管理检测与响应

产品介绍

文档版本 25

发布日期 2021-05-31

华为技术有限公司

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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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 什么是管理检测与响应.....1
2 功能介绍.....7
3 产品优势.....8
4 业务流程.....9
5 计费说明.....13
6 MDR 权限管理.....15
7 访问和使用.....17
8 与其他云服务的关系.....19
9 个人数据保护机制.....21
10 相关概念.....23
A 修订记录.....25

1 什么是管理检测与响应

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、等保安全、等保建设助手和等保套餐4种服务。

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用户实际业务场景，通过云服务方式，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1-1。

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、脆弱性等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 • 服务结束后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》。

服务内容	响应时间	交付件
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；提供相应的整改建议，并在用户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 • 单人单次10-20个系统服务结束后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，协助用户快速恢复业务。	• 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、中木马等应急处理事宜，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台设备以内结束后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》。
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，并输出整改建议报告	• 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》。

服务内容	响应时间	交付件
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》。

等保安全

华为安全专家团队为客户量身定制等保合规整改建议，指导用户进行安全服务的选型和部署，对网络、主机、数据库、安全管理制度等进行整改，优选具有资质的权威等保测评机构，提供专业的测评报告或差距分析报告或整改解决方案。

等保安全服务提供基础版、高级版和APP检测3种服务类型，服务内容和典型应用场景如**表1-2**所示。用户可根据实际业务需求，选择购买需要的服务类型。

表 1-2 等保安全服务说明

服务类型	服务内容	典型应用场景
基础版	• 助手式服务，华为云安全专家远程支持 • 仅提供等保的安全整改建议 • 定级系统的服务器数量<=10 • 权威机构的测评服务	适用于政府、金融等机构的如下场景： • 非首次测评 • 有专业安全人员 • 知道怎么过等保 • 简单系统，一般门户网站
高级版	• 教练式服务，华为云安全等保专家现场支持 • 提供等保全流程的贴身指导服务（协助系统定级备案、差距分析、规划设计、落实整改、等级测评、安全保障） • 权威机构的测评服务	适用于政府、金融等机构的如下场景： • 首次测评 • 无专业安全人员 • 不知道怎么过等保 • 复杂系统，重要信息系统 • 希望全面提升系统的整体安全防护能力
APP检测	APP合规建设检查，提供iOS/安卓APP等保合规检测服务	-

等保套餐

等保2.0产品优惠套餐，为客户提供一站式的安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保合规要求。提供等保二级方案、等保三级方案基础版、等保三级方案高级版及多云安全方案套餐。各套餐内容和典型应用场景如**表1-3**所示。用户可根据实际业务系统情况，选择购买套餐类型。

表 1-3 等保套餐说明

套餐类型	套餐内容	典型应用场景
等保二级方案	• 企业主机安全 • Web应用防火墙（WAF） • SSL证书 • 云堡垒机 • 态势感知	适用于用户量和敏感数据较少，如果发生安全问题，不会对企业自身及用户造成特别严重影响的。如普通企业的门户网站，企业内部用的OA系统。

套餐类型	套餐内容	典型应用场景
等保三级方案基础版	• 企业主机安全 • Web应用防火墙（WAF） • 云堡垒机 • 数据库安全审计 • 态势感知 • SSL证书 • 数据安全中心	适用于存有用户敏感信息的行业，信息外泄会造成特别严重影响，甚至会社会秩序和公共利益造成损失。
等保三级方案高级版	• 企业主机安全 • 漏洞扫描服务 • Web应用防火墙（WAF） • 云堡垒机 • 数据库安全审计 • 态势感知 • SSL证书 • DDoS高防 • 加密服务 • 数据安全中心	适用于存有用户敏感信息的行业，信息外泄会造成特别严重影响，甚至会社会秩序和公共利益造成损失。如政务、教育、医疗、物流、金融等相关行业。
多云安全方案套餐	根据业务系统的情况，自定义购买以下安全方服务： • 企业主机安全 • 漏洞扫描服务 • Web应用防火墙（WAF） • 云堡垒机 • 数据库安全审计 • 态势感知 • SSL证书 • DDoS高防 • 加密服务 • 数据安全中心	-

等保建设助手

等保建设助手是华为安全团队凭借自身及客户等保认证经验，为用户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1-4所示。用户可根据实际业务需求，选择购买需要的服务类型。

表 1-4 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	适用于用户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	

2 功能介绍

管理检测与响应提供以下功能：

- 购买管理检测与响应
  - 用户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，用户只需要反馈购买的个数和用户信息。

  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》。
- 执行管理检测与响应
  - 企业版

    当服务单补全了信息且华为安全专家审核通过后，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。
  - 等保安全

    当订单成功支付后，华为安全专家团队将为客户量身定制等保合规整改建议，指导客户进行安全服务的选型和部署，对网络、主机、数据库、安全管理制度等进行整改，优选具有资质的权威等保测评机构，提供专业的测评服务。
- 下载管理检测与响应报告

  管理检测与响应完成后，系统自动生成管理检测与响应报告，用户会收到邮件和短信通知信息。用户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查看：**下载管理检测与响应报告**。
- 验收管理检测与响应

  管理检测与响应完成后，用户会收到短信通知信息。用户可在收到消息通知起的10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。

  如何验收管理检测与响应请查看：**验收管理检测与响应**。
- 评价管理检测与响应

  管理检测与响应完成后，用户会收到邮件和短信通知信息。用户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查看：**评价管理检测与响应**。

3 产品优势

管理检测与响应具有一键下单即刻服务、大数据加持获取全局威胁情报能力、服务规模化的优势。

专业保障

提供华为云安全能力，客户可进行相应的安全防护。

效率提高

持续提升安全效率，减少安全运维人员的投入。

方便快捷

快速构建安全能力，提供安全防护使用支持。

策略管理

快速帮助客户提高防御级别，做好安全运营。

4 业务流程

管理检测与响应服务为用户提供购买、体检报告下载、验收管理检测与响应服务业务流程。

本章节介绍管理检测与响应企业版、等保安全的业务流程。

企业版业务流程

企业版是华为与权威的第三方机构合作提供的专业的安全专家人工服务并提供专业的检测报告。

企业版业务流程如图4-1所示。各步骤说明如表4-1所示。

图 4-1 企业版业务流程图

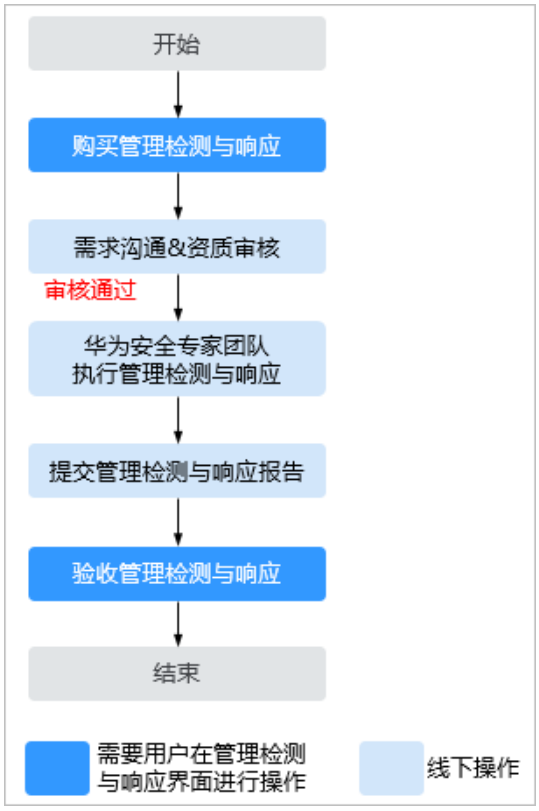

表 4-1 企业版业务流程说明

步骤	流程操作	说明
1	购买企业版	在购买时，您需要反馈购买资源数量。
2	需求沟通&资质审核	购买成功后，华为安全专家将在1个工作日内联系您，与您沟通确定服务内容和审核资质。
3	华为安全专家团队执行管理检测与响应	审核通过后，华为云安全专家团执行本次管理检测与响应。 • 网站安全体检 • 主机安全体检 • 安全加固指导 • 安全监测服务 • 应急响应服务 • 安全配置服务 • 安全防护服务开通与部署 • 定期策略更新与维护 • 安全漏洞预警服务 • 主动安全预警服务 • 安全设备维护服务 • 漏洞管理服务 • 电子取证、司法鉴定
4	提交安全专家服务报告	服务周期到期后，华为安全专家上传本次安全专家服务报告。
5	验收管理检测与响应	华为安全专家完成审核后，上传管理检测与响应报告，此时您会收到验收短息，请您前往管理检测与响应管理控制台进行验收本次管理检测与响应。

等保安全业务流程

华为安全专家团队为客户量身定制等保合规整改建议，指导用户进行安全服务的选型和部署，对网络、主机、数据库、安全管理制度等进行整改，优选具有资质的权威等保测评机构，提供专业的测评报告或差距分析报告或整改解决方案。

等保安全业务流程如图4-2所示，各流程步骤说明如表4-2所示。

图 4-2 等保安全业务流程图

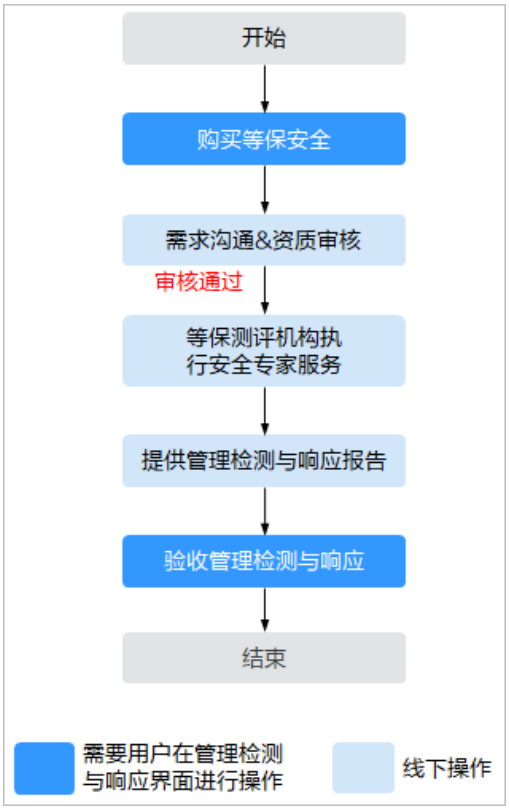

表 4-2 等保安全业务流程说明

步骤	操作	说明
1	**购买等保安全**	购买等保安全前，请用户先与华为云联系确定项目后再下单。 购买时，用户需要反馈基础版和高级版数量，以及用户信息。
2	需求沟通&资质审核	购买成功后，华为安全专家将在1个工作日内联系用户，与用户沟通确定等保需求。指导用户进行安全服务的选型和部署，对网络、主机、数据库、安全管理制度等进行整改。
3	等保测评机构执行管理检测与响应	审核通过后，由权威等保测评机构执行等保测评工作。
4	提交管理检测与响应报告	华为安全专家上传整改解决方案和差距分析报告。 **说明** 等保测评报告由测评机构出具，因涉及用户隐私，测评报告由测评机构按照用户提供的地址直接邮寄给用户。
5	**验收管理检测与响应**	服务完成后，用户验收本次管理检测与响应。

等保建设助手

等保建设助手是华为安全团队凭借自身及客户等保认证经验，为用户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。

等保建设助手流程如图4-3所示，各流程步骤说明如表4-3所示。

图 4-3 等保建设助手业务流程图

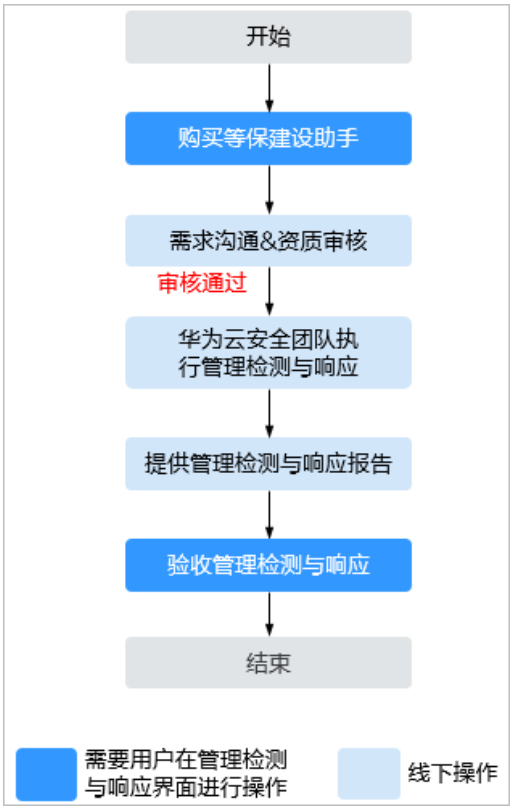

表 4-3 等保建设助手业务流程说明

步骤	操作	说明
1	购买等保建设助手	购买等保建设助手前，请用户先与华为云联系确定项目后再下单。 购买时，用户需要反馈基础版和高级版数量，以及用户信息。
2	需求沟通&资质审核	购买成功后，华为安全专家将在1个工作日内联系用户，与用户沟通确定需求并审核资质。
3	华为安全团队执行管理检测与响应	审核通过后，华为安全专家团队将根据用户IT系统的实际情况提供定级意见、差距分析以及安全加固建议。
4	提交管理检测与响应报告	华为安全专家上传安全加固方案或差距分析报告。
5	验收管理检测与响应	服务完成后，用户验收本次管理检测与响应。

5 计费说明

本章节主要介绍管理检测与响应的计费说明，包括计费项、计费模式以及续费等。

计费项

表 5-1 计费项说明

计费项	计费说明
企业版	根据您购买的“资源数”进行计费。
等保安全	根据您购买的“基础版数量”和“高级版数量”进行计费。
等保套餐	根据您购买的“推荐套餐”、“套餐商品配置”和“购买时长”进行计费。
等保建设助手	根据您购买的“基础版数量”和“高级版数量”进行计费。

计费模式

管理检测与响应属于按需计费，且为一次性计费产品。

详细的服务资费和费率标准，请参见**产品价格详情**。

变更配置

管理检测与响应不支持退订，在购买时，用户可以参考**典型应用场景**和根据自身业务的实际情况购买管理检测与响应。

续费

- 管理检测与响应的**企业版**、**等保安全**和**等保建设助手**属于一次性消费，不支持续费。到期后，需重新购买。
- **等保套餐**内的安全服务到期后，如果没有按时续费，公有云平台会提供一定的保留期。
  保留期的时长由客户等级而定，具体请参见**保留期**。

当您购买的安全服务到期后，安全服务将停止服务。为了防止造成不必要的损失，请您及时续费。如果未续费，您将不能使用购买的安全服务，不影响您的业务。

如需续费，请在管理控制台**续费管理**页面进行续费操作。详细操作请参考**续费管理**。

到期与欠费

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。

FAQ

更多计费相关FAQ，请参见**MDR常见问题**。

6 MDR 权限管理

如果您需要对华为云上购买的管理检测与响应服务（MDR）资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云帐号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有管理检测与响应（MDR）的使用权限，但是不希望他们拥有删除MDR等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用MDR，但是不允许删除MDR的权限，控制他们对MDR资源的使用范围。

如果华为云帐号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用MDR服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。关于IAM的详细介绍，请参见**IAM产品介绍**。

MDR 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

MDR部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问MDR时，需要先切换至授权区域。

如**表6-1**所示，包括了MDR的所有系统角色。由于华为云各服务之间存在业务交互关系，管理检测与响应服务的角色依赖其他服务的角色实现功能。因此给用户授予管理检测与响应的角色时，需要同时授予依赖的角色，管理检测与响应的权限才能生效。

表 6-1 MDR 系统角色

角色名称	描述	依赖关系
SES Administrator	管理检测与响应服务的管理员权限。	购买实例需要具有BSS Administrator角色。 BSS Administrator：对帐号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级策略，在同项目中勾选。

相关链接

- **IAM产品介绍**
- **创建用户组、用户并授予MDR权限**

7 访问和使用

如何访问

请使用管理控制台方式访问管理检测与响应。如果用户已注册公有云，可直接登录管理控制台，在页面上方选择“区域”后，单击 ，选择“安全 > 管理检测与响应”访问。

如何使用

管理检测与响应服务使用流程说明如表7-1所示。

表 7-1 管理检测与响应服务使用流程说明

子流程	说明
购买业务	• 用户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，用户只需要反馈购买的个数和用户信息。
申请交付标准版管理检测与响应	如果用户成功购买了标准版管理检测与响应，在成功购买标准版的1年内，用户需要申请交付服务单信息。
执行管理检测与响应	• 企业版 当订单成功支付后，华为安全专家将快速响应并结合用户实际业务场景，通过云服务方式，提供华为云安全标准化的运维运营服务。 • 等保安全 当订单成功支付后，华为安全专家团队将为客户量身定制等保合规整改建议，指导客户进行安全服务的选型和部署，对网络、主机、数据库、安全管理制度等进行整改，优选具有资质的权威等保测评机构，提供专业的测评服务。 • 等保建设助手 当订单成功支付后，华为安全专家团队将为用户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。

子流程	说明
验收服务	• 企业版 企业版完成管理检测与响应并上传服务报告后，本次管理检测与响应完成。 • 等保安全 权威等保测评机构完成测评后，上传测评证明后，本次管理检测与响应完成。 • 等保建设助手 华为云安全专家上传安全加固方案或差距分析报告后，本次管理检测与响应完成。

8 与其他云服务的关系

与消息中心的关系

消息中心是为用户提供各类通知消息的接收和管理的服务平台。通过消息中心，设置“服务单提醒”通知，方便您及时了解服务单进展，从而避免信息遗漏造成不必要的损失。

关于消息中心的详细介绍，请参见《 消息中心用户指南 》。

与统一身份认证服务的关系

统一身份认证服务（ Identity and Access Management，简称IAM ）为管理检测与响应提供了权限管理的功能。需要拥有MDR Administrator权限的用户才能使用MDR服务。如需开通该权限，请联系拥有Security Administrator权限的用户，详细内容请参考《 统一身份认证服务用户指南 》。

与云审计服务的关系

云审计服务（ Cloud Trace Service，CTS ）记录了管理检测与响应相关的操作事件，如表8-1所示。方便用户日后的查询、审计和回溯，具体请参见《 云审计服务用户指南 》。

表 8-1 云审计服务支持的 MDR 操作列表

操作名称	资源类型	事件名称
管理检测与响应-创建订单	PSDM	createMdrOrder
管理检测与响应-租户申请交付	PSDM	mdrCustomerApplication
租户侧上传附件	PSDM	customerUploadAccessory
租户侧下载指定模板文件	PSDM	customerDownloadTemplate
服务单附件下载	PSDM	downLoadAccessories

操作名称	资源类型	事件名称
服务单验收通过	PSDM	professionalTicketsAcceptanceSuccess
服务单验收延期	PSDM	professionalTicketsAcceptanceExtend
服务单评价	PSDM	professionalTicketsEvaluate

9 个人数据保护机制

为了确保您的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，MDR通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

MDR收集及产生的个人数据如**表9-1**所示。

表 9-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
用户名	在购买服务时由客户在界面输入用户名	否	是 用户名是用户身份的标识信息
手机号	在购买服务时由客户在界面输入手机号	否	是 手机号是联系客户提供专家服务的方式
邮箱	在购买服务时由客户在界面输入邮箱	否	是 邮箱是联系客户提供专家服务的方式

存储方式

MDR通过加密算法对用户个人敏感数据加密后进行存储。

访问权限控制

用户个人数据通过加密后存储在MDR数据库中，数据库的访问需要通过白名单的认证与授权。

日志记录

用户个人数据的所有操作，包括增加、修改、查询和删除，MDR都会记录审计日志并上传至云审计服务（CTS），用户可以并且仅可以查看自己的审计日志。

10 相关概念

本章节介绍管理检测与响应常用的概念，包括服务单、网站安全体检、主机安全体检、安全加固、安全监测、应急响应和等保安全。

服务单

服务单是用户在管理检测与响应界面，购买管理检测与响应后所生成的申请单。

网站安全体检

网站安全体检是由权威的第三方机构安全专家远程提供的网站安全评估服务，覆盖SQL注入、XSS跨站、文件上传、文件下载、文件包含、敏感信息泄露、弱口令等风险的检测。

主机安全体检

主机安全体检是由权威的第三方机构安全专家远程提供主机安全评估服务，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。

安全加固

安全加固是由权威的第三方机构安全专家远程提供安全加固，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，提供相应的整改建议，并在用户的许可下完成相关漏洞的修复和补丁组件的加固工作。

安全监测

安全监测是由权威的第三方机构安全专家远程提供安全监测，提供7x24小时化监测服务，发现安全问题实时通过电话、邮件等形式进行告警，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、脆弱性等六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，让用户全面了解网站的运行情况。

应急响应

应急响应是由权威的第三方机构安全专家远程提供事件处置服务，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，协助用户快速恢复业务。

等保安全

等保安全为客户量身定制等保合规整改建议，指导客户进行安全服务的选型和部署，对网络、主机、数据库、安全管理制度等进行整改，优选具有资质的权威等保测评机构，提供专业的测评服务。

等保建设助手

等保建设助手是华为安全团队凭借自身及客户等保认证经验，为用户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。

A 修订记录

发布日期	修改说明
2021-05-31	第二十五次正式发布。 **什么是管理检测与响应**，等保套餐内容增加数据安全中心服务。
2020-12-02	第二十四次正式发布。 管理检测与响应标准版功能下线。
2020-10-10	第二十三次正式发布。 • 全新**企业版**功能上线。 • **计费说明**，新增企业版相关内容描述。 • **访问和使用**，新增企业版相关内容描述。
2020-09-16	第二十二次正式发布。 **与其他云服务的关系**，新增与云审计服务的关系。
2020-09-14	第二十一次正式发布。 • **什么是管理检测与响应**，新增**等保建设助手**版本。 • **访问和使用**，新增“等保建设助手”相关内容描述。 • **相关概念**，新增“等保建设助手”描述。
2020-08-25	第二十次正式发布。 **什么是管理检测与响应**，等保套餐内容变更。
2020-07-30	第十九次正式发布。 • “安全专家服务”更名为“管理检测与响应”。 • **什么是管理检测与响应**，新增**等保套餐**内容。 • 下线企业版相关内容。
2020-05-20	第十八次正式发布。 新增**计费说明**。

发布日期	修改说明
2020-05-07	第十七次正式发布。 **与其他云服务的关系**，优化相关内容描述。
2020-02-21	第十六次正式发布。 • **功能介绍**，优化相关内容。 • **业务流程**，新增流程说明。
2020-01-20	第十五次正式发布。 **MDR权限管理**，优化相关内容描述。
2019-12-10	第十四次正式发布。 **与其他云服务的关系**，删除与云审计服务的关系相关内容。
2019-11-12	第十三次正式发布。 **业务流程**，优化相关内容描述。
2019-11-01	第十二次正式发布。 • 新增**个人数据保护机制**。 • **业务流程**，调整流程内容。
2019-08-02	第十一次正式发布。 • **MDR权限管理**，修改相关策略内容描述。 • 新增**计费说明**。
2019-07-11	第十次正式发布。 • **相关概念**，优化相关内容描述。 • **访问和使用**，优化相关内容描述。 • **与其他云服务的关系**，优化相关内容描述。
2019-05-22	第九次正式发布。 新增**MDR权限管理**。
2019-05-10	第八次正式发布。 **什么是管理检测与响应**，增加功能介绍以及典型应用场景。
2018-11-02	第七次正式发布。 **与其他云服务的关系**，增加“与统一身份认证服务的关系”。
2018-08-30	第六次正式发布。 **功能介绍**，修改了功能的相关功能描述。

发布日期	修改说明
2018-08-16	第五次正式发布。 • **功能介绍**，修改了功能的相关功能描述。 • **业务流程**，修改了企业版和等保安全的业务流程图。 • **访问和使用**，修改了功能的相关内容描述。
2018-07-19	第四次正式发布。 **与其他云服务的关系**，更新了云审计服务支持的管理检测与响应操作列表内容。
2018-06-06	第三次正式发布。 **功能介绍**和**业务流程**，修改了相关内容描述。
2018-01-30	第二次正式发布。 **功能介绍**，优化了部分描述内容。
2017-09-26	第一次正式发布。