广东省科学院网络安全运营建设项目

技术需求书

2021 年 6 月 4 日

目录

一、 项目背景

在实施创新驱动发展战略的大背景下，网络安全和信息化是事关国家安全和国家发展的重大战略问题。广东省科学院作为广东实施创新驱动发展的一支重要战略科技力量，已建设成为国内一流的省级科学院。为保障广东省科学院及下属分支机构的重要业务网络系统免遭外部危险因素干扰，逐步收缩外部暴露面，为广东省科学院健康稳定可持续发展保驾护航，故发布广东省科学院及分支机构网络安全运营体系的建设需求。

二、 总体要求

1、 标有“★”的条款为必须完全满足的实质性要求，投标人如有一项带“★”的条款未响应或负偏离，将按无效投标处理。

2、 标有“▲”的条款为重要性要求，投标人如有“▲”的条款未响应或负偏离的将被严重扣分。

3、 投标人在响应详细内容中需列出具体数值或明确承诺。如果投标人只注明“正偏离”或“无偏离”，将被视为“负偏离”，从而可能导致影响评标结果。

4、 ★中标后三个工作日内，供应商提供样机进行上述功能要求的逐一测试验证，全部通过后才能执行合同流程，测试中发现虚假应标的行为将予以废标处理并保留对该厂商追究相关责任的权利；

5、 投标人没有在投标文件中注明偏离（文字说明或在用户需求应表注明）的参数、配置、条款视为被投标人完全接受 。

6、 投标人应保证，采购人在中华人民共和国使用该货物或货物的任何一部分时，免受第三方提出的侵犯其专利权、商标权、著作权或其它知识产权的起诉。

三、 投标报价要求

1、 本次投标报价采用的币种为人民币。

2、 投标报价应包含设备安装及验收、设备开发所需软硬件购置费用，维护服务费，交通、材料、税费等一切不可预见的全部费用。

四、 需求采购清单

序号	产品名称	产品描述	单位	数量
一、终端安全管理系统				
1	终端安全管理控制中心	集中管控平台，需支持软件部署。提供三年服务。	套	1
2	PC 终端安全管理客户端	防病毒、补丁修复、统一运维管控功能客户端软件（Windows PC 终端）。	套	150
3	服务器终端安全管理客户端	防病毒，补丁管理功能功能客户端软件（Windows 服务器系统）。	套	2
二、SD-WAN 分支互联系统				
1	SD-WAN 管控平台	统一管控总部 SD-WAN 网关、分支 SD-WAN 网关，支持软件化部署。提供三年维保服务。	套	1
2	SD-WAN 一级网关	SD-WAN 硬件平台，网络吞吐≥4.5G，支持 VPN、防火墙、应用识别、URL 过滤、病毒防御、入侵防护功能，提供三年维保服务。	台	3
3	SD-WAN 二级网关	SD-WAN 硬件平台，网络吞吐≥	台	9

		4G，支持 VPN、防火墙、应用识别、URL 过滤、病毒防御、入侵防护功能。 提供三年维保服务。		
三、态势感知运营系统				
1	总部态势感知平台	以 3 台物理服务器实现平台集群。 支持外部威胁检测，采集数据源的统一分析，整网态势感知功能。 提供三年维保服务。	套	1
2	一级流量采集探针	采集探针硬件平台，网络采集性能≥1Gbps。提供三年维保服务。	台	2
3	二级流量采集探针	采集探针硬件平台，网络采集性能≥600Mbps。提供三年维保服务。	台	10
4	态势感知运营服务	提供安全运营人员基于态势感知平台的运营服务，针对突发安全事件提供现场应急响应服务。	年	1

五、 技术参数要求

5.1. 终端安全管理系统技术参数

序号	指标项	指标要求
1	产品配置	★控制中心 1 套；150 套 Windows PC 客户端（防病毒、补丁管理、运维管控），2 套 Windows Server 客户端（防病毒、补丁

		管理）；支持信创版本替换；
2	系统管理	控制中心：采用 B/S 架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理、准入控制以及各种报表和查询等功能；
3		支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行；
4	资产管理	按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；支持硬盘序列号收集、支持 SN 号收集；
5		支持温度检测以折线图形式实时展示 CPU、主板、显卡、硬盘的温度变化；
6		支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件；
7		▲支持正版软件的正版序列号的读取功能，确保软件正版化；（提供功能截图并加盖厂商公章）
8	日志报表	展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表；
9		展示指定时间段内指定终端修复漏洞，病毒查杀，木马查杀的情况；
10		要求支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人。邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等
11	防病毒功能	支持病毒木马威胁的快速扫描、全盘扫描、强力扫描、文件专杀、隔离区恢复、系统修复、插件管理；

12		立体防护系统，包含浏览器防护，系统防护，入口防护和隔离防护 4 大类，其中浏览器防护包含网页防护，看片防护，网购防护，搜索防护，首页锁定，默认浏览器防护，邮件安全防护。系统防护包含摄像头防护，键盘记录防护，文件系统防护，驱动防护，进程防护，注册表防护。入口防护包含下载安全防护，U 盘防护，黑客入侵防护，漏洞入侵防护，DNS 防护，局域网防护。隔离防护包含可疑程序隔离防护；
13		文件系统实时防护，支持开机延迟加载，实时监控级别设置高中低三种配置，监控文件类型包含所有文件或者程序及文档。选择级别高监控所有文件对系统有一定影响，需要根据设备配置启用配置；
14		能够监控间谍文件，拦截局域网病毒，宏病毒免疫，DLL 劫持免疫；
15		支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置；
16		▲检测 QQ、MSN、阿里旺旺等常用聊天软件传输文件的安全性，确保传输文件不中毒；对方发来网址的安全性，聊天软件传输某些文件会添加“.重命名”，如果文件安全，将自动去除“.重命名”；（提供功能截图并加盖厂商公章）
17		可对备份区、隔离区的文件进行有效管理。能够对单个、指定的文件和全部文件，进行文件的删除、恢复等多项管理措施；
18		▲对敲诈者病毒提供专有的防护功能；（提供功能截图并加盖厂商公章）
19	补丁分发与漏洞修复	要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、功能性补丁等修复类型；
20		支持按 CVE 编号查询漏洞，支持按 KB 号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况，如果还有未修复的终端则可立即下发修复任务；

21		▲简化补丁运维工作，支持补丁灰度发布，支持设置对特定分组优先进行补丁分发，自定义测试一段时间后再全网升级，实现补丁自动化运维；（提供功能截图并加盖厂商公章）
22		终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁；
23		▲产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能；（提供功能截图并加盖厂商公章）
24	防病毒+补丁管理（Windows服务器）	至少支持 Windows Server 2003、2008、2012、2016 版本操作系统平台的杀毒防护与漏洞管理，并可对 Windows Server 2003 提供后续漏洞防护。
25		为阻止入侵者关闭或者破坏客户端防护、以及放行勒索病毒，将阻止服务器客户端退出和卸载，终端无法添加信任和开发者信任，客户端无法关闭自我保护，禁止应用程序加载驱动。
26	运维管控	▲支持终端在互联网 NAT 环境下的远程控制；（提供功能截图并加盖厂商公章）
27		可监控指定终端网络、应用程序的上传，下载速度与流量；
28		支持软件分发，分发前条件检查，分发任务执行详情及失败重发；
29		▲支持禁用安全模式或者设置安全模式登录密码；（提供功能截图并加盖厂商公章）
30		支持对终端桌面系统的账号密码、本地安全策略、控制面板、屏保与壁纸、浏览器安全、杀毒软件检查；
31		支持能耗管理，支持定时关机策略，规定时间提示倒计时关机；支持终端工作时间外的开机告警；
32		▲支持对终端各种外设（USB 存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB 口、串口、并口、1394、PCMIA）设置使用权限；（提供功能截图并加盖厂商公章）

33		支持自定义外设黑白名单，且支持分组执行、支持以设备名称或者 PID/VID 例外；
34	产品服务	★提供原厂三年软件升级服务

5.2. SD-WAN 分支互联系统技术参数

5.2.1. SD-WAN 管控平台技术参数

序号	指标项	指标要求
1	部署模式	★平台产品支持 SaaS 化、虚拟化、软硬件一体化部署；
2	CPE 配置	▲支持导出一个或多个指定 CPE 设备的配置向导，可实现批量化上线 CPE 设备；（提供功能截图并加盖厂商公章）
3		支持在设备注册上线过程中，通过双向认证向设备进行认证并授权；
4		支持设备在每次加电/指定时间，与设备进行配置比对，确保配置一致性；
5		支持为指定的 CPE 设备或 CPE 设备组下发配置；
6		▲支持自定义业务及对业务进行编排，后台自动下发业务编排对应的路由及隧道配置，不需要管理员再手动配置路由和隧道；（提供功能截图并加盖厂商公章）
7		支持为不同安全级别的 CPE 下发不同的模板；
8		支持为指定的 CPE 设备或 CPE 设备组添加上网配置；
9	智能流量调度	支持基于全网路径的探测，可探测全网链路的丢包率、时延、抖动、跳数，实现基于全网最优路径的选路策略；
10		▲当某条链路失效或者是链路质量过差不可用时，会主动下发策略让相应的 SD-WAN 网关切换路径到当前最优链路；（提供功能截图并加盖厂商公章）

11	监控管理	▲支持在地图上展示所有CPE的基础信息及CPE之间的数据传输通道信息和状态；（提供功能截图并加盖厂商公章）
12		支持通过监控大屏，集中展示当前全网组网图、站点健康度、隧道状态、链路状态、威胁活动；
13	运维管理	支持统一展示管理下发给指定CPE的配置、CPE系统升级、CPE库升级及许可下发的任务进度及任务状态；
14		▲对指定设备进行重启或版本切换；（提供功能截图并加盖厂商公章）
15		可通过管理平台下发ping测试指令，并将ping结果信息回传管理平台；
16		▲可通过SD-WAN控制器SSH访问、WEB访问CPE设备；（提供功能截图并加盖厂商公章）
17		可通过管理平台下发抓包指令，并将抓包信息回传管理平台；
18	产品服务	★提供原厂三年软件升级服务

5.2.2. **SD-WAN一级网关技术参数**

序号	指标项	指标要求
1	规格性能	★千兆电口≥6个，Console接口≥1个，USB接口≥2个，整机吞吐量≥4.5G，最大并发连接数≥200万，IPSec隧道吞吐量≥400M，隧道数≥200条，设备规格≥1U，冗余电源；
2	部署模式	支持网关和单臂方式部署；
3	系统可靠	▲支持双系统，支持故障时启动备份系统；（提供功能截图并加盖厂商公章）
4	接口	接口支持WAN/LAN互转，不限制接口的WAN/LAN属性；
5	DHCP	支持作为DHCP服务器为内网用户分配IP地址、网关及DNS；
6	路由	支持静态路由、策略路由、OSPF、BGP；

7	NAT	支持基于源 NAT、目的 NAT；
8	DNS	支持 DNS 代理；支持内网 DNS 访问路径优化；
9	隧道加密	▲支持国际算法；支持商密 SM2/SM3/SM4 算法；（提供功能截图并加盖厂商公章）
10	预配置向导	引导用户完成 SD-WAN CPE 与 SD-WAN 控制器建立连接所需配置。配置下发后自动保存。
11		支持通过静态 IP、PPPoE、DHCP、4G/LTE 方式连接 SD-WAN 控制器。
12	零配置上线	CPE 与 SD-WAN 控制器建立连接并认证通过后可自动获取所属的完整配置，不需要分支本地人员人工配置；
13		▲支持通过预配置向导、批处理脚本、邮件、无线方式上线；（提供功能截图并加盖厂商公章）
14		支持专线 IP、DHCP、PPPoE、4G/LTE 场景下的零配置上线
15	故障线路切换	链路出现故障时立即切换到备份线路并上报 SD-WAN 控制器；
16		▲主链路故障修复后，由 SD-WAN 控制器下发切换指令从备份链路切回主链路；（提供功能截图并加盖厂商公章）
17	安全功能	支持下一代防火墙功能，可基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、服务、应用、时间下发安全策略；
18		▲通过漏洞防护功能，配合安全策略可以对特定的网络、服务、应用、用户进行识别，对隐藏在正常数据中利用漏洞的异常行为进行阻断。同时，漏洞防护功能集成了暴力破解防护，可实现针对 FTP、SMTP、POP3、IMAP、MYSQL 协议的暴力破解防护功能；（提供功能截图并加盖厂商公章）
19		▲通过防间谍软件功能，配合安全策略可针对木马后门、病毒蠕虫、僵尸网络对特定网络、服务、应用、用户进行防护，拦截间谍软件的攻击行为；（提供功能截图并加盖厂商公章）
20		▲支持通过对 HTTP、SMB 和 FTP 方式上传、下载文件、页面，

		或对 SMTP、POP3、IMAP 协议发送的电子邮件及其附件等进行病毒扫描，并可以根据扫描结果进行相应的处理；（提供功能截图并加盖厂商公章）
21		预置应用识别特征库，应用识别库≥3000+；
22		支持本地 URL 识别，通过 URL 分类识别能够快速发现并识别可疑网站，能有效的防御挂马网站、钓鱼网站；
23	产品服务	★提供原厂三年软硬件升级服务，三年特征库升级服务

5.2.3. **SD-WAN 二级网关技术参数**

序号	指标项	指标要求
1	规格性能	★千兆电口≥6 个，千兆光口≥1 个，Console 接口≥1 个，USB 接口≥2 个，整机吞吐量≥4G，最大并发连接数≥20 万，IPSec 隧道吞吐量≥300M，隧道数≥100 条，设备规格≥1U，单电源；
2	部署模式	支持网关和单臂方式部署；
3	系统可靠	▲支持双系统，支持故障时启动备份系统；（提供功能截图并加盖厂商公章）
	接口	接口支持 WAN/LAN 互转，不限制接口的 WAN/LAN 属性；
4	DHCP	支持作为 DHCP 服务器为内网用户分配 IP 地址、网关及 DNS；
5	路由	支持静态路由、策略路由、OSPF、BGP；
6	NAT	支持基于源 NAT、目的 NAT；
7	DNS	支持 DNS 代理；支持内网 DNS 访问路径优化；
8	隧道加密	▲支持国际算法；支持商密 SM2/SM3/SM4 算法；（提供功能截图并加盖厂商公章）
10	预配置向导	引导用户完成 SD-WAN CPE 与 SD-WAN 控制器建立连接所需配置。配置下发后自动保存；
11		支持通过静态 IP、PPPoE、DHCP、4G/LTE 方式连接 SD-WAN 控

		制器；
12	零配置上线	CPE 与 SD-WAN 控制器建立连接并认证通过后可自动获取所属的完整配置，不需要分支本地人员人工配置；
13		▲支持通过预配置向导、批处理脚本、邮件、无线方式上线；
14		支持专线 IP、DHCP、PPPoE、4G/LTE 场景下的零配置上线；
15	故障线路切换	链路出现故障时立即切换到备份线路并上报 SD-WAN 控制器；
16		▲主链路故障修复后，由 SD-WAN 控制器下发切换指令从备份链路切回主链路；（提供功能截图并加盖厂商公章）
18	安全功能	支持下一代防火墙功能，可基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、服务、应用、时间下发安全策略；
19		▲通过漏洞防护功能，配合安全策略可以对特定的网络、服务、应用、用户进行识别，对隐藏在正常数据中利用漏洞的异常行为进行阻断。同时，漏洞防护功能集成了暴力破解防护，可实现针对 FTP、SMTP、POP3、IMAP、MYSQL 协议的暴力破解防护功能；（提供功能截图并加盖厂商公章）
20		▲通过防间谍软件功能，配合安全策略可针对木马后门、病毒蠕虫、僵尸网络对特定网络、服务、应用、用户进行防护，拦截间谍软件的攻击行为；（提供功能截图并加盖厂商公章）
21		▲支持通过对 HTTP、SMB 和 FTP 方式上传、下载文件、页面，或对 SMTP、POP3、IMAP 协议发送的电子邮件及其附件等进行病毒扫描，并可以根据扫描结果进行相应的处理；（提供功能截图并加盖厂商公章）
23		预置应用识别特征库，应用识别库≥3000+；
22		支持本地 URL 识别，通过 URL 分类识别能够快速发现并识别可疑网站，能有效的防御挂马网站、钓鱼网站；
23	产品服务	★提供原厂三年软硬件升级服务

5.3. 态势感知系统技术参数

5.3.1. 总部态势感知平台技术参数

序号	指标项	指标要求
1	部署方式	支持集群部署，基于大数据架构可水平扩展至多台设备集群；
2	硬件配置	★满足如下硬件平台资源 3 台以上： CPU：2 颗 10 核 CPU 主频 2.20GHz 以上； 内存：256G DDR4 内存； 系统盘：960GB 及以上固态硬盘 2 块，并提供 Raid 进行备份； 存储盘：48TB 企业级 SATA 盘； 网卡：4 个千兆电口及 2 个万兆光口； 电源：冗余电源； 提供 250 个数据源的采集能力； 集群实时处理事件性能 20000EPS，支持扩展到 100000EPS 的处理性能能力；集群支持百亿级日志秒级查询；
3	数据采集与存储	支持接入并管理日志采集器、流量采集器，可支持第三方采集器接入；
4		支持对日志采集器进行采集配置并下发；提供 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、agent 等采集方式；支持对网络设备、主机系统等安全日志、网络流量以及业务信息等多种数据源的采集；
5		▲日志接入支持界面交互式配置，简化日志接入复杂度，通过图形化界面配置日志解析条件，利用正则表达式、分隔符、Key-Value、JSON 等方法定义解析规则，实现灵活的日志格式范式化，系统自动生成解析规则，无需通过代码编写解析规则；（提供功能截图并加盖厂商公章）

6		支持自定义过滤规则功能，通过配置 AND、OR 等嵌套关联逻辑、条件及丰富的操作符来实现复杂的日志过滤需求，减少无用日志数量；
7		支持自定义富化规则功能，可引用值映射表来实现富化规则，达到字段转换和丰富日志信息的目的；
8	威胁情报	▲支持本地威胁情报的检索，检索类型支持域名、IP 地址、文件 MD5 值；威胁情报内容支持 IOC、攻击链阶段、置信度、类型描述、威胁家族、攻击事件/团伙、影响平台、情报状态、威胁描述等；（提供功能截图并加盖厂商公章）
9		支持云端威胁情报查询，支持 IP、域名威胁类型分类，流行度评估，创建时间、更新时间、过期时间查看，支持开源情报判定对比、相关样本分析、情报拓线分析、历史 A 记录信息、注册信息（包含域名注册人、注册人所属组织、管理员邮箱、电话、传真、所属国家、服务运营商等），支持查看关联域名，域名数字证书等信息；
10		能够自定义威胁情报，支持类型包含 IP、MD5、域名、URL、IP 地址:Port、IP 地址：URI、IP:Port/URI、域名:Port、域名:Port/URI。支持自定义 IPv6 的威胁情报；
11	资产管理	▲支持管理资产主机设备、网络设备、安全设备、应用系统等资产类型管理；（提供功能截图并加盖厂商公章）
12		支持资产详情信息的展示，能够展现资产基础信息（资产名称、IP 地址、分组、厂家、型号、操作系统类型、物理地址、资产使用状态等）；
13		支持资产服务信息管理，支持对服务的 IP 地址、端口号、服务名、服务版本、协议、Banner 等服务属性进行管理，支持对 IPV6 资产的管理；
14		支持资产分组管理；支持资产组的批量导入，提供预制的资产组导入模板；

15		支持通过网络流量被动发现资产信息、支持通过脆弱性发现资产信息，资产信息至少包含：IP 地址、服务、服务版本、协议、端口、操作系统、主机名、mac 等；
16	威胁预警	支持对重大网络安全事件（如永恒之蓝，Struts 2 漏洞利用等新生大面积爆发的严重事件）进行威胁预警。通过厂商对重大网络安全事件的追踪生成预警包，并赋能分发给用户。支持通过预警包导入完成网络安全事件的影响面评估，并持续的跟进事态的发展，快速完成重大网络安全事件的预警及处置；
17		▲针对此类风险支持统计潜在风险资产数、受攻击资产数、失陷资产数以支持对重大网络安全事件（如永恒之蓝，Struts 2 漏洞利用等新生大面积爆发的严重事件）进行威胁预警。通过厂商对重大网络安全事件的追踪生成预警包，并赋能分发给用户。支持通过预警包导入完成网络安全事件的影响面评估，并持续的跟进事态的发展，快速完成重大网络安全事件的预警及处置；（提供功能截图并加盖厂商公章）
18	脆弱性管理	▲支持导入第三方漏洞扫描报告，漏洞可自动关联匹配到影响的资产，支持漏洞标签添加、删除、编辑、检索，支持对漏洞批量添加标签信息支持通过 CVE 编号和 CNNVD 编号关联漏洞知识库中的信息；支持通过 CVE 编号和 CNNVD 编号关联漏洞知识库中的信息；（提供功能截图并加盖厂商公章）
19		配置核查可自动关联匹配到影响的资产，支持配置核查标签添加、删除、编辑、检索，支持对配置核查批量添加标签信息；
20	关联分析	支持接入各种类型数据包括但不限于：设备日志、网络流量、失陷类威胁情报数据、资产数据、漏洞数据等数据进行关联分析，支持对 IPV6 日志进行关联分析；
21		▲支持上百种规则语义，并提供 420+条预置规则；支持类 VISIO 的图形化连线拖拽的交互配置方式而非编辑逻辑语法树配置方式，以降低操作配置难度；灵活组合规则建模中的计算

		单元，计算单元至少包括关联分析、统计分析和序列分析等以应对不同威胁场景建模；（提供功能截图并加盖厂商公章）
22		支持基于规则的告警动作设置，比如基于规则，触发告警后通过短信、邮件、系统消息、企业微信等至少四种途径通知告警的发生，并支持配置通知频率。支持告警发生后，自动下发工单，推进告警处置动作。支持告警发生后，自动下发联动处置封禁任务和命令；
23	告警管理	支持对告警进行批量操作，支持告警状态变更、添加到工单任务、添加到调查任务等。支持导入和导出告警记录。支持告警标签管理功能；支持标签的增删改查；告警信息可直接调用工单系统，告警信息可直接添加到调查任务，支持添加到已有任务或创建新的调查任务；
24		告警详情中支持关联与告警/告警集合相关的告警基本信息、告警趋势信息、威胁情报、相关网段、资产，资产的漏洞详细信息和触发告警的日志信息；
25		告警详情中能够关联与该告警相关的原始告警和相关日志信息，能直观了解与该告警关联的日志、事件、资产、情报、漏洞等信息列表；
26	攻击者分析	支持从攻击者视角对最近 30 天时间范围的告警进行归纳分析，列表展示包括：攻击者 IP、IP 归属地、IP 来源、攻击手段、攻击链阶段、最高危害等级、受害者 IP 数、威胁告警数、首次攻击时间、最新一次攻击时间。
27	事件调查	▲支持通过创建调查任务对威胁事件和可疑事件进行调查分析，通过人工调查分析确定威胁以及威胁的严重程度和影响范围；调查任务中可添加完整的：日志数据、告警数据、漏洞数据、弱口令数据、配置核查数据、自定义富文本数据（调查分析者从其他途径获取的相关数据）；支持对以攻击者和受害者情况视角对调查任务中的数据做统计分析；支持调查结果的图

		形化展示；（提供功能截图并加盖厂商公章）
28	工单处置	并对工单处理流程对告警事件、漏洞、弱口令及配置核查问题进行跟踪；
29		支持对最近 1 天、7 天、30 天等维度以仪表视图的方式展示新增工单量、处置中工单量、处置工单、工单处置周期分布、新增工单变化趋势、处置中工单优先级分布、新增工单状态分布、责任人处置工单排行、责任人新增工单排行、最近的工单等统计数据；
30	联动处置	▲支持对终端安全管理系统联动设备下发的联动处置命令，命令包含 ：全网终端隔离特定文件，特定终端隔离特定文件、终端隔离（被隔离终端只能访问控制中心）；（提供功能截图并加盖厂商公章）
31		支持对接第三方防火墙，可以自定义处置命令封装，简化下发联动处置命令的复杂度，当发现失陷主机、恶意域名等威胁事件后，可实现快速下发联动处置命令且自定义配置联动处置命令支持对生效时长的配置；
32	日志统计	支持对最近 1 天、7 天、30 天等维度以仪表视图的方式展示日志总量、流量日志总量、日志变化趋势、日志采集器日志数量、各类型日志统计等统计数据；
33	报表管理	提供快速/周期报表功能，可指定报表统计的时间范围、内容、执行时间，快速生成各种临时性的报表统计结果，也可根据选定的周期以及周期开始时间生成以日、周、月、季度、年为跨度的报表，报表内容可自定义，能自动生成报表并通过邮件、短信、消息中心、企业微信发送给指定责任人，提供 PDF、Word、HTML 三种格式的报表下载；
34	态势大屏展示	支持大屏的轮播投放，支持设定轮播投放时间间隔、轮播时大屏是否展示以及大屏的轮播顺序。

35		支持全局风险态势和每个资产组节点的风险态势计算（包括风险值、资产数量、威胁数量、脆弱性数量），支持统计 TOP30 的风险最高的资产组和风险最低的资产组；支持轮播展示资产组的风险情况，支持统计最近 30 天的风险趋势；
36		▲支持通过 3D 地图炮/2D 世界地图/2D 中国地图展示外部威胁攻击，可以统计外部威胁总数、受攻击 IP 总数和受攻击资产总数，TOP5 的受攻击资产，威胁来源国家/地区的分布情况，TOP5 的攻击源 IP，支持按威胁级别统计威胁分布情况，按威胁类型统计威胁分布情况，统计最近 30 天的威胁分布情况，支持对内部 IP 自定义区域位置，并在地图炮展现该区域；（提供功能截图并加盖厂商公章）
37		▲支持可视化呈现内网中是否存在威胁告警，威胁是否在内网网络中蔓延，能够聚焦于核心资产网段，提供对攻击者维度和受害者维度的攻击情况分析，对威胁类型、等级和趋势等进行统计呈现。支持发现内网中的攻击者，以帮助快速定位内网威胁的根源。提供相关统计数据的详情查看能力。支持最近 30 天时间范围内的数据统计；（提供功能截图并加盖厂商公章）
38		支持从综合风险值、资产数量、威胁数量、脆弱性数量和日志接入量五个维度展示综合安全情况；
39	系统管理	▲支持用户角色管理，可以为不同角色赋予不同系统功能模块及数据的读写权限，未赋予此模块读写权限的用户，将无此功能模块的显示或配置的权限；（提供功能截图并加盖厂商公章）
40		▲支持通过邮件方式、短信方式、企业微信方式发送系统消息通知；（提供功能截图并加盖厂商公章）
41		支持系统巡检功能，检测系统当前是否存在异常或者需要特意关注状态；支持在线查看巡检结果和导出巡检结果，巡检结果至少保留 7 次以上；
42	产品服务	★提供原厂三年软硬件升级服务，三年威胁情报升级授权，三

		年漏洞知识库升级授权

5.3.2. 一级流量采集探针

序号	指标项	指标要求
1	硬件配置	★千兆电口≥6 个，Console 口≥1 个，扩展板卡插槽≥2 个；企业混合流应用层吞吐量≥1Gbps，HTTP 并发连接数≥300 万，每秒 HTTP 新建连接数≥10 万/秒；
2	部署模式	支持通过流量镜像的方式旁路部署在数据链路中，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断 TCP 威胁会话连接，支持通过流量被动识别资产；
3	数据采集策略	▲支持基于源地址、目的地址、服务、流量采样比、时间进行选择数据采集对象，可以针对采集对象进行网络流量数据采集和威胁检测数据采集，网络流量数据采集支持自定义流量载荷的格式和流量上下行载的长度；（提供功能截图并加盖厂商公章）
4		支持基于 SSL 协议的 HTTPS 流量进行解密，可添加基于源地址、目的地址的解密策略；
5	流量日志采集提取能力	▲支持 VXLAN、GRE、VLAN 报文解析；（提供功能截图并加盖厂商公章）
6		支持解析、生成及外发 TCP 流量日志。包括：传感器序列号、TCP 数据流的结束方式、TCP 数据流开始的时间、源 IP、源端口、目的 IP、目的端口、源 mac、目的 mac、协议、上行字节数、下行字节数、客户端系统信息、服务端系统信息、TCP 流的统计信息等字段；
7		支持解析、生成及外发 UDP 流量日志。包含：传感器序列号、UDP 数据流开始的时间、UDP 数据流结束的时间、源 ip、源端

		口、目的 ip、目的端口、源 mac、目的 mac、协议、上行字节数、下行字节数、上行包数、下行包数字段；
8		▲支持解析、生成及外发 Web 访问日志。包括：传感器序列号、日志生成时间、源 ip、源端口、目的 ip、目的端口、HTTP 请求方法、HTTP 包头的 URI 字段、uri_md5 值、host 字段、host_md5 值、origin 字段、cookie 字段、ser-Agent 字段、referer 字段、链接来源、原始数据、http 状态码、Content 类型等字段；（提供功能截图并加盖厂商公章）
9		支持解析、生成及外发域名解析日志。包括：时间、源 ip、源端口、目的 ip、目的端口、DNS 访问类型、Host、Host 字段_MD5 值、地址资源、MX 记录、响应结果状态、域名规范名称等字段；
10		▲支持 FTP/SMB/TFTP 三种协议的解析、生成及外发文件传输日志。包括：传感器序列号、协议、日志生成时间、客户端 IP、客户端应用端口、服务端 IP、服务端应用口、传输模式、文件名字、文件 md5、文件类型等字段；（提供功能截图并加盖厂商公章）
11		支持解析、生成及外发 LDAP 行为日志。包括：传感器序列号、协议、日志生成时间、源 ip、源端口、目的 ip、目的端口、用户名、LDAP 版本、ldap 操作类别、op 的具体操作描述等字段；
12		支持解析、生成及外发 ftp、smb、oracle、mysql、mssql、postgresql、ssh、pop3、smtp 协议的登陆动作日志。包括：日志生成时间、源 ip、源端口、目的 ip、目的端口、协议、登陆密码、登陆结果、用户名等字段；
13		▲支持解析、生成及外发 pop3、smtp、imap、webmail 协议的邮件行为日志。包括：传感器序列号、协议、message-id 信息、生成时间、源 ip、源端口、目的 ip、目的端口、邮件发

		送/接收时间、邮件抄送人、主题、被当前邮件回复的邮件 ID、密送人、附件名字、回访路径、邮件实际接收者、附件 md5、mime_type、邮件正文等字段；（提供功能截图并加盖厂商公章）
14		支持解析、生成及外发 Oracle、MySQL、MSSQL、PostgreSQL、MongoDB、DB2、Redis 等协议的数据库操作日志。包括：传感器序列号、日志生成时间、源 ip、源端口、目的 ip、目的端口、协议、协议版本、用户、数据库类型、数据库操作返回的状态信息、操作信息等字段；
15		支持分析多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB；可执行文件还原格式包含：EXE、DLL、OCX、SYS、COM、apk 等；压缩文件还原格式包含：RAR、ZIP、GZ、7Z 等；文档类型的还原格式包含：word、excel、pdf、rtf、ppt 等；
16	流量威胁检测能力	▲支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库≥3000+；（提供功能截图并加盖厂商公章）
17		支持实现基于威胁情报的失陷主机检测及日志外发；
18	产品服务	★提供原厂三年软硬件升级服务，三年特征库升级服务

5.3.3. 二级流量采集探针

序号	指标项	指标要求
1	硬件配置	★千兆电口≥6 个，Console 口≥1 个，扩展板卡插槽≥2 个；企业混合流应用层吞吐量≥600Mbps，HTTP 并发连接数≥200 万，每秒 HTTP 新建连接数≥8 万/秒；

2	部署模式	支持通过流量镜像的方式旁路部署在数据链路中，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断 TCP 威胁会话连接，支持通过流量被动识别资产；
3	数据采集策略	▲支持基于源地址、目的地址、服务、流量采样比、时间进行选择数据采集对象，可以针对采集对象进行网络流量数据采集和威胁检测数据采集，网络流量数据采集支持自定义流量载荷的格式和流量上下行载的长度；（提供功能截图并加盖厂商公章）
4		支持基于 SSL 协议的 HTTPS 流量进行解密，可添加基于源地址、目的地址的解密策略；
5	流量日志采集提取能力	▲支持 VXLAN、GRE、VLAN 报文解析；（提供功能截图并加盖厂商公章）
6		支持解析、生成及外发 TCP 流量日志。包括：传感器序列号、TCP 数据流的结束方式、TCP 数据流开始的时间、源 IP、源端口、目的 IP、目的端口、源 mac、目的 mac、协议、上行字节数、下行字节数、客户端系统信息、服务端系统信息、TCP 流的统计信息等字段；
7		支持解析、生成及外发 UDP 流量日志。包含：传感器序列号、UDP 数据流开始的时间、UDP 数据流结束的时间、源 ip、源端口、目的 ip、目的端口、源 mac、目的 mac、协议、上行字节数、下行字节数、上行包数、下行包数字段；
8		▲支持解析、生成及外发 Web 访问日志。包括：传感器序列号、日志生成时间、源 ip、源端口、目的 ip、目的端口、HTTP 请求方法、HTTP 包头的 URI 字段、uri_md5 值、host 字段、host_md5 值、origin 字段、cookie 字段、ser-Agent 字段、referer 字段、链接来源、原始数据、http 状态码、Content 类型等字段；（提供功能截图并加盖厂商公章）
9		支持解析、生成及外发域名解析日志。包括：时间、源 ip、

		源端口、目的 ip、目的端口、DNS 访问类型、Host、Host 字段_MD5 值、地址资源、MX 记录、响应结果状态、域名规范名称等字段；
10		▲支持 FTP/SMB/TFTP 三种协议的解析、生成及外发文件传输日志。包括：传感器序列号、协议、日志生成时间、客户端 IP、客户端应用端口、服务端 IP、服务端应用口、传输模式、文件名字、文件 md5、文件类型等字段；（提供功能截图并加盖厂商公章）
11		支持解析、生成及外发 LDAP 行为日志。包括：传感器序列号、协议、日志生成时间、源 ip、源端口、目的 ip、目的端口、用户名、LDAP 版本、ldap 操作类别、op 的具体操作描述等字段；
12		支持解析、生成及外发 ftp、smb、oracle、mysql、mssql、postgresql、ssh、pop3、smtp 协议的登陆动作日志。包括：日志生成时间、源 ip、源端口、目的 ip、目的端口、协议、登陆密码、登陆结果、用户名等字段；
13		▲支持解析、生成及外发 pop3、smtp、imap、webmail 协议的邮件行为日志。包括：传感器序列号、协议、message-id 信息、生成时间、源 ip、源端口、目的 ip、目的端口、邮件发送/接收时间、邮件抄送人、主题、被当前邮件回复的邮件 ID、密送人、附件名字、回访路径、邮件实际接收者、附件 md5、mime_type、邮件正文等字段；（提供功能截图并加盖厂商公章）
14		支持解析、生成及外发 Oracle、MySQL、MSSQL、PostgreSQL、MongoDB、DB2、Redis 等协议的数据库操作日志。包括：传感器序列号、日志生成时间、源 ip、源端口、目的 ip、目的端口、协议、协议版本、用户、数据库类型、数据库操作返回的状态信息、操作信息等字段；

15		支持分析多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB；可执行文件还原格式包含：EXE、DLL、OCX、SYS、COM、apk 等；压缩文件还原格式包含：RAR、ZIP、GZ、7Z 等；文档类型的还原格式包含：word、excel、pdf、rtf、ppt 等；
16	流量威胁检测能力	▲支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库≥3000+；（提供功能截图并加盖厂商公章）
17		支持实现基于威胁情报的失陷主机检测及日志外发；
18	产品服务	★提供原厂三年软硬件升级服务，三年特征库升级服务

5.3.4. 运营服务技术参数

序号	指标项	指标要求
1	日常运营服务	安全运营人员需每天远程通过态势感知平台对整网安全动态做值守监控，发现在严重高危告警及时通报并协助整改；
2		当遇到突发信息安全事件，如病毒攻击、网络勒索、APT 等事件，投标人需采取应急措施，限制事件扩散和影响范围，协助进行事件的处置。
3		安全运营人员需根据实际要求，按月/季/年输出网络风险分析报告，包含但不限安全事件告警监控、安全加固建议协助使用方进行整改；
4	服务期限	安全运营服务期限≥1 年；

六、 服务要求

6.1. 技术支持服务

1、 投标人需承诺为保障本次项目所投产品稳定运行，提供产品维保期内的专项技术支持服务，并在投标文件中详细说明；

2、 投标人需在投标文件中详细说明本次项目所投产品维保期满后，每年的收费维护内容及服务方式、范围。

6.1.1. 服务年限

1、 本次项目所投软件产品提供原厂制造商三年授权升级服务；

2、 本次项目所投硬件设备提供原厂制造商三年维保服务；

3、 本次项目所配备态势感知运营服务须提供一年服务期。

6.1.2. 服务内容

软件更新服务

1、 本次项目所供软件产品及硬件设备，授权维保在服务期内，可享受当前可升级范围内的版本、规则库升级服务；

2、 当官方发布针对本次项目所供产品的重大补丁时，投标人须经过必要性测试并及时通知，如双方针对更新升级达成一致，投标人须协助完成补丁的更新加固。

远程支持服务

1、 通过热线电话支持服务提供在线支持，通过在线交流、语音方式向用户提供问题诊断，以判断问题原因并提供解决方案；

2、 提供远程服务支持，经用户授权同意，技术人员通过远程方式连接用户使用相关产品的应用现场，进行查看、定位、诊断，提供解决方案及应用指导。

现场支持服务

如通过电话热线及远程支持均无法解决产品问题，投标人须提供现场支持服务，服务时间为周一至周五 9:00-18:00 期间 30 分钟响应，2 小时内到场；非工作时间为 2 小时响应，4 小时内到场；自接到问题报障在 4-8 小时内提供解决方案。

6.2. 培训服务

6.2.1、 实施交付服务

投标人中标并完成项目实施交付后，需针对用户运维人员、关键岗位专员提供系统化的专业培训，目的为了让用户相关人员掌握本项目所供产品的基本运维使用和排障方法，并输出相关电子文档培训课件。

6.2.2、 版本升级培训

当官方发布针对本次项目产品的重大版本时，投标人应当协助用户完成重大版本更新，并提供新版本运维使用培训，目的帮助用户运维人员完善专业知识及技能。

七、 验收标准

1、 验收的标准按照国家最新相关标准实施（若无国家标准按行业标准）；
2、 验收流程由中标人给出科学可行性的验收报告，并经由采购人认可，方可进行验收；
3、 验收测试的过程和结果必须详细记录，测试中如发现设备性能指标或功能上不符合招标文件和合同要求时，将被看作性能不合格，用户有权拒收并要求赔偿；
4、 技术文件和资料：所有设备必须提供电子版使用说明书、操作手册、维护手册等技术文件和资料。