostupné pro produkt IBM Security Trusteer Rapport for Business:

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

Další nabídky dostupné pro produkt IBM Security Trusteer Rapport for Retail:

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

Pro každý doplněk Obchodní nebo Maloobchodní aplikace k nabídkám IBM Security Trusteer Rapport je s výjimkou doplňků IBM Security Trusteer Rapport Mandatory Service za další poplatek k dispozici související podporu Premium.

Registrace produktu IBM Security Trusteer Rapport for Business nebo IBM Security Trusteer Rapport for Retail je předpokladem pro další související nabídky registrace IBM SaaS uvedené v této části.

1.4 Další nabídky registrace IBM SaaS pro nabídky IBM Security Trusteer Pinpoint Malware Detection

Další nabídky dostupné pro produkt IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Další nabídky dostupné pro produkt IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition:

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

Za další poplatek je pro každou další nabídku IBM SaaS uvedenou v této části k dispozici podpora Premium.

Registrace nabídek IBM Security Trusteer Pinpoint Malware Detection for Business nebo IBM Security Trusteer Pinpoint Malware Detection for Retail je předpokladem pro další související nabídky registrace IBM SaaS uvedené v této části.

1.5 Další dodatečné registrace IBM SaaS

Jakékoli dodatečné registrace IBM SaaS pro základní registrace výše, které zde nejsou uvedeny, ať už aktuálně dostupné nebo ve vývoji, nejsou považovány za aktualizaci a musí být uděleny odděleně.

1.6 Definice

Vlastník účtu – označuje koncového uživatele Zákazníka, který si nainstaloval software s podporou klienta, přijal licenční smlouvu s koncovým uživatelem ("EULA") a minimálně jednou se ověřil v Maloobchodní nebo Obchodní aplikaci, pro kterou Zákazník získal registraci pro pokrytí nabídek IBM SaaS.

Software klienta vlastníka účtu – označuje software s podporou klienta IBM Security Trusteer Rapport nebo software s podporou klienta IBM Security Trusteer Mobile Browser či jakýkoli jiný software s podporou klienta, který je poskytován s některými registracemi pro IBM SaaS k instalaci na zařízení koncového uživatele.

Úvodní stránka Trusteer – označuje úvodní stránku, která je poskytována Zákazníkovi na základě dostupných šablon úvodních stránek.

Vstupní stránka – označuje stránku hostovanou IBM, která je poskytována Zákazníkovi s úvodní stránkou Zákazníka a Softwarem klienta vlastníka účtu ke stažení.

2. Nabídky IBM Security Trusteer Rapport

2.1 IBM Security Trusteer Rapport for Retail nebo IBM Security Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport poskytuje vrstvu ochrany proti útokům phishing a útokům malwaru Man-in-the-Browser (MitB). S využitím sítě desítek milionů koncových bodů po celé zemi IBM Security Trusteer Rapport shromažďuje informace o aktivních útocích phishing a malwaru cílených na organizace po celém světě. IBM Security Trusteer Rapport aplikuje behaviorální algoritmy s cílem blokovat útoky phishing a zabránit instalaci a běhům filtrace malwaru MitB.

Tato nabídka IBM SaaS má metriku poplatku Vybraný účastník. Obchodní nabídka je prodávána v balíčcích po 10 Vybraných účastnících. Maloobchodní nabídka je prodávána v balíčcích po 100 Vybraných účastnících.

Tato nabídka IBM SaaS zahrnuje:

a. Trusteer Management Application ("TMA"):

   Aplikace TMA je zpřístupněna v prostředí IBM Security Trusteer hostovaném v cloudu, prostřednictvím kterého Zákazník (a neomezený počet jeho oprávněných pracovníků) může: (i) přijímat úkoly vytváření reportů s daty událostí a posouzení rizik, (ii) zobrazovat, konfigurovat a nastavovat zásady související s vytvářením reportů s daty událostí a (iii) zobrazovat konfiguraci softwaru s podporou klienta licencovaného veřejnosti na základě licenční smlouvy pro koncového uživatele ("EULA") a zpřístupnit takový software, který je také označován jako sada softwaru Trusteer Rapport ("Software klienta vlastníka účtu"), ke stažení do stolních počítačů a zařízení Vybraných účastníka (PC/MAC). Zákazník může nabízet Software klienta vlastníka účtu pouze pomocí Úvodní stránky Trusteer nebo rozhraní API Rapport a Zákazník tento software nesmí používat pro své interní obchodní operace nebo k použití svými zaměstnanci (mimo osobního použití zaměstnanců).

b. Webový skript:

   Pro přístup na web pro účely přístupu nebo použití nabídek IBM SaaS.

c. Data události:

   Zákazník (a neomezený počet jeho oprávněných pracovníků) může TMA používat k přijímání dat událostí generovaných ze Softwaru klienta vlastníka účtu v důsledku online interakcí Vlastníků účtu s jejich Obchodní nebo Maloobchodní aplikací, pro kterou Zákazník získal registraci pokrytí nabídek IBM SaaS. Data události budou přijata ze Softwaru klienta vlastníka účtu Vybraných účastníků běžícího na jejich zařízeních, kteří uzavřeli smlouvu EULA a minimálně jednou provedli ověření v Obchodní nebo Maloobchodní aplikaci Zákazníka; konfigurace Zákazníka musí zahrnovat shromažďování ID uživatele.

d. Úvodní stránka Trusteer:

   Marketingová platforma Úvodní stránky Trusteer identifikuje a prodává Software klienta vlastníka účtu Vybraným účastníkům přistupujícím k Obchodním nebo Maloobchodním aplikacím, pro které si Zákazník zaregistroval pokrytí nabídek IBM SaaS. Zákazník si může vybrat z dostupných šablon Úvodní stránky. Na základě samostatné smlouvy nebo rozsahu prací lze sjednat přizpůsobenou úvodní stránku.

Zákazník může souhlasit s poskytnutím ochranných známek, log nebo ikon k použití v souvislosti s TMA a pouze pro využití Úvodní stránky Trusteer a zobrazení v Softwaru klienta vlastníka účtu nebo na vstupních stránkách hostovaných IBM a na webu IBM Security Trusteer. Každé použití poskytnutých ochranných známek, log nebo ikon bude v souladu s přiměřenými zásadami IBM týkajícími se inzerce a využití ochranných známek.

Zákazník se musí přihlásit k registraci nabídky IBM Security Trusteer Rapport Mandatory Service SaaS, pokud si přeje využít jakýkoli typ povinné implementace Softwaru klienta vlastníka účtu.

Povinná implementace Softwaru klienta vlastníka účtu zahrnuje mimo jiné jakýkoli typ povinné implementace za využití libovolného mechanismu nebo libovolného prostředku, který přímo nebo nepřímo nutí Vybraného účastníka ke stažení Softwaru klienta vlastníka účtu, nebo libovolné metody, nástroje, postupu, smlouvy či mechanismu, které nevytvořila nebo neschválila IBM a které byly vytvořeny k obejití licenčních požadavků této povinné implementace Softwaru klienta vlastníka účtu.

2.2 Volitelné další nabídky IBM SaaS pro IBM Security Trusteer Rapport pro Business nebo IBM Security Trusteer Rapport for Retail

Registrace nabídek IBM Security Trusteer Rapport je předpokladem registrace jakékoli z následujících dodatečných nabídek IBM SaaS. Pokud je služba IBM SaaS označena jako "for Business", musí být získaná dodatečná nabídka IBM SaaS také označena jako "for Business". Pokud je služba IBM SaaS označena jako "for Retail", musí být získaná dodatečná nabídka IBM SaaS také označena jako "for Retail". Zákazník bude přijímat data události od Vybraných účastníků používajících Software klienta vlastníka účtu, kteří uzavřeli smlouvu EULA pro koncové uživatele a minimálně jednou provedli ověření v Obchodní nebo Maloobchodní aplikaci Zákazníka; konfigurace Zákazníka musí zahrnovat shromažďování ID uživatele.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business nebo IBM Security Trusteer Rapport Fraud Feeds for Retail

Zákazník (a neomezený počet jeho oprávněných pracovníků) může TMA používat k přijímání dat událostí souvisejících s infikováním malwarem nebo jiným ohrožením koncového bodu na stolním počítači konkrétního Vlastníka účtu.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business nebo IBM Security Trusteer Rapport Phishing Protection for Retail

Zákazník (a neomezený počet jeho oprávněných pracovníků) může TMA používat k přijímání oznámení o datech událostí souvisejících s poskytnutím přihlašovacích údajů Vlastníka účtu na webu s podezřením na phishing nebo na potenciálně podvodném webu. Legitimní online aplikace (adresy URL) mohou být chybně označeny jako phishingové weby a služba IBM SaaS může Vlastníky účtu upozornit, že legitimní web je phishingový web. V takovém případě musí Zákazník na tuto chybu upozornit IBM, která ji odstraní. Toto bude výhradní náprava Zákazníka v případě takové chyby.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business nebo IBM Security Trusteer Rapport Mandatory Service for Retail

Zákazník smí používat instanci marketingové platformy Úvodní stránky Trusteer k povolení stahování Softwaru klienta vlastníka účtu Vybraným účastníkům přistupujícím k Obchodním nebo Maloobchodním aplikacím, pro které si Zákazník zaregistroval pokrytí nabídek IBM SaaS.

IBM Security Trusteer Rapport Premium Support for Business je předpokladem pro IBM Security Rapport Mandatory Service for Business.

IBM Security Trusteer Rapport Premium Support for Retail je předpokladem pro IBM Security Rapport Mandatory Service for Retail.

Zákazník smí implementovat další funkce IBM Security Trusteer Rapport Mandatory Service, pouze pokud byly objednány a konfigurovány pro použití s Obchodními nebo Maloobchodními aplikacemi, pro které si Zákazník zaregistroval pokrytí nabídek IBM SaaS.

3. Nabídky IBM Security Trusteer Pinpoint

IBM Security Trusteer Pinpoint je cloudová služba, která je určena k zajištění další vrstvy ochrany a jejím cílem je zjistit a zmírnit útoky malwaru a phishingu a snahu o převzetí účtu. Trusteer Pinpoint lze integrovat do Obchodních nebo Maloobchodních aplikací Klienta, pro které Zákazník získal registraci pokrytí a procesů prevence zneužití nabídek IBM SaaS.

Tato nabídka IBM SaaS zahrnuje:

a. TMA:

   Aplikace TMA je zpřístupněna v prostředí IBM Security Trusteer hostovaném v cloudu, prostřednictvím kterého Zákazník (a neomezený počet jeho oprávněných pracovníků) může: (i) přijímat úkoly vytváření reportů s daty událostí a posouzení rizik, (ii) zobrazovat, konfigurovat a nastavovat zásady zabezpečení a zásady související s vytvářením reportů s daty událostí.

b. Webový skript nebo rozhraní API:

   Pro implementaci na webu pro účely přístupu nebo použití IBM SaaS.

3.1 IBM Security Trusteer Pinpoint Malware Detection a IBM Security Trusteer Pinpoint Criminal Detection

V případě zjištění malwaru v nabídkách IBM Security Trusteer Pinpoint Malware Detection nebo zjištění převzetí účtu v nabídkách IBM Security Trusteer Pinpoint Criminal Detection musí Zákazník dodržovat příručku s osvědčenými postupy Pinpoint Best Practices Guide. Nepoužívejte nabídky IBM Security Trusteer Pinpoint Malware Detection nebo IBM Security Trusteer Pinpoint Criminal Detection způsobem, který ovlivní prostředí Vybaných účastníků ihned po zjištění malwaru nebo převzetí účtu tak, aby ostatní uživatelé mohli propojit akce Zákazníka s použitím nabídek IBM Security Trusteer Pinpoint (např. oznámení, zprávy, blokování zařízení nebo blokování přístupu k Obchodní nebo Maloobchodní aplikaci ihned po zjištění malwaru nebo převzetí účtu).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business nebo IBM Security Trusteer Pinpoint Criminal Detection for Retail

Detekce podezřelého převzetí účtu bez klienta ze strany prohlížečů připojujících se k Obchodní nebo Maloobchodní aplikaci za použití ID zařízení, detekce phishingu a detekce odcizení pověření iniciované malwarem. Nabídky IBM Security Trusteer Pinpoint Criminal Detection poskytují další vrstvu ochrany a jejich cílem je zjistit pokusy o převzetí účtu a poskytnout skóre posouzení rizika prohlížečů nebo mobilních zařízení (prostřednictvím nativního prohlížeče nebo mobilní aplikace zákazníka) přistupujících k Obchodní nebo Maloobchodní aplikaci přímo pro Zákazníka.

a. Data události:

   Zákazník (a neomezený počet jeho oprávněných zaměstnanců) může TMA používat k přijímání dat událostí generovaných v důsledku online interakcí Vybraných účastníků s Maloobchodními nebo Obchodními aplikacemi Zákazníka, pro které získal Zákazník pokrytí nabídek IBM SaaS, nebo Zákazník může přijímat data události prostřednictvím režimu doručování backendového rozhraní API.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile a/nebo IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

Nabídky IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) jsou určeny k poskytnutí další vrstvy ochrany a jejich cílem je chránit před převzetím účtu a podvodnými aktivitami identifikováním nezákonného přístupu k účtu a generováním závěrečného doporučení pro Zákazníka. Tato nabídka IBM SaaS shromažďuje informace pocházející z Obchodních a Maloobchodních aplikací Zákazníka za použití PPCD Mobile API a z mobilních zařízení Vybraných účastníků. Nabídky IBM Security Trusteer PPCD Mobile jsou určeny ke korelaci složitých informací souvisejících s mobilními zařízeními Vybraných účastníků s ostatními datovými zdroji, například zasažení malwarem a incidenty phishingu, které jsou integrovány prostřednictvím ostatních nabídek IBM SaaS pro Security Trusteer uvedených v těchto Podmínkách užívání.

Zákazník může k nabídkám IBM Security Trusteer PPCD Mobile přistupovat a používat je v prostředí IBM Security Trusteer hostovaném v cloudu a může přijímat data posouzení rizika z mobilních zařízení Vybraných účastníků generovaná jako výsledek online interakcí těchto mobilních zařízení s Obchodní nebo Maloobchodní aplikací zákazníka, pro které se Zákazník zaregistroval k nabídce IBM SaaS. Pro účely těchto nabídek zahrnují "mobilní zařízení" pouze podporované mobilní telefony a tablety, nikoli počítače PC nebo MAC.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Detekce připojení prohlížečů infikovaných finančním malwarem bez klienta během připojování k Obchodní nebo Maloobchodní aplikaci. Nabídky IBM Security Trusteer Pinpoint Malware Detection poskytují další vrstvu ochrany a jejich cílem je umožnit organizacím zaměřit se na procesy prevence podvodů na základě rizika malwaru tím, že Zákazníkovi zajistí posouzení a výstrahy na přítomnost finančního malwaru MitB.

a. Data události:

   Zákazník (a neomezený počet jeho oprávněných zaměstnanců) může TMA používat k přijímání dat událostí generovaných v důsledku online interakcí Vybraných účastníků s Maloobchodními nebo Obchodními aplikacemi Zákazníka.

b. Advanced Edition:

   Edice Advanced Edition for Business nebo for Retail nabízí další úroveň detekce a ochrany, která je přizpůsobena struktuře a toku Obchodních a Maloobchodních aplikací Zákazníka a lze ji upravit podle konkrétního prostředí hrozeb zacílených na Zákazníka. Produkty lze začlenit na různých pracovištích do Obchodních nebo Maloobchodních aplikací Zákazníka.

   Advanced Edition je Zákazníkovi nabízena s minimálním množstvím minimálně 100 000 Maloobchodních oprávněných účastníků nebo 10 000 Obchodních vybraných účastníků, což je 1000 balíčků 100 Vybraných účastníků pro Maloobchodní aplikace nebo 1000 balíčků 10 Vybraných účastníků pro Obchodní aplikace.

c. Standard Edition:

Standard Edition for Business nebo for Retail je řešení s rychlou implementací, které poskytuje základní funkce této nabídky IBM SaaS popsané v tomto dokumentu.

3.2 Volitelné další nabídky IBM SaaS pro IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Pro nabídky IBM Security Trusteer Rapport Remediation for Retail je jako předpoklad vyžadován produkt IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition.

Pro IBM Security Trusteer Pinpoint Carbon Copy for Retail je jako předpoklad vyžadován produkt IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition. Pro IBM Security Trusteer Pinpoint Carbon Copy for Business je jako předpoklad vyžadován produkt IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition nebo IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business nebo IBM Security Trusteer Pinpoint Carbon Copy for Retail

Nabídky IBM Security Trusteer Pinpoint Carbon Copy určené k zajištění další vrstvy ochrany a monitorovacích služeb, které pomohou identifikovat případy, kdy byla pověření Vybraných účastníků kompromitována útoky phishing na Maloobchodní nebo Obchodní aplikace Zákazníka, pro které Zákazník získal registraci pokrytí nabídek IBM SaaS.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

Cílem produktu IBM Security Trusteer Rapport Remediation for Retail je prošetřit, napravit, zablokovat a odebrat infekce malwaru typu man-in-the-browser (MitB) z infikovaných zařízení (PC/MAC) Vybraných účastníků Zákazníka, kteří přistupují k Maloobchodní aplikaci Zákazníka na ad-hoc bázi, kde infekce malwaru MitB byla zjištěna daty událostí IBM Security Trusteer Pinpoint Malware Detection. Zákazník musí mít aktuální registraci produktu IBM Security Trusteer Pinpoint Malware Detection, který je používán v Maloobchodní aplikaci Zákazníka. Zákazník smí tuto nabídku IBM SaaS použít pouze ve spojení s Vybranými účastníky, kteří přistupují k Maloobchodní aplikaci Zákazníka, a výhradně jako nástroj, jehož cílem je prošetřit a opravit konkrétní infikované zařízení (PC/MAC) na ad-hoc bázi. IBM Security Trusteer Rapport Remediation for Retail musí běžet na dotčených zařízeních Vybraného účastníka (PC/MAC) a takový Vybraný účastník musí uzavřít smlouvu EULA a minimálně jednou provést své ověření v Maloobchodní aplikaci Zákazníka; konfigurace Zákazníka musí zahrnovat shromažďování ID uživatele. Aby nedošlo k pochybnostem, tato nabídka IBM SaaS nezahrnuje právo na používání Úvodní stránky Trusteer nebo k jiné podpoře Softwaru klienta vlastníka účtu určené pro obecné Vybrané účastníky Zákazníka.

4. Nabídky IBM Security Trusteer Mobile

4.1 IBM Security Trusteer Mobile Browser for Business nebo IBM Security Trusteer Mobile Browser for Retail

Produkt IBM Security Trusteer Mobile Browser je určen k přidání další úrovně ochrany a slouží k zajištění bezpečného online přístupu mobilních zařízení Vybraných účastníků přistupujících k Maloobchodním nebo Obchodním aplikacím Zákazníka, pro které si Zákazník zaregistroval pokrytí nabídek IBM SaaS, posouzení rizika mobilních zařízení a ochranu proti phishingu. Zabezpečená detekce Wi-Fi je k dispozici pouze pro platformu Android. Pro účely této nabídky IBM SaaS mobilní zařízení zahrnují mobilní telefony nebo tablety a nezahrnují notebooky a počítače MAC.

Prostřednictvím TMA může Zákazník (a neomezený počet jeho oprávněných pracovníků) přijímat data události, analýzy a informace o statistikách související se zařízeními, jejichž Vybraní účastníci: (i) si zdarma stáhli Software klienta vlastníka účtu, aplikaci licencovanou veřejnosti v rámci smlouvy pro koncové uživatele, která je k dispozici ke stažení do mobilních zařízení Vybraných účastníků, a (ii) uzavřeli smlouvu pro koncové uživatele a minimálně jednou se ověřili v Obchodní nebo Maloobchodní aplikaci Zákazníka, pro kterou si Zákazník zaregistroval pokrytí nabídek IBM SaaS. Zákazník může

nabízet Software klienta vlastníka účtu pouze pomocí Úvodní stránky Trusteer a nesmí tento software používat pro své interní obchodní operace.

a. Data události:

   Zákazník (a neomezený počet jeho oprávněných pracovníků) může TMA používat k přijímání dat událostí generovaných v důsledku online interakcí mobilních zařízení s Maloobchodními nebo Obchodními aplikacemi Zákazníka, pro které získal Zákazník pokrytí nabídek IBM SaaS.

b. Úvodní stránka Trusteer:

   Marketingová platforma Úvodní stránky Trusteer identifikuje a prodává Software klienta vlastníka účtu Vybraným účastníkům přistupujícím k Obchodním nebo Maloobchodním aplikacím, pro které si Zákazník zaregistroval pokrytí nabídek IBM SaaS. Zákazník si může vybrat z dostupných šablon Úvodní stránky ("Šablona úvodní stránky"). Na základě samostatné smlouvy nebo rozsahu prací lze sjednat přizpůsobenou úvodní stránku.

Zákazník může souhlasit s poskytnutím ochranných známek, log nebo ikon k použití v souvislosti s TMA a pouze pro využití Úvodní stránky Trusteer a zobrazení v Softwaru klienta vlastníka účtu nebo na vstupních stránkách hostovaných IBM nebo na webu IBM Security Trusteer. Každé použití poskytnutých ochranných známek, log nebo ikon bude v souladu s přiměřenými zásadami IBM týkajícími se inzerce a využití ochranných známek.

4.2 IBM Security Trusteer Mobile SDK for Business nebo IBM Security Trusteer Mobile SDK for Retail

Nabídky IBM Security Trusteer Mobile SDK jsou určeny k přidání další úrovně ochrany a slouží k zajištění bezpečného webového přístupu k Maloobchodním nebo Obchodním aplikacím Zákazníka, pro které si Zákazník zaregistroval pokrytí nabídek IBM SaaS, posouzení rizika mobilních zařízení a ochranu proti phishingu. Zabezpečená detekce Wi-Fi je k dispozici pouze pro platformu Android.

Nabídky IBM Security Trusteer Mobile SDK zahrnují vlastní mobilní sadu pro vývojáře softwaru ("SDK"), softwarový balík obsahující dokumentaci, programovací vlastní knihovny softwaru a ostatní související soubory a položky známé jako mobilní knihovna IBM Security Trusteer, a "Komponentu běhového prostředí" nebo "Opakovaně šiřitelný" vlastní kód generovaný sadou IBM Security Trusteer Mobile SDK, který lze vložit a integrovat do chráněných samostatných mobilních aplikací sytému iOS nebo Android Zákazníka, pro které se Zákazník přihlásil k registraci nabídek IBM SaaS.("Integrované mobilní aplikace Zákazníka").

Produkt IBM Security Trusteer Mobile SDK for Retail je k dispozici v balíčcích po 100 Vybraných účastnících nebo balíčcích po 100 Zařízeních Zákazníka a produkt IBM Security Trusteer Mobile SDK for Business je k dispozici v balíčcích po 10 Vybraných účastnících nebo balíčcích po 10 Zařízeních Zákazníka.

Prostřednictvím TMA může Zákazník (a neomezených počet jeho oprávněných pracovníků) přijímat reporty o datech událostí a hodnocení trendů rizik. Prostřednictvím Integrované mobilní aplikace Zákazníka může Zákazník přijímat analýzy rizik a informace o mobilním zařízení související s mobilními zařízeními Vybraných účastníků, kteří si stáhli Integrovanou mobilní aplikaci Zákazníka. Zákazník tak může vytvořit zásady prevence podvodů, které budou vynucovat zmírňující akce zaměřené na tato rizika. Pro účely této nabídky zahrnují "mobilní zařízení" pouze podporované mobilní telefony, nikoli počítače PC a MAC.

Zákazník může:

a. interně používat sadu IBM Security Trusteer Mobile SDK výhradně pro účely vývoje Integrovaných mobilních aplikací Zákazníka;

b. vnořit Opakovaně šiřitelný kód (výhradně ve formátu objektového kódu) jako integrální neoddělitelný způsob do Integrované mobilní aplikace Zákazníka. Jakákoli změněná nebo sloučená část Opakovaně šiřitelného kódu v souladu s touto licencí podléhá stejným podmínkám těchto Podmínek užívání; a

c. prodávat Opakovaně šiřitelný kód a distribuovat jej ke stažení do mobilních zařízení Vybraných účastníků nebo vlastníkovi Zařízení Zákazníka za předpokladu, že:

- S výjimkou případů výslovně povolených v této Smlouvě Zákazník nesmí (1) používat, kopírovat, měnit nebo distribuovat sadu SDK; (2) zpětně sestavovat, kompilovat nebo jinak překládat nebo provádět zpětnou analýzu sady SDK s výjimkou případů výslovně povolených zákonem bez možnosti smluvního vzdání se práv; (3) sadu SDK poskytovat v rámci dílčí licence, pronajímat nebo poskytovat na leasing; (4) odstranit soubory, jež jsou předmětem autorských práv, a sdělení obsažená v Opakovaně šiřitelném kódu; (5) používat stejný název cesty jako původní soubory nebo moduly Opakovaně šiřitelného kódu; a (6) používat názvy nebo ochranné známky IBM, jejích poskytovatelů licence a distributorů v souvislosti s marketingem Integrované mobilní aplikace Zákazníka bez předchozího písemného souhlasu těchto stran.
- Opakovaně šiřitelný kód zůstane neoddělitelným způsobem integrovaný do Integrované mobilní aplikace Zákazníka. Opakovaně šiřitelný kód musí být pouze ve formě objektového kódu a musí splňovat všechny pokyny a specifikace v sadě SDK a v příslušné dokumentaci. Licenční smlouva s koncovým uživatelem pro Integrovanou mobilní aplikaci Zákazníka musí koncového uživatele upozornit, že Opakovaně šiřitelný kód nesmí být i) použit k účelu jinému než k povolení Integrované mobilní aplikace Zákazníka, ii) zkopírován (s výjimkou pro účely zálohování), iii) dále distribuován nebo přenesen ani iv) zpětně získán, kompilován nebo jinak přeložen s výjimkou konkrétně povolenou právními předpisy a bez možnosti smluvního vzdání se práv. Licenční smlouva Zákazníka musí zajistit minimálně stejnou ochranu IBM jako podmínky této Smlouvy.
- Sadu SDK lze implementovat pouze v rámci interní implementace Zákazníka a testování jednotky na určených mobilních testovacích zařízeních Zákazníka. Zákazník nesmí sadu SDK používat pro účely zpracování produktivní zátěže, simulace produktivní zátěže nebo testování škálovatelnosti kódu, aplikace nebo systému. Zákazník nesmí používat žádnou část sady SDK k jakýmkoli jiným účelům.

Zákazník nese odpovědnost za veškerou technickou asistenci pro Integrovanou mobilní aplikaci Zákazníka a jakékoli modifikace Opakovatelně šiřitelných kódů provedené Zákazníkem v souladu s tímto dokumentem.

Zákazník je oprávněn instalovat a používat Opakovaně šiřitelné kódy a sadu IBM Security Mobile SDK pouze k podpoře svého používání nabídky IBM SaaS.

IBM otestovala ukázkové aplikace vytvořené prostřednictvím mobilních nástrojů poskytnutých v sadě IBM Security Trusteer Mobile SDK ("Mobilní nástroje"), aby zjistila, zda bude možno je řádně spouštět v určitých verzích mobilních platforem OS ze zařízení Apple (iOS) a Google (Android) (společné označení "Mobilní platformy OS"). Mobilní platformy OS jsou však poskytovány třetími stranami, nejsou pod kontrolou IBM a mohou být změněny, aniž by o tom byla IBM informována. Vzhledem k tomu a bez ohledu na jakékoli jiné podmínky IBM nezaručuje, že jakékoli aplikace nebo jiné výstupy, které byly vytvořeny pomocí Mobilních nástrojů, bude možné na jakýchkoli Mobilních platformách OS nebo mobilních zařízeních správným způsobem spouštět, že budou s těmito platformami a nástroji spolupracovat nebo že s nimi budou kompatibilní.

Zákazník vyjadřuje souhlas, že vytvoří, uchová a IBM a jejím auditorům poskytne přesné písemné záznamy, výstupy ze systémových nástrojů a ostatní informace systému postačující k poskytnutí auditovatelného ověření, že používání sady IBM Security Trusteer Mobile SDK Zákazníkem je v souladu s ustanoveními těchto Podmínek užívání.

5. Implementace nabídek IBM SaaS Fraud Protection

Základní registrace Zákazníka zahrnuje požadované činnosti nastavení a počáteční implementace, včetně počátečního jednorázového spuštění, konfigurace, šablony úvodní stránky, testování a školení.

Další služby lze sjednat za dodatečný poplatek v rámci samostatné smlouvy.

Příloha B

IBM poskytuje pro nabídku IBM SaaS následující úroveň služeb ("SLA"), která je platná, je-li uvedena v Transakčním dokumentu Zákazníka:

Bude platit taková verze smlouvy o úrovni služeb, která je platná a účinná v okamžiku zahájení nebo prodloužení období registrace Zákazníka. Zákazník bere na vědomí, že smlouva o úrovni služeb ve vztahu k Zákazníkovi nepředstavuje záruku.

1. Definice

a. **Oprávněná kontaktní osoba** – označuje fyzickou osobu, jejíž jméno Zákazník sdělil IBM a která je oprávněna uplatňovat Nároky na základě této úrovně služeb.

b. **Kredity za porušení úrovně dostupnosti služeb** – představují náhradu, kterou IBM poskytne v případě uznaného Nároku. Tyto Kredity za porušení úrovně dostupnosti služeb budou poskytnuty formou vrácení peněz nebo slevy u následující fakturace poplatků za registraci služby IBM SaaS.

c. **Nárok** – označuje nárok, který uplatnila Oprávněná kontaktní osoba Zákazníka u společnosti IBM na základě této úrovně služeb v souvislosti s tím, že v rámci Smluvního měsíčního období nebylo dosaženo sjednané úrovně služeb.

d. **Smluvní měsíční období** – znamená každý celý měsíc doby trvání poskytování IBM SaaS, počítáno od 0:00 Greenwichského času (GMT) prvního dne měsíce až do 23:59 GMT posledního dne v měsíci.

e. **Zákazník** znamená subjekt, který si objednal Služby přímo od IBM a který řádně plní všechny podstatné povinnosti, včetně platebních povinností, jež stanoví jeho smlouva s IBM týkající se IBM SaaS.

f. **Odstávka** – označuje časové období, v jehož průběhu se zastavilo zpracování prováděné systémem v souvislosti se Službami, a kdy všichni uživatelé nemohou užívat všechny aspekty Služeb, k nimž mají příslušná oprávnění. Do Odstávky se nezapočítává doba, kdy Služby nejsou dostupné v důsledku:

- plánované odstávky systému;
- vyšší moci;
- problémů s aplikacemi, zařízeními nebo daty Zákazníka nebo třetí strany;
- Jednání nebo opomenutí Zákazníka nebo třetí strany (včetně situace, kdy kdokoliv získá přístup ke službě IBM SaaS pomocí hesel nebo vybavení Zákazníka);
- nedodržení požadovaných konfigurací systému a podporovaných platforem pro přístup k IBM SaaS;
- skutečnosti, že IBM jednala v souladu s jakýmikoli návrhy, specifikacemi nebo pokyny, jež vydal Zákazník nebo třetí strana jménem Zákazníka;

g. **Událost** – znamená okolnost nebo sled okolností posuzovaných společně, v jejichž důsledku není dosaženo úrovně služeb.

h. **Vyšší moc** – znamená živelnou pohromu, teroristický útok, stávku, požár, záplavy, zemětřesení, nepokoje, válečný konflikt, postup vlády, rozkazy nebo omezení, viry, útoky typu "odmítnutí služby" a jiné jednání ve zlém úmyslu, výpadky veřejných služeb a síťové konektivity nebo nedostupnost IBM SaaS z jiného důvodu, nad nimiž nemá IBM přiměřenou kontrolu.

i. **Plánovaná odstávka systému** – znamená plánovaný výpadek IBM SaaS z důvodu údržby.

j. **Úroveň služeb** – označuje standard uvedený níže, jímž IBM měří úroveň služeb, kterou stanoví v této úrovni služeb.

2. Kredity za porušení úrovně dostupnosti služeb

a. Aby mohl Zákazník uplatnit Nárok, musí mít u střediska zákaznické podpory IBM pro příslušnou službu IBM SaaS zaznamenán požadavek na podporu pro každou Událost v souladu s postupem IBM pro nahlašování problémů se Závažností 1. Zákazník musí poskytnout všechny potřebné detailní informace týkající se Události a přiměřeným způsobem spolupracovat s IBM, pokud jde o

diagnostiku a vyřešení Události v takovém rozsahu, který vyžadují Záznamy požadavku na podporu se Závažností 1. Tento Záznam požadavku na podporu musí být nahlášen do 24 hodin od okamžiku, kdy Zákazník poprvé zjistil, že Událost měla dopad na jeho užívání IBM SaaS.

b. Oprávněná kontaktní osoba Zákazníka musí uplatnit Zákazníkův Nárok na Kredity za porušení úrovně dostupnosti služeb nejpozději do tří (3) pracovních dní po skončení Smluvního měsíčního období, jehož se Nárok týká.

c. Oprávněná kontaktní osoba Zákazníka musí sdělit IBM všechny odpovídající informace týkající se Nároku, včetně - nikoli však pouze - podrobných popisů všech relevantních Událostí a Úrovně služeb, jejíž nedosažení Zákazník reklamuje.

d. IBM interně změří celkovou kombinovanou Odstávku během každého Smluvního měsíčního období vztahujícího se na příslušnou Úroveň služeb, jak je uvedena v tabulce níže. Kredity za porušení úrovně dostupnosti služeb vycházejí z trvání Odstávky, měřeno od okamžiku, který Zákazník nahlásil jako čas, kdy byl Odstávkou poprvé dotčen. Nahlásí-li Zákazník nějakou Událost Odstávky aplikace a souběžně se vyskytne událost Odstávky zpracování příchozích dat, bude IBM překrývající se období Odstávky považovat za jedno období Odstávky, a nikoli za dvě samostatná období Odstávky. U každého platného Nároku bude IBM aplikovat nejvyšší použitelné Kredity za porušení úrovně dostupnosti služeb vycházející z dosažené úrovně služeb během každého Smluvního měsíčního období, jak je uvedeno v tabulkách níže. IBM nebude poskytovat vícenásobné Kredity za porušení úrovně dostupnosti služeb u stejné(ých) Události(í) ve stejném Smluvním měsíčním období.

e. U služeb Bundled Service (jednotlivé Služby prodávané formou balíku za jednu kombinovanou cenu) se při výpočtu Kreditů za porušení úrovně dostupnosti služeb bude vycházet z jediné kombinované měsíční ceny za službu Bundled Service, nikoliv z měsíčního poplatku za registraci každé jednotlivé služby IBM SaaS. Zákazník smí vznášet pouze Nároky, které se týkají jedné individuální služby IBM SaaS v balíku v rámci jakéhokoliv Smluvního měsíčního období. IBM nenese odpovědnost za Kredity za porušení úrovně dostupnosti služeb pro více než jednu službu IBM SaaS v balíku za jedno Smluvní měsíční období.

f. Pokud si Zákazník službu IBM SaaS zakoupil od oprávněného prodejce IBM prostřednictvím prodejní transakce, u níž IBM nese primární odpovědnost za plnění závazků týkajících se IBM SaaS a úrovně služeb, budou Kredity za porušení úrovně dostupnosti služeb vycházet z tehdy platné ceny RVSP (Relationship Suggested Value Price) za službu IBM SaaS užívanou ve Smluvním měsíčním období, kterého se Nárok týká. Tato cena bude snížena o 50 %.

g. Celkové přiznané Kredity za porušení úrovně dostupnosti služeb vztahující se k jakémukoliv Smluvnímu měsíčnímu období nesmí za žádných okolností přesáhnout deset procent (10 %) z jedné dvanáctiny (1/12) ročního poplatku, který Zákazník zaplatil IBM za službu IBM SaaS.

h. IBM objektivně posoudí Nároky na základě informací, které jsou dostupné v záznamech IBM. Tyto záznamy budou mít rozhodující váhu v případě eventuálního rozporu s údaji uvedenými v záznamech Zákazníka.

i. KREDITY ZA PORUŠENÍ ÚROVNĚ DOSTUPNOSTI SLUŽEB, KTERÉ BUDOU ZÁKAZNÍKOVI PŘIZNÁNY V SOULADU S TOUTO ÚROVNÍ SLUŽEB, PŘEDSTAVUJÍ JEDINOU A VÝHRADNÍ NÁHRADU ZÁKAZNÍKA V PŘÍPADĚ JAKÉHOKOLIV NÁROKU.

3. Úrovně služeb

Dostupnost služby IBM SaaS během Smluvního měsíčního období

Dosažená úroveň služeb (během Smluvního měsíčního období)	Kredity za porušení úrovně dostupnosti služeb (% měsíčního registračního poplatku za Smluvní měsíční období, za které je uplatňován Nárok)
< 99,5 %	2 %
< 98,0 %	5 %
< 96,0 %	10 %

Procento "Dosažené úrovně služeb" se vypočítá jako: (a) celkový počet minut v rámci Smluvního měsíčního období minus (b) celkový počet minut Odstávky za Smluvní měsíční období, děleno (c) celkovým počtem minut za Smluvní měsíční období.

Příklad: celkový počet minut Odstávek = 250 minut za Smluvní měsíční období

Celkem 43 200 minut za 30denní Smluvní měsíční období - 250 minut Odstávek = 42 950 minut _____ 43 200 minut celkem	= 2% Kreditů za porušení úrovně dostupnosti služeb pro 99,4% Dosaženou úroveň služeb během Smluvního měsíčního období

3.1 Výjimky

Tato smlouva o úrovni služeb je dostupná pouze pro Zákazníky IBM. Tato smlouva o úrovni služeb se nevztahuje na:

- Beta verze a zkušební verze Služeb.
- Neproduktivní prostředí, včetně - nikoli však pouze - testování, obnovy po zhroucení systému, kontroly kvality a vývoje.
- Nároky, které uplatnili uživatelé Zákazníka IBM, jeho hosté, účastníci a schválené přizvané osoby užívající IBM SaaS.
- Pokud Zákazník porušil nějakou podstatnou povinnost uvedenou v Podmínkách užívání, včetně - nikoli pouze - porušení jakéhokoliv platebního závazku.