IBM Trusteer Pinpoint Verify

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

1. Cloud-Service

Zu IBM Trusteer Pinpoint Verify gehört das Feature Step-Authenticate, eine erweiterte Authentifizierung, die für ausgewählte Hochrisikofälle gestartet werden kann, um sicherzustellen, dass sicherheitsrelevante digitale Interaktionen durch Pinpoint geschützt werden. Damit wird das Risiko gemindert, wenn Trusteer das Risiko einer beabsichtigten betrügerischen Handlung vorhersagt oder wenn für die Benutzeraktivität eine höhere Stufe der Identitätssicherung erforderlich ist.

1.1 Angebote

1.1.1 IBM Trusteer Pinpoint Verify

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

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

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.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=D7AB2D30CB2C11E99CFB3A1B59E5A549

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 Technischer Support

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.

4. Gebühren

4.1 Gebührenmetriken

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

Für diesen Cloud-Service gelten die folgenden Gebührenmetriken:

- „Berechtigter Teilnehmer“ ist eine Einzelperson oder Entität, die zur Teilnahme an einem von den Cloud-Services verwalteten oder überwachten Servicebereitstellungsprogramm berechtigt ist.
- „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.

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 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.

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 (ausgenommen Erkenntnissen) ergeben, für die Verbesserung des Cloud-Service zu verwenden. Des Weiteren ist IBM berechtigt, Bedrohungs-IDs und weitere Sicherheitsinformationen, die in Inhalten eingebettet sind, zum Zweck der Erkennung von Sicherheitsbedrohungen und zum Schutz vor Sicherheitsbedrohungen weiterzugeben.