2024180001

郑州财经技师学院中职学校标准化工程项目

A 包：网络设施加固项目合同书

甲方（需方）：郑州财经技师学院

乙方（供方）：河南优溪智能科技有限公司

依据郑州财经技师学院中职学校标准化工程项目 A 包:网络设施加固项目采购（招标/项目编号：郑财招标采购-2024-9）的招标（谈判）结果，现依照《中华人民共和国合同法》及有关法律、法规、规章规定的内容，为明确供、需双方责任，双方达成如下协议：

1、合同标的与合同价格

品　　名	制造商	规格型号	质保期	数量	单　价（元）	金额（元）
应用交付网关	杭州迪普科技股份有限公司	ADX3000-GA-XI	五年	1	117000	117000
异常流量清洗系统	杭州迪普科技股份有限公司	Guard3000-GA-X	五年	1	112000	112000
防火墙系统	杭州迪普科技股份有限公司	FW1000-GA-X	五年	1	158000	158000
综合接入审计网关	杭州迪普科技股份有限公司	UAG3000-GA-XI	五年	1	146000	146000
威胁态势感知探针	杭州迪普科技股份有限公司	SAC3000-S-GS	五年	1	126000	126000
威胁态势感知平台	杭州迪普科技股份有限公司	SAC3000-P-GS	五年	1	158000	158000
高级威胁检测系统	杭州迪普科技股份有限公司	APT1000-GS-X	五年	1	108000	108000
统一管理中心系统	杭州迪普科技股份有限公司	SW-UMC-PLAT	五年	1	80000	80000

特征库升级服务	杭州迪普科技股份有限公司	LIS-FW1000-TS-X-A-1Y/LIS-FW1000-TS-X-I-1Y/LIS-UAG3000-MA-XI-A-1Y/LIS-UAG3000-MA-XI-P-1Y	五年	1	180000	180000
合同总价（小写）：人民币　1185000.00 元						
合同总价（大写）：人民币　壹佰壹拾捌万伍仟　元整						
备注说明： 1、合同总价包括但不限于设备费、运至甲方指定地点的运输费、保险费、伴随服务费、安装调试费、质保期内的维修维护费（人为损坏的除外）、操作人员培训费、国家强制要求检验费用、税费等所产生的一切费用。 2、乙方向甲方提供由制造商（杭州迪普科技股份有限公司 公司）出具对本合同项下设备全免费维保 五年 年确认函。 3、合同货物的技术参数等详见合同附件。						

2、质量要求和技术标准

2.1 质量要求：乙方应保证所供货物是全新的，未使用过的，并必须达到或高于招标（谈判）要求及投标（报价）承诺。

2.2 技术标准：合同货物应符合产品说明所述的技术规格和标准。如果没有提及适用标准，则应符合货物来源国适用的国家标准，这些标准必须是有关机构发布的最新版本的标准。

2.3 乙方保证，其提供的合同货物具备相关资质证明（证书），并且满足国内相关行业管理的有关规定。

3、交货

3.1 交货方式：乙方负责送货到交货地点完成安装调试，并承担运输过程中发生的一切费用及风险。

3.2 交货期：合同签订之日起 60 个日历天内完成交货及安装调试。

3.3 交货地点： 甲方指定地点 。

4、供货清单及包装、运输要求

4.1 供货清单：（详情见合同附件）

4.2 包装及运输要求：箱体包装/汽运

4.2.1 乙方所提供的全部货物是厂家出厂的原包装。

4.2.2 乙方提供的全部货物须采用相应标准及保护措施进行包装，这种包装方式适用于相应的运输方式，并有良好的防潮、防震、防锈和防野蛮装卸等保护措施，以便保证货物安全运抵现场。货物在运输过程中所发生锈、损坏和丢失及其他任何损失由乙方承担责任和费用。

4.2.3 每件包装应附有详细装箱清单和质量合格证书。

5、验收

5.1 合同货物到达交货地点且乙方完成安装、调试工作后，甲乙双方同意，货物由甲方验收并以甲方的验收意见为准。合同货物安装调试后经甲方验收合格视为最终验收合格。

5.2 乙方应积极配合甲方建立确保货物安全运行的工作环境，并对完善相应的操作规范等工作制度提出专业性的意见和建议。

5.3 合同货物验收时，由甲方签署货物验收单。

5.4 乙方应派代表参与验收过程，乙方未派代表参与或对验收意见有异议但未在 3 个工作日内书面提出的，视为卖方对验收意无异议。如乙方在验收完成后 3 个工作日内书面提出异议，以甲方委托的第三方验收意见为准。

5.5 最终验收合格后，乙方应在甲方要求的时间内直接交付甲方使用。合同货物交付使用前由乙方负责保管，合同货物的毁损或灭失风险由乙方承担。

5.6 甲方根据本合同约定提出换货、退货或解除合同的，乙方应在收到甲方通知后 3 个工作日内自行收回不符合合同约定的货物，并承担因退换货或解除合同所产生的一切费用。

6、售后服务

6.1 质保期为货物经最终验收合格之日起___5___年。质保期内，乙方向甲方提供免费服务（若设备有主机系统软件还应提供免费主机系统软件升级）和免费更换（人为损坏除外）。

6.2 故障响应时间：在质保期内接到甲方通知后，乙方需在__2__小时内到

达，__24__小时内修复；__24__小时内无法修复的，乙方提供相应配置的代用设备或更换新设备，以保证甲方工作生产部中断，其中发生一切费用由乙方承担。特殊情况下，由乙方与甲方协商，并经甲方同意后在双方约定的时间内完成设备的修复或更换。

6.3 质保期内，设备开机率须≥98%。若 90%≤设备开机率＜98%，则质保期按 1:3 延长；若 80%≤设备开机率＜90%，则免费保修期按 1:5 延长；若设备开机率＜80%，乙方应予以无条件退货。

6.4 质保期结束后，乙方仍应负责提供终身维修服务，但只能收取零配件费，零配件价格不得高于市场同类产品价格。乙方保证能长期提供维修配件，具体的维修服务协议待质保期满另行签订。

6.5 回访及不定期维修：乙方承诺对所有维修服务工作进行定期回访（__1月__一次），乙方应每__3__个月向甲方提供维修服务，维修报告应包括每次维修或保养到长时间、维修持续时间、故障地方、更换的配件等，并接受甲方的监督和检查。甲方可根据合同货物的使用情况要求乙方在规定时间内免费为合同货物进行检修、日常维护及保养服务，以保证合同货物的长期正常使用。

6.6 技术培训：乙方应向甲方免费提供合同货物的操作使用及基础维护的培训，直至使用单位的技术人员能完全掌握设备操作技能。

6.7 技术资料：乙方应向甲方提供完整的中文技术资料，包括：产品验收标准，技术说明书，使用说明书，操作手册，设备安装调试材料，安装维修手册，维修线路原理图及其维修资料，零部件目录，备品备件易耗件清单（含价格）及专用工具清单（如有的话），代理商与厂家之间的维保合同（如乙方为设备代理商）等文件资料。

7、付款条件与方式

7.1 付款条件

乙方同意，甲方按 7.2 约定的付款进度将相应款项汇入乙方指定账户。乙方账户信息如下：

户　　名：河南优溪智能科技有限公司

开户银行：中国银行股份有限公司郑州金融广场支行

账　　号：255970485416

7.2 付款方式：

7.2.1 合同签订后付总价款的 50%，即人民币：592500.00 元整（大写：伍拾玖万贰仟伍佰元整），所提供产品正常运行并验收合格后支付剩余总价款的 50%，即人民币：592500.00 元整（大写：伍拾玖万贰仟伍佰元整）

8.知识产权

乙方须保障甲方在使用该货物或其任何一分时不受到第三方关于侵犯专利权、商标权或工业设计权等知识产权的指控。如果任何第三方提出侵权指控与甲方和使用单位无关，乙方须与第三方交涉并承担可能发生的责任与一切费用。如甲方因此而遭致损失的，乙方应赔偿该损失。

9、违约责任

9.1 乙方未能按时交货或未能按时交付使用的，每逾期一日，乙方应支付逾期交货货款 1‰违约金。逾期超过 30 个日历日，甲方有权单方解除本合同，乙方应另外支付合同总价 5% 的违约金。

9.2 合同货物验收不合格的，甲方有权选择解除合同或换货。如甲方选择换货，乙方重新供货导致的交货延期的，按 9.1 条处理；若甲方选择单方解除合同的，乙方支付合同总价 5% 的违约金。

9.3 乙方提供的货物不符合 2.3 条规定，在合同货物最终验收合格前发现的，按 9.2 条处理；在合同货物最终验收合格后发现的，甲方有权退货，如甲方已支付货物价款，乙方应在甲方规定的时间内予以返还，此外，乙方应另外向甲方支付合同总价 5% 的违约金（如验收合格后发现货物不合格，由甲方委托的第三方鉴定确认）。

9.4 乙方的投标（报价）资料有弄虚作假、隐瞒事实内容等情形，在合同货物最终验收合格前发现的，按 9.2 条处理；在合同货物最终验收合格后发现的，甲方有权退货，如甲方已支付货物价款，乙方应在甲方规定的时间内予以返还，此外，乙方应另外向甲方支付合同总价 5% 的违约金。（如验收合格后发现货物不合格，由甲方委托的第三方鉴定确认）。

9.5 因乙方原因导致退换货的，乙方应承担退换货所需的一切费用。如乙方未在规定的时间内收回不合格的货物，甲方不对上述货物的灭失或损坏承担任何责任。如乙方逾期超过 30 个日历日仍未收回的，甲方有权自行处理上述货物。

9.6 质保期内，若乙方实际的维修响应（到达现场）时间不满足本合同要求的，每次应支付 1‰ 违约金，甲方有权另聘第三方对设备提供技术维修服务，由此产生的维修费用由乙方承担；乙方未按照本合同其他要求及投标（报价）文件售后服务承诺书的条款履行义务的，每次应支付 1% 违约金。

9.7 除本合同另有约定外，在补救违约而采取的任何其他措施未能实现的情况下，即在甲方发出违约通知后 10 个日历日内乙方仍未纠正其任何一种违约行为，甲方有权单方解除本合同，乙方除应退还甲方已支付的款项外，还应向甲方支付合同总价 5% 的违约金。

9.8 本合同约定的违约金无法弥补甲方损失的，乙方应继续承担相应的赔偿责任。甲方有权直接从未付的款项中扣除乙方根据本合同应付未付的违约金，赔偿金等。

9.9 甲方应按照合同条款 7.2 约定的付款进度将相应款项汇入乙方指定账户，如甲方未按照约定的时间及进度向乙方支付款项，甲方每逾期 1 个工作日，将向乙方支付 1‰ 的违约金。

10、不可抗力

10.1 因不可抗力造成违约的，遭受不可抗力一方应及时向对方通报不能履行或不能完全履行的理由，并在随后取得有关主管部门证明后的 15 个日历日内向另一方提供不可抗力发生以及持续期间的充分证据。基于以上行为，允许不可抗力一方延期履行、部分履行或不履行合同，并根据情况可部分或全部免于承担违约责任。

10.2 本合同中的不可抗力指不能预见、不能避免并不能克服的客观情况，包括但不限于：自然灾害如地震、台风、洪水、火灾；政府行为、法律规定或其适用的变化或者其他任何无法预见、避免或者控制的事件。

10.3 当事人一方因不可抗力的原因不能履行合同的，应及时通知对方，以减轻可能给对方造成的损失，并应当在合理期限内提供证明。

11、保密及廉洁条款

11.1 保密条款：双方应对本协议的内容（包括补充协议）及在本协议的签订、履行过程中获悉的对方所有商业信息（秘密信息）和相关资料承担保密义务，未经对方的事先书面同意，不得向第三方透露或以履行本合同以外的目的使用相

关秘密信息，造成损失的应向对方承担赔偿责任。

11.2 廉洁条款：双方员工不得以任何形式向对方相关人员提供回扣或返利。对于一方员工未经授权擅自向另一方做出的承诺，双方一概不予承认，由此造成的损失，由过错方自行承担。

12、合同的转让

乙方不得擅自部分或全部转让其应履行的合同义务。

13、合同纠纷处理方式

因本合同或与本合同有关的一切事项发生争议，由双方友好协商解决。协商不成的，任何一方均可向甲方所在地有管辖权的人民法院提起诉讼。

14、其他约定

14.1 招标文件、投标文件和招标现场谈判补充的条款是本合同的有效组成部分，具有与本合同同等的法律效力。

14.2 上述条款如有未尽事宜，应经过双方协商一致后以书面补充，作为附件，具有与本合同同等的法律效力。

14.3 本合同一式 柒 份，甲方执 伍 份，乙方执 贰 份，具有同等法律效力。

14.4 本合同自双方签订并加盖公章之日起生效。

甲　　方：郑州财经技师学院

单位地址：郑州市中原中路 128 号

法定代表人：

授权代表：

签订时间：2024.2.29

乙　　方：河南优溪智能科技有限公司

单位地址：河南省郑州市惠济区新城路 27 号碧源月湖景园 4 号楼 1 单元 2907 室

法定代表人：

授权代表：

签订时间：2024.2.29

附件 1：

序号	名称	技术参数	数量	单位
1	应用交付网关	1、标准式机架式设备，业务接口：千兆电口≥8 个，万兆光口≥12 个；扩展插槽≥2 个；内置 ssl 芯片；内存≥16G；双电源； 2、四层吞吐量≥20G；并发连接数≥1000 万，四层新建连接数≥15 万； 3、支持 TCP、HTTP、ICMP、DNS、SNMP、UDP、SMTP、POP3、SSL、Oracle、FTP、RADIUS、自定义等健康监测方式，支持 TCP 半连接健康检查； 4、支持源 IP、目的 IP、http cookie、http header、URL、Radius、DHCP、SSL ID、自定义等多种会话保持方式； 5、支持轮询、加权轮询、最小连接、加权最小连接、源地址源端口散列、目的地址散列、最小流量、加权最佳性能等负载均衡调度算法，并支持 URL、HTTP Header 等自定义服务器负载均衡算法； 6、支持在虚拟服务 WEB 页面配置界面里，同时新建并且配置高级策略；支持双机热备、VRRP 多主、静默双机、N+M 集群部署等多种模式； 7、支持主动方式的硬件故障诊断功能。通过 WEB 页面，非命令行的方式，实现负载均衡的硬件故障检测功能，可检测如 cpu、内存、电源、风扇等硬件的运行状态； 8、支持流量调度功能，对于出方向流量，可以基于目的地址运营商属性、哈希权重、加权最小带宽、加权最小连接、加权轮询等算法进行选路； 9、支持自动方式的双机配置一致性检查功能，每隔一定时间双机会自动检测彼此之间的配置是否保持一致，并且显示上次检查时间以及检查结果； 10、支持 x-fordward-for 功能，用来识别通过 HTTP 代理或负载均衡方式连接到 Web 服务器的客户端最原始的 IP 地址的 HTTP 请求头字段，实现对访问源的溯源；	1	台
2	异常流量清洗系统	1、标准机架式设备，具备千兆电口≥8 个，万兆光口≥12 个，支持扩展 4 千兆电/4 千兆光/4 万兆光接口卡；扩展槽≥2 个，双电源； 2、整机吞吐量≥6Gbps，每秒新建连接数≥4 万，最大并发连接数≥300 万；	1	台

		3、支持基本的网络层、应用层 DDoS 攻击检测及防护，包括但不限于：SYN Flood、UDP Flood、ICMP Flood、DNS Flood、HTTP Flood、HTTPS Flood 等； 4、支持 xFlow 报文转发、flow 分流模式、分布式部署，通过 xFlow 分流转发、聚合分析实现大流量攻击检测能力； 5、支持新建连接数及并发数限制防护策略，可对 TCP、UDP 协议设置阈值及周期； 6、支持根据报文特征进行自定义攻击防护类型，通过这种方式防护未知攻击防护，可提供基于报文长度、报文 ID、TTL、源 IP、目的 IP、序列号、确认号、源端口、目的端口、flag 标记、key 偏移、key 长度等进行匹配的模式匹配规则； 7、支持在一个界面中可对以下网络行为进行配置：对 ICMP 重定向报文、Tracert 报文、源路由选项 IP 报文、路由记录选项 IP 报文、超大 ICMP 报文、反向路由检测、TcpFlag 攻击、ICMP MTU 欺骗报文等网络行为阻断，并发送日志和统计攻击次数；对 IP 地址扫描、端口扫描、漏洞扫描等行为识别，并加入黑名单，黑名单可自主设置周期； 8、支持针对协议头中各字段配置自定义过滤策略，字段包括但不限于：Method、Cookie、Host、Referer、Request URI、Verion、User-Agent 等 9、支持单 IP 自学习及策略下发；即针对防护对象内所有单一 IP 自学习流量基线，支持设置带宽、最低阈值、学习敏感度等策略，支持查看学习结果、手动修改学习结果，学习结果自动下发； 10、具有中国网络安全审查技术与认证中心颁发的《IT 产品信息安全认证证书》。		
3	防火墙系统	1、标准机架式设备，千兆电口≥8 个，万兆光口≥12 个，双电源； 2、最大吞吐量≥35Gbps，最大并发连接数≥1200 万，每秒新建连接数≥17 万； 3、支持 SYN Flood、ICMP Flood、UDP 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； 4、访问控制策略支持基于源/目的 IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式； 5、支持静态路由、RIP v1/2、OSPF、路由，支持 PIM 和组播 NAT 功能； 6、入侵防护漏洞规则特征库数量在 6000 条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞名称，危险等级，对应 CVE 编号；	1	台

		7、支持杀毒白名单功能，可以根据 URL 或者 IP 进行排除不检测病毒； 8、可提供最新的威胁情报信息，官方网站每周会进行安全通告，能够对新爆发的流行高危漏洞进预警和自动检测； 9、支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备； 10、支持自动生成安全策略。统一管理平台可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率； 11、为保证业务连通性，设备支持 CPU 利用率过高时，自动停用部分应用层攻击防护功能； 12、具备中国信息安全测评中心颁发的《信息技术产品安全测评证书 EAL4+》。		
4	综合接入审计网关	1、标准机架式设备，具备千兆电口≥8 个，万兆光口≥12 个，支持扩展 4 千兆电/4 千兆光/4 万兆光接口卡，扩展槽≥2 个，双电源； 2、整机吞吐量≥20Gbps，并发连接数≥300 万，每秒新建连接数≥3.5 万，最大在线用户数≥2048，最大认证用户数≥5 万； 3、支持透明在线模式、网桥模式、网关模式、旁挂模式部署，支持分布式与集中式部署，对于分布式部署，可分权分域与集中管理； 4、支持 NAT 功能，支持源 NAT、目的 NAT、一对一 NAT 的等功能； 5、支持会话监控功能，支持统计设备会话数、IPv4、IPv4 TCP、IPv4 UDP、IPv6、IPv6 TCP、IPv6 UDP 并发会话数等及趋势图信息； 6、支持在外置设备管理平台在 TOP 用户连接数列表中可以看到 TOP 用户连接数排行图及统计，统计支持用户最大并发数、最大新建速率、当前新建速率、当前并发数； 7、支持自定义应用：支持通过 IP+端口方式自定义网络应用及基于深度检测方式（应用特征）自定义网络应用； 8、支持诊断功能：支持设备页面抓包，页面抓包支持 IP 地址、协议、接口、抓包方向、抓包时间、抓包数量等多种灵活的过滤条件，抓取需要的流量报文，是网络故障排除和分析的有效工具； 9、支持 VIP 网段和普通网段，当超过设备处理性能时 VIP 网段优先 bypass； 10、支持监控指定 IP 或 IP 范围的用户速率、关注的设备接口速率超过阈值时，能够通过日志、声音、邮件等方式进行告警。	1	台

5	威胁态势感知探针	1、高度 2U；千兆电口≥6 个，USB 接口≥2 个；硬盘容量≥4T；内存≥16G；双电源； 2、1G 流量采集能力； 3、支持多种主机渗透攻击检测，至少包括：系统漏洞攻击、命令注入、应用程序漏洞攻击、Shellcode 攻击、DNS 漏洞攻击、FTP 漏洞攻击、邮件漏洞攻击、文件漏洞攻击、网络设备漏洞攻击、浏览器漏洞攻击、Web 系统漏洞攻击、多媒体应用漏洞攻击、TELNET 漏洞攻击、TFTP 漏洞攻击等； 4、支持多种协议的隐匿隧道通信检测，至少包括：ICMP、HTTP、DNS 等协议的隧道通信； 5、支持全流量报文的存储，以及远程调取、查看和下载功能； 6、支持基于机器学习的加密流量下的恶意软件通信识别，至少包括加密的 Botnet 僵尸网络行为检测；支持基于机器学习的提取攻击者真实访问的 URL，全面掌握攻击者的攻击意图和访问记录，包括：攻击者 IP、攻击者 URL、访问行为的原始报文等； 7、支持多种类型挖矿病毒检测，至少包括：XMRig 挖矿病毒、Wannaminer 挖矿木马、LifeCalendarWorm 挖矿蠕虫、WorkMiner 挖矿木马等。	1	台
6	威胁态势感知平台	1、高度 2U，千兆电口≥2 个，万兆光口≥2 个，USB 接口≥4 个，扩展槽≥4 个；硬盘≥8T；CPU 不少于（8 核心 8 线程）×2 颗，内存≥64G；双电源； 2、单台最大流量处理能力 1G； 3、支持查看 5G 威胁的日志统计数据，包括攻击级别分布，攻击名称 Top5 和手机号 Top5 统计图以及 5G 威胁事件的列表；支持查看 5G 威胁日志的攻击列表展示，包括攻击者、受害者、所属机构、攻击类型、攻击名称、关键字、发现时间； 4、支持资产管理，支持通过 5G 流量自动提取和分析出资产手机号码信息，并关联资产呈现，点击资产详情可以查看事件详细信息、访问关系； 5、支持从攻击者和受害者视角分别展示用户威胁列表，至少包括：用户名称、攻击类型、攻击名称、发起或遭受攻击次数等，并支持下钻展示单个用户发起或遭受攻击的列表及详情； 6、支持自定义攻击事件分析模型，至少包括：事件规则匹配模型、事件统计分析模型、事件关联分析模型；内置 38 种及以上安全事件分析模型，如冰蝎 webshell 通信、利用 Sqlmap 上传 webshell、Acunetix 安全工具扫描、APPSCAN 工具扫描等；	1	台

		7、支持攻击事件时间溯源轴展示匹配上的威胁建模模型信息，攻击手段显示模型名称，事件类型显示威胁建模设置的事件标签，覆盖的攻击阶段显示威胁建模设置的攻击链，安全处置建议显示威胁建模设置的处置建议； 8、支持基于 ATT&CK 框架的攻击链分析，内置 13 个入侵阶段的攻击链知识库，入侵阶段包括但不限于：扫描探测、投放利用、代码执行、持续突防、权限提升、防御绕过、账户破解、环境洞察、横向扩散、数据采集、命令控制、数据窃取、深度影响； 9、支持 AI 判真功能，存在多个攻击手段的攻击事件显示为 AI 判真事件，AI 判真事件存在 AI 判真标识； 10、支持 AI 自动处置功能，当处置列表有昨天的处置信息，今天没有处置信息时，攻击事件支持自动按照昨天的处置历史信息进行处置，攻击事件被盖上相应的处置标签，历史处置记录按时间轴形式显示处置时间、设备信息或备注信息，处置列表新增一条处置信息，显示处置目标、所属机构、数据来源、威胁等级、威胁资产数量、事件类型、处置来源、处置手段、处置时间、生效日期和备注信息； 11、具备中国网络安全审查技术与认证中心颁发的《IT 产品信息安全认证》。		
7	高级威胁检测系统	1、标准机架式设备，千兆电口≥6 个，扩展槽≥2 个，支持扩展 4 千兆光/4 千兆电/8 千兆光/8 千兆电/4 千兆电+4 千兆光/2 万兆光/4 万兆光接口卡，USB 接口≥2 个；CPU ≥4 核，内存≥32GB,存储≥1T；冗余电源； 2、整机吞吐量≥1Gbps； 3、支持告警事件分析，能够展示安全事件级别、攻击类型，源 IP、目的 IP、源端口、目的端口、源位置、目标位置情况； 4、支持监测流量状态，基于时间维度记录并展示流入、流出流量情况，并记录流量的总流入流出情况。支持流量监测的开关控制； 5、支持沙箱分析功能，分析结果包括但不限于文件名称、文件 MD5、受感染主机、威胁指数、传播次数、动态检测结果、静态检测结果、病毒检测结果。支持跳转展示沙箱分析详情，展示文件的静态检测、动态检测、病毒检测结果； 6、支持文件审计功能，记录审计流量中流转文件的名称、类型、源 IP、目的 IP、时间、风险描述、协议类型，并支持审计文件下载、文件审计报表导出； 7、支持多种病毒检测引擎，集成第三方专业防病毒厂商的专业病毒库，特征规则数量不少于 20000 条； 8、支持可疑文件的离线上传检测，对文件进行静态、动态的离线检测；	1	台

		9、支持沙箱状态控制设置，一键开启、关闭沙箱，设置沙箱并发数； 10、支持边界完整性检测，可针对专网中的非法外联主机进行有效检测和定位，可检测出目标设备通过连接智能手机热点、通过智能手机 USB 共享网络、私接无线 AP、共享 Wi-Fi、以 NAT 方式接入的路由设备等方式的违规外联行为。		
8	统一管理中心系统	1、支持对安全设备进行集中管理，可通过访问控制策略的配置，实现大规模部署环境下的灵活、便捷的安全策略管理，阻止敏感信息外泄和非核心业务的滥用，确保网络的整体安全； 2、全面集成日志采集器、数据库、日志分析、审计、报表等功能部件，可实现对整张网络进行全面的网络流量分析，自动关联安全事件，帮助管理员实时了解整网状况，发现潜在安全风险，保障网络安全； 3、支持集中管理和分级管理两种模式。集中管理可以在平台上针对网络中所有设备进行统一的配置和安全事件管理;对于较大规模和分区域的网络环境，支持通过分级管理的方式进行总部和分部的统一管理； 4、采用 B/S 架构，内建 HTTP 服务器，管理员可以在任意位置通过 HTTP 或 HTTPS 方式登录统一管理中心对网络进行监控和管理； 5、支持 TR-069、SNMP 管理协议，对网内安全设备、网络设备、服务器等进行实时运行状态监控，分析研判各类安全事件； 6、支持统一升级被管理设备的特征库,支持配置静态路由表，并提供批量下发设备； 7、支持对现网的安全设备进行统一的管理； 8、支持对网内安全设备进行配置管理和下发，包括设备间业务配置迁移，批量配置下发，路由、接口、MAC 地址、ACL、地址对象等配置和批量下发； 9、具备国家版权局的《著作权登记证书》。	1	套
9	特征库升级服务	与原有设备（①防火墙：品牌：迪普；型号：FW1000-TS-X；②网络安全审计：品牌：迪普；型号：UAG3000-MA-XI）功能相匹配，对原有设备（一台防火墙、一台网络安全审计）进行 AV 防病毒安全 License、IPS 特征库、URL 特征库升级服务。	1	项