

IBM QRadar Advisor with Watson

本“服务描述”介绍 IBM 向客户提供的服务。客户表示公司、公司授权用户或 Cloud Service 接收方。提供适用的“报价”和“权利证明”(PoE) 作为独立的交易文档。

1. Cloud Service

1.1 IBM QRadar Advisor with Watson Service

IBM QRadar Advisor with Watson 将认知分析功能扩展到 QRadar Security Platform，帮助客户和安全分析师快速调查和应对威胁。它利用 Watson for Cyber Security 的知识语料库，深入挖掘非结构化数据（包括安全网站、博客和研究报告等），并与本地安全事件关联。因此，它有助于揭示隐藏的威胁，自动获取洞察，从而进行快速响应，提高决策水平。QRadar Advisor with Watson 使安全分析师能够向 Watson 发送安全攻击信息，让 Watson 利用其包含成千上万个结构化和非结构化数据源的知识库，执行威胁发现操作，从而追溯到与原始安全攻击相关的威胁实体，例如恶意文件、可疑 IP 地址、恶意实体以及它们之间的关系。这在确定安全攻击是否与已知的恶意活动相关方面特别有效。如果事实果真如此，Watson 会提供与恶意软件有关的背景资料、被攻击的漏洞、威胁的范围（包括可能影响的其他端点）以及其他洞察。

此 Cloud Service 要求客户部署一个活动的 IBM Security QRadar，并在该部署上安装此 Cloud Service 的支持代码，以便客户可以使用它的功能。此 Cloud Service 包含对安全攻击查询数量的“软限制”，也就是在客户授权范围内，客户可以按每天每秒每 1000 个事件向 Cloud Service 发送十五 (15) 个查询。超出此限制而发送的查询数量，也将由 Cloud Service 进行处理，但是优先级会降低，而且返回速度变慢。

1.2 IBM QRadar Advisor with Watson Trial

IBM QRadar Advisor with Watson Trial (“Trial Cloud Service”) 以试用形式提供 IBM QRadar Advisor with Watson 的功能。客户对“Trial Cloud Service”的访问最高可达到交易文档或其他文档中规定的时间长度，该时间结束，客户的访问权限也将终止。此外，客户在试用期内，每天只能发送最多 5 个安全攻击查询。Trial Cloud Service 不提供保证，仅“按现状”提供，客户只能将其用于内部测试和非生产环境。根据当前流量水平的不同，在试用期间查询的响应时间也各不相同。

2. 安全描述

此 Cloud Service 遵循 <http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp> 中提供的针对 IBM SaaS 的 IBM 数据安全和隐私原则，以及本部分中提供的任何其他条款。对于 IBM 数据安全和隐私原则的任何更改都不会降低 Cloud Service 的安全性。

如果客户（作为数据控制者）确定技术和组织安全措施适合于处理过程带来的风险以及要保护的数据的性质，那么可以使用此 Cloud Service 来处理选择的包含个人数据的内容。客户承认此 Cloud Service 不提供相关功能用于保护个人敏感数据或受其他法规需求约束的数据。客户确认 IBM 并不了解内容中包含的数据类型，并且无法对 Cloud Service 或已实施的安全保护的适用性进行评估。

Cloud Service 只允许客户输入和管理以下内容，其中一些内容可能是适用隐私法律所规定的个人信息 (PI):

- 目标/源 IP 地址
- URL
- 域
- 文件散列

2.1 安全特性和责任

Cloud Service 实施以下安全特性:

此 Cloud Service 会在 IBM 网络与客户的 IBM Security QRadar 部署之间传输数据时对内容进行加密。在处于静止状态以等待数据传输时，Cloud Service 不加密内容。

Cloud Service 在对数据执行功能之后，不会保留或永久存储输入的内容。

3. 技术支持

针对 Cloud Service 的技术支持通过电子邮件、在线论坛和在线问题报告系统来提供，如下所述。技术支持随附于 Cloud Service，不作为独立产品提供。

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对运营产生重大影响。这一情况需要立刻解决。	1 小时内	24x7 方式
2	严重业务影响： 服务特性或服务功能在使用中受到严重限制，或者客户可能错过业务截止期限。	在 2 个工作小时之内	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。	在 1 个工作日之内	周一到周五的工作时间

对于参与 Cloud Service beta 测试并仍在使用 QRadar Platform V7.2.7 的客户，一些技术支持问题可能无法得到解决，此类客户需要升级到 V7.2.8 并安装最新版本的修补程序，以便能够获得全面的技术支持。

4. 权利和计费信息

4.1 收费标准

Cloud Service 根据交易文档中指定的收费标准提供：

- a. **每秒 100 起事件** - 获取 Cloud Service 时所采用的一种计量单位。一起事件是指出现一次通过使用 Cloud Service 处理或者与使用 IBM SaaS 相关的特定事件。客户必须获取足够的权利以涵盖权利证明 (PoE) 或交易文档中指定的评估期间的每秒事件数量（四舍五入至最接近的整百数）。

5. 期限和续约选项

Cloud Service 期限自 IBM 通知客户可访问 PoE 中记录的 Cloud Service 之日算起。PoE 将指定 Cloud Service 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 天发出不再续订的书面通知，否则将按照 PoE 中指定的期限对 Cloud Service 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，Cloud Service 将以月为单位继续有效。Cloud Service 的有效期将于 90 天期限过后的日历月末终止。

6. 支持软件

Cloud Service 需要使用客户下载至客户系统的支持软件，以方便 Cloud Service 使用。客户仅可在与 Cloud Service 的使用关联的情况下使用支持软件。支持软件是“按现状”提供的。

客户可以从地址为 <https://exchange.xforce.ibmcloud.com/hub> 的 IBM Security App Exchange 站点下载 Cloud Service 的支持软件。

7. 附加条款

7.1 通用条款

客户同意 IBM 可在宣传或市场营销中将客户公开为 Cloud Services 的订户。

7.2 支持软件

Cloud Service 需要使用客户下载至客户系统的支持软件，以方便 Cloud Service 使用。客户仅可在与 Cloud Service 的使用关联的情况下使用支持软件。支持软件是“按现状”提供的。

客户可以从地址为 <https://exchange.xforce.ibmcloud.com/hub> 的 IBM Security App Exchange 站点下载 Cloud Service 的支持软件。

7.3 Cloud Service 的合法使用

Cloud Service 旨在帮助客户改进其安全环境和数据。对 Cloud Service 的使用可能涉及不同的法律或法规，包括与隐私、数据保护、雇佣、电子通信和存储相关的法律法规。Cloud Service 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 Cloud Service，并承担所有责任，遵守适用的法律、法规和政策。客户声明，自己将获取或已经获取合法使用 Cloud Service 所需的任何同意书、权限或许可。

7.4 Cloud Service 到期

在 Cloud Service 到期或终止之前，客户可以使用 Cloud Service 提供的任何报告或导出功能来抽取数据。

7.5 安全性数据

作为 Cloud Service（包括报告活动）的一部分，IBM 将准备并维护从 Cloud Service 收集的去标识化的信息和/或汇总信息（“安全性数据”）。“安全性数据”将不会识别客户或个人，以下 (d) 中提供内容除外。客户在此同意 IBM 只能出于以下目的使用和/或复制“安全性数据”：

- a. 发布和/或分发“安全性数据”（例如，与网络安全相关的编译和/或分析中）；
- b. 开发或增强产品或服务；
- c. 开展内部研究或与第三方一起开展研究；以及
- d. 合法共享已确认的第三方罪犯信息。