IBM Trusteer Fraud Protection

Tento Popis služby stanovuje podmínky služby Cloud Service, kterou IBM poskytuje Zákazníkovi. Zákazník znamená smluvní stranu a její oprávněné uživatele a příjemce služby Cloud Service. Příslušná Cenová nabídka a Dokument o oprávnění (Proof of Entitlement) jsou poskytnuty ve formě samostatných Transakčních dokumentů.

1. Cloud Service

Tento Popis služeb zahrnuje následující služby Cloud Service:

Služby Pinpoint Assure Cloud Services:

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

Služby Rapport Cloud:

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

Služby Pinpoint Cloud:

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

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

Služby Mobile Cloud:

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

1.1 Obchodní a maloobchodní cloudové služby

Služby IBM Trusteer Cloud Service jsou poskytovány 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 samostatné nabídky.

a. Maloobchodní aplikace je definována jako aplikace online bankovnictví, mobilní aplikace nebo aplikace e-commerce určená pro zákazníky služby. Zásady Zákazníka mohou klasifikovat určité malé podniky jako vhodné pro maloobchodní přístup.

b. Obchodní aplikace je definována jako aplikace online bankovnictví, mobilní aplikace nebo aplikace e-commerce určená pro podnikové, institucionální nebo ekvivalentní subjekty nebo jakákoli aplikace, která není kategorizována jako Maloobchodní.

1.1.1 Obchodní cloudové služby

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

1.1.2 Maloobchodní cloudové služby

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

Pro každou z obchodních a maloobchodních služeb Cloud Service je za další poplatek k dispozici související podpora Premium, a to s výjimkou služeb IBM Trusteer Mobile SDK Cloud Service.

1.1.3 Další služby Cloud Services pro produkt IBM Trusteer Rapport II

a. Další služby Cloud Services dostupné pro produkt IBM Trusteer Rapport II for Business:
   - IBM Trusteer Rapport Fraud Feeds for Business
   - IBM Trusteer Rapport Phishing Protection for Business
   - IBM Trusteer Rapport Mandatory Service for Business
   - IBM Trusteer Rapport Additional Applications for Business

b. Další služby Cloud Services dostupné pro produkt IBM Trusteer Rapport II for Retail:
   - IBM Trusteer Rapport Fraud Feeds for Retail
   - IBM Trusteer Rapport Phishing Protection for Retail
   - IBM Trusteer Rapport Mandatory Service for Retail
   - IBM Trusteer Rapport Additional Applications For Retail

Pro každý obchodní nebo maloobchodní doplněk pro služby IBM Trusteer Rapport Cloud Service je s výjimkou doplňků IBM Trusteer Rapport Mandatory Service za další poplatek k dispozici související podpora Premium.

Registrace produktu IBM Trusteer Rapport II for Business nebo IBM Trusteer Rapport II for Retail je předpokladem pro další související služby Cloud Service uvedené v této části.

1.1.4 Další služby Cloud Services pro produkt IBM Trusteer Pinpoint Malware Detection II

a. Další služby Cloud Services dostupné pro produkt IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business nebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business:
   - IBM Trusteer Rapport Remediation for Business
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. Další služby Cloud Services dostupné pro produkt IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail nebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail:
   - IBM Trusteer Rapport Remediation for Retail

- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

Podpora Premium je poskytována pro konkrétní nabídky podle ustanovení tohoto dokumentu. Registrace produktu IBM Trusteer Pinpoint Malware Detection II for Business nebo IBM Trusteer Pinpoint Malware Detection II for Retail je předpokladem pro další související služby Cloud Services uvedené v tomto oddílu.

1.1.5 Další služby Cloud Services pro produkt IBM Trusteer Pinpoint Detect Standard a/nebo IBM Trusteer Pinpoint Detect Premium a/nebo IBM Trusteer Pinpoint Detect Standard for Retail a/nebo IBM Trusteer Pinpoint Detect Premium for Retail a/nebo IBM Trusteer Pinpoint Detect Standard for Business a/nebo IBM Trusteer Pinpoint Detect Premium for Business

a. Další služby Cloud Services dostupné pro produkt IBM Trusteer Detect Standard for Business a/nebo IBM Trusteer Pinpoint Detect Premium for Business:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
   - IBM Trusteer Digital Content Pack for Business
   - IBM Trusteer New Account Fraud for Business

b. Další služby Cloud Services dostupné pro produkt IBM Trusteer Detect Standard for Retail a/nebo IBM Trusteer Pinpoint Detect Premium for Retail:
   - IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
   - IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
   - IBM Trusteer Digital Content Pack for Retail
   - IBM Trusteer New Account Fraud for Retail

c. Další služby Cloud Services dostupné pro produkt IBM Trusteer Pinpoint Detect Standard a/nebo IBM Trusteer Pinpoint Premium:
   - IBM Trusteer Pinpoint Detect Standard Application
   - IBM Trusteer Pinpoint Detect Premium Application

d. Další služby Cloud Services dostupné pro produkt IBM Trusteer Pinpoint Detect Premium
   - IBM Trusteer Pinpoint Verify

Registrace produktů IBM Trusteer Pinpoint Detect Standard nebo IBM Trusteer Pinpoint Detect Premium nebo IBM Trusteer Pinpoint Detect Standard for Retail nebo IBM Trusteer Pinpoint Detect Premium for Retail nebo IBM Trusteer Pinpoint Detect Standard for Business nebo IBM Trusteer Pinpoint Detect Premium for Business je předpokladem pro další související služby Cloud Service uvedené v tomto oddílu.

1.1.6 Další dodatečné služby Cloud Service

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

1.2 Definice

Vlastník účtu – označuje koncového uživatele Zákazníka, který si nainstaloval software s podporou klienta, uzavřel licenční smlouvu pro koncového uživatele ("EULA") a minimálně jednou se ověřil v Maloobchodní nebo Obchodní aplikaci, pro kterou si Zákazník zaregistroval pokrytí služeb IBM Cloud Service.

Software klienta vlastníka účtu – označuje aktivační software klienta IBM Trusteer Rapport či jakýkoli jiný aktivační software zákazníka, který je poskytován s některými službami Cloud Service k instalaci na zařízení koncového uživatele.

Úvodní stránka Trusteer Splash – 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.

1.3 IBM Trusteer Rapport Cloud Services

1.3.1 IBM Trusteer Rapport II for Retail anebo IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Trusteer Rapport II Cloud Service je nová forma produktu IBM Trusteer Rapport, která pomáhá standardizovat poplatky týkající se ochrany více Aplikací a nahrazuje jednorázové poplatky při přidávání Aplikací.

Trusteer Rapport II poskytuje vrstvu ochrany proti phishingovým útokům a malwarovým útokům Man-in-the-Browser (MitB). S využitím sítě desítek milionů koncových bodů všude na světě IBM Trusteer Rapport shromažďuje informace o aktivních phishingových a malwarových útocích cílených na organizace po celém světě. IBM Trusteer Rapport aplikuje behaviorální algoritmy s cílem blokovat phishingové úroky a zabránit instalaci a běhům filtrace malwaru MitB.

Tato služba Cloud Service má metriku poplatku Vybraný účastník nebo Zařízení zákazníka. Obchodní nabídka je prodávána v balíčcích po 10 Vybraných účastnících nebo 10 Zařízeních zákazníka. Maloobchodní nabídka je prodávána v balíčcích po 100 Vybraných účastnících nebo 100 Zařízeních zákazníka.

Tato nabídka služby Cloud Service zahrnuje:

a. Trusteer Management Application ("TMA"):

   Aplikace TMA je zpřístupněna v prostředí IBM Trusteer hostovaném v cloudu, prostřednictvím kterého Zákazník (a neomezený počet jeho oprávněných pracovníků) může: (i) zobrazovat a stahovat určité úkoly vytváření sestav s daty událostí a posouzení rizik, (ii) zobrazovat konfiguraci aktivačního softwaru klienta licencovaného Vybraným účastníkům Zákazníka na základě licenční smlouvy s koncovým uživatelem ("EULA"), a to bez poplatku, a zpřístupnit takový software, který je také označován jako sada softwaru Trusteer Rapport ("Software klienta vlastníka účtu"), ke stažení do stolních počítačů a zařízení Vybraného účastníka (PC/MAC). Zákazník může nabízet Software klienta vlastníka účtu pouze pomocí Úvodní stránky Trusteer Splash 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 webovou stránku pro účely přístupu nebo použití služby Cloud Service.

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 si Zákazník zaregistroval pokrytí služeb IBM Cloud Service. 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 Splash:

   Marketingová platforma Úvodní stránky Trusteer Splash identifikuje a prodává Software klienta vlastníka účtu Vybraným účastníkům přistupujícím k Obchodním anebo Maloobchodním aplikacím Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb IBM Cloud Service. 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 svých ochranných známek, log nebo ikon k použití v souvislosti s TMA a pouze pro využití Úvodní stránky Trusteer Splash a zobrazení v Softwaru klienta vlastníka účtu nebo na vstupních stránkách hostovaných společností IBM a na webu IBM Trusteer. Každé použití poskytnutých ochranných známek, log nebo ikon bude v souladu s přiměřenými zásadami IBM týkajícími se inzerce a využití ochranných známek.

Zákazník si musí zaregistrovat službu IBM Trusteer Rapport Mandatory Service Cloud Service, pokud si přeje využít jakýkoli typ povinného nasazení Softwaru klienta vlastníka účtu.

Povinné nasazení Softwaru klienta vlastníka účtu zahrnuje mimo jiné jakýkoli typ povinného nasazení za využití libovolného mechanizmu nebo libovolného prostředku, který přímo nebo nepřímo nutí Vybraného účastníka ke stažení Softwaru klienta vlastníka účtu, nebo libovolné metody, nástroje, postupu, smlouvy

či mechanizmu, které nevytvořila nebo neschválila IBM a které byly vytvořeny k obejití licenčních požadavků tohoto povinného nasazení Softwaru klienta vlastníka účtu.

Trusteer Rapport II for Business anebo Trusteer Rapport II for Retail zahrnují ochranu pro jednu Aplikaci. Pro každou další Aplikaci by Zákazník měl získat oprávnění pro další aplikace IBM Trusteer Rapport Additional Applications.

1.3.2 Volitelné další služby Cloud Services pro produkt IBM Trusteer Rapport II for Business a/nebo IBM Trusteer Rapport II for Retail

Registrace produktu IBM Trusteer Rapport II Cloud Services je předpokladem registrace jakékoli z následujících dodatečných služeb Cloud Services. Pokud jsou služba Cloud Service označeny jako "for Business", musí být získané dodatečné služby Cloud Service také označeny jako "for Business". Pokud jsou služba Cloud Service označeny jako "for Retail", musí být získané dodatečné služby Cloud Service také označeny jako "for Retail". Zákazník bude přijímat data události od Vybraných účastníků nebo Zařízení zákazníka používajících Software klienta vlastníka účtu, kteří uzavřeli smlouvu EULA pro koncové uživatele a minimálně jednou provedli ověření v Obchodní anebo Maloobchodní aplikaci Zákazníka; konfigurace Zákazníka musí zahrnovat shromažďování ID uživatele.

1.3.3 IBM Trusteer Rapport Fraud Feeds for Business nebo IBM Trusteer Rapport Fraud Feeds for Retail

Po registraci této doplňkové služby Cloud Service může Zákazník (a neomezený počet jeho oprávněných pracovníků) používat aplikaci TMA k zobrazování, registraci a konfiguraci doručení kanálů hrozeb generovaných službou Trusteer Rapport Cloud Service. Kanály lze odesílat prostřednictvím e-mailu na určené e-mailové adresy nebo prostřednictvím SFTP jako textové soubory.

Tato nabídka má pouze metriku poplatku Vybraný účastník.

1.3.4 IBM Trusteer Rapport Phishing Protection for Business nebo IBM 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 službu Cloud Service 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.

Tato služba Cloud Service má metriku poplatku Vybraný účastník nebo Zařízení zákazníka. Obchodní nabídka je prodávána v balíčcích po 10 Vybraných účastnících nebo 10 Zařízeních zákazníka. Maloobchodní nabídka je prodávána v balíčcích po 100 Vybraných účastnících nebo 100 Zařízeních zákazníka.

Pro tuto službu Cloud Service lze získat podporu Premium na základě metriky poplatku Vybraný účastník nebo Zařízení zákazníka. Obchodní nabídka je prodávána v balíčcích po 10 Vybraných účastnících nebo 10 Zařízeních zákazníka. Maloobchodní nabídka je prodávána v balíčcích po 100 Vybraných účastnících nebo 100 Zařízeních zákazníka.

1.3.5 IBM Trusteer Rapport Mandatory Service for Business nebo IBM Trusteer Rapport Mandatory Service for Retail

Zákazník smí používat instanci marketingové platformy Úvodní stránky Trusteer Splash k povolení stahování Softwaru klienta vlastníka účtu Vybraným účastníkům přistupujícím k Obchodním anebo Maloobchodním aplikacím Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service.

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

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

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

Tato služba Cloud Service má metriku poplatku Vybraný účastník. Obchodní nabídka je prodávána v balíčcích po 10. Maloobchodní nabídka je prodávána v balíčcích po 100 Vybraných účastnících.

1.3.6 IBM Trusteer Rapport Large Redeployment anebo IBM Trusteer Rapport Small Redeployment

Zákazníci, kteří během období poskytování služby znovu nasadí své aplikace pro online bankovnictví, a vyžadují proto změny svého nasazení služby IBM Trusteer Rapport II, by si měli zakoupit službu IBM Trusteer Rapport Redeployment Cloud Service.

Nové nasazení může být vyžadováno z důvodu změny domény nebo hostující adresy URL Aplikace Zákazníkem, použití změn konfigurace úvodní stránky nebo přechodu na novou platformu online bankovnictví.

Během přechodového období nového nasazení v délce šesti měsíců má Zákazník nárok na další Aplikace (vždy po jedné aplikaci), které běží na již registrovaných Aplikacích.

IBM Trusteer Rapport Large Redeployment se vztahuje na prostředí s maximálně 20 000 uživateli a IBM Trusteer Rapport Small Redeployment se vztahuje na prostředí, kde je počet uživatelů menší nebo roven 20 000.

1.3.7 IBM Trusteer Rapport Additional Applications for Business anebo IBM Trusteer Rapport Additional Applications for Retail

Nasazení na jakékoliv další Obchodní aplikaci nad rámec první Aplikace vyžaduje pro IBM Trusteer Rapport II for Business oprávnění k IBM Trusteer Rapport Additional Applications for Business Cloud Service. IBM Trusteer Rapport II for Retail vyžaduje pro nasazení na další Maloobchodní aplikaci nad rámec první Aplikace oprávnění k IBM Trusteer Rapport Additional Applications for Retail Cloud Service.

1.4 Služby IBM Trusteer Pinpoint Cloud Service

IBM 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 anebo Maloobchodních aplikací Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service a procesů prevence podvodu.

Tato služba Cloud Service zahrnuje:

a. TMA:

   Aplikace TMA je zpřístupněna v prostředí IBM Trusteer hostovaném v cloudu, prostřednictvím kterého Zákazník (a neomezený počet jeho oprávněných pracovníků) může: (i) zobrazovat a stahovat určité úkoly vytváření sestav s daty událostí a posouzení rizik, (ii) zobrazovat, registrovat a konfigurovat doručení kanálů hrozeb generovaných z nabídek Pintpoint.

b. Webový skript nebo rozhraní API:

   Pro implementaci na webu pro účely přístupu nebo použití služby Cloud Service.

1.4.1 IBM Trusteer Pinpoint Malware Detection

V případě detekce malwaru ve službách IBM Trusteer Pinpoint Malware Detection II Cloud Services musí Zákazník postupovat podle příručky Pinpoint Best Practices Guide. Služby IBM Trusteer Pinpoint Malware Detection II Cloud Services nepoužívejte žádným způsobem, který by ovlivnil zkušenost Vybraných účastníků, ihned po detekci malwaru nebo převzetí účtu, například by umožnil ostatním propojit činnost Zákazníka s použitím nabídek IBM Trusteer Pinpoint Cloud Services (např. oznámení, zprávy, blokování zařízení nebo blokování přístupu k Obchodní anebo Maloobchodní aplikaci ihned po detekci malwaru nebo převzetí účtu).

1.4.2 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business anebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail anebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business anebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II je nová forma produktu IBM Trusteer Pinpoint Malware Detection, která pomáhá standardizovat poplatky týkající se ochrany více Aplikací a nahrazuje jednorázové poplatky při přidávání Aplikací.

Detekce připojení prohlížečů infikovaných finančním malwarem bez klienta během připojování k Obchodní anebo Maloobchodní aplikaci. Služby IBM Trusteer Pinpoint Malware Detection Cloud Service 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 anebo Obchodními aplikacemi Zákazníka.

b. Advanced Edition:

Edice Advanced Edition for Business nebo 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 anebo Maloobchodních aplikací Zákazníka.

Advanced Edition je Zákazníkovi nabízena s minimálním množstvím alespoň 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:

Edice Standard Editions for Business a/nebo Retail jsou řešení s rychlým nasazením, která poskytují základní funkce této služby Cloud Service popsané v tomto dokumentu.

Tato služba Cloud Service zahrnuje ochranu pro jednu Aplikaci. Pro každou další Aplikaci musí Zákazník získat oprávnění pro IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.4.3 Volitelné další služby Cloud Services pro produkt IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail a/nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail a/nebo IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business a/nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- Pro službu IBM Trusteer Rapport Remediation for Retail Cloud Service je jako předpoklad vyžadován produkt IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Pro službu IBM Trusteer Rapport Remediation for Business Cloud Service je jako předpoklad vyžadován produkt IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

1.4.4 IBM Trusteer Rapport Remediation for Retail anebo IBM Trusteer Rapport Remediation for Business

Cílem produktů IBM Trusteer Rapport Remediation Retail a IBM Trusteer Rapport Remediation for Business je prošetřit, napravit, zablokovat a odebrat napadení malwarem typu man-in-the-browser (MitB) z infikovaných zařízení (PC/MAC) Vybraných účastníků Zákazníka, kteří přistupují k Aplikaci Zákazníka na ad hoc bázi, kde bylo napadení malwarem MitB zjištěno daty událostí IBM Security Trusteer Pinpoint Malware Detection. Zákazník musí mít aktuální registraci produktu IBM Trusteer Pinpoint Malware Detection II, který je používán v Aplikaci Zákazníka. Zákazník smí tuto nabídku Cloud Service použít pouze ve spojení s Vybranými účastníky, kteří přistupují k Aplikaci Zákazníka, a výhradně jako nástroj, jehož cílem je prošetřit a opravit konkrétní infikované zařízení (PC/MAC) na ad hoc bázi. IBM Trusteer Rapport Remediation musí běžet na dotčených zařízeních Vybraného účastníka (PC/MAC) a tento dotčený Vybraný účastník musí uzavřít smlouvu EULA a minimálně jednou provést své ověření v Aplikaci (Aplikacích) Zákazníka a konfigurace Zákazníka musí zahrnovat shromažďování ID uživatele. Pro vyloučení pochybností se uvádí, že tato nabídka Cloud Service nezahrnuje právo na používání Úvodní stránky Trusteer Splash nebo k jiné podpoře Softwaru klienta vlastníka účtu určené pro obecné Vybrané účastníky Zákazníka.

1.4.5 IBM Trusteer Pinpoint Malware Detection Redeployment

Zákazníci, kteří během období poskytování služby znovu nasadí své aplikace pro online bankovnictví, a vyžadují proto změny svého nasazení služby IBM Trusteer Pinpoint Malware Detection II, by si měli zakoupit službu IBM Trusteer Pinpoint Malware Detection Redeployment.

Nové nasazení může být vyžadováno z důvodu změny domény nebo hostující adresy URL Aplikace Zákazníkem, převodu online Aplikace na novou technologii, přechodu na novou platformu online bankovnictví nebo přidání nového postupu přihlašování do stávající Aplikace.

Během přechodového období nového nasazení v délce šesti měsíců má Zákazník nárok na další Aplikace (vždy po jedné aplikaci), které běží na již registrovaných Aplikacích.

Nasazení na jakékoli další Maloobchodní aplikaci nad rámec první Aplikace vyžaduje pro IBM Trusteer Pinpoint Malware Detection Additional Applications For IBM Trusteer Pinpoint Malware Detection II Standard Edition nebo IBM Trusteer Pinpoint Malware Detection II Advanced Edition oprávnění k IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.4.6 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail anebo IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- Nasazení na jakékoli další Maloobchodní aplikaci nad rámec první Aplikace vyžaduje pro IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail oprávnění k IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.
- Nasazení na jakékoli další Obchodní aplikaci nad rámec první Aplikace vyžaduje pro IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business oprávnění k IBM Trusteer Pinpoint Malware Detection Additional Applications for Business.

1.5 IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Sada") je kolekce cloudových služeb, která poskytuje vrstvu ochrany proti podvodům a lze ji integrovat s dalšími produkty IBM za účelem poskytnutí řešení pro správu životního cyklu. Sada zahrnuje následující cloudové služby:

- IBM Trusteer Pinpoint Detect, jejímž cílem je detekovat a zmírňovat útoky malwaru, phishingové útoky a útoky zacílené na převzetí účtu. Službu Trusteer Pinpoint Detect lze integrovat do Obchodních anebo Maloobchodních aplikací Zákazníka, pro které si Zákazník sjednal registraci pokrytí služby Cloud Service, a do procesů prevence podvodů.
- IBM Trusteer Rapport for Mitigation, jejímž cílem je obnovit a chránit infikované koncové body.

Tyto služby Cloud Service zahrnují:

a. TMA:

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

b. Data události:

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

c. Webový skript nebo rozhraní API:

   Pro implementaci na webu pro účely přístupu nebo použití služby Cloud Service.

Osvědčené postupy pro produkt Pinpoint

V případě detekce malwaru nebo převzetí účtu musí Zákazník postupovat podle příručky Pinpoint Best Practices Guide. Služby IBM Trusteer Pinpoint Detect Cloud Service nepoužívejte žádným způsobem, který by ovlivnil zkušenost Vybraných účastníků ihned po detekci malwaru nebo převzetí účtu, například by umožnil ostatním propojit činnost Zákazníka s použitím nabídek IBM Trusteer Pinpoint Detect (např. oznámení, zprávy, blokování zařízení nebo blokování přístupu k Obchodní anebo Maloobchodní aplikaci ihned po detekci malwaru nebo převzetí účtu).

1.5.1 IBM Trusteer Pinpoint Detect Standard for Retail a/nebo IBM Trusteer Pinpoint Detect Standard for Business

Tato služba Cloud Service kombinuje služby Cloud Service IBM Trusteer Pinpoint Criminal Detection a IBM Trusteer Pinpoint Malware Detection a nabízí jedno jednotné řešení.

Toto řešení pomáhá s detekcí malwaru anebo podezřelé činnosti prohlížečů připojených k Obchodní nebo Maloobchodní aplikaci zaměřené na převzetí účtu bez klienta, s použitím ID zařízení, detekce phishingu a detekce odcizení pověření řízeného malwarem. Nabídky IBM Trusteer Pinpoint poskytují další vrstvu ochrany. 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 Zákazníkovi.

Součástí této služby Cloud Service je standardní podpora (definována v části Technická podpora níže). Pro podporu Premium si Zákazník musí zakoupit podporu Pinpoint Standard Premium Support.

Tato služba Cloud Service zahrnuje ochranu pro jednu Aplikaci. Pro každou další Aplikaci by Zákazník měl získat oprávnění pro další aplikace IBM Trusteer Pinpoint Detect Standard.

Službu si lze zakoupit v balíčcích po 100 Oprávněných účastnících nebo balíčcích po 100 Připojení. V případě, že se Zákazník rozhodne pro zakoupení služby podle Připojení, od první aplikace se uplatní poplatek za Dodatečné aplikace.

1.5.2 IBM Trusteer Pinpoint Detect Premium for Retail a/nebo IBM Trusteer Pinpoint Detect Premium for Business

Tato služba Cloud Service kombinuje služby IBM Trusteer Pinpoint Criminal Detection a IBM Trusteer Pinpoint Malware Detection a nabízí jedno jednotné řešení se snadnou integrací.

Toto řešení pomáhá s detekcí malwaru anebo podezřelé činnosti prohlížečů připojených k Obchodní nebo Maloobchodní aplikaci zaměřené na převzetí účtu bez klienta, s použitím ID zařízení, detekce phishingu a detekce odcizení pověření řízeného malwarem. Nabídky IBM Trusteer Pinpoint poskytují další vrstvu ochrany. 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 Zákazníkovi.

Služba zahrnuje rozšířenou funkčnost a služby včetně rozšířených služeb nasazení a nastavení, přizpůsobených zásad zabezpečení, služeb šetření atd. Služba zahrnuje až 200 hodin sdílených zdrojů pro služby nasazení na aplikaci a 200 hodin sdílených zdrojů pro analýzu zabezpečení na aplikaci při nastavení. Průběžné služby zahrnují 20 hodin údržby nasazení ročně na aplikaci a 100 hodin průzkumu zabezpečení na aplikaci ročně. Na případné dodatečné práce se vztahují dodatečné poplatky.

Pinpoint Detect může využívat transakce z obou kanálů: mobilního a webového. Pokud jsou zahrnuty mobilní transakce, uplatní se přesné určení dle připojení. Tato služba Cloud Service zahrnuje ochranu pro jednu Aplikaci. Pro každou další Aplikaci by Zákazník měl získat oprávnění pro další aplikace IBM Trusteer Pinpoint Detect Premium.

Součástí této služby Cloud Service je podpora Premium.

Služby IBM Trusteer Pinpoint Detect Premium for Retail and Business si lze zakoupit v balíčcích po 100 Oprávněných účastnících nebo balíčcích IBM Trusteer Pinpoint Detect Premium po 100 Připojeních. V případě, že se Zákazník rozhodne pro zakoupení služby podle Připojení, od první aplikace se uplatní poplatek za Dodatečné aplikace.

Pinpoint Detect Policy Manager:

Správce Policy Manager je obsažen ve službě Pinpoint Detect Premium a je k dispozici v prostředí IBM Trusteer hostovaném v cloudu, díky kterému Zákazník (a neomezený počet jeho oprávněných pracovníků) může: (i) navrhovat, testovat a nasazovat do logiky produktivního prostředí ke zjištění podvodné činnosti, (ii) navrhovat sestavy a ovládací panely dashboard a (iii) zobrazovat, konfigurovat a nastavovat zásady zabezpečení a zásady ke zjištění podezřelé činnosti u aplikace Zákazníka.

Konzultační služby jsou nezbytné pro aktivaci správce Policy Manager a požadovanou nadstandardní hloubku podpory. Podrobnosti o konzultačních službách budou vymezeny samostatně v popisu práce.

Pokud dojde k aktivaci správce Policy Manager, společnost IBM si vyhrazuje právo přístupu do prostředí Zákazníka pro účely podpory při úpravách zásad Zákazníka v rámci řešení zásadních problémů, které souvisejí se změnou zásad.

Zákazník se zavazuje chránit veškerá data, která jsou dostupná prostřednictvím správce Policy Manager, proti zneužití.

Když je aktivován správce Policy Manager, Zákazník je povinen dodržovat pokyny společnosti IBM pro stanovení pravidel, jak je uvedeno v dokumentaci. Zákazník potvrzuje, že společnost IBM nenese odpovědnost za žádnou situaci, která může vzniknout v důsledku nedodržení těchto doporučení na straně Zákazníka.

Jakékoliv problémy se stabilitou anebo zhoršením služby, které případně vzniknou v důsledku chybné konfigurace správce Policy Manager Zákazníkem, nebudou považovány za Odstávku pro potřeby výpočtu SLA.

1.5.3 Volitelné služby pro IBM Trusteer Pinpoint Detect Standard anebo IBM Trusteer Pinpoint Detect Premium

Pro služby Cloud Service uvedené v tomto oddíle platí prerekvizita oprávnění pro IBM Trusteer Pinpoint Detect Premium nebo IBM Trusteer Pinpoint Detect Standard.

1.5.4 IBM Trusteer Rapport for Mitigation for Retail anebo IBM Trusteer Rapport for Mitigation for Business

- Cílem služby IBM Trusteer Rapport for Mitigation for Retail je prošetřit, napravit, zablokovat a odstranit infekce malwarem z napadených zařízení (PC/MAC) Vybraných účastníků Zákazníka, kteří přistupují k Maloobchodní aplikaci Zákazníka na ad hoc bázi, v případech, kdy data událostí IBM Trusteer Pinpoint Detect Premium nebo IBM Trusteer Pinpoint Detect Standard zjistila napadení malwarem. Zákazník musí mít ve své Maloobchodní aplikaci spuštěnu aktuální registraci produktu IBM Trusteer Pinpoint Detect Premium nebo IBM Trusteer Pinpoint Detect Standard. Zákazník smí tuto službu Cloud Service 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. Produkt IBM Trusteer Rapport for Mitigation for Retail musí být na takovém dotčeném zařízení Vybraného účastníka (PC/MAC) spuštěn a takový dotčený Vybraný účastník musí přijmout smlouvu EULA, minimálně jednou se přihlásit k Maloobchodní aplikaci (Maloobchodním aplikacím) Zákazníka a konfigurace Zákazníka musí zahrnovat kolekci ID uživatele. Pro vyloučení pochybností se uvádí, že tato služba Cloud Service nezahrnuje právo na používání Úvodní stránky Trusteer Splash nebo k jiné podpoře Softwaru klienta vlastníka účtu určené pro obecné Vybrané účastníky Zákazníka.
- Cílem služby IBM Trusteer Rapport for Mitigation for Business je prošetřit, napravit, zablokovat a odstranit infekce malwarem z napadených zařízení (PC/MAC) Vybraných účastníků Zákazníka, kteří přistupují k Obchodní aplikaci Zákazníka na ad hoc bázi, v případech, kdy data událostí IBM Trusteer Pinpoint Detect Premium nebo IBM Trusteer Pinpoint Detect Standard zjistila napadení malwarem. Zákazník musí mít ve své Obchodní aplikaci spuštěnu aktuální registraci produktu IBM Trusteer Pinpoint Detect Premium nebo IBM Trusteer Pinpoint Detect Standard. Zákazník smí tuto službu Cloud Service použít pouze ve spojení s Vybranými účastníky, kteří přistupují k Obchodní aplikaci Zákazníka, a výhradně jako nástroj, jehož cílem je prošetřit a opravit konkrétní infikované zařízení (PC/MAC) na ad-hoc bázi. Produkt IBM Trusteer Rapport for Mitigation for Business musí být na takovém dotčeném zařízení Vybraného účastníka (PC/MAC) spuštěn a takový dotčený Vybraný účastník musí přijmout smlouvu EULA, minimálně jednou se přihlásit k Obchodní aplikaci (Obchodním aplikacím) Zákazníka a konfigurace Zákazníka musí zahrnovat kolekci ID uživatele. Pro vyloučení pochybností se uvádí, že tato služba Cloud Service nezahrnuje právo na používání Úvodní stránky Trusteer Splash nebo k jiné podpoře Softwaru klienta vlastníka účtu určené pro obecné Vybrané účastníky Zákazníka.

1.5.5 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail a/nebo IBM Trusteer Pinpoint Detect Standard Additional Applications for Business a/nebo IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail a/nebo IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

Služba zahrnuje až 200 hodin sdílených zdrojů pro služby nasazení na aplikaci a 200 hodin sdílených zdrojů pro analýzu zabezpečení na aplikaci při nastavení. Průběžné služby zahrnují 20 hodin údržby nasazení ročně na aplikaci a 100 hodin průzkumu zabezpečení na aplikaci ročně.

- Nasazení IBM Trusteer Pinpoint Detect Standard for Retail na jakékoli další Maloobchodní aplikaci nad rámec první Aplikace vyžaduje oprávnění pro IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.
- Nasazení IBM Trusteer Pinpoint Detect Standard for Business na jakékoli další Obchodní aplikaci nad rámec první Aplikace vyžaduje oprávnění pro IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.
- Nasazení IBM Trusteer Pinpoint Premium for Retail na jakékoli další Maloobchodní aplikaci nad rámec první Aplikace vyžaduje oprávnění pro IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.
- Nasazení IBM Trusteer Pinpoint Premium for Business na jakékoli další Obchodní aplikaci nad rámec první Aplikace vyžaduje oprávnění pro IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

1.5.6 IBM Trusteer Pinpoint Detect Standard Application a/nebo IBM Trusteer Pinpoint Detect Premium Application

Tato služba platí pro webový i mobilní kanál.

Služba zahrnuje až 200 hodin sdílených zdrojů pro služby nasazení na aplikaci a 200 hodin sdílených zdrojů pro analýzu zabezpečení na aplikaci při nastavení. Průběžné služby zahrnují 20 hodin údržby nasazení ročně na aplikaci a 100 hodin průzkumu zabezpečení na aplikaci ročně.

- Nasazení IBM Trusteer Pinpoint Detect Standard vyžaduje oprávnění k IBM Trusteer Pinpoint Detect Standard Application pro každou Aplikaci.
- Nasazení IBM Trusteer Pinpoint Premium vyžaduje oprávnění k IBM Trusteer Pinpoint Detect Premium Application pro každou Aplikaci.

1.5.7 IBM Trusteer Pinpoint Detect Standard Redeployment anebo IBM Trusteer Pinpoint Detect Premium Redeployment

Zákazníci, kteří během období poskytování služby znovu nasadí své aplikace pro online bankovnictví, a vyžadují proto změny svého nasazení služby IBM Trusteer Pinpoint Detect, by si měli zakoupit službu IBM Trusteer Pinpoint Detect Redeployment.

Nové nasazení může být vyžadováno z důvodu změny domény nebo hostující adresy URL Aplikace Zákazníkem, převodu online Aplikace na novou technologii, přechodu na novou platformu online bankovnictví nebo přidání nového postupu přihlašování do stávající Aplikace.

Během přechodového období nového nasazení v délce šesti měsíců má Zákazník nárok na další Aplikace (vždy po jedné aplikaci), které běží na již registrovaných Aplikacích.

1.5.8 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support a/nebo IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Zákazník, který si zakoupí Pinpoint Detect Standard Cloud Service, si může zakoupit i službu Premium Support. Rozsah služeb Premium Support je uveden v části 4 níže.

1.5.9 IBM Trusteer Digital Content Pack for Retail a/nebo IBM Trusteer Digital Content Pack for Business

Služba IBM Trusteer Digital Content Pack umožňuje analytikům zabezpečení integrovat nové modely podvodů při zachování plné podpory pro tvorbu a úpravy ad hoc modelů pro reakci na vznikající hrozby. Zahrnuje rozsáhlou sadu pravidel, poznatků a zásad, které lze zakoupit jako dodatečnou nebo nedílnou součást řešení. Balíček Digital Content Pack pomáhá dále zúžit integraci mezi funkcemi prevence digitálních podvodů Trusteer a bezpečnějšími bezhotovostními platebními kanály IBM Safer Payments. Efektivním využitím zabudovaných pravidel a specifické obchodní logiky umožňuje balíček Digital Content Pack bankám a dalším finančním institucím dále posílit stávající funkce detekce a prevence podvodů.

Služba IBM Trusteer Digital Content Pack for Retail je k dispozici v balíčcích po 100 Vybraných účastnících. Služba IBM Trusteer Digital Content Pack for Business je k dispozici v balíčcích po 10 Vybraných účastnících.

Konzultační služby se vyžadují pro integraci Digital Content Pack with Pinpoint Detect a IBM Safer Payments i pro služby podpory, které vyžadují vysokou pozornost. Konzultační služby jsou nakupovány samostatně v souladu s individuálním popisem služeb.

1.5.10 IBM Trusteer New Account Fraud for Retail anebo IBM Trusteer New Account Fraud for Business

Tato služba dostupná pro předplatitele Pinpoint je určena pro zjišťování anomálií, označení podezřelých činností a včasné generování výstrah v procesu vytváření nového účtu. Služba monitoruje nové účty pro identifikaci nové činnosti související s podvody po vytvoření účtu nebo profilování čerstvě založeného účtu pro poskytnutí včasných varovných znamení, že nový účet může být falešný účet nebo může být používán k podvodům, a to prostřednictvím sestav o využití, které jsou k dispozici v TMA.

Služby IBM Trusteer New Account Fraud for Retail a IBM Trusteer New Account Fraud for Business jsou k dispozici v balících po 10 voláních rozhraní API.

1.5.11 IBM Trusteer Pinpoint Verify

Zákazník musí mít před registrací této služby Cloud Service aktuální registraci produktu IBM Trusteer Pinpoint Detect Premium.

Tato služba Cloud Service poskytuje funkce pro výzvu uživatelům k zadání druhého ověřovacího faktoru pro ověření jejich identity při přístupu k digitální službě. Je k dispozici pro Pinpoint Detect Premium za účelem poskytnutí druhého ověřovacího faktoru pro chráněné aplikace. Rozhodnutí o tom, kdy vyzvat uživatele k ověření druhým faktorem, je odvozeno od chráněné aplikace a může vycházet z doporučení získaných z platformy Pinpoint Detect Premium nebo jakýchkoliv jiných zásad stanovených chráněnou aplikací.

1.6 IBM Trusteer Pinpoint Assure

Tato služba označuje příznakem podezřelé činnosti a generuje varování v procesu vytváření/registrace nového účtu. Služba monitoruje proces registrace účtu pro identifikaci činnosti související s podvodem, aby poskytla včasné varování, že nový účet může být falešný účet nebo může být používán k podvodům, a to prostřednictvím sestav o využití, které jsou k dispozici v TMA.

IBM Trusteer Pinpoint Assure je k dispozici v balíčcích po 100 připojeních.

1.6.1 Volitelné služby pro IBM Trusteer Pinpoint Assure

1.6.2 IBM Trusteer Pinpoint Assure Application

Nasazení IBM Trusteer Pinpoint Assure u libovolné Aplikace vyžaduje oprávnění k IBM Trusteer Pinpoint Assure Application.

IBM Trusteer Pinpoint Assure si lze zakoupit pro aplikaci.

1.6.3 IBM Trusteer Mobile Carrier Intelligence a/nebo IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Zákazník musí mít před registrací k této službě Cloud Service spuštěnu aktuální registraci produktu IBM Trusteer Pinpoint Assure nebo IBM Trusteer Pinpoint Detect.

Tato služba Cloud Service rozšiřuje produkty IBM Trusteer Pinpoint Assure a/nebo IBM Trusteer Pinpoint Detect poskytnutím dalších informací a kontextu o mobilních číslech poskytovaných některé z těchto služeb Cloud Services, což pomáhá určit riziko podvodu u dané relace. Zákazník se může dotazovat služby Cloud Service, aby zjistil charakteristiky daného mobilního čísla, např. informace o operátorovi přidružené k danému číslu.

Údaje poskytované touto službou Cloud Service týkající se mobilních čísel ("Mobile Intelligence") mohou být použity pouze pro interní účely Zákazníka a mohou být uchovávány pouze po dobu třiceti (30) dnů. Po uplynutí této doby musí Zákazník znovu provést dotaz na službu Cloud Service ohledně stejného mobilního čísla, aby získal pro dané číslo údaje Mobile Intelligence, a nesmí prostě jen znovu použít Mobile Intelligence z předchozího dotazu. Zákazník nesmí jakékoli údaje Mobile Intelligence ukládat do mezipaměti, s výjimkou výše povolených možností, opakovaně je používat nebo používat ve spojení, zcela nebo částečně, s jakýmkoliv dolováním dat nebo pro archivaci.

1.7 IBM Trusteer Remotely Delivered Services

Služby IBM Trusteer Remotely Delivered Services jsou k dispozici jako volitelný doplněk pro služby Pinpoint Detect Premium a Pinpoint Assure Cloud Services.

1.7.1 IBM Trusteer Project Management and Consultancy Services

Tato služba poskytuje až 200 hodin poradenských služeb, během nichž společnost IBM poskytne některé nebo všechny následující položky:

a. Služby počátečního nastavení: častá pravidelná setkání, služby řízení projektu

b. Správce zásad: průběžná podpora

Nabídku lze zakoupit podle Sjednaných služeb.

1.7.2 IBM Trusteer Security Research Consultancy Services

Tato konzultační služba zahrnuje až 200 hodin sdíleného prostředku pro analýzu zabezpečení k poskytování dodatečných služeb navíc vedle definovaného řešení a prémiové podpory (v příslušných případech) a zahrnuje:

a. Rozšířené vyhledávání podvodů: týdenní setkání a školení.

b. Podpora vydání Zákazníka s vysokou prioritou

c. Průběžné přizpůsobené zásady vyšetřování a podpory

Nabídku lze zakoupit podle Sjednaných služeb.

1.7.3 IBM Trusteer Training Services

Tato konzultační služba je určena k poskytování dodatečných služeb navíc vedle definovaného řešení a prémiové podpory (v příslušných případech) a zahrnuje služby školení o portfoliu Trusteer pro zaměstnance Zákazníka.

Nabídku lze zakoupit podle Sjednaných služeb.

1.8 Služby IBM Trusteer Mobile Cloud Service

1.8.1 IBM Trusteer Mobile SDK for Business nebo IBM Trusteer Mobile SDK for Retail

Služby IBM Trusteer Mobile SDK Cloud Service 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 služeb Cloud Service, posouzení rizika mobilních zařízení a ochraně proti pharmingu. Zabezpečená detekce Wi-Fi je k dispozici pouze pro platformu Android.

Služby IBM Trusteer Mobile SDK Cloud Service 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 Trusteer, a "Komponentu běhového prostředí" nebo "Opakovaně šiřitelný" vlastní kód generovaný sadou IBM Trusteer Mobile SDK, který lze vložit a integrovat do chráněných samostatných mobilních aplikací sytému iOS nebo Android Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service. ("Integrované mobilní aplikace Zákazníka").

Produkt IBM Trusteer Mobile SDK for Retail je k dispozici v balíčcích po 100 Vybraných účastnících nebo balíčcích po 100 Zařízeních Zákazníka a produkt IBM 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 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 tohoto Popisu služeb; 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 jinému účelu

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 výhradní odpovědnost za vývoj, testování a podporu Integrované mobilní aplikace Zákazníka. 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 služeb Cloud Service.

IBM nezaručuje, že jakákoli aplikace nebo výstup vytvářený pomocí mobilních nástrojů obsažených v sadě IBM Security Mobile SDK bude fungovat a spolupracovat nebo bude kompatibilní s danou konkrétní platformou mobilního operačního systému nebo mobilním zařízením.

Zdrojové komponenty a vzorové materiály - IBM Trusteer Mobile SDK může zahrnovat určité komponenty ve formě zdrojového kódu ("Zdrojové komponenty") nebo jiné materiály, které jsou označeny jako Vzorové materiály. Zákazník smí kopírovat a upravovat Zdrojové komponenty a Vzorové materiály pouze pro interní účely, za předpokladu, že toto užívání splňuje limity licenčních práv podle této Smlouvy, avšak pod podmínkou, že Zákazník nesmí pozměňovat ani odstraňovat žádné informace o autorských právech nebo výhrady autorských práv, které jsou uvedeny ve Zdrojových komponentách či Vzorových materiálech. IBM poskytuje Zdrojové komponenty a Vzorové materiály bez závazku podpory a "JAK JSOU". Upozorňujeme, že Zdrojové komponenty nebo Vzorové materiály jsou poskytovány výhradně jako příklad implementace Integrovatelného obsahu do CIMA; Zdrojové komponenty a Vzorové materiály nemusejí být kompatibilní s vývojovým prostředím Zákazníka a Zákazník nese výhradní odpovědnost za testování a implementaci Integrovatelného obsahu do CIMA.

2. Ochrana obsahu a údajů

Datový list zpracování a ochrany údajů (Datový list) poskytuje specifické informace o službě Cloud Service týkající se typu Obsahu, který je povoleno zpracovávat, využívaných činností vztahujících se ke zpracování, funkcí ochrany údajů a specifických aspektů uchovávání a vrácení Obsahu. Veškeré detaily nebo vysvětlení a podmínky, včetně povinností Zákazníka, vztahující se k využívání služby Cloud Service a případných prvků ochrany dat jsou definovány v tomto oddíle. K využívání služby Cloud Service Zákazníkem se může vztahovat i více Datových listů, v závislosti na možnostech zvolených Zákazníkem. Datové listy mohou být dostupné pouze v angličtině, nikoli v místním jazyce. Bez ohledu na jakoukoliv místní zákonnou praxi nebo zvyklosti strany potvrzují, že rozumí angličtině a souhlasí s jejím využitím jako vhodného jazyka pro získání a používání služeb Cloud Service. Následující Datové listy platí pro službu Cloud Service a její dostupné možnosti. Zákazník potvrzuje, že i) společnost IBM smí dle potřeby a okolností upravit Datové listy dle vlastního uvážení a ii) takové změny budou mít přednost před předchozími verzemi. Účelem jakékoliv změny Datových listů bude i) zlepšit nebo vyjasnit stávající závazky, ii) zachovat soulad s aktuálně platnými normami a platnými právními předpisy nebo iii) upravit další závazky. Žádné změny Datových listů nebudou podstatným způsobem snižovat ochranu dat služby Cloud Service.

Odkaz(y) na příslušné Datové listy:

IBM Trusteer Mobile SDK

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

IBM Trusteer Mobile Secure Browser

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

IBM Trusteer Pinpoint Assure

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

IBM Trusteer Pinpoint Criminal Detect

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

IBM Trusteer Pinpoint Detect

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

IBM Trusteer Pinpoint Malware Detection

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

IBM Trusteer Rapport

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

IBM Trusteer Pinpoint Verify

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

(Datový list IBM Cloud Identity Verify odráží IBM Trusteer Pinpoint Verify)

Zákazník je povinen učinit nezbytné kroky za účelem objednání, aktivace nebo používání dostupných funkcí ochrany údajů pro službu Cloud Service a přijímá odpovědnost za využívání služeb Cloud Service, pokud Zákazník tyto kroky, včetně splnění zákonných požadavků na ochranu údajů nebo jiných zákonných požadavků týkajících se Obsahu, neučiní.

Dodatek o zpracování údajů (Data Processing Addendum, DPA) společnosti IBM na adrese http://ibm.com/dpa a Přílohy DPA se uplatní pro tuto Smlouvu a odkazuje se na ně jako na její součást, pokud se na osobní údaje zahrnuté v Obsahu vztahuje Evropské obecné nařízení o ochraně údajů (EU/2016/679) (GDPR). Příslušný Datový list pro tuto službu Cloud Service bude sloužit jako Dodatek DPA. Pokud se uplatňuje DPA, platí závazek společnosti IBM zasílat oznámení o změnách Dílčím zpracovatelům a právo Zákazníka vznášet námitky proti těmto změnám dle ustanovení DPA.

2.1 EULA a základ pro zpracování údajů Subjektů údajů

Pro služby IBM Trusteer Rapport Cloud Services (včetně Rapport Remediation nebo Rapport for Mitigation v případě nasazení ve spojení se službami Pinpoint Cloud Services):

Pokud nebude dohodnuto jinak a v souladu se základem pro zpracování, který Zákazník nezávisle vytvořil, Zákazník opravňuje IBM k tomu, aby poskytla Licenční smlouvu koncového uživatele, která je dostupná na adrese https://www.trusteer.com/support/end-user-license-agreement, aby IBM mohla shromažďovat a zpracovávat informace nezbytné pro poskytování služeb Cloud Services.

2.2 Využití údajů

IBM nepoužije ani nesdělí výsledky pocházející z používání služby Cloud Service Zákazníkem, které jsou jedinečné vzhledem k vašemu Obsahu (Poznatky) nebo jinak identifikují Zákazníka. IBM je však oprávněna využít Obsah a další informace (s výjimkou Poznatků), které vyplynou z Obsahu v průběhu poskytování předmětu služby Cloud Service, k odstranění osobních identifikátorů tak, aby již nadále nebylo možné osobní údaje přiřadit konkrétnímu jednotlivci bez uplatnění dalších informací. IBM použije tyto údaje pouze pro účely průzkumů, testování a vývoje nabídek.

2.3 Zpracování a ukládání dat

2.3.1 Informace o dodatečném místě zpracování

Pro služby Trusteer Pinpoint Verify jsou všechna místa hostování a zpracování stanovená v příslušném Datovém listu.

Pro všechny další služby poskytované prostřednictvím německého datového střediska společnost IBM omezí zpracování Osobních údajů na zemi smluvního subjektu společnosti IBM a následující země: Německo, Izrael, Irsko, Nizozemsko a jakékoli dodatečné země uvedené v příslušném datovém listě pro Nezávislé dílčí zpracovatele IBM.

Pro všechny další služby poskytované prostřednictvím japonského datového střediska společnost IBM omezí zpracování Osobních údajů na zemi smluvního subjektu společnosti IBM a následující země: Japonsko, Izrael, Irsko a jakékoli dodatečné země uvedené v příslušném datovém listě pro Nezávislé dílčí zpracovatele IBM.

Pro všechny další služby poskytované prostřednictvím datového střediska v USA společnost IBM omezí zpracování Osobních údajů na zemi smluvního subjektu společnosti IBM a následující země: USA, Izrael, Irsko, Singapur, Austrálie a jakékoli dodatečné země uvedené v příslušném datovém listě pro Nezávislé dílčí zpracovatele IBM.

Služby podpory a údržby účtu IBM Trusteer mohou být rovněž poskytovány dle potřeby a základě dostupnosti příslušného personálu IBM, místě Zákazníka a datového střediska, kde jsou data hostována.

2.3.2 Údaje Vlastníka účtu

Údaje Vlastníka účtu budou zpracovány v oblasti, ve které Vlastník účtu původně nainstaloval Software klienta vlastníka účtu. To znamená, že obsah Vlastníka účtu může být zpracováván v původní oblasti i v oblasti odsouhlasené Zákazníkem.

2.3.3 Integrovaná řešení

Pro účely vysvětlení se uvádí, že vzhledem k tomu, že Trusteer Fraud Protection je integrované řešení; pokud Zákazník ukončí některou z těchto služeb Cloud Services, IBM si může uchovat data Zákazníka pro účely poskytování zbývajících služeb Cloud Services Zákazníkovi v souladu s tímto Popisem služby.

3. Dohoda o úrovni služeb

IBM poskytuje pro službu Cloud Service následující Dohodu o úrovni služeb, jak je uvedeno v Dokumentu o oprávnění (Proof of Entitlement). Dohoda o úrovni služeb nepředstavuje záruku. Dohoda o úrovni služeb je k dispozici pouze pro Zákazníka a vztahuje se pouze na používání v produktivních prostředích.

3.1 Kredity za porušení úrovně dostupnosti služeb

Zákazník musí u IBM střediska technické podpory zaregistrovat tiket podpory se Závažností 1 do 24 hodin od okamžiku, kdy poprvé zjistil, že událost měla dopad na dostupnost služby Cloud Service. Zákazník musí s IBM přiměřeně spolupracovat při diagnostice a řešení problémů.

Nárok na tiket podpory za nesplnění Dohody o úrovni služeb musí být předložen do tří pracovních dní od konce smluvního měsíčního období. Kompenzací za platný nárok týkající se Dohody o úrovni služeb bude dobropis vydaný oproti budoucí faktuře za službu Cloud Service na základě doby, během které nebylo zpracování produktivního systému pro službu Cloud Service k dispozici ("Odstávka"). Odstávka se měří od okamžiku, kdy Zákazník nahlásí událost, do okamžiku obnovení Cloud Service a nezahrnuje čas související s plánovanou nebo nahlášenou odstávkou v rámci údržby, příčinami mimo kontrolu IBM, problémy s obsahem, technologií Zákazníka nebo třetí osoby, návrhy nebo pokyny, nepodporovanými konfiguracemi systému a platformami nebo jinými chybami Zákazníka či incidentem zabezpečení způsobeným Zákazníkem nebo testováním zabezpečení Zákazníka. IBM bude aplikovat nejvyšší použitelnou kompenzaci vycházející ze souhrnné dostupnosti služby Cloud Service dosažené během každého smluvního měsíčního období, jak je uvedeno v tabulce níže. Celková kompenzace vztahující se k jakémukoliv smluvnímu měsíčnímu období nesmí přesáhnout 10 procent z jedné dvanáctiny (1/12) ročního poplatku za službu Cloud Service.

3.2 Úrovně služeb

Dostupnost služby Cloud Service v průběhu smluvního měsíčního období

Dostupnost v průběhu smluvního měsíčního období	Kompenzace (% měsíčního registračního poplatku* za smluvní měsíční období, za které je uplatňován nárok)
<99,9%	2 %
< 99,0 %	5 %

Dostupnost v průběhu smluvního měsíčního období	Kompenzace (% měsíčního registračního poplatku* za smluvní měsíční období, za které je uplatňován nárok)
< 95,0 %	10 %

* Pokud byla služba Cloud Service získána od Obchodního partnera IBM, bude měsíční registrační poplatek vypočítán na základě aktuálního ceníku pro Cloud Service, který je platný pro smluvní měsíční období, na které se nárok vztahuje, se slevou 50 %. IBM Zákazníkovi přímo poskytne slevu.

Úrovně služeb a související Kredity kompenzací jsou měřeny odděleně pro každou službu Cloud Service a Aplikaci Zákazníka.

Při výpočtu kreditů SLA pro službu Cloud Service pro oprávnění Aplikací se Dostupnost vypočte na základě následujících pokynů:

- Každé Aplikaci bude přidělen vážený podíl zjištěného počtu objemu relací během smluvního měsíce.
- Odstávky jednotlivých služeb Cloud Service pro každou Aplikaci se budou akumulovat samostatně pro smluvní měsíc.

Následuje příklad výpočtu za jeden měsíc činnosti a souvisejících vah. Slouží pouze k ilustračním účelům:

Maloobchodní aplikace	Podíl z celkového počtu relací za příslušný smluvní měsíc	Celková doba odstávky za smluvní měsíc	Vážené minuty odstávky
Maloobchodní aplikace A	40 %	300 minut	40 % x. 300 minut = 120 minut
Maloobchodní aplikace B	20 %	250 minut	20 % x 250 minut = 50 minut
Maloobchodní aplikace C	40 %	150 minut	40 % x 150 minut = 60
			Celkový počet vážených minut odstávky = 230

Procento dostupnosti se vypočítá jako: celkový počet minut v rámci smluvního měsíčního období minus celkový počet vážených minut Odstávky za smluvní měsíční období, děleno celkovým počtem minut za smluvní měsíční období. Příklad vzorového výpočtu na základě výše uvedených vah je následující:

Celkem 43 200 minut za 30denní Smluvní měsíční období - 230 vážených minut odstávky = 42 970 minut _____ Celkem 43 200 minut	Kredity za porušení úrovně dostupnosti služeb = 2 % pro 99,4% dostupnost během smluvního měsíčního období

4. Technická podpora

Technická podpora pro služby Cloud Service je Zákazníkovi a jeho Vybraným účastníkům poskytována s cílem poskytnout jim asistenci při užívání služeb Cloud Service.

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 službu Cloud Service je za dodatečný poplatek k dispozici registrace podpory Premium, a to s výjimkou produktů **IBM Trusteer Mobile SDK Cloud Services** a **IBM Trusteer Rapport Mandatory Service Cloud Services**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital Content Pack** a **IBM Trusteer Mobile Carrier Intelligence**. Obraťte se na Prodejního zástupce nebo Obchodního partnera IBM.

Standardní podpora:

- Podpora poskytovaná od 8:00 do 17:00 místního času.
- Zákazníci a jejich Vybraní účastníci mohou odesílat záznamy požadavku podpory elektronicky podle příručky podpory SaaS IBM na adrese https://www.ibm.com/software/support/saas_support_guide.html.
- Zákazníci naleznou oznámení, dokumenty, sestavy jednotlivých případů a časté dotazy na portálu zákaznické podpory na adrese: http://www-01.ibm.com/software/security/trusteer

Podpora Premium:

- Nepřetržitá podpora pro všechny úrovně závažnosti.
- Zákazníci mohou podporu získat přímo telefonicky a prostřednictvím zpětného volání.
- 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, sestavy jednotlivých případů a časté dotazy na portálu zákaznické podpory na adrese: http://www.ibm.com/software/security/trusteer/support/.
- Volby a podrobnosti podpory naleznete v příručce podpory SaaS (software as a service) IBM dostupné na adrese https://www.ibm.com/software/support/saas_support_guide.html.

5. Oprávnění a informace o fakturaci

5.1 Metriky poplatků

Služba Cloud Service je poskytována v rámci metriky poplatků uvedené v Transakčním dokumentu:

- Sjednaná služba je měrnou jednotkou, na jejímž základě lze získat služby. Sjednaná služba sestává z odborných služeb a/nebo ze služeb v oblasti vzdělávání týkajících se služby Cloud Service. Je nutno získat dostatečný počet oprávnění, který bude pokrývat každou Sjednanou službu.
- Vybraný účastník je měrnou jednotkou, na jejímž základě lze získat službu Cloud Service. Vybraným účastníkem je každá fyzická nebo právnická osoba, která je způsobilá k účasti na jakémkoli programu poskytování služeb, který je spravován nebo sledován prostřednictvím služby Cloud Service. Je nutno získat dostatečný počet oprávnění, který bude pokrývat všechny Vybrané účastníky spravované nebo sledované v rámci Cloud Service během období měření specifikovaného v Transakčním dokumentu Zákazníka.

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

  Pro účely oprávnění těchto služeb Cloud Service je Vybraný účastník koncový uživatel Zákazníka s přihlašovacími pověřeními k Obchodní nebo Maloobchodní aplikaci Zákazníka.
- Zařízení Zákazníka je měrnou jednotkou, na jejímž základě lze získat službu Cloud Service. 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 v oblasti zpracování nebo může být programovatelné, aby uživateli umožňovalo výkon práce. Zákazník je povinen získat oprávnění pro každé Zařízení Zákazníka, které spouští službu Cloud Service, poskytuje data pro službu Cloud Service, používá služby poskytované službou Cloud Service nebo jinak přistupuje ke službě Cloud Service během období měření uvedeného v Transakčním dokumentu Zákazníka.
- Aplikace je měrnou jednotkou, na jejímž základě lze získat službu Cloud Service. Aplikace je softwarový program s jedinečným názvem. Pro každou Aplikaci zpřístupněnou a používanou během období měření uvedeného v Zákazníkově Dokumentu o oprávnění (Proof of Entitlement) nebo Transakčním dokumentu je nutno získat dostatečný počet oprávnění.

  Pro účely této služby Cloud Service představuje Aplikace jednu Obchodní nebo Maloobchodní aplikaci Zákazníka.

- Volání API je měrnou jednotkou, na jejímž základě lze získat službu Cloud Service. Volání API je vyvolání služby Cloud Service prostřednictvím programového rozhraní. Je nutno získat takový počet oprávnění, který bude postačující pro pokrytí celkového počtu Volání API, zaokrouhleného nahoru na nejbližších deset, během období měření uvedeného v Zákazníkově Dokumentu o oprávnění (Proof of Entitlement) nebo Transakčním dokumentu.
- Připojení je měrnou jednotkou, na jejímž základě lze získat službu Cloud Service. Připojení je odkaz nebo spojení databáze, aplikace, serveru nebo jiného typu zařízení ke službě Cloud Service. Je nutno získat takový počet oprávnění, který bude postačující pro pokrytí celkového počtu Připojení, jež byla nebo jsou vytvořena ke Cloud Service během období měření uvedeného v Zákazníkově Dokumentu o oprávnění (Proof of Entitlement) nebo Transakčním dokumentu.

  Pro účely této služby Cloud Service je Připojení relací nebo tokem v aplikaci Zákazníka.

5.2 Poplatky za překročení limitu

Pokud skutečné používání služby Cloud Service během období měření překračuje oprávnění uvedená v Dokumentu o oprávnění (Proof of Entitlement), bude poplatek za překročení účtován v sazbě stanovené v Transakčním dokumentu v měsíci následujícím po takovém překročení.

5.3 Fakturační frekvence

Na základě vybrané fakturační frekvence bude IBM fakturovat Zákazníkovi splatné poplatky na začátku období fakturační frekvence, s výjimkou typu poplatků za překročení a použití, které budou fakturovány zpětně.

6. Smluvní období a možnost obnovení

Smluvní období pro poskytování služby Cloud Service začíná datem, kdy IBM Zákazníkovi oznámí, že mu byl udělen přístup ke službě Cloud Service, jak je uvedeno v Dokumentu o oprávnění (Proof of Entitlement). Dokument o oprávnění určí, zda se Cloud Service obnovuje automaticky, je používána nepřetržitě, nebo zda je po uplynutí smluvního období ukončena.

V případě automatického obnovení platí, že pokud Zákazník neposkytne 90 dní před datem ukončení období písemné oznámení o záměru nabídku neobnovit, bude služba Cloud Service automaticky obnovena na období uvedené v Dokumentu o oprávnění (Proof of Entitlement). Obnovení podléhá ročnímu zvýšení ceny dle ustanovení cenové nabídky. V případě, že k automatickému obnovení dojde po doručení oznámení IBM o stažení služby Cloud Service, doba obnovení skončí ke konci aktuálního období prodloužení nebo k ohlášenému datu stažení, podle toho, co nastane dříve.

V případě průběžného používání bude služba Cloud Service dále dostupná na měsíční bázi, dokud Zákazník neposkytne 90 dní předem písemnou výpověď. Po ukončení takového 90denního období zůstane služba Cloud Service k dispozici do konce kalendářního měsíce.

7. Dodatečné podmínky

7.1 Obecné

Zákazník souhlasí, že IBM může Zákazníka veřejně označovat jako odběratele služby Cloud Service v reklamních nebo marketingových sděleních.

Zákazník nesmí používat služby Cloud Services samostatně nebo v kombinaci s jinými službami či produkty, na podporu kterékoliv z níže uvedených vysoce rizikových činností: návrh, výstavba, řízení nebo údržba jaderných zařízení, systémů hromadné přepravy, systémů řízení automobilů, systémů řízení letecké dopravy, zbrojních systémů nebo letecké navigace či komunikace; nebo jakékoliv jiné činnosti, při které by mohlo selhání služby Cloud Service způsobit vznik závažného rizika smrti nebo vážného úrazu.

7.2 Aktivační software

Služba Cloud Service vyžaduje použití aktivačního softwaru, který si Zákazník stáhne do svých systémů pro usnadnění používání služby Cloud Service. Zákazník je oprávněn používat aktivační software výhradně ve spojení s užíváním služby Cloud Service. Aktivační software se poskytuje "tak, jak je".

7.3 Nasazení produktu IBM Trusteer Fraud Protection

Pro každou Aplikaci, kterou si Zákazník zaregistroval, zahrnuje základní registrace Zákazníka požadované činnosti nastavení a počátečního nasazení v cloudu IBM Trusteer, včetně počátečního jednorázového spuštění, konfigurace, šablony úvodní stránky, testování a školení.

Činnosti nasazení nezahrnují činnosti implementace, které jsou vyžadovány v Aplikacích nebo systémech Zákazníka.

Fáze implementace různých služeb Cloud Service je navržena pro časové rámce uvedené v relevantních příručkách implementace.

Provedení těchto fází implementace v rámci přiděleného časového rámce závisí na plné angažovanosti a účasti vedoucích pracovníků a zaměstnanců Zákazníka. Zákazník je povinen poskytnout požadované informace včas. Podmínkou pro plnění ze strany IBM je včasné poskytnutí informací a včasné učinění jakýchkoli rozhodnutí ze strany Zákazníka; jakékoli prodlení může mít za následek dodatečné náklady anebo prodlení s realizací těchto služeb v oblasti implementace.

Pro každou zaregistrovanou Aplikaci zahrnuje základní registrace Zákazníka požadované činnosti nastavení a počáteční implementace v cloudu IBM Trusteer, včetně počátečního jednorázového spuštění, konfigurace, šablony úvodní stránky, testování a školení.

Registrace Zákazníka zahrnuje podporu a testování pro stránky v rámci takové aplikace Zákazníka, která bude označena IBM jako doporučená během počátečního nasazení. IBM nenese odpovědnost za: (i) částečné nasazení, (ii) rozhodnutí Zákazníka nenasadit služby IBM Cloud Service podle doporučení IBM, (iii) za rozhodnutí Zákazníka provést nasazení, nastavení a testování samostatně, ani za (IV) částečné nasazení nebo ochranu v důsledku nedostatečných informací poskytnutých Zákazníkem. Za dodatečný poplatek a na základě samostatné smlouvy mohou být smluvně sjednány dodatečné služby, včetně činností nasazení nad rámec počátečního nasazení.