

IBM Security Trusteer Fraud Protection

使用条款 (“ToU”) 由 IBM 使用条款 - 特定于 SaaS 的服务产品条款 (“特定于 SaaS 的服务产品条款”) 以及标题为“IBM 使用条款 - 通用条款 (“通用条款”)”组成, 可通过以下 URL 获得:

<http://www.ibm.com/software/sla/slabd.nsf/sla/tou-gen-terms/>。

如果发生冲突, 那么这些“特定于 SaaS 的服务产品条款”优先于“通用条款”。订购、访问或使用 IBM SaaS, 即表示客户同意此 ToU。

此 ToU 受适用的“IBM Passport Advantage 国际协议”、“IBM Passport Advantage Express 国际协议”或“针对所选的 IBM SaaS 产品的 IBM 国际协议” (“协议”) 的管辖, 这些协议与此 ToU 构成完整的协议。

1. IBM SaaS

以下 IBM SaaS 服务产品受这些“特定于 SaaS 的服务产品条款”的约束:

1.1 Rapport IBM SaaS 服务产品

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 Pinpoint IBM SaaS 服务产品

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 Mobile IBM SaaS 服务产品

- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Business
- IBM Security Trusteer Mobile Browser for Business Premium Support
- IBM Security Trusteer Mobile Browser for Retail
- IBM Security Trusteer Mobile Browser for Retail Premium Support

2. 收费标准

IBM SaaS 根据交易文档中指定的以下收费标准之一出售：

- 合格参与者** - 获取 IBM SaaS 时所采用的一种计量单位。每个符合条件参与 IBM SaaS 所管理或跟踪的任何服务交付计划的个人或实体都称为一个“合格参与者”。必须获得足够的权利，以便涵盖在客户的“交易文档”中所规定的评估期间，在 IBM SaaS 内管理或跟踪的所有合格参与者。

由 IBM SaaS 管理的每个服务交付计划均单独进行分析，然后添加在一起。有资格享受多项服务交付计划的个人或实体需要获得单独的授权。

对于这些服务产品，服务交付计划包含客户的单一企业应用程序或零售应用程序，每个应用程序都具有一个主登录页面和若干相关页面。合格参与者是客户的最终用户，他们持有企业应用程序或零售应用程序的登录凭证。

- 客户端设备** - 获取 IBM SaaS 时所采用的一种计量单位。“客户端设备”指单个用户计算设备或特殊用途的传感器或遥测设备，该设备向另一个通过称作服务器或由服务器管理的计算机系统，请求执行一系列命令、过程或应用程序或接收执行的结果，或向其提供数据。多个客户端设备可以共享对一台公共服务器的访问。客户端设备可以具有某些处理能力或者可进行编程以允许用户进行工作。客户必须获取在客户的交易文档中指定的评估期间运行、提供数据、使用提供的服务或访问 IBM SaaS 的每个客户机设备的权利。

3. 费用和计费

IBM SaaS 的应付金额在交易文档中进行说明。

3.1 部分月度费用

交易文档中指定的部分月度费用可按比例进行评估。

4. 合规性与审计

对 IBM Security Trusteer Fraud Protection 服务产品的访问受到交易文档中指定的合格参与者或客户设备最大数量的限制。客户负责确保合格参与者或客户设备的数量不超过“交易文档”中规定的最大数量。

可能需要审计验证是否符合合格参与者或客户设备最大数量要求。

5. IBM SaaS 订购周期续约选项

客户的“交易文档”通过指定以下某一项，规定 IBM SaaS 在订购周期结束时是否续约：

5.1 自动续约

如果客户的“交易文档”规定客户续约自动进行，那么客户可以通过在“交易文档”中规定的到期日期前至少 90 天，以书面方式向客户的 IBM 销售代表或 IBM 业务合作伙伴提出请求，终止即将到期的 IBM SaaS 订购周期。如果 IBM 或 IBM 业务合作伙伴在到期日期前未收到此类终止通知，那么到期订购周期将按照交易文档中的规定自动续约 1 年或与原始订购周期相同。

5.2 持续计费

当“交易文档”规定客户的续约连续进行时，客户可以继续访问 IBM SaaS，并持续收到有关使用 IBM SaaS 的账单。要终止使用 IBM SaaS 并停止持续计费过程，客户必须提前 90 天向 IBM 或 IBM 业务合作伙伴提供请求取消其 IBM SaaS 的书面通知。在取消客户访问之后，将在取消生效月份就未支付的访问费用向客户开具账单。

5.3 需要续约

当“交易文档”规定客户续约类型为“终止”时，IBM SaaS 将在订购周期结束时终止，并且将取消客户对 IBM SaaS 的访问权。要在结束日期之后继续使用 IBM SaaS，客户需要通过客户的 IBM 销售代表或 IBM 业务合作伙伴下订单，以购买新的订购周期。

6. 技术支持

客户及其合格参与者可获得有关 IBM SaaS 的技术支持，以帮助他们使用 IBM SaaS。

在所有服务产品的订购中均包含标准支持。Trusteer Rapport Mandatory Service 是 Trusteer Rapport 的附加组件，其先决条件是对 Trusteer Rapport 基本订购的金牌支持。

对于每一种 IBM SaaS 服务产品，可通过额外收费提供金牌支持订购，IBM Security Trusteer Mobile SDK 服务产品和 IBM Security Trusteer Rapport Mandatory Service 服务产品除外。

标准支持：

- 上午 8 点到下午 5 点本地时间支持。
- 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-01.ibm.com/software/security/trusteer/support/>。
- 要获取支持选项和详细信息，请访问 IBM 软件即服务 [SaaS] 支持手册：<http://www-01.ibm.com/software/support/handbook.html>。

金牌支持：

- 针对所有严重性的全天候支持。
- 客户可以通过电话直接联系支持人员。
- 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-01.ibm.com/software/security/trusteer/support/>。
- 要获取支持选项和详细信息，请访问 IBM 软件即服务 [SaaS] 支持手册：<http://www-01.ibm.com/software/support/handbook.html>。

7. IBM SaaS 产品附加条款

7.1 安全港合规性

IBM 遵守美国商务部与欧盟委员会合作制定的“美国 - 欧盟安全港框架”。IBM Security Trusteer 产品都包含在 IBM 的“欧盟 - 美国安全港”证书中。有关“安全港”和“安全港”公司名单的更多信息，可在以下网址中找到：<http://export.gov/safeharbor/>。

7.2 客户订购年费增加

IBM 保留调整 IBM SaaS 订购费用的权利，调整频率每十二 (12) 个月不超过一次，百分比由 IBM 确定但不超过 3%。订购费用调整将于初始启动覆盖时段日期满一年时生效。此费用调整不会改变客户的 IBM SaaS 权利或者获取 IBM SaaS 的收费标准。IBM 业务合作伙伴独立于 IBM，单独制定其价格和条款。

7.3 金牌支持

只有当客户已订购金牌支持服务后，才能获得相关 IBM SaaS 服务产品的金牌支持。

7.4 合法使用和同意

收集和处理数据的权限

IBM SaaS 旨在帮助客户改进其安全环境和数据。IBM SaaS 将收集有关合格参与者和客户设备的信息，这些参与者和客户设备将与客户已订购了 IBM SaaS 服务产品覆盖范围的企业应用程序或零售应用程序进行互动。IBM SaaS 收集的信息在某些管辖区域可以单独与其他信息一起被视为个人数据。“个人数据”是可用于识别特定个人的任何信息，例如，提供给 IBM 以代表客户进行存储、处理或传输的姓名、电子邮件地址、家庭住址或电话号码。

数据收集和处理实践可更新以改进 IBM SaaS 的功能。根据需要，将更新包含数据收集和处理实践的完整描述的文档并根据客户请求提供给客户。客户授权 IBM 按照本 ToU 的“跨境传输”部分和“数据隐私”部分以及“ToU 一般条款”的“数据隐私和数据安全”部分，收集并处理这些信息。

对于 IBM Security Trusteer Pinpoint 服务产品：

收集的数据可能包含用户的 IP 地址、加密的或单向散列形式的用户 ID、未过滤的域 Cookie、对受保护的应用程序和钓鱼站点的访问、地理位置以及输入到钓鱼站点的凭证。

对于 IBM Security Trusteer Mobile SDK 服务产品和 IBM Security Trusteer Mobile Browser 服务产品：

收集的数据可能包含用户的 IP 地址、加密的或单向散列形式的用户 ID、地理位置、对受保护应用程序的访问、SIM 卡信息、设备名称以及客户附属关系。

对于 IBM Security Trusteer Rapport 服务产品：

收集的数据可能包括用户 IP 地址、加密或单向散列的用户标识、安全事件、为联系 IBM 以获取客户支持而提供的用户名和电子邮件地址、客户附属关系、在受保护的站点上输入的加密密码、对受保护的应用程序和钓鱼站点的访问、加密的支付卡号以及由 IBM 人员远程收集用于检测可疑恶意软件、恶意活动或故障的文件和数据。

来自数据主题的同意书：

对 IBM SaaS 的使用可能涉及不同的法律或法规。IBM SaaS 只可出于合法目的、采用合法方式使用。客户同意按照规定使用 IBM SaaS，并承担所有责任，遵守适用的法律、法规和政策。

对于 IBM Security Trusteer Pinpoint 服务产品和 IBM Security Trusteer Mobile SDK 服务产品：

客户同意已获得或者将获得合法使用 IBM SaaS 和允许 IBM 通过 IBM SaaS 收集并处理信息所需的任何完整的同意书、准许或许可。

对于 IBM Security Trusteer Rapport 服务产品和 IBM Security Trusteer Mobile Browser 服务产品：

客户授权 IBM 获取合法使用 IBM SaaS 以及按照“最终用户许可协议”(<https://www.trusteer.com/support/end-user-license-agreement>) 中的规定收集和处理信息所需的完整同意书。如果客户确定自己（而非 IBM）将与最终用户就同意事宜进行沟通，那么客户同意自己已获得或者将获得合法使用 IBM SaaS 和允许 IBM 作为客户的数据处理机构通过 IBM SaaS 收集并处理信息所需的任何完整同意书、准许或许可。

7.5 跨境传输

客户同意，IBM 可以按照相关法律和要求，将内容（包括任何个人数据）跨国家或地区传输到欧洲经济区以外的下列国家或地区以及被欧盟委员会视为具有足够安全性级别的国家或地区中的处理机构和分支处理机构：美国。

7.6 数据隐私

如果客户将个人数据提供给欧盟成员国、冰岛、列支敦士登、挪威或瑞士境内的 IBM SaaS，或者，如果客户的合格参与者或客户设备位于这些国家或地区中，那么客户作为唯一控制者，指派 IBM 作为处理机构，按照欧盟指令 95/46/EC 中的条款处理这些个人数据。IBM 将仅在根据 IBM 发布的 IBM SaaS 描述提供 IBM SaaS 服务产品所需的范围内处理此类个人数据；并且客户同意，任何此类处理均符合客户的指令。如果 IBM 在执行 IBM SaaS 的过程中，对处理位置或保护个人数据的方式作出重大更改，那么 IBM 将提前发出合理的通知。客户可以在 IBM 向客户发出更改通知后的三十 (30) 天内，向 IBM 发出书面通知，终止受影响的 IBM SaaS 的当前订购期。客户同意，IBM 可以将内容（包括个人数据）跨国家或地区传输到以下处理机构或分支处理机构：

| 处理机构/分支处理机构的名称 | 角色（数据处理机构或分支处理机构） | 位置* |
|-------------------------|-------------------|--|
| IBM 签约实体 | 处理机构 | 按交易文档中所述 |
| Amazon Web Services LLC | 分支处理机构 | 410 Terry Ave. N Seattle, WA 98109 United States |
| Connectria Corp. | 分支处理机构 | 10845 Olive Blvd., Suite 300 St. Louis, MO 63141 United States |
| IBM Israel Ltd. | 分支处理机构 | 94 Derech Em-Hamoshavot 49527 Petach-Tikva 以色列 |
| IBM Corp | 分支处理机构 | 1 New Orchard Rd. Armonk, NY 10504 United States |

客户同意 IBM 在合理决定有必要提供 IBM SaaS 时，在事先通知的情况下，对此国家或地区位置列表进行更改。

客户同意，对于在配置过程中确定的通过德国数据中心提供的服务，IBM 可以将内容（包括个人数据）跨国家或地区传输到以下处理机构或分支处理机构：

| 处理机构/分支处理机构的名称 | 角色（数据处理机构或分支处理机构） | 位置* |
|-------------------------|-------------------|--|
| IBM 签约实体 | 处理机构 | 按交易文档中所述 |
| Amazon Web Services（德国） | 分支处理机构 | 德国，慕尼黑 |
| IBM Israel Ltd. | 分支处理机构 | 94 Derech Em-Hamoshavot 49527 Petach-Tikva 以色列 |

客户同意，对于在配置过程中确定的通过日本数据中心提供的服务，IBM 可以将内容（包括个人数据）跨国家或地区传输到以下处理机构或分支处理机构：

| 处理机构/分支处理机构的名称 | 角色（数据处理机构或分支处理机构） | 位置* |
|-------------------------|-------------------|--|
| IBM 签约实体 | 处理机构 | 按交易文档中所述 |
| Amazon Web Services（日本） | 分支处理机构 | 日本，东京 |
| IBM Israel Ltd. | 分支处理机构 | 94 Derech Em-Hamoshavot 49527 Petach-Tikva 以色列 |

* 上表中标识的位置包括处理机构/分支处理机构的企业办公地址。数据中心位于所标识的同一国家或地区中。

各方或其相关的关联公司可根据 EC 决议 2010/87/EU（可选条款已移除）单独签署有关各自角色的未经修改的标准欧盟模型条款协议。即使是由关联公司签订的协议，这些协议下所产生的争议或责任都将被各方视为由于此协议条款产生的争议或责任。

附录 A

1. IBM SaaS 服务产品

IBM 提供这些服务作为独立的服务和产品，或者作为附加的服务和产品。在客户的 PoE 中指定了订购的具体 IBM SaaS 服务产品。

1.1 企业和零售定义

许可 IBM Security Trusteer Fraud 产品与特定类型的应用程序配合使用。应用程序定义为如下类型之一：零售或企业。针对零售应用程序和企业应用程序提供独立的服务产品。

- 零售应用程序定义为旨在为消费者提供服务的在线银行应用程序、移动应用程序或电子商务应用程序。客户策略可将某些小型企业分类为有资格访问零售应用程序。
- 企业应用程序定义为旨在为企业、机构或同等实体提供服务的在线银行应用程序、移动应用程序或电子商务应用程序，或者未分类为零售应用程序的任何应用程序。

1.2 IBM SaaS 基本订购服务产品

企业服务产品：

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

零售服务产品：

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

对于每一种企业和零售服务产品，可通过额外收费提供关联的金牌支持产品，IBM Security Trusteer Mobile SDK 服务产品除外。

1.3 针对 IBM Security Trusteer Rapport 服务产品的附加 IBM SaaS 订购服务产品

针对 IBM Security Trusteer Rapport for Business 提供的附加服务产品：

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Mandatory Service for Business

针对 IBM Security Trusteer Rapport for Retail 提供的附加服务产品：

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

对于 IBM Security Trusteer Rapport 服务产品的每个企业和零售附加组件（IBM Security Trusteer Rapport Mandatory Service 附加组件除外），可通过额外收费提供关联的金牌支持产品。

IBM Security Trusteer Rapport for Business 或 IBM Security Trusteer Rapport for Retail 的订购是本节中所列的关联的附加 IBM SaaS 订购服务产品的先决条件。

1.4 针对 IBM Security Trusteer Pinpoint Malware Detection 服务产品的附加 IBM SaaS 订购服务产品

针对 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 或 IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 提供的额外服务产品：

- IBM Security Trusteer Pinpoint Carbon Copy for Business

针对 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 或 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 提供的额外服务产品：

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

针对本节中所列的每一种附加 IBM SaaS 服务产品，可通过额外收费获取金牌支持订购。

对 IBM Security Trusteer Pinpoint Malware Detection for Business 服务产品或 IBM Security Trusteer Pinpoint Malware Detection for Retail 服务产品的订购是本节中所列的关联的附加 IBM SaaS 订购服务产品的先决条件。

1.5 其他附加 IBM SaaS 订购

针对以上基本订购的任何附加 IBM SaaS 订购，如果未在此处列出，那么无论当前可用的订购或者正在开发中的订购均不被视为更新并且必须单独授权。

1.6 定义

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 IBM SaaS 服务产品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 Security Trusteer Rapport 客户端支持的软件或者 IBM Security Trusteer Mobile Browser 客户端支持的软件，或随某些 IBM SaaS 订购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。

Trusteer 启动 - 表示基于可用启动模板提供给客户的启动。

登录页面 - 表示随客户启动和可下载的“帐户持有者客户端软件”一起提供给客户的 IBM 托管的页面。

2. IBM Security Trusteer Rapport 服务产品

2.1 IBM Security Trusteer Rapport for Retail 和/或 IBM Security Trusteer Rapport for Business (“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 Security 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 Security 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算法。

此 IBM SaaS 服务产品具有合格参与者收费标准。企业服务产品打包出售，每 10 个合格参与者为一包。零售服务产品打包出售，每 100 个合格参与者为一包。

此 IBM SaaS 服务产品包括：

a. Trusteer Management Application (“TMA”)：

TMA 在 IBM Security Trusteer 云托管环境中提供，通过 TMA，客户（以及数量不限的授权人员）可以：(i) 接收事件数据报告和风险评估，(ii) 查看、配置和设置与事件数据报告相关的策略，以及 (iii) 查看客户端支持的软件的配置，此类软件根据最终用户许可协议（“EULA”）免费许可给公众使用，并且可下载到合格参与者的桌面或设备 (PC/MAC) 上，也称为 Trusteer Rapport 软件套件（“帐户持有者客户端软件”）。客户只能使用“Trusteer 启动”或 Rapport API 推销“帐户持有者客户端软件”，并且客户不得将“帐户持有者客户端软件”用于内部业务运营或者供自己的员工使用（员工个人使用除外）。

b. Web 脚本:

适用于旨在访问或使用 IBM SaaS 服务产品的 Web 站点访问。

c. 事件数据:

客户（以及数量不限的授权人员）可以使用 TMA，接收由于“帐户持有者”与客户订购了 IBM SaaS 服务产品覆盖范围的企业应用程序或零售应用程序在线交互，而从“帐户持有者客户端软件”生成的事件数据。将从以下合格参与者的设备上运行的“帐户持有者客户端软件”接收事件数据：已接受 EULA、已至少通过一次客户的企业应用程序或零售应用程序的认证，并且客户的配置必须包含用户标识的集合。

d. Trusteer 启动:

“Trusteer 启动”市场营销平台可以向访问客户订购了 IBM SaaS 服务产品覆盖范围的企业应用程序和/或零售应用程序的合格参与者标识或推销“帐户持有者客户端软件”。客户可以从可用“启动模板”中进行选择。可根据独立协议或工作声明签订定制启动的合同。

客户可以同意提供自己的商标、徽标或图标，以便与 TMA 结合使用，并且仅用于“Trusteer 启动”，显示在“帐户持有者客户端软件”或 IBM 托管的登录页面以及 IBM Security Trusteer Web 站点上。对其提供的商标、徽标或图标的任何使用都将遵循 IBM 有关广告和商标使用的合理策略。

如果客户希望采用任何类型的“帐户持有者客户端软件”强制部署，那么客户必须订购 IBM Security Trusteer Rapport Mandatory Service SaaS 服务产品。

“帐户持有者客户端软件”的强制部署包含但不限于以下任何类型的强制部署：直接或间接强制要求合格参与者下载“帐户持有者客户端软件”的任何机制或方式，或者并非由 IBM 创建或核准，用于为绕过“帐户持有者客户端软件”的这项强制部署的许可要求而采取的任何方法、工具、程序、协议或机制。

2.2 针对 IBM Security Trusteer Rapport for Business 和/或 IBM Security Trusteer Rapport for Retail 的可选附加 IBM SaaS 服务产品

IBM Security Trusteer Rapport 服务产品的订购是订购以下任何附加 IBM SaaS 服务产品的先决条件。如果将 IBM SaaS 指定为“用于企业”，那么获取的附加 IBM SaaS 服务产品也必须指定为“用于企业”。如果将 IBM SaaS 指定为“用于零售”，那么获取的附加 IBM SaaS 服务产品也必须指定为“用于零售”。客户将从以下运行“帐户持有者客户端软件”的合格参与者接收事件数据：已接受 EULA、已至少通过一次客户的企业应用程序和/或零售应用程序的认证，并且客户的配置必须包含用户标识的集合。

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business 和/或 IBM Security Trusteer Rapport Fraud Feeds for Retail

客户（及其数量不限的授权人员）可以使用 TMA 来接收有关恶意软件感染以及特定“帐户持有者”的桌面上其他端点漏洞的事件数据。

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business 和/或 IBM Security Trusteer Rapport Phishing Protection for Retail

客户（及其数量不限的授权人员）可以使用 TMA 来接收有关将“帐户持有者”的登录凭证提交至可疑钓鱼或潜在欺诈站点的事件数据通知。合法的在线应用程序 (URL) 可能被错误标记为钓鱼站点，IBM SaaS 可能警告“帐户持有者”某个合法站点是一个钓鱼站点。在此类事件中，客户必须将此类错误通知 IBM，IBM 将纠正错误。客户应单独承担补救此类错误的责任。

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business 和/或 IBM Security Trusteer Rapport Mandatory Service for Retail

客户可以使用“Trusteer 启动”市场营销平台的实例强制访问客户订购了 IBM SaaS 服务产品覆盖范围的企业应用程序或零售应用程序的合格参与者下载“帐户持有者客户端软件”。

IBM Security Trusteer Rapport Premium Support for Business 是 IBM Security Rapport Mandatory Service for Business 的先决条件。

IBM Security Trusteer Rapport Premium Support for Retail 是 IBM Security Rapport Mandatory Service for Retail 的先决条件。

仅当订购了 IBM Security Trusteer Rapport Mandatory Service 的其他功能，并配置为与客户订购了 IBM SaaS 服务产品覆盖范围的企业应用程序或零售应用程序一起使用时，客户才能实施此类其他功能。

3. IBM Security Trusteer Pinpoint 服务产品

IBM Security 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 IBM SaaS 服务产品覆盖范围的企业应用程序和/或零售应用程序以及防欺诈流程中。

此 IBM SaaS 服务产品包括：

a. TMA:

TMA 在 IBM Security Trusteer 云托管环境中提供，通过 TMA，客户（以及数量不限的授权人员）可以：(i) 接收事件数据报告和风险评估，并且 (ii) 查看、配置和设置安全策略以及与事件数据报告相关的策略。

b. Web 脚本和/或 API:

适用于旨在访问或使用 IBM SaaS 的 Web 站点部署。

3.1 IBM Security Trusteer Pinpoint Malware Detection 和 IBM Security Trusteer Pinpoint Criminal Detection

在 IBM Security Trusteer Pinpoint Malware Detection 服务产品中进行恶意软件检测，或者在 IBM Security Trusteer Pinpoint Criminal Detection 服务产品中进行帐户接管检测时，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 Security Trusteer Pinpoint Malware Detection 服务产品或 IBM Security Trusteer Pinpoint Criminal Detection 服务产品，否则将使他人能够将客户的操作与 IBM Security Trusteer Pinpoint 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/或零售应用程序）。

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business 和/或 IBM Security 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 Security Trusteer Pinpoint Criminal Detection 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（以及数量不限的授权人员）可以使用 TMA，接收由于合格参与者与客户订购了 IBM SaaS 服务产品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。

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile 和/或 IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) 服务产品旨在提供另一层保护，通过识别罪犯帐户访问并向客户提供建议，防止帐户接管和欺诈活动。此 IBM SaaS 服务产品使用 PPCD Mobile API 收集来自客户的企业和/或零售应用程序的信息，以及来自合格参与者的移动设备的信息。IBM Security Trusteer PPCD Mobile 服务产品旨在将与合格参与者的移动设备有关的信息与其他数据源（例如，通过本 ToU 中指定的 IBM Security Trusteer 的其他 IBM SaaS 服务产品集成的实时恶意软件感染和网络钓鱼事件）进行关联。

客户可以在 IBM Security Trusteer 的云托管环境中访问和使用 IBM Security Trusteer PPCD Mobile 服务产品，接收来自合格参与者的移动设备的风险评估数据，这些数据是由于移动设备与客户订购了 IBM SaaS 服务产品覆盖范围的企业应用程序或零售应用程序在线交互而生成的。对于这些服务产品，“移动设备”仅包括受支持的手机和平板电脑，不包括 PC 或 MAC。

3.1.3 **IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 和/或 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 和/或 IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 和/或 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition**

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 Security Trusteer Pinpoint Malware Detection 服务产品可提供另一层保护，通过为客户提供针对 MitB 金融恶意软件的评估和警报，帮助企业关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与客户的企业的程序和/或零售应用程序在线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:

针对企业或零售的 Standard Edition 是快速部署解决方案，可提供此处所述的 IBM SaaS 服务产品的核心功能。

3.2 **针对 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 和/或 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 和/或 IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 和/或 IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 的可选附加 IBM SaaS 服务产品**

对于 IBM Security Trusteer Rapport Remediation for Retail 服务产品，IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 或 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 是先决条件。

对于 IBM Security Trusteer Pinpoint Carbon Copy for Retail，IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition 或 IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition 是先决条件。对于 IBM Security Trusteer Pinpoint Carbon Copy for Business，IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition 或 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition 是先决条件。

3.2.1 **IBM Security Trusteer Pinpoint Carbon Copy for Business 和/或 IBM Security Trusteer Pinpoint Carbon Copy for Retail**

IBM Security Trusteer Pinpoint Carbon Copy 服务产品旨在提供另一层保护以及监视服务，帮助客户及时发现因为客户订购了 IBM SaaS 服务产品覆盖范围的企业应用程序或零售应用程序遭受网络钓鱼攻击，而导致合格参与者的凭证受到威胁。

3.2.2 **IBM Security Trusteer Rapport Remediation for Retail**

IBM Security Trusteer Rapport Remediation 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 Security 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 IBM Security Trusteer Pinpoint Malware Detection 的当前订购，并且实际运行于客户的零售应用程序上。客户只能将此 IBM SaaS 服务产品与访问客户零售应用程序的合格参与者结合使用，并且只能作为一种工具，专门用于临时调查和补救受感染的特定设备 (PC/MAC)。IBM Security Trusteer Rapport Remediation 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 IBM SaaS 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一般合格参与者人群推广“帐户持有者客户端软件”的权利。

4. IBM Security Trusteer Mobile 服务产品

4.1 IBM Security Trusteer Mobile Browser for Business 和/或 IBM Security Trusteer Mobile Browser for Retail

IBM Security Trusteer Mobile Browser 旨在提供另一层保护，确保合格参与者的移动设备能够安全地在线访问客户订购了 IBM SaaS 服务产品覆盖范围的企业应用程序或零售应用程序。仅针对 Android 平台提供安全的 Wi-Fi 检测。对于本 IBM SaaS 产品，其中包含移动设备（包括移动手机或平板电脑），不包含笔记本电脑和 Mac。

通过 TMA，客户（以及数量不限的授权人员）可以接收与设备相关的事件数据、分析和统计信息，前提是拥有这些设备的合格参与者已：(i) 下载了“帐户持有者客户端软件”，此应用程序根据最终用户许可协议（“EULA”）免费许可给公众使用，并且可下载到合格参与者的移动设备上，(ii) 接受了 EULA，并至少在客户订购了 IBM SaaS 服务产品覆盖范围的企业应用程序或零售应用程序中进行过一次认证。客户只能使用“Trusteer 启动”营销“帐户持有者客户端软件”，不得将“帐户持有者客户端软件”用于内部业务运营。

a. 事件数据：

客户（以及数量不限的授权人员）可以使用 TMA，接收由于移动设备与客户订购了 IBM SaaS 服务产品覆盖范围的企业应用程序或零售应用程序在线交互而生成的事件数据。

b. Trusteer 启动：

“Trusteer 启动”市场营销平台可以向访问客户订购了 IBM SaaS 服务产品覆盖范围的企业应用程序和/或零售应用程序的合格参与者标识或推销“帐户持有者客户端软件”。客户可以从可用启动模板（“启动模板”）中进行选择。可根据独立协议或工作声明签订定制启动的合同。

客户可以同意提供自己的商标、徽标或图标，以便与 TMA 结合使用，并且仅用于“Trusteer 启动”，显示在“帐户持有者客户端软件”或 IBM 托管的登录页面以及 IBM Security Trusteer Web 站点上。对其提供的商标、徽标或图标的任何使用都将遵循 IBM 有关广告和商标使用的合理策略。

4.2 IBM Security Trusteer Mobile SDK for Business 和/或 IBM Security Trusteer Mobile SDK for Retail

IBM Security Trusteer Mobile SDK 服务产品旨在提供另一层保护，为客户订购了 IBM SaaS 服务产品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 Security Trusteer Mobile SDK 服务产品包含专有的移动软件开发工具箱（“SDK”）；包含文档、专有编程软件库和其他相关文件与项目的软件包，称为 IBM Security Trusteer 移动库以及“运行时组件”或“可再分发版”；以及由 IBM Security Trusteer Mobile SDK 生成的专有代码，可嵌入并集成到客户订购了 IBM SaaS 服务产品覆盖范围的受保护独立 iOS 或 Android 移动应用程序中。

IBM Security Trusteer Mobile SDK for Retail 按每包 100 个合格参与者或每包 100 个客户设备提供，IBM Security Trusteer Mobile SDK for Business 按每包 10 个合格参与者或每包 10 个客户设备提供。

通过 TMA，客户（以及数量不限的授权人员）可以接收事件数据报告和风险趋势评估。通过“客户集成的移动应用”，客户可以接收与已下载“客户集成的移动应用”的合格参与者的移动设备相关的风险分析和移动设备信息，从而使客户能够制定欺诈预防策略，采取行动以实施这些风险。对于本服务产品，“移动设备”仅包括受支持的手机和平板电脑，不包括 PC 或 MAC。

客户可以：

- a. 在内部使用 IBM Security 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 ToU 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。

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，可以安装和使用“可再分发版”和 IBM Security Mobile SDK 仅用于支持客户使用 IBM SaaS 服务产品。

IBM 已测试了使用 IBM 程序中提供的 IBM Security Trusteer Mobile SDK (“移动工具”) 创建的样本应用程序，以确定这些应用程序在来自 Apple (iOS) 和 Google (Android) 等的移动操作系统平台（统称“移动操作系统平台”) 的某些版本上是否正常执行，但由第三方提供的移动操作系统平台不在 IBM 控制范围内，并且可能随时发生更改，而不会预先通知 IBM。因此，无论是否存在任何相反的声明，IBM 都不保证使用“移动工具”创建的任何应用程序和其他输出都将在任何移动操作系统平台或移动设备上正常执行、与之互操作或者与之兼容。

客户同意创建、保留并向 IBM 及其审计员提供准确书面记录、系统工具输出以及其他系统信息，以可审计的方式充分证明客户对 IBM Security Trusteer Mobile SDK 的使用符合此 ToU 条款。

5. IBM SaaS Fraud Protection 服务产品的部署

客户的基本订购包含所需的设置和初始部署活动，包括初始一次性启动、配置、启动模板、测试和培训。

可根据独立协议通过支付额外费用签订附加服务合同。

附录 B

IBM 为 IBM SaaS 提供了以下可用性服务级别协议 (SLA)，如果在客户的交易文档中规定了该 SLA，那么它就适用：

本 SLA 是在客户订购开始时或续订时适用的最新版本。客户了解本 SLA 并不构成对客户的保证。

1. 定义

- a. **授权联系人** - 指客户向 IBM 指定的授权其根据本 SLA 提出索赔的个人。
- b. **可用性积分** - 指 IBM 针对经验证的索赔将提供的补救措施。可用性积分将以针对 IBM SaaS 的将来订购费用的发票的贷记金额或折扣形式应用。
- c. **索赔** - 表示由客户的授权联系人根据本 SLA 向 IBM 提交的索赔，其内容为在约定的月份内未达到约定的服务级别。
- d. **约定的月份** - 表示在 IBM SaaS 期限内的每个完整月份，度量方式为从格林威治标准时间当月第一天凌晨 00:00 起至当月最后一天 23:59 止。
- e. **客户** - 表示直接从 IBM 订购 IBM SaaS 的实体，根据其与 IBM 签订的 IBM SaaS 合同，不存在任何重大违约行为，包括付款义务。
- f. **停机时间** - 表示该服务的生产系统处理停止，并且客户的所有用户均无法使用具有相应许可权的服务的所有方面的时间段。停机时间不包含服务由于以下原因而不可用的时间段：
 - 计划内系统停机时间；
 - 不可抗力；
 - 由于客户或第三方应用程序、设备或数据而导致的问题；
 - 客户或第三方的行为或疏忽（包括通过使用客户的密码或设备获取 IBM SaaS 访问权的任何人）；
 - 未能遵守访问 IBM SaaS 所需的系统配置及未使用受支持的平台；或
 - IBM 遵守客户或代表客户的第三方提供的任何设计、规范或指令。
- g. **事件** - 表示导致无法满足服务级别的某种或某一系列同时发生的状况。
- h. **不可抗力** - 表示自然因素、恐怖袭击、罢工、火灾、洪水、地震、骚乱、战争、政府行为、命令或限制、病毒、拒绝服务攻击及其他恶意行为、公用事业和网络连接故障或任何 IBM 合理控制范围之外导致的 IBM SaaS 不可用的其他因素。
- i. **计划内的系统停机时间** - 表示出于系统维护目的而安排的 IBM SaaS 中断。
- j. **服务级别** - 表示以下所述标准，IBM 根据此标准来衡量其在本 SLA 中所提供服务的级别。

2. 可用性积分

- a. 为获取提交索赔的资格，客户必须根据 IBM 报告 1 级严重性支持问题的程序，针对适用的 IBM SaaS，通过 IBM 客户支持帮助中心对各项事件记录支持凭单。客户必须提供有关该事件的所有必要的详细信息，并在合理范围内根据 1 级严重性支持凭单的要求帮助 IBM 诊断并解决该事件。此类凭单必须在客户首次发现事件影响客户使用 IBM SaaS 的二十四 (24) 个小时内进行记录。
- b. 客户的授权联系人必须在受索赔的“约定的月份”结束后的三 (3) 个工作日内，针对可用性积分提交客户的“索赔”。
- c. 客户的授权联系人必须就该“索赔”向 IBM 提供所有合理的详细信息，包括但不限于对所有相关事件的详细描述，以及声明未达成的服务级别。
- d. IBM 将在内部计算适用于下表中所示的对应服务级别的每个“约定的月份”内的停机时间总和。可用性积分将基于停机时间计算，该停机时间从客户报告首次受停机时间影响时开始计算。如果客户报告同时发生“应用程序停机时间”事件和“入站数据处理停机时间”事件，那么 IBM 会将重叠的停机时间长度

视为一个停机时间长度，而不是两个单独的停机时间长度。对于每一项有效的索赔，IBM 会根据每个“约定的月份”内达到的服务级别应用可适用的最高可用性积分，如下表中所示。IBM 不负责对于同一个“约定的月份”内的相同事件适用多个可用性积分。

- e. 对于“捆绑服务”（打包并以单一组合价格一起销售的单项 IBM SaaS），可用性积分的计算将基于“捆绑服务”的每月单一组合价格，而非基于每个单项 IBM SaaS 的每月订购费用。在任何“约定的月份”内，客户只能针对捆绑服务中的一个单项 IBM SaaS 提出相关索赔，IBM 不负责适用任何“约定的月份”内捆绑服务中的多项 IBM SaaS 有关的可用性积分。
- f. 如果客户通过转售交易（IBM 在此交易中对履行 IBM SaaS 及 SLA 承诺承担主要责任）从有效的 IBM 经销商购买 IBM SaaS，那么可用性积分的计算将基于当时针对受索赔的“约定的月份”期间所提供 IBM SaaS 的有效“关系建议合理价 (RSVP)”，适用折扣费率为 50%。
- g. 针对任何“约定的月份”奖励的可用性积分总额，在任何情况下均不应超过客户向 IBM 支付的年度 IBM SaaS 费用的十二分之一 (1/12) 的百分之十 (10%)。
- h. IBM 将基于 IBM 记录中可用的信息，使用合理的判断来对索赔加以验证，如果与客户记录中的数据存在冲突，那么将以 IBM 的记录为准。
- i. 根据本 SLA 向客户提供的可用性积分是客户针对任何索赔获取的唯一且全部的补救措施。

3. 服务级别

约定月份内的 IBM SaaS 可用性

| 实现的服务级别 (在“约定的月份”期间) | 可用性积分 (受索赔的“约定的月份”的每月订购费用的百分比) |
|-------------------------|-----------------------------------|
| < 99.5% | 2% |
| < 98.0% | 5% |
| < 96.0% | 10% |

“已达成的服务级别”（以百分比形式表示）计算方法为：**(a)**“约定的月份”内总分钟数减去**(b)**“约定的月份”内停机时间的总分钟数，再除以**(c)**“约定的月份”内总分钟数。

示例：约定的月份内停机时间总计 250 分钟

| | |
|---|-------------------------------------|
| 30 天的“约定的月份”内总计 43,200 分钟 - 停机时间 250 分钟 = 42,950 分钟 <hr style="width: 50%; margin: 0 auto;"/> 总时间 43,200 分钟 | = 2% 可用性积分，在约定的月份内实现 99.4% 已达成的服务级别 |
|---|-------------------------------------|

3.1 除外条款

本 SLA 仅适用于 IBM 客户。本 SLA 不适用于：

- 测试版和试用版服务。
- 非生产环境，包括但不限于测试、灾难恢复、质量保证或开发环境。
- 由 IBM 客户的用户、访客、参与者以及 IBM SaaS 的获准受邀者提出的索赔。
- 如果客户违反本 ToU 中的任何主要义务，包括但不限于违反任何付款义务。