附件：

一、招标参数：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备名称 | 招标参数 | 数量 |
| 1 | WEB应用防火墙 | ★1.硬件参数不少于6个千兆电口，4个千兆光口，2个万兆光口，不少于2个高速USB2.0接口，标准2U架构2.性能参数：网络层吞吐量≥10Gbps，应用层吞吐量≥2Gbps,并发连接数≥2,000,000,每秒新建连接数≥100,0003.部署方式：支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式。4.网络特性：支持链路聚合功能，支持端口联动，支持802.1Q VLAN Trunk、access接口，子接口。支持IPV6环境部署，包括接口/区域配置、路由配置等网络适应性功能，支持核心常用安全功能5.基础功能：IP、目的IP和双向IP连接数控制；支持NAT64、NAT46 地址转换；支持DNS-Mapping； 访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式，支持长连接功能并可以配置连接时长； 6.内容安全支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，并给出恶意邮件的提示，支持根据邮件附件类型进行文件过滤； ★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；支持识别管控的应用类型超过1200种，应用识别规则总数超过3000条；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； 7.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；（需提供相关功能截图证明）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； 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告； 8.支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；具备对常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能；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；9.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；★10.资质要求：要求厂商是微软安全响应中心（Microsoft Security Response Center）发起的MAPP（Microsoft Active Protection Program）计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护；厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位；设备生产商的研发体系具备国际CMMI 5级认证（以上提供相关证明并加盖公章） | 1 |
| 2 | 终端检测与响应 | 1.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，要求产品采用轻代理架构；支持在控制台上启用、禁用、重启、远程卸载和移除终端agent，方便管理员对终端agent的远程管理；本次提供500个终端杀毒许可，30个服务器杀毒许可2.支持全网安全和终端安全状态分布，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；3.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、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；（提供界面截图并加盖厂商公章）4.支持管理员权限分级，支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限，支持超级管理员接入/编辑/删除/同步下级分支，支持其他管理员仅可查看下级分支包括下下级分支的名称/IP/终端数/最近同步时间/上级控制中心；5.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，支持对病毒文件进行批量勾选一键隔离、信任和忽略操作，支持宏病毒和感染型病毒的查杀修复，支持对已隔离的病毒文件进行批量勾选一键恢复，支持将已信任的病毒文件移出信任区，支持彻底删除已隔离的病毒文件；支持插入U盘时主动扫描U盘文件，支持U盘窗口信息展示：剩余空间、总空间，支持U盘窗口操作：打开、弹出、查杀；6.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。7.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，展示终端检测到的暴力破解事件及事件详情，包括攻击源、攻击类型、检测引擎、最后攻击时间、攻击方法、攻击内容、攻击历史，能够自动封堵攻击源的IP地址，封停时间支持配置；（提供界面截图并加盖厂商公章）8.厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位；★9.支持与安全态势感知平台联动，将Agent检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到同厂商安全态势感知平台，安全态势感知平台进行分析和展示；★10.支持与上网行为管理联动，支持在上网行为管理平台下发快速查杀任务，查看各个终端的查杀状态、查杀任务的查杀结果，并对其下发的查杀任务中查杀出来的病毒进行处置 | 1套 |
| 3 | 网站安全监测服务 | 1、实时带宽100Mb/s、防护域名数量1个、为用户网站提供云端的Web应用安全防护、IPS，独享防护、防绕过、失陷监测、安全可视化、动态防护、定向防护、实时对抗、应急对抗；以及安全专家代管服务。2、 支持关键资产系统域名发现，自动发现客户所填入域名相关的所有子域名，并检测网站服务器端口开放情况，比如数据库端口、Ftp服务端口等，支持对Web漏洞进行扫描，覆盖技术漏洞、配置错误、rdp，ssh弱口令检测等；3、 支持对目标站点提供7×24小时网页敏感词检测能力。发现网页敏感词事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现；4、 支持页面响应监测，通过模拟用户请求实时获取站点的响应状态和请求详情，5分钟检测一次，连续3次访问失败时判断为业务不可用；5、 支持对目标站点提供7×24小时网页黑链监测能力。发现网页黑链事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现。6、 支持自动选路功能，支持PING、TCP、HTTP等多种方式监控链路的连通性并自动切换链路；7、 支持对常见http应用服务的口令暴力破解防护功能，支持对web服务漏洞攻击的防护，具备http应用服务的弱密码扫描功能；8、★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，云端安全专家自动生成防护规则；9、 0Day发布后24小时内进行全面排查，第一时间告知用户是否存在该风险，并针推出针对性防护方案，针对DDOS、CC等恶意流量攻击行为增加专家在线分析环节，并封锁攻击源IP地址；10、所投服务厂商具备CMMI 5认证证书，提供证明材料复印件并加盖投标单位公章；11、所投服务厂商具有国家信息安全测评中心颁发的《信息安全服务资质证书》安全工程类证书，提供证明材料复印件并加盖投标单位公章；12、★所投服务厂商是微软安全响应中心MAPP成员，提供证明材料复印件并加盖投标单位公章；13、★所投服务厂商取得国家级网络安全应急服务支撑单位，提供证书并加盖投标单位公章； | 2年 |