API 安全治理

常见问题

产品文档

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

常见问题

最近更新时间：2022-09-05 10:20:02

API 安全治理是什么?

API 安全治理是一款针对 API 服务提供全生命周期管理与精细化安全防护的安全产品。能够帮助客户对 API 资产进行梳理，发现 API 漏洞和风险，识别和阻断 API 的攻击，降低重要数据资产的泄漏风险。

API 安全治理能够解决什么 API 安全问题?

支持解决如下几类 API 安全问题：

- 流量风险：对于异常的请求进行及时的告警和阻断。
- 入侵风险：智能识别 API 运行过程中的攻击入侵行为，识别 API 可能存在的漏洞。
- 业务风险：智能识别机器人爬虫，防止业务数据被恶意拖取；同时可对 API 进行规范化管理，避免因为研发规范缺失而导致的业务风险。
- 数据风险：根据 API 请求进行数据分析，找出 API 可能存在数据泄漏的情况。

API 安全治理是否依赖其他的组件?

API 安全治理可不依赖于其他的组件进行部署。其本身内置了 API 网关，可实现对 API 的全生命周期管理；同时 API 安全治理也支持与其他网关进行集成，支持与其他网关实现 API 安全管理能力。

本地部署模式下，API 安全治理管理系统对于服务器、存储、网络等资源有何具体要求?

一般需要根据客户实际业务场景和业务访问量来衡量服务器等资源需求，最小服务器资源投入数量不小于1台。

如何体验 API 安全治理管理系统?

可通过平台 申请咨询体验 API 安全治理管理系统，收到您的申请后，我们将进入审核阶段，并会在3-5个工作日内完成审核。申请审核通过之后，API 安全治理产品团队将与您联系，确认需求并进行商务洽谈。