服务器网络杀毒软件

1、产品控制中心：1套，服务器端点安全软件（Windows Server客户端授权）数量25套，，三年质保及升级服务

2、支持全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell后门、高危漏洞及其各自影响的终端数量

3、支持系统信息的清点，包括操作系统及其版本、环境变量、内核模块、运行服务、启动项、计划任务、注册表、网络连接、开放共享以及国产化终端替代率（真替真用）

4、支持展示最新公布的热点漏洞信息，并且梳理出其中的高可利用漏洞统一展示在热点漏洞页面，方便运维人员一键对当前已接入的终端进行漏洞检测，同时支持设置热点漏洞定时检测（需提供产品截图证明）

5、支持禁止黑客工具启动，包含：冰刃、xuetr、ProcessHacker、PCHunter、火绒剑、Mimikatz的自启动，可以防止黑客攻击

6、支持windows服务器RDP远程登录保护，可开启RDP远程登录二次认证，以防止黑客对服务器的入侵

7、支持流行Windows高危漏洞的轻补丁免疫防御，支持Windows补丁批量一键修复

8、支持图形化显示业务系统、服务器及流量详情 （需提供产品截图证明 ）

9、具备《网络关键设备和网络安全专用产品安全认证》证书。

10、如需配服务器自带服务器。

PC机网络杀毒软件

1、PC端点安全软件（PC-Windows客户端模块授权）150套；三年授权及升级服务。

2、终端防护系统对现有网络兼容，可以对威胁联动处置。

3、为了保证交付质量，产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署；

4、单一管理控制中心可统一管理分别部署在Windows PC，Win服务器以及Linux服务器的客户端软件，简化运维管理。

5、为了保证简单运维，设备需支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议

6、支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、僵尸网络、WebShell后门数量、高危漏洞及其各自影响的终端数量

7、为了保证安全防护的有效性，设备支持本地查杀缓存，具备二级缓存机制：终端侧使用全盘文件缓存，加速本地二次扫描速度，减少对本地虚拟化环境的资源消耗；管理平台侧使用全网文件缓存，加速云查杀速度，减少通过互联网进行云查杀的带宽消耗。

8、支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描，及时发现尚未纳入管控的终端

9、支持对服务器重要目录进行权限控制，仅允许配置的可信进程操作该目录并提供配置指引

10、为了保障单位能够合理划分运维工作权限，设备支持精细化管理，可以在设备上配置不同的权限角色，且支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限；并配置可管辖的终端范围。

11、具备基于本地缓存信誉检测与全网信誉检测，构建医院全网信誉库的检测引擎，做到医院内网一台威胁，全网感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置有效提升查杀效率，减少终端资源开销。

12、能对文件进行实时监控与威胁防御，要求所投软件可实时监控文件的状态，能够在文件读、写、执行或者进入主机时主动进行扫描，且支持根据用户性能偏好设置高、中、低等3种防护级别。

13、为便于医院进行勒索病毒防护，要求产品能够基于勒索病毒攻击的过程，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，并能展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御；支持监控诱饵文件，能够拦截勒索病毒对该文件的修改或加密操作。

14、支持快速定位出全网终端病毒的感染情况；能够与同厂商的安全感知平台进行安全联动，支持管理员在安全感知平台管理界面下发快速查杀任务，并查看任务状态、结果并进行处置；支持与同厂商的网络防火墙进行安全联动，管理员可以在网络防火墙管理界面下发快速查杀任务。

15、为全方位保障医院终端安全，产品需支持威胁检测、终端自保护、文件实时监控、WebShell事件处理、Windows终端安全加固、勒索病毒专防、挖矿病毒巡检、暴力破解检测、Windows终端合规检查、Linux终端合规检查、威胁同步处置与违规外联等各个层面的威胁防御。

16、为保证医院终端的使用合规性，要求软件支持一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果。

17、具备《网络关键设备和网络安全专用产品安全认证》证书。

18、如需配服务器自带服务器。