

API 安全治理

常见问题

产品文档



腾讯云

【 版权声明 】

©2013–2023 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分內容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 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。