阜外华中心血管病医院杀毒系统维保服务采购项目采购需求

技术要求

（一）内网高级持续性威胁检测系统续保服务

序号	要求
1	# 1台内网高级威胁监测设备（型号为TDA 680）三年保修服务、三年基本软件升级维护、特征库和病毒码升级服务。
2	可扫描网络第2层至第7层数据流量。
3	支持超过 100 种以上的网络协议支持，如 HTTP, FTP, TFTP, SMTP, POP3, IMAP, SNMP, IRC, DNS, DHCP, P2P, SMB, RDP, VNC, TELNET, TCP, UDP 等协议。
4	支持恶意文件侦测，能够侦测各种文件型病毒，如木马、僵尸、后门等
5	支持恶意行为分析侦测，如零日攻击、网络蠕虫、木马、后门、僵尸、间谍软件、网络漏洞、网页威胁（网页漏洞、跨网站攻击）、钓鱼邮件、暴力攻击、数据库注入攻击等。
6	支持威胁流量的自动存储，及威胁流量PCAP文件格式下载。
7	能够自动关联不同协议、不同会话的威胁日志，筛选出严重事件，节省事件处理的人力成本。
8	# 能够与医院现有云主机深度安全防护系统及防病毒网络版软件进行联动，提供联动对接方案
9	# 服务期：三年，中标后签订合同时中标人需提供系统原厂商针对此项目的7*24小时售后服务承诺函并加盖原厂商公章。

（二）云主机深度安全防护系统续保服务

序号	要求
1	# 对现有的284点云主机有代理客户端系统进行3年特征库、病毒码升级服务。
2	支持恶意程序防护、Web信誉（阻止用户访问恶意站点）、主机防火墙、日志审查功能。
3	支持本地扫描和云安全扫描，具备本地病毒码和云端病毒码，支持实时扫描，预设扫描和、手动扫描和快速扫描。
4	对病毒的处理措施支持：清除、删除、拒绝访问、隔离、不予处理，系统针对不同的病毒类型提供默认配置，同时支持用户自定义。
5	支持和外部沙箱实现集成，同步沙箱的检测结果，检测未知威胁，并处理。
6	支持对主机的日志审计，包括收集和分析操作系统和应用程序日志中的安全事件

7	产品需要支持自定义升级某一个或者某一些客户端的病毒码，而不是只能一次升级所有客户端的病毒码。
8	# 具备入侵检测、虚拟补丁、防火墙功能。
9	# 服务期：三年，中标后签订合同时中标人需提供系统原厂商针对此项目的7*24小时售后服务承诺函并加盖原厂商公章。

（三）防毒墙网络版软件续保服务

序号	要求
1	# 对现有的1300点防毒墙网络版软件V16.0客户机版进行3年特征库、病毒码升级服务。
2	产品采用B/S架构，支持通过HTTPS方式登录管理控制台，管理控制台访问需进行加密访问。
3	产品管理端需要提供工具集，针对管理端、客户端提供用于自身配置的工具。同时WEB界面，需要提供有关如何使用工具的帮助信息。
4	产品需要支持根据IP地址（包含IPv6）、操作系统、在线状态、处理器结构、病毒码版本、防火墙状态、爆发阻止状态等条件的组合搜索出符合条件的终端进行管理。
5	产品需提供多种扫描引擎不少于五种，针对于机器学习必须使用独立扫描引擎，同时所有防毒引擎必须为自主知识产品非OEM产品。
6	对于文件扫描方式至少支持三种以上，包括所有文件统一措施、推荐扫描措施、以及针对不同类型病毒/恶意软件提供不同扫描措施，同时不同病毒/恶意软件类型不少于7种分类。
7	具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新。
8	具备病毒爆发防御功能。当最新病毒爆发时，可在病毒代码未完成之前自动对企业网络中的病毒传播端口、共享等进行关闭，切断病毒传播途径，预防最新病毒的攻击。
9	# 服务期：三年，中标后签订合同时中标人需提供系统原厂商针对此项目的7*24小时售后服务承诺函并加盖原厂商公章。