合作市人民检察院
全流量综合安全危险分析系统探针采购项目清单

设备名称	基本要求	数量	单位
综合威胁分析探针	1、基本硬件要求：标准机架式设备,内存 32G（ 2*16G），机械硬盘 4TB，8 个千兆电口（含 1 个 HA 口和 1 个管理口），4 个千兆光口插槽，1 个 CONSOLE 口,冗余电源,2 个扩展槽位。 2、基本性能要求：最大并发连接数：100W，综合威胁检测能力：2Gbps。含：3 年攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库、URL 分类库。3 年原厂维保服务。 3、基本功能要求：1）支持独立的攻击检测引擎，涵盖 13000 种以上的攻击检测规则库。规则库支持按照攻击类型、操作系统、风险等级、应用类型、流行程度等方式进行分类。（提供截图证明）2）采用僵尸主机与控制主机异常通信行为检测的方式，具有独立的僵尸主机特征库，能够对 11000 种以上僵尸主机行为进行监测，包括僵尸网络、木马控制、蠕虫、挖矿、勒索、移动端木马控制、APT 等多类型的僵尸主机行为。支持对 Windows、Linux、IOS、Android、Unix、MacOS 等多种操作系统的僵尸主机检测，并对规则可设置相应警告、联动阻断动作（提供截图证明）3）机器学习检测功能能够实现对目标文件实时检测实时还原的效果，不依赖规则库即可实现对未知恶意程序检测。（提供截图证明）4）支持虚拟沙箱，可对文件进行多维深度检测，并记录文件传输会话信息。（提供截图证明）5）支持通过威胁情报检测已知 APT 事件，通过恶意程序检测未知 APT 事件，通过僵尸主机规则库检测已知的 APT 组织。（提供截图证明）。 4、安全品质及应急保障能力要求：1）产品具有公安部颁发的计算机信息系统安全专用产品销售许可证 VDS 增强级；2）产品具有中华人民共和国版权局颁发的计算机软件著作权登记证书；3）项目本地原厂具有 7 名注册信息安全专业人员 CISP 和 1 名注册信息安全专业讲师（提供至少一年的本地社保证明）；4）原厂具有信息系统建设及服务能力评估资质（CS4 级）证书；TL9000 品质管理体系认证证书； 具有云安全成熟度模型 CSA-CMMI 5 级认证证书 。	1	台