序号	大类	分类	服务项目
1	安全运维服务（专业版&企业版）	服务群	工单支持
			400电话支持
			邮件请求支持
			IM企业群在线咨询
2		ITSM	服务请求
			事件管理
			问题管理
			变更管理
3		云安全配置	访问控制安全配置
			功能设置与策略配置
			产品运行情况支撑
			配置项风险识别与策略优化
4		监测预警	云安全产品监控
			事件监测及告警管理
			威胁识别与策略调整
5		安全加固服务	云主机安全防护配置
			云安全产品防护配置
			PaaS产品安全防护
			安全基线加固
			应用层防护策略定制化
			安全组访问控制优化
6		专业级安全运营	资产梳理
			安全巡检服务
			协助修复及建议
			威胁情报通告
			安全事件研判分析
			网络安全威胁识别与原因分析服务

		安全值守	应急响应
7			制定值守方案
			安全值守巡检
			值守期间安全告警处理
			安全值守总结报告
8		报告	月报
9	安全运维服务（企业版）	风险评估管理（企业版）	主机漏洞评估
			应用安全漏洞评估
			互联网暴漏面检查
			网络边界隔离评估
			基线合规检查评估
			脆弱性评估/病毒评估
			敏感信息泄露检测
10		企业级安全运营（企业版）	安全运维规范
			事件处置流程定制
			持续性安全防护
			告警事件分析溯源
			业务安全规则优化
			规则用例（userCase）管理
			用户权限核验审计
			用户行为及API操作审计
			安全产品操作记录审计
			安全产品防护日志审计
11		应急演练（企业版）	制定应急演练方案
			应急演练实施


应急演练总结报告

新版安全运维服务（专业版 企业版）
详细描述
提供专属群工单支持，可通过微信页面，微信公众号提交服务工单；
提供 7x24hx365d 电话热线服务；
支持通过发邮件到我方指定邮箱的形式提出服务请求&事件；
提供IM沟通交流群支持；（仅限问题技术咨询、进度同步、在线讨论，不作为服务级别SLA统计对象）。
提供ITSM服务平台及IT服务管理流程，保障每个甲方请求&事情都得到有效及时的处理，并作为服务级别管理SLA指标的统计对象。
支持对云身份和访问控制相关配置使用管理。包括：腾讯-CAM、AWS-IAM、阿里云-RAM、华为云-IAM、Azure身份管理等。
针对客户云平台资源情况，通过安全产品的资产识别、网站接入、防护配置、告警及日志等功能的进行配置；根据业务运行情况和业务新增与变更情况，逐步对接入策略、防护配置策略、告警与日志策略进行优化等管理服务。
日常对云安全产品的运行情况与功能情况进行监控，对出现的各类运行问题、功能问题、告警或日志问题等，及时反客服团队并督促尽快解决，及时同步客户方运维团队或安全团队。
通过安全防护功能所反馈安全情况，以及与客户安全团队、运维团队在协作过程中所发现可能存在的关联安全策略或配置问题，将提供相关建议，或对必要的处理提供配合服务。
支持云厂商监控策略创建、配置、优化等配置操作；
日常监测云平台各安全产品告警信息，研判安全事件触发情况，及时发现事件、定义事件、处置事件，按需触发应急响应，高效管理告警信息，闭环安全运营相关工作；
定期分析监测预警信息，识别威胁趋势与风险脆弱项，及时对策略做出调整，提升安全运营效率；
提供漏洞修复、主机病毒及木马查杀、os安全配置(安全规范实施)、主机侧入侵防护策略与安全模块配置；
包括DDoS、WAF、云防火墙、主机安全、SSL证书配置、密钥管理等配置项管理
各公有云环境PaaS产品安全配置（白名单、访问控制策略），如 CDN、对象存储、云数据库等
各公有云环境使用云主机安全产品对主机基线进行扫描检查，对应用基线提供加固建议，OS基线配合提供加固服务；
提供应用漏洞修复建议；针对应用脆弱项或漏洞情况，提供临时自定义WAF防护策略，以及对访问IP进行黑白名单防护策略配置，直至应用漏洞或脆弱项得以彻底加固。
提供云资源安全组策略合规梳理及配置优化；云防火墙出入站ACL策略配置，及各VPC间的访问控制与优化。
梳理平台资产情况，包括公网IP、VPN、CLB、防火墙、CVM等资产和安全防护情况等，定期进行维护与整理。
针对安全防护或扫描功能进行全面的安全巡检服务，包括资产识别情况、网站接入情况、漏洞情况、基线风险情况、云平台配置情况、安全防护及攻击告警等情况、告警与统计报表情况、日志记录情况、访问控制与操作审计情况等等；安全巡检将体现在定期报告中。
针对安全防护建议、安全事件分析、威胁情报通告，提供专业的整改建议或配合运维侧、业务侧人员进行修复处置等服务。
持续关注行业内最新紧急安全风险、致命漏洞、威胁情报信息，以及平台业务场景，研判此威胁是否会影响业务系统连续性，提出处置建议，并通告各业务团队。
针对于已发生的安全事件，如勒索病毒、后门、挖矿等，提供专业的安全事件的研判与分析服务，依托安全日志、服务器操作记录、系统命令等维度分析安全事件告警原因以及影响程度等。
依托云安全产品的检测功能，对告警信息、安全相关的日志信息以及告警策略信息等，进行汇总梳理并进行深度分析与甄别研判，排查根本原因的服务。

针对已发生的安全事件，提供事件抑制、事件根除、事后分析、事后加固等快速应急响应和处置服务。

制定值守方案（值守时间、值守人员、值守地点、值守工作时长、云平台归属、安全产品范围界限、巡检范围界定、应急事件处置措施及流程）
按照值守方案（云平台归属、安全产品方位界限、巡检范围界定）的规定进行安全巡检，并在巡检结束后输出对应巡检结果。
值守期间如若发现有异常安全事件，将按照值守方案（应急事件处置措施及流程）模块进行响应并处理。
对此次安全值守工作进行总结，并输出总结报告。
每月提供《云安全报告》内容详情见服务SOW文件
针对云平台各主机资产，定期进行主机漏洞扫描，并给出漏洞修复方案；可采用云平台自带安全扫描功能，或提供开源扫描工具的评估服务；
对客户在线网站应用的安全漏洞扫描，检测漏洞出具扫描结果报告；
梳理暴漏在互联网上的云上资产，提供暴露面检测服务，帮助发现潜在的风险点，包括扫描IP、端口、域名、路径等；
梳理客户所有业务系统的网络架构，根据实际情况评估当前网络环境的风险，对云环境南北向边界防护、东西向访问控制、VPC业务隔离情况等进行扫描与评估，提出风险优化建议或整改方案；缩小业务系统在互联网上的暴露面，减少被入侵的风险
基于等保基线标准2.0 通用标准（OS、数据库、中间件、常用应用组件等），脆弱性或风险进行扫描评估，是否合规
梳理客户资产，进行全面病毒扫描，安全评估；
梳理客户关键字信息，通过相关软件在github等平台上进行敏感信息泄露检测，对检测出来的泄露点进行确认以及消除；
针对客户已有安全防护产品及用户使用情况，安畅团队将针对客户实际情况输出安全运维规范及操作流程，指导规范化执行安全运维操作。
制定安全事件的识别、响应处置、恢复和上报的全响应周期措施，指导响应与处置服务的流程与规范，并输出事件处置的SOP材料。
提供构建基于云环境整体的安全措施，进行全面的安全防护管理体系，从系统安全防护到满足等保安全合规审计，再到日常安全运行管理以及安全情报、风险分析防御、安全事件应急处置与整体安全架构优化建议等服务内容。
针对于已发生的安全事件，进行攻击链逐级分析，并对攻击源头进行溯源及复现，梳理安全事件告警根因以及影响程度等，形成事件分析报告。
贴合业务侧安全告警信息，依赖SOC和SIEM平台收集到的各类安全日志进行深度分析，制定BOT行为特征、恶意爬虫行为识别、恶意URI研判、潜在恶意IP分析等业务安全规则与策略，形成贴合业务场景的防护规则与目标特征的封禁征罚策略
针对SOC和SIEM平台的日志，将各项目积累的规则用例（userCase）进行适配与优化，符合业务场景的深度防护与告警机制，对高持续APT攻击行为、CC攻击特征、DDOS攻击行为等日志信息及时进行告警发现，并持续完善规则用例（userCase）
按照等保2.0要求及业务场景，落实用户权限三权分立原则，即配置、授权、审计的权限划分，包括用户权限及API权限管理，并进行定期核验审计。
按照行业要求和客户内部安全规范对用户操作和API调用记录进行定期审计。
定期为安全产品的操作记录、安全产品防护日志进行审计，包括云平台安全防护产品以及部署的三方安全产品，以及主机安全产品、防火墙、waf、堡垒机、VPN等等相关安全产品的操作记录进行审计。
根据应用系统特征，制定对应的个性化应急演练方案（演练时间、演练地点、演练环境、演练参与人员、安全工具说明、演练流程说明）
根据应急演练方案，在规定时间、规定环境进行应急演练。使用（木马入侵、挖矿病毒、网页防篡改）等入侵方式对演练服务器进行入侵攻击，使用的安全工具为（菜刀、一句话木马、挖矿程序）等，入侵成功之后即可进入应急响应流程，对入侵事件进行抑制止血，之后进行加固溯源处置，使用的安全工具为（河马、D盾、火

输出应急演练总结报告。

必要支持限制	专业版	企业版	频次	限制
华为云平台	✔	✔	无限制	
华为云平台	✔	✔	无限制	
云平台自带安全功能、第三方安全产品	✔	✔	每月	
云平台自带安全功能监测告警、第三方安全告警； 以及告警接入消息、webhook接入企微公告警群等；	✔	✔	每月	
云平台自带功能：阿里云安全中心、腾讯云主机安全、华为云企业主机安全、AWS云Amazon Inspector、Azure云Defender for Cloud	✔	✔	每月	
云平台自带安全功能，第三方安全软件功能				
云平台自带PaaS产品功能				
云平台自带安全功能				
云平台自带安全功能				
云平台自带安全功能				
云平台自带 资产管理系统	✔	✔	每月1次	
云平台自带、自动化巡检工具	✔	✔	每周	
云平台自带	✔	✔	每月	
云平台自带/行业公开	✔	✔		
云平台自带、SIEM平台、LogParser、火绒剑、河马、D盾	✔	✔		
云平台自带	✔	✔		

云平台自带、日志分析工具、后门排查工具、系统命令等	✔	✔		
云平台自带安全功能，第三方安全软件功能	16H/年	48H/年	标准服务累计16H/年 专业服务累计48小时	超期另计
云平台自带	✔	✔	1次/月	
云平台自带、人工	×	✔	1次 (接入时或续约期)	
云平台自带、人工				
云平台自带、人工				
云平台自带、人工				
云平台自带、人工				
云平台自带、人工				
云平台自带、人工				
云平台自带	×	✔	入场提供1次	边界限制需要明确！材料按照科目提供标准版
云平台自带			入场提供1次	
云平台自带	×	✔	每季度1次	
业务应用防护产品（如WAF、云防火墙等），开通安全日志查询与告警日志查询功能；	×	✔	每周	必须依赖应安全产品，并且开通日志服务功能。
SOC和SIEM平台日志分析功能，如Splunk、QRadar、态势感知平台等；				
云平台自带功能、安全审计记录表	×	✔	1季度/次	
云平台自带安全功能、第三方安全软件功能、开源安全组件等	×	✔	2次/年	

交付物
/
/
/
/
/
邮件通报 按需
《安全事件分析报告》 按需

《安全值守总结报告》	
《MSS月度分析报告》	
《风险评估报告》 接入/续约期进行一次	
标准流程规范材料：包括sow、sla、sop	
《事件分析报告》中呈现	
《季度安全内审记录报告》	
《应急演练报告》