

暴露面管理服务

常见问题



腾讯云

【 版权声明 】

©2013–2024 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内容。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或 95716。

常见问题

最近更新时间：2024-03-21 14:17:51

什么是暴露面管理服务？

暴露面管理服务是一个主动的风险管理服务，旨在根据企业的授权、从攻击者视角出发，通过一系列工具对企业资产的暴露面及潜在威胁进行监测和清点，借助自动化入侵模拟等手段并进行风险实际验证，动态评估企业在数字和物理资产的可访问性、暴露面及可利用性，帮助企业降低漏洞利用风险，优化运营流程。

暴露面管理服务交付方式是什么？

服务期间，当监测发现重要暴露面威胁后，会人工组合暴露面风险要素形成攻击路径，并人工进行优先级分级，生成精准修复建议，当未监测到重大暴露面威胁时，会定期提供监测分析报告，报告监测项内容。

暴露面管理是否会影业务运行？

不会，暴露面管理数据部分来自于扫描，部分来自于第三方测绘引擎及互联网/暗网渠道数据，如涉及扫描动作，会在取得客户服务授权后，采取速率控制、扫描时间沟通等方式进行风险规避，不会影响业务正常运转。

暴露面管理服务必须购买安全产品吗？

不需要，暴露面管理服务依托腾讯云的安全服务平台暴露面识别引擎以及攻防团队服务能力，对安全产品无要求。

暴露面管理服务用到了哪些新技术？

不同环节会采用不同的技术能力，如在测绘引擎环节，为实现更快和更及时的发现能力，会在 T-SCAN 自研引擎的基础上，购买国内外第三方资产指纹库和引擎测绘数据，风险的优先级划分方面，会采用 VPT 评估方法对漏洞风险进行快速评级，在暴露面风险验证方面，会采用人工+BAS（入侵攻击模拟系统）进行暴露面和威胁的快速对抗验证。

暴露面管理服务与攻击面管理有什么区别？

暴露面管理服务与攻击面管理（以下简称 ASM）具备较大区别，主要体现在如下几个方面：

1. 交付形式：暴露面管理服务是一种安全服务，覆盖了相关能力和人工服务，攻击面管理则属于产品能力。
2. 主要功能：暴露面管理服务覆盖了对抗评估验证的能力和动员修复的能力，在识别相关外部风险数据后，同时会通过人工+自动化对抗验证等手段关联和验证发现的暴露面数据，形成真实有效的攻击路径，并在组织动员层面提供精准防护建议。
3. 目标定位：暴露面管理服务是通过安全工具平台+人工服务方式开展风险闭环管理，ASM 聚焦攻击者视角识别外部安全风险。

暴露面管理服务与漏洞扫描有什么区别？

暴露面管理服务是一种安全服务，漏洞扫描通常聚焦于资产的漏洞风险识别，基于已知漏洞库规则，其主要区别在于：

1. 持续性：暴露面管理服务具备持续性，可7*24小时进行持续监测，而漏洞扫描为单次或多次间隔扫描，不具备连续性。
2. 主要功能：漏洞扫描主要聚焦已知漏洞，不具备基线配置检查、云服务风险发现以及暗网数据泄露等相关能力，而暴露面管理服务包含了漏洞扫描及以上多个能力。
3. 目标定位：暴露面管理服务是一个更为闭环的风险管理方案，漏洞扫描是暴露面管理服务服务子能力或抓手之一。