IBM Trusteer Fraud Protection

Diese Servicebeschreibung beschreibt den Cloud-Service, den IBM für den Kunden erbringt. Als Kunde werden der Vertragspartner und seine berechtigten Benutzer sowie die Empfänger des Cloud-Service bezeichnet. Das maßgebliche Angebot und der Berechtigungsnachweis (Proof of Entitlement = PoE) werden als separate Auftragsdokumente zur Verfügung gestellt.

1. Cloud-Service

Diese Servicebeschreibung gilt für die folgenden Cloud-Services:

Pinpoint Assure Cloud Services:

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

Rapport-Cloud-Services:

- 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

Pinpoint-Cloud-Services:

- 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

Mobile-Cloud-Services:

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

1.1 Business- und Retail-Cloud-Services

Die IBM Trusteer-Cloud-Services werden für die Nutzung mit bestimmten Anwendungsarten bereitgestellt. Eine Anwendung ist entweder als „Retail“ oder als „Business“ definiert. Für Retail-Anwendungen und Business-Anwendungen stehen jeweils unterschiedliche Angebote zur Verfügung.

a. Eine Retail-Anwendung ist eine Online-Banking-Anwendung, mobile Anwendung oder E-Commerce-Anwendung, die speziell für Endverbraucher ausgelegt ist. Nach der Richtlinie des Kunden können bestimmte kleinere Unternehmen so klassifiziert werden, dass sie zur Nutzung von Retail-Anwendungen berechtigt sind.

b. Eine Business-Anwendung ist eine Online-Banking-Anwendung, mobile Anwendung oder E-Commerce-Anwendung, die für Unternehmen, institutionelle oder vergleichbare Einrichtungen ausgelegt ist, oder jede andere Anwendung, die nicht zur Kategorie der Retail-Anwendungen gehört.

1.1.1 Business-Cloud-Services

- 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 Retail-Cloud-Services

- 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

Für jeden der Business- und Retail-Cloud-Services, mit Ausnahme der IBM Trusteer Mobile SDK-Cloud-Services, ist ein zugehöriges Premium-Support-Produkt gegen Zahlung einer zusätzlichen Gebühr erhältlich.

1.1.3 Zusätzliche Cloud-Services für IBM Trusteer Rapport II

a. Zusätzlich verfügbare Cloud-Services für 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. Zusätzlich verfügbare Cloud-Services für 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

Für jedes der Business- und Retail-Add-ons zu den IBM Trusteer Rapport-Cloud-Services, mit Ausnahme der IBM Trusteer Rapport Mandatory Service-Add-ons, ist ein zugehöriges Premium-Support-Produkt gegen Zahlung einer zusätzlichen Gebühr erhältlich.

Voraussetzung für die zugehörigen zusätzlichen Cloud-Services, die in diesem Abschnitt aufgelistet sind, ist eine Subscription für IBM Trusteer Rapport II for Business oder IBM Trusteer Rapport II for Retail.

1.1.4 Zusätzliche Cloud-Services für IBM Trusteer Pinpoint Malware Detection II

a. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business oder 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. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail oder 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

Für bestimmte Angebote ist, wie in diesem Dokument angegeben, Premium Support verfügbar. Voraussetzung für die zugehörigen zusätzlichen Cloud-Services, die in diesem Abschnitt aufgelistet sind, ist eine Subscription für IBM Trusteer Pinpoint Malware Detection II for Business oder IBM Trusteer Pinpoint Malware Detection II for Retail.

1.1.5 Zusätzliche Cloud-Services für IBM Trusteer Pinpoint Detect Standard und/oder IBM Trusteer Pinpoint Detect Premium und/oder IBM Trusteer Pinpoint Detect Standard for Retail und/oder IBM Trusteer Pinpoint Detect Premium for Retail und/oder IBM Trusteer Pinpoint Detect Standard for Business und/oder IBM Trusteer Pinpoint Detect Premium for Business

a. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Pinpoint Detect Standard for Business und/oder 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. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Pinpoint Detect Standard for Retail und/oder 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. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Pinpoint Detect Standard und/oder IBM Trusteer Pinpoint Detect Premium:

- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application

d. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Pinpoint Detect Premium

- IBM Trusteer Pinpoint Verify

Voraussetzung für die zugehörigen zusätzlichen Cloud-Services, die in diesem Abschnitt aufgelistet sind, ist eine Subscription für IBM Trusteer Pinpoint Detect Standard oder IBM Trusteer Pinpoint Detect Premium oder IBM Trusteer Pinpoint Detect Standard for Retail oder IBM Trusteer Pinpoint Detect Premium for Retail oder IBM Trusteer Pinpoint Detect Standard for Business oder IBM Trusteer Pinpoint Detect Premium for Business.

1.1.6 Weitere zusätzliche Cloud-Services

Alle zusätzlichen Cloud-Services-Subscriptions für die obigen Basis-Subscriptions, die hierin nicht aufgelistet sind, unabhängig davon, ob sie derzeit verfügbar sind oder sich in der Entwicklung befinden, gelten nicht als Update und müssen separat erworben werden.

1.2 Begriffsbestimmungen

Kontoinhaber bezieht sich auf den Endbenutzer des Kunden, der die Clientaktivierungssoftware installiert, die Endbenutzerlizenzvereinbarung („EULA“) akzeptiert und sich mindestens einmal bei der Retail- oder Business-Anwendung authentifiziert hat, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat.

Client-Software für Kontoinhaber bezieht sich auf die Clientaktivierungssoftware von IBM Trusteer Rapport oder jede andere Clientaktivierungssoftware, die mit einigen Cloud-Services für die Installation auf dem Gerät des Endbenutzers bereitgestellt wird.

Trusteer Splash bezieht sich auf den Splash, der dem Kunden basierend auf den verfügbaren Splash-Vorlagen bereitgestellt wird.

Landing-Page bezieht sich auf die von IBM gehostete Seite, die dem Kunden zusammen mit dem Kunden-Splash und der für den Download verfügbaren Client-Software für Kontoinhaber bereitgestellt wird.

1.3 IBM Trusteer Rapport-Cloud-Services

1.3.1 IBM Trusteer Rapport II for Retail und/oder IBM Trusteer Rapport II for Business („Trusteer Rapport II“)

Der Trusteer Rapport II-Cloud-Service ist eine Neuentwicklung von IBM Trusteer Rapport, die dazu beitragen soll, Gebühren in Bezug auf den Schutz mehrerer Anwendungen zu standardisieren, und ersetzt Einmalgebühren, wenn Anwendungen hinzugefügt werden.

Trusteer Rapport II bietet Schutz vor Phishing-Attacken und Man-in-the-Browser-Attacken (MitB). Mit einem globalen Netzwerk bestehend aus mehreren zehn Millionen Endpunkten erfasst IBM Trusteer Rapport weltweit relevante Informationen über aktive Phishing- und Malware-Attacken auf Unternehmen. IBM Trusteer Rapport wendet Verhaltensalgorithmen an, die darauf abzielen, Phishing-Attacken zu blockieren sowie die Installation und Ausführung von MitB-Malware-Stämmen zu verhindern.

Für diesen Cloud-Service kommen die Gebührenmetriken zur Anwendung, die auf berechtigten Teilnehmern oder auf Clienteinheiten basieren. Das Business-Angebot wird in Paketen mit jeweils 10 berechtigten Teilnehmern oder 10 Clienteinheiten verkauft. Das Retail-Angebot wird in Paketen mit jeweils 100 berechtigten Teilnehmern oder 100 Clienteinheiten verkauft.

Dieses Cloud-Service-Angebot beinhaltet Folgendes:

a. Trusteer Management Application („TMA“):

   Die TMA wird über die in der Cloud gehostete IBM Trusteer-Umgebung zur Verfügung gestellt, über die der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) (i) bestimmte Ereignisdatenberichte und Risikobewertungen anzeigen und herunterladen sowie (ii) die Konfiguration der Clientaktivierungssoftware anzeigen kann, die für die berechtigten Teilnehmer des Kunden unter einer Endbenutzerlizenzvereinbarung („EULA“) kostenlos lizenziert und zum Download auf ihre Desktops oder Geräte (PC/MACs) zur Verfügung gestellt wird. Die Software wird auch als Trusteer Rapport-Softwaresuite bezeichnet („Client-Software für Kontoinhaber“). Die Client-Software für Kontoinhaber darf vom Kunden nur über den Trusteer Splash oder die Rapport-API weitergegeben werden. Die Nutzung dieser Software für unternehmensinterne Zwecke des Kunden oder zur Verwendung durch Mitarbeiter des Kunden (außer zum persönlichen Gebrauch der Mitarbeiter) ist nicht zulässig.

b. Web-Script:

   Für den Zugriff auf eine Website zum Aufruf oder zur Verwendung des Cloud-Service.

c. Ereignisdaten:

   Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Ereignisdaten zu empfangen, die von der Client-Software für Kontoinhaber infolge der Online-Interaktionen der Kontoinhaber mit der Business- oder Retail-Anwendung generiert werden, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat. Die Ereignisdaten werden von der Client-Software für Kontoinhaber übertragen, die auf den Geräten der berechtigten Teilnehmer ausgeführt wird, die die EULA akzeptiert und sich mindestens einmal bei der Business- oder Retail-Anwendung des Kunden authentifiziert haben, und sofern die Konfiguration des Kunden die betreffenden Benutzer-IDs enthält.

d. Trusteer Splash:

   Über die Trusteer Splash-Marketing-Plattform wird den berechtigten Teilnehmern, die auf die Business- und/oder Retail-Anwendungen zugreifen, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat, die Client-Software für Kontoinhaber zum Download angeboten. Der Kunde kann eine Splash-Vorlage aus einer Reihe verfügbarer Vorlagen auswählen. Eine Splash-Anpassung kann unter einem separaten Vertrag oder einer Leistungsbeschreibung vereinbart werden.

Der Kunde kann seine Marken, Logos oder Symbole zur Verwendung in Verbindung mit der TMA und dem Trusteer Splash bereitstellen, damit diese in der Client-Software für Kontoinhaber oder auf den von

IBM gehosteten Landing-Pages sowie auf der IBM Trusteer-Website dargestellt werden. Der Umgang mit den vom Kunden bereitgestellten Marken, Logos und Symbolen erfolgt gemäß den IBM Richtlinien für Werbung und die Nutzung von Marken.

Der Kunde muss eine Subscription für den Cloud-Service „IBM Trusteer Rapport Mandatory Service“ erwerben, wenn er die Bereitstellung der Client-Software für Kontoinhaber in irgendeiner Form erzwingen möchte.

Als zwingende Bereitstellung der Client-Software für Kontoinhaber werden alle Arten der Bereitstellung durch Mechanismen oder Verfahren angesehen, die einen berechtigten Teilnehmer direkt oder indirekt zum Download der Client-Software für Kontoinhaber zwingen, sowie alle Methoden, Tools, Prozeduren, Vereinbarungen oder Mechanismen, die die Umgehung der Lizenzierungsanforderungen für die zwingende Bereitstellung der Client-Software für Kontoinhaber ermöglichen und von IBM weder erstellt noch genehmigt wurden.

Trusteer Rapport II for Business und/oder Trusteer Rapport II for Retail bieten jeweils Schutz für eine einzelne Anwendung. Für jede weitere Anwendung muss der Kunde eine Berechtigung für IBM Trusteer Rapport Additional Applications erwerben.

1.3.2 Optionale zusätzliche Cloud-Services für IBM Trusteer Rapport II for Business und/oder IBM Trusteer Rapport II for Retail

Voraussetzung für die im Folgenden aufgelisteten zusätzlichen Cloud-Services ist eine Subscription für die IBM Trusteer Rapport II-Cloud-Services. Ist der Cloud-Service als „for Business“ gekennzeichnet, dann müssen die zusätzlich erworbenen Cloud-Services ebenfalls als „for Business“ gekennzeichnet sein. Ist der Cloud-Service als „for Retail“ gekennzeichnet, dann müssen die zusätzlich erworbenen Cloud-Services ebenfalls als „for Retail“ gekennzeichnet sein. Der Kunde erhält Ereignisdaten von den berechtigten Teilnehmern oder den Clienteinheiten, die die Client-Software für Kontoinhaber ausführen, wenn diese die EULA akzeptiert, sich mindestens einmal bei der Business- und/oder Retail-Anwendung des Kunden authentifiziert haben und die Konfiguration des Kunden Benutzer-IDs erfasst.

1.3.3 IBM Trusteer Rapport Fraud Feeds for Business und/oder IBM Trusteer Rapport Fraud Feeds for Retail

Bei Erwerb einer Subscription für diesen Add-on-Cloud-Service kann der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) die TMA verwenden, um die vom Cloud-Service Trusteer Rapport generierten Bedrohungsdaten (Threat Feeds) anzuzeigen, zu subskribieren und deren Zustellung zu konfigurieren. Die Bedrohungsdaten können per E-Mail an bestimmte E-Mail-Adressen oder über SFTP als Textdateien gesendet werden.

Für dieses Angebot kommt nur die Gebührenmetrik zur Anwendung, die auf berechtigten Teilnehmern basiert.

1.3.4 IBM Trusteer Rapport Phishing Protection for Business und/oder IBM Trusteer Rapport Phishing Protection for Retail

Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Benachrichtigungen über Ereignisdaten zu empfangen, die sich auf die Eingabe der Anmeldeinformationen eines Kontoinhabers auf mutmaßlichen Phishing-Sites oder potenziell betrügerischen Sites beziehen. Wenn seriöse Online-Anwendungen (URLs) fälschlicherweise als Phishing-Sites markiert sind, warnt der Cloud-Service die Kontoinhaber ggf. vor einer Phishing-Site, obwohl es sich um eine seriöse Site handelt. In solchen Fällen muss der Kunde IBM den Fehler melden, woraufhin der Fehler von IBM behoben wird. Diese Maßnahme ist der einzige Abhilfeanspruch des Kunden für einen solchen Fehler.

Für diesen Cloud-Service kommen die Gebührenmetriken zur Anwendung, die auf berechtigten Teilnehmern oder auf Clienteinheiten basieren. Das Business-Angebot wird in Paketen mit jeweils 10 berechtigten Teilnehmern oder 10 Clienteinheiten verkauft. Das Retail-Angebot wird in Paketen mit jeweils 100 berechtigten Teilnehmern oder 100 Clienteinheiten verkauft.

Für diese Cloud-Services kann Premium Support unter den Gebührenmetriken erworben werden, die auf berechtigten Teilnehmern oder auf Clienteinheiten basieren. Das Business-Angebot wird in Paketen mit jeweils 10 berechtigten Teilnehmern oder 10 Clienteinheiten verkauft. Das Retail-Angebot wird in Paketen mit jeweils 100 berechtigten Teilnehmern oder 100 Clienteinheiten verkauft.

1.3.5 IBM Trusteer Rapport Mandatory Service for Business und/oder IBM Trusteer Rapport Mandatory Service for Retail

Der Kunde kann eine Instanz der Trusteer Splash-Marketing-Plattform verwenden, um den Download der Client-Software für Kontoinhaber für berechtigte Teilnehmer zu erzwingen, die auf die Business- und/oder Retail-Anwendungen zugreifen, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat.

IBM Trusteer Rapport Premium Support for Business ist die Voraussetzung für IBM Security Rapport Mandatory Service for Business.

IBM Trusteer Rapport Premium Support for Retail ist die Voraussetzung für IBM Security Rapport Mandatory Service for Retail.

Der Kunde kann die zusätzliche Funktionalität des IBM Trusteer Rapport Mandatory Service nur implementieren, wenn dieser Service für die Nutzung mit der Retail- oder Business-Anwendung bestellt und konfiguriert wurde, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat.

Für diesen Cloud-Service kommt die Gebührenmetrik zur Anwendung, die auf berechtigten Teilnehmern basiert. Das Business-Angebot wird in Paketen mit jeweils 10 berechtigten Teilnehmern verkauft. Das Retail-Angebot wird in Paketen mit jeweils 100 berechtigten Teilnehmern verkauft.

1.3.6 IBM Trusteer Rapport Large Redeployment und/oder IBM Trusteer Rapport Small Redeployment

Kunden, die ihre Online-Banking-Anwendungen während der Servicelaufzeit erneut bereitstellen und infolgedessen Änderungen an ihrer Bereitstellung von IBM Trusteer Rapport II benötigen, müssen den Cloud-Service IBM Trusteer Rapport Redeployment erwerben.

Eine erneute Bereitstellung kann erforderlich sein, wenn der Kunde die Domäne oder Host-URL der Anwendung geändert hat, Änderungen an der Splash-Konfiguration vorgenommen hat oder auf eine neue Online-Banking-Plattform umzieht.

Während der 6-monatigen Übergangszeit für die erneute Bereitstellung hat der Kunde auf Eins-zu-eins-Basis Anspruch auf zusätzliche Anwendungen, die neben den bereits per Subscription erworbenen Anwendungen ausgeführt werden können.

IBM Trusteer Rapport Large Redeployment gilt für Umgebungen mit mehr als 20.000 Benutzern und IBM Trusteer Rapport Small Redeployment für Umgebungen mit bis zu 20.000 Benutzern.

1.3.7 IBM Trusteer Rapport Additional Applications for Business und/oder IBM Trusteer Rapport Additional Applications for Retail

Soll IBM Trusteer Rapport II for Business nach der Bereitstellung für eine einzelne Business-Anwendung noch für weitere Anwendungen bereitgestellt werden, muss jeweils eine Berechtigung für den Cloud-Service IBM Trusteer Rapport Additional Applications for Business erworben werden. Soll IBM Trusteer Rapport II for Retail nach der Bereitstellung für eine einzelne Retail-Anwendung noch für weitere Anwendungen bereitgestellt werden, muss jeweils eine Berechtigung für den Cloud-Service IBM Trusteer Rapport Additional Applications for Retail erworben werden.

1.4 IBM Trusteer Pinpoint-Cloud-Services

IBM Trusteer Pinpoint ist ein cloudbasierter Service, der eine zusätzliche Schutzstufe bietet und dafür ausgelegt ist, Malware- und Phishing-Attacken sowie Attacken zur Kontoübernahme zu erkennen und abzuwehren. Trusteer Pinpoint kann in die Business- und/oder Retail-Anwendungen, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat, und in die Prozesse zur Betrugsprävention integriert werden.

Dieser Cloud-Service umfasst folgende Funktionen:

a. TMA:

   Die TMA wird über die in der Cloud gehostete IBM Trusteer-Umgebung zur Verfügung gestellt, über die der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) (i) bestimmte Ereignisdatenberichte und Risikobewertungen anzeigen und herunterladen sowie (ii) die von den Pinpoint-Angeboten generierten Bedrohungsdaten (Threat Feeds) anzeigen, subskribieren und deren Zustellung konfigurieren kann.

b. Web-Script und/oder APIs:

   Für die Bereitstellung auf einer Website zum Aufruf oder zur Verwendung des Cloud-Service.

1.4.1 IBM Trusteer Pinpoint Malware Detection

Im Falle einer Malware-Erkennung durch die IBM Trusteer Pinpoint Malware Detection II-Cloud-Services muss der Kunde die Anweisungen im Pinpoint Best Practices Guide befolgen. Der Kunde darf die IBM Trusteer Pinpoint Malware Detection II-Cloud-Services nicht in einer Weise verwenden, die sich auf das Verhalten des berechtigten Teilnehmers unmittelbar nach einer Malware-Erkennung oder der Erkennung einer Kontoübernahme auswirkt und beispielsweise Dritte vermuten lässt, dass die Maßnahmen des Kunden mit der Verwendung der IBM Trusteer Pinpoint-Cloud-Services in Verbindung stehen (z. B. Meldungen, Nachrichten, Blockieren von Geräten oder Sperrung des Zugriffs auf die Business- und/oder Retail-Anwendung sofort nach einer Malware-Erkennung oder der Erkennung einer Kontoübernahme).

1.4.2 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business und/oder IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail und/oder IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business und/oder IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II ist eine Neuentwicklung von IBM Trusteer Pinpoint Malware Detection, die dazu beitragen soll, Gebühren in Bezug auf den Schutz mehrerer Anwendungen zu standardisieren, und ersetzt Einmalgebühren, wenn Anwendungen hinzugefügt werden.

Clientlose Erkennung von Browsern, die durch Man-in-the-Browser-Attacken (MitB) mit Finanz-Malware infiziert sind und eine Verbindung zu einer Business- und/oder Retail-Anwendung herstellen. Die IBM Trusteer Pinpoint Malware Detection-Cloud-Services bieten eine zusätzliche Schutzstufe und ermöglichen es den Unternehmen, sich auf Prozesse zur Betrugsprävention zu konzentrieren, die auf der Erkennung von Malwarerisiken basieren, indem bei einer Infizierung mit MitB-Finanz-Malware Risikobewertungen und Benachrichtigungen an den Kunden gesendet werden.

a. Ereignisdaten:

   Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Ereignisdaten zu empfangen, die infolge der Online-Interaktionen der berechtigten Teilnehmer mit den Business- und/oder Retail-Anwendungen des Kunden generiert werden.

b. Advanced Edition:

   Die Advanced Editions for Business und/oder for Retail bieten zusätzliche Erkennungs- und Schutzstufen, die an die Struktur und den Ablauf der Business- und/oder Retail-Anwendungen des Kunden angepasst sind und auf die Bedrohungslandschaft, der das Unternehmen des Kunden ausgesetzt ist, abgestimmt werden können. Sie können an verschiedenen Standorten in die Business- und/oder Retail-Anwendungen des Kunden integriert werden.

   Die Advanced Edition wird mit einer Mindestbestellmenge von 100.000 berechtigten Teilnehmern im Retail-Bereich und 10.000 berechtigten Teilnehmern im Business-Bereich angeboten. Dies entspricht 1.000 Paketen mit jeweils 100 berechtigten Teilnehmern für Retail-Angebote und 1.000 Paketen mit jeweils 10 berechtigten Teilnehmern für Business-Angebote.

c. Standard Edition:

   Die Standard Editions for Business und/oder for Retail sind Lösungen, die in kurzer Zeit einsatzbereit sind und die hierin beschriebene Kernfunktionalität dieses Cloud-Service bereitstellen.

Bei diesem Cloud-Service ist der Schutz einer einzelnen Anwendung eingeschlossen. Für jede weitere Anwendung muss der Kunde eine Berechtigung für IBM Trusteer Pinpoint Malware Detection Additional Applications erwerben.

1.4.3 Optionale zusätzliche Cloud-Services für IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail und/oder IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail und/oder IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business und/oder IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- Als Voraussetzung für den Cloud-Service IBM Trusteer Rapport Remediation for Retail muss IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail oder IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail erworben werden.
- Als Voraussetzung für den Cloud-Service IBM Trusteer Rapport Remediation for Business muss IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business oder IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business erworben werden.

1.4.4 IBM Trusteer Rapport Remediation for Retail und/oder IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail und IBM Trusteer Rapport Remediation for Business sind dazu ausgelegt, Malware-Infizierungen durch Man-in-the-Browser-Attacken (MitB) auf betroffenen Geräten (PC/MACs) der berechtigten Teilnehmer des Kunden, die auf Ad-hoc-Basis auf die Anwendung des Kunden zugreifen, zu untersuchen, zu beheben, zu blockieren und zu entfernen, wenn die MitB-Malware-Infizierungen anhand der Ereignisdaten von IBM Trusteer Pinpoint Malware Detection festgestellt wurden. Der Kunde muss über eine aktuelle Subscription für IBM Trusteer Pinpoint Malware Detection II verfügen, die tatsächlich im Rahmen der Anwendung des Kunden ausgeführt wird. Der Kunde darf dieses Cloud-Service-Angebot nur für berechtigte Teilnehmer, die auf seine Anwendung zugreifen, und ausschließlich als Tool zum Untersuchen und Wiederherstellen eines bestimmten infizierten Geräts (PC/MAC) auf Ad-hoc-Basis verwenden. IBM Trusteer Rapport Remediation muss auf dem betroffenen Gerät (PC/MAC) des berechtigten Teilnehmers tatsächlich ausgeführt werden und der berechtigte Teilnehmer muss die EULA akzeptiert und sich mindestens einmal bei der Anwendung des Kunden authentifiziert haben, und in der Konfiguration des Kunden müssen die betreffenden Benutzer-IDs enthalten sein. Zwecks Klarstellung wird darauf hingewiesen, dass dieses Cloud-Service-Angebot weder zur Nutzung des Trusteer Splash berechtigt noch dazu, die Client-Software für Kontoinhaber auf irgendeine andere Weise allen berechtigten Teilnehmern des Kunden verfügbar zu machen.

1.4.5 IBM Trusteer Pinpoint Malware Detection Redeployment

Kunden, die ihre Online-Banking-Anwendungen während der Servicelaufzeit erneut bereitstellen und infolgedessen Änderungen an ihrer Bereitstellung von IBM Trusteer Pinpoint Malware Detection II benötigen, müssen IBM Trusteer Pinpoint Malware Detection Redeployment erwerben.

Eine erneute Bereitstellung kann erforderlich sein, wenn der Kunde die Domäne oder Host-URL der Anwendung geändert hat, die Online-Anwendung auf eine neue Technologie umstellt, auf eine neue Online-Banking-Plattform umzieht oder einer vorhandenen Anwendung einen neuen Anmeldeablauf hinzufügt.

Während der 6-monatigen Übergangszeit für die erneute Bereitstellung hat der Kunde auf Eins-zu-eins-Basis Anspruch auf zusätzliche Anwendungen, die neben den bereits per Subscription erworbenen Anwendungen ausgeführt werden können.

IBM Trusteer Pinpoint Malware Detection Additional Applications. Soll IBM Trusteer Pinpoint Malware Detection II Standard Edition oder IBM Trusteer Pinpoint Malware Detection II Advanced Edition nicht nur für eine einzelne Anwendung bereitgestellt werden, muss für jede weitere Anwendung eine Berechtigung für IBM Trusteer Pinpoint Malware Detection Additional Applications erworben werden.

1.4.6 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail und/oder IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- Soll IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail oder IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail nach der Bereitstellung für eine einzelne Retail-Anwendung noch für weitere Anwendungen bereitgestellt werden, muss jeweils eine Berechtigung für IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail erworben werden.
- Soll IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business oder IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business nach der Bereitstellung für eine einzelne Business-Anwendung noch für weitere Anwendungen bereitgestellt werden, muss jeweils eine Berechtigung für IBM Trusteer Pinpoint Malware Detection Additional Applications for Business erworben werden.

1.5 IBM Trusteer Fraud Protection Suite

Die IBM Trusteer Fraud Protection Suite („Suite“) besteht aus einer Gruppe cloudbasierter Services, die Schutz vor Betrug bieten und mit weiteren IBM Produkten integriert werden können, um eine Managementlösung für den gesamten Lebenszyklus bereitzustellen. Zur Suite gehören die folgenden cloudbasierten Services:

- IBM Trusteer Pinpoint Detect ist dafür ausgelegt, Malware- und Phishing-Attacken sowie feindliche Kontoübernahmen zu erkennen und abzuwehren. Trusteer Pinpoint Detect kann in Business- und/oder Retail-Anwendungen, für die der Kunde eine Abdeckung über eine Subscription für einen Cloud-Service erworben hat, und in Prozesse zur Betrugsverhinderung integriert werden.

- IBM Trusteer Rapport for Mitigation ist dafür ausgelegt, infizierte Endpunkte wiederherzustellen und zu schützen.

Die Cloud-Services umfassen:

a. TMA:

Die TMA wird über die in der Cloud gehostete IBM Trusteer-Umgebung zur Verfügung gestellt, die dem Kunden (und einer unbegrenzten Zahl seiner autorisierten Mitarbeiter) folgende Funktionen bietet: (i) Erhalt von Ereignisdatenberichten und Risikobewertungen sowie (ii) Anzeigen, Konfigurieren und Definieren von Sicherheitsrichtlinien und Richtlinien für die Erstellung von Berichten aus Ereignisdaten.

b. Ereignisdaten:

Der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) kann die TMA verwenden, um Ereignisdaten zu empfangen, die infolge der Online-Interaktionen der berechtigten Teilnehmer mit Kundenanwendungen generiert werden, für die der Kunde eine Abdeckung über eine Subscription für einen Cloud-Service erworben hat. Die Ereignisdaten können auch über eine Back-End-API an den Kunden übermittelt werden.

c. Web-Script und/oder APIs:

Für die Bereitstellung auf einer Website zum Aufruf oder zur Verwendung des Cloud-Service.

Best Practices bei Pinpoint

Im Falle einer Malware-Erkennung oder der Erkennung einer Kontoübernahme muss der Kunde die Anweisungen im Pinpoint Best Practices Guide befolgen. Die IBM Trusteer Pinpoint Detect-Cloud-Services sollten nicht in einer Weise verwendet werden, die sich auf das Verhalten des berechtigten Teilnehmers unmittelbar nach einer Malware-Erkennung oder der Erkennung einer Kontoübernahme auswirkt und beispielsweise Dritte vermuten lässt, dass die Maßnahmen des Kunden mit der Verwendung der IBM Trusteer Pinpoint Detect-Angebote in Verbindung stehen (z. B. durch Meldungen, Nachrichten, Blockieren von Geräten oder Zugangssperren auf die Business- und/oder Retail-Anwendung sofort nach einer Malware-Erkennung oder der Erkennung einer Kontoübernahme).

1.5.1 IBM Trusteer Pinpoint Detect Standard for Retail und/oder IBM Trusteer Pinpoint Detect Standard for Business

In diesem Cloud-Service sind die Cloud-Services IBM Trusteer Pinpoint Criminal Detection und IBM Trusteer Pinpoint Malware Detection zusammengefasst, um eine einzelne, einheitliche Lösung anzubieten.

Diese Lösung unterstützt die clientlose Erkennung von Malware und/oder verdächtigen Kontoübernahmeaktivitäten von Browsern, die unter Verwendung einer Geräte-ID eine Verbindung zu einer Retail- oder Business-Anwendung herstellen, sowie Phishing-Erkennung und Erkennung des Diebstahls von Zugangsdaten durch Malware. Die IBM Trusteer Pinpoint-Angebote bieten eine zusätzliche Schutzstufe und sind für das Erkennen von Kontoübernahmeversuchen ausgelegt. Sie übermitteln Risikobewertungen von Browsern oder mobilen Geräten (über den nativen Browser oder die mobile Anwendung des Kunden), die auf eine Retail- oder Business-Anwendung zugreifen, direkt an den Kunden.

Standard Support (gemäß der Definition im nachstehenden Abschnitt „Technische Unterstützung“) ist bei diesem Cloud-Service mit eingeschlossen. Um Premium Support zu erhalten, muss der Kunde Pinpoint Standard Premium Support erwerben.

Bei diesem Cloud-Service ist der Schutz einer einzelnen Anwendung eingeschlossen. Für jede weitere Anwendung muss der Kunde eine Berechtigung für IBM Trusteer Pinpoint Detect Standard Additional Applications erwerben.

Der Service ist in Paketen mit jeweils 100 berechtigten Teilnehmern oder Paketen mit jeweils 100 Verbindungen verfügbar. Wenn der Kunde den Service auf Verbindungsbasis erwirbt, fällt ab der ersten Anwendung eine Gebühr für Additional Application an.

1.5.2 IBM Trusteer Pinpoint Detect Premium for Retail und/oder IBM Trusteer Pinpoint Detect Premium for Business

In diesem Cloud-Service sind IBM Trusteer Pinpoint Criminal Detection und IBM Trusteer Pinpoint Malware Detection zusammengefasst, um eine einzelne, einfach zu integrierende, einheitliche Lösung anzubieten.

Diese Lösung unterstützt die clientlose Erkennung von Malware und/oder verdächtigen Kontoübernahmeaktivitäten von Browsern, die unter Verwendung einer Geräte-ID eine Verbindung zu einer Retail- oder Business-Anwendung herstellen, sowie Phishing-Erkennung und Erkennung des Diebstahls von Zugangsdaten durch Malware. Die IBM Trusteer Pinpoint-Angebote bieten eine zusätzliche Schutzstufe und sind für das Erkennen von Kontoübernahmeversuchen ausgelegt. Sie übermitteln Risikobewertungen von Browsern oder mobilen Geräten (über den nativen Browser oder die mobile Anwendung des Kunden), die auf eine Business- oder Retail-Anwendung zugreifen, direkt an den Kunden.

Dieser Service beinhaltet erweiterte Funktionen und Services, einschließlich erweiterter Bereitstellungs- und Einrichtungsservices, angepasster Sicherheitsrichtlinien, Untersuchungsservices usw., sowie bis zu 200 Stunden an gemeinsam genutzten Ressourcen für Bereitstellungsservices pro Anwendung und 200 Stunden an gemeinsam genutzten Ressourcen für eine Sicherheitsanalyse pro Anwendung bei der Bereitstellung. Die fortlaufenden Services schließen 20 Stunden an Wartungsleistungen für die Bereitstellung pro Anwendung und Jahr sowie 100 Stunden an Sicherheitsuntersuchungen pro Anwendung und Jahr ein. Für alle weiteren Tätigkeiten fallen zusätzliche Gebühren an.

Pinpoint Detect kann Transaktionen sowohl aus mobilen als auch aus Webkanälen verarbeiten. Falls mobile Transaktionen eingeschlossen sind, kommt Pinpoint auf Verbindungsbasis zur Anwendung. Bei diesem Cloud-Service ist der Schutz einer einzelnen Anwendung eingeschlossen. Für jede weitere Anwendung muss der Kunde eine Berechtigung für IBM Trusteer Pinpoint Detect Premium Additional Applications erwerben.

Premium Support ist bei diesem Cloud-Service eingeschlossen.

Die Services IBM Trusteer Pinpoint Detect Premium for Retail und IBM Trusteer Pinpoint Detect Premium for Business sind in Paketen mit jeweils 100 berechtigten Teilnehmern oder im Fall von IBM Trusteer Pinpoint Detect Premium in Paketen mit jeweils 100 Verbindungen verfügbar. Wenn der Kunde den Service auf Verbindungsbasis erwirbt, fällt ab der ersten Anwendung eine Gebühr für Additional Application an.

Pinpoint Detect Policy Manager:

Der Policy Manager ist Bestandteil des Pinpoint-Detect-Premium-Service und wird über die in der Cloud gehostete IBM Trusteer-Umgebung zur Verfügung gestellt, über die der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) (i) Logik zum Erkennen betrügerischer Aktivitäten entwerfen, testen und in der Produktionsumgebung bereitstellen, (ii) Berichte und Dashboards entwerfen sowie (iii) Sicherheitsrichtlinien und Richtlinien für die Erkennung verdächtiger Aktivitäten im Zusammenhang mit der Kundenanwendung anzeigen, konfigurieren und festlegen kann.

Für die Aktivierung des Policy-Manager-Features und wenn zusätzliche tief greifende Unterstützung benötigt wird, sind Beratungsleistungen erforderlich. Einzelheiten der Beratungsleistungen werden in einer Leistungsbeschreibung gesondert geregelt.

Wenn der Policy Manager aktiviert wird, behält IBM sich das Recht vor, zu Unterstützungszwecken auf die Umgebung des Kunden zuzugreifen, um Richtlinien des Kunden anzupassen und größere Probleme, die aufgrund von Richtlinienänderungen auftreten, zu beseitigen.

Der Kunde verpflichtet sich, über den Policy Manager zugängliche Daten vor Missbrauch zu schützen.

Wenn das Policy-Manager-Feature aktiviert wird, muss der Kunde die in der Dokumentation beschriebenen IBM Leitlinien für die Festlegung von Regeln einhalten. Der Kunde bestätigt, dass IBM nicht für Situationen haftet, die dadurch entstehen, dass er diese Empfehlungen nicht eingehalten hat.

Alle Probleme aufgrund von Stabilitäts- und/oder Serviceverschlechterungen, die sich ggf. aus der fehlerhaften Konfiguration des Policy-Manager-Features durch den Kunden ergeben, werden bei der SLA-Berechnung nicht als Ausfallzeit angesehen.

1.5.3 Optionale Services für IBM Trusteer Pinpoint Detect Standard und/oder IBM Trusteer Pinpoint Detect Premium

Voraussetzung für die Cloud-Services in diesem Abschnitt ist der Erwerb von Berechtigungen für IBM Trusteer Pinpoint Detect Premium oder IBM Trusteer Pinpoint Detect Standard.

1.5.4 IBM Trusteer Rapport for Mitigation for Retail und/oder IBM Trusteer Rapport for Mitigation for Business

- IBM Trusteer Rapport for Mitigation for Retail ist dazu ausgelegt, Malware-Infizierungen betroffener Geräte (PC/MACs) von berechtigten Teilnehmern des Kunden, die auf Ad-hoc-Basis auf die Retail-Anwendung des Kunden zugreifen, zu untersuchen, zu beheben, zu blockieren und zu entfernen, wenn Malware-Infizierungen anhand der Ereignisdaten von IBM Trusteer Pinpoint Detect Premium oder IBM Trusteer Pinpoint Detect Standard festgestellt wurden. Der Kunde muss über eine aktuelle Subscription für IBM Trusteer Pinpoint Detect Premium oder IBM Trusteer Pinpoint Detect Standard verfügen, die tatsächlich für die Retail-Anwendung des Kunden ausgeführt wird. Der Kunde darf diesen Cloud-Service nur für berechtigte Teilnehmer, die auf seine Retail-Anwendung zugreifen, und ausschließlich als Tool zum Untersuchen und Wiederherstellen eines bestimmten infizierten Geräts (PC/MAC) auf Ad-hoc-Basis verwenden. IBM Trusteer Rapport for Mitigation for Retail muss auf dem betroffenen Gerät (PC/MAC) des berechtigten Teilnehmers tatsächlich ausgeführt werden, der berechtigte Teilnehmer muss die EULA akzeptieren und sich mindestens einmal bei der Retail-Anwendung des Kunden authentifizieren und die Konfiguration des Kunden muss zur Erfassung von Benutzer-IDs eingerichtet sein. Zwecks Klarstellung wird darauf hingewiesen, dass dieser Cloud-Service weder zur Nutzung des Trusteer Splash berechtigt noch dazu, die Client-Software für Kontoinhaber auf irgendeine andere Weise allen berechtigten Teilnehmern des Kunden verfügbar zu machen.
- IBM Trusteer Rapport for Mitigation for Business ist dazu ausgelegt, Malware-Infizierungen betroffener Geräte (PC/MACs) von berechtigten Teilnehmern des Kunden, die auf Ad-hoc-Basis auf die Business-Anwendung des Kunden zugreifen, zu untersuchen, zu beheben, zu blockieren und zu entfernen, wenn Malware-Infizierungen anhand der Ereignisdaten von IBM Trusteer Pinpoint Detect Premium oder IBM Trusteer Pinpoint Detect Standard festgestellt wurden. Der Kunde muss über eine aktuelle Subscription für IBM Trusteer Pinpoint Detect Premium oder IBM Trusteer Pinpoint Detect Standard verfügen, die tatsächlich für die Business-Anwendung des Kunden ausgeführt wird. Der Kunde darf diesen Cloud-Service nur für berechtigte Teilnehmer, die auf seine Business-Anwendung zugreifen, und ausschließlich als Tool zum Untersuchen und Wiederherstellen eines bestimmten infizierten Geräts (PC/MAC) auf Ad-hoc-Basis verwenden. IBM Trusteer Rapport for Mitigation for Business muss auf dem betroffenen Gerät (PC/MAC) des berechtigten Teilnehmers tatsächlich ausgeführt werden und der berechtigte Teilnehmer muss die EULA akzeptiert und sich mindestens einmal bei der Business-Anwendung des Kunden authentifiziert haben und in der Konfiguration des Kunden müssen die betreffenden Benutzer-IDs enthalten sein. Zwecks Klarstellung wird darauf hingewiesen, dass dieser Cloud-Service weder zur Nutzung des Trusteer Splash berechtigt noch dazu, die Client-Software für Kontoinhaber auf irgendeine andere Weise allen berechtigten Teilnehmern des Kunden verfügbar zu machen.

1.5.5 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail und/oder IBM Trusteer Pinpoint Detect Standard Additional Applications for Business und/oder IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail und/oder IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

Dieser Service beinhaltet bis zu 200 Stunden an gemeinsam genutzten Ressourcen für Bereitstellungsservices pro Anwendung und 200 Stunden an gemeinsam genutzten Ressourcen für eine Sicherheitsanalyse pro Anwendung beim Setup. Die fortlaufenden Services schließen 20 Stunden an Wartungsleistungen für die Bereitstellung pro Anwendung und Jahr sowie 100 Stunden an Sicherheitsuntersuchungen pro Anwendung und Jahr ein.

- Soll IBM Trusteer Pinpoint Detect Standard for Retail nach der Bereitstellung für eine einzelne Retail-Anwendung noch für weitere Anwendungen bereitgestellt werden, muss jeweils eine Berechtigung für IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail erworben werden.
- Soll IBM Trusteer Pinpoint Detect Standard for Business nach der Bereitstellung für eine einzelne Business-Anwendung noch für weitere Anwendungen bereitgestellt werden, muss jeweils eine Berechtigung für IBM Trusteer Pinpoint Detect Standard Additional Applications for Business erworben werden.
- Soll IBM Trusteer Pinpoint Premium for Retail nach der Bereitstellung für eine einzelne Retail-Anwendung noch für weitere Anwendungen bereitgestellt werden, muss jeweils eine Berechtigung für IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail erworben werden.

- Soll IBM Trusteer Pinpoint Premium for Business nach der Bereitstellung für eine einzelne Business-Anwendung noch für weitere Anwendungen bereitgestellt werden, muss jeweils eine Berechtigung für IBM Trusteer Pinpoint Detect Premium Additional Applications for Business erworben werden.

1.5.6 IBM Trusteer Pinpoint Detect Standard Application und/oder IBM Trusteer Pinpoint Detect Premium Application

Dieser Service ist für Web- und mobile Kanäle anwendbar.

Dieser Service beinhaltet bis zu 200 Stunden an gemeinsam genutzten Ressourcen für Bereitstellungsservices pro Anwendung und 200 Stunden an gemeinsam genutzten Ressourcen für eine Sicherheitsanalyse pro Anwendung beim Setup. Die fortlaufenden Services schließen 20 Stunden an Wartungsleistungen für die Bereitstellung pro Anwendung und Jahr sowie 100 Stunden an Sicherheitsuntersuchungen pro Anwendung und Jahr ein.

- Die Bereitstellung von IBM Trusteer Pinpoint Detect Standard erfordert eine Berechtigung für IBM Trusteer Pinpoint Detect Standard Application für jede Anwendung.
- Die Bereitstellung von IBM Trusteer Pinpoint Detect Premium erfordert eine Berechtigung für IBM Trusteer Pinpoint Detect Premium Application für jede Anwendung.

1.5.7 IBM Trusteer Pinpoint Detect Standard Redeployment und/oder IBM Trusteer Pinpoint Detect Premium Redeployment

Kunden, die ihre Online-Banking-Anwendungen während der Servicelaufzeit erneut bereitstellen und folglich Änderungen an ihrer Bereitstellung von IBM Trusteer Pinpoint Detect benötigen, müssen IBM Trusteer Pinpoint Detect Redeployment erwerben.

Eine erneute Bereitstellung kann erforderlich sein, wenn der Kunde die Domäne oder Host-URL der Anwendung geändert hat, die Online-Anwendung auf eine neue Technologie umstellt, auf eine neue Online-Banking-Plattform umzieht oder einer vorhandenen Anwendung einen neuen Anmeldeablauf hinzufügt.

Während der 6-monatigen Übergangszeit für die erneute Bereitstellung hat der Kunde auf Eins-zu-eins-Basis Anspruch auf zusätzliche Anwendungen, die neben den bereits per Subscription erworbenen Anwendungen ausgeführt werden können.

1.5.8 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support und/oder IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Kunden, die den Cloud-Service Pinpoint Detect Standard erwerben, können in Verbindung damit Premium-Support-Service erwerben. Der Leistungsumfang der Premium-Support-Services wird unten in Abschnitt 4 beschrieben.

1.5.9 IBM Trusteer Digital Content Pack for Retail und/oder IBM Trusteer Digital Content Pack for Business

Das IBM Trusteer Digital Content Pack ermöglicht Sicherheitsanalysten die Integration neuer Betrugsmodelle und unterstützt gleichzeitig die Erstellung und Bearbeitung von Ad-hoc-Modellen, um auf entstehende Bedrohungen reagieren zu können. Das Paket besteht aus umfangreichen Regeln, Erkenntnissen und Richtlinien und kann als zusätzlicher und integraler Bestandteil der Lösung erworben werden. Mit dem Digital Content Pack wird die Integration zwischen den digitalen Betrugsverhinderungsfunktionen von Trusteer und den Kanälen für den bargeldlosen Zahlungsverkehr von IBM Safer Payments noch weiter vertieft. Durch Nutzung der integrierten Regeln und der besonderen Geschäftslogik ermöglicht das Digital Content Pack Banken und anderen Finanzinstituten die weitere Verbesserung vorhandener Betrugserkennungs- und -verhinderungsfunktionen.

Das IBM Trusteer Digital Content Pack for Retail ist in Paketen mit jeweils 100 berechtigten Teilnehmern verfügbar. Das IBM Trusteer Digital Content Pack for Business ist in Paketen mit jeweils 10 berechtigten Teilnehmern verfügbar.

Für die Integration des Digital Content Packs mit Pinpoint Detect und IBM Safer Payments und für Unterstützungsleistungen mit besonderen Anforderungen sind Beratungsleistungen erforderlich. Diese können gesondert im Rahmen einer Leistungsbeschreibung erworben werden.

1.5.10 IBM Trusteer New Account Fraud for Retail und/oder IBM Trusteer New Account Fraud for Business

Dieser für Pinpoint-Subskribenten verfügbare Service ist dazu ausgelegt, bei der Erstellung neuer Konten frühzeitig Unregelmäßigkeiten zu erkennen, verdächtige Aktivitäten zu markieren und Warnungen zu generieren. Der Service überwacht neue Konten über die in der TMA verfügbaren Nutzungsberichte, um betrügerische Aktivitäten, die neu angelegte Konten und danach die bestehenden Konten betreffen, durch Account Profiling aufzudecken und durch eine Frühwarnung anzuzeigen, dass es sich bei dem neuen Konto möglicherweise um einen „Mule Account“ handelt oder um ein Konto, das für Betrügereien benutzt wird.

IBM Trusteer New Account Fraud for Retail und IBM Trusteer New Account Fraud for Business sind in Paketen mit jeweils 10 API-Aufrufen erhältlich.

1.5.11 IBM Trusteer Pinpoint Verify

Der Kunde muss über eine aktuelle Subscription für IBM Trusteer Pinpoint Detect Premium verfügen, bevor er eine Subscription für diesen Cloud-Service erwirbt.

Dieser Cloud-Service bietet Funktionen, um von Benutzern beim Zugriff auf einen digitalen Service die Eingabe eines zweiten Authentifizierungsfaktors zur Überprüfung ihrer Identität zu verlangen. Der Service ist für Pinpoint Detect Premium verfügbar, um einen zweiten Authentifizierungsfaktor für geschützte Anwendungen bereitzustellen. Die Entscheidung darüber, wann die Benutzer zur Zwei-Faktor-Authentifizierung aufgefordert werden, wird durch die geschützte Anwendung abgeleitet und kann auf den Empfehlungen der Pinpoint Detect Premium-Plattform oder anderen von der geschützten Anwendung definierten Richtlinien basieren.

1.6 IBM Trusteer Pinpoint Assure

Dieser Service markiert verdächtige Aktivitäten und generiert Warnungen während des Erstellungs-/Registrierungsprozesses eines neuen Kontos. Der Service überwacht den Kontoregistrierungsprozess, um betrügerische Aktivitäten aufzudecken und durch eine Frühwarnung anzuzeigen, dass es sich bei dem neuen Konto möglicherweise um einen „Mule Account“ oder um ein Konto handelt, das für Betrügereien benutzt wird. Entsprechende Nutzungsberichte sind in der TMA verfügbar.

IBM Trusteer Pinpoint Assure ist in Paketen mit 100 Verbindungen verfügbar.

1.6.1 Optionale Services für IBM Trusteer Pinpoint Assure

1.6.2 IBM Trusteer Pinpoint Assure Application

Wenn IBM Trusteer Pinpoint Assure für eine Anwendung bereitgestellt werden soll, muss eine Berechtigung für IBM Trusteer Pinpoint Assure Application erworben werden.

IBM Trusteer Pinpoint Assure kann pro Anwendung erworben werden.

1.6.3 IBM Trusteer Mobile Carrier Intelligence und/oder IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Der Kunde muss über eine aktuelle Subscription für entweder IBM Trusteer Pinpoint Assure oder IBM Trusteer Pinpoint Detect verfügen, bevor er eine Subscription für diesen Cloud-Service erwirbt.

Dieser Cloud-Service erweitert IBM Trusteer Pinpoint Assure und/oder IBM Trusteer Pinpoint Detect. Er bietet zusätzliche Informationen und zusätzlichen Kontext zu Mobiltelefonnummern, die diesen beiden Cloud-Services zur Verfügung gestellt werden, und trägt so dazu bei, das Betrugsrisiko einer bestimmten Sitzung zu ermitteln. Der Kunde kann durch eine Abfrage des Cloud-Service Merkmale einer bestimmten Mobiltelefonnummer herausfinden, z. B. Informationen über den Mobilfunkanbieter im Zusammenhang mit dieser Nummer.

Die von diesem Cloud-Service bereitgestellten Daten zu Mobiltelefonnummern (nachfolgend „Mobile-Intelligence-Daten“ genannt) dürfen vom Kunden nur zu internen Zwecken verwendet und nur dreißig (30) Tage lang aufbewahrt werden. Nach diesem Zeitraum muss der Kunde eine erneute Abfrage des Cloud-Service bezüglich derselben Mobiltelefonnummer durchführen, um Mobile-Intelligence-Daten zu dieser Nummer zu erhalten, und kann nicht einfach die bei einer früheren Abfrage erhaltenen Mobile-Intelligence-Daten wiederverwenden. Der Kunde darf Mobile-Intelligence-Daten weder ganz noch teilweise zwischenspeichern (ausgenommen wie oben erlaubt), wiederverwenden oder in Verbindung mit Data-Mining nutzen oder archivieren.

1.7 IBM Trusteer Remotely Delivered Services

Die IBM Trusteer Remotely Delivered Services sind als optionales Add-on für die Cloud-Services Pinpoint Detect Premium und Pinpoint Assure verfügbar.

1.7.1 IBM Trusteer Project Management and Consultancy Services

Dieser Service bietet Beratungsleistungen im Umfang von bis zu 200 Stunden, in denen IBM einige oder alle der folgenden Maßnahmen durchführen wird:

a. Anfängliche Einrichtungsservices: häufige regelmäßige Besprechungen, Projektmanagementservices

b. Richtlinienmanager: fortlaufender Support

Dieses Angebot kann auf der Basis eines Kundenprojekts erworben werden.

1.7.2 IBM Trusteer Security Research Consultancy Services

Dieser Beratungsservice beinhaltet bis zu 200 Stunden an gemeinsam genutzten Ressourcen für eine Sicherheitsanalyse, um zusätzlich zum Leistungsumfang der definierten Lösung und des Premium Support (sofern zutreffend) folgende Leistungen bereitzustellen:

a. Erweiterte Betrugsuntersuchung: wöchentliche Besprechungen und Schulung

b. Support mit hoher Priorität für das Kunden-Release

c. Fortlaufende Untersuchung angepasster Regeln und Support

Dieses Angebot kann auf der Basis eines Kundenprojekts erworben werden.

1.7.3 IBM Trusteer Training Services

Dieser Beratungsservice bietet zusätzlich zum Leistungsumfang der definierten Lösung und des Premium Supports (sofern zutreffend) weitere Leistungen und beinhaltet Schulungsservices für die Mitarbeiter eines Kunden zum Trusteer-Portfolio.

Dieses Angebot kann auf der Basis eines Kundenprojekts erworben werden.

1.8 IBM Trusteer Mobile-Cloud-Services

1.8.1 IBM Trusteer Mobile SDK for Business und/oder IBM Trusteer Mobile SDK for Retail

Die IBM Trusteer Mobile SDK-Cloud-Services sorgen für zusätzlichen Schutz, indem sie sicheren Webzugriff auf die Business- und/oder Retail-Anwendungen ermöglichen, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat, und bieten Risikobewertungen für Geräte sowie Pharming-Schutz. Die Erkennung sicherer WiFi-Umgebungen ist nur für Android-Plattformen verfügbar.

Die IBM Trusteer Mobile SDK-Cloud-Services enthalten ein proprietäres Mobile Software Developer Kit („SDK“) (dabei handelt es sich um ein Softwarepaket, das Dokumentation, proprietäre Softwareprogrammierbibliotheken sowie weitere zugehörige Dateien und Elemente enthält, die sogenannte IBM Trusteer Mobile Library) sowie die „Run-time-Komponente“ bzw. „weiterverteilbare Komponente (Redistributable)“, einen proprietären Code, der vom IBM Trusteer Mobile SDK generiert wird und in die geschützten eigenständigen mobilen iOS- oder Android-Anwendungen eingebettet und integriert werden kann, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat („Integrierte mobile App des Kunden“) („Integrierte mobile App des Kunden“).

IBM Trusteer Mobile SDK for Retail ist in Paketen mit jeweils 100 berechtigten Teilnehmern oder 100 Clienteinheiten verfügbar und IBM Trusteer Mobile SDK for Business ist in Paketen mit jeweils 10 berechtigten Teilnehmern oder 10 Clienteinheiten verfügbar.

Über die TMA kann der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) Ereignisdatenberichte und Einschätzungen zu Risikobewertungen empfangen. Über die integrierte mobile App kann der Kunde Risikoanalyseinformationen und Informationen empfangen, die sich auf die mobilen Geräte der berechtigten Teilnehmer beziehen, die seine integrierte mobile App heruntergeladen haben. Diese Informationen ermöglichen dem Kunden die Definition einer Betrugspräventionsrichtlinie, um Maßnahmen zur Minderung dieser Risiken durchzusetzen. Für die Zwecke dieses Angebots schließt der Begriff „mobile Geräte“ nur unterstützte Mobiltelefone und Tablets ein, aber keine PCs oder Mac-Computer.

Der Kunde darf:

a. das IBM Trusteer Mobile SDK ausschließlich intern für die Entwicklung der integrierten mobilen App des Kunden nutzen.

b. die weiterverteilbare Komponente (nur in Objektcodeformat) als festen, untrennbaren Bestandteil in seine integrierte mobile App einbetten. Jeder geänderte oder eingefügte Bestandteil einer weiterverteilbaren Komponente unterliegt gemäß der Lizenz den Bestimmungen dieser Servicebeschreibung; und

c. die weiterverteilbare Komponente zum Download auf die mobilen Geräte der berechtigten Teilnehmer oder des Inhabers der Clienteinheit vertreiben und weitergeben, sofern folgende Bedingungen eingehalten werden:

   - Soweit nicht ausdrücklich in dieser Vereinbarung vorgesehen, ist es dem Kunden untersagt, (1) das SDK zu verwenden, zu kopieren, zu ändern oder weiterzugeben, (2) das SDK rückumzuwandeln (reverse assemble, reverse compile), in anderer Weise zu übersetzen oder rückzuentwickeln, sofern eine solche Umwandlung nicht durch ausdrückliche gesetzliche Regelung unabdingbar vorgesehen ist, (3) das SDK zu vermieten, zu verleasen oder diesbezügliche Unterlizenzen zu erteilen; (4) Copyright- oder Notice-Dateien zu entfernen, die in der weiterverteilbaren Komponente enthalten sind, (5) dieselben Pfadnamen wie für die Dateien/Module der ursprünglichen weiterverteilbaren Komponente zu verwenden und (6) die Namen oder Marken von IBM, ihren Lizenzgebern oder Distributoren ohne ihre vorherige schriftliche Zustimmung in Verbindung mit der Vermarktung seiner integrierten mobilen App zu verwenden.
   - Die weiterverteilbare Komponente muss als fester, untrennbarer Bestandteil in die integrierte mobile App des Kunden eingebettet bleiben. Sie darf nur in Objektcodeformat vorhanden sein und muss allen Anweisungen, Instruktionen und Spezifikationen im SDK und der zugehörigen Dokumentation entsprechen. In der Endbenutzerlizenzvereinbarung für die integrierte mobile App des Kunden muss ein Hinweis für den Endbenutzer enthalten sein, dass die weiterverteilbare Komponente i) nur zur Aktivierung der integrierten mobilen App des Kunden verwendet werden darf, ii) nicht kopiert werden darf (außer für Sicherungszwecke), iii) nicht weitergegeben oder übertragen werden darf und iv) nicht rückumgewandelt (reverse assemble, reverse compile) oder in anderer Weise übersetzt werden darf, soweit nicht durch gesetzliche Regelung etwas anderes zwingend vorgeschrieben ist. Die Lizenzvereinbarung des Kunden muss die Rechte von IBM in mindestens demselben Maße schützen, wie sie durch die Bedingungen dieser Vereinbarung geschützt werden.
   - Das SDK darf nur für interne Entwicklungszwecke und Komponententests auf den angegebenen mobilen Testgeräten des Kunden eingesetzt werden. Der Kunde ist nicht berechtigt, das SDK zur Verarbeitung oder Simulation von Produktionsworkloads oder zum Testen der Skalierbarkeit von Code, Anwendungen oder Systemen zu nutzen. Er ist ferner nicht berechtigt, Teile des SDK für andere Zwecke zu verwenden.

Der Kunde ist allein verantwortlich für die Entwicklung, das Testen und die Unterstützung seiner integrierten mobilen App. Der Kunde trägt die Verantwortung für die gesamte technische Unterstützung seiner integrierten mobilen App sowie für sämtliche von ihm durchgeführten Bearbeitungen der weiterverteilbaren Komponenten, die gemäß diesem Dokument zulässig sind.

Der Kunde darf die weiterverteilbare Komponente und das IBM Security Mobile SDK nur zur Unterstützung seiner Nutzung der Cloud-Services installieren und verwenden.

IBM garantiert nicht, dass eine Anwendung oder Ausgabe, die mit den mobilen Tools im IBM Security Mobile SDK erstellt wird, mit einer bestimmten mobilen Betriebssystemplattform oder einem bestimmten Mobilgerät funktioniert, interoperabel oder kompatibel ist.

Quellenkomponenten und Beispielmaterialien – Das IBM Trusteer Mobile SDK kann einige Komponenten in Quellcodeform (nachfolgend „Quellenkomponenten“ genannt) und sonstige Materialien enthalten, die als Beispielmaterialien gekennzeichnet sind. Der Kunde darf die Quellenkomponenten und Beispielmaterialien nur zur internen Verwendung kopieren und ändern, sofern eine solche Verwendung im Rahmen der Lizenzrechte unter dieser Vereinbarung erfolgt und keine in den Quellenkomponenten oder Beispielmaterialien enthaltenen Copyrightvermerke geändert oder gelöscht werden. IBM stellt die Quellenkomponenten und Beispielmaterialien ohne Verpflichtung zur Unterstützung im gegenwärtigen Zustand (auf „as-is“-Basis) zur Verfügung. Es wird ausdrücklich darauf hingewiesen, dass die Quellenkomponenten oder Beispielmaterialien lediglich als Beispiel für die Implementierung der

Embeddable in das CIMA bereitgestellt werden. Die Quellenkomponenten oder Beispielmaterialien sind mit der Entwicklungsumgebung des Kunden unter Umständen nicht kompatibel, und der Kunde ist allein für das Testen und die Implementierung der Embeddable in das CIMA verantwortlich.

2. Inhalte und Datenschutz

Das Datenblatt für Datenverarbeitung und Datenschutz (Data Processing and Protection Data Sheet, nachfolgend „Datenblatt“ genannt) enthält relevante Informationen über den Cloud-Service in Bezug auf die Art der Inhalte, die für die Verarbeitung freigegeben sind, die damit verbundenen Verarbeitungsaktivitäten, die Datenschutzfunktionen und die Besonderheiten hinsichtlich der Aufbewahrung und Rückgabe der Inhalte. Alle Einzelheiten oder Erläuterungen und Bedingungen, einschließlich der Verantwortlichkeiten des Kunden, im Zusammenhang mit der Nutzung des Cloud-Service und der Datenschutzfunktionen, sofern anwendbar, werden in diesem Abschnitt beschrieben. Abhängig von den vom Kunden gewählten Optionen und dessen Nutzung des Cloud-Service können mehrere Datenblätter zur Anwendung kommen. Das Datenblatt ist ggf. nur in englischer Sprache und nicht in einer Landessprache verfügbar. Trotz lokaler Gesetze oder Gepflogenheiten bestätigen die Vertragsparteien, dass sie Englisch verstehen und diese Sprache für den Erwerb und die Nutzung der Cloud-Services geeignet ist. Die folgenden Datenblätter beziehen sich auf den Cloud-Service und die verfügbaren Optionen. Der Kunde bestätigt, dass i) IBM die Datenblätter von Zeit zu Zeit nach eigenem Ermessen ändern kann und dass ii) diese Änderungen frühere Versionen ersetzen. Alle Änderungen an den Datenblättern werden mit der Absicht durchgeführt, i) bestehende Verpflichtungen von IBM zu verbessern oder transparenter zu gestalten, ii) die Umsetzung neu eingeführter Standards und anwendbarer Gesetze sicherzustellen oder iii) zusätzliche Verpflichtungen seitens IBM aufzunehmen. Durch Änderungen an den Datenblättern wird der Datenschutz in Bezug auf einen Cloud-Service nicht verringert.

Link(s) zu den anwendbaren Datenblättern:

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

(Das Datenblatt für IBM Cloud Identity Verify spiegelt IBM Trusteer Pinpoint Verify wider.)

Der Kunde ist dafür verantwortlich, die verfügbaren Datenschutzfunktionen für einen Cloud-Service zu bestellen, zu aktivieren und anzuwenden, und übernimmt die Verantwortung für die Nutzung der Cloud-Services, wenn er dieser Verpflichtung nicht nachkommt. Dies gilt auch für die Erfüllung von Datenschutzanforderungen sowie anderer rechtlicher Anforderungen in Bezug auf Inhalte.

Die Ergänzenden Bedingungen zur Auftragsverarbeitung (EB-AV) von IBM unter http://ibm.com/dpa und die zugehörigen Anlagen finden Anwendung und ergänzen diese Vereinbarung, wenn und soweit IBM personenbezogene Daten im Auftrag des Kunden verarbeitet und die europäische Datenschutz-Grundverordnung (EU/2016/679) (DSGVO) auf diese Verarbeitung Anwendung findet. Die für diesen Cloud-Service anwendbaren Datenblätter dienen als Anlagen zu den EB-AV. Sofern die EB-AV Anwendung finden, richtet sich die Verpflichtung von IBM, Änderungen bezüglich der Unterauftragsverarbeiter bekannt zu geben, und das Recht des Kunden, Einspruch gegen eine solche Änderung einzulegen, nach den Regelungen in den EB-AV.

2.1 EULA und die Grundlage für die Verarbeitung von Daten betroffener Personen

Für IBM Trusteer Rapport-Cloud-Services (einschließlich Rapport Remediation oder Rapport for Mitigation, wenn die Bereitstellung in Verbindung mit den Pinpoint-Cloud-Services erfolgt):

Sofern nicht abweichend vereinbart und gemäß der Verarbeitungsgrundlage, die der Kunde selbst festgelegt hat, erteilt der Kunde IBM die Berechtigung, die unter https://www.trusteer.com/support/end-user-license-agreement verfügbare Endbenutzerlizenzvereinbarung bereitzustellen, damit IBM die für die Erbringung der Cloud-Services benötigten Informationen erfassen und verarbeiten kann.

2.2 Nutzung von Daten

IBM wird die Ergebnisse, die sich aus der Nutzung des Cloud-Service durch den Kunden ergeben und sich eindeutig auf Kundeninhalte beziehen (Erkenntnisse) oder den Kunden anderweitig identifizieren, weder verwenden noch offenlegen. IBM ist jedoch berechtigt, Inhalte und andere Informationen (ausgenommen Erkenntnisse), die sich im Laufe der Erbringung des Cloud-Service aus den Inhalten ergeben, zu verwenden, sofern persönliche Kennungen entfernt wurden und personenbezogene Daten ohne die Verwendung zusätzlicher Informationen nicht mehr einer bestimmten Person zugeordnet werden können. IBM wird diese Daten ausschließlich für Forschungs- und Testzwecke sowie für die Angebotsentwicklung verwenden.

2.3 Datenverarbeitung und -speicherung

2.3.1 Zusätzliche Informationen zum Verarbeitungsstandort

Alle für die Trusteer Pinpoint Verify Services relevanten Hosting- und Verarbeitungsstandorte sind im maßgeblichen Datenblatt angegeben.

Bei allen anderen Services, die über das Rechenzentrum in Deutschland erbracht werden, beschränkt IBM die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, und auf die folgenden Länder: Deutschland, Israel, Irland, die Niederlande und alle zusätzlichen Länder, die im anwendbaren Datenblatt für externe Unterauftragsverarbeiter von IBM aufgelistet sind.

Bei allen anderen Services, die über das Rechenzentrum in Japan erbracht werden, beschränkt IBM die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, und auf die folgenden Länder: Japan, Israel, Irland und alle zusätzlichen Länder, die im anwendbaren Datenblatt für externe Unterauftragsverarbeiter von IBM aufgelistet sind.

Bei allen anderen Services, die über das Rechenzentrum in den USA erbracht werden, beschränkt IBM die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, und auf die folgenden Länder: USA, Israel, Irland, Singapur, Australien und alle zusätzlichen Länder, die im anwendbaren Datenblatt für externe Unterauftragsverarbeiter von IBM aufgelistet sind.

IBM Trusteer-Support- und Kontowartungsservices können bei Bedarf ebenfalls erbracht werden und richten sich nach der Verfügbarkeit der entsprechenden IBM Mitarbeiter, dem Standort des Kunden und dem Rechenzentrum, in dem die Daten gehostet sind.

2.3.2 Daten des Kontoinhabers

Die Daten des Kontoinhabers werden in der Region verarbeitet, in der die Client-Software für Kontoinhaber ursprünglich vom Kontoinhaber installiert wurde. Dies kann bedeuten, dass die Inhalte des Kontoinhabers sowohl in der Ursprungsregion als auch in der mit dem Kunden vereinbarten Region verarbeitet werden können.

2.3.3 Integrierte Lösungen

Zur Erläuterung: Da Trusteer Fraud Protection eine integrierte Lösung ist, kann IBM, selbst wenn der Kunde einen dieser Cloud-Services kündigt, Kundendaten aufbewahren, um die übrigen Cloud-Services weiterhin gemäß dieser Servicebeschreibung für den Kunden zu erbringen.

3. Service-Level-Agreement

Das folgende Service-Level-Agreement („SLA“) von IBM, das im Berechtigungsnachweis angegeben ist, beinhaltet Angaben zur Verfügbarkeit des Cloud-Service. Das SLA stellt keine Gewährleistung dar. Es wird nur Kunden zur Verfügung gestellt und gilt ausschließlich für Produktionsumgebungen.

3.1 Gutschriften für Ausfallzeiten

Der Kunde muss innerhalb von 24 Stunden, nachdem er zum ersten Mal festgestellt hat, dass ein Vorfall die Verfügbarkeit des Cloud-Service beeinträchtigt, ein Support-Ticket der Fehlerklasse 1 beim IBM Help-Desk für technische Unterstützung öffnen. Der Kunde ist verpflichtet, IBM in angemessener Weise bei der Diagnose und Lösung des Problems zu unterstützen.

Der Anspruch aus einem Support-Ticket aufgrund der Nichteinhaltung eines SLA muss innerhalb von drei Arbeitstagen nach Ablauf des Vertragsmonats geltend gemacht werden. Die Entschädigung für einen berechtigten Anspruch aus einem SLA wird als Gutschrift gewährt und mit einer künftigen Rechnung für den Cloud-Service verrechnet. Sie basiert auf dem Zeitraum, in dem das Produktionssystem nicht zur Verarbeitung des Cloud-Service zur Verfügung stand („Ausfallzeit“). Die Erfassung der Ausfallzeit beginnt mit der Meldung des Vorfalls durch den Kunden und endet, wenn der Cloud-Service wiederhergestellt ist. Als Ausfallzeit zählen nicht: Zeiten für vorab geplante oder angekündigte Unterbrechungen zur Durchführung von Wartungsarbeiten; Gründe, die IBM nicht zu vertreten hat; Probleme mit dem Inhalt, der Technologie, den Entwürfen oder Anweisungen des Kunden oder Dritter; nicht unterstützte Systemkonfigurationen und Plattformen oder andere Fehler des Kunden; vom Kunden verursachte Sicherheitsvorfälle oder vom Kunden durchgeführte Sicherheitstests. IBM wird die höchstmögliche Entschädigung basierend auf der kumulierten Verfügbarkeit des Cloud-Service während jedes einzelnen Vertragsmonats anwenden (siehe die nachstehende Tabelle). Die Gesamtentschädigung für einen beliebigen Vertragsmonat wird 10 Prozent (%) von einem Zwölftel (1/12) der Jahresgebühr für den Cloud-Service nicht überschreiten.

3.2 Service-Levels

Verfügbarkeit des Cloud-Service in einem Vertragsmonat

Verfügbarkeit in einem Vertragsmonat	**Entschädigung (in Prozent (%) der monatlichen Subscription-Gebühr* für den Vertragsmonat, der Gegenstand des Anspruchs ist)**
< 99,9 %	2 %
< 99,0 %	5 %
< 95,0 %	10 %

* Wurde der Cloud-Service von einem IBM Business Partner erworben, so wird die monatliche Subscription-Gebühr auf der Basis des zum jeweiligen Zeitpunkt gültigen Listenpreises für den Cloud-Service berechnet, der in dem Vertragsmonat wirksam war, der Gegenstand des Anspruchs ist, mit einem Abschlag von 50 Prozent (%). Eine eventuelle Rückvergütung von IBM wird direkt an den Kunden geleistet.

Service-Levels und damit verbundene Gutschriften werden separat pro Cloud-Service und pro Kundenanwendung ermittelt.

Bei der Berechnung von SLA-Gutschriften für Cloud-Services, die auf Anwendungsberechtigungen basieren, wird die Verfügbarkeit anhand der folgenden Leitlinien festgestellt:

- Jede Anwendung erhält eine Gewichtung ausgehend von ihrem Anteil am Volumen aller gezählten Sitzungen in einem bestimmten Vertragsmonat.
- Die Ausfallzeit jedes einzelnen Cloud-Service wird pro Anwendung separat für den jeweiligen Vertragsmonat kumuliert.

Im Folgenden wird in einem Beispiel die Berechnung der Aktivität für einen Monat und die entsprechende Gewichtung dargestellt. Das Beispiel dient nur zur Veranschaulichung:

Retail-Anwendungen	Anteil an der Gesamtzahl der Sitzungen in einem bestimmten Vertragsmonat	Gesamtausfallzeit in dem Vertragsmonat	Gewichtung der Ausfallminuten
Retail-Anwendung A	40 %	300 Minuten	40 % x 300 Minuten = 120 Minuten
Retail-Anwendung B	20 %	250 Minuten	20 % x 250 Minuten = 50 Minuten
Retail-Anwendung C	40 %	150 Minuten	40 % x 150 Minuten = 60 Minuten
			Gesamtausfallzeit in gewichteten Minuten = 230

Die Verfügbarkeit, ausgedrückt als Prozentsatz, wird wie folgt berechnet: Gesamtzahl der Minuten in einem Vertragsmonat, minus der Gesamtzahl der gewichteten Ausfallminuten in dem betreffenden Vertragsmonat, dividiert durch die Gesamtzahl der Minuten in dem Vertragsmonat. Die beispielhafte Berechnung basierend auf dem obigen Gewichtungsbeispiel sieht wie folgt aus:

$$\frac{\text{43.200 Minuten insgesamt in einem Vertragsmonat mit 30 Tagen} - \text{230 Minuten gewichtete Ausfallzeit} = \text{42.970 Minuten}}{\text{43.200 Minuten insgesamt}}$$

= Gutschrift für Ausfallzeiten in Höhe von 2 % bei einer Verfügbarkeit von 99,4 % in einem Vertragsmonat

4. Technische Unterstützung

Für die Cloud-Services ist technische Unterstützung verfügbar, um dem Kunden und seinen berechtigten Teilnehmern Hilfestellung bei der Nutzung der Cloud-Services zu leisten.

Bei allen Angeboten ist Standard Support in der Subscription eingeschlossen. Der Trusteer Rapport Mandatory Service ist ein Add-on zu Trusteer Rapport und setzt voraus, dass Premium Support im Rahmen der Basis-Subscription für Trusteer Rapport erworben wird.

Für jeden Cloud-Service ist eine Subscription für Premium Support gegen Zahlung einer zusätzlichen Gebühr erhältlich, mit Ausnahme der Cloud-Services **IBM Trusteer Mobile SDK** und **IBM Trusteer Rapport Mandatory Service**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital Content Pack** und **IBM Trusteer Mobile Carrier Intelligence**. Weitere Informationen können über den IBM Vertriebsbeauftragten oder den IBM Business Partner eingeholt werden.

Standard Support:

- Unterstützung von 08:00 Uhr bis 17:00 Uhr Ortszeit
- Die Kunden und ihre berechtigten Teilnehmer können Support-Tickets elektronisch einreichen, wie im „Software as a Service Support Guide“ unter https://www.ibm.com/software/support/saas_support_guide.html beschrieben.
- Über das Kundenunterstützungsportal unter http://www-01.ibm.com/software/security/trusteer haben die Kunden Zugriff auf Meldungen, Dokumente, Fallberichte und häufig gestellte Fragen (FAQs).

Premium Support:

- Unterstützung rund um die Uhr (24x7) für alle Fehlerklassen
- Der Support ist direkt per Telefon und Rückrufanfrage erreichbar
- Die Kunden und ihre berechtigten Teilnehmer können Support-Tickets elektronisch einreichen, wie im Software as a Service [SaaS] Support Handbook ausführlich beschrieben
- Über das Kundenunterstützungsportal unter http://www.ibm.com/software/security/trusteer/support/ haben die Kunden Zugriff auf Meldungen, Dokumente, Fallberichte und häufig gestellte Fragen (FAQs).

- Informationen über Unterstützungsoptionen und weitere Einzelheiten sind im „Software as a Service Support Guide“ unter https://www.ibm.com/software/support/saas_support_guide.html zu finden.

5. Informationen zur Berechtigung und Abrechnung

5.1 Gebührenmetriken

Der Cloud-Service ist mit der im Auftragsdokument angegebenen Gebührenmetrik verfügbar:

- „Kundenprojekt“ (Engagement) ist eine Maßeinheit für den Erwerb der Services. Ein Kundenprojekt besteht aus Professional Services und/oder Schulungsservices im Zusammenhang mit dem Cloud-Service. Der Kunde muss ausreichende Berechtigungen zur Abdeckung aller Kundenprojekte erwerben.
- „Berechtigter Teilnehmer“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Jede Einzelperson oder Entität, die zur Teilnahme an einem vom Cloud-Service verwalteten oder überwachten Servicebereitstellungsprogramm berechtigt ist, gilt als berechtigter Teilnehmer. Der Kunde muss ausreichende Berechtigungen erwerben, um alle berechtigten Teilnehmer abzudecken, die während des Messzeitraums, der im Auftragsdokument angegeben ist, innerhalb des Cloud-Service verwaltet oder überwacht werden.

  Die einzelnen vom Cloud-Service verwalteten Servicebereitstellungsprogramme werden separat analysiert und anschließend zusammengefasst. Alle Einzelpersonen oder Entitäten, die für mehrere Servicebereitstellungsprogramme berechtigt sind, benötigen separate Berechtigungen.

  Bezüglich der Berechtigung für diese Cloud-Services ist ein berechtigter Teilnehmer ein Endbenutzer eines Kunden, der über eindeutige Anmeldeinformationen für eine Business- oder Retail-Anwendung des Kunden verfügt.
- „Clienteinheit“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Eine Clienteinheit ist eine Datenverarbeitungseinheit eines einzelnen Benutzers, ein Spezialsensor oder ein Telemetriegerät, das eine Reihe von Befehlen, Prozeduren oder Anwendungen zur Ausführung an ein anderes Computersystem, das üblicherweise als Server bezeichnet wird, übergibt oder von diesem zur Ausführung empfängt, Daten für den Server bereitstellt oder vom Server verwaltet wird. Mehrere Clienteinheiten können gemeinsam auf einen Server zugreifen. Eine Clienteinheit kann über gewisse Verarbeitungsfunktionen verfügen oder programmierbar sein, sodass ein Benutzer Arbeiten ausführen kann. Der Kunde muss für jede Clienteinheit Berechtigungen erwerben, die in Verbindung mit dem Cloud-Service ausgeführt wird, Daten an den Cloud-Service liefert, vom Cloud-Service bereitgestellte Services nutzt oder auf andere Weise während des Messzeitraums, der im Auftragsdokument angegeben ist, auf den Cloud-Service zugreift.
- „Anwendung“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Eine Anwendung ist ein eindeutig benanntes Softwareprogramm. Der Kunde muss ausreichende Berechtigungen für alle Anwendungen erwerben, die während des Messzeitraums, der im Berechtigungsnachweis oder Auftragsdokument angegeben ist, zum Zugriff und zur Nutzung bereitgestellt werden.

  Für die Zwecke dieses Cloud-Service ist eine Anwendung eine einzelne Business- oder Retail-Anwendung des Kunden.
- „API-Aufruf“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Ein API-Aufruf ist der Aufruf des Cloud-Service über eine programmierbare Schnittstelle. Es müssen ausreichende Berechtigungen erworben werden, um die Gesamtzahl der API-Aufrufe (aufgerundet auf die nächsten Zehn) während des Messzeitraums abzudecken, der im Berechtigungsnachweis oder Auftragsdokument des Kunden angegeben ist.
- „Verbindung“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Eine Verbindung ist die Anbindung oder Zuordnung einer Datenbank, einer Anwendung, eines Servers oder einer anderen Art von Einheit zum Cloud-Service. Der Kunde muss ausreichende Berechtigungen erwerben, um die Gesamtzahl der Verbindungen abzudecken, die während des Messzeitraums, der im Berechtigungsnachweis oder Auftragsdokument angegeben ist, zum Cloud-Service hergestellt wurden oder hergestellt werden.

  Für die Zwecke dieses Cloud-Service ist eine Verbindung eine Sitzung oder ein Datenfluss in der Anwendung des Kunden.

5.2 Zusatzgebühren

Wenn die tatsächliche Nutzung des Cloud-Service während des Messzeitraums die im Berechtigungsnachweis angegebene Berechtigung überschreitet, wird die Nutzungsüberschreitung im Folgemonat zu dem im Auftragsdokument angegebenen Gebührensatz in Rechnung gestellt.

5.3 Abrechnungshäufigkeit

Ausgehend von der gewählten Abrechnungshäufigkeit wird IBM dem Kunden die fälligen Gebühren zu Beginn des Abrechnungszeitraums in Rechnung stellen, mit Ausnahme von Gebühren für Nutzungsüberschreitungen und spezifischen Nutzungsgebühren, die rückwirkend berechnet werden.

6. Laufzeit und Verlängerungsoptionen

Die Laufzeit des Cloud-Service beginnt an dem Datum, an dem IBM dem Kunden mitteilt, dass sein Zugriff auf den Cloud-Service gemäß der Angabe im Berechtigungsnachweis freigeschaltet ist. Im Berechtigungsnachweis ist festgelegt, ob sich der Cloud-Service automatisch verlängert, auf fortlaufender Basis genutzt werden kann oder am Ende der Laufzeit abläuft.

Bei automatischer Verlängerung wird der Cloud-Service automatisch um die im Berechtigungsnachweis angegebene Laufzeit verlängert, es sei denn, der Kunde teilt IBM mindestens 90 Tage vor dem Ablaufdatum schriftlich mit, dass er keine Verlängerung wünscht. Verlängerungen unterliegen einer jährlichen Preiserhöhung gemäß der Angabe in einem Angebot. Falls die automatische Verlängerung nach der Benachrichtigung von IBM über die Vertriebseinstellung des Cloud-Service eintritt, endet die Verlängerungslaufzeit mit Ablauf der derzeitigen Verlängerungslaufzeit oder zum angekündigten Datum der Vertriebseinstellung, wobei das frühere Datum maßgeblich ist.

Bei fortlaufender Nutzung steht der Cloud-Service auf monatlicher Basis ununterbrochen zur Verfügung, bis der Kunde unter Einhaltung einer Frist von 90 Tagen schriftlich kündigt. Der Cloud-Service bleibt nach Ablauf der 90-Tage-Frist bis zum Ende des Kalendermonats verfügbar.

7. Zusätzliche Bedingungen

7.1 Allgemein

Der Kunde erklärt sich damit einverstanden, dass IBM in Werbe- oder Marketingmaterial öffentlich auf den Kunden als Subskribenten der Cloud-Services verweisen darf.

Es ist dem Kunden untersagt, Cloud-Services, allein oder in Kombination mit anderen Services oder Produkten, zur Unterstützung risikoreicher Aktivitäten wie Planung, Errichtung, Kontrolle oder Wartung von Nuklearanlagen, Massentransportsystemen, Luftverkehrskontrollsystemen, Fahrzeugsteuerungssystemen, Waffensystemen oder für die Luftfahrzeugnavigation oder Luftfahrzeugkommunikation oder für andere Aktivitäten zu verwenden, bei denen ein Versagen des Cloud-Service zum Tod oder zu ernsthaften Verletzungen führen kann.

7.2 Aktivierungssoftware

Für den Cloud-Service ist Aktivierungssoftware erforderlich, die der Kunde auf seine Systeme herunterladen muss, um die Nutzung des Cloud-Service zu ermöglichen. Der Kunde darf die Aktivierungssoftware nur in Verbindung mit dem Cloud-Service verwenden. Die Aktivierungssoftware wird im gegenwärtigen Zustand (auf „as-is“-Basis) bereitgestellt.

7.3 Bereitstellung von IBM Trusteer Fraud Protection

Für jede vom Kunden per Subscription erworbene Anwendung sind in der Basis-Subscription des Kunden die erforderlichen Aktivitäten für die Einrichtung (Setup) und erstmalige Bereitstellung in der IBM Trusteer-Cloud sowie die einmalige Inbetriebnahme, die Konfiguration, die Splash-Vorlage sowie Tests und Schulungen eingeschlossen.

Die Bereitstellungsaktivitäten beinhalten keine Implementierungsaktivitäten, die für die Anwendungen oder Systeme des Kunden erforderlich sind.

Die Implementierungsphase der verschiedenen Cloud-Services soll innerhalb des Zeitrahmens abgeschlossen werden, der in den jeweiligen Deployment Guides angegeben ist.

Der Abschluss dieser Implementierungsphasen innerhalb des vorgesehenen Zeitrahmens ist vom uneingeschränkten Einsatz und der Beteiligung durch das Management und Personal des Kunden

abhängig. Die erforderlichen Informationen müssen vom Kunden zeitnah bereitgestellt werden. Voraussetzungen für die Leistungserbringung durch IBM sind die rechtzeitige Bereitstellung von Informationen sowie zeitnahe Entscheidungen des Kunden, und sämtliche Verzögerungen können zusätzliche Kosten und/oder Verzögerungen bei der Durchführung der Implementierungsservices zur Folge haben.

Für jede vom Kunden per Subscription erworbene Anwendung sind in der Basis-Subscription des Kunden die erforderlichen Aktivitäten für die Einrichtung (Setup) und erstmalige Bereitstellung in der IBM Trusteer-Cloud sowie die einmalige Inbetriebnahme, die Konfiguration, die Splash-Vorlage sowie Tests und Schulungen eingeschlossen.

Die Subscription des Kunden beinhaltet Unterstützung und Durchführung von Tests für die Seiten innerhalb der Kundenanwendung, die, wie von IBM bei der erstmaligen Bereitstellung empfohlen, markiert („getaggt“) werden. IBM ist nicht verantwortlich für (i) eine nur teilweise durchgeführte Bereitstellung, (ii) die Entscheidung des Kunden, die IBM Cloud-Services nicht nach der Empfehlung von IBM bereitzustellen, (iii) die Entscheidung des Kunden, die Bereitstellung, Einrichtung und Tests selbst durchzuführen, oder (iv) eine nur teilweise durchgeführte Bereitstellung oder Absicherung aufgrund unzureichender Informationen des Kunden. Weitere Services, einschließlich Bereitstellungsaktivitäten, die über die erstmalige Bereitstellung hinausgehen, können gegen Zahlung einer zusätzlichen Gebühr unter einem separaten Vertrag vereinbart werden.