IBM Trusteer Pinpoint Detect

Diese Servicebeschreibung beschreibt den Cloud-Service. Die anwendbaren Auftragsdokumente enthalten Preisangaben und weitere Einzelheiten zur Bestellung des Kunden.

1. Cloud-Service

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 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 von den Pinpoint-Angeboten generierten Bedrohungsdaten (Threat Feeds) anzeigen, subskribieren und deren Zustellung konfigurieren kann. IBM Trusteer Pinpoint Detect und IBM Trusteer Pinpoint Verify werden als Teil der TMA-Anmeldung verwendet.

b. Web-Script und/oder APIs:

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

Eine Pinpoint-Sitzung wird zwischen Start und Ende einer Benutzerinteraktion gemessen. Der Sitzungsstart wird nach der Übergabe der Berechtigungsnachweise oder einer alternativen Überprüfung der Berechtigungsnachweise auf der Anmeldeseite des Kunden erfasst. Das Sitzungsende wird erfasst, wenn eines der folgenden Ereignisse eintritt:

- Die Sitzung wird durch normales Abmelden von der Anwendung zurückgesetzt
- Browser oder Registerkarte wird geschlossen
- Cookies werden gelöscht
- Zeitlimitüberschreitung

1.1 Angebote

Folgende Angebote stehen für den Kunden zur Wahl.

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

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

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

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

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

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

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

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

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

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

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

Premium Support ist bei diesem Cloud-Service eingeschlossen.

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

Pinpoint Detect Policy Manager:

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

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

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

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

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

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

1.1.3 IBM Trusteer Pinpoint Detect for Connections

Dieser Cloud-Service bietet Schutz, ist für das Erkennen von Kontoübernahmeversuchen ausgelegt und übermittelt Risiko-/Zuverlässigkeitsbewertungen von Browsern und/oder mobilen Geräten (über den nativen Browser oder die mobile Anwendung des Kunden), die auf eine Business- oder Retail-Anwendung zugreifen. Die Lösung verwendet verschiedene Risikoindikatoren, die das Gerät, die Verbindung und das Verhalten des Endbenutzers analysieren, und vergleicht sie mit der Benutzerhistorie, um verdächtige Nutzungen festzustellen.

Der Cloud-Service kann sowohl Verbindungen über mobile als auch über Webkanäle verarbeiten. IBM Trusteer Pinpoint Detect beinhaltet eine Berechtigung für das IBM Trusteer Mobile SDK, sofern erforderlich.

Der Cloud-Service kann in Paketen mit jeweils 100 Verbindungen pro Jahr erworben werden.

1.2 Optionale Services

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

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

Der Begriff „Kundenanwendung“ bezieht sich auf eine Webanwendung und/oder eine mobile Anwendung. Eine Webanwendung gruppiert alle Funktionen, die den berechtigten Teilnehmern des Kunden über mehrere Webseiten oder von einer Anmelde- oder Identifikationsanzeige angeboten und als einzelne Anwendung in der Trusteer-Konsole (Trusteer Management Application) überwacht werden. Eine mobile Anwendung gruppiert alle Funktionen, die den berechtigten Teilnehmern des Kunden über ein einzelnes Softwareprogramm, das aus einem Application Store (Store) heruntergeladen werden kann, oder von einer Anmelde- oder Identifikationsanzeige angeboten und als einzelne Anwendung in der Trusteer-Konsole (Trusteer Management Application) überwacht werden.

Für die IBM Trusteer Pinpoint-Integration ist für jede Anwendung eine Berechtigung für IBM Trusteer Pinpoint Application erforderlich.

- Für die Bereitstellung von IBM Trusteer Pinpoint Detect Standard ist für jede Anwendung eine Berechtigung für IBM Trusteer Pinpoint Detect Standard Application erforderlich.

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

Der Begriff „Kundenanwendung“ bezieht sich auf eine Webanwendung und/oder eine mobile Anwendung. Eine Webanwendung gruppiert alle Funktionen, die den berechtigten Teilnehmern des Kunden über mehrere Webseiten oder von einer Anmelde- oder Identifikationsanzeige angeboten und als einzelne Anwendung in der Trusteer-Konsole (Trusteer Management Application) überwacht werden. Eine mobile Anwendung gruppiert alle Funktionen, die den berechtigten Teilnehmern des Kunden über ein einzelnes Softwareprogramm, das aus einem Application Store (Store) heruntergeladen werden kann, oder von einer Anmelde- oder Identifikationsanzeige angeboten und als einzelne Anwendung in der Trusteer-Konsole (Trusteer Management Application) überwacht werden.

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

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

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

Dieser für Pinpoint-Subskribenten verfügbare Service ist dazu ausgelegt, bei der Erstellung neuer Konten frühzeitig Unregelmäßigkeiten zu erkennen, verdächtige Aktivitäten zu markieren und Warnungen zu generieren. Der Service überwacht neue Konten über die in der TMA verfügbaren Nutzungsberichte, um

betrügerische Aktivitäten, die neu angelegte Konten und danach die bestehenden Konten betreffen, durch Account Profiling aufzudecken und durch eine Frühwarnung anzuzeigen, dass es sich bei dem neuen Konto möglicherweise um einen „Mule Account“ handelt oder um ein Konto, das für Betrügereien benutzt wird.

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

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

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

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

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

1.2.5 IBM Trusteer Pinpoint Malware Detection

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

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

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

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

a. Ereignisdaten:

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

b. Advanced Edition:

   Die Advanced Editions for Business und/oder for Retail bieten zusätzliche Erkennungs- und Schutzstufen, die an die Struktur und den Ablauf der Business- und/oder Retail-Anwendungen des Kunden angepasst sind und auf die Bedrohungslandschaft, der das Unternehmen des Kunden

ausgesetzt ist, abgestimmt werden können. Sie können an verschiedenen Standorten in die Business- und/oder Retail-Anwendungen des Kunden integriert werden.

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

c. Standard Edition:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Dieser Service beinhaltet bis zu 200 Stunden an gemeinsam genutzten Ressourcen für Bereitstellungsservices pro Anwendung und 200 Stunden an gemeinsam genutzten Ressourcen für eine Sicherheitsanalyse pro Anwendung beim Setup. Die fortlaufenden Services schließen 20 Stunden an

Wartungsleistungen für die Bereitstellung pro Anwendung und Jahr sowie 100 Stunden an Sicherheitsuntersuchungen pro Anwendung und Jahr ein.

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

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

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

1.2.14 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

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

Dieser Cloud-Service erweitert IBM Trusteer Pinpoint Detect. Er bietet zusätzliche Informationen und Kontext zu Mobiltelefonnummern, die diesem Cloud-Service zur Verfügung gestellt werden, und trägt so dazu bei, das Betrugsrisiko einer bestimmten Sitzung zu ermitteln. Der Kunde kann durch eine Abfrage des Cloud-Service Merkmale einer bestimmten Mobiltelefonnummer herausfinden, z. B. Informationen über den Mobilfunkanbieter, zu dem diese Nummer gehört.

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

1.3 Acceleration Services

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

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

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

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

1.3.2 IBM Trusteer Pinpoint Malware Detection Redeployment

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

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

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

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

2. Datenblätter für Datenverarbeitung und Datenschutz

Die Ergänzenden Bedingungen zur Auftragsverarbeitung von IBM unter http://ibm.com/dpa (EB-AV) und die Datenblätter für Datenverarbeitung und Datenschutz (Data Processing and Protection Data Sheet(s), nachfolgend „Datenblätter“ oder „Anlagen zu den EB-AV“ genannt) unter den nachstehenden Links enthalten zusätzliche Datenschutzinformationen für die Cloud-Services und deren Optionen in Bezug auf die Arten der Inhalte, die verarbeitet werden können, die damit verbundenen Verarbeitungstätigkeiten, die Datenschutzfunktionen und die Besonderheiten hinsichtlich der Aufbewahrung und Rückgabe der Inhalte. Die EB-AV finden Anwendung, wenn und soweit IBM personenbezogene Daten im Auftrag des Kunden verarbeitet und i) die europäische Datenschutz-Grundverordnung (EU/2016/679) (DSGVO) oder ii) eines der unter http://ibm.com/dpa/dpl aufgeführten weiteren Datenschutzgesetze auf diese Verarbeitung Anwendung findet.

Dazu ist anzumerken, dass in den Datenblättern im Allgemeinen alle Standorte aufgelistet werden, an denen IBM (sowie die externen Unterauftragsverarbeiter) personenbezogene Daten hosten und verarbeiten, ungeachtet des Rechenzentrums, von dem die Services erbracht werden. Eine Liste der Hosting- und Verarbeitungsstandorte, die dem Rechenzentrum zugeordnet sind, von dem die Services erbracht werden, ist in Abschnitt 5.2 (Zusätzliche Informationen über den Verarbeitungsstandort) zu finden.

IBM Trusteer Pinpoint Criminal Detect

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

IBM Trusteer Pinpoint Detect

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

IBM Trusteer Pinpoint Malware Detection

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

IBM Trusteer Mobile SDK

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

3. Service-Levels und technische Unterstützung

3.1 Service-Level-Agreement

IBM stellt dem Kunden das folgende Verfügbarkeits-Service-Level-Agreement („SLA“) bereit. IBM wird die höchstmögliche Entschädigung basierend auf der kumulierten Verfügbarkeit des Cloud-Service anwenden (siehe die nachstehende Tabelle). Der Prozentsatz der Verfügbarkeit wird berechnet als Gesamtzahl der Minuten in einem Vertragsmonat, minus der Gesamtzahl der Serviceausfallminuten in dem betreffenden Vertragsmonat, dividiert durch die Gesamtzahl der Minuten in dem Vertragsmonat. Die Definition von Serviceausfall, der Prozess zur Bearbeitung von Ansprüchen und die Kontaktaufnahme mit IBM bei Problemen mit der Serviceverfügbarkeit sind im IBM Cloud Service-Supporthandbuch unter https://www.ibm.com/software/support/saas_support_overview.html enthalten.

Verfügbarkeit	Gutschrift (in Prozent (%) der monatlichen Subscription-Gebühr*)
Unter 99,9 %	2 %
Unter 99,0 %	5 %
Unter 95,0 %	10 %

* Die Subscription-Gebühr ist der vertraglich vereinbarte Preis für den Monat, der Gegenstand des Anspruchs ist.

3.2 Technische Unterstützung

Eine Beschreibung der technischen Unterstützung für den Cloud-Service, einschließlich Support-Kontaktinformationen, Fehlerklassen, Unterstützungszeiten, Reaktionszeiten und sonstiger Unterstützungsinformationen und -prozesse, finden Sie durch Auswahl des Cloud-Service im IBM Support Guide, der unter https://www.ibm.com/support/home/pages/support-guide/ verfügbar ist.

Premium Support:

Eine Premium Support-Subscription ist gegen Aufpreis für den Cloud-Service verfügbar und umfasst Folgendes:

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

4. Gebühren

4.1 Gebührenmetriken

Die Gebührenmetriken für den Cloud-Service sind im Auftragsdokument angegeben.

Für diesen Cloud-Service gelten die folgenden Gebührenmetriken:

- „Kundenprojekt“ (Engagement) ist ein Professional Service oder Schulungsservice im Zusammenhang mit den Cloud-Services.
- „Berechtigter Teilnehmer“ ist eine Einzelperson oder Entität, die zur Teilnahme an einem von den Cloud-Services verwalteten oder überwachten Servicebereitstellungsprogramm berechtigt ist.
- „Anwendung“ ist ein eindeutig benanntes Softwareprogramm, das von den Cloud-Services entwickelt oder für den Zugriff auf die Cloud-Services und zu ihrer Verwendung zur Verfügung gestellt wurde.
- „API-Aufruf“ ist der Aufruf der Cloud-Services über eine programmierbare Schnittstelle.
- „Verbindung“ ist die Anbindung oder Zuordnung einer Datenbank, einer Anwendung, eines Servers oder einer anderen Art von Einheit, die für die Cloud-Services verfügbar gemacht wurden oder werden.

4.2 Gebühren für Remote Services

Ein Remote Service endet 90 Tage nach dem Erwerb, unabhängig davon, ob er in Anspruch genommen wurde.

5. Zusätzliche Bedingungen

Für Vereinbarungen für Cloud-Services (oder vergleichbare Cloud-Basisvereinbarungen), die vor dem 1. Januar 2019 unterzeichnet wurden, finden die Bedingungen unter https://www.ibm.com/acs Anwendung.

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

Folgende Regelung gilt für IBM Trusteer Rapport-Cloud-Services (einschließlich Rapport Remediation oder Rapport for Mitigation, wenn die Bereitstellung in Verbindung mit den Pinpoint-Cloud-Services erfolgt): Sofern nicht abweichend vereinbart und gemäß der Verarbeitungsgrundlage, die der Kunde selbst festgelegt hat, erteilt der Kunde IBM die Berechtigung, die unter https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA verfügbare Endbenutzerlizenzvereinbarung anzuwenden, damit IBM die für die Erbringung der Cloud-Services benötigten Informationen erfassen und verarbeiten kann.

In Bezug auf IBM Trusteer Rapport-Cloud-Services berechtigt der Kunde IBM, als Auftragsverarbeiter des Sponsorunternehmens, das Programm für die Erfassung von Malware und Malware-Artefakten, d. h. Dateien, die mit böswilligen Aktivitäten oder mit einer ungewöhnlichen Fehlfunktion des Programms in Zusammenhang stehen, zu nutzen. IBM verwendet das Programm nicht, um Dateien mit personenbezogenen Daten des Endbenutzers abzugreifen; es könnte jedoch sein, dass die erfassten Dateien personenbezogene Daten enthalten, die von der Malware ohne die Genehmigung des Endbenutzers erfasst wurden. IBM wird 1) alle Dateien unverzüglich löschen, die für eine solche Analyse nicht relevant sind, und 2) relevante Dateien nur für die Dauer der Analyse und auf keinen Fall länger als drei Monate aufbewahren.

5.2 Zusätzliche Informationen zum Verarbeitungsstandort

Alle personenbezogenen Daten werden an den nachstehend angegebenen Standorten gehostet und verarbeitet, auch wenn das Hosting und die Verarbeitung von den im Datenblatt angegebenen externen Unterauftragsverarbeitern durchgeführt wird:

Bei allen Services, die über das Rechenzentrum in Deutschland erbracht werden, beschränkt IBM das Hosting und die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, sowie auf die folgenden Länder: Deutschland, Israel, Irland und die Niederlande.

Bei allen Services, die über das Rechenzentrum in Japan erbracht werden, beschränkt IBM das Hosting und die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, sowie auf die folgenden Länder: Japan, Israel und Irland.

Bei allen Services, die über das Rechenzentrum in den USA erbracht werden, beschränkt IBM das Hosting und die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, sowie auf die folgenden Länder: USA, Israel, Irland, Singapur und Australien.

Hinsichtlich aller Services, die über Rechenzentren in Deutschland, Japan und den USA erbracht werden, können zusätzlich zu den obigen Standorten (1) unterstützende Daten in Deutschland und Frankreich von Salesforce.Com als externem Unterauftragsverarbeiter von IBM gehostet und verarbeitet werden und (2) für Kunden, die es bevorzugen, Daten an Mobile Carrier Intelligence-Provider zu senden, personenbezogene Daten in den Ländern der jeweiligen externen Unterauftragsverarbeiter, die im Datenblatt aufgeführt sind, gehostet und verarbeitet werden. Ungeachtet gegenteiliger Angaben im Datenblatt haben die in Klausel (2) des unmittelbar vorangehenden Satzes angegebenen externen Unterauftragsverarbeiter unter Umständen keine Compliance-Zertifizierung für ISO 27001 oder SOC2.

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

5.3 Daten des Kontoinhabers

Zur Erläuterung: Falls mehr als ein IBM Kunde mit der Client-Software für Kontoinhaber eines bestimmten Kontoinhabers verbunden ist (solche IBM Kunden werden als „Verbundene Kunden“ (Affiliated Customers) bezeichnet) und die Services unter dieser Servicebeschreibung von IBM für diese verbundenen Kunden über Rechenzentren in verschiedenen Regionen erbracht werden, dann können die Daten des Kontoinhabers an allen Standorten verarbeitet werden, die den einzelnen oben in Abschnitt 5.2 angegebenen Rechenzentren zugeordnet sind.

5.4 Integrierte Lösungen

Es wird ausdrücklich darauf hingewiesen, dass die verschiedenen Angebote der Marke Trusteer als integrierte Lösung implementiert sein können. Selbst wenn der Kunde einen dieser Cloud-Services kündigt, kann IBM Kundendaten aufbewahren, damit sowohl die übrigen Cloud-Services, die durch diese

Servicebeschreibung abgedeckt sind, als auch andere Trusteer-Services gemäß den für sie anwendbaren Servicebeschreibungen erbracht werden können.

5.5 Aktivierungssoftware

Der Cloud-Service enthält die folgende Aktivierungssoftware:

- IBM Rapport Agents

5.6 Best Practices bei Pinpoint

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

5.7 Datenerfassung im Rahmen der Bereitstellung

Bei der Bereitstellung des Cloud-Service können bestimmte Daten des Kunden an IBM weitergegeben werden. Diese Daten dürfen keine Informationen enthalten, die es ermöglichen, bestimmte Personen zu identifizieren, oder die bestimmten Personen zugeordnet werden können. Weitere Richtlinien zu Daten, die im Rahmen der Bereitstellung an IBM weitergegeben werden, sind in den Trusteer Deployment Guidelines zu finden, die dem Kunden zur Verfügung gestellt werden müssen.

6. Übergeordnete Bedingungen

6.1 Nutzung von Daten

Folgende Bestimmung hat Vorrang vor gegenteiligen Bestimmungen im Abschnitt „Inhalte und Datenschutz“ der Basisbedingungen für Cloud-Services zwischen den Vertragsparteien: IBM wird die Ergebnisse, die sich aus der Nutzung des Cloud-Service durch den Kunden ergeben und sich eindeutig auf Kundeninhalte beziehen (Erkenntnisse) oder den Kunden anderweitig identifizieren, weder verwenden noch offenlegen. IBM ist jedoch berechtigt, Inhalte und andere Informationen, die sich im Rahmen des Cloud-Service aus den Inhalten ergeben, zu verwenden, sofern persönliche Kennungen entfernt wurden, sodass personenbezogene Daten ohne die Verwendung zusätzlicher Informationen nicht mehr einer bestimmten Person zugeordnet werden können. IBM wird diese Daten ausschließlich für Forschungs- und Testzwecke sowie für die Angebotsentwicklung verwenden.