IBM Trusteer Pinpoint Detect

Tento Popis služby stanovuje podmínky služby Cloud Service. Příslušné dokumenty objednávky poskytují podrobnosti o ceně a další podrobnosti o objednávce Zákazníka.

1. 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. Trusteer Management Application (TMA) a Trustboard:

   TMA je tradiční aplikace správy pro řešení Trusteer, která umožňuje Zákazníkům vyhodnotit a klasifikovat výstrahy. Trustboard je novější aplikace správy, která se primárně používá pro výzkum. Zákazníci se mohou rozhodnout použít TMA nebo Trustboard v kterémkoli okamžiku. Aplikace TMA a Trustboard jsou zpřístupněny 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. IBM Trusteer Pinpoint Detect a IBM Trusteer Pinpoint Verify jsou použity jako součást přihlášení TMA a Trustboard.

b. Webový skript nebo rozhraní API:

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

"Relace" je interakce mezi aplikací Zákazníka (Webovou nebo Mobilní) a službou Cloud Service, která generuje jedno nebo více posouzení rizik v reálném čase. Relace se měří od doby začátku interakce do konce interakce. Ukončení interakce se zaznamená, když nastane některá z následujících událostí:

- Interakce se resetuje normálním způsobem při odhlášení z aplikace.
- Prohlížeč, aplikace nebo karta jsou zavřeny.
- Cookies jsou odstraněny.
- Vyprší časový limit.

Relace může zahrnovat libovolný počet aktivit, například: přihlášení, prohlížení, zapůjčení, nastavení plateb a další, jak je definováno v aplikaci Zákazníka. Upřesňujeme, že pro účely této služby Cloud Service je jedno Připojení (jak je definováno níže) jedna Relace.

1.1 Nabídky

Zákazník si může vybrat z následujících dostupných nabídek.

1.1.1 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. Tuto Službu lze také použít pro vzdálené přístupy pracovníků za účelem posouzení rizika ze spravovaných a nespravovaných zařízení.

Součástí této služby Cloud Service je podpora Premium (definována v části Technická podpora níže).

Službu si lze zakoupit v balíčcích po 100 Oprávněných účastnících nebo balíčcích po 100 Připojení.

1.1.2 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.

1.1.3 IBM Trusteer Pinpoint Detect for Connections

Tato služba Cloud Service nabízí ochranu a jejím cílem je detekovat pokusy o převzetí účtu a poskytuje skóre rizik / důvěry prohlížečů a/nebo mobilních zařízení (prostřednictvím nativního prohlížeče mobilní aplikace Zákazníka) při přístupu do aplikace Business nebo Retail. Řešení využívá různé ukazatele rizik při analýze zařízení koncového uživatele, připojení a chování a porovnává je s historií uživatele pro identifikaci podezřelého využití.

Služba Cloud Service může využívat připojení z mobilního, tak webového kanálu. IBM Trusteer Pinpoint Detect zahrnuje oprávnění k IBM Trusteer Mobile SDK, pokud je to relevantní.

Službu Cloud Service lze zakoupit v balíčcích po 100 připojeních ročně.

1.2 Volitelné služby

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

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

Aplikace Zákazníka odkazuje na webovou a/nebo mobilní aplikaci. Webové aplikace seskupují veškeré funkce nabízené oprávněným účastníkům Zákazníka prostřednictvím několika webových stránek z přihlašovací nebo identifikační obrazovky a monitorují se jako jediná aplikace v konzole Trusteer (Aplikace správy Trusteer). Mobilní aplikace seskupuje společně veškeré funkce nabízené Oprávněným uživatelům Zákazníka prostřednictvím jednoho softwarového programu, který lze stáhnout z obchodu s aplikacemi (obchod), z přihlašovací nebo identifikační obrazovky jako jediné aplikace v konzole Trusteer (Aplikace správy Trusteer).

Integrace IBM Trusteer Pinpoint vyžaduje oprávnění k IBM Trusteer Pinpoint Application pro každou Aplikaci.

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

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

Aplikace Zákazníka odkazuje na webovou a/nebo mobilní aplikaci. Webové aplikace seskupují veškeré funkce nabízené oprávněným účastníkům Zákazníka prostřednictvím několika webových stránek z přihlašovací nebo identifikační obrazovky a monitorují se jako jediná aplikace v konzole Trusteer (Aplikace správy Trusteer). Mobilní aplikace seskupuje společně veškeré funkce nabízené Oprávněným uživatelům Zákazníka prostřednictvím jednoho softwarového programu, který lze stáhnout z obchodu s aplikacemi (obchod), z přihlašovací nebo identifikační obrazovky jako jediné aplikace v konzole Trusteer (Aplikace správy Trusteer).

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

1.2.3 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.

1.2.4 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.

1.2.5 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).

1.2.6 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.

1.2.7 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.

1.2.8 IBM Trusteer Pinpoint Criminal Detection for Business nebo IBM 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. Služby IBM Trusteer Pinpoint Criminal Detection Cloud Service 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:

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

1.2.9 IBM Trusteer Pinpoint Criminal Detection II for Business anebo IBM Trusteer Pinpoint Criminal Detection II for Retail

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

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. Služby IBM Trusteer Pinpoint Criminal Detection II Cloud Service 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:

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

Tato služba Cloud Service zahrnuje ochranu pro jednu Aplikaci. Pro každou další Aplikaci by Zákazník měl získat oprávnění pro další Aplikace IBM Trusteer Pinpoint Criminal Detection.

1.2.10 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. Pro účely tohoto Popisu služby 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 služby IBM Cloud Service. Software Zákazníka 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.

1.2.11 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.

1.2.12 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.

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

- 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.

1.2.14 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 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.

1.2.15 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.

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

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

Tato služba Cloud Service rozšiřuje produkty 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.

1.3 Akcelerační služby

1.3.1 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.

1.3.2 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.

1.3.3 IBM Trusteer Pinpoint Criminal 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 Criminal Detection Cloud Service, by si měli zakoupit službu IBM Trusteer Pinpoint Criminal 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.

2. Datové listy ochrany a zpracování údajů

Dodatek o zpracování údajů (Data Processing Addendum, DPA) společnosti IBM na adrese http://ibm.com/dpa a Datový list zpracování a ochrany údajů (označováno jako Datový list nebo Dodatek DPA) v odkazech níže poskytují další informace o ochraně údajů pro služby Cloud Services a volby týkající se typů Obsahu, které lze zpracovat, využívaných činností vztahujících se ke zpracování, funkcí ochrany údajů a specifických aspektů uchovávání a vrácení Obsahu. Dodatek DPA se uplatní, pokud se na osobní údaje zahrnuté v Obsahu vztahuje/í i) Evropské obecné nařízení o ochraně údajů (EU/2016/679) (GDPR); nebo ii)jiné zákony o ochraně údajů uvedené na adrese http://ibm.com/dpa/dpl.

Upřesňujeme, že Datové listy, obvykle uvádějí seznam všech lokalit, kde IBM (včetně případných nezávislých dílčích zpracovatelů) hostuje a zpracovává Osobní údaje, bez ohledu na datové středisko, ze kterého jsou služby nasazovány. Pro seznam lokalit hostování a zpracování, které jsou specifické pro datové středisko, ze kterého jsou služby nasazovány, viz část 5.2 níže (Informace o dodatečném místě zpracování).

IBM Trusteer Pinpoint Criminal Detect

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

IBM Trusteer Pinpoint Detect

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

IBM Trusteer Pinpoint Malware Detection

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

IBM Trusteer Mobile SDK

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

3. Úrovně služby a Technická podpora

3.1 Dohoda o úrovni služeb

IBM poskytuje Zákazníkovi pro dostupnost následující Dohodu o úrovni služeb (SLA). IBM uplatní nejvyšší použitelnou kompenzaci vycházející ze souhrnné dostupnosti služby Cloud Service, jak je uvedeno v tabulce níže. Procento dostupnosti se vypočítá jako celkový počet minut v rámci smluvního měsíčního období minus celkový počet minut Odstávky za smluvní měsíční období, děleno celkovým počtem minut za smluvní měsíční období. Definice Odstávky, proces uplatňování nároku a pokyny, jak kontaktovat IBM ohledně problémů s dostupností služby, jsou uvedeny na stránkách IBM v příručce Cloud Service Support Guide na adrese https://www.ibm.com/software/support/saas_support_overview.html.

Dostupnosti služeb	Dobropis (% měsíčního registračního poplatku*)
Méně než 99,9 %	2 %
Méně než 99,0 %	5 %
Méně než 95,0 %	10 %

* Registrační poplatek je smluvní cena za měsíc, za který je uplatňován nárok.

3.2 Technická podpora

Informace o technické podpoře pro službu Cloud Service, včetně kontaktních údajů na podporu, úrovní závažnosti, hodin dostupnosti podpory, dob odezvy a dalších informací a procesů podpory, lze zjistit výběrem služby Cloud Service v příručce podpory IBM na adrese https://www.ibm.com/support/home/pages/support-guide/.

Podpora Premium:

Registrace Premium Support je za dodatečný poplatek k dispozici podpora Premium a zahrnuje:

- 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/.

4. Poplatky

4.1 Metriky poplatků

Metriky poplatků za službu Cloud Service jsou uvedeny v Transakčním dokumentu.

Na tuto službu Cloud Service se uplatní následující metriky poplatků:

- Sjednaná služba je profesionální nebo školicí služba související se službami Cloud Services.
- Vybraný účastník je každá fyzická nebo právnická osoba, která je způsobilá k účasti v jakémkoli programu poskytování služeb spravovaném nebo sledovaném prostřednictvím služeb Cloud Services.
- Aplikace je softwarový program s jedinečným názvem vyvinutý nebo zdostupněný pro přístup nebo použitý službami Cloud Service.
- Volání API je vyvolání služeb Cloud Services prostřednictvím programového rozhraní.
- Připojení je odkaz nebo přidružení databáze, aplikace, serveru nebo jiného typu zařízení, které bylo nebo je dostupné, ke službám Cloud Services.

4.2 Poplatky za vzdálené služby

Vzdálená služba končí 90 dní od nákupu, bez ohledu na to, zda byla vzdálená služba používána.

5. Dodatečné podmínky

Na Smlouvy o službě Cloud Service (nebo ekvivalentní smlouvy o základním cloudu) uzavřené před 1. lednem 2019 se vztahují podmínky dostupné na adrese https://www.ibm.com/acs.

5.1 EULA a základ pro zpracování údajů Subjektů údajů

Pro služby IBM Trusteer Rapport (včetně Rapport Remediation nebo Rapport for Mitigation v případě nasazení ve spojení se službami Pinpoint Cloud Service): 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://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA, aby IBM mohla shromažďovat a zpracovávat informace nezbytné pro poskytování služeb Cloud Services.

Pro služby IBM Trusteer Rapport Cloud Services Zákazník udílí společnosti IBM jako zpracovateli údajů Vašeho sponzorujícího podniku právo používat Program pro shromažďování malwaru a artefaktů malwaru, tj. souborů souvisejících se škodlivou činností nebo souborů souvisejících s neobvyklou poruchou Programu. Společnost IBM nepoužívá Program k zaměření na soubory s osobními údaji uživatele; nicméně shromážděné soubory mohou obsahovat osobní údaje, které byly získány malwarem bez povolení uživatele. Společnost IBM 1) neprodleně vymaže veškeré soubory, které nejsou relevantní pro takovou analýzu a 2) uchová příslušné soubory pouze po dobu trvání analýzy a v žádném případě ne déle než tři měsíce.

5.2 Informace o dodatečném místě zpracování

Veškeré hostování a zpracování Osobních údajů, včetně případných nezávislých dílčích zpracovatelů uvedených v Datových listech, budou probíhat v lokalitách uvedených níže:

Pro všechny služby poskytované prostřednictvím německého datového střediska společnost IBM omezí hostování a zpracování Osobních údajů na zemi smluvního subjektu společnosti IBM a následující země: Německo, Izrael, Irsko a Nizozemsko.

Pro všechny služby poskytované prostřednictvím japonského datového střediska společnost IBM omezí hostování a zpracování Osobních údajů na zemi smluvního subjektu společnosti IBM a následující země: Japonsko, Izrael a Irsko.

Pro všechny služby poskytované prostřednictvím datového střediska USA společnost IBM omezí hostování a zpracování Osobních údajů na zemi smluvního subjektu společnosti IBM a následující země: USA, Izrael, Irsko, Singapur a Austrálie.

Kromě výše uvedených lokalit ve vztahu ke všem službám poskytovaným přes datová střediska v Německu, Japonsku a USA (1) mohou být podpůrná data hostována a zpracovávána v Německu a Francii společností Salesforce.Com jako nezávislým dílčím zpracovatelem společnosti IBM a (2) pro zákazníky, kteří se rozhodnou pro zasílání dat poskytovatelům Mobile Carrier Intelligence, Osobní údaje mohou být hostovány a zpracovávány v zemích příslušných nezávislých dílčích zpracovatelů v souladu s ustanovením Datového listu. Aniž by tím bylo dotčeno případné odlišné ustanovení Datového listu, nezávislí dílčí zpracovatelé uvedeni v článku (2) bezprostředně předchozí věty nemusí být v souladu s normou ISO 27001 nebo SOC2.

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.

5.3 Údaje Vlastníka účtu

Pro účely vyjasnění, pokud je více než jeden zákazník IBM propojen se Softwarem klienta držitele účtu konkrétního Držitele účtu (např. zákazníci IBM "Propojení zákazníci") a služby v souladu s tímto Popisem služeb budou poskytovány společností IBM těmto Propojeným zákazníkům prostřednictvím datových středisek v různých regionech, pak mohou být data Držitele účtu zpracovávána ve všech lokalitách souvisejících s každých z těchto datových středisek v souladu s ustanovením v části 5.2 výše.

5.4 Integrovaná řešení

Pro účely vyjasnění představují různé nabídky pod značkou Trusteer integrovaná řešení. Z tohoto důvodu, pokud Zákazník kteroukoliv z těchto služeb Cloud Services ukončí, IBM bude oprávněna ponechat si data Zákazníka pro účely poskytování dalších služeb Cloud Service Zákazníkovi v souladu s tímto Popisem služeb, stejně jako dalších služeb Trusteer v souladu s popisy služeb, které se k takovým službám Trusteer vztahují.

5.5 Aktivační software

Služba Cloud Service obsahuje následující Aktivační software:

- IBM Rapport Agents

5.6 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).

5.7 Data shromažďovaná v rámci nasazení

Nasazení služby Cloud Service může být spojeno s tím, že Zákazník poskytne společnosti IBM určitá data. Tato data nesmí obsahovat informace, které mohou identifikovat nebo která lze přiřadit ke konkrétním fyzickým osobám. Další pokyny ohledně dat poskytovaných společnosti IBM v rámci nasazení jsou uvedeny v pokynech k implementací Trusteer, které budou Zákazníkovi poskytnuty.

6. Přednostní podmínky

6.1 Využití údajů

Dále uvedené má přednost v případě rozporu s částí Ochrana obsahu a údajů v základních podmínkách služby Cloud Service mezi stranami: IBM nepoužije ani nesdělí výsledky pocházející z používání služby Cloud Service Zákazníkem, které jsou jedinečné vzhledem k Obsahu Zákazníka (Poznatky) nebo jinak identifikují Zákazníka. Společnost IBM však bude používat Obsah a další informace, které vyplynou z Obsahu (kromě Insights) v průběhu poskytování služby Cloud Service, pro účely vylepšování služby Cloud Service. IBM může rovněž sdílet identifikátory hrozeb a další bezpečnostní informace vložené do Obsahu pro účely detekce hrozeb a ochranu.