**“集团核心机房架设项目”竞价参数**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 产品类型 |   | 规格参数 | 数量 |  价 | 备注 |
| **一、外网部分** |
| 1-1 | 外网下一代防火墙 |  | 详见参数及服务指标一览表 | 1 | 70000 |  |
| 1-2 | 上网行为管理功能 |  | 1 | 48000 |  |
| 1-3 | 外网服务器 |  | 1 | 50000 |  |
| 1-4 | 外网核心交换机 |  | 1 | 3000 |  |
| 1-5 | KVM一体机 |  | 1 | 10000 |  |
| **二、内网部分** |
| 2-1 | 内网下一代防火墙 |  | 详见参数及服务指标一览表 | 1 | 70000 |  |
| 2-3 | 内网服务器 |  | 2 | 100000 |  |
| 2-4 | 内网安全管理系统 |  | 1 | 8000 |  |
| 2-5 | 内网杀毒系统 |  | 1 | 10000 |  |
| 2-6 | 内网核心交换机 |  | 1 | 3000 |  |
| 三、其他 |
| 3-1 | 服务器机柜 |  | 详见参数及服务指标一览表 | 1 | 6000 |  |
| 合计 | 378000 |

**配置参数指标一览表**

* 1. **外网下一代防火墙：**
1. 1U构架、最大吞吐量≥2.5G、至少含有传统防火墙、流量管理、应用管理、IPSec VPN、资产识别、防病毒、入侵防护及联动，≥180天日志功能。包含≥三年产品维保、升级等服务。
2. ★支持多链路负载路由，能够基于IP、端口、协议、ISP、应用类型以及国家地域来进行选路由选路；（需提供上述功能截图证明）
3. ★一旦出现故障时排除顺利，或者在部署设备前进行快速调试，访问控制规则必须支持数据模拟匹配，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；（需提供相关功能截图证明）
4. 访问控制规则必须支持基于网络对象／用户，端口，区域，应用/服务类型的应用访问控制和基于国家/地区的地域访问控制，实现精细化管控；（需提供相关功能截图证明）
5. 支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件内容检测、附件杀毒、URL过滤等，支持根据邮件附件类型进行文件过滤；（需提供相关功能截图证明）
6. 设备必须提供最新的威胁情报，能够对新爆发的流行高危漏洞进行预警和自动处置，支持新的安全事件爆发时，自动扫描内网存在的漏洞，并自动开启防御功能；（需提供相关功能截图证明）
7. ★扩展支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞；（需提供相关功能截图证明）
8. ★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；（需提供相关功能截图证明）
9. ★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；（需提供相关功能截图证明）
10. ★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；（需提供相关功能截图证明）
11. ★支持资产的自动发现以及资产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；（需提供相关功能截图证明）
12. ★支持基于攻击不同阶段的方式来匹配并展示当前资产遭受到攻击的具体所处状态，并详细给出针对性处理建议，展示具体的攻击链并可对威胁进行取证；（需提供相关功能截图证明）
13. ★支持安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况；（需提供相关功能截图证明）
14. ★为保证产品后续技术支持和研发能力，投标厂商具有CMMI L5，提供截图证明

**1-2、上网行为管理功能：**

1. 标准1U机架式;4个千兆电口 ，128GB-SSD硬盘，支持带宽≥200Mb，支持用户数≥600个。
2. ★支持两台及两台以上设备同时做主机（提供以上3种设备部署模式以及多机、多主模式部署配置界面截图）
3. 设备需要支持使用VPN做专线备份，支持链路故障检测；（提供四种多链路负载算法功能、VPN专线备份功能、链路故障检测截图）
4. ★应用管控有效性需要基于完整有效的应用识别规则库，设备必须内置全面的应用识别规则库，支持超过4600条应用规则数，支持超过2100种以上的应用，650种以上移动应用，保证应用识别的准确率（提供产品应用识别库总应用数量及移动应用数量界面截图）
5. ★需要支持基于管控P2P的上行流量，抑制P2P下行流量的P2P流量管控技术。（提供抑制P2P下行丢包的配置界面截图）
6. ★支持对内网用户的访问质量进行检测，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访问质量检测（提供访问质量检测功能产品界面截图）
7. 需要对外部访客上网行为进行审计，同时保障访客的用户体验，支持二维码认证，管理员扫描访客的二维码后对其网络访问授权。
8. ★设备必须支持能自动发现网络中个人手动创建无线上网的热点和移动终端的IP和终端类型，且支持基于时间和终端数量设置进行自动阻断冻结。（提供共享网络接入检测、自动阻断冻结和移动终端管理配置功能截图）
9. ★所有功能都支持IPv6配置（提供认证、应用控制、内容审计、报表功能支持ipv6配置界面截图）
10. 需要支持细化的日志查询功能，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（提供细化日志查询功能配置截图）
11. ★支持基于黑名单的流量管控功能，管控粒度需要基于“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（提供设置配额、流控黑名单惩罚通道界面配置截图）
12. 设备需要具备公安部颁发的《网络通讯安全审计 销售许可证》、《互联网公共上网场所信息安全管理系统（无线接入前端）销售许可证》

**1-3、外网服务器：**

1. 规格：工业标准2U机架式服务器
2. 处理器：≥2颗英特尔® 至强® 处理器可扩展家族处理器4110，主频2.1GHz，8核，L3缓存≥11MB
3. 内存：32GB RDIMM ECC 2666 DDR4 内存，≥24条扩展插槽，最大1.5TB内存扩展
4. 硬盘：3块2TB 7.2K 12Gbps热插拔3.5寸SAS硬盘，最大支持8个硬盘扩展。标配支持快擦硬盘/SSD，服务器生命周期结束或者挪作它用时一键删除硬盘/SSD所有信息，只需要几分钟就能保证信息不泄露。
5. RAID功能：独立12Gb RAID卡,支持0,1,5,10,50，可选高端RAID卡，
6. GPU：支持≥3个内部全宽300W或者≥6个内部半宽半高的150W GPU
7. 网卡：标配4个千兆以太网端口，支持failover,loadbalance，可选4个万兆10Gbase\_T/SFP+ 接口以太网卡, 或者2个25GE接口以太网卡，支持独立于交换机的万兆网卡分区技术.
8. 电源：配置1+1冗余热插拔钛金级能效电源，电源输出功率≥750W
9. 安全功能：加密签名固件，硬件根信任，安全启动，自动BIOS恢复，快速OS恢复，系统一键锁定，安全的缺省密码，配置和固件漂移检测，持久日志（包括用户形迹），出厂预装正版服务器安全狗SMART版，随时了解电脑运行情况，系统优化，网络防火墙功能；
10. 服务器管理：前面板上配备有液晶屏，可显示默认或定制信息，包括IP地址、服务器名称、支持服务编号等。如果系统发生故障，该液晶屏上将显示关于故障的具体信息。可监控、报告及控制处理器、内存及系统级的能耗，允许通过一体化管理控制台实现基于策略的功耗封顶。虚拟机功耗映射，可以根据功耗对于虚拟机进行负载平衡以及按虚拟机报告功能；前置专用USB管理口，能够通过手机和平板电脑管理服务器，可以做现场的资产清点
11. 操作系统：需配置有正版win server 2012 R2数据中心版系统
12. 售后服务：3年7x24，部分城市当日4小时原厂备件上门更换服务，配置专属金牌服务经理及专属800/400技术支持电话。

**1-4、外网核心交换机：**

1. 固定可用千兆端口>=28个，其中千兆电口>=24个，千兆SFP光端口>=4，Console口>=1,
2. 交换容量>=3.36Tbps，包转发速率>=108Mpps
3. 支持IRF2智能弹性架构，最大堆叠台数>=9台，最大堆叠带宽>=16G，支持跨设备链路聚合，单一IP管理，分布式弹性路由，支持通过标准以太端口进行堆叠，支持完善的堆叠分裂检测机制，支持远程堆叠
4. 支持黑洞MAC地址，支持设置端口MAC地址学习最大个数，支持基于端口的VLAN，支持QinQ，支持Voice VLAN，支持协议VLAN，支持MAC VLAN，最大VLAN数(不是VLAN ID)>=4094
5. 支持GE端口聚合，支持静态聚合，支持动态聚合，支持跨设备聚合，支持最多8个端口聚合；支持最多128个聚合组（IRF2）；支持LACP支持本地端口镜像和远程端口镜像RSPAN；支持流镜像，同时支持N：M的端口镜像（M大于1）
6. 支持IPv4静态路由、RIP V1/V2、OSPF V1/V2/V3
7. 支持RRPP（快速环网保护协议），支持Smartlink，支持RSTP功能，支持MSTP功能，支持PVST功能
8. 支持基于第二层、第三层和第四层的ACL；支持SP/WRR/SP+WRR队列调度；支持基于端口的限速；支持基于流的重定向；
9. 整机提供ACl条目数不小于512条；支持基于端口和VLAN的 ACL；支持IPv6 ACL；支持双向ACL，以便于灵活实现数据包过滤；支持802.1x认证，支持集中式MAC地址认证；
10. DHCP client，支持DHCP Snooping，支持DHCP Snooping trust，支持DHCP Snooping option 82，支持DHCP Server
11. 支持用户分级管理和口令保护，支持SSH2.0，支持端口隔离，支持 802.1X，支持端口安全，支持MAC地址认证，支持IP Source Guard，支持HTTPs，支持EAD
12. ★支持SNMP V1/V2/V3、RMON、SSHV2，支持iMC网管系统
13. 端口定时down功能（Schedule job），支持端口休眠，关闭没有应用的端口，节省能源

14、所提供的光模块（如果选配），必须贴有防伪标签，并且可通过命令行方式验证光模块是否原厂认证的模块，提供相关命令和说明

**1-5、KVM一体机：**

 机架式KVM切换器，接口数：≥8个VGA，USB+PS/2双接口，最大支持连接数：256台；三合一液晶套件带键盘，鼠标，≥19寸LCD机架式一体机，显示分辨率≥1280\*1024；售后服务：三年免费上门保修。

**1-6、外网杀毒软件：**

1. 控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能,支持50≥客户端，包含≥三年产品维保、升级等服务。
2. 客户端支持操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10/Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012及MAC OS；
3. 支持三家以上主流国产操作系统，包括中标麒麟/Deepin/银河麒麟等
4. 产品支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行；
5. 支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告；
6. 支持加密SSL的控制中心远程访问，支持管理账户并发、密码有效期、鉴别失败锁定等设置；
7. 要求产品生产公司具备面向微软官方级别漏洞发现能力
8. 要求产品具备本地多引擎查杀能力，且引擎可配置；
9. 要求产品具备公有云检测能力，并且公有云特征储备超过100亿；
10. 要求支持以自定义黑白名单的方式来管理全网终端的文件；管理员可以将文件加入白名单或者黑名单；如果文件被加入白名单，客户端就不会再查杀此文件，加入黑名单，客户端就不可以执行此文件；
11. 要求支持客户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽；
12. 支持云复修功能，扫描发现文件遭破坏或被感染时触发修复流程，修复通过360公有云下载正常文件替换遭破坏的文件；
13. 支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置 系统能够对勒索病毒提供防护机制，同时提供解密工具，并支持 “敲诈先赔”服务；在开启时中勒索病毒时，可提供赎金 支持统计指定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率；
14. 支持自动发现设备的IP-MAC地址的绑定；
15. 展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表；
16. 要求支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人；邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等；

**2.1、内网下一代防火墙**

1. 1U构架、最大吞吐量≥2.5G、至少含有传统防火墙、流量管理、应用管理、IPSec VPN、资产识别、防病毒、入侵防护及联动，≥180天日志功能。包含≥三年产品维保、升级等服务。
2. ★支持多链路负载路由，能够基于IP、端口、协议、ISP、应用类型以及国家地域来进行选路由选路；（需提供上述功能截图证明）
3. ★访问控制规则必须支持数据模拟匹配，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；（需提供相关功能截图证明）
4. 访问控制规则必须支持基于网络对象／用户，端口，区域，应用/服务类型的应用访问控制和基于国家/地区的地域访问控制，实现精细化管控；（需提供相关功能截图证明）
5. 支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件内容检测、附件杀毒、URL过滤等，支持根据邮件附件类型进行文件过滤；（需提供相关功能截图证明）
6. 设备必须提供最新的威胁情报，能够对新爆发的流行高危漏洞进行预警和自动处置，支持新的安全事件爆发时，自动扫描内网存在的漏洞，并自动开启防御功能；（需提供相关功能截图证明）
7. ★扩展支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞；（需提供相关功能截图证明）
8. ★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；（需提供相关功能截图证明）
9. ★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；（需提供相关功能截图证明）
10. ★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；（需提供相关功能截图证明）
11. ★支持包含敏感数据业务的识别；（需提供相关功能截图证明）
12. ★支持基于攻击不同阶段的方式来匹配并展示当前资产遭受到攻击的具体所处状态，并详细给出针对性处理建议，展示具体的攻击链并可对威胁进行取证；（需提供相关功能截图证明）
13. ★支持安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况；（需提供相关功能截图证明）
14. ★投标厂商具有CMMI L5，提供截图证明

**2-3、内网服务器：**

1. 规格：工业标准2U机架式服务器
2. 处理器：≥2颗英特尔® 至强® 处理器可扩展家族处理器4110，主频2.1GHz，8核，L3缓存≥11MB
3. 内存：16GB RDIMM ECC 2666 DDR4 内存，≥24条扩展插槽，最大1.5TB内存扩展
4. 硬盘：3块2TB 7.2K 12Gbps热插拔3.5寸SAS硬盘，最大支持8个硬盘扩展。标配支持快擦硬盘/SSD，服务器生命周期结束或者挪作它用时一键删除硬盘/SSD所有信息，只需要几分钟就能保证信息不泄露。
5. RAID功能：独立12Gb RAID卡,支持0,1,5,10,50，可选高端RAID卡，
6. GPU：支持≥3个内部全宽300W或者≥6个内部半宽半高的150W GPU
7. 网卡：标配4个千兆以太网端口，支持failover,loadbalance，可选4个万兆10Gbase\_T/SFP+ 接口以太网卡, 或者2个25GE接口以太网卡，支持独立于交换机的万兆网卡分区技术.
8. 电源：配置1+1冗余热插拔钛金级能效电源，电源输出功率≥750W
9. 安全功能：加密签名固件，硬件根信任，安全启动，自动BIOS恢复，快速OS恢复，系统一键锁定，安全的缺省密码，配置和固件漂移检测，持久日志（包括用户形迹），出厂预装正版服务器安全狗SMART版，随时了解电脑运行情况，系统优化，网络防火墙功能（并提供运行截图）；
10. 服务器管理：前面板上配备有液晶屏，可显示默认或定制信息，包括IP地址、服务器名称、支持服务编号等。如果系统发生故障，该液晶屏上将显示关于故障的具体信息。可监控、报告及控制处理器、内存及系统级的能耗，允许通过一体化管理控制台实现基于策略的功耗封顶。虚拟机功耗映射，可以根据功耗对于虚拟机进行负载平衡以及按虚拟机报告功能；前置专用USB管理口，能够通过手机和平板电脑管理服务器，可以做现场的资产清点
11. 操作系统：需配置有正版win server 2012 R2数据中心版系统
12. 售后服务：3年7x24，部分城市当日4小时原厂备件上门更换服务，配置专属金牌服务经理及专属800/400技术支持电话。

**2-4、内网安全管理系统：**

1. 控制中心：采用B / S架构管理端，支持多级中心统一管理，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能；
2. 客户端支持操作系统：W i n d o w s X P\_S P 3及以上/W i n d o w s V i s t a /W i n d o w s 7/W i n d o w s 8/W i n d o w s 10/W i n d o w s S e r v e r 2003\_S P 2 /W i n d o w s S e r v e r  2008 /W i n d o w s S e r v e r 2012及以上版本，l i n u x 等;
3. 支持中标、麒麟等主流国产操作系统;（提供操作系统厂商提供的兼容证书）
4. 支持W i n d o w s、l i n u x、u n i x、国产系统平台的终端统一平台管控，虚拟机、物理机一致化管理 ；
5. 产品支持终端保护密码，设置密码后，终端退出或卸载杀毒软件、安装或卸载控制中心，都需要输入正确的密码方可执行；
6. 支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告；
7. 杀毒软件生产厂商应具备面向微软官方级别漏洞发现能力;（提供2014年至今少200个以上微软漏洞发现案例，提供微软官方确认链接）
8. 要求产品具备本地多引擎查杀能力，且引擎可配置；（提供产品界面截图）
9. 要求支持以自定义黑白名单的方式来管理全网终端的文件；管理员可以将文件加入白名单或者黑名单；如果文件被加入白名单，客户端就不会再查杀此文件，加入黑名单，客户端就不可以执行此文件；
10. 要求支持客户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽；
11. 产品具备操作系统漏洞集中分发、集中修复，强制修复，自动修复；具备蓝屏修复功能；
12. ）产品具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端P 2 P 补丁分发加速，有效节省带宽资源；
13. 支持统计指 定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率；
14. 支持自动发现设备的I P -M A C地址的绑定；展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表；
15. 要求支持报警（包括邮件、短信、P C端等方式），可以设定多种触发条件，满足条件后自动发送到相关人；报警触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等；
16. 支持与旁路威胁检测系统设备、NGFW、上网行为管理产品联动，达到网关边界联动防御效果；
17. 支持主机防火墙，新建、修改和删除防火墙规则，支持T C P、U D P 和I C M P协议，支持规则优先级；
18. 可统计全网终端或终端应用程序的上传，下载速度与流量；可限制指 定或全网终端的上传及下载速度；
19. 支持冗余有线网卡、无线网卡、3 G网卡、M O D E M、A D S L、I S D N 等设备的外联控制；违规外联发生时可针对内外网连接状态分别设置违规处理措施；
20. 对永恒之蓝勒索病毒等提供有效防护机制，同时可提供相关解密工具，解密工具为自主研发；
21. 支持终端进程红名单、黑名单、白名单功能，可设置核心进程必须运行，也可保护核心进程不被结束；
22. 支持网址黑白名单，通过信任网址白名单可以管理企业网络内信任的网址，加入信任后终端不再将此网址视为威胁；
23. 支持自定义账户登录记录、U盘使用记录、IE浏览记录、最近打开文档、搜索历史记录、共享目录等检查项配置，来评估终端是否被渗透；
24. 支持管理员根据检查项评定终端配置的脆弱程度，定性的标准可由管理员自定义；检查项至少包括身份鉴别、安全审计、访问控制、资源控制、入侵防范几个方面，且可进行扩充;
25. 支持对终端各种外设（U S B存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（U S B口、串口、并口、1 3 9 4、P C M I A）设置使用权限；
26. 支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指 定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件;
27. 支持操作系统、办公软件等正版软件的正版序列号的读取功能，确保软件正版化;
28. 支持软件分发功能，包括分发路径、执行方式、执行提示、执行前条件、执行成功条件等众多分发可配置参数，使分发任务支持更多的使用场景；
29. 支持特定路径或扩展名的文件访问、修改、删除、移动等行为的限制并审计；
30. 支持终端入网健康检查策略，策略检查项至少包括：远程桌面、U盘自动运行、防火墙、I P获取方式、文件共享、屏幕保护、空密码、IE代 理；支持终端修复向导，对不合规的终端提供软隔离、断网;
31. 支持远程协助终端（不依赖W i n d o w s 远程桌面协议）、远程关机、重启终端；远程操作时锁定屏幕、截取屏幕，远程锁定屏幕后需要输入解锁密码才可再次使用；（提供功能截图）
32. 产品应免费提供与第三方运维平台的管理监测数据交换接口，向用户方统一运维平台提供安全监测数据（包括但不限于安装数量、当日查杀病毒数量、当日病毒发现次数、查杀次数等统计数据等）。

**2-5、内网杀毒系统：**

1. 控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能；支持50≥客户端,2个服务器端，包含≥三年产品维保、升级等服务。
2. 客户端支持操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10/Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012及MAC OS；
3. 支持三家以上主流国产操作系统，包括中标麒麟/Deepin/银河麒麟等
4. 产品支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行；
5. 支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告；
6. 支持加密SSL的控制中心远程访问，支持管理账户并发、密码有效期、鉴别失败锁定等设置；
7. 要求产品生产公司具备面向微软官方级别漏洞发现能力
8. 要求产品具备本地多引擎查杀能力，且引擎可配置；
9. 要求产品具备公有云检测能力，并且公有云特征储备超过100亿；
10. 要求支持以自定义黑白名单的方式来管理全网终端的文件；管理员可以将文件加入白名单或者黑名单；如果文件被加入白名单，客户端就不会再查杀此文件，加入黑名单，客户端就不可以执行此文件；
11. 要求支持客户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽；
12. 支持云复修功能，扫描发现文件遭破坏或被感染时触发修复流程，修复通过360公有云下载正常文件替换遭破坏的文件；
13. 支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置 系统能够对勒索病毒提供防护机制，同时提供解密工具，并支持 “敲诈先赔”服务；在开启时中勒索病毒时，可提供赎金 支持统计指定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率；
14. 支持自动发现设备的IP-MAC地址的绑定；
15. 展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表；
16. 要求支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人；邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等；

**2-6、外网核心交换机：**

1. 固定可用千兆端口>=28个，其中千兆电口>=24个，千兆SFP光端口>=4，Console口>=1,。
2. 交换容量>=3.36Tbps，包转发速率>=108Mpps。
3. 支持IRF2智能弹性架构，最大堆叠台数>=9台，最大堆叠带宽>=16G，支持跨设备链路聚合，单一IP管理，分布式弹性路由，支持通过标准以太端口进行堆叠，支持完善的堆叠分裂检测机制，支持远程堆叠。
4. 支持黑洞MAC地址，支持设置端口MAC地址学习最大个数，支持基于端口的VLAN，支持QinQ，支持Voice VLAN，支持协议VLAN，支持MAC VLAN，最大VLAN数(不是VLAN ID)>=4094。
5. 支持GE端口聚合，支持静态聚合，支持动态聚合，支持跨设备聚合，支持最多8个端口聚合；支持最多128个聚合组（IRF2）；支持LACP支持本地端口镜像和远程端口镜像RSPAN；支持流镜像，同时支持N：M的端口镜像（M大于1）。
6. 支持IPv4静态路由、RIP V1/V2、OSPF V1/V2/V3。
7. 支持RRPP（快速环网保护协议），支持Smartlink，支持RSTP功能，支持MSTP功能，支持PVST功能。
8. 支持基于第二层、第三层和第四层的ACL；支持SP/WRR/SP+WRR队列调度；支持基于端口的限速；支持基于流的重定向。
9. 整机提供ACl条目数不小于512条；支持基于端口和VLAN的 ACL；支持IPv6 ACL；支持双向ACL，以便于灵活实现数据包过滤；支持802.1x认证，支持集中式MAC地址认证。
10. DHCP client，支持DHCP Snooping，支持DHCP Snooping trust，支持DHCP Snooping option 82，支持DHCP Server。
11. 支持用户分级管理和口令保护，支持SSH2.0，支持端口隔离，支持 802.1X，支持端口安全，支持MAC地址认证，支持IP Source Guard，支持HTTPs，支持EAD。
12. ★支持SNMP V1/V2/V3、RMON、SSHV2，支持iMC网管系统。
13. 端口定时down功能（Schedule job），支持端口休眠，关闭没有应用的端口，节省能源。
14. 所提供的光模块（如果选配），必须贴有防伪标签，并且可通过命令行方式验证光模块是否原厂认证的模块，提供相关命令和说明。

**3-1、服务器机柜：**

标准19英寸，42U服务器机柜，前后网孔门，尺寸：600\*1000\*2000MM，原厂三年免费上门保修服务。