三中科技工控安全卫士系统

产品名称	三中科技工控安全卫士系统
公司名称	郑州三中网安科技有限公司
价格	.00/个
规格参数	
公司地址	郑州高新技术开发区长椿路11号
联系电话	0371-55519655

产品详情

产品简介

工控卫士是专门保护工控主机环境的一款安全软件产品，通过在工控上位机和服务工控卫士完整性保护等，它实现了对工控主机全面的安全防护。

工控卫士通过监控工控主机的进程状态、网络端口状态、USB端口状态，以白名单的技术方式，全方位地保护主机的资源使用。根据白名单策略，工控卫士会禁止非法进程的运行，禁止非法网络端口的打开与服务，禁止非法USB设备的接入，从而切断病毒和木马的传播与破坏路径。

工控卫士提供严格的USB存储设备管理，U盘、USB硬盘等存储设备在接入工控主机使用前，必须先经过使用授权。未经授权的USB存储设备不能使用，经过授权的设备，也不能进行超越其权限的操作。通过授权管理，工控卫士能够有效防止文件泄密。同时，工控卫士还会审计USB存储设备的文件操作行为，为事后追责提供依据。

工控卫士依托三中科技的技术优势，充分研究、吸收工控网络安全攻防技术的前沿成果，极具技术前瞻性。对于近年发现的Havex、沙虫等最新工控病毒、BadUSB等最新攻击方法，工控卫士都提供了有效的防护方法，在国内工控安全业界具备领先优势。

产品特点

专业

专业针对工业控制主机的防护需求

专业防护网络病毒和工控病毒

专业防护最新攻击手段

全面

提供从工控上位机到工控服务器的全面防护

监控进程运行状态，阻止不明进程启动

监控网络端口、网络流量

监控USB口使用，防止U盘攻击.

易用

支持服务器的统一管理，易于管理和大规模部署

支持白名单导入导出，易于定制化

数秒内扫描主机状态，易于建立白名单

操作简单快捷，易于用户理解

产品价值

专业解决工控上位机、服务器的安全问题。

工控卫士专业针对工控网络上位机、服务器的防护需求，能有效防护IT网络病毒和工控病毒（如Havex）的运行，针对工控网络最新的攻击手段（BadUSB攻击等）也能被有效阻止。

防范用户违规操作和误操作，增强工控网络的综合“ 免疫 ”能力。

工控卫士通过应用程序、网络、USB移动存储的白名单策略，可以有效防止用户的违规操作和误操作，阻止不明程序、移动存储介质和网络通信的滥用，有效提高工控网络的综合“ 免疫 ”能力。

监控操作行为，方便事后审计。

工控卫士能对上位机和服务器上的违规操作进行监控，如监测进程的运行状态、监测USB接口及操作，并记录详细的日志，方便事后的审计和追查。

典型应用

工控卫士部署于工控现场的监控管理层。

工控卫士监控上位机与服务器的进程、网络、USB状态，及时禁止非法进程的运行、非法网络端口的打开、以及非法USB设备的接入。

工控卫士监控USB存储设备的接入，按照权限设置，严格控制USB存储设备的使用，防止机密文件泄漏，并为事后追责提供依据。

产品参数

进程管理

进程白名单 禁止白名单以外的非法进程运行，并产生安全事件，记录非法进程的运行企图。

进程检查 采用独创性的“ 暂停-检查-启动 ”三步过程，任何进程在启动前，都必须暂停下来接受特征验证，从而可以在恶意进程真正运行前将其终止。

隐藏进程检测 能够发现被隐藏的病毒进程，禁止其运行。

全面进程信息 能够列出进程句柄，并能发现隐藏的DLL。

程序完整性检查 通过检查程序的证书、校验值，来确认程序的完整性，从而在有害进程启动前即将其终止。

网络管理

网络限速 当主机网卡的通信速度过高时，能够控制其网络流量，避免网络拥塞。

网络端口搜索 能发现使用PCAP发包方式隐藏起来的网络通信。

智能网络优化 提供QoS管理，当网络流量过高时，能通过限速来降低流量，而不需要封杀网络端口，从而降低系统运行风险。

USB管理

USB白名单 禁止白名单以外的非法USB设备连接，并产生安全事件，记录非法USB设备的连接企图。

USB端口保护 提供端口级保护。

USB监控状态 提供内核态PNP监听。

USB设备识别 支持复合型USB设备识别。

USB设备授权 提供USB存储设备的多种操作权限授予：读写、只读、禁止使用。

USB设备行为审计 提供USB存储设备的操作记录，此记录不可删除、不可篡改。

白名单管理

主机扫描 提供主机扫描功能，快速建立白名单。

白名单导入导出 提供白名单的导入导出功能，快速复制白名单，提高部署速度。

白名单追加 需要运行新的程序、添加新的网络服务和USB设备时，可以很方便地将这些新的设置追加到白名单中。

安全事件管理

安全事件通知 探测到非法进程、非法网络端口、非法USB设备时，会产生安全事件，提醒用户。

安全事件日志 提供安全事件的记录，此记录不可删除、不可篡改。