安全专家服务

常见问题

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或95716。

文档目录

常见问题
渗透测试服务

最近更新时间：2026-07-10 15:02:31

计费相关

如何购买渗透测试服务?

进入 安全专家服务购买页，选择**渗透测试服务**，根据需要进行测试的应用或模块数量，选择资产测试类型，输入购买次数，单击**立即购买**完成购买即可。

渗透测试服务如何收费的?

渗透测试服务 PTS 收费标准，主要根据测试的应用及模块数量来测算，PTS 服务的测试类型可分为 Web/小程序/移动 App/桌面客户端文件四类，具体的计算方式可查阅 计费概述 。

产品功能

什么是渗透测试服务?

渗透测试服务是模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统安全做深入的探测，发现系统脆弱的环节。

渗透测试是不是相当于入侵系统?

不是，渗透测试和黑客入侵最大区别在于渗透测试是经过用户授权，采用可控制、非破坏性的方法和手段发现目标和网络设备中的弱点，帮助管理者知道自己网络所面临的问题。

渗透测试对业务系统有什么风险?

在测试过程中，无法避免会发生很多可预见和不可预见的风险，因此实施团队在测试之前会提供风险防范措施，以免对系统造成重大的影响，如：

- 尽量使用测试系统进行测试，而非直接在正式运行的系统上测试。
- 有风险的测试行为应在实施前与业务系统负责人进行沟通确认。
- 避免在业务高峰期进行测试。
- 测试过程出现异常情况时立即停止测试并及时恢复系统。

渗透测试服务会造成敏感数据泄露么?

不会，腾讯云渗透测试服务实施前会签署保密协议，对安全人员使用的设备和信息等严格管控，保证用户数据严格保密。

渗透测试服务发现的漏洞，如果用户方面修补不了，腾讯云是否会支持修补呢?

会提供相关支持，渗透结束后，会生成一个专业的测试报告交付给用户，报告中会为用户提供修补建议，如果最后发现漏洞仍然存在，腾讯云也会为用户进行人工答疑，协助用户修补漏洞。

一般渗透的周期是多久？

渗透测试，对于不同应用：如 Web、App、二进制文件，或不同数量的功能，整体周期不等，通常单个应用的测试周期不会超过10天。

在进行渗透作业之前，都会做哪些准备工作呢？

- 了解用户的系统网络架构。
- 明晰用户的网络安全强度。
- 对渗透目标进行确认。
- 询问用户是否做了信息备份。
- 对渗透辅助的工具进行选择。
- 对渗透作业的时间进行选择。
- 让用户签署渗透测试授权书。

渗透测试服务是否支持现场实施？

支持，腾讯云渗透测试服务一般对于内网是驻场实施，外网可以远程实施，如果用户要求驻场，也可以进行驻场实施但是价格也会相应增加。

渗透测试服务主要测试哪些应用？

渗透测试服务（Penetration Test Service，PTS）可以对 Web 应用系统、移动端的 iOS、Android、HarmonyOS 平台上 App、微信小程序、桌面的 Windows 及 macOS 的客户端展开测试。

渗透测试服务是否提供漏洞复测？

渗透测试服务（Penetration Test Service，PTS）对同一版本应用中已发现的漏洞免费提供三次回归测试，以确保漏洞完全修复。

服务实施

如何确保用户信息不外泄？

- 腾讯云有完善的信息安全服务防控体系。
- 腾讯云渗透测试服务实施前获取用户授权文件，签订保密协议。
- 对于内部系统安全则分别在主要出口处部署安全设备，从流量、文件、已知行为和未知行为等方面检测保密能力。

渗透测试是否存在风险？是否会对业务系统的运行产生影响？

渗透测试确实存在一定的操作风险，但正规的测试流程设计初衷就是在发现安全问题的同时，将业务影响降至最低。腾讯云渗透测试服务有相应的风险防范措施，在时间安排上，会将测试时间安排在非高峰期，不会对业务系统的连续性产生影响。

渗透测试服务是否用漏洞扫描服务来替代呢?

渗透测试的检测广度和深度是漏洞扫描无法覆盖的，可以发现漏洞扫描不涉及的业务逻辑漏洞以及高复杂性的漏洞挖掘如二次注入。
同时渗透测试服务除了定位漏洞外，还需要进一步尝试对漏洞进行攻击利用、提权以及维持对目标系统的控制权，而漏洞扫描是清楚地展示出系统中存在的所有缺陷，但不会衡量这些缺陷对系统造成的影响。

腾讯云渗透测试服务需要用户配合什么?

- 需要用户提供渗透测试的范围。
- 需要用户对渗透测试进行授权。
- 有时需要用户提供测试账号以及安全产品对测试 IP 加白名单。

漏洞扫描能达到实时监控的目的吗?

- 漏洞扫描跟实时监控是不一样的。
- 漏洞扫描可以进行周期性扫描，及时发现新的漏洞，提醒用户进行修复。

安全攻防对抗服务

最近更新时间：2026-07-10 15:02:30

什么是安全攻防对抗服务?

安全攻防对抗服务（Cybersecurity Attack-Defense Confrontation, CADC）基于腾讯安全专家能力及多年的攻防对抗经验构建。面向对安全能力有较高要求的企业用户，在用户授权后，通过模拟 APT 攻击的方式，对企业信息化资产以及可能产生危害的安全风险进行测试。通过多维度、多视角的安全攻防对抗，动态检测企业安全防护的整体水位。

做了渗透测试，还需要做安全攻防对抗吗?

渗透测试的检测维度较为单一，仅能检测所测试应用自身及承载服务器、组件的安全性。企业安全除应用安全外，可能还存在其他诸多隐患，这些是渗透测试无法覆盖的。而安全攻防对抗能够对这些风险面进行测试，检验企业整体安全防护能力。

安全攻防对抗与渗透测试的区别?

攻防演习与传统渗透测试存在明显的区别，主要区别在以下方面：

- **目的：**传统渗透测试是对业务系统自身开展安全检查与渗透性测试，核心目的是找到业务系统自身存在的可利用漏洞。攻防演习是在渗透测试的基础上，以获取目标系统的最高控制权为目标，目的是检验客户人机结合、协同处置等方面的综合防护能力。
- **人员配比：**渗透测试在实施中主要由渗透工程师完成，配备的人员比较单一。而在攻防演习过程中，一般以演习预期目标为导向，要求与渗透测试相比更为复杂，一般由不同技术背景人员来组成攻击小组。
- **侧重点：**渗透测试检验侧重点主要是渗透目标的安全性，是否存在可利用的安全漏洞。而在攻防演习过程中，检验的侧重点则是参演目标的安全性、参演单位的安全防护能力、参演单位的应急响应能力，更注重对参演单位整个网络安全体系的有效性检验。

安全攻防对抗可以对非腾讯云资产进行检测么?

安全攻防对抗服务可以对公有云、私有云、混合云、IDC 等多场景下的资产进行检测，但您需保证对所测试的资产具有合法权利、保证有权委托腾讯云对相关资产进行安全测试，且在测试正式开始前，您需出具授权函，允许腾讯云服务团队对您的所属资产进行攻防对抗测试。

安全攻防对抗的购买有什么限制么?

因安全攻防对抗服务测试的对象和范围较复杂，为保障安全攻防服务效果，本服务对攻击团队人员数量及演练周期时长限制了最小购买数量。攻击团队人员数量的最小购买数为3（人），演练周期时长的最小购买数量为5（天）。

重要时期安全保障服务

最近更新时间：2026-07-10 15:02:30

什么是重要时期安全保障服务?

重要时期安全保障服务（Cybersecurity in Important Period, CIP），在重大事件期间或法定节假日期间，为用户提供针对于云上资产的安全保障服务。整体服务周期包含保障前期的风险面探测、服务器协助加固，保障期间的安全设备监控、安全事件的应急响应处理，保障后期的整体过程复盘与提升。使用重要时期安全保障服务，高效发现并阻断安全事件，降低资产的网络攻击风险。

重要时期安全保障服务具备哪些安全能力?

重要时期安全保障服务提供了保障前期的安全评估、风险检测、风险处置、渗透测试，保障中期的漏洞感知与泄漏监测、安全监控、应急响应等能力，覆盖重要时期安全保障服务的各个关键阶段。

重要时期安全保障服务主要分析哪些安全事件?

重要时期安全保障服务主要分析安全产品的事件、产品安全策略配置事件、最新安全漏洞事件及数据泄露事件等。

重要时期安全保障服务有什么条件限制么?

建议在重要时期安全保障服务开始前至少五天完成购买，需要为安全评估以及加固预留时间。

在处置安全事件时，是否会告知风险或危害?

重要时期安全保障团队在重要时期安全保障服务前期会与用户明确在服务期间，各类安全事件的应急预案和处置办法。当处置操作可能会影响用户业务自身稳定性及可用性时，会与用户沟通并在取得用户同意后才会进行处理。

风险评估服务

最近更新时间：2026-07-10 15:02:30

什么是风险评估服务?

风险评估服务（Risk Assessment Services，RAS），是指腾讯云在客户授权后，结合工具及专家服务对用户业务进行安全风险发现，提供安全加固建议，提升整体安全能力。包含：云安全风险评估、暴露面风险评估、防御能力风险评估、安全检查等服务。

风险评估服务与暴露面服务有什么区别?

风险评估服务是一项综合性的安全风险评估服务，可针对不同的资产类型、风险类别及检测手段，结合企业实际需求开展全面或专项性风险评估。暴露面风险评估服务属于风险评估服务中的其中一种评测手段，主要是针对互联网业务进行资产测绘及风险测绘。

风险评估服务交付方式是什么?

风险评估服务主要通过远程服务交付，企业可根据自身安全需求，增购现场专家支持服务。

风险评估服务有什么条件限制吗?

风险评估服务中的云业务风险评估服务，需要客户业务部署在指定厂商的公有云上。另各项风险评估服务均需客户前置进行服务授权并提供必要服务调研信息，如评估单位主题、资产范围等，腾讯云方可合规地提供服务。

服务购买后，可以提供哪些增值服务?

可增值提供专家分析服务、安全加固指导服务、报告翻译服务、现场支持服务，完善不同客户不同需求的服务体验，详情请参见 购买指南 。

风险评估服务可以根据用户需求提供个性化服务吗?

可以，如防御能力检验服务可根据客户需求定制化安全验证的剧本。详情请咨询 腾讯云官网客服 或您的腾讯云客户经理。

风险评估服务是如何收费的?

采取预付费模式进行收费，详情请参见 计费概述 。

服务购买后，有相应的操作指导吗?

服务购买后，我们将线下提供服务交付标准和需配合的指导说明。

等级保护服务

最近更新时间：2025-11-06 11:18:31

等级保护服务如何收费?

腾讯云等级保护服务采用预付费模式，收费标准根据中国大陆不同地域、等保级别及交付形式而定。详情请参见 购买指南 。

等保测评服务（定制版）包含什么服务内容?

等保测评服务（定制版）包括定级、备案、测评对接、建设整改、监督审查，等保测评服务（定制版）将联合腾讯云网络安全合作生态，为客户提供本地化、系统化、专业的等级保护合规建设与测评咨询一站式服务。

为什么要做等保?

- 从法律要求层面来说，《中华人民共和国网络安全法》明确规定网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，如果拒不履行，将会受到相应处罚。
- 从行业要求层面来说，部分行业主管单位明确要求从业机构的信息系统要开展等保工作，例如金融、电力、广电、医疗、教育等行业。
- 从安全要求层面来说，信息系统运营、使用单位通过开展等保工作可以发现系统内部的安全隐患与不足之处，可通过安全整改提升系统的安全防护能力，降低被攻击的风险。

等级保护服务是否有区域或行业限制?

服务全国范围可用，不受地域限制，并支持政府、金融、医疗、教育、互联网等多行业需求。

等级保护服务如何定价?

通常根据系统数量、定级级别（如二级、三级）、服务地区、及服务内容（定制版服务或测评服务等）、服务形式（远程或现场）进行套餐式或定制化报价。

是否支持与其他安全服务组合使用?

支持与渗透测试、漏洞扫描、应急响应等服务组合，形成深度合规解决方案，提升整体安全水平。
注意：其他服务需额外购买。

等保服务是否包含等保合规安全产品?

服务不包括安全产品售卖，可参考 等保合规产品套餐方案 采用此方案选配的安全技术类产品，可使被测的业务系统在技术层面达到对应的等级保护的基本要求。

云租户还需单独再做等保?

根据 “ 谁运营谁负责，谁使用谁负责，谁主管谁负责 ” 的原则，系统的责任主体还是属于网络运营者自己，所以云租户还是得承担相应的网络安全责任。由于腾讯云平台本身就已经通过等保，所以在做等保的过程中，云租户无需再关注物理环境和网络环境，只需关注本身业务系统合规即可。

应急响应服务

最近更新时间：2026-07-10 15:02:30

计费相关

如何购买应急响应服务?

进入 安全专家服务购买页 ，选择应急响应服务，根据当前受灾资产数量，选择输入相应的资产数字，单击**立即购买**即可。

应急响应服务收费标准是?

应急响应服务 CIRS 收费标准，主要根据受影响的资产数量来测算。服务详细价格请参考如下表格：

受灾机器数量（台）	总体价格（元/次）
1-10	21,200
11-30	42,400
31-60	63,600
61-100	84,800
101-150	106,000
151-250	127,200
251-400	159,000
401-600	212,000
>600	请 联系我们 进行咨询

产品功能

机器被入侵了首先应该怎么做?

应及时关闭网络连接，保留现场，阻止损失扩散，必要时可寻求腾讯云安全专家应急响应服务的帮助。

机器上发现异常行为，但无法确认是否被入侵，可参考什么文档解决?

可参见 Windows 入侵类问题排查思路 或 Linux 入侵类问题排查思路 。

应急响应服务有什么特点吗?

腾讯云应急响应提供7 × 24小时远程处理服务，工作日1小时内响应、非工作日4小时内响应、服务结束后2-3个工作日内提交报告，及时地为用户解决问题，控制紧急事件的影响范围，尽量把用户损失最小化。

应急响应服务能处理哪些紧急事件?

一般的应急事件包括黑客攻击、病毒爆发、木马、后门程序、脱库、入侵事件、挂马等，此类问题腾讯云应急响应服务均可处理。

应急响应服务工具是否支持标准化的管理?

支持。应急响应服务的管理员将会记录：应用工具、工具的升级情况、升级前的版本、升级后的版本、新添加了哪些工具及其功能等信息。

安全托管服务

最近更新时间：2026-07-10 15:02:30

什么是安全托管服务?

安全托管服务（Managed Security Service，MSS）可为您提供持续且高效的安全监控和运营管理服务。通过安全托管服务，能够快速响应主机、网络、应用及数据等安全产品的各类安全风险事件，利用 SOAR 技术进行智能分类和高效运营处置，并针对云资产进行持续风险监视和泄露监控等，同时提供应急值守团队进行全天候安全保障，提升用户运营效率。

安全托管服务具备哪些安全能力?

安全托管服务（Managed Security Service，MSS）提供了安全评估、风险检测、漏洞感知与风险监测、安全监控、风险处置和应急响应等能力，覆盖安全运营的各个关键阶段。

安全托管服务主要分析哪些安全事件?

安全托管服务主要分析安全产品的事件、产品安全策略配置事件、安全漏洞事件及数据泄露事件等。

安全托管服务有条件限制吗?

由于安全托管服务中的安全监控服务，涉及对用户业务环境中的安全告警及攻击事件进行分析，因此需要用户具备基础安全检测和防护产品（如主机安全、Web 应用防火墙）获取相关事件，进而对事件进行深度分析。

安全托管服务是如何收费的?

腾讯云安全托管服务采用预付费模式，按照阶梯计价的模式进行收费，详情请参见 购买指南 。

如何快速接入并使用产品?

如需快速接入并使用产品，请参见 快速入门 。

服务购买后，有相应的操作指导吗?

服务购买后，我们将线下提供服务交付标准和需配合的指导说明。

服务购买后，有哪些服务保障?

- 服务购买后，腾讯云 MSS 服务团队将立即启动后台安全事件分析，并将事件分析结果在服务控制台进行呈现，定期输出整体安全风险服务报告，按照 SLA 协议承诺对客户服务内容进行交付。
- 若遇到问题，MSS 服务团队会提供支持和解答。

安全托管服务可以根据用户需求提供个性化服务吗?

安全运营托管服务当前为标准化服务内容，如果客户有特定需要，可与 MSS 服务团队联系并另外购买，根据自身关注需求进行重点运营监控。

密评咨询服务

最近更新时间：2026-07-10 15:02:30

什么是商用密码？

商用密码是指采用特定变换的方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务。

什么是商用密码应用安全性评估（密评）？

商用密码应用安全性评估（简称“密评”）是指按照有关法律法规和标准规范，对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性、有效性进行检测分析和评估验证的活动。

腾讯云密评服务是什么？

腾讯云密评服务是腾讯云结合腾讯云上密码产品和最佳实践，提供需求沟通、差距分析、方案制定、业务改造等全流程一站式的密评咨询服务，帮助用户高效开展密评。

密评与网络安全等级保护（等保）是什么关系？

两者都是国家法定的网络安全制度，关系紧密：

- 目标一致：都是为了提升系统安全性，满足合规要求。
- 侧重不同：等保是覆盖网络、主机、应用、数据、管理的全面安全保护体系；密评是等保在密码应用领域的深化和专项要求，重点关注密码技术的合规、正确、有效应用。
- 关系：密评是等保（尤其是三级以上系统）测评中的重要组成部分和必备项。一个系统通过等保测评，不代表其密码应用一定合规，仍需单独进行密评。

为什么需要进行密评？

- 法律要求：根据《密码法》等相关规定，法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统，其运营者应当使用商用密码进行保护，定期开展密评。
- 合规驱动：是落实网络安全、信息系统安全的必备环节。
- 风险防控：通过评估发现密码使用中的隐患（如弱算法、弱密钥、不当部署等），提升系统整体安全防护能力，防范数据泄露、身份冒用、交易篡改等安全风险。

密评的法律法规依据是什么？

主要依据包括：

- 《中华人民共和国密码法》
- 《中华人民共和国网络安全法》
- 《关键信息基础设施安全保护条例》
- 《商用密码应用安全性评估管理办法》
- 《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）

国家密码管理局发布的一系列配套管理办法和技术标准。

大模型备案咨询服务

最近更新时间：2026-07-10 15:02:30

什么是大模型备案？为什么必须做大模型备案？

是指根据《生成式人工智能服务管理暂行办法》等相关规定，提供具有舆论属性或者社会动员能力的生成式人工智能服务的，应当按照国家有关规定开展安全评估，并履行算法备案手续。

如果我只调用第三方模型 API，还需要备案吗？

对于通过 API 接口或其他方式直接调用已备案模型能力的生成式人工智能应用或功能，应向地方网信办申请和履行登记。

备案是一次性的吗？模型更新怎么办？

不是。若模型架构、参数量级、生成模态（如新增视频生成）等备案信息发生变更的，应当按要求在指定期限内办理变更手续。