IBM Trusteer Pinpoint Detect

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 是基于云的服务，旨在提供另一层保护，用于检测并缓解恶意软件、钓鱼和帐户接管攻击。Trusteer Pinpoint 可集成到客户订购了云服务覆盖范围的客户企业应用程序和/或零售应用程序以及防欺诈流程中。

此云服务包括：

a. Trusteer Management Application (TMA) 和 Trustboard：

TMA 是 Trusteer 的传统管理应用程序，允许客户评估和分类警报。Trustboard 是一个较新的管理应用程序，主要用于研究。客户可以随时选择使用 TMA 或 Trustboard。TMA 和 Trustboard 均在 IBM Trusteer 云托管环境中提供，通过 TMA 和 Trustboard，客户（及其数量不限的授权人员）可以：(i) 查看和下载特定事件数据报告和风险评估，以及 (ii) 查看、订购从 Pinpoint 服务产品生成的威胁订阅源并配置其交付。IBM Trusteer Pinpoint Detect 和 IBM Trusteer Pinpoint Verify 用作 TMA 和 Trustboard 登录的一部分。

b. Web 脚本和/或 API：

适用于旨在访问、测试或使用云服务的 Web 站点部署。

“会话”是客户应用程序（Web 或移动）和云服务之间的交互，生成一个或多个实时风险评估。会话是从交互开始时到交互结束时测量的。在发生以下某个事件时记录交互结束时间：

- 通过正常注销应用程序重置交互。
- 关闭浏览器、应用程序或选项卡。
- 删除 Cookie。
- 超时。

会话可以包含任意数量的活动，例如：登录、浏览、结账、付款设置和由客户应用程序定义的其他活动。需要说明的是，对于此云服务，一个连接（定义如下）是一个会话。

1.1 服务产品

客户可以从以下可用服务产品中选择。

1.1.1 IBM Trusteer Pinpoint Detect Standard for Retail 和/或 IBM Trusteer Pinpoint Detect Standard for Business

此云服务将 IBM Trusteer Pinpoint Criminal Detection 和 IBM Trusteer Pinpoint Malware Detection 两个云服务加以结合，以提供单一的统一解决方案。

该解决方案有助于使用设备标识、钓鱼检测和恶意软件驱动的凭证盗窃检测对连接到零售或企业应用程序的浏览器的恶意软件和/或可疑帐户接管活动进行无客户端检测。IBM Trusteer Pinpoint 服务产品可提供另一层保护，旨在检测帐户接管的尝试，并将（通过本机浏览器或客户移动应用）访问零售或企业应用程序的浏览器或移动设备的风险评估得分直接提供给客户。此服务还可用于远程员工访问，以评估受管和非受管设备的风险。

在此云服务中包含高级支持（根据以下“技术支持”部分中的定义）。

服务可按每包 100 个合格参与者购买，或每包 100 个连接。

1.1.2 IBM Trusteer Pinpoint Detect Premium for Retail 和/或 IBM Trusteer Pinpoint Detect Premium for Business

此云服务将 IBM Trusteer Pinpoint Criminal Detection 和 IBM Trusteer Pinpoint Malware Detection 结合，以提供单一、易于集成的统一解决方案。

该解决方案有助于使用设备标识、钓鱼检测和恶意软件驱动的凭证盗窃检测对连接到零售或企业应用程序的浏览器的恶意软件和/或可疑帐户接管活动进行无客户端检测。IBM Trusteer Pinpoint 服务产品可提供另一层保护，旨在检测帐户接管的尝试，并将（通过本机浏览器或客户移动应用）访问企业或零售应用的浏览器或移动设备的风险评估得分直接提供给客户。

此服务拥有增强的功能和服务，包括：扩展的部署和设置服务、定制的安全策略、调查服务等。此服务包括为每个应用提供多达 200 小时的共享资源以进行部署服务，以及每个应用 200 小时的共享资源以对设置进行安全分析。正在进行的服务包括每个应用每年 20 小时的部署维护，以及每个应用每年 100 小时的安全研究。任何附加工作都需要附加费用。

Pinpoint Detect 可通过手机与网页渠道开展交易。如果包含手机交易，那么 Pinpoint by Connection 适用。此云服务包含对一个应用程序的保护。对于每个额外应用，客户应获取 IBM Trusteer Pinpoint Detect Premium Additional Applications 的权利。

此云服务包含金牌支持。

IBM Trusteer Pinpoint Detect Premium for Retail and Business 服务可按每包 100 个合格参与者购买，或者按每包 100 个连接购买 IBM Trusteer Pinpoint Detect Premium。若客户选择按连接购买服务，则附加应用收费适用于第一个应用。

Pinpoint Detect Policy Manager：

Policy Manager 包含在 Pinpoint Detect Premium 服务中，在 IBM Trusteer 云托管环境中提供，通过此服务，客户（以及数量不限的授权人员）可以：(i) 设计、测试和部署到生产环境逻辑以检测欺诈活动，(ii)设计报告和仪表板，并且 (iii) 查看、配置和设置安全策略以及用于检测客户应用程序中的可疑活动的其他策略。

要激活 Policy Manager 功能部件和其他必需的深入支持，需要咨询服务。咨询服务的详细信息将在工作说明中单独列出。

激活 Policy Manager 后，IBM 保留访问客户环境以获得支持的权利，以调整客户的策略来修复由于策略更改导致的主要问题。

客户承诺保护通过 Policy Manager 公开的数据不被滥用。

激活 Policy Manager 功能后，客户必须遵循文档中所列的 IBM 规则设置准则。客户承认 IBM 对于客户不遵循这些建议而导致的任何情况不承担任何责任。

由于客户对 Policy Manager 功能配置错误所造成的任何稳定性和/或服务降级问题将不被视为 SLA 计算的宕机。

1.1.3 IBM Trusteer Pinpoint Detect for Connections

此云服务可提供保护，旨在检测帐户接管尝试，并提供（通过客户移动应用程序的本机浏览器）访问企业或零售应用程序的浏览器和/或移动设备的风险/信任评估得分。此解决方案使用多个风险指标来分析最终用户的设备、连接和行为，并将其与用户历史记录进行比较，从而确定可疑的使用。

此云服务可使用与移动和 Web 通道的连接。IBM Trusteer Pinpoint Detect 中包括 IBM Trusteer Mobile SDK（如果相关）的权利。

此云服务可按每包 100 个连接/年进行购买。

1.1.4 IBM Trusteer Pinpoint Detect Bundle

本云服务包由 IBM Trusteer Pinpoint Detect、IBM Trusteer Mobile SDK 和 IBM Trusteer Rapport 提供支持。此云服务可提供保护，旨在检测帐户接管尝试，并提供（通过客户移动应用程序的本机浏览器）访问企业或零售应用程序的浏览器和/或移动设备的风险/信任评估得分。此解决方案使用多个风险指标来分析最终用户的设备、连接和行为，并将其与用户历史记录进行比较，从而确定可疑的使用。

此服务可供有效用户购买。

此云服务可使用与移动和 Web 通道的连接。IBM Trusteer Pinpoint Detect 包含针对 IBM Trusteer Mobile SDK 的访问权。

IBM Trusteer Pinpoint Detect Bundle 包括针对 IBM Trusteer Rapport 的访问权。除非 IBM 另有书面规定，否则此访问权不包括 Trusteer Splash 和 IBM Trusteer Rapport Rapport MandatoryService。

IBM Trusteer Mobile SDK

IBM Trusteer Mobile SDK Cloud Service 旨在提供另一层保护，为客户订购了云服务覆盖范围的企业应用程序和/或零售应用程序提供安全的 Web 访问，另外还提供设备风险评估和网络钓鱼攻击防御。仅针对 Android 平台提供安全的 Wi-Fi 检测。

IBM Trusteer Mobile SDK Cloud Service 包含专属的移动软件开发者工具箱（“SDK”），该软件包中包含文档、编程专用软件库和其他相关文件与项目，称为 IBM Trusteer 移动库以及“运行时组件”或“可再分发版”，这是一个专用代码，此代码由可嵌入并集成到客户的受保护独立 iOS 或 Android 移动应用程序中的 IBM Trusteer Mobile SDK 生成，客户已为这些独立 iOS 或 Android 移动应用程序订购了 Cloud Service 覆盖范围。（“客户集成的移动应用”）。

客户可以：

a. 在内部使用 IBM Trusteer Mobile SDK，但仅限用于开发“客户集成的移动应用”；

b. 将“可再分发版”（仅限以对象代码格式）以整体性不可分割方式嵌入“客户集成的移动应用”。根据本许可证授权的“可再分发版”的任何已修改或合并部分应受到本服务描述的条款的约束；并且

c. 营销和分发“可再分发版”以下载到合格参与者的移动设备或客户设备持有者，假设：

- 除非本协议明确许可，否则客户 (1) 不得使用、复制、修改或分发 SDK；(2) 不得对 SDK 进行反汇编、反编译或以其他方式执行转换或反向工程，除非法律明确许可且不存在合同弃权的可能性；(3) 不得再许可、出租或租赁 SDK；(4) 不得移除“可再分发版”中包含的任何版权或声明文件；(5) 不得使用与原始“可再分发版”文件/模块相同的路径名； (6) 未经 IBM 或其供应商或分销商的事先书面同意，不得在“客户集成的移动应用”相关营销中使用 IBM、其供应商或分销商的名称或商标。
- “可再分发版”必须以不可分割的方式集成在“客户集成的移动应用”中。“可再分发版”只能采用目标代码形式，必须符合 SDK 及其文档中的所有指示、指令和规范。“客户集成的移动应用”的最终用户许可协议必须告知最终用户“可再分发版”：i) 不得用于除支持“客户集成的移动应用”之外的任何其他目的；ii) 不得拷贝（除非出于备份目的）；iii) 不得进一步分发或转让；iv) 不得反汇编、反编译或者以其他方式进行转换，除非法律明确许可且不存在合同弃权的可能性。客户的许可协议必须至少与 IBM 在本协议中提供的保护相同。
- SDK 只能在对客户指定的移动测试设备进行内部开发和单元测试的过程中进行部署。客户无权使用此 SDK 处理生产工作负载，模拟生产工作负载或测试任何代码、应用程序或系统的可扩展性。客户无权将此 SDK 的任何部分用于任何其他用途。

客户单独负责开发、测试和支持“客户集成的移动应用”。在此处允许的范围内，客户负责“客户集成的移动应用”的所有技术援助和对“可再分发版”的任何修改。

客户获得授权安装和使用“可再分发版”和 IBM Security Mobile SDK 仅用于支持客户对云服务的使用。

IBM 不保证使用 IBM Security Mobile SDK 附带的移动工具创建的任何应用程序或输出将与任何特定的移动操作系统平台或移动设备一起运行、相互操作或相互兼容。

源组件和样本资料 - IBM Trusteer Mobile SDK 可能包含源代码形式的一些组件（“源组件”）和其他标识为“样本资料”的资料。客户可以复制和修改源组件和样本资料，但仅供内部使用，前提是此类使用在本协议的许可权限范围内；并且客户不得更改或删除源组件和样本资料中包含的任何版权信息或声明。IBM“按现状”提供源组件和样本资料，不带任何支持义务。请注意，提供源组件或样本资料仅作为如何在 CIMA 中实施可嵌入项的示例，源组件或样本资料可能与客户的开发环境不兼容，并且客户自行负责 CIMA 中可嵌入项的测试和实施。

如果本协议中的云服务由国际商业机器公司（一家位于纽约的公司，简称“IBM 公司”）以外的其他公司提供，则本段落中的以下规定适用。本协议中的 SDK 和 Redistributable 的权利由 IBM 公司提供。IBM 作为分销商，根据本协议提供 SDK 和 Redistributable，并负责执行条款，履行与此 SDK 和 Redistributable 相关的所有义务。本协议不赋予任何权利或诉因以支持客户对 IBM 公司提起诉讼。客户放弃针对 IBM 公司的所有索赔和诉因，同意仅向 IBM 提出有关 SDK 和 Redistributable 的任何相关权利和补救措施。

IBM Trusteer Rapport

Trusteer Rapport 提供了一层针对钓鱼和浏览器中间人 (MitB) 恶意攻击的保护。IBM Trusteer Rapport 使用全球数千万个端点组成的网络收集有关针对全球组织的主动钓鱼和恶意攻击的情报。IBM Trusteer Rapport 应用旨在阻止钓鱼攻击和预防 MitB 恶意软件家族的安装和操作的行为算法。

此云服务服务产品包括：

a. Web 脚本：

用于访问、测试或使用云服务的网站访问权。

1.2 可选服务

本部分中的云服务需要满足一项先决条件，即获取 IBM Trusteer Pinpoint Detect Premium、IBM Trusteer Pinpoint Detect Standard、IBM Trusteer Pinpoint for Connections 或 IBM Trusteer Pinpoint Detect Bundle 的权利。

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

客户应用程序是指 Web 应用程序和/或移动应用程序。Web 应用程序在登录或标识屏幕中将通过多个 Web 页面提供给客户合格参与者的所有功能分组在一起，然后在 Trusteer 控制台 (Trusteer Management Application) 中将其作为单个应用程序进行监控。移动应用程序在登录或标识屏幕中将通过一个软件程序（可从应用商店下载）提供给客户合格参与者的所有功能分组在一起，然后在 Trusteer 控制台 (Trusteer Management Application) 中将其作为单个应用程序进行监控。

IBM Trusteer Pinpoint 集成需要为每个应用程序获取 IBM Trusteer Pinpoint Application 的权利。

- IBM Trusteer Pinpoint Detect Standard 部署需要为每个应用程序获取 IBM Trusteer Pinpoint Detect Standard Application 的权利。

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

客户应用程序是指 Web 应用程序和/或移动应用程序。Web 应用程序在登录或标识屏幕中将通过多个 Web 页面提供给客户合格参与者的所有功能分组在一起，然后在 Trusteer 控制台 (Trusteer Management Application) 中将其作为单个应用程序进行监控。移动应用程序在登录或标识屏幕中将通过一个软件程序（可从应用商店下载）提供给客户合格参与者的所有功能分组在一起，然后在 Trusteer 控制台 (Trusteer Management Application) 中将其作为单个应用程序进行监控。

此服务包括为每个应用程序提供多达 200 小时的共享资源以进行部署服务，以及每个应用程序 200 小时的共享资源以对设置进行安全分析。正在进行的服务包括每个应用程序每年 20 小时的部署维护，以及每个应用程序每年 100 小时的安全研究。

- IBM Trusteer Pinpoint Premium 部署需要为每个应用程序获取 IBM Trusteer Pinpoint Detect Premium Application 的权利。

1.2.3 IBM Trusteer New Account Fraud for Retail 和/或 IBM Trusteer New Account Fraud for Business

此服务针对 Pinpoint 订户提供，旨在检测异常情况，标记可疑活动，以及在新帐户创建过程中及早生成警报。此服务会对新帐户进行监控，以识别与旧欺诈帐户和新建帐户概要分析相关的新活动，通过 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 New Account Fraud for Retail 和 IBM Trusteer New Account Fraud for Business 打包提供，每 10 个“API 调用”为一包。

1.2.4 IBM Trusteer Digital Content Pack for Retail 和/或 IBM Trusteer Digital Content Pack for Business

IBM Trusteer Digital Content Pack 支持安全分析人员整合新的欺诈模式，同时完全支持创建和修改特定模式来应对不断演变的威胁。IBM Trusteer Digital Content Pack 由一系列规则、洞察和策略构成，这些内容可作为该解决方案的附加部分和组成部分购买。Digital Content Pack 有助于进一步加强 Trusteer 的数字欺诈预防功能和 IBM Safer Payments 无现金支付渠道之间的整合。通过利用其内置规则和特定业务逻辑，Digital Content Pack 支持银行及其他金融机构进一步增强现有的欺诈检测和预防能力。

IBM Trusteer Digital Content Pack for Retail 按每包 100 个合格参与者提供。IBM Trusteer Digital Content Pack for Business 按每包 10 个合格参与者提供。

要集成 Digital Content Pack with Pinpoint Detect 和 IBM Safer Payments，需要咨询服务；需要重点关注的支持服务也需要咨询服务。咨询服务需根据另行签署的工作说明书单独购买。

1.2.5 IBM Trusteer Pinpoint Malware Detection

在 IBM Trusteer Pinpoint Malware Detection II Cloud Service 中进行恶意软件检测时，客户必须遵循“Pinpoint 最佳实践指南”。在进行恶意软件或帐户接管检测后，请勿立即采用会对合格参与者的体验产生影响的任何方式使用 IBM Trusteer Pinpoint Malware Detection II Cloud Service，否则将使他人能够将客户的操作与 IBM Trusteer Pinpoint Cloud Service 的使用联系起来（例如，进行恶意软件或帐户接管检测后立即发送通知、发送消息、阻止设备或者阻止访问企业和/或零售应用）。

1.2.6 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 和/或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 和/或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 和/或 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II 是新的 IBM Trusteer Pinpoint Malware Detection 结构，可帮助标准化与保护多个应用程序相关的费用，用于取代添加应用程序时的一次性费用。

对连接到企业和/或零售应用程序的受到浏览器中间人 (MitB) 财务恶意软件入侵的浏览器进行无客户端检测。IBM Trusteer Pinpoint Malware Detection Cloud Service 可提供另一层保护，旨在通过为客户提供对是否存在 MitB 财务恶意软件的评估和警报来支持组织专注于基于恶意软件风险的欺诈预防流程。

a. 事件数据：

   客户（及其数量不限的授权人员）可以使用 TMA 来接收由于合格参与者在线与客户的企业应用程序和/或零售应用程序进行交互而生成的事件数据。

b. Advanced Edition：

   针对企业和/或零售的 Advanced Edition 可额外提供一层检测和保护，这层检测和保护是根据客户的企业和/或零售应用程序结构和流程进行调整和定制的，可按客户面临的具体威胁情况加以定制。可将其整合到客户的企业和/或零售应用程序中的多个位置。

   Advanced Edition 按至少 10 万个零售合格参与者或 1 万个企业合格参与者的最低数量提供给客户，即针对零售为 1000 组每组 100 个合格参与者，或针对企业为 1000 组每组 10 个合格参与者。

c. Standard Edition：

   针对企业和/或零售的 Standard Edition 是快速部署解决方案，可提供此处所述的云服务的核心功能。

此云服务包含对一个应用程序的保护。对于每个额外应用程序，客户必须获取 IBM Trusteer Pinpoint Malware Detection Additional Applications 的权利。

1.2.7 针对 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 和/或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 和/或 IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business 和/或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 的可选附加云服务

- 对于 IBM Trusteer Rapport Remediation for Retail Cloud Service，IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail 是先决条件。
- 对于 IBM Trusteer Rapport Remediation for Business Cloud Service，IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business 为先决条件。

1.2.8 IBM Trusteer Pinpoint Criminal Detection for Business 和/或 IBM Trusteer Pinpoint Criminal Detection for Retail

使用设备标识、钓鱼检测和恶意软件驱动的凭证盗窃检测对连接到企业或零售应用程序的浏览器的可疑帐户接管活动进行无客户端检测。IBM Trusteer Pinpoint Criminal Detection Cloud Service 可提供另一层保护，旨在检测帐户接管的尝试并将（通过本机浏览器或客户移动应用程序）访问企业或零售应用程序的浏览器或移动设备的风险评估得分直接提供给客户。

a. 事件数据：

客户可以随时选择使用 TMA 或 Trustboard。客户（以及数量不限的授权人员）可以使用 TMA 或 Trustboard，接收由于合格参与者与客户订购了 Cloud Service 覆盖范围的企业应用程序和/或零售应用程序在线交互而生成的事件数据，或者客户可以通过后端 API 交付方式接收事件数据。

1.2.9 IBM Trusteer Pinpoint Criminal Detection II for Business 和/或 IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Security Pinpoint Criminal Detection II 是新的 IBM Trusteer Pinpoint Criminal Detection 结构，可帮助标准化与保护多个应用程序相关的费用，用于取代添加应用程序时的一次性费用。

使用设备标识、钓鱼检测和恶意软件驱动的凭证盗窃检测对连接到企业或零售应用程序的浏览器的可疑帐户接管活动进行无客户端检测。IBM Trusteer Pinpoint Criminal Detection II Cloud Service 可提供另一层保护，旨在检测帐户接管的尝试并将（通过本机浏览器或客户移动应用程序）访问企业或零售应用程序的浏览器或移动设备的风险评估得分直接提供给客户。

a. 事件数据：

客户可以随时选择使用 TMA 或 Trustboard。客户（以及数量不限的授权人员）可以使用 TMA 或 Trustboard，接收由于合格参与者与客户订购了 Cloud Service 覆盖范围的企业应用程序和/或零售应用程序在线交互而生成的事件数据，或者客户可以通过后端 API 交付方式接收事件数据。

此云服务包含对一个应用程序的保护。对于每个额外应用程序，客户应获取 IBM Trusteer Pinpoint Criminal Detection Additional Applications 的权利。

1.2.10 IBM Trusteer Rapport Remediation for Retail 和/或 IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail 和 IBM Trusteer Rapport Remediation for Business 旨在调查、补救、阻止并移除客户的合格参与者的受感染设备 (PC/MAC) 受到的浏览器中间人 (MitB) 恶意软件感染，这些合格参与者临时访问客户的零售应用程序，并且 IBM Trusteer Pinpoint Malware Detection 事件数据已在其中检测到 MitB 恶意软件感染。客户必须具有实际运行于客户应用程序上的 IBM Trusteer Pinpoint Malware Detection II 的当前订购。客户只能将此云服务产品提供给访问客户应用程序的合格参与者使用，并且只能将其作为一种工具，专门用于临时调查和补救受感染的特定设备 (PC/MAC)。IBM Trusteer Rapport Remediation 必须实际在此类受感染的合格参与者设备 (PC/MAC) 上运行，此类受影响的合格参与者必须接受 EULA、至少一次通过客户应用程序的认证，并且客户的配置必须包含用户标识的集合。为避免疑问，此云服务服务产品不包含使用“Trusteer 启动”和/或以任何其他方式向客户的常规合格参与者人群推广“帐户持有者客户端软件”的权利。对于本服务描述，“帐户持有者”表示客户的最终用户，该用户已安装客户端支持的软件，已接受最终用户许可协议（“EULA”），并在客户订购了云服务覆盖范围的零售应用程序或企业应用程序中，至少已认证一次。“帐户持有者客户端软件”表示 IBM Trusteer Rapport 客户端支持的软件，或随某些云服务提供的任何其他客户端支持的软件，用于安装在最终用户的设备上。

1.2.11 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail 和/或 IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- 对于 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail，第一个应用程序之外的任何其他零售应用程序的部署都需要获取 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail 权利。
- 对于 IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business 或 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business，第一个应用程序之外的任何其他企业应用程序的部署都需要获取 IBM Trusteer Pinpoint Malware Detection Additional Applications for Business 的权利。

1.2.12 IBM Trusteer Rapport for Mitigation for Retail 和/或 IBM Trusteer Rapport for Mitigation for Business

- IBM Trusteer Rapport for Mitigation for Retail 旨在调查、补救、阻止并移除客户的合格参与者的受感染设备 (PC/MAC) 受到的恶意软件感染，这些合格参与者临时访问客户的零售应用程序，并且 IBM Trusteer Pinpoint Detect Premium 或 IBM Trusteer Pinpoint Detect Standard 事件数据已在其中检测到恶意软件感染。客户必须具有实际运行于客户的零售应用上的 IBM Trusteer Pinpoint Detect

Premium 或 IBM Trusteer Pinpoint Detect Standard 的当前订购。客户只能将此云服务与访问客户的零售应用程序的合格参与者结合使用，并且只能作为旨在专门用于临时调查和补救特定受感染设备 (PC/MAC) 的工具。IBM Trusteer Rapport for Mitigation for Retail 必须实际在此类受感染的合格参与者设备 (PC/MAC) 上运行，此类受影响的合格参与者必须接受 EULA、至少通过一次客户零售应用的认证，并且客户的配置必须包含用户标识的集合。为避免疑问，此云服务不包含使用“Trusteer 启动”和/或以任何其他方式向客户的常规合格参与者人群推广“帐户持有者客户端软件”的权利。

- IBM Trusteer Rapport for Mitigation for Business 旨在调查、补救、阻止并移除客户的合格参与者的受感染设备 (PC/MAC) 受到的恶意软件感染，这些合格参与者临时访问客户的企业应用程序，并且 IBM Trusteer Pinpoint Detect Premium 或 IBM Trusteer Pinpoint Detect Standard 事件数据已在其中检测到恶意软件感染。客户必须具有实际运行于客户的业务应用程序上的 IBM Trusteer Pinpoint Detect Premium 或 IBM Trusteer Pinpoint Detect Standard 的当前订购。客户只能将此云服务用于访问客户的业务应用程序的合格参与者，并且只能作为临时调查和补救特定受感染设备 (PC/MAC) 的工具使用。IBM Trusteer Rapport for Mitigation for Business 必须实际在此类受感染的合格参与者设备 (PC/MAC) 上运行，此类受影响的合格参与者必须接受 EULA、至少通过一次客户的企业应用程序的认证，并且客户的配置必须包含用户标识的集合。为避免疑问，此云服务不包含使用“Trusteer 启动”和/或以任何其他方式向客户的常规合格参与者人群推广“帐户持有者客户端软件”的权利。

1.2.13 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail 和/或 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business

- 对于 IBM Trusteer Pinpoint Detect Standard for Retail，第一个应用程序之外的任何其他零售应用程序的部署都需要获取 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail 的权利。
- 对于 IBM Trusteer Pinpoint Detect Standard for Business，第一个应用程序之外的任何其他企业应用程序的部署都需要获取 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business 的权利。

1.2.14 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail 和/或 IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

此服务包括为每个应用程序提供多达 200 小时的共享资源以进行部署服务，以及每个应用程序 200 小时的共享资源以对设置进行安全分析。正在进行的服务包括每个应用程序每年 20 小时的部署维护，以及每个应用程序每年 100 小时的安全研究。

- 对 IBM Trusteer Pinpoint Premium for Retail，第一个应用程序之外的任何其他零售应用程序上的部署都需要获取 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail 的权利。
- 对于 IBM Trusteer Pinpoint Premium for Business，第一个应用程序之外的任何其他企业应用程序上的部署都需要获取 IBM Trusteer Pinpoint Detect Premium Additional Applications for Business 的权利。

1.2.15 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support 和/或 IBM Trusteer Pinpoint Detect Standard for Business Premium Support

购买 Pinpoint Detect Standard Cloud Service 的客户可以购买 Premium Support 服务。Premium Support 服务范围列在下面第 4 部分。

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

在订购此云服务之前，客户必须具有 IBM Trusteer Pinpoint Detect 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，增强了 IBM Trusteer Pinpoint Detect，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。

1.3 加速服务

1.3.1 IBM Trusteer Pinpoint Detect Standard Redeployment 和/或 IBM Trusteer Pinpoint Detect Premium Redeployment

如果客户在服务期限内重新部署在线银行应用程序并因此要求更改 IBM Trusteer Pinpoint Detect 部署时，那么应购买 IBM Trusteer Pinpoint Detect Redeployment。

重新部署可以是由于客户更改应用程序的域或主机 URL，将在线应用程序转换为新技术，移至新的在线银行平台，或者向现有应用程序添加新的登录流。

对于 6 个月的重新部署过渡期，授权客户在已订购的应用程序上运行额外的应用程序，比例为一比一。

1.3.2 IBM Trusteer Pinpoint Malware Detection Redeployment

如果客户在服务期限内重新部署在线银行应用程序并因此要求更改 IBM Trusteer Pinpoint Malware Detection II 部署时，那么应购买 IBM Trusteer Pinpoint Malware Detection Redeployment。

重新部署可以是由于客户更改应用程序的域或主机 URL，将在线应用程序转换为新技术，移至新的在线银行平台，或者向现有应用程序添加新的登录流。

对于 6 个月的重新部署过渡期，授权客户在已订购的应用程序上运行额外的应用程序，比例为一比一。

适用于 IBM Trusteer Pinpoint Malware Detection II Standard Edition 或 IBM Trusteer Pinpoint Malware Detection II Advanced Edition 的 IBM Trusteer Pinpoint Malware Detection Additional Applications，第一个应用程序之外的任何其他应用程序上的部署都需要获取 IBM Trusteer Pinpoint Malware Detection Additional Applications 的权利。

1.3.3 IBM Trusteer Pinpoint Criminal Detection Redeployment

如果客户在服务期限内重新部署在线银行应用程序并因此要求更改 IBM Trusteer Pinpoint Criminal Detection Cloud Service 部署时，那么应购买 IBM Trusteer Pinpoint Criminal Detection Redeployment。

重新部署可以是由于客户更改应用程序的域或主机 URL，将在线应用程序转换为新技术，移至新的在线银行平台，或者向现有应用程序添加新的登录流。

对于 6 个月的重新部署过渡期，授权客户在已订购的应用程序上运行额外的应用程序，比例为一比一。

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 5.2 节（附加处理位置信息）。

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

IBM Trusteer Rapport

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402483908375

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。

金牌支持：

可通过额外收费向云服务提供金牌支持订购，其中包括：

- 针对所有严重性的全天候支持。
- 客户可以通过电话或回拨请求直接联系支持人员。
- 按软件即服务 [SaaS] 支持手册中详细描述的过程，客户及其合格参与者可以通过电子方式提交支持凭单。
- 客户可以访问位于以下地址的客户支持门户网站以获取通知、文档、案例报告和常见问题及解答：http://www.ibm.com/software/security/trusteer/support/。

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：

- 互动是与云服务相关的专业或培训服务。
- “合格参与者”是指每个符合条件参与云服务所管理或跟踪的任何服务交付计划的个人或实体。
    - 有效用户是可通过任何方式和途径，直接或间接（例如：通过多路复用程序、设备或应用程序服务器）访问云服务的唯一用户。
- 对于 IBM Trusteer Pinpoint Detect Bundle，有效用户是指在过去 12 个月内（在指定时间之前）通过任何方式至少访问一次云服务的唯一个人。
- 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。
- API 调用是通过可编程接口调用云服务。

- 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。

4.2 远程服务费用

无论是否使用远程服务，远程服务都将在购买之日起 90 天后到期。

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 用于处理数据主体数据的 EULA 和基础

对于 IBM Trusteer Rapport Cloud Services（在与 Pinpoint Cloud Services 一起部署时，包括 Rapport Remediation 或 Rapport for Mitigation）：除非另有约定，否则客户将按照自己独立制定的处理方式来授权 IBM 提供“最终用户许可协议”（可从以下地址获取：https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA），以便 IBM 能够收集和处理提供云服务所需的信息。

对于 IBM Trusteer Rapport Cloud Services，客户授权 IBM 作为“发起企业”的数据处理机构，使用本程序来收集恶意软件和恶意软件工件，即与恶意活动相关的文件或与非常规程序故障相关的文件。IBM 不会使用本程序将包含最终用户个人信息的文件作为收集目标，但所收集的文件可能包含恶意软件在未经最终用户许可的情况下获取的个人数据。IBM 将 1) 立即删除与此类分析无关的任何文件；以及 2) 仅在分析期间保留相关文件，并且在任何情况下保留时间都不应超过三个月。

5.2 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。

5.3 帐户持有者数据

为澄清起见，如果存在多个与特定”帐户持有者“的”帐户持有者客户端软件”关联的 IBM 客户（此类 IBM 客户称为“关联客户”），且此服务描述下的服务由 IBM 通过其他区域的数据中心提供给此类关联客户，那么帐户持有者的数据可按上述第 5.2 节中的规定，在与每个此类数据中心关联的所有位置进行处理。

5.4 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。

5.5 支持软件

云服务包含以下支持软件：

- IBM Rapport Agents

5.6 Pinpoint 最佳实践

在恶意软件检测或帐户接管检测时，客户必须遵循“Pinpoint 最佳实践指南”。在进行恶意软件或帐户接管检测后，请勿立即采用会对合格参与者的体验产生影响的任何方式使用 IBM Trusteer Pinpoint Detect Cloud Service，否则将使他人能够将客户的操作与 IBM Trusteer Pinpoint Detect 服务产品的使用联系起来（例如，进行恶意软件或帐户接管检测后立即发送通知、发送消息、阻止设备或者阻止访问企业和/或零售应用）。

5.7 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。