- **工控主机卫士 NESM3000-GK-S7000 产品简介**

NetEye 工控主机卫士系统是东软专门为工业主机打造的一款安全防护管理软件。系统采用分布式架构，安装在工业上位机 和工业服务器上，基于白名单智能匹配、智能杀毒、主机加固等技术，有效地防止病毒和恶意程序入侵攻击、控制移动储存的非 法接入和集中管理工业主机，从而有效解决工业主机安全威胁问题，提高工业主机系统安全防护能力。

- **功能描述**

资产自动发现能力

东软统一安全管理平台具备完善的资产管理能，可通过资产自动发现能力，主动和被动收集采集网络中的资产信息，并可直接一键入库，方便大规模的资产录入。

白名单

➢程序白名单，加入白名单的程序能正常运行，防篡改。支持白名单的一键初始化、 单个程序或单个目录中程序的添加和删除、批量导入和导出功能；

➢支持白名单功能开启、关闭；

➢支持对白名单外程序防护模式设置，可对异常程序进行告警或阻断。

设备管控

➢ 支持 USB 设备管理，USB 设备插入默认为不可访问状态，可单个或整体关闭 USB 设备防护状态，可允许/禁止 USB 程序执行或禁止；（Windows）

➢ 支持 USB 设备管理，USB 设备插入默认为不可访问状态，可单个或整体关闭 USB 设备防护状态；（Linux）

➢ 支持网卡管理，网络配置信息，可启用/禁用网卡；（Windows）；

➢ 支持存储设备管理，管理分区状态和磁盘列表的总容量、剩余流量等信息，可对 C 盘进行病毒查杀；（Windows）

➢ 支持 DVD/CD-ROM 驱动器管理，管理光驱信息，可启用和禁用光驱；（Windows）

➢ 支持可信 U 盘管理，自动识别出可信 U 盘，以列表形式展示，可信 U 盘默

认可访问， 并且不可设置为防护状态；

➢ 支持串口设备的启用和禁用；（Windows）

➢ 支持对蓝牙设备的启用、禁用功能。（Windows）

主机加固

➢ 支持一键扫描当前操作系统近 40 项安全配置基线，并支持自主选择加固基线配置；

➢ 支持对 Email、Web、FTP 等高风险服务精准管控；

➢ 支持对主机加固的所有配置项进行一键备份和恢复；

➢ 支持对注册表安全防护，可将注册表中某个键值添加到注册表防护列表中，防止用 户对它的恶意或者无意的修改和删除；（Windows）

➢ 支持 ssh、ftp、mysql 服务的防暴力破解功能，支持系统防端口扫描功能，并能针 对超时时间及重试次数做相应限制，并产生相应告警。支持通过配置单 ip 请求时间 范围、错误次数来防止暴力破解 ssh、ftp、mysql 服务。（Linux）

➢ 支持添加、删除对应的非法 IP，主机访问对应 IP 触发非法外联告警。（Linux）

➢ 支持对 IP、IP 段、单个端口或者多个端口的安全防护，并且可自主选择传输协议，可允许或阻止符合规则的 IP/端口出入站操作，支持已定义规则删除；

➢ 支持对常见危险端口的加固操作，降低病毒或异常程序入侵风险，支持恢复已加固 端口的状态；

➢ 支持对系统用户管理，可禁用/启用对应的系统用户。

病毒查杀

通过对文件进行启发式病毒特征匹配，实现对病毒文件的隔离清理；在病毒查杀的基础 上，对应用程序进行自定义加入白名单，保障只允许正常工业应用执行；

➢ 支持显示当前扫描文件，精确显示扫描进度，可以立即停止当前扫描，仅显示当前 扫描到的病毒；

➢ 支持快速扫描，对系统关键路径进行快速病毒查杀；

➢ 支持全盘扫描，对系统全路径、全文件进行彻底扫描；

➢ 支持自定义扫描，自定义路径进行病毒扫描；

➢ 支持病毒库升级功能，分为在线升级和离线升级两种方式；

➢ 信任区，支持查杀出的病毒加入信任区，支持对信任区文件“取消信任”操作；

➢ 隔离区，支持查杀出的病毒加入隔离区，支持对隔离区文件“取消隔离”和“彻底 删除”操作。

日志审计

➢ 支持全面的行为审计，支持对关键操作进行事后审计，如：文件操作、进程操作、 服务操作、网络外联、系统信息、以及软件用户和系统用户登录等；

➢ 实时的资源监控，支持对 CPU、内存、流量做实时状态跟踪监控。

超低的主机资源占用

系统包含多个子系统。安全芯片散列计算小于 1 毫秒，白 名单检索小于 3 微秒，进程完整性校验小于 1 秒。内存占 用低，极大地节省了主机资源。