管理检测与响应

产品介绍

文档版本 32

发布日期 2024-04-12

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 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》。

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》。
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》。

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。

服务类型	服务内容	典型应用场景
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
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	
	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》

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
  - 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**。

3 产品优势

管理检测与响应具有一键下单（直接结算）即刻给您服务、大数据加持（使您获取全局威胁情报）能力、服务规模化的优势。

专业保障

提供安全体检、网站监测，应急响应，企业安全服务托管等管理检测与响应服务（另付费）。

极简

预置接入200+类安全数据，8个云服务、23类安全运营基线合规情况，100+安全处置剧本。

智能

快速构建安全能力，提供安全防护使用支持。

- 分析强劲，基于AI对用户行为、实体画像等多种维度数据关联分析。
- 全面解析云原生的数据结构，运用AI驱动的智能检索引擎，海量数据秒级检索。

开放

- 云原生的数据采集能力，天然与云网络、云服务的数据对接。
- 开放的云原生架构，支持与第三方生态的能力和数据集成。

4 业务流程

管理检测与响应服务为您提供购买企业版、等保建设助手、专项版、密评建设助手，提交管理检测与响应服务报告、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、等保建设助手、专项版、密评建设助手的业务流程。

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

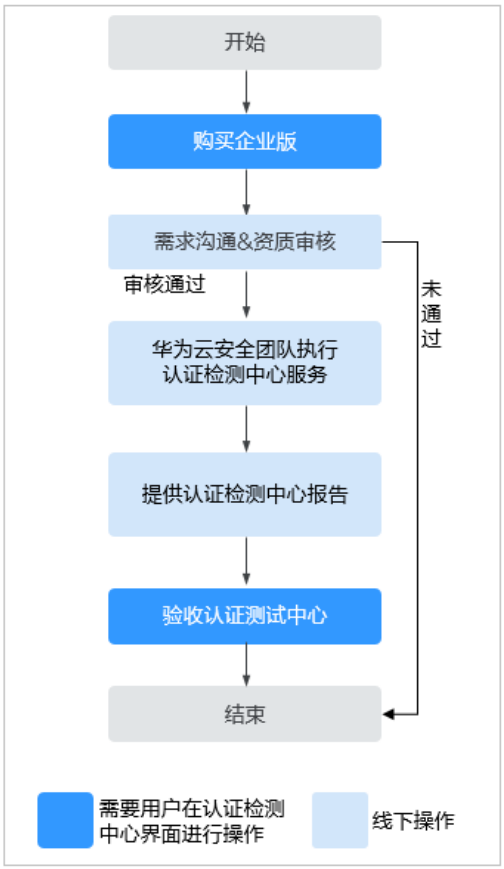

表 4-1 企业版业务流程说明

步骤	流程操作	说明
1	购买企业版	在购买时，您需要选择购买资源数量。
2	需求沟通&资质审核	购买成功后，管理检测与响应将在1个工作日内联系您，与您沟通确定服务内容和审核资质。

步骤	流程操作	说明
3	管理检测与响应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	提交管理检测与响应服务报告	服务周期到期后，管理检测与响应上传本次管理检测与响应服务报告。
5	**验收管理检测与响应**	管理检测与响应完成审核后，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 等保建设助手业务流程图

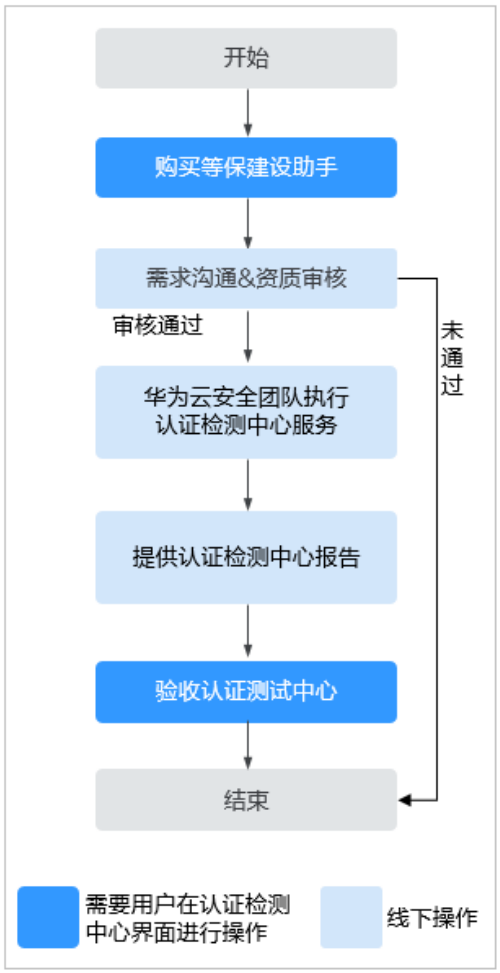

表 4-2 等保建设助手业务流程说明

步骤	操作	说明
1	购买等保建设助手	购买前，请拨打950808按1转1或直接联系您的客户经理，确定项目报价后再下单。 购买时，您需要选择服务类型、数量，以及您的信息。
2	需求沟通&资质审核	购买成功后，管理检测与响应将在1个工作日内联系您，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，管理检测与响应团队将根据您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	管理检测与响应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，您验收本次管理检测与响应。

专项版业务流程

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。

专项版业务流程如图4-3所示，各流程步骤说明如表4-3所示。

图 4-3 专项版业务流程图

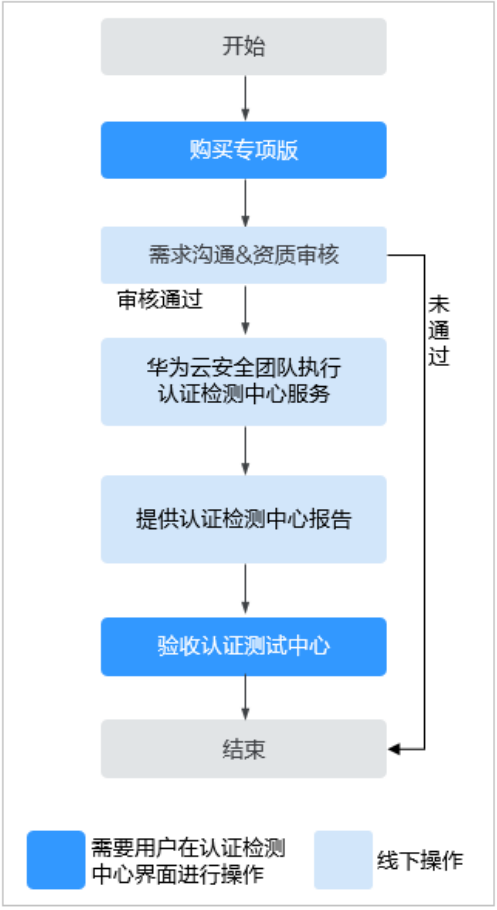

表 4-3 专项版业务流程说明

步骤	操作	说明
1	购买专项版	购买前，请拨打950808按1转1或直接联系您的客户经理，确定项目报价后再下单。 购买时，您需要选择服务类型、数量，以及您的信息。
2	需求沟通&资质审核	购买成功后，管理检测与响应将在1个工作日内联系您。指导您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。

步骤	操作	说明
4	提交管理检测与响应报告	管理检测与响应上传整改解决方案和差距分析报告。
5	验收管理检测与响应	服务完成后，您验收本次管理检测与响应。

密评建设助手业务流程

密评建设助手提供“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。

密评建设助手业务流程如所示，各流程步骤说明如表4-4所示。

图 4-4 密评建设助手业务流程图

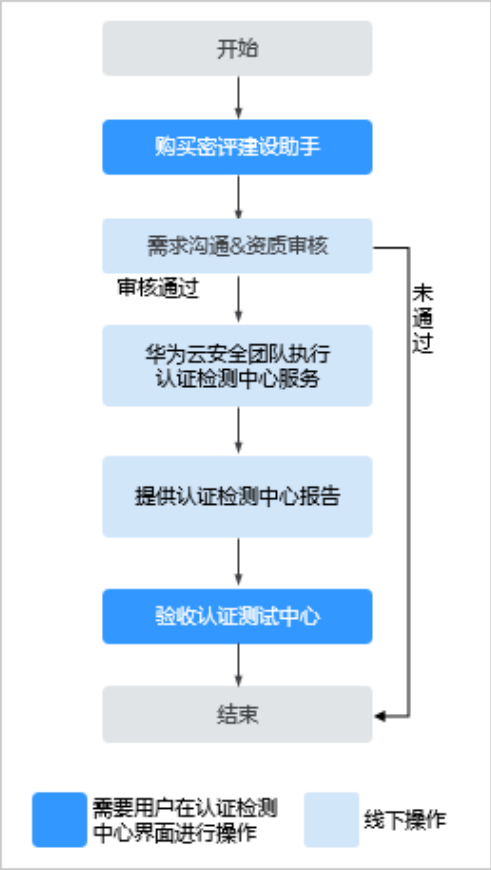

表 4-4 密评建设助手业务流程说明

步骤	操作	说明
1	购买密评建设助手	购买前，请拨打950808按1转1或直接联系您的客户经理，确定项目报价后再下单。 购买时，您需要选择服务类型、数量，以及您的信息。

步骤	操作	说明
2	需求沟通&资质审核	购买成功后，管理检测与响应将在1个工作日内联系您。指导您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	管理检测与响应上传整改解决方案和差距分析报告。
5	**验收管理检测与响应**	服务完成后，您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	● 以周期为单位进行计费，单次购买默认周期为1年。 ● 资源数最低需要购买数量为50，单次最多可购买数量为1000，实际费用以最终账单为准。
等保建设助手	● 支持基础版和高级版服务类型。 ● 以次数为单位进行周期计费，单次购买默认为1次，1次为1年的使用周期。 ● 可同时购买基础版和高级版，分别选择购买数量即可，单个版本最大可购买数量为1000，实际费用以最终账单为准。
专项版	● 支持云会议安全保障、特级安全保障和小型会议保障服务类型。 ● 以次数为单位进行周期计费，单次购买默认为1次，1次为1年的使用周期。 ● 初始最多保障50台ECS，超过50台需要增加系统数量或者资源数。 ● 购买是需分别选择系统数量、资源数或数量、增量包， – 云会议安全保障、特级安全保障的系统数量和资源数单次最大可购买数量为1000。 – 小型会议保障的数量单次最大可购买500，增量包单次最大可够买数量为1000。
密评建设助手	● 服务类型仅支持标准版。 ● 一次性付款使用，1次为一年的使用周期。 ● 单次最多可购买数量为1000，实际费用以最终账单为准。

计费项	计费说明
检查与加固	• 支持安全产品托管、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服务类型。 • 计费如下： – 安全产品托管：按年计费，单次购买为1年的使用周期，单次购买最大数量为500。 – 应急响应：按次计费，单次购买默认为1次，1次为1年的使用周期，最小需选择数量为10 ，最大可选择500。 – 网站安全体检：一次性付款，1次为1年的使用周期，单次最大可够买数量为1000。 – 主机安全体检：一次性付款，1次为1年的使用周期，单次最大可够买数量为1000。 – 安全加固：一次性付款，1次为1年的使用周期，单次最大可够买数量为1000。 – 攻击路径评估：一次性付款，1次为1年的使用周期，单次最大可够买数量为1000。

计费模式

管理检测与响应属于包周期计费，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，您可以参考**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、等保建设助手、专项版和密评建设助手均**属于一次性消费，不支持续费。到期后，需重新购买。

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。该服务提供您身份认证、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，您可以在华为云账号中给员工创建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。

如果华为云账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，您只需要为您账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部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问MDR时，不需要切换区域。

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：对账号中心、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。如果您已注册公有云，可直接登录管理控制台，在页面上方选择“区域”后，单击 ☰ ，选择“安全与合规 > 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	• 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。

子流程	说明
执行管理检测与响应	• 企业版 当订单成功支付后，管理检测与响应将快速响应并结合您实际业务场景，通过云服务方式，提供华为云安全标准化的运维运营服务。 • 等保建设助手 当订单成功支付后，管理检测与响应团队将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。 • 专项版 当订单成功支付后，管理检测与响应团队将为您进行会议安全保障服务，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 当订单成功支付后，管理检测与响应团队将为您提供“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。
验收服务	华为云安全专家上传服务报告后，本次管理检测与响应完成。 **说明** 检测完成后，系统自动生成管理检测与响应报告，并将报告保留15天，您可以在此期间下载并查看管理检测与响应报告。如果超出该时间范围，您需要获取管理检测与响应报告，请联系客服处理。

8 与其他云服务的关系

与消息中心的关系

消息中心是为您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。方便您日后的查询、审计和回溯，详情请参见**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
服务单验收通过	PSDM	professionalTicketsAcceptanceSuccess

操作名称	资源类型	事件名称
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 用户名是您身份的标识信息
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），您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。

服务单

服务单是您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。

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，让您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，协助您快速恢复业务。

