IBM Trusteer Pinpoint Verify

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order.

1. Cloud Service

IBM Trusteer Pinpoint Verify features Step-Authenticate, a step-up authentication that can be initiated on selected high risk cases to help ensure security-enabled digital interactions are protected by Pinpoint. This remediates the risk when Trusteer predicts a risk of intended fraudulent activity, or when the user activity requires a higher level of identity assurance.

1.1 Offerings

1.1.1 IBM Trusteer Pinpoint Verify

Client must have a current subscription to IBM Trusteer Pinpoint Detect or IBM Trusteer Pinpoint Assure prior to subscribing to this Cloud Service.

This Cloud Service provides capabilities to challenge users for a second factor of authentication in order to verify their identities when accessing a digital service. It is available for Pinpoint Detect and Pinpoint Assure, in order to provide a second factor authentication for protected applications. The decision on when to challenge users for second factor authentication is derived by the protected application, and can be based on the recommendations returned by the Pinpoint Detect or Pinpoint Assure platforms or any other policies defined by the protected application. This Cloud Service is powered by IBM Cloud Identity Verify technology.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at http://ibm.com/dpa (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below provide additional data protection information for the Cloud Services and its options regarding the types of Content that may be processed, the processing activities involved, the data protection features, and specifics on retention and return of Content. The DPA applies to personal data contained in Content, if and to the extent i) the European General Data Protection Regulation (EU/2016/679) (GDPR); or ii) other data protection laws identified at http://ibm.com/dpa/dpl apply.

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

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at https://www.ibm.com/support/home/pages/support-guide/.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Eligible Participant is an individual or entity eligible to participate in any service delivery program managed or tracked by the Cloud Services.
- Connection is a link or association of a database, application, server, or any other type of device which have been or are made available to the Cloud Services.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at https://www.ibm.com/acs apply.

5.1 Integrated Solutions

For purposes of clarification, the various offerings under the Trusteer brand could constitute an integrated solution. Therefore, if Client terminates any of these Cloud Service, IBM may retain Client data for purposes of providing to Client the remaining Cloud Services under this Service Description as well as other Trusteer services pursuant to the service descriptions applicable to such other Trusteer services.

6. Overriding Terms

6.1 Data Use

The following prevails over anything to the contrary in the Content and Data Protection section of the base Cloud Service terms between the parties: IBM will not use or disclose the results arising from Client's use of the Cloud Service that are unique to Client's Content (Insights) or that otherwise identify Client. IBM will however use Content and other information that result from Content (except for Insights) as part of the Cloud Service for the purpose of improving the Cloud Service. IBM may also share threat identifiers and other security information embedded in Content for threat detection and protection purposes.