IBM Trusteer Pinpoint Assure

本“服务描述”描述云服务。适用的订单文档提供有关客户订单的定价和其他详细信息。

1. 云服务

IBM Trusteer Pinpoint Assure 是一款高度安全的分层解决方案，专门帮助防止带有欺诈意图的个人使用被盗身份、向真实身份添加虚假数据，或创建合成身份以用于开展访客交易、开通新帐户或代表现有客户开通新的数字帐户。

1.1 服务产品

1.1.1 IBM Trusteer Pinpoint Assure

此服务标记为可疑活动并在新帐户创建/注册过程中生成警报。此服务会对帐户注册过程进行监控，以识别与欺诈相关的活动，通过 Trusteer Management Application (TMA) 中提供的使用情况报告，提供早期警告信号，提醒新帐户可能为“骡子”帐户或者过去常用于执行欺诈。IBM Trusteer Pinpoint Detect 和 IBM Trusteer Pinpoint Verify 用作 TMA 登录的一部分。

IBM Trusteer Pinpoint Assure 打包提供，每年每 100 个连接为一包。

1.2 可选服务

1.2.1 IBM Trusteer Pinpoint Assure Application

对于 IBM Trusteer Pinpoint Assure，任何应用程序上的部署都需要获取 IBM Trusteer Pinpoint Assure Application 的权利。

IBM Trusteer Pinpoint Assure 可按应用购买。

1.2.2 IBM Trusteer Mobile Carrier Intelligence

在订购此云服务之前，客户必须具有 IBM Trusteer Pinpoint Assure 的当前订购。

此云服务通过提供有关向这些云服务中的任意服务提供的移动号码的其他信息和上下文，增强 IBM Trusteer Pinpoint Assure，从而帮助确定给定会话的欺诈风险。客户可以查询此云服务来了解有关给定移动号码的特征，如与该号码关联的运营商信息。

该云服务提供的有关移动号码的数据（“移动情报”）仅可用于客户的内部目的，并且只能保留 30 天。客户必须在此期限后重新查询就相同移动号码重新查询云服务，以获取有关该号码的移动情报，并且不能简单地重新使用从先前查询收到的移动情报。除了以上允许的情况外，客户不得缓存、重新使用或与任何数据挖掘整体或部分结合使用或存档任何移动情报。

2. 数据处理和保护数据表

位于 http://ibm.com/dpa 的 IBM 数据处理附录 (DPA) 以及下面链接中的“数据处理和保护数据表”（称为数据表或 DPA 附录）提供针对云服务及其选项的其他数据保护信息，关于可处理的内容类型、所涉及的处理活动、数据保护功能以及有关内容保留和返回的细节。如果 i) 欧盟通用数据保护条例 (EU/2016/679) (GDPR)；或 ii) http://ibm.com/dpa/dpl 上标示的其他数据保护法律适用于内容中包含的个人数据，那么 DPA 也适用于这些个人数据。

据澄清，数据表一般列出 IBM（包括任何第三方分包处理机构）托管和处理个人数据的所有位置，与部署服务的数据中心无关。有关特定于部署服务的数据中心的托管和处理位置列表，请参阅以下第 5.1 节（附加处理位置信息）。

IBM Trusteer Assure

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=CF0C527046E011E8ADCBA344DE8FB657

IBM Trusteer Mobile SDK

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

3. 服务级别和技术支持

3.1 服务标准协议

IBM 为客户提供以下可用性服务级别协议 (SLA)。IBM 会根据累积的可用云服务应用适用的最高赔偿，如下表中所示。可用性百分比的计算方法为：“约定的月份”内总分钟数减去“约定的月份”内服务停用的总分钟数，再除以“约定的月份”内总分钟数。“服务停用”定义、索赔过程以及如何联系 IBM 反馈服务可用性问题在 IBM 的云服务支持手册 (https://www.ibm.com/software/support/saas_support_overview.html) 中进行了说明。

可用性	积分 （每月订购费用的百分比*）
小于 99.9%	2%
低于 99.0%	5%
低于 95.0%	10%

* 订购费用是当月该索赔相关的合同价格。

3.2 技术支持

通过在位于 https://www.ibm.com/support/home/pages/support-guide/ 的 IBM 支持指南中选择云服务来查找针对云服务的技术支持，包括支持联系人详细信息、严重性级别、可用性的支持小时数、响应时间以及其他支持信息和流程。

4. 费用

4.1 收费标准

云服务的收费标准在交易文档中指定。

以下收费标准适用于此云服务：

- 连接是数据库、应用程序、服务器或已连接到云服务并可供云服务使用的任何其他类型设备的链接或关联。
- 应用程序是由云服务开发、访问或使用的具有唯一名称的软件程序。

5. 附加条款

对于 2019 年 1 月 1 日之前执行的云服务协议（或等效的基础云协议），可用的条款 (https://www.ibm.com/acs) 将适用。

5.1 附加处理位置信息

个人数据的所有托管和处理，包含数据表中标识的任何第三方分包处理机构负责的托管和处理，都将在以下指定位置进行：

对于通过德国数据中心提供的所有服务，IBM 会将个人数据的托管和处理工作限制在 IBM 合同实体所在国家或地区，以及以下国家或地区：德国、以色列、爱尔兰及荷兰。

对于通过日本数据中心提供的所有服务，IBM 会将个人数据的托管和处理工作限制在 IBM 合同实体所在国家或地区，以及以下国家或地区：日本、以色列及爱尔兰。

对于通过美国数据中心提供的所有服务，IBM 会将个人数据的托管和处理工作限制在 IBM 合同实体所在国家或地区，以及以下国家或地区：美国、以色列、爱尔兰、新加坡及澳大利亚。

除了上述位置，对于通过德国、日本和美国数据中心提供的所有服务，(1) 支持数据可由 Salesforce.Com 作为 IBM 的第三方分包处理机构在德国和法国进行托管或处理，以及 (2) 对于选择将数据发送到 Mobile

Carrier Intelligence 提供程序的客户，个人数据可按数据表中的规定，在适用的第三方分包处理机构所在国家或地区内进行托管和处理。无论数据表中有任何相反的规定，前一条的第 (2) 款中指定的第三方分包处理机构可能不符合 ISO 27001 或 SOC2。

根据相关 IBM 人员的可用性、客户端的位置以及托管数据的数据中心，还可根据需要提供 IBM Trusteer 支持和帐户维护服务。

5.2 集成解决方案

为澄清起见，Trusteer 品牌下的各服务产品可构成一个集成解决方案。因此，如果客户终止了其中的任何云服务，IBM 会保留客户数据，以便按照此服务描述向客户提供剩余的云服务，以及根据适用于此类其他 Trusteer 服务的服务描述，提供其他 Trusteer 服务。

5.3 部署中收集的数据

云服务的部署可能需要客户向 IBM 提供特定数据。此类数据不得包含可识别或可归因于具体个人的信息。有关在部署中提供给 IBM 的数据的更多准则，包含在提供给客户的《Trusteer 部署指南》中。

6. 覆盖条款

6.1 数据使用

以下条款优先于双方之间基本云服务条款的“内容和数据保护”部分中的任何相反内容：IBM 不会使用或披露客户使用云服务而产生的专属于客户的内容的结果（洞察）或以其他方式表明客户身份的结果。但是，IBM 将在提供云服务的过程中使用这些内容以及由这些内容生成的其他信息（洞察除外）来改进云服务。IBM 可能还会共享威胁标识和嵌入在内容中的其他安全信息，以进行威胁检测和实施保护。