临安区昌化人民医院HIS配套设施升级及技术服务项目合同

甲方（采购人）：杭州市临安区国瑞健康产业投资有限公司

乙方（供应商）：浙江赢科慧康科技有限公司

甲、乙双方根据杭州市临安区国瑞健康产业投资有限公司关于项目编号为LA[2019]1483号的临安区昌化人民医院HIS配套设施升级及技术服务项目竞争性磋商的结果，签署本合同。

一、货物和服务内容及合同价格

金额单位： 元

名称	型号规格	配置要求	数量	单价	小计
服务器	联想 SR860	详见附件	2台	100000	200000
存储	联想 DE6000H	详见附件	1台	400000	400000
互联网出口防火墙	深信服 AF-1000-D420	详见附件	1套	70000	70000
服务器防火墙	深信服 AF-1000-D600P	详见附件	1台	90000	90000
内网边界防火墙	深信服 AF-1000-D440D	详见附件	1台	90000	90000
日志审计	深信服 LAS-1000-A600	详见附件	1台	90000	90000
行为管理	深信服 AC-1000-C400Y	详见附件	1台	80000	80000
数据库审计	深信服 DAS-1000-A620	详见附件	1台	120000	120000
杀毒软件	深信服 EDR	详见附件	1套	50000	50000
光纤交换机扩容	赢科定制	详见附件	1项	41000	41000
测评服务	赢科定制	详见附件	1项	100000	100000
系统集成	赢科定制	详见附件	1项	95000	95000
合　计					1426000
合同总价大写：壹佰肆拾贰万陆仟元整				小写：￥1426000.00	

注：1、产品技术指标、数量及使用单位地址等详见附件清单；

2、以上合同总价包括货款、备品备件、专用工具、人工、运杂、包装、装卸、安 装、调试、验收、培训、保修、售后服务、技术服务、保险、购买及制作标书、风险、 税金、采购代理服务费等为完成本次项目涉及的一切费用。属于完成本次项目所必需的 但乙方未列入报价的费用将被视为乙方优惠，甲方均不予支付。

二、双方责任

1、甲方责任

在本合同签订后 10 天内，组建一个由甲方领导、相关职能科室负责人参加的系统实施领导小组，负责系统实施的组织协调工作；组建一个由主管领导、相关职能科室人员参加的系统实施工作小组，负责系统安装调试过程的具体事宜。

2、乙方责任

乙方指定操春洪为本合同的负责人，代表乙方在合同履行过程中行驶权利和履行义务，其他任何未经授权人员的任何签字、承诺均不发生法律效力。

乙方负责对合同项目系统运行必须的计算机硬件、网络提出合理化建议。

在甲方提供的条件符合后，乙方负责在合同约定期限内完成安装调试运行工作，待甲方验收合格后或视验收合格后交付甲方正式使用。

三、技术资料

1. 乙方应按采购文件规定的时间向甲方提供使用货物的有关技术资料。

2. 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。

五、产权担保

乙方保证所交付的货物的所有权完全属于甲方且无任何抵押、查封等产权瑕疵。

六、转包或分包

本合同范围内的货物，应由乙方直接供应，不得转让他人供应（但系统接口改造部分允许转包、分包），否则，甲方有权解除合同并追究乙方的违约责任。

七、质保期

硬件产品质保期3年（验收合格之日起计算）。

八、工期、交货地点

1. 工期：合同签订后12个月内完成设备采购并安装调试运行完成。投标人应切实做好项目进度管理规划，在确保项目质量和安全的原则下，控制项目进度，以便在规定期限内通过验收。

2. 交货方式及交货地点：乙方将产品送到甲方指定地点，所产生的相关费用由乙方承担。

九、货款支付及发票

合同签订后七个工作日内，由甲方支付合同总价的40%预付款，设备安装调试完成后七个工作内，由甲方支付合同总价的50%，验收通过后七个工作日内，由甲方支付合同总价的10%。

合同共1426000元内发票分为两部分开取：第一部分为货物类增值税专用发票（税点：13%），第二部分为技术服务类增值税专用发票（税点：6%）

十、税费

本合同执行中相关的一切税费均由乙方负担。

十一、质量保证、售后服务及培训

1. 乙方保证本合同中所供应的商品是最新研发的符合国家技术规格和质量标准的出厂原装合格产品。如发生所供商品与合同不符，甲方（使用方）有权拒收或退货，由此产生的一切责任和后果由乙方承担。

2. 乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑶退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

3. 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

4. 售后服务：

1）在整个使用期内，乙方应确保设备的正常使用。提供 24 小时技术支持热线，30 分钟内电话响应，2 小时之内上门维修，12 小时内解决问题；不能当场修复的，必须采取提供备品、备件或备机等措施，以保证采购单位的正常使用。

2）质保期内上门维修，必须出具维修服务单，服务单应包括：用户姓名、联系方式、报修时间、上门时间、完成维修时间、报修设备信息、维修情况等内容，并由用户签字。

3）免费服务期满后，乙方以合同金额的15%向甲方收取每年的维护费，以提供长期、不间断的技术服务。

上述货物在质保期内免费维护、升级，因人为因素出现的故障不在免费保修范围内。超过保修期的系统，终生维护，维护时只收工时费。

十二、调试和验收

1. 甲方对乙方提交的货物依据招标文件上的技术规格要求和国家有关质量标准进行现场验收。货到后，甲方需在 7 个工作日内验收。

2. 乙方交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

3. 甲方对乙方提供的货物在使用前进行调试时，乙方需负责安装并培训甲方的使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验收。

4. 对技术复杂的货物，甲方应请国家认可的专业检测机构参与验收，并由其出具质量检测报告。

5. 验收时乙方必须在现场，验收完毕后作出验收结果报告；验收费用由乙方负责。

十三、货物包装

1. 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

2. 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

十四、违约责任

1. 甲方无正当理由拒收货物的，甲方向乙方偿付拒收货款总值的百分之五违约金。

2. 甲方无故逾期验收和办理货款支付手续的，甲方应按逾期付款总额每日万分之五向乙方支付违约金。

3. 乙方逾期交付货物的，乙方应按逾期交货总额每日千分之六向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期30个工作日不能交货的，甲方可解除本合同。乙方因逾期交货或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值0.5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

4. 乙方所交的货物技术指标、质量不符合合同规定及招标文件

规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

十五、不可抗力事件处理

1. 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3. 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

十六、诉讼

双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向甲方所在地法院起诉。

十七、合同生效及其它

1. 合同经甲、乙双方签字并加盖单位公章后生效。

2. 合同执行中涉及采购资金和采购内容修改或补充的，必须签订书面补充协议后，方可作为主合同不可分割的一部分。

3. 招标文件、投标文件与本合同具有同等法律效力。

4. 本合同未尽事宜，遵照《合同法》有关条文执行。

5. 本合同一式 5 份，具有同等法律效力，甲、乙双方各执 2 份，鉴证方执 1 份。

甲方（盖章）：杭州市临安区国瑞健康产业投资有限公司

法定代表人：

或受委托人（签字）：

联系人：

地址：浙江省杭州市临安区锦南街道九州街 599 号

电话：0571-61066311

传真：

开户银行：兴业银行临安支行

账号： 358530100100208962

日期：2019年12月31日

乙方（盖章）：浙江赢科慧康有限公司

法定代表人：

或受委托人（签字）：

联系人：操春洪

地址：浙江省杭州市临安区锦城街道国瑞中心北区（北幢106）

电话：0571-63710385

传真：0571-23658255

开户银行；上海浦东发展银行杭州分行临安支行

账号： 95080154700001108

日期：2019年12月31日

鉴证方（盖章）：杭州西成建设管理有限公司

法定（授权）代表人：

地址：临安区衣锦街596号农资大楼二楼

电话：0571-23616815

传真：0571-23616807

日期：2019年12月31日

附件清单

1.3.3.1 服务器

项目	要求
品牌	国产主流品牌
外观	4U 机架式服务器
处理器	配置两个 Intel 至强可扩展处理器 5117(主频 2.0GHz，14 核)金牌处理器，最大可扩展至 4 个 28 核处理器
内存	配置 6*64GB 2666GHz DDR4 RDIMM
	标配 48 条内存插槽
硬盘	配置 2*480GB 企业级 2.5" SSD 硬盘；
阵列卡	配置 1 块阵列卡含 2GB 闪存(带超级电容保护)，支持 RAID0/1/10/5/50/ ，可选缓存最大可升级至 8GB
网卡	配置 4 个千兆以太网端口,1 个独享的管理端口
HBA	配置 1 块双口 16Gb FC HBA 卡
电源	满配电源输出功率 750W 80+铂金电源，热插拔冗余电源
	支持 110V AC 到 220V AC 自适应
风扇	满配冗余热插拔系统风扇，支持带故障预报警功能的；支持 N+1 冗余
I/O 扩展	最大支持 6 个可用的 PCIe 插槽及一个为 M.2 适配器预留的专用接口
	支持 iOS 和安卓系统手机 APP 管理服务器
工作温度	支持 ASHARE A4 标准，工作温度 5° C 到 45° C
带外管理	1、提供专用管理端口 2、提供 IPMI 企业版功能，并支持 Redfish 3、支持以 java 或者 h5 模式进行带外管理 4、UI 功能菜单简明清晰 5、具备电源功耗图形显示 6、支持查看 RAID 级别、硬盘、内存、CPU 等具体型号信息
	7、支持命令行修改 BIOS 设置 8、支持虚拟介质 HTTP URL 挂载 9、支持 Syslog 告警

统一管理软件	配置数据中心资源平台统一管理软件，该软件具有适用于 VMware vCenter 和 MircoSoft System Center 系统管理 能实现设备批量裸机安装操作系统，可支持 25 个设备同时部署；另外需要管理监控原有老旧服务器存储设备
认证报告	合同签订前提供 CCC、中国环境标志产品认证、中国节能产品相关证明文件。
操作系统	支持主流操作系统，本次配置 Windows Server 2016 标准版一套，可降级到 Windows Server 2012 版本
服务	3 年 7x24 小时保修服务以及硬盘介质保留服务，全国所有省份设有服务站，为保证设备的可靠性服务，签订合同时提供原厂针对本项目售后服务承诺函原件，在设备使用城市拥有备件库。

1.3.3.2 存储

指标项	技术参数
品牌	国产知名品牌，与服务器同品牌
存储架构	高速点对点传输总线，双控制 Active-Active 架构
存储缓存	双控制器缓存本次实配容量 32GB（不含任何性能加速模块、FlashCache、PAM 卡，SSD Cache 等），最大可扩展至 128GB
	缓存具备 UPS 断电保护功能， 在出现电源故障时，可提供充足的电源，将高速缓存内容转储至非易失性内部存储设备上（非通用服务器架构）。
前端主机通道接口	本次双控配置：4*16Gb+8*32Gb 主机接口；配置 4 个 16Gb FC 模块；预留 8 个 32Gb 主机端口用于扩展。具备控制器在线主机接口 IO 模块热拔插功能。
主机接口类型	支持 8/16Gbps FC、1/10Gbps iSCSI 以及智能 IO 卡(4 口，同时支持 8/16Gb FC、10GE)，或更高配置。
硬盘规格	双控制器下最大支持磁盘数量 480 个，本次实配硬盘数量规格如下： 20*1.2TB 10K SAS 硬盘和 4*800GB SSD 硬盘。
支持 RAID	支持 RAID 1、RAID 10、RAID50、RAID 5、RAID6 等可选配置
性能	设备 4KB 情况下随机读 IOPS100 万；顺序读带宽 20GBps
可维护性	磁盘、电源、IO 模块都可以不停机热插拔。
快速恢复	提供故障快速恢复技术，能够保障硬盘失效后的故障时间最短，减少风险。
资源使用效	配置存储快照功能许可，支持快照数量 500 个。

率提升	配置 SSD 二级缓存许可。
可管理性	有功能全面，图形化的管理软件，包括：盘阵，卷管理软件。配置存储的图形化管理配置和监控软件。
制造商资质	合同签订前提供中国环境标志认证产品证书、中国节能产品认证证书、CCC 认证等
保修及安装服务	1、 原厂 3 年 7*24 硬件保修以及硬盘介质不返还服务，设备生产商需在国内设有技术服务热线； 2、 原厂提供安装调试服务，原厂在杭州地区设立备件库； 3、 签订合同时提供原厂针对本项目售后服务承诺函原件

1.3.3.3 互联网出口防火墙

指标项	主要技术参数
性能配置	网络层吞吐量:5G;应用层吞吐量:550M;并发连接数:1800000;新建连接数（CPS）:35000;电源:单电源;尺寸:1U;接口:4 电 2 光;
部署及网络特性	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式，支持链路聚合功能，支持端口联动
基础功能	能够识别应用类型超过 1200 种，应用识别规则总数超过 3000 条；
	支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能；
	支持基于应用类型，网站类型，文件类型进行流量控制，支持基于 IP 段、时间、国家/地区、认证用户、子接口和 VLAN 进行流量控制；
	访问控制规则支持数据模拟匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；
	支持场景化的配置向导功能，可以选择不同的部署方式以及使用场景实现产品的快速实施；
DoS 攻击防护	支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护、支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测；
	支持对信任区域主机外发的异常流量进行检测，如 ICMP，UPD，SYN，DNS Flood 等 DDoS 攻击行为；

内容安全	内置病毒样本数量超过 200 万； 支持应用协议命令级控制，如 FTP 可细化到 rmdir、get、put 等命令级控制； 支持压缩文件查杀
	支持从多维度聚合分析主机的中毒情况，并根据主机的夜间外联次数，恶意访问 IP 分布，云鉴情报等多个维度
	支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告；
入侵防护	为了保证入侵防御系统识别的专业性，要求入侵防护漏洞规则特征库数量在 7400 条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号，参考信息和建议的解决方案；
	为了帮助管理员更好的应对一些突发的热点安全事件，要求设备可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；
Web 应用安全防护	具备独立的 Web 应用防护规则库，Web 应用防护规则总数在 3500 条以上；
	支持对 web 页面黑链进行检测；
	支持对网站的恶意扫描防护和恶意爬虫攻击防护；支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等；（提供相关功能截图证明）
	支持针对网站的漏洞扫描进行深度防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测，支持基于目录访问频率和敏感文件扫描等恶意扫描行为进行防护；
	支持对已经植入 webshell 后门的服务器持续检测，对后续非法的通信动作进行识别和阻断；
	设备需要具备 web 业务自学习能力，可自行判断与标记业务特征，确认业务模型学习趋势；
僵尸主机检测	设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等，特征总数在 60 万条以上；
	支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机 IP 地址；
	支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；
	支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；
安全可视化	支持业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；

	支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息；
	支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险；
	支持自动生成综合安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的统计，具备有效攻击行为次数统计和攻击举证；
安全管理中心	为了更好的管理多台设备，要求支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能。
	支持安全策略一体化配置，通过一条策略既可实现不同安全功能的配置；
	支持 SD-WAN 智能选路功能；
	支持高级威胁事件分析，并展示热点事件详情，如全网威胁情报、高级黑客、持续性攻击、网站存在后门（webshell）、黑链、感染流行僵尸网络、大面积病毒感染、外发攻击等，并将高危事件推送到运维管理员手机微信端进行预警；
其他	投标时提供原厂针对本项目授权书和 3 年原厂质保函，签订合同时提供样机进行测试比对，测试结果未达到技术文件要求时，采购人有权拒签合同并取消中标资格，采购人亦有权选择第二中标人。

1.3.3.4 服务器防火墙

指标项	主要技术参数
品牌	与互联网出口防火墙同品牌
性能配置	网络层吞吐量:7G;应用层吞吐量:700M;并发连接数:1800000;新建连接数（CPS）:50000;电源:单电源;尺寸:1U;接口:6 电 2 万兆光口；
部署及网络特性	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式，支持链路聚合功能，支持端口联动
基础功能	能够识别应用类型超过 1200 种，应用识别规则总数超过 3000 条；
	支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能；
	支持基于应用类型，网站类型，文件类型进行流量控制，支持基于 IP 段、时间、国家/地区、认证用户、子接口和 VLAN 进行流量控制；

	访问控制规则支持数据模拟匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；
	支持场景化的配置向导功能，可以选择不同的部署方式以及使用场景实现产品的快速实施；
DoS 攻击防护	支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护、支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测；
	支持对信任区域主机外发的异常流量进行检测，如 ICMP，UPD，SYN，DNS Flood 等 DDoS 攻击行为；
内容安全	内置病毒样本数量超过 200 万； 支持应用协议命令级控制，如 FTP 可细化到 rmdir、get、put 等命令级控制； 支持压缩文件查杀；
	支持从多维度聚合分析主机的中毒情况，并根据主机的夜间外联次数，恶意访问 IP 分布，云鉴情报等多个维度；
	支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告；
入侵防护	为了保证入侵防御系统识别的专业性，要求入侵防护漏洞规则特征库数量在 7400 条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号，参考信息和建议的解决方案；
	为了帮助管理员更好的应对一些突发的热点安全事件，要求设备可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；
Web 应用安全防护	具备独立的 Web 应用防护规则库，Web 应用防护规则总数在 3500 条以上；
	支持对 web 页面黑链进行检测；
	支持对网站的恶意扫描防护和恶意爬虫攻击防护；支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等；
	支持针对网站的漏洞扫描进行深度防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测，支持基于目录访问频率和敏感文件扫描等恶意扫描行为进行防护；
	支持对已经植入 webshell 后门的服务器持续检测，对后续非法的通信动作进行识别和阻断；

	设备需要具备 web 业务自学习能力，可自行判断与标记业务特征，确认业务模型学习趋势；
僵尸主机检测	设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等，特征总数在 60 万条以上；
	支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机 IP 地址；
	支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；（提供截图证明）
	支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；
安全可视化	支持业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；
	支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息；
	支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险；
	支持自动生成综合安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的统计，具备有效攻击行为次数统计和攻击举证；
安全管理中心	为了更好的管理多台设备，要求支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能。
	支持安全策略一体化配置，通过一条策略既可实现不同安全功能的配置；
	支持 SD-WAN 智能选路功能；
	支持高级威胁事件分析，并展示热点事件详情，如全网威胁情报、高级黑客、持续性攻击、网站存在后门（webshell）、黑链、感染流行僵尸网络、大面积病毒感染、外发攻击等，并将高危事件推送到运维管理员手机微信端进行预警；

1.3.3.5 内网边界防火墙

指标项	主要技术参数
品牌	与服务器防火墙同品牌

性能配置	网络层吞吐量:6G;应用层吞吐量:650M;并发连接数:1800000;新建连接数（CPS）:40000;电源:冗余电源;尺寸:1U;接口:4 电 4 光;
部署及网络特性	支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式，支持链路聚合功能，支持端口联动
基础功能	能够识别应用类型超过 1200 种，应用识别规则总数超过 3000 条;
	支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能;
	支持基于应用类型，网站类型，文件类型进行流量控制，支持基于 IP 段、时间、国家/地区、认证用户、子接口和 VLAN 进行流量控制;
	支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机 IP 地址;
	支持场景化的配置向导功能，可以选择不同的部署方式以及使用场景实现产品的快速实施;
DoS 攻击防护	支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护、支持 SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测;
	支持对信任区域主机外发的异常流量进行检测，如 ICMP，UPD，SYN，DNS Flood 等 DDoS 攻击行为;
内容安全	内置病毒样本数量超过 200 万; 支持应用协议命令级控制，如 FTP 可细化到 rmdir、get、put 等命令级控制; 支持压缩文件查杀
	支持从多维度聚合分析主机的中毒情况，并根据主机的夜间外联次数，恶意访问 IP 分布，云鉴情报等多个维度
	支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告;
入侵防护	为了保证入侵防御系统识别的专业性，要求入侵防护漏洞规则特征库数量在 7400 条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应 CVE 编号，参考信息和建议的解决方案;
	为了帮助管理员更好的应对一些突发的热点安全事件，要求设备可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则

Web 应用安全防护	具备独立的 Web 应用防护规则库，Web 应用防护规则总数在 3500 条以上；
	支持对 web 页面黑链进行检测；
	支持对网站的恶意扫描防护和恶意爬虫攻击防护；支持其他类型的 Web 攻击，如文件包含，目录遍历，信息泄露攻击等；
	支持针对网站的漏洞扫描进行深度防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测，支持基于目录访问频率和敏感文件扫描等恶意扫描行为进行防护；
	支持对已经植入 webshell 后门的服务器持续检测，对后续非法的通信动作进行识别和阻断；
	设备需要具备 web 业务自学习能力，可自行判断与标记业务特征，确认业务模型学习趋势；
僵尸主机检测	设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等，特征总数在 60 万条以上；
	支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机 IP 地址；
	支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；
	支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；
安全可视化	支持业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；
	支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息；
	支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险；
	支持自动生成综合安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的统计，具备有效攻击行为次数统计和攻击举证；
安全管理中心	为了更好的管理多台设备，要求支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能。
	支持安全策略一体化配置，通过一条策略既可实现不同安全功能的配置；
	支持 SD-WAN 智能选路功能；
	支持高级威胁事件分析，并展示热点事件详情，如全网威胁情报、高级黑客、持续性攻击、

	网站存在后门（webshell）、黑链、感染流行僵尸网络、大面积病毒感染、外发攻击等，并将高危事件推送到运维管理员手机微信端进行预警；
其他	投标时提供原厂针对本项目授权书和3年原厂质保函，签订合同时提供样机进行测试比对，测试结果未达到技术文件要求时，采购人有权拒签合同并取消中标资格，采购人有权选择第二中标人。

1.3.3.6 日志审计

指标项	主要技术参数
品牌	与内网边界防火墙同品牌
产品结构	要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁；
产品架构	采用标准2U机架式硬件
操作系统	深度定制优化的Linux系统；
管理方式	B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端；
设备部署	提供旁路接入模式，设备部署不影响原有网络结构；
性能配置	主机审计许可证书50；硬盘容量2T；接口：6个千兆电口；；支持获取各种主流网络及数据库访问行为，支持Syslog、WMI、OPSEC Lea、SNMP trap和LAS-1000专用协议等协议事件日志，支持通过Http、Https、FTP、SFTP、SMB等协议获取各类文件型日志，支持基于SQL/XML标准内容获取；
数据采集	1.支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、GIftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、GIftpd、Serv-u]； 2.支持SNMP日志采集，支持日志类型：网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神] 3.支持Opsec Lea日志采集； 4.支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、

	MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览、论坛微博]、入侵检测、业务检测、流量监控； 5.支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储； 6.支持文本型日志原始文件管理，可将系统作为日志服务器使用；
监控功能	1.支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况； 2.支持自定义配置实时监控的日志类型； 3.支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警； 4.支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况； 5.支持实时监控系统当前运行状态，包括系统CPU、内存、硬盘状态及管理员操作；
报表分析功能	1.系统内置多种类报表模板； 2.支持动态\静态（日报、周报、月报）两种系统生成方式； 3.支持报告的邮件转发、生成提醒功能；支持多人邮件接收； 4.支持自定义审计报告； 5.支持导出html、Excel、PDF； 6.支持管理员自定义审计报表模板；
查询分析功能	1.支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索； 2.支持以日志类型、时间范围及条件字段快速检索过滤； 3.支持高级检索以多条件组合查询方式，可以将每一个日志字段作为查询条件进行查询； 4.支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件； 5.支持查询模版创建、修改、删除功能； 6.支持查询结果导出；
策略管理功能	1.支持内置归并策略，对HTTP数据进行自动归并处理； 2.支持内置关联分析策略，可设定用户在规定时间内连续多次输入错误口令产生告警或事件； 3.支持数据策略，可设定采集多种WEB访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问； 4.支持自定义创建实时审计规则：根据日志字段为条件预设置分析策略； 5.规则条件设定支持逻辑运算符与支持正则表达式； 6.支持自定义三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息； 7.支持以告警页面、短信、邮件、SYSLOG、SNMP等各种方式呈现告警信息；
数据管理功	1.支持按日志属性、日志类型、时间范围进行数据备份；

能	2.支持 WEB 界面备份及日志恢复导入工作； 3.支持自动与手动两种备份归档方式； 4.系统支持以 FTP 上传方式将归档文件存储到第三方存储系统中；
系统自身安全	系统内置安全防火墙；支持控制访问审计主机范围； 必需提供内部通讯检查机制，传输 128 加密； 管理接口支持串口或电口的方式管理； 管理界面与其他功能模块分离；
日志数据安全	审计日志文件方式存储； 审计日志加密导出审计系统； 支持对所有审计管理员操作审计系统的动作进行审计；
日志权限	审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明； 支持日志类型、IP 地址权限设置； 支持页面功能模块权限设置；
其他	投标时提供原厂针对本项目授权书和 3 年原厂质保函，签订合同时提供样机进行测试比对，测试结果未达到技术文件要求时，采购人有权拒签合同并取消中标资格，采购人有权选择第二中标人。

1.3.3.7 行为管理

指标项	主要技术参数
品牌	与日志审计同品牌
性能配置	带宽性能:200Mb；支持用户数:600；电源:单电源；尺寸:1U 接口:4 电
集中管理	多台设备支持通过统一平台集中管理、集中配置等；
部署方式	要求设备支持网关模式，支持 NAT、路由转发、DHCP 等功能；支持网桥模式，以透明方式串接在网络中；支持旁路模式，无需更改网络配置，实现上网行为审计； 支持两台及两台以上设备同时做主机的部署模式；
IPv6 支持	支持部署在 IPv6 环境中，设备接口及部署模式均支持 ipv6 配置； 所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持 IPv6；
IPsec VPN	须具有 IPSec VPN 远程加密访问和连接的模块，并能提供 IPSec VPN 客户端授权远程接入访问； 支持配置主备线路组和流量分配模式的多线路选路策略；（提供产品界面截图）

链路负载	为了提高出口多链路利用率，要求支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载。支持使用 VPN 做专线备份； 支持链路故障检测
多线路技术	网关必须能同时连接多条外网线路，且支持多条线路流量复用和智能选择流速最快线路的技术 虚拟多线路:必须支持将多条外网线路虚拟映射到设备上，实现对多线路的分别流控
终端管理	支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等； 支持检测 windows 重要补丁的安装情况，并反馈检测结果； 系统识别：支持识别终端操作系统版本、系统补丁安装情况；
业务需要	为减少短信费用投入，要求设备支持微信身份验证，用户可以通过微信“扫一扫”、关注公众号等操作获取上网权限，后台能够记录下用户微信的 ID，支持与第三方微信平台对接，无需修改第三方平台代码对私接无线上网的行为管理,要求设备能自动发现网络中通过无线上网的热点和移动终端的 IP 和终端类型，匹配管理员配置的热点信任列表，对信任列表外非法接入的热点和终端能够进行阻止上网，支持冻结用户 IP，并通过邮件形式告警通知管理员，支持显示以 IP 或用户名的维度统计一段时间内的趋势图。 为确保单位不会通过 SSL 加密内容发生通过互联网出口泄密事件,要求设备必须能够识别并过滤 SSL 加密的钓鱼网站、金融购物网站；识别和审计加密的邮箱（如 GMAIL）等 针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向 web 访问质量检测（提供配置界面截图证明）
应用识别规则库	支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖 6 大类；此外可根据我单位需求自定义标签，根据标签做应用控制；
应用控制	设备内置应用识别规则库，支持超过 6700 条应用规则数，支持超过 2800 种以上的应用，1000 种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率； 能够对百度网盘、百度文库等网络应用的上传动作进行细分控制
移动应用的细分控制	支持对移动应用的细分权限控制，微信：微信网页版、微信传文件、微信朋友圈、微信游戏。移动 QQ：QQ 传文件、QQ 视频语音等； 支持对 QQ 远程桌面、teamview 等远程控制应用做细分控制，如：接受对方远程控制；
URL 访问及	要求设备内置海量的 URL 地址库，可根据访问 URL 的网页关键字进行过滤控制，特别对于 SSL

关键字控制	加密的网页、论坛、BBS 上的发帖行为也需要支持关键字过滤控制
流控黑名单	基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中
认证黑名单	每条认证策略提供黑名单功能，在黑名单中的用户不能通过认证上线。
动态流控	要求设备可以针对整体线路或者某流量通道内流量情况进行实时监控,根据设定的流量空闲值自动的调整流控控制策略，提升带宽使用率
P2P 智能流控	支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；
流控黑名单	基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中
移动 APP 审计	支持常见论坛（天涯社区、猫扑社区、百度贴吧、新浪论坛、搜狐社区等）、微博（新浪）、新闻评论类（腾讯新闻、网易新闻、搜狐新闻、新浪新闻）的移动 APP 内容审计
IM 审计	支持对 QQ（客户端版本）、阿里旺旺、万德（Wind）、路透等应用的聊天，群聊天等内容的审计； 支持记录 QQ、微信传文件动作和传文件内容，并可记录传文件类型和文件长度；
SSL 加密内容审计和过滤	针对 SSL 加密的网站、论坛发帖、web 邮箱的内容进行关键字过滤和内容审计；支持 SSL 硬件加速卡解密，从而可提高 SSL 全流量解密性能；
加密证书自动分发	审计 SSL 网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台 PC 单独安装证书的问题
网络整体状况报表	设备能根据管理者自定义的风险行为特征自动挖掘并输出离职风险、泄密风险、安全风险、工作效率风险、法律风险智能报表
单用户行为分析	针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）
下钻分析	下钻查询 在流量时长分析、用户行为分析、终端接入分析等纬度相关页面支持对统计结果的向下钻取查询
数据分析应用	数据中心可以对上网日志进行大数据分析，并支持多个大数据分析模型，包括泄密分析、离职倾向分析、上网态势分析、带宽分析、工作效率分析。
病毒查杀	必须具有防火墙功能模块； 设备可扩展支持业界知名杀毒引擎； 必须能查杀网页、Email、FTP 等流量中的病毒；

数据中心	要求设备必须支持将审计数据备份到外置数据中心，实现海量存储；必须支持通过USBKEY方式对数据中心管理员进行身份验证，确保我单位核心数据不会外泄；
支持与多种网安日志平台对接	内置多套日志模板与各省市网安日志平台对接，至少支持以下平台：派博、任子行、网博、云辰、烽火、中新软件、兆物、新网程、美亚柏科、爱思等。
其他	投标时提供原厂针对本项目授权书和3年原厂质保函，签订合同时提供样机进行测试比对，测试结果未达到技术文件要求时，采购人有权拒签合同并取消中标资格，采购人有权选择第二中标人。

1.3.3.8 数据库审计

功能指标	指标要求
品牌	与行为管理同品牌
性能要求	吞吐量400M，数据库流量比200Mb/s，日志10亿条/天，日志留存180天，日志检索20000条/秒，SQL吞吐10000条SQL语句/s，标准1U机架式，单电源，6电2光，内存8GB，2TB SATA 硬盘。
部署模式	支持数据库审计产品可以虚拟机形式旁路镜像模式部署，支持集中管理，可集中管理多台审计设备审计事件的存储、分析，实现统一配置、统一报表、统一查询；
部署管理	采用B/S管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务；
审计功能	支持主流数据库Oracle、SQL-Server、DB2、MySQL、Informix、Sybase、Postgresql、Cache、MongDB，K-DB、达梦、人大金仓、南大通用
	支持同时审计多种数据库及跨多种数据库平台操作
	支持时间段、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索；
统计功能	支持以图表方式（饼图、柱图、曲线图、清单列表）显示日志数据分布情况；
	支持以源IP、业务主机、操作类型、SQL模版、数据库用户为维度的数据库行为排行；
	支持指定源IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询；
	精细化日志秒级查询 通过SQL串模式抽取保障磁盘IO的读写性能；分离式存储SQL语句保障数据审计速度快

功能指标	指标要求
品牌	与行为管理同品牌
	TB 级日志秒级查询、支持指定源 IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多 SQL 语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询。
	自定义报表拖拽 通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果。(提供截图证明)
	支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模版为条件的数据库风险查询。
	支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险排行。
数据库安全	内置大量 SQL 安全规则 包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等；
	数据库访问可视： 数据库安全系统联动数据安全系统（BA）提供数据库系统、业务系统、运维人员、互联网接入之间的访问关系以及交互式分析，可以通过多维度展示具体人员、具体事件、具体内容、高危操作、登录失败、访问次数的视图支持查看最近的账号安全事件；(提供截图证明)
	数据库威胁分析： 可以通过自定义交互分析设置正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统、风险总次数这几个维度实时监控内网数据威胁态势并且提供交互式分析视图帮助企业快速溯源。
	支持基于 SQL 命令的 webshell 检测
	支持与下一代防火墙联动，实现 webshell 攻击的检测和阻断
风险分析	支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模版为条件的数据库风险查询；

功能指标	指标要求
品牌	与行为管理同品牌
	支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险排行，趋势；
响应方式	支持 Syslog 告警、SNMP trap 告警、邮件告警、短信告警； 支持旁路阻断；
系统管理	提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能；
日志数据安全	支持 SNMP 方式，提供系统运行状态给第三方网管系统； 支持 Syslog 方式向外发送审计日志；支持对所有审计管理员操作审计系统的动作进行审计； 支持日志类型、IP 地址权限设置；支持页面功能模块权限设置；
系统升级二次开发	根据用户需求定制开发相关内容，包括关联报表和特定业务日志审计等功能；
其他	投标时提供原厂针对本项目授权书和 3 年原厂质保函，签订合同时提供样机进行测试比对，测试结果未达到技术文件要求时，采购人有权拒签合同并取消中标资格，采购人有权选择第二中标人。

1.3.3.9 EDR 杀毒软件

技术指标		指标要求
品牌		必须与数据库审计同品牌
产品组成	产品形态	产品是软件形态，包含管理平台和终端Agent软件； 管理平台要求其操作系统为64位的Centos7或ubuntu操作系统； Agent软件支持32位和64位的Windows系统和64位的Linux系统。 产品和国内主流云平台实现解耦和，适用于Vmware、华为云、华三云、阿里云、腾讯云等国内主流云平台的主机；支持20个物理服务器或者虚拟机杀毒
	组件要求	管理平台采用软件包方式提供安装，安装后其中必须具备终端管理、终端病毒查杀、文件实时监控防护、东西向访问微隔离、暴力破解检测响应、WebShell检测响应、设备联动响应等功能组件，保障平台的扩展性和兼容性。
联动要求	设备联动	为方便我单位的安全管理智能化，要求虚拟机杀毒可以和本次采购的防火墙设备，上网行为管理设备同时联动，综合响应杀毒

		上网行为管理联动：支持管理员在上网行为管理平台通过EDR管理平台对其下属终端下发快速查杀任务，并查看其下发的查杀任务中各个终端的查杀状态、查杀结果以及查杀任务中查杀出来的病毒进行处置
		防火墙联动：支持防火墙通过配置终端检测响应管理平台IP地址实现与EDR平台的联动，实现端网安全联动；支持在防火墙上对下发的查杀任务中查杀出来的病毒进行处置；
管理平台要求	简化终端管理	支持终端资产盘点管理，支持自动收集终端资产状况，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端Agent版本、病毒库版本、最近登录时间、最近登录的用户名；
		支持控制台显示当前平台终端总数、在线/离线数量、服务器终端/PC终端数量；支持Vmware、Ctrix、Hyper-V、华为云、华三云、阿里云、腾讯云等国内主流云平台的虚拟机防护，并可在同一个管理平台进行统一管理。
	全网风险可视	支持病毒查杀、Webshell、暴力破解等威胁事件的事件趋势和TOP5事件展示。 支持控制台动态显示当前未处理的勒索病毒数量、暴力破解数量、WebShell后门数量及其各自影响的终端数量，支持点击对应的威胁类别，下钻到响应中心对应的威胁事件列表；支持热点安全事件动态更新和展示及全网终端已发生的热点安全事件及其数量；
	安全策略一体化	支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、WebShell检测的检测和威胁处置方式、暴力破解的威胁处置方式和Windows系统下信任区文件目录配置；
	多维度日志查询	支持根据统计周期、终端名称、IP地址、脚本命令名称和执行结果查询全网终端脚本执行日志，内容包括：任务名称、任务执行脚本名称、执行类型、执行时间、执行状态和脚本执行日志的导出；
		支持设备联动日志按策略来源、设备IP、终端名称、操作类型（新增、编辑、删除）、封堵方向、封堵IP 、 封堵端口、封堵时长的设备联动日志查询和展示；
	可视化报表	支持图形化显示病毒、WebShell事件爆发top5终端，并会显示出该终端未处理的威胁事件数；支持图形化显示暴力破解入侵中最活跃的攻击发起者top10、被攻击最多的主机top10；支持在报表中给用户提供安全规划建设建议。
	安装升级场景化	支持本地安装包部署、网页推广部署、上网行为管理系统联动部署、虚拟机模板部署，终端安装部署可根据客户环境选择最优部署方式。

		支持管理平台更新检测、自动下载升级和离线导入升级包升级； 支持agent根据升级域的配置自动升级到最新版本；
		支持病毒库和引擎组件的更新检测、自动下载升级和离线导入升级包升级； 支持全网终端统一病毒库和引擎组件升级。
终端Agent软件要求	基础防护能力要求	终端病毒查杀：具备基于多维度轻量级的无特征检测技术，多引擎协同工作，包括：基于AI技术的自研引擎、基于家族基因分析的特征检测引擎、基于虚拟执行和操作系统环境仿真技术的行为引擎、基于大数据分析平台的云查引擎。
		支持极速、均衡、低耗三种扫描模式，以控制扫描时对业务系统CPU资源的占用；（提供界面截图）终端侧使用全盘文件缓存，加速本地二次扫描速度，减少对本地虚拟化环境的资源消耗；管理平台侧使用全网文件缓存，加速云查杀速度，减少通过互联网进行云查杀的带宽消耗。
		支持通过管理平台下发立即扫描杀毒的任务，可针对某一台终端，也可针对某一组终端进行扫描杀毒；支持错峰扫描，可以设置定时扫描任务，实现终端分批错峰扫描、非业务时段扫描；支持配置跳过一定大小的文件，大小范围支持1M~100M；
		支持展示勒索病毒事件、木马病毒事件、蠕虫病毒事件和其他病毒文件事件及其详情，包括：病毒文件名称，事件等级，受感染的文件，发现时间，检测引擎，文件Hash值，文件大小，文件创建时间。
		支持威胁文件同步处置病毒时，选择是否在其它终端上同步处置。
	暴力破解防护	支持基于Agent的RDP和SSH登录日志检测的暴力破解入侵检测，支持开启暴力破解实时检测，自动封堵攻击源的IP地址，封停时间支持配置；
		支持对暴力破解事件攻击源IP加入黑名单，已加入黑名单的IP无法访问网内所有终端；
	基线合规检查	支持对指定终端/终端组进行终端基线合规性检查，对不合规的检查项提供设置建议；合规项包括不限于：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范；支持windows系统永恒之蓝漏洞（MS17-010）的检测；
	WebShell检测	支持配置WebShell定时扫描任务，配置参数包括：扫描周期（每日、每周、每月）、扫描时间精确到分、发现威胁处置方式（自动隔离、仅上报不隔离）； 支持配置WebShell实时扫描，一旦发现WebShell文件，自动隔离或仅上报不隔离。
		支持展示终端检测到的WebShell事件及事件详情，支持对WebShell事件的文件进行批量勾选一键隔离、信任和忽略操作；

	微隔离流量访问控制	支持对流量进行过滤，包括未放通流量、已放通流量、业务之间流量、业务内部流量、业务流量、运维流量和其他流量；
		支持微隔离功能主界面图形化显示业务系统、服务器及流量详情；流量线详情支持展示该流量线对应的微隔离策略；支持图形化显示服务器间流量关系，包括访问详情、流量趋势等；
		支持对业务系统配置微隔离策略规则；支持选择微隔离安全级别，支持高低两种级别；高级别：所有业务都被保护，默认拒绝所有出入站策略；低级别：默认放通策略，所有业务都允许访问，用户可根据实际配置拒绝的访问策略；

1.3.3.10 光纤交换机扩容

光纤交换机扩容	现有的 24 口交换机，激活 14 口，含 14 个模块+14 根光纤跳线

1.3.3.11 测评服务

测评服务	基础支撑系统+面向患者系统（检测费）

1.3.3.12 系统集成

系统集成	完成新建设备和原有硬件设备软硬件集成至交付