终端安全—防病毒软件参数要求

指标项	指标要求
数量要求	提供 300 个 Windows PC 客户端功能授权，15 个服务器端授权，此数量提供 3 年防病毒、主机防火墙、补丁管理功能服务授权。
平台环境要求	软件形态需要包含管理控制中心、客户端软件。
	管理中心操作系统支持 Windows Server 2012 R2/2016/2019/2022 的 64 位版本（简体中文版）；支持 CentOS 7 系统。
	控制中心支持级联管理，可支持 5 级级联部署，亦可单机和集群部署混合级联。
	客户端支持操作系统：Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10/windows 11。
	支持单个页面展示在线终端数量、控制中心当前 CPU、内存、硬盘使用百分比、终端在线率、终端正常率、病毒查杀趋势、感染病毒终端、漏洞补丁统计等信息，均可通过图形化展示。
	支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心。
	支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护。支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性。
防病毒防护	病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本。
	病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间显示。
	病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。
	支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务。
	支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少 10 层模式下的扫描。
	支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护。【提供功能截图并加盖厂商公章】
	支持网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁。
	支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。
	支持防护对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。

	客户端弹窗支持免打扰模式和智能模式，使用免打扰模式可以对不能弹窗的终端设备中避免弹窗。使用智能模式是智能调整弹窗，对已知的病毒自动处理，对未知的病毒提示处理。
补丁管理	支持对 Windows 操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat 和 Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复。
	每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。【提供功能截图并加盖厂商公章】
	允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复。
主机防火墙	支持主机防火墙功能，通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围，支持对设定进程名称、进程路径，支持模糊规则。
	支持展示防火墙上报日志，展示终端基础信息、拦截规则名称、拦截时间、操作、协议、源地址，目的 IP/域名、源端口、目的端口。