H3C 工控主机安全卫士

产品概述

H3C 工控主机安全卫士是针对工业控制网络主机安全提供的智能化软件形态安全防护产品，通过智能识别工业主机应用程序，基于进程白名单管理机制，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。

H3C 工控主机安全卫士通过完善的 USB 移动存储设备权限与操作管理，禁止非法 USB 设备连接到工控主机，同时对合法 USB 设备的操作行为进行审计和追溯，确保没有非法设备连接、没有越权操作行为以及有效防止文件泄密。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。

产品特点

工控主机运行环境全面保护

- 通过白名单机制为终端计算机创建了一个安全的运行环境，非法进程和应用程序无法通过安全检验，确保将病毒、木马以及恶意软件阻挡在终端运行环境之外；
- 用户建立白名单，若有程序运行时会与白名单进行比对，阻止白名单之外的应用程序运行；
- 终端用户可通过申请、管理员审批的方式扩展白名单或形成新的白名单；
- 运行模式分为执行与观察，执行会禁止白名单外的应用程序启动；观察则会允许启动；无论哪种都会以桌面通知的方式进行提醒，并记录日志。

USB 设备全面安全管控

- 针对工业主机上 USB 存储设备的使用，提供全面的包括授权、操作、审计和追溯等在内的安全管控能力，在防御 USB 病毒木马传播、勒索病毒等攻击行为的同时，向用户提供完整的 USB 操作审计记录，帮助客户提升事后追溯能力；
- 严格控制终端随意使用 USB 存储设备来传递数据，防止来历不明的 USB 存储设备接入系统；
- 外设状态分为自由使用，禁用，禁止向 USB 存储设备拷贝文件，并记录日志。

主机外设统一管理

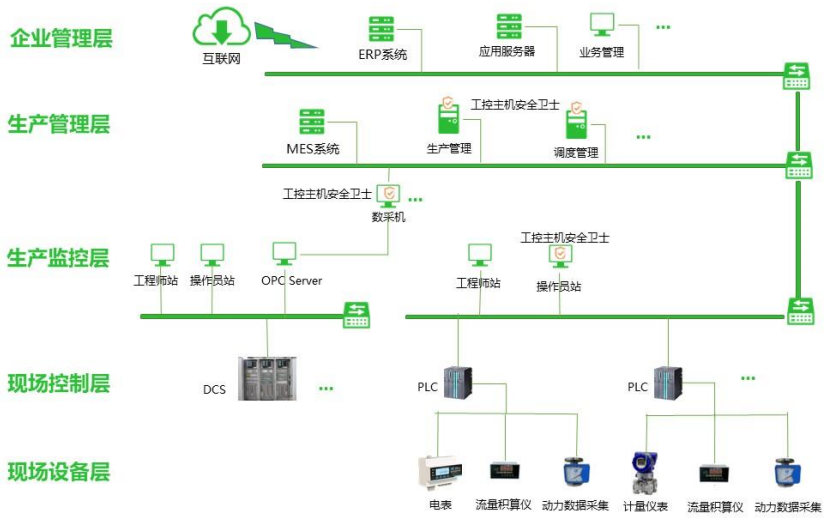
- 支持多种类型的外设管控（光驱、刻录机、网卡、软驱、串口、并口、蓝牙等）
- 严格控制终端随意开启外设，并会生成审计日志
- 可统一、单独为终端设置外设管理策略。

轻量稳定 简单易用

- 工控主机安全卫士产品，采用一键式安装，部署方便，简单易用，完美兼容各类工控主机系统；
- 具有强大的自我防护能力，支持程序防卸载、文件防删除、服务防关闭、进程防关闭等功能。

典型组网

在现场控制层的工程师站、操作员站、服务器以及网关机（Buffer）上部署专用的工控主机安全卫士，通过应用程序、USB 移动存储设备的白名单策略，防止用户的违规操作和误操作，阻止不明程序、移动存储介质的滥用，有效提高工控网络的综合“免疫”能力。



H3C 工控主机安全卫士应用组网图

订购信息

选购一览表

模块	数量	备注
H3C SecPath ISG 工控主机安全卫士 10 个主机授权函	1	必配
H3C SecPath ISG 工控主机安全卫士 50 个主机授权函	1	必配

新华三技术有限公司

北京总部
北京市朝阳区广顺南大街 8 号院 利星行中心 1 号楼
邮编：100102

杭州总部
杭州市滨江区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

http://www.h3c.com

客户服务热线

400-810-0504