力控科技 FORCECON | HUACON 力控华康

工业主机
安全卫士
HC-IMG

北京力控华康科技有限公司

www.sunwayland.com

目 录

产品概述 02

产品架构 03

产品特点 04

典型应用 06

产品概述

行业背景

工业控制系统已广泛应用于电力、轨道交通、石油石化、航空航天等领域。目前，大量的涉及国计民生的关键基础设施依靠工业控制系统来实现自动化操作。工业控制系统已经成为国家关键基础设施的重要组成部分。

随着工业化与信息化进程的不断交叉融合，越来越多的信息技术应用到了工业领域。由于工业控制系统广泛采用通用网络设备和IT设施，以及与企业信息管理系统的集成，传统信息网络所面临的病毒、木马、入侵攻击、拒绝服务等安全威胁也正在向工业控制系统扩散。工业系统由于环境封闭，往往只注重功能是否可靠、可用，降低了对系统安全性的关注，也不会对系统存在的安全漏洞进行升级或打补丁，这就导致系统长期运行后会存在大量的安全漏洞，也因为缺乏对移动接入设备的有效管理和对当前设备安全设置的不了解，使得系统安全在面对网络安全攻击时显得极其脆弱，给生产环境带来极大的安全隐患。

针对广泛部署的工业设备，我司推出了基于白名单防御的工业主机安全卫士，解决工业主机安全隐患。

工业控制系统上位机面临的安全威胁

◉安全补丁缺，操作系统、数据库及应用软件存在漏洞，补丁没有及时安装。此类漏洞可被轻易利用获取操作系统权限进行恶意破坏；

◉没有安全漏洞发现设备，控制系统内未部署漏洞发现设备，无法对站内主机存在的安全漏洞进行定期监测；

◉进行维护工作时会使用移动存储介质接入操作员站和工程师站，虽然经过格式化或者一些数据摆渡、单向传输等手段，避免了一些常见的病毒和木马的传播，但多数工控系统病毒和木马都是特意研制的，能够通过技术手段渗透进主机中，工控数据和配置文件仍存在外泄的可能，给工控数据的完整性、保密性带来严重威胁；

◉不完整的配置变更管理，控制系统的配置变更管理不完全，在系统漏洞发现、故障处理、紧急预案执行等方面存在隐患。

工业主机安全卫士

工业主机安全卫士是针对工业控制系统的主机安全类产品，基于应用程序白名单管理机制，禁止非法进程运行，阻断工控主机中病毒等恶意程序的运行以及木马、蠕虫的传播。

工业主机安全卫士支持控制USB移动存储设备权限，具有读写、只读、禁用三种模式。禁止非法USB设备连接到主机，确保没有非法设备连接、没有越权操作行为，有效防止文件泄密。目前产品广泛应用在工程师站、操作员站、接口机、服务器等各个场景。

工业主机安全卫士具有审计与告警功能，实时记录非白名单程序运行、违反USB管控策略、管理员操作等行为，为用户提供安全审计依据。

“针对工业控制系统的主机安全类产品；

支持控制USB移动存储设备权限；

具有审计与告警功能。”

产品架构


工控主机安全卫士产品架构图(网络版)
平台层
统一管理
策略下发
信息收集
资产登记
syslog日志
业务层
一键扫描
白名单管理
系统设置
告警管理
日志审计
系统托盘
防疫卫士
外设管控
服务层
Windows/Linux Native API服务管理
Sqlite日志管理
Sqlite+tiny-AES-c用户管理
USB外设管理
Boost Sericliza-tion+tiny-AES-c设置
c++17 Filesystem文件扫描
授权管理
驱动管理
驱动层
Kernel API SSDT Hook/ Ob Callback/Syscall Hook进程防护、自保护
USB过滤
tiny-AES-c关键设置/白名单读写
日志上报

产品特点

程序白名单

工业主机安全卫士支持扫描工业主机所有可执行文件，生成程序白名单，识别、阻止任何白名单外的程序运行。可以通过应用程序白名单内的观察列表实时监控到试图运行的白名单外程序，针对性制定防护策略，阻止恶意程序的执行与扩散。

可选防护文件类型

支持自定义选择文件防护类型，选中后的文件类型若不在白名单内，会受到白名单防护策略限制。

外设管控

工业主机安全卫士支持制定外设设备接入主机策略，对外设设备如U盘、移动硬盘进行策略配置（读写、只读、禁用），有效阻止数据泄漏，阻止主机通过U口感染病毒。

除U盘管控外，工业主机安全卫士还支持对串口、并口、网口、无线网卡、无线热点、3G4G网卡、虚拟网卡、蓝牙、光驱、软驱、无线热点等设置启用禁用策略，多方位保证外设环境安全。

注册U盘管控

支持对注册U盘的访问控制，包括禁用、只读、读写，支持普通U盘注册为可信U盘，并显示和管理注册U盘列表。

安全U盘管控

支持对安全U盘的访问控制，包括禁用、只读、读写。

防疫卫士

工业主机安全卫士支持通过防疫卫士保护关键业务软件，通过内核级防护保障工业软件的静态资源和动态资源不被恶意破坏，（静态资源包括文件/数据/注册表），可以防止内存被恶意篡改，进程被恶意杀死，系统被意外重启等。

支持防疫卫士自动建模，通过自身软件库精准识别关键业务软件，可以对关键业务软件全生命周期全面防护。

专杀工具

工业主机安全卫士软件附带“永恒之蓝”蠕虫专杀工具，对已经感染“永恒之蓝”勒索蠕虫病毒的主机，可以进行病毒清除，且支持通过禁用端口阻断永恒之蓝病毒扩散，避免感染内网其它终端。

白名单管理

工业主机安全卫士支持管理全部白名单，可对白名单库追加文件/目录。且对特定的目录和文件可以加入扫描例外，扫描例外的文件或程序受白名单策略管控。（用户可以自定义将不信任的软件加入扫描例外）。

对频繁更新的软件可以加入信任文件，信任文件中的程序运行不受白名单策略的限制。

告警与审计

工业主机安全卫士会根据系统策略记录日志，如白名单防护模式为防护/U盘管控为禁用时，白名单外程序运行/禁用外设设备插入时，会产生相关告警信息，气泡告警提示并产生详细告警记录。

工业主机安全卫士会对程序运行、外设管控、用户操作等行为记录详细日志并支持导出功能，供工作人员做安全审计工作。

Syslog 日志上传

工业主机安全卫士支持设置Syslog上传的IP和端口，方便上传自身的告警、事件日志到工控安全管理平台以及支持Syslog协议的第三方管理平台。

网络防护

工业主机安全卫士支持根据现场环境，自定义对高危端口或不常用端口禁用，保障工业现场安全性。

集中管理

工业主机安全卫士可以在安管平台进行集中管理：部署在不同位置的多个工业主机安全卫士可以通过安管平台进行集中/单点策略下发、集中管控白名单扫描、主机加固、加固设置、网络防护等策略，并可以集中收集日志和告警信息供安管平台统计分析。

集中管控范围包括但不限于以下功能：

1. 终端概况

工业主机安全卫士可以实时上报主机CPU占用率、内存占用率、硬盘占用率、实时流量、在线离线状态等信息，支持在工控安全管理平台统一查看主机卫士整体态势。

2. 应用级白名单库

工业主机安全卫士支持上报所有应用级白名单到安管平台，平台可以查看所有主机卫士的全部白名单，支持对所有白名单库进行编辑，防止盗版软件混入白名单库，引起客户方法律纠纷。

3. 白名单管理

工业主机安全卫士支持通过安管平台进行远程白名单扫描、信任路径、扫描例外添加等操作。

4. 用户管理

工业主机安全卫士支持通过安管平台进行远程用户增删改查等操作。

5. 系统设置

工业主机安全卫士支持通过安管平台进行远程系统设置，包括白名单防护模式、外设管控策略、告警阈值设置、Sylsog设置、自启动开关设置等。

6. 资产登记

现场操作员可以在工业主机安全卫士软件自助在线录入主机所属的业务部门、编号等信息，实现资产属性的统一维护，代替传统手工登记方式，降低管理成本。

7. 策略同步

工业主机安全卫士在离线情况下，和安管平台断开连接后可能会导致和安管平台策略不一致，待安全卫士与安管平台恢复连接后可以一键同步策略，保持网络版主机卫士的策略统一性。

8. 自动注册

工业主机安全卫士在网络联通情况下，安装后可以自动注册到安管平台，无需手动输入安管平台IP和端口，提高用户体验，节省部署时间。

9. 告警与审计日志

工业主机安全卫士支持实时向安管平台上报自身告警与审计日志，安管平台支持饼状图、柱状图形式可视化查看告警与审计日志的分布状态、TOP5日志和告警分布状态等。

“永恒之蓝”专杀工具—防勒索

工业主机安全卫士软件附带“永恒之蓝”蠕虫专杀工具，可有效解决工业主机感染“永恒之蓝”勒索蠕虫病毒问题。

“最小集”白名单认证

支持白名单删除时做是否为系统文件的校验，防止防护状态下误删在白名单内的系统文件导致系统无法运行。

“自定义”防护文件类型

支持自定义选择文件防护类型，选中后的文件类型若不在白名单内，会受到白名单防护策略限制，有效防止文档或者其他非可执行文件类型被病毒攻击导致工业主机安全性受到威胁。

防疫卫士“自动建模”

支持关键业务软件自动建模，精准防护关键业务安全，对业务软件实行全生命周期防护，保障工业主机稳定运行。

无侵入对接安管平台

工业主机安全卫士可以无侵入式快速接入安管平台，在网络联通的状态下可以自动注册到安管平台，无需手动填写安管平台的IP和地址。

以插件化方式存在于安管平台内，当工业主机安全卫士更新后，安管平台会同步更新插件，无需同步针对更新内容开发，减少后期维护成本。

资产登记

能够自动上报工业主机CPU、内存、硬盘等基础信息，形成资产清单；同时，管理员可以自助在线录入主机所属的业务部门、编号等信息，实现资产属性的统一维护，代替传统手工登记方式，降低管理成本。

工业软件全面兼容

对主机资源占用低（CPU占用小于5%，内存平均占用小于15MB，单文件平均扫描时间3s左右），不会对工业现场主机的监控软件或组态软件等的正常使用造成任何影响。

多系统全面兼容

支持全系列Windows系统、支持RedHat、CentOS、Ubuntu等主流Linux操作系统、支持银河麒麟、中标麒麟、凝思、统信等国产系统，满足自主可控性。

◉Windows：Windows 2000及以上版本均可（如Windows XP、Windows7、Windows8、Windows10、Windows11），32、64位版本均支持，Windows Server 2003及以上版本（如Windows Server 2008、Windows Server 2012、Windows Server 2016）；

◉Linux：支持 Redhat6.x、Redhat7.x 、CentOS6.x、CentOS7.x、Ubuntu10.x、Ubuntu12.x、Ubuntu14.x、Ubuntu16.x、Ubuntu18.x、Ubuntu19.x、Ubuntu20.x、Ubuntu22.x、Debian7.x；

◉国产系统：银河麒麟（服务器版/桌面版）、中标麒麟操作系统、凝思安全操作系统 、统信服务器操作系统 、湖南麒麟、openEuler；

支持国产海光 、兆芯、飞腾系列处理器。

典型应用

工业主机安全卫士支持但不限于以下工控环境中：

◉ 电力发电、电力输送；
◉ 石油开采、石油运输、石化炼油；
◉ 煤矿开采、煤化工；
◉ 生产制造业。

降低成本，防范未知威胁

工业主机安全卫士通过建立稳定的计算机环境，能对未知的病毒进行免疫。无论是通过社会工程学的方式，还是利用零日漏洞的高级可持续威胁攻击，都无法侵入计算机环境。工业主机安全卫士不需要做任何的更新就能抵御不明攻击行为。安全维护成本大大降低。

安全审计，及时告警

工业主机安全卫士能对系统上的操作进行监控，如检测进程运行，检测USB接口的接入状态和时间，白名单外的应用程序信息及时告警，方便还原安全真相。

保障关键业务，阻止病毒及其变种

工业主机安全卫士设计初衷是专门针对工控网络中的操作系统进行安全防护，提供完全适用于工控行业的安全防护。首先为保障关键业务的运行，建立稳定的运行环境，同时遏制迄今为止爆发的病毒（震网、Havex、勒索）等变种的运行。因为有针对移动设备的安全管控，从多方面阻止了病毒感染主机的途径。

杜绝非法应用，保护关键对象，保障核心资产的完整；工业主机安全卫士通过白名单机制，可以有效的杜绝非法应用运行，杜绝恶意程序修改、删除核心注册表和文件，同时也能阻止内部员工误操作等行为。

力控科技 FORCECON

北京力控华康科技有限公司

地址：北京市海淀区天秀路10号中国农大国际创业园1号楼
总机：010-62839678
全国统一服务热线：400 650 1353
www.huacon.com.cn

关注公众号　关注小程序