1.终端防病毒招标参数

|  |  |  |
| --- | --- | --- |
| 推荐品牌 | | 360天擎 |
| 技术指标 | | 参数 |
| ▲系统管理 | | 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、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。  终端许可60个，10个物理服务器杀毒，配置杀毒和补丁分发升级功能,3年软件升级服务 |
| 客户端：与安全控制中心通信，提供控制中心管理所需的相关数据信息；执行最终的木马病毒查杀、漏洞修复等安全操作。 |
| ▲病毒、恶意代码、木马防护 | | 要求产品本身具备病毒检测功能，并且通过CheckMark、ICSA、OPSWAT等各大国际评测机构联合认证。 |
| 要求产品具备本地引擎查杀能力 |
| 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。(提供相关证明) |
| 支持私有云查杀，预置至少2亿黑名单及2000万全面的白名单，终端威胁统一到控制中心查询黑白并进行查杀（提供截图） |
| 要求产品在断网状态下具备不依赖病毒库特征的情况下对未知病毒查杀的能力（提供国内知识产权局的专利受理证明与国际PCT专利受理证明） |
| 要求产品具备主动防御技术（提供至少3项以上技术专利受理证明） |
| ▲补丁分发与漏洞修复 | | 要求产品生产公司具备面向微软官方级别漏洞发现能力（提供2014年至今少20个以上微软漏洞发现案例，提供微软官方确认链`接） |
| 要求产品生产公司具备面向微软官方级别漏洞发现能力（提供2013年至今少15个以上微软漏洞发现案例与相关截图，与微软官方确认截图） |
| 产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能（提供截图） |
| 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P2P补丁分发加速，有效节省外网带宽资源（提供截图） |
| 资产管理 | 单点维护 | 按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控CPU温度、硬盘温度和主板温度 |
| 支持硬件变更，展示终端硬件变动记录，可确认变更或删除记录 |
| 支持正版软件的正版序列号的读取功能，确保软件正版化（提供截图） |
| 支持软件变更，展示终端软件变动记录，可确认变更或删除记录 |
| 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（提供截图） |
| 支持远程协助终端、远程关机、重启终端 |
| 终端发现 | 支持手动配置服务器、扫描参数、进行周期性扫描，可手动配置发现的终端类型 |
| 支持统计指定分组或全网的终端扫描数、终端安装数、未安装终端数及安装率。 |
| 支持自动发现设备的IP-MAC地址的绑定（提供截图） |
| 移动存储介质管理 | | 支持客户端自主申请移动存储介质注册； 支持移动存储介质权限划分设置，有效控制不明来历的移动存储可能带来的病毒传播等隐患 支持移动存储介质外出管理、例外管理等 |
| XP盾甲 | | 支持对XP系统进行系统加固、热补丁修复、危险应用隔离、“非白即黑”安全策略四大修复措施 |
| 终端准入 | | 支持旁路终端准入部署方式，避免串行设备部署单点故障； 支持有线、无线基于应用协议准入方式，准入配置支持保护服务器区域、例外终端等灵活的配置方式 支持标准802.1X准入，支持动态VLAN、动态ACL下发； |
| 支持基于终端的ACL，可以基于协议、端口来控制终端流量，从而无需操作交换机达到终端网络控制目的（提供截图） |
| 支持入网健康检查策略，策略检查项至少包括：远程桌面、U盘自动运行、防火墙、IP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，并进行修复向导和一键修复功能 |
| 安全审计 | | 支持指定扩展名的文件访问、修改、删除、移动等行为的审计 |
| 支持网络共享输出控制与审计 |
| 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 |
| 日志报表 | | 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； 展示全网终端木马库日期比例，可方便的查看全网终端木马库的情况； 展示全网终端病毒库日期比例，可方便的查看全网终端病毒库的情况 |
| 展示指定时间段内指定终端修复漏洞，病毒查杀，木马查杀的情况（提供截图证明） |
| 支持大数据引擎系统，可将全网终端日常运维数据汇聚存储分析，并根据客户运维管理所需的要求定制报表（提供截图证明） |
| 其它 | | 支持与旁路威胁检测系统设备、下一代防火墙、联动，达到网关边界联动防御效果（提供截图证明） |
| 支持控制中心数据恢复与备份 |
| ▲产品资质 | | 公安部销售许可证 |
| 计算机软件著作权证书 |
| 军B+级军用信息安全产品认证证书 |
| ▲厂家资质 | | 公司具备网络安全应急服务支撑单位（国家级） |
| 中国国家信息安全漏洞库支撑单位 |
| 商用密码产品生产定点单位 |
| 国家信息安全漏洞共享平台技术组成员 |
| 微软MAPP伙伴 |
| 公司具备向国家信息安全漏洞库（CNNVD）提交漏洞的能力，2015年提交漏洞数量不少于10个 |