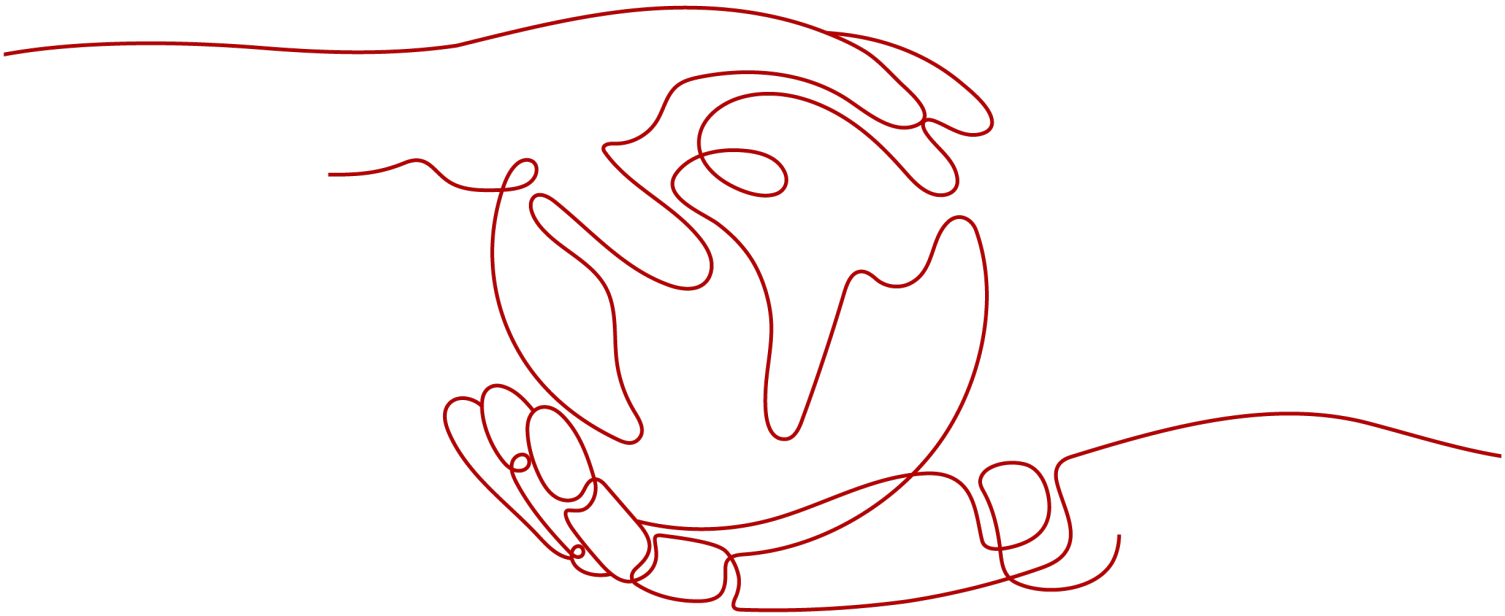
管理检测与响应

常见问题

文档版本	31
发布日期	2024-03-30



华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 产品咨询

1.1 管理检测与响应提供几种服务项目?

管理检测与响应提供以下4种服务版本:

- 企业版
- 等保建设助手
- 专项版
- 密评建设助手

1.2 管理检测与响应的服务内容是什么?

管理检测与响应（Managed Detection Response，MDR）是结合华为30年安全经验积累，以云服务的形式，为客户建立由管理、技术与运维构成的安全风险管控体系，结合企业与机构业务的安全需求反馈和防控效果对用户安全防护进行持续改进，帮助企业与机构实现对安全风险与安全事件的有效监控，并及时采取有效措施持续降低安全风险，消除安全事件带来的损失。

管理检测与响应提供企业版、等保建设助手、专项版和密评建设助手5种服务类型。

须知

管理检测与响应的有效期为1年，请务必在有效期内使用。到期以后，需重新购买。

企业版

企业版管理检测与响应结合您实际业务场景，通过云服务方式，为您提供华为云安全标准化的运维运营服务。企业版服务详细内容请参见**表 企业版服务说明**。

表 1-1 企业版服务说明

服务内容	响应时间	交付件
网站安全体检：远程提供安全监测服务支持HTTP/HTTPS协议进行实时安全监测；支持网页木马、恶意篡改、坏链、对外开放服务、可用性、审计、脆弱性这七个维度对网站进行监测；支持WEB安全漏洞扫描及域名劫持进行实时安全监测； 定期推送网站安全体检报告。	• 8小时内响应 • 服务后5个工作日内提交测试报告	提供专业的《监控季度总结报告》和《年度总结报》。
主机安全体检：通过日志分析、漏洞扫描等技术手段对主机进行威胁识别；通过基线检查发现主机操作系统、中间件存在的错误配置、不符合项和弱口令等风险。	• 8小时内响应 • 5个工作日内评估主机安全	提供专业的《主机安全评估报告》。
安全加固：对主机服务器、中间件进行漏洞扫描、基线配置加固；分析操作系统及应用面临的安全威胁，分析操作系统补丁和应用系统组件版本；提供相应的整改方案，并在您的许可下完成相关漏洞的修复和补丁组件的加固工作。	• 8小时内响应 • 单次服务10-20个系统后10个工作日内提交测试报告。	提供专业的《安全加固交付报告》。
安全监测：通过远程查找及处置主机系统内的恶意程序，包括病毒、木马、蠕虫等；通过远程查找及处置Web系统内的可疑文件，包括Webshell、黑客工具和暗链等；提出业务快速恢复建议，协助您快速恢复业务。	• 工作日内8小时响应。 • 5个工作日内评估项目总体人工天与预计周期。	提供专业的《安全监测报告》。
应急响应：业务系统出现安全问题的情况下，提供24小时安全应急响应服务，由安全团队协助处理中毒、中木马等应急事宜，每次处理完成后华为侧提供应急响应报告，分析问题根因，并提供改进建议。	• 工作日1小时内响应，非工作日内4小时响应。 • 单次服务10台设备以内后3个工作日内以提交报告时间为准。	提供专业的《应急响应报告》。
安全配置服务：根据客户业务需求，如主机IP、主机系统版本、域名、流量、加密、数据库防护等级等信息。输出安全解决方案并制订安全防护体系包括安全服务规格、数量、策略。	工作日1小时内响应，非工作日内4小时响应。	提供专业的《安全配置方案》。
安全防护服务开通与部署：安全服务交付，如主机安全、WAF、DDoS高防、堡垒机、漏洞扫描等服务的部署。云安全设置，提供云安全设置服务，包括安全组、防火墙策略等的设置操作	工作日1小时内响应，非工作日内4小时响应。	提供专业的《安全服务交付报告》。

服务内容	响应时间	交付件
定期策略更新与维护：从主机安全、应用安全、网络安全、数据安全、安全管理等方面定期完成漏洞检测、基线扫描、策略优化、巡检监控等操作，并输出整改方案报告。	• 工作日8小时内响应。 • 7个工作日内评估项目总体人工天与预计周期。	提供专业的《安全运维服务周期性报告》。
安全漏洞预警：根据最新的安全漏洞、病毒木马、黑客技术和安全动态信息，结合客户实际的操作系统、中间件、应用和网络情况等，定期将相关安全信息如安全漏洞、病毒木马资讯、安全隐患/入侵预警和安全事件动态等内容，以电子邮件方式进行通报，并提出合理建议和解决方案等。	• 固定发送安全资讯周报 • 工作日1小时内响应，非工作日内4小时响应。 • 不定时发送漏洞预警	提供专业的《安全周报和漏洞预警》。
主动安全预警：主机存在被入侵并对外攻击问题，主动邮件或电话知会客户排查；针对主动发现的影响客户使用的安全问题，进行主动通知工作。	工作日1小时内响应，非工作日内4小时响应。	提供专业的《配置核查报告》、《安全策略优化报告》、《弱口令检查报告》。
安全设备维护：对各类安全设备开展基础维护，包括设备配置定期备份、设备特征库升级、设备版本升级、设备切换、设备配置调整等。	每周固定发送安全巡检周报，不定时发送设备维护报告	提供专业的《安全设备维护报告》。
漏洞管理：通过华为云主机安全、漏洞扫描等安全服务，对实现云上业务系统的web应用、操作系统、中间件等漏洞的统一管理。	• 工作日1小时内响应，非工作日内4小时响应。 • 单次服务结束后3个工作日内以提交报告时间为准。	提供专业《漏洞扫描报告》。

等保建设助手

等保建设助手凭借华为安全团队自身及客户等保认证经验，为您提供等保定级和差距评估咨询，并根据系统情况提供定级参考意见和相关技术建议书以及等保条款分析情况汇总。

等保建设助手提供基础版和高级版两种服务类型，服务内容和典型应用场景如**表 等保建设助手说明**所示。您可根据实际业务需求，选择购买需要的服务类型。

表 1-2 等保建设助手说明

服务类型	服务内容	典型应用场景
基础版	• 提供等保定级和差距评估咨询，根据系统情况提供定级参考意见和相关技术建议书以及等保条款分析情况汇总 • 等保安全加固方案：根据等级保护差距要求，远程方式提供安全加固建议	适用于您已找好等保测评机构，但缺乏对等保要求的深入了解，不知道如何整改且拖延整改周期。
高级版	• 提供等保定级和差距评估咨询，现场方式进行系统情况提供定级参考意见和相关技术建议书以及分析情况汇总 • 等保安全加固方案：根据等级保护差距要求，现场方式提供安全加固建议	

专项版

专项版通过业务信息收集、安全保障方案制定、安全自查与整改、安全防护加固、安全团队建设、现场+远程监控及响应、安全服务保障总结等方式，支撑各类会议稳定、圆满进行。

专项版提供云会议安全保障和特级安全保障两种服务类型，服务内容和典型应用场景如**表 专项版说明**所示。您可根据实际业务需求，选择购买需要的服务类型。

表 1-3 专项版说明

服务类型	服务内容	服务特色	典型应用场景
云会议安全保障	• 业务信息收集 • 安全保障方案制定 • 安全自查与整改 • 安全防护加固 • 安全团队建设 • 现场+远程监控及响应 • 安全服务保障总结	• 针对您的业务问题提供修复建议 • 提供保障服务的历史漏洞和修复建议 • 安排专职专家远程职守、实时监控	适用于重大会议

服务类型	服务内容	服务特色	典型应用场景
特级安全保障	• 业务信息收集 • 安全保障方案制定 • 安全自查与整改 • 安全防护加固 • 安全团队建设 • 现场+远程监控及响应 • 安全服务保障总结	• 对您的业务问题进行修复并提供建议 • 对您的保障业务系统进行风险评估并整改 • 修复保障服务的历史漏洞并定期跟踪 • 安排专职专家现场职守、实时监控	适用于特级会议

密评建设助手

密评建设助手面向政府和大型企事业单位提供“密评”合规、国密改造、密码安全评估咨询服务，根据密码应用情况提供密码合规参考意见、相关技术建议书以及密评条款分析情况汇总。密评建设助手详细服务内容请参见**表 密评建设助手说明**。

表 1-4 密评建设助手说明

服务项	服务内容	交付件
用户调研	项目需求沟通	提供需求沟通会议纪要
	信息收集与分析 • 填写《信息系统调研表》 • 调研表分析及评审	提供《信息系统调研表》
差距分析	密评技术条例分析	提供《差距分析报告》
	密评管理条例分析	
	现状分析与差距评估	
整改方案	密评技术条例整改指导 • 密评技术条例解读 • 根据测评结果判定，指导进行密评技术条例不满足项的整改	提供整改方案、管理制度模板
	密评管理条例整改指导 • 密评管理条例解读 • 根据测评结果判定，指导进行密评管理条例不满足项的整改	

服务项	服务内容	交付件
	技术及管理层面整改取证指导	
方案评估	密评专家进行方案评估 • 密评专家进行方案评估，审查被测系统责任单位的密码应用/密码设计/实施/应急方案 • 专家评估结论输出	提供《评估报告》

1.3 服务单有哪些状态?

服务单状态包括：

- 待处理

  用户购买企业版管理检测与响应，服务单付款成功，服务单状态为“待处理”。
- 处理中
  - 用户购买企业版管理检测与响应，通过沟通联系并审核资质后，服务单状态为“处理中”。
  - 用户购买等保建设助手，服务单付款成功，服务单状态为“处理中”。
- 服务取消

  华为云终止本次管理检测与响应，系统将服务单状态更新为“服务取消”。
- 待用户验收

  管理检测与响应报告由管理检测与响应审核通过后，系统将服务单状态更新为“待用户验收”。
- 已完成

  服务完成后，用户对本次管理检测与响应进行验收后，系统将服务单状态更新为“已完成”。

  说明

  - 服务单列表展示了用户名下的所有服务单，以上服务单状态说明为管理检测与响应服务单状态说明。
  - 服务单的处理进展您可前往服务单详情界面的“处理日志”区域查看。详细操作步骤请查看：**查看服务单信息**。

1.4 服务单的有效期是多长?

从您成功购买管理检测与响应起计算，服务单的有效期为1年。请您务必在有效期内使用，到期以后，需重新购买。

1.5 执行等保测评的专业机构是什么?

执行等保测评的专业机构是具有等保测评资质的权威机构。华为云等保服务团队将全流程贴心服务。

1.6 哪些区域可以使用管理检测与响应?

管理检测与响应的**企业版**和**等保建设助手**属于线下服务。可购买的区域为：“华北-北京四”。

1.7 管理检测与响应支持跨平台和线下服务吗?

管理检测与响应服务的**企业版**和**等保建设助手**支持跨平台和线下服务。

1.8 管理检测与响应是第三方服务吗?

企业版的测评机构是第三方服务，其第三方服务提供者如下：

- 企业版：由华为联合优质的第三方机构一起提供

1.9 管理检测与响应提供现场服务吗?

管理检测与响应根据不同版本提供不同的服务支持，详细内容如**表1-5**所示。

表 1-5 管理检测与响应技术支持说明

服务版本	远程服务	现场服务
企业版	支持	不支持
等保建设助手	支持基础版	支持高级版不高于5人天的服务

1.10 管理检测与响应是否对中国以外的您提供服务?

不能对中国以外的您提供服务。

根据当前的业务策略，管理检测与响应目前仅对中国您提供服务。

1.11 管理检测与响应能给您带来什么好处?

管理检测与响应可以通过主动的方法来检测和管理安全事件，与通过服务解决方案部署的扫描、检测和保障的持续响应相结合，从而限制安全事件的影响。

1.12 管理检测与响应可以对华为云外的站点提供服务吗?

可以。管理检测与响应服务的企业版可以对华为云外的站点提供服务。

1.13 管理检测与响应服务和传统漏洞扫描的主要区别是什么?

管理检测与响应服务的核心是安全专家人工服务，相比传统漏洞扫描，管理检测与响应团队审核您申请范围的归属权和体检报告，且由第三方具有权威的资质和专业的技术的信息安全测评机构进行管理检测与响应服务，检测深度和广度更有显著优势，能够发现普通扫描器无法发现的安全风险。

1.14 管理检测与响应提供了哪些沟通渠道?

管理检测与响应提供以下沟通渠道：

线上：提交咨询工单。

线下：拨打400电话或发送邮件到sasnotice@huawei.com进行管理检测与响应咨询。

1.15 管理检测与响应审核服务单的什么内容?

审核服务单的测试范围和申请范围的归属权。

您提交服务单后，管理检测与响应会电话和您沟通，明确您的测试范围并对您申请范围的归属权进行审核。

1.16 管理检测与响应审核体检报告的什么内容?

审核体检报告是否满足此次服务的交付标准。

管理检测与响应团队对权威的第三方机构提供的体检报告的测试覆盖范围进行审核，确认测试范围是否满足对应的体检服务的交付标准。

1.17 您通过管理检测与响应获得的最终交付件是什么?

管理检测与响应最终的交付件为经过管理检测与响应团队审核通过的管理检测与响应报告，详情请参见如**表1-6**所示。

表 1-6 管理检测与响应交付件

服务版本	服务类型	交付成果
企业版	-	提供专业的企业版管理检测与响应报告
等保建设助手	• 基础版 • 高级版	提供安全加固方案或差距分析报告

1.18 是否可以下载管理检测与响应报告（等保测评报告）？

当管理检测与响应完成，您会收到短信通知信息。此时，您可登录管理控制台在“支持与服务 > 专业服务 > 我的服务单”页面，下载并查看管理检测与响应服务报告。详细操作步骤请查看：**下载管理检测与响应报告**。

1.19 管理检测与响应是否提供纸质体检报告?

管理检测与响应服务报告可以加盖信息安全测评机构的印章。

您可以通过sasnotice@huawei.com邮箱申请纸质管理检测与响应报告。

1.20 什么是区域和可用区?

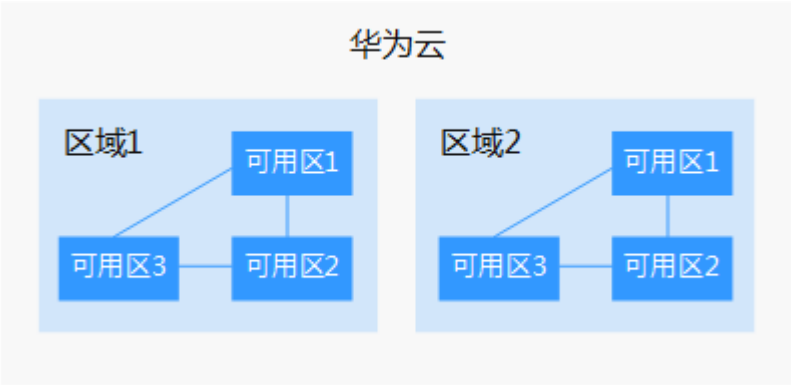
什么是区域、可用区?

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图1-1阐明了区域和可用区之间的关系。

图 1-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

2 等保问题

华为云等保备案证书下载

华为云平台已完成等保三级认证，华为云部分Region节点的安全保护等级为第四级。

华为云将提供以下材料，协助租户云上系统通过等保测评：

- 华为云等保备案证明，请前往**信任中心>安全合规**下载。
- 华为云测评报告封面及结论页，联系客户经理或提交**等保咨询**。
- 华为云安全产品销售许可证。

更多信息

- 单击查看**等保合规安全解决方案**详情。
- **华为云总体安全性**。

如何获取华为云等保合规白皮书?

如果您需要华为云等保合规白皮书，请您联系客户经理或单击**华为云等保合规白皮书下载**，注册/登录华为云后，提交信息并下载白皮书。

更多关于华为云安全的信息，请前往**信任中心**了解详情。

如何过等保?

客户需要先对系统进行定级和备案，根据等保有关规定和标准，对信息系统进行安全建设整改，然后找专门的测评机构对系统开展测评工作，测评结束后，测评结果符合国家相应标准就可以获取等保认证。

更多关于等保相关问题，您可以提交**等保合规安全解决方案**咨询工单，华为云专家将在1个工作日内和您联系。

如何给系统定级?

信息系统运营单位按照《 网络安全等级保护定级指南 》，自行定级。三级以上系统定级结论需进行专家评审，由网监受理备案申请。

信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。信息安全等级定级标准详情如**表2-1**所示。

表 2-1 信息安全等级定级标准

受侵害的客体	对客体的一般损害	对客体的严重损害	对客体的特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

等保测评周期

二级系统至少每两年一次，三级系统至少每年一次。

等保测评报告多久可以拿到?

依照整改标准进行整改，从完成备案后到拿到测评报告需要1~2个月不等。

过等保时，为系统配置华为云安全服务会对业务有影响吗?

购买华为云安全服务，正确配置不会对您的业务造成影响，且安装完成后，服务器也不需要重启。

过等保，系统中的日志至少需要保存多少天?

根据《 网络安全等级保护基本要求 》，对于系统中的日志至少需要保存180天。

等保通过后，升级软件对等保有影响吗?

没有影响。软件升级不影响已通过的等保。

3 管理类

3.1 如何使用管理检测与响应?

使用管理检测与响应的流程说明如下：

- 购买管理检测与响应
  - 您购买管理检测与响应时，可以根据实际业务需求选择服务版本。
  - 在购买管理检测与响应时，您只需要选择购买的个数和您的信息。

  购买管理检测与响应的详细操作，请参见**管理检测与响应用户指南**的**购买管理检测与响应**。
- 执行管理检测与响应
  - 企业版

    当服务单补全了信息且管理检测与响应审核通过后，第三方信息安全测评机构将根据订单中描述的站点进行安全服务。
  - 等保建设助手

    等保建设助手为您提供等保定级和差距评估咨询，根据系统情况提供定级参考意见和相关技术建议书以及等保条款分析情况汇总，根据等保差距要求，服务类型以远程或现场方式提供安全加固建议。
  - 专项版

    专项版服务内容包括业务信息收集、安全保障方案制定、安全自查与整改、安全防护加固、安全团队建设、现场+远程监控及响应、安全服务保障总结。
  - 密评建设助手

    密评建设助手面向政府和大型企事业单位提供“密评”合规、国密改造、密码安全评估咨询服务，根据密码应用情况提供密码合规参考意见、相关技术建议书以及密评条款分析情况汇总。
  - 检查与加固

    检查与加固服务包括安全产品托管、应急响应、网站安全体检、主机安全体检、安全加固以及攻击路径评估。
- 下载管理检测与响应报告

  服务完成后，系统自动生成管理检测与响应报告，您会收到邮件和短信通知信息。您可在收到通知信息后下载管理检测与响应报告。

  如何下载管理检测与响应报告，请参考：**下载管理检测与响应报告**。

- 验收管理检测与响应

  服务完成后，您会收到短信通知信息。您可在收到消息通知起的60日内，对本次管理检测与响应进行验收。如果超出该时间范围，系统将对本次管理检测与响应进行自动验收。

  须知

  验收完管理检测与响应服务后，MDR服务默认此服务单已交付完成，验收后此服务单将不再提供服务。

  如何验收管理检测与响应，请参考：**验收管理检测与响应**。

- 评价管理检测与响应

  服务完成后，您会收到邮件和短信通知信息。您可在收到消息通知后，对本次管理检测与响应进行评价，并反馈建议或意见。

  如何评价管理检测与响应，请参考：**评价管理检测与响应**。

4 费用类

4.1 管理检测与响应是否支持退款?

管理检测与响应不支持退款。

如果您对服务有任何意见，可以在管理控制台右上方单击“工单”提交工单，或者联系客服进行处理。