IBM Application Security on Cloud

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/sladb.nsf/sla/tou-gen-terms/。

如果上述条款存在冲突，则“特定于 SaaS 的服务产品条款”优先于“常规条款”。客户订购、访问或使用 IBM SaaS，即表示同意本 ToU。

本 ToU 由适用的“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”）约束，这些协议与此 ToU 构成完整的协议。

1. IBM SaaS

以下 IBM SaaS 服务产品遵循“特定于 SaaS 服务产品的条款”：

- IBM Application Security Analyzer
- IBM Application Security Analyzer Per Scan
- IBM Application Security Analyzer Premium

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：

a. **作业** - 获取 IBM SaaS 时所采用的一种计量单位。“作业”是 IBM SaaS 内部不能进一步分割的对象，表示包含其所有子过程的计算过程。客户必须获得足够的权利，以涵盖客户的权利证明（PoE）或交易文档中指定的衡量期间 IBM SaaS 所处理或管理的作业总数。

b. **应用程序实例** - 获取 IBM SaaS 时所采用的一种计量单位。连接到 IBM SaaS 的应用程序的每一个实例都需要一份应用程序实例权利。如果应用程序包含多个组件，每个组件都为不同的目的和/或用户群提供服务，并且每个组件都可连接到 IBM SaaS 或由 IBM SaaS 进行管理，那么每个此类组件都被视为一个单独的应用程序。此外，应用程序的测试、开发、登台和生产环境均被认为是应用程序的单独实例，每个实例都必须获得一份权利。单一环境中的多个应用程序实例中的每一个均被认为是应用程序的单独实例，每个实例都必须获得一份权利。客户必须获取足够的权利，以涵盖客户的权利证明 (PoE) 或交易文档中规定的评估期间连接到 IBM SaaS 的应用程序实例的数量。

c. **实例** 是获得 IBM SaaS 时所使用的一种计量单位。一个实例是指对 IBM SaaS 一项具体配置的访问权。客户必须获取足够的权利以涵盖客户的权利证明 (PoE) 或交易文件中所规定的评估期间可供访问和使用的所有 IBM SaaS 实例。

对于每份实例权利，执行的作业或应用程序实例（连接的应用程序）的数量并没有限制，但是，在任意给定时间内，同时运行的作业不得超过 30 个。

3. 费用和账单

IBM SaaS 的应付金额在交易文件中规定。

3.1 按使用付费

如果按照交易文档中规定的价格使用服务，那么将在下个月采用“按使用付费”选项开具发票。

3.2 未满一个月的收费标准

根据交易文件的规定，使用未满一个月的将按比例收取费用。

4. 期限和续约选项

IBM SaaS 期限自 IBM 通知客户可访问 PoE 中记录的 IBM SaaS 之日算起。PoE 将指定 IBM SaaS 是自动续订、在持续使用基础上继续，还是在期限结束时终止。

对于自动续订，除非客户在期限到期日期之前，至少提前 90 天发出不再续约的书面通知，否则将按照 PoE 中指定的期限对 IBM SaaS 自动续订。

对于持续使用，在客户提前 90 天发出终止书面通知之前，IBM SaaS 将以月为单位继续有效。IBM SaaS 的有效期将于 90 天期限过后的日历月末终止。

5. 技术支持

在订购周期内，当 IBM 通知客户可以访问 IBM SaaS 之后，将通过在线论坛提供技术支持，并作为客户产生“按使用付费”费用期间的标准支持。在 IBM SaaS 中，客户可以提交支持凭单或打开交谈会话以获取支持。IBM 将提供《IBM 软件即服务支持手册》，其中提供了技术支持联系信息以及其他信息和流程。

严重性	严重性定义	响应时间目标	响应时间覆盖
1	**关键业务影响/服务停止：** 业务关键功能无法运行或关键接口已故障。这通常适用于生产环境，并且表示无法访问服务从而对运营产生重大影响。这一情况需要立刻解决。	1 小时内	全天候
2	**严重业务影响：** 服务的一项业务功能或特性的使用严重受限，或您正面临不能按时完成业务任务的危险。	2 个工作小时内	周一到周五的工作时间
3	**轻微业务影响：** 表明服务或功能还可使用，不会对运营产生关键影响。	4 个工作小时内	周一到周五的工作时间
4	**最小业务影响：** 咨询或非技术请求	1 个工作日内	周一到周五的工作时间

5.1 访问客户数据

IBM 将仅出于诊断服务问题和便于服务扫描应用程序的目的而访问客户数据。IBM 将仅出于纠正缺陷或为 IBM 产品或服务提供支持之目的访问数据。

6. IBM SaaS 服务产品其他条款

安全扫描可能不会发现应用程序中的所有安全风险。

IBM SaaS 可用于帮助客户满足基于法律、法规、标准或实践的合规性义务的要求。 该服务提供的任何指示、建议用法或指南并未包含法律、财务或其他专业建议，提醒客户获取自己的法律顾问或其他专家顾问建议。客户自行负责确保客户及其活动、应用程序和系统遵守所有适用的法律、法规、标准和实践。对本服务的使用并不能保证遵循任何法律、法规、标准或实践。

IBM SaaS 在 Web 站点上执行入侵性和非入侵性测试，Web 或移动应用程序客户选择进行扫描，从而测试某些固有风险，包括但不限于以下：

a. 客户的计算机系统在测试状态下运行应用程序时可能暂挂或崩溃，导致系统暂时不可用或数据丢失；

b. 客户系统的性能和吞吐量以及相关联的路由器和防火墙的性能和吞吐量可能在测试期间暂时降级；

c. 可能生成过多日志消息，导致耗费过多的日志文件磁盘空间；

d. 探测漏洞可能导致数据被更改或删除；

e. 入侵检测系统可能触发警报；

f. 所测试 Web 应用程序的电子邮件功能可能触发电子邮件；

g. IBM SaaS 可能在查找事件时阻断受监控网络的流量。

为防止客户将所测试应用程序的已认证登录凭证输入到服务中，客户只能针对测试帐户（而不是生产用户）输入此类凭证。使用生产用户凭证可能导致个人数据通过本服务传输。

可以配置 IBM SaaS 以扫描生产 Web 应用程序。当客户将扫描类型设置为“生产”时，服务旨在以降低上述风险的方式执行扫描；但是，在特定情况下，IBM SaaS 可能会导致测试的生产站点和基础结构性能下降或不稳定。IBM 对于使用 IBM SaaS 扫描时生产站点的适用性无任何保证或表示。

客户需自行承担责任，决定本服务是否适用于客户的 Web 站点、Web 应用程序、移动应用程序或技术环境及其安全性。

IBM SaaS 旨在识别移动和 Web 应用程序以及 Web 服务中的各种潜在安全和合规性问题。它不会测试所有漏洞或合规性风险，也不能阻止安全攻击。安全威胁、法规和标准不断变化，本服务可能不会反应所有此类变化。客户需自行承担其 Web 应用程序、系统和员工的安全性和合规性责任，并采取任何补救措施。客户自行决定是否使用本服务提供的任何信息。

某些法律禁止在未经授权的情况下尝试进入或访问计算机系统。客户需负责确保不使用本服务扫描任何客户所有及客户有权扫描的 Web 站点和/或应用程序之外的 Web 站点和/或应用程序。

6.2 Cookies

客户知晓并同意，作为 IBM SaaS 正常运行和支持的一部分，IBM 可向客户（您的员工和承包商）通过跟踪和其他技术收集有关 IBM SaaS 使用的个人信息。IBM 公司以此收集有关 IBM SaaS 的使用统计信息和有效性信息，旨在改善用户体验和/或定制与客户的交互。客户确认其将取得或已取得同意，允许 IBM 在遵守适用法律的情况下，在 IBM、其他 IBM 公司及其承包商内部处理收集到的个人信息用于上述目的，无论我们和我们的承包商在何处开展业务。IBM 将履行客户的员工和承包商访问、更新、纠正或删除所收集的个人信息的请求。

6.3 派生的收益地点

基于客户指定为接收 IBM SaaS 获益的场所缴纳税款（如果适用）。除非客户向 IBM 提供其他信息，否则 IBM 将基于订购 IBM SaaS 时列为主要获益场所的业务地址适用税项。客户负责确保此类信息保持最新状态，并向 IBM 提供任何更新。

附录 A

1. IBM Application Security on Cloud 一般说明

IBM Application Security on Cloud 提供单个场所以帮助客户发现各个应用程序的安全漏洞（例如，SQL 注入、跨站点脚本编制和数据泄漏）。服务包括各种类型的应用程序安全扫描技术，其中每个都发现此应用程序中的安全问题。

IBM Application Security on Cloud 提供以下功能：

- 扫描移动应用程序以查找安全漏洞。通过动态（黑盒）和交互式（白盒）安全分析技术来完成。
- 扫描生产或预生产面向公众或专用网络上的 Web 站点以查找安全漏洞。通过动态（黑盒）安全分析技术来完成。
- 扫描 Web 和桌面应用程序中的数据流以查找安全漏洞。通过静态（白盒）安全分析技术来完成。
- 详细的安全漏洞报告，其中包含发现以及开发人员可采用的补救步骤的高级摘要。
- 集成各种 DevOps 平台