工控安全监测与审计系统

产品概述

工控主机安全卫士系统是一套对操作员站、工程师站和服务器等工控系统主机进行安全加固的软件产品。产品颠覆了传统防病毒软件的 “黑名单“思想，采用与其相反的轻量级白名单 “ 方式，可以快速 有效阻止如震网病毒 BlackEnergy 等工控恶意代码在主机上的执行、感染和扩散。在此基础上，对 U 盘等移动存储介质也做了安全防护和管理，防止病毒木马通过移动存储介质在内网主机上交叉感染。产品有单机版和网络版两种形态，网络版本可以对部署在主机上的主机安全卫士进行集中管控，包括策略统一下发、软件统一管理、日志统一查看、外设统一管控等。

产品特点

- 自学习建立程序白名单

一键式智能学习工控主机系统中程序文件及其它可执行文件特征，快速建立白名单库和安全基线。

- 阻断病毒木马的执行和扩散

精准阻断一切白名单安全基线外的可执行文件在主机上运行，有效隔离病毒、木马等恶意代码，防止通过主机向网络进行扩散。

- 可信证书白名单

对可执行程序的签名证书进行检查，带有可信厂商证书的应用程序得以执行，从而简化可信厂商应用发布和部署成本。

- 核心系统文件保护

提供主机操作系统重要配置文件路径和注册表的完整性检查和安全保护，防止被恶意软件破坏。

- USB 管理

对接入的 USB 设备进行管控，对移动存储介质支持“只读” 、 “读写"、 “禁用“ 三种管理方式，防止携带病毒威胁的存储介质感染主机。

- 全面丰富的告警信息

告警信息种类标记包括程序白名单告警、U 盘外设使用不合规告警、注册表和关键配置破坏告警、白名单安全基线 告警等，直观展示系统中存在的安全问题。

- 兼容更多工控系统、资源占用小

全面支持工控环境下微软已停止维护的老旧 Windows 系统并兼容各类厂商工控软件，不会误杀工控系统文件。占用系统空间小，对工控主机系统性能要求低，不会对工控系统的监控软件和其他组态软件运行造成影响。

典型部署

- 单机版安装在工业网络的各类主机（工程师站、操作员站及各类服务器）上
- 网络版除在主机上安装软件外，还需要在网络中部署国泰网信安全管理平台(GTEC-UM)设备进行集中管理

江南三体河北信息安全技术有限公司

地址：河北省廊坊市广阳区友谊路462号

网址：http://www.stiot.net

邮箱：jnst@jnsanti.net