IBM Trusteer Fraud Protection

Diese Servicebeschreibung bezieht sich auf den von IBM für den Kunden bereitgestellten Cloud-Service. 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:

Rapport-Cloud-Services:

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail
- 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 for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Business

- IBM Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Criminal Detection Additional Applications 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 Criminal Detection Redeployment
- 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 Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- 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 with access management integration for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support
- IBM Trusteer Pinpoint Detect Standard For Business Premium Support

Mobile-Cloud-Services:

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

- IBM Trusteer Mobile Browser for Retail
- IBM Trusteer Mobile Browser for Retail Premium Support

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 for Business
- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business

1.1.2 Retail-Cloud-Services

- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser 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

a. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Rapport 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 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.

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

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

a. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition oder IBM Trusteer Pinpoint Malware Detection for Business Standard Edition bzw. für IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business oder IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business:
   - IBM Trusteer Pinpoint Carbon Copy 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 for Retail Advanced Edition oder IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition bzw. für IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition oder IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition:
   - IBM Trusteer Pinpoint Carbon Copy 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. Eine Subscription für IBM Trusteer Pinpoint Malware Detection for Business oder IBM Trusteer Pinpoint Malware Detection for Retail oder IBM Trusteer Pinpoint Malware Detection II for Business oder IBM Trusteer Pinpoint Malware Detection II for Retail ist die Voraussetzung für die zugehörigen zusätzlichen Cloud-Services, die in diesem Abschnitt aufgelistet sind.

1.1.5 Zusätzliche Cloud-Services für IBM Trusteer Pinpoint Criminal Detection und/oder IBM Trusteer Pinpoint Criminal Detection II

a. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Pinpoint Criminal Detection for Business oder IBM Trusteer Pinpoint Criminal Detection II:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Pinpoint Criminal Detection for Retail und/oder IBM Trusteer Pinpoint Criminal Detection II for Retail:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Für bestimmte Angebote ist, wie in diesem Dokument angegeben, Premium Support verfügbar.

Eine Subscription für IBM Trusteer Pinpoint Criminal Detection for Business oder IBM Trusteer Pinpoint Criminal Detection for Retail oder IBM Trusteer Pinpoint Criminal Detection II for Business oder IBM

Trusteer Pinpoint Criminal Detection II for Retail ist die Voraussetzung für die zugehörigen zusätzlichen Cloud-Services, die in diesem Abschnitt aufgelistet sind.

1.1.6 Zusätzliche Cloud-Services für IBM Trusteer Pinpoint Detect Standard und/oder IBM Trusteer Pinpoint Detect Premium und/oder IBM Security Pinpoint Detect Standard with access management integration und/oder IBM Security Detect Premium with access management integration

a. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Detect Standard for Business und/oder IBM Trusteer Pinpoint Detect Premium for Business und/oder IBM Security Pinpoint Detect Standard with access management integration for Business und/oder IBM Security Detect Premium with access management integration for Business:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

b. Zusätzlich verfügbare Cloud-Services für IBM Trusteer Detect Standard for Retail und/oder IBM Trusteer Pinpoint Detect Premium for Retail und/oder IBM Security Pinpoint Detect Standard with access management integration for Retail und/oder IBM Security Detect Premium with access management integration for Retail:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

Eine Subscription für IBM Trusteer Detect Standard oder IBM Trusteer Pinpoint Detect Premium oder IBM Security Pinpoint Detect Standard with access management integration oder IBM Security Detect Premium with access management integration ist die Voraussetzung für die zugehörigen zusätzlichen Cloud-Services, die in diesem Abschnitt aufgelistet sind.

1.1.7 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, die Clientaktivierungssoftware von IBM Trusteer Mobile Browser oder jede andere Clientaktivierungssoftware, die mit einigen Cloud-Services zur 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.

2. IBM Trusteer Rapport-Cloud-Services

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

Trusteer Rapport 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.

Dieser Cloud-Service ist mit der Gebührenmetrik erhältlich, 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.

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 den 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 beim Zugriff auf die Business- und/oder Retail-Anwendungen, 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. Unter einem separaten Vertrag oder einer separaten Leistungsbeschreibung kann eine Splash-Anpassung vereinbart werden.

Der Kunde kann Marken, Logos oder Symbole zur Verwendung in Verbindung mit der TMA zur Verfügung stellen, die im Trusteer Splash und in der Client-Software für Kontoinhaber oder auf den von IBM gehosteten Landing-Pages sowie auf der IBM Trusteer-Website angezeigt werden können. 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.

2.2 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 eine Schutzstufe 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 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.

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 den 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 beim Zugriff auf die Business- und/oder Retail-Anwendungen, 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. Unter einem separaten Vertrag oder einer separaten Leistungsbeschreibung kann eine Splash-Anpassung vereinbart werden.

Der Kunde kann Marken, Logos oder Symbole zur Verwendung in Verbindung mit der TMA zur Verfügung stellen, die im Trusteer Splash und in der Client-Software für Kontoinhaber oder auf den von IBM gehosteten Landing-Pages sowie auf der IBM Trusteer-Website angezeigt werden können. 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.

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

Eine Subscription für die IBM Trusteer Rapport-Cloud-Services oder die IBM Trusteer Rapport II-Cloud-Services ist die Voraussetzung für die Subscription für einen der folgenden zusätzlichen 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, die die Client-Software für Kontoinhaber ausführen, den EULA akzeptiert und sich bei mindestens einer Business- und/oder Retail-Anwendung des Kunden authentifiziert haben, und sofern die Konfiguration des Kunden die betreffenden Benutzer-IDs enthält.

2.3.1 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.

2.3.2 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.

2.3.3 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.

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

Kunden, die ihre Online-Banking-Anwendungen während der Servicelaufzeit erneut bereitstellen und folglich Änderungen an ihrer Bereitstellung von IBM Trusteer Rapport oder 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.

2.3.5 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.

3. 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.

3.1 IBM Trusteer Pinpoint Malware Detection und IBM Trusteer Pinpoint Criminal Detection

Im Falle einer Malware-Erkennung durch die Cloud-Services für IBM Trusteer Pinpoint Malware Detection oder die Cloud-Services für IBM Trusteer Pinpoint Malware Detection II bzw. der Erkennung einer Kontoübernahme durch die Cloud-Services für IBM Trusteer Pinpoint Criminal Detection oder die Cloud-Services für IBM Trusteer Pinpoint Criminal Detection II, muss der Kunde die Anweisungen im Pinpoint Best Practices Guide befolgen. Der Kunde darf die Cloud-Services für IBM Trusteer Pinpoint Malware Detection oder IBM Trusteer Pinpoint Malware Detection II bzw. die Cloud-Services für IBM Trusteer Pinpoint Criminal Detection oder IBM Trusteer Pinpoint Criminal Detection II 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 Cloud-Services für IBM Trusteer Pinpoint 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).

3.2 IBM Trusteer Pinpoint Criminal Detection for Business und/oder IBM Trusteer Pinpoint Criminal Detection for Retail

Clientlose Erkennung verdächtiger Kontoübernahmeaktivitäten von Browsern, die unter Verwendung einer Geräte-ID eine Verbindung zu einer Business- oder Retail-Anwendung herstellen, Phishing-Erkennung und Erkennung des Diebstahls von Zugangsdaten durch Malware. Die Cloud-Services für IBM Trusteer Pinpoint Criminal Detection 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 über die mobile Anwendung des Kunden), die auf eine Business- oder Retail-Anwendung zugreifen, direkt an den Kunden.

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 generiert werden, für die der Kunde eine

Abdeckung über eine Subscription für Cloud-Services erworben hat. Die Ereignisdaten können auch von einer Back-End-API an den Kunden übermittelt werden.

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business und/oder IBM Trusteer Pinpoint Criminal Detection II for Retail

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

Clientlose Erkennung verdächtiger Kontoübernahmeaktivitäten von Browsern, die unter Verwendung einer Geräte-ID eine Verbindung zu einer Business- oder Retail-Anwendung herstellen, Phishing-Erkennung und Erkennung des Diebstahls von Zugangsdaten durch Malware. Die Cloud-Services für IBM Trusteer Pinpoint Criminal Detection 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 über die mobile Anwendung des Kunden), die auf eine Business- oder Retail-Anwendung zugreifen, direkt an den Kunden.

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 generiert werden, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat. Die Ereignisdaten können auch von einer Back-End-API an den Kunden übermittelt werden.

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

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

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 Cloud-Services für IBM Trusteer Pinpoint Malware Detection 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 Edition for Business oder die Standard Edition for Retail ist eine Lösung, die in kurzer Zeit einsatzbereit ist und die hierin beschriebene Kernfunktionalität dieser Cloud-Services bereitstellt.

3.5 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 Cloud-Services für IBM Trusteer Pinpoint Malware Detection 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 Edition for Business oder die Standard Edition for Retail ist eine Lösung, die in kurzer Zeit einsatzbereit ist und die hierin beschriebene Kernfunktionalität dieser Cloud-Services bereitstellt.

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.

3.6 Optionale zusätzliche Cloud-Services für IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition und/oder IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition und/oder IBM Trusteer Pinpoint Malware Detection for Business Standard Edition und/oder IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition und/oder IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail und/oder IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business und/oder IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 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 for Retail oder IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail bzw. 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 for Business oder IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business bzw. IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business oder IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business erworben werden.

- Als Voraussetzung für IBM Trusteer Pinpoint Carbon Copy for Retail muss IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail oder IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail bzw. 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 IBM Trusteer Pinpoint Carbon Copy for Business muss IBM Trusteer Pinpoint Malware Detection Standard Edition for Business oder IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business bzw. IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business oder IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business erworben werden.

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business und/oder IBM Trusteer Pinpoint Carbon Copy for Retail

Die IBM Trusteer Pinpoint Carbon Copy-Angebote bieten eine zusätzliche Schutzstufe und einen Überwachungsservice, der dabei hilft, Anmeldeinformationen berechtigter Teilnehmer zu identifizieren, die durch Phishing-Attacken auf die Retail- oder Business-Anwendungen beschädigt wurden, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Service-Angebote erworben hat.

3.6.2 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 oder 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 den 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.

3.6.3 IBM Trusteer Pinpoint Malware Detection Redeployment

Kunden, die ihre Online-Banking-Anwendungen während der Servicelaufzeit erneut bereitstellen und folglich Änderungen an ihrer Bereitstellung von IBM Trusteer Pinpoint Malware Detection und/oder 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.

3.6.4 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 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. 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.

3.7 Optionale zusätzliche Cloud-Services für IBM Trusteer Pinpoint Criminal Detection for Business und/oder IBM Trusteer Pinpoint Criminal Detection for Retail und/oder für IBM Trusteer Pinpoint Criminal Detection II for Business und/oder IBM Trusteer Pinpoint Criminal Detection II for Retail

3.7.1 IBM Trusteer Pinpoint Criminal Detection Redeployment

Kunden, die ihre Online-Banking-Anwendungen während der Servicelaufzeit erneut bereitstellen und folglich Änderungen an ihrer Bereitstellung des Cloud-Service für IBM Trusteer Pinpoint Criminal Detection benötigen, müssen IBM Trusteer Pinpoint Criminal 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.

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business und/oder IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Soll IBM Trusteer Pinpoint Criminal Detection 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 Criminal Detection Additional Applications for Business erworben werden. Soll IBM Trusteer Pinpoint Criminal Detection 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 Criminal Detection Additional Applications for Retail erworben werden.

4. IBM Trusteer Fraud Protection Suite

Die IBM Trusteer Fraud Protection Suite („Suite“) besteht aus einer Gruppe cloudbasierter Services, die eine Schutzstufe gegen 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 gehosteten IBM Trusteer-Umgebung zur Verfügung gestellt und bietet dem Kunden (und einer unbegrenzten Zahl seiner autorisierten Mitarbeiter) folgende Funktionen: (i) Erhalt von Ereignisdatenberichten und Risikobewertungen sowie (ii) Anzeigen, Konfigurieren und Definieren von Sicherheitsrichtlinien und Richtlinien zur 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 den Business- und/oder Retail-Anwendungen 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 Cloud-Services für IBM Trusteer Pinpoint Detect 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).

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

In diesem Cloud-Service sind die Cloud-Services IBM Trusteer Pinpoint Criminal Detection und IBM Trusteer Pinpoint Malware Detection zusammengefasst, um eine 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 Business- oder Retail-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 über die mobile Anwendung des Kunden), die auf eine Business- oder Retail-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 Detect Premium 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.

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

Dieser Cloud-Service kombiniert IBM Trusteer Pinpoint Criminal Detection und IBM Trusteer Pinpoint Malware Detection, um eine einzige, einfach zu integrierende, einheitliche Lösung mit erweiterter Funktionalität und erweiterten Services anzubieten, einschließlich erweiterter Bereitstellungs- und Einrichtungsservices, angepasster Sicherheitsrichtlinien, Untersuchungsservices usw.

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.

4.3 IBM Trusteer Pinpoint Detect Standard with access management integration for Business und/oder IBM Trusteer Pinpoint Detect Standard with access management integration for Retail

Der Cloud-Service IBM Trusteer Pinpoint Detect Standard with access management integration beinhaltet die Funktionalität von IBM Security Pinpoint Detect Standard, die in Abschnitt 4.1 oben ausführlich erläutert wird.

IBM Trusteer Pinpoint Detect Standard with access management integration kommt beim Erwerb in Verbindung mit Zugriffsmanagementsystemen, wie beispielsweise IBM Security Access Management („ISAM“), zum Einsatz. Beim Erwerb mit ISAM müssen beide Angebote aktiviert werden. Dieses Angebot beinhaltet die Option für die Integration mit dem Zugriffsmanagementsystem. Die Berechtigung für das Zugriffsmanagementsystem ist nicht enthalten.

Bei diesem Angebot 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.

Standard Support (gemäß der Definition im Abschnitt „Technische Unterstützung“) ist bei diesem Cloud-Service mit eingeschlossen. IBM Trusteer Pinpoint Detect Premium with access management integration

for Business und/oder IBM Trusteer Pinpoint Detect Premium with access management integration for Retail

Der Cloud-Service IBM Trusteer Pinpoint Detect Premium with access management integration beinhaltet die Funktionalität von IBM Security Pinpoint Detect Premium, die in Abschnitt 4.2 oben ausführlich erläutert wird, sowie die Option für die Integration mit dem Zugriffsmanagementsystem.

IBM Trusteer Pinpoint Detect Premium with access management integration kommt beim Erwerb in Verbindung mit Zugriffsmanagementsystemen, wie beispielsweise IBM Security Access Management („ISAM“), zum Einsatz. Beim Erwerb mit ISAM müssen beide Angebote aktiviert werden. Dieser Cloud-Service beinhaltet die Option für die Integration mit dem Zugriffsmanagementsystem. Die Berechtigung für das Zugriffsmanagementsystem ist nicht enthalten.

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 Angebot eingeschlossen.

4.4 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 for Retail oder IBM Trusteer Pinpoint Detect Standard for Retail.

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

IBM Trusteer Rapport for Mitigation ist dazu ausgelegt, Malware-Infizierungen auf betroffenen Geräten (PC/MACs) der berechtigten Teilnehmer 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 den 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.

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

Soll IBM Trusteer Pinpoint 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 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 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.

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.

4.5.2 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.

5. IBM Trusteer Mobile-Cloud-Services

5.1 IBM Trusteer Mobile Browser for Business und/oder IBM Trusteer Mobile Browser for Retail

IBM Trusteer Mobile Browser bietet eine zusätzliche Schutzstufe und sicheren Onlinezugriff über die mobilen Geräte der berechtigten Teilnehmer auf die Business- oder Retail-Anwendungen, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat, sowie Risikobewertungen von mobilen Geräten und Phishing-Schutz. Die Erkennung sicherer WiFi-Umgebungen ist nur für Android-Plattformen verfügbar. Dieser Cloud-Service schließt mobile Geräte, Mobiltelefone und Tablets ein, aber keine Laptops oder Mac-Computer.

Über die TMA kann der Kunde Ereignisdaten sowie Analyse- und Statistikdaten empfangen, die sich auf Geräte beziehen, deren berechtigte Teilnehmer (i) die Client-Software für Kontoinhaber heruntergeladen haben (eine kostenlose Anwendung, die unter einer Endbenutzerlizenzvereinbarung (EULA) frei lizenziert und zum Download auf die mobilen Geräte der berechtigten Teilnehmer zur Verfügung gestellt wird) sowie (ii) die EULA akzeptiert und sich mindestens einmal bei Business- oder Retail-Anwendungen authentifiziert haben, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat. Der Kunde darf die Client-Software für Kontoinhaber nur über den Trusteer Splash weitergeben. Die Nutzung dieser Software für unternehmensinterne Zwecke des Kunden ist nicht zulässig.

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 mobilen Geräte mit den Business- oder Retail-Anwendungen generiert werden, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat.

b. Trusteer Splash:

   Über die Trusteer Splash-Marketing-Plattform wird den berechtigten Teilnehmern beim Zugriff auf die Business- und/oder Retail-Anwendungen, 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. Unter einem separaten Vertrag oder einer separaten Leistungsbeschreibung kann eine Splash-Anpassung vereinbart werden.

Der Kunde kann Marken, Logos oder Symbole zur Verwendung in Verbindung mit der TMA zur Verfügung stellen, die im Trusteer Splash und in der Client-Software für Kontoinhaber oder auf den von IBM gehosteten Landing-Pages oder auf der IBM Trusteer-Website angezeigt werden können. Der Umgang mit den vom Kunden bereitgestellten Marken, Logos und Symbolen erfolgt gemäß den IBM Richtlinien für Werbung und die Nutzung von Marken.

5.2 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 hat Beispielanwendungen getestet, die mit den zum Lieferumfang des IBM Trusteer Mobile SDK gehörenden Tools für mobile Geräte („Mobile Tools“) erstellt wurden, um festzustellen, ob diese auf bestimmten Versionen von Betriebssystemplattformen für mobile Geräte von Apple (iOS), Google (Android) und anderen (gemeinsam „OS-Plattformen für mobile Geräte“ genannt) ordnungsgemäß ausgeführt werden. Die OS-Plattformen für mobile Geräte werden jedoch von Drittherstellern angeboten, befinden sich nicht unter der Kontrolle von IBM und können ohne Mitteilung an IBM geändert werden. Aus diesem Grund und ungeachtet gegenteiliger Aussagen gewährleistet IBM nicht, dass mit den Mobile Tools erstellte Anwendungen oder sonstige damit erstellte Ausgaben auf OS-Plattformen für mobile Geräte oder auf mobilen Endgeräten ordnungsgemäß ausgeführt werden, mit diesen zusammenarbeiten oder mit diesen kompatibel sind.

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) und ohne jegliche ausdrückliche oder stillschweigende Gewährleistung zur Verfügung, insbesondere ohne Gewährleistung für Rechtsmängel, für die Freiheit von Rechten Dritter, für das Recht auf Nichtbeeinträchtigung, für die Handelsüblichkeit und für die Verwendungsfähigkeit für einen bestimmten Zweck. 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.

Der Kunde verpflichtet sich, korrekte schriftliche Aufzeichnungen, Ausgaben von Systemtools und sonstige Systemdaten zu erstellen, aufzubewahren und IBM sowie ihren Prüfern bereitzustellen, um prüffähige Nachweise dafür zu erbringen, dass die Nutzung des IBM Trusteer Mobile SDK durch den Kunden in Übereinstimmung mit den Bestimmungen dieser Servicebeschreibung erfolgt.

6. Premium Support

Premium Support darf nur für die Cloud-Services in Anspruch genommen werden, für die der Kunde eine Subscription für das zugehörige Premium-Support-Angebot erworben hat.

7. 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.

8. Datenschutz und Sicherheit

Dieser Cloud-Service orientiert sich an den unter http://www.ibm.com/cloud/data-security verfügbaren IBM Datensicherheits- und Datenschutzrichtlinien für IBM SaaS sowie etwaigen weiteren Bedingungen in diesem Abschnitt. Änderungen der IBM Datensicherheits- und Datenschutzrichtlinien führen nicht zu einer Beeinträchtigung der Sicherheit des Cloud-Service.

Dieser Cloud-Service kann zur Verarbeitung von Inhalten verwendet werden, die personenbezogene Daten enthalten, wenn der Kunde als der für die Verarbeitung Verantwortliche sich davon überzeugt hat, dass die technischen und organisatorischen Sicherheitsmaßnahmen den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen sind. Der Kunde ist sich dessen bewusst, dass dieser Cloud-Service keine Funktionen zum Schutz von sensiblen personenbezogenen Daten oder von Daten bietet, die zusätzlichen regulatorischen Anforderungen unterliegen.

Dieser Cloud-Service fällt unter die Privacy-Shield-Zertifizierung von IBM, die zur Anwendung kommt, wenn der Kunde sich für das Hosten des Cloud-Service in einem Rechenzentrum in den USA entscheidet, und unterliegt der Privacy-Shield-Datenschutzrichtlinie von IBM, die unter http://www.ibm.com/privacy/details/us/en/privacy_shield.html eingesehen werden kann.

8.1 Sicherheitsfunktionen und Verantwortlichkeiten

Mit dem Cloud-Service werden die folgenden Sicherheitsfunktionen implementiert:

Im Rahmen des Cloud-Service werden Inhalte sowohl bei der Datenübertragung in das und aus dem IBM Netz als auch im Wartezustand zur Übertragung vom Endpunkt verschlüsselt.

8.2 Rechtmäßige Nutzung und Zustimmung

Rechtmäßige Nutzung

Bei der Nutzung dieses Cloud-Service können mehrere Gesetze oder Bestimmungen zur Anwendung kommen. Der Cloud-Service darf nur für gesetzlich zulässige Zwecke und in rechtmäßiger Weise verwendet werden. Der Kunde willigt ein, den Cloud-Service gemäß den anwendbaren Gesetzen, Bestimmungen und Richtlinien zu verwenden und die gesamte Verantwortung für deren Einhaltung zu übernehmen.

Ermächtigung zur Erfassung und Verarbeitung von Daten

Der Cloud-Service erfasst Informationen über berechtigte Teilnehmer und Clienteinheiten, die mit den Business- oder Retail-Anwendungen interagieren, für die der Kunde eine Abdeckung über eine Subscription für einen Cloud-Service erworben hat. Die vom Cloud-Service erfassten Informationen können allein oder in Kombination in einigen Rechtsordnungen als personenbezogene Daten gelten. Personenbezogene Daten sind sämtliche Informationen, die zur Identifizierung einer bestimmten Person dienen (beispielsweise Name, E-Mail-Adresse, Privatadresse oder Telefonnummer), die IBM zur Speicherung, Verarbeitung oder Übertragung im Auftrag des Kunden zur Verfügung gestellt werden.

Die Datenerfassungs- und Datenverarbeitungsverfahren können aktualisiert werden, um die Funktionalität des Cloud-Service zu verbessern. Das Dokument mit einer vollständigen Beschreibung der Datenerfassungs- und Datenverarbeitungsverfahren wird bei Bedarf aktualisiert und dem Kunden auf

Anfrage zur Verfügung gestellt. Der Kunde ermächtigt IBM zur Erfassung dieser Informationen und zu deren Verarbeitung gemäß den Bestimmungen der Abschnitte „Grenzüberschreitende Datenübermittlung“ und „Datenschutz“ in dieser Servicebeschreibung.

Für IBM Trusteer-Angebote, die die Trusteer Management Application (TMA) enthalten:

Die folgenden Daten werden für TMA-Administratoren des Sponsorunternehmens in der Trusteer Management Application (TMA) erfasst und gespeichert: E-Mail-Adresse (als Login), gehashtes Kennwort, Vorname, Nachname, Position und Abteilung.

Für IBM Trusteer Pinpoint-Cloud-Services:

Zu den erfassten Daten können gehören:

- Benutzer- oder Endpunkt-ID, wie beispielsweise die verschlüsselte oder mittels Einweg-Hashfunktion erzeugte Benutzer-ID, die persistente Benutzer-ID (PUID), der Rapport Agent Key und die Kundensitzungs-ID
- Daten, die sich auf die geschützte Anwendung beziehen, wie beispielsweise bestimmte Attribute/Elemente aus der Online-Banking-Anwendung des Kunden, die im Browser des Endbenutzers wiedergegeben werden, Websitebesuche und Browserverlauf
- Informationen zur installierten Softwareumgebung, Browser-/Geräteattribute und -einstellungen sowie Umfang des Browserverlaufs
- Hardwareinformationen und Zeitmarke
- Browser-Header und Kommunikationsprotokolldaten, wie beispielsweise IP-Adresse des Benutzers, Cookies, Header der Verweisseite (Referrer Header) und andere HTTP-Header
- Mausbewegungsdaten des Endbenutzers, wie beispielsweise die Koordinaten des Mauszeigers, Klicks, Bewegungen des Mausrads (sowie ähnliche Daten) und die Zeitmarke der Interaktion mit der Online-Banking-Anwendung des Kunden
- Phishing-Sites und an Phishing-Sites übergebene Informationen
- Auf Wunsch des Kunden, Transaktionsdaten (Transaktionsbetrag, Transaktionswährung und Zielcodes, mittels Einweg-Hashfunktion erzeugte Zielbank-ID der Transaktion, mittels Einweg-Hashfunktion erzeugte Zielkonto-ID der Transaktion, Binärwert, wenn es sich um eine Transaktion mit einem neuen Zahlungsempfänger handelt, sowie Transaktionsdatum/-zeit) und optional eine Bewertung der Risikodaten
- Auf Wunsch des Kunden, Eingaberhythmen an der Tastatur und Abfolge der Tastenanschläge, die vom Endbenutzer bei der Eingabe von Benutzernamen, Kennwörtern und anderen Texten verwendet werden (aber keine Buchstaben, Zahlen oder Sonderzeichen und ohne die Möglichkeit, Benutzernamen oder Kennwörter zu erkennen)

Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass IBM keine Geschäftsdaten und/oder -unterlagen des Kunden erfasst, speichert, verwaltet oder pflegt.

Wenn der Kunde eine Subscription für das IBM Trusteer Rapport for Remediation-Angebot erwirbt oder bei einigen Pinpoint-Unterstützungsfällen kann es vorkommen, dass IBM die Installation der Client-Software für Kontoinhaber von Rapport auf der Maschine eines berechtigten Teilnehmers empfiehlt, um vermutete Malware-Infizierungen zu untersuchen und zu überprüfen. Die Daten, die für Rapport-Angebote erfasst werden, sind nachstehend aufgeführt.

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

Zu den erfassten Daten können gehören:

- URLs und Internet-Protocol-Adressen (IP-Adressen) der von einem Kontoinhaber besuchten Websites, die IBM als potenzielle Phishing-Websites oder Websites mit betrügerischen oder ausbeuterischen Absichten erachtet, sowie Informationen über die Beschaffenheit der identifizierten Bedrohungen
- URLs und IP-Adressen der von einem Kontoinhaber besuchten Websites, die vom Kunden kontrolliert und durch den Cloud-Service geschützt werden, wie beispielsweise Online-Banking-Sites; IP-Adressen des Kontoinhabers

- Informationen über die Hardwarekennzeichnung, Betriebssysteme, Anwendungssoftware, Peripheriegeräte, Sicherheitskonfiguration, Systemeinstellungen und Netzverbindungen des Endpunkts sowie die ID, der Name, die Verwendungsmuster und sonstige Informationen zur Identifizierung des Endpunkts
- Informationen über die Installation und den Betrieb des Programms, die Programm-ID, die Programmversion, vom Endpunkt generierte sicherheitsrelevante Ereignisse und Informationen über Programmfehler
- Nutzungsstatistiken und statistische Informationen über die vom Programm erkannten Bedrohungen; Protokolldateien, in denen Browser-Abstürze, Datum und Zeit der Infizierung sowie Informationen über die Beschaffenheit der identifizierten Bedrohungen oder Störungen verzeichnet sind
- Kundenbeziehung, wird auch als Sponsorunternehmen bezeichnet. Eine Beziehung wird aufgebaut, wenn ein Endbenutzer Rapport von der Website des Kunden herunterlädt, einen bestimmten Kunden beim Herunterladen von Rapport auf der Trusteer-Support-Site auswählt oder sich bei der Banking-Anwendung des Kunden anmeldet. Ein Endbenutzer kann über mehrere Kundenbeziehungen verfügen
- Eine Kopie der verschlüsselten Benutzer-ID, die vom Kontoinhaber für die Interaktion mit dem Kunden verwendet wird (optional)
- Eine verschlüsselte Kopie der Kreditkartennummer, die vom Kontoinhaber auf einer Site eingegeben wird, nachdem das Programm ihn darüber informiert hat, dass es die Site als gefährlich einstuft
- Dateien und weitere Informationen des Endpunkts, von denen IBM Sicherheitsexperten annehmen, dass sie mit Malware oder anderen bösartigen Aktivitäten bzw. mit allgemeinen Fehlfunktionen des Programms in Zusammenhang stehen könnten
- Persönliche Kontaktinformationen, einschließlich Name und E-Mail-Adresse, wenn der Endbenutzer Unterstützung anfordert

Für IBM Trusteer Mobile SDK-Angebote und IBM Trusteer Mobile Browser-Cloud-Services:

Zu den erfassten Daten können gehören:

- Benutzer-IDs, wie beispielsweise verschlüsselte oder mittels Einweg-Hashfunktion verschlüsselte Benutzer-IDs
- Gerätedaten, wie beispielsweise IP-Adresse, gehashte Geräte-ID, Zeitmarke, MD5-Werte des installierten Pakets sowie Informationen über Gerätehardware und Software
- Version und Installationsdatum des Mobile SDK oder Mobile Browser
- Zugriffe auf geschützte Anwendungen
- Informationen zur Kundenbeziehung
- Risikodaten des Geräts (z. B. Vorhandensein von Malware, Root Hiders, WiFi-Verschlüsselungsstatus, ob ein Gerät per Jailbreak manipuliert wurde)
- Stack-Trace bei Absturz (im Falle einer unerwarteten Beendigung einer Anwendung)
- Produktionsdaten des Telefons (z. B. Modell, Hersteller)
- Touchscreen-Interaktionen der Endbenutzer, einschließlich x-y-Koordinaten, Touchbereich und Aktionsart (nach oben oder unten und bewegen)
- Bewegungssensordaten, Strom-/Ressourcenverbrauch, Verbindungseinstellungen, Umgebungssensoren, wie Temperatur, Helligkeit und Luftdruck, sowie allgemeine Geräteeinstellungen (Lautstärke, Rufton, Bildschirmhelligkeit usw.)

8.3 Einverständniserklärung der betroffenen Personen

Für IBM Trusteer Pinpoint-Cloud-Services und IBM Trusteer Mobile SDK-Cloud-Services:

Der Kunde versichert, dass er alle Einverständniserklärungen, Genehmigungen oder Lizenzen eingeholt hat oder einholen wird, die für die rechtmäßige Nutzung des Cloud-Service sowie die Erfassung und Verarbeitung der Informationen durch IBM über den Cloud-Service erforderlich sind.

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

Der Kunde ermächtigt IBM, die Einverständniserklärungen einzuholen, die für die rechtmäßige Nutzung des Cloud-Service sowie die Erfassung und Verarbeitung der Informationen gemäß der Beschreibung in der Endbenutzerlizenzvereinbarung erforderlich sind, die unter https://www.trusteer.com/support/end-user-license-agreement verfügbar ist. Falls der Kunde den Schriftverkehr mit den Endbenutzern zur Einholung der Zustimmungen selbst erledigt (und nicht IBM überlässt), versichert er, dass er alle Einverständniserklärungen, Genehmigungen oder Lizenzen eingeholt hat oder einholen wird, die für die rechtmäßige Nutzung des Cloud-Service sowie die Erfassung und Verarbeitung der Informationen durch IBM als Auftragsverarbeiter des Kunden über den Cloud-Service erforderlich sind.

8.4 Nutzung von Sicherheitsdaten

Im Rahmen des Cloud-Service, der eine Berichterstattung beinhaltet, wird IBM anonymisierte und/oder aggregierte Informationen, die aus dem Cloud-Service erfasst wurden, aufbereiten und verwalten („Sicherheitsdaten“). Die Sicherheitsdaten lassen keine Rückschlüsse auf den Kunden, seine berechtigten Teilnehmer oder eine Person zu, außer wie unten in Absatz (d) vorgesehen. Der Kunde erklärt sich damit einverstanden, dass IBM die Sicherheitsdaten nur für folgende Zwecke zeitlich unbegrenzt verwenden und/oder kopieren darf:

a. Veröffentlichung und/oder Weitergabe der Sicherheitsdaten (z. B. in Datensammlungen und/oder Analysen im Zusammenhang mit Cybersicherheit)

b. Entwicklung oder Verbesserung von Produkten oder Services

c. Durchführung interner Recherchen oder mit Dritten

d. Rechtmäßige Weitergabe von bestätigten Informationen über externe Täter

8.5 Grenzüberschreitende Datenübermittlung

Der Kunde willigt ein, dass IBM die Inhalte, einschließlich der personenbezogenen Daten, die oben im Abschnitt „Rechtmäßige Nutzung und Zustimmung“ aufgeführt sind, unter Einhaltung der einschlägigen Gesetze und Anforderungen grenzüberschreitend durch Auftragsverarbeiter und Unterauftragsverarbeiter in den folgenden Ländern außerhalb des Europäischen Wirtschaftsraums (EWR) und in Ländern, die von der Europäischen Kommission als Länder mit einem angemessenen Schutzniveau eingestuft werden, verarbeiten lassen kann: in den USA.

8.6 Datenschutz

Wenn der Kunde personenbezogene Daten in den EU-Mitgliedstaaten sowie in Island, Liechtenstein, Norwegen oder in der Schweiz im Cloud-Service verfügbar macht oder wenn sich berechtigte Teilnehmer oder Clienteinheiten des Kunden in diesen Ländern befinden, beauftragt der Kunde als alleiniger Verantwortlicher IBM als Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten (gemäß der Definition dieser Begriffe in der EU-Richtlinie 95/46/EG). IBM wird personenbezogene Daten nur in dem Umfang verarbeiten, der zur Bereitstellung des Cloud-Service-Angebots gemäß den von IBM veröffentlichten Beschreibungen der Cloud-Services erforderlich ist, und der Kunde stimmt zu, dass eine solche Verarbeitung seinen Anweisungen entspricht. IBM wird wesentliche Änderungen in Bezug auf den Verarbeitungsstandort oder den Schutz personenbezogener Daten im Rahmen des Cloud-Service durch rechtzeitige Benachrichtigung über das Kundenportal bekannt geben. Der Kunde kann die derzeitige Subscription-Laufzeit für den betroffenen Cloud-Service durch schriftliche Mitteilung an IBM innerhalb von dreißig (30) Tagen nach Erhalt der Benachrichtigung über die Änderung kündigen.

Die Vertragsparteien oder ihre verbundenen Unternehmen können in ihren jeweiligen Rollen separate Vereinbarungen basierend auf den unveränderten EU-Standardvertragsklauseln gemäß dem EU-Beschluss 2010/87/EU unter Ausschluss der optionalen Klauseln abschließen. Alle Rechtsstreitigkeiten oder Verbindlichkeiten, die aus diesen Vereinbarungen entstehen, selbst wenn die Vereinbarungen zwischen verbundenen Unternehmen geschlossen wurden, werden von den Vertragsparteien so behandelt, als seien sie unter den Bedingungen der vorliegenden Vereinbarung entstanden.

a. Bei Services, die gemäß der Festlegung während des Einrichtungsprozesses über das Rechenzentrum in Deutschland bereitgestellt werden, erklärt der Kunde sich damit einverstanden, dass IBM Inhalte, einschließlich personenbezogener Daten, grenzüberschreitend von den folgenden Auftragsverarbeitern und Unterauftragsverarbeitern verarbeiten lassen kann:

Name des Auftragsverarbeiters/Unterauftragsverarbeiters	Rolle (Auftragsverarbeiter oder Unterauftragsverarbeiter)	Standort
IBM Vertragspartei	Auftragsverarbeiter	Laut Auftragsdokument
Amazon Web Services (Deutschland)	Unterauftragsverarbeiter	Deutschland
IBM Ireland Ltd.	Auftragsverarbeiter	Irland
IBM Israel Ltd.	Auftragsverarbeiter	Israel

Bei Services, die über das Rechenzentrum in Deutschland bereitgestellt werden, können für die Erbringung von Kundenunterstützungsleistungen Trusteer Mitarbeiter in anderen EU-Ländern eingesetzt werden.

b. Bei Services, die gemäß der Festlegung während des Einrichtungsprozesses über das Rechenzentrum in Japan bereitgestellt werden, erklärt der Kunde sich damit einverstanden, dass IBM Inhalte, einschließlich personenbezogener Daten, grenzüberschreitend von den folgenden Auftragsverarbeitern und Unterauftragsverarbeitern verarbeiten lassen kann:

Name des Auftragsverarbeiters/Unterauftragsverarbeiters	Rolle (Auftragsverarbeiter oder Unterauftragsverarbeiter)	Standort
IBM Vertragspartei	Auftragsverarbeiter	Japan, laut Auftragsdokument
Amazon Web Services (Japan)	Unterauftragsverarbeiter	Japan
IBM Ireland Ltd.	Auftragsverarbeiter	Irland
IBM Israel Ltd.	Auftragsverarbeiter	Israel

c. Bei Services, die über das Rechenzentrum in den USA bereitgestellt werden, erklärt der Kunde sich damit einverstanden, dass IBM Inhalte, einschließlich personenbezogener Daten, grenzüberschreitend von den folgenden Auftragsverarbeitern und Unterauftragsverarbeitern verarbeiten lassen kann:

Name des Auftragsverarbeiters/Unterauftragsverarbeiters	Rolle (Auftragsverarbeiter oder Unterauftragsverarbeiter)	Standort
IBM Vertragspartei	Auftragsverarbeiter	Laut Auftragsdokument
Amazon Web Services LLC	Unterauftragsverarbeiter	USA
IBM Ireland Ltd.	Auftragsverarbeiter	Irland
IBM Israel Ltd.	Auftragsverarbeiter	Israel
IBM Corporation	Auftragsverarbeiter	USA

d. Bei Services, die über die oben in Abschnitt 8.5.c („Rechenzentrum in den USA“) aufgelisteten Rechenzentren bereitgestellt werden, kann IBM ferner gemäß der Festlegung während des Einrichtungsprozesses auf einen oder mehrere der folgenden Unterauftragsverarbeiter zurückgreifen:

Name des Auftragsverarbeiters/Unterauftragsverarbeiters	Rolle (Auftragsverarbeiter oder Unterauftragsverarbeiter)	Standort
Amazon Web Services (Australien)	Unterauftragsverarbeiter	Australien
Amazon Web Services (Singapur)	Unterauftragsverarbeiter	Singapur
Amazon Web Services (Irland)	Unterauftragsverarbeiter	Irland

e. Der Kunde erklärt sich damit einverstanden, dass IBM nach Bekanntmachung über das Kundenportal die Verarbeitung von Amazon Web Services in IBM Rechenzentren verlagern kann. Ferner kann IBM nach Bekanntmachung über das Kundenportal die obigen Listen der Unterauftragsverarbeiter ändern.

f. 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.

g. Daten im Zusammenhang mit der Kundenunterstützung werden auf einem Cloud-Server von Salesforce.com gespeichert, der sich in Irland befindet.

h. 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 bereitzustellen.

9. Service-Level-Agreement

Das folgende Verfügbarkeits-Service-Level-Agreement („SLA“) wird von IBM, so wie im Berechtigungsnachweis angegeben, für den Cloud-Service bereitgestellt. Das SLA stellt keine Gewährleistung dar. Es wird nur Kunden zur Verfügung gestellt und gilt ausschließlich für Produktionsumgebungen.

9.1 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 (3) 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 den 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.

9.2 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)**
< 99,5 %	2 %
< 98,0 %	5 %
< 96,0 %	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 die entsprechenden Servicegutschriften 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

10. 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 Premium-Support-Subscription gegen Zahlung einer zusätzlichen Gebühr erhältlich, mit Ausnahme der Cloud-Services für das IBM Trusteer Mobile SDK und der Cloud-Services für den IBM Trusteer Rapport Mandatory Service. Weitere Einzelheiten sind über den IBM Vertriebsbeauftragten oder den IBM Business Partner erhältlich.

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 [SaaS] Support Handbook ausführlich beschrieben
- Über das Kundenunterstützungsportal unter http://www-01.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 IBM Software as a Service [SaaS] Support Handbook unter http://www-01.ibm.com/software/support/handbook.html zu finden

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-01.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 IBM Software as a Service [SaaS] Support Handbook unter http://www-01.ibm.com/software/support/handbook.html zu finden

11. Informationen zur Berechtigung und Abrechnung

11.1 Gebührenmetriken

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

a. **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.

b. **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.

c. **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 des Cloud-Service ist eine Anwendung eine einzelne Business- oder Retail-Anwendung des Kunden.

d. **Kundenprojekt** (Engagement) ist eine Maßeinheit für den Erwerb der Services. Ein Kundenprojekt besteht aus Professional Services und/oder Schulungsservices im Zusammenhang mit den Cloud-Services. Der Kunde muss ausreichende Berechtigungen zur Abdeckung aller Kundenprojekte erwerben.

11.2 Anteilige Monatsgebühren

Die im Auftragsdokument angegebene anteilige Monatsgebühr wird anteilig basierend auf der Nutzung ermittelt.

12. Compliance und Prüfung

Der Zugriff auf die IBM Trusteer Fraud Protection-Cloud-Services ist auf die maximale Anzahl der Anwendungen, berechtigten Teilnehmer und/oder Clienteinheiten begrenzt, die im Auftragsdokument angegeben ist. Der Kunde ist dafür verantwortlich, sicherzustellen, dass die im Auftragsdokument angegebene maximale Anzahl nicht überschritten wird.

Im Rahmen eines Audits kann von IBM geprüft werden, ob die maximale Anzahl der Anwendungen, berechtigten Teilnehmer und/oder Clienteinheiten eingehalten wird.

13. 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.

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.

14. Aktivierungssoftware

Dieser Cloud-Service enthält Aktivierungssoftware, die nur in Verbindung mit dem Cloud-Service während seiner Laufzeit verwendet werden darf.

15. Erhöhung der jährlichen Subscription-Gebühr für IBM Trusteer

IBM behält sich das Recht vor, die Subscription-Gebühr für die Cloud-Services anzupassen. Die Anpassung der Subscription-Gebühr wirkt sich auf die Preise aus, die im jeweiligen Angebot und für die Laufzeit des Angebots angegeben sind. Weitere Anpassungen der Subscription-Gebühr, die höchstens ein Mal innerhalb von zwölf (12) Monaten um einen von IBM festzulegenden Prozentsatz, maximal jedoch um 3 %, vorgenommen werden, können dann erfolgen, wenn die Laufzeit der Cloud-Services automatisch oder durchfortlaufende Nutzung verlängert wird. Die Gebührenanpassungen haben keine Auswirkung auf die Berechtigung des Kunden für die Cloud-Services oder die Gebührenmetrik, mit der die Cloud-Services erworben wurden. IBM Business Partner sind von IBM unabhängig und entscheiden allein über ihre Preise und Bedingungen.