SaaS模式下，企业用户无需维护系统，只需登录就可以享受系统功能带来的便利。但是SaaS服务和数据部署在云端而不是本地机房，可能存在不可控问题。

企业用户最关注的是自己的数据能不能得到有效的保护。

本文整理了10个必问的SaaS安全问题，包括基础安全，应用安全，安全合规、数据安全、安全责任划分等方面，可以快速了解SaaS厂商的安全能力。

1、SaaS软件的部署方式？

A、是否支持私有化(本地)部署？

本地化的安全系数相较于SaaS会更高，如果是企业核心数据的系统，安全性要求较高，不希望这些核心数据由第三方来负责，可以选择SaaS私有化部署。

B、SaaS平台部署在私有云，还是公有云？

选择SaaS平台，需考虑托管平台的基础保障能力和安全防护能力甚至包括云平台服务商的安全资质。
公有云平台与普通的IDC机房相比，具有高可用性、安全性和弹性的优势。
建议优选AWS、阿里云、腾讯云和华为云等主流云平台。

2、SaaS平台有哪些资质?

第三方资质认证作为一个参考指标，应包含云平台服务商和云租户SaaS厂商，云平台的安全能力并不等同于SaaS应用的安全能力，平台提供的是基础能力，系统自身需具备保障安全的能力。

比如：ISO27001体系认证、等级保护认证、GDPR认证等。
通过了ISO27001的认证，表示企业的信息安全管理已建立了一套科学有效的管理体系作为保障。
通过了等级保护备案测评，意味着系统已具备相应等级的基本安全保护能力。

3、SaaS平台现有的安全防护措施有哪些？

SaaS平台应具备一定的安全防护能力，需配备相应的安全产品/服务。
比如运维审计（堡垒机）、应用防护（WAF）、访问控制（防火墙）、入侵防御（HIDS/EDR）。

4、SaaS平台是否会定期的进行渗透测试？

定期渗透测试，并出具相关安全厂商/服务商的安全检测报告。
比如：专业的安全公司的渗透检测报告或可靠的众测服务平台的安全众测报告。

5、数据在存储和传输时是如何加密的，以及数据变现和数据销毁问题?

传输加密：SSL加密
数据类型：数据库、文件附件
相关方式，如：数据加解密/文件加密解密服务、图片转成二进制流加密存储、OSS服务端加密、RDS透明数据加密TDE、云盘加密、DLP、硬件加密机等

确认数据变现和数据销毁问题？
虽然SaaS用户的数据存放在SaaS厂商的数据中心，但数据的所有权是归用户所有。SaaS厂商未经用户同意，不得对使用数据，更不得售卖数据。SaaS厂商有责任确保用户的数据安全，并对数据泄露、数据丢失造成的用户损失要进行经济赔偿。
需要确认的两点：不针对客户数据变现、将没有必要保存的历史数据进行销毁。

6、SaaS多租户数据如何隔离？

SaaS基于多租户架构，多个租户共用一套实例，可能存在数据安全性问题；
SaaS多租户在数据存储上存在三种主要的方案，分别是：独立数据库、共享数据库（逻辑数据隔离、共享数据）。

7、SaaS平台如何实现系统容灾和高可用性？

高可用技术架构、数据备份策略、容灾切换方案。

8.SaaS应用可能涉及的安全合规问题？

重点关注，个人隐私保护、GDPR，以及爬虫、AI等技术的应用，可能带来一定的风险。

9.SaaS平台在身份验证、权限管理、日志审计方面分别是怎么做的？

身份验证机制，是否支持双因子认证，密码复杂度/登录失败处理/验证码/强制修改初始密码。
权限管理，基于角色的用户权限系统，对用户和角色进行授权。
日志审计，日志是否可以预警，敏感的业务操作日志，管理员无法删除/修改日志。

10、一旦出现数据泄露事件，责任如何划分？

目前，安全责任共担模式在业界已经达成共识，亚马逊AWS、微软Azure、阿里云、腾讯云均采用了与用户共担风险的安全策略。
用简单例子来看责任的划分：

A、应用系统的漏洞（应用安全）带来的安全事件
- 租户使用了SAAS服务，责任方在腾讯云平台（SAAS业务由平台方提供，由平台方负责管理）

B、用户弱密码，身份被盗用（数据安全），造成安全事件：
- 不管用户使用的是IASS,PAAS还是SAAS服务，用户身份和数据安全都由租户方管理负责


Bypass