奇安信网神工业主机安全防护系统IEP

守护信息世界通往物理世界的大门

奇安信网神工业主机安全防护系统是工业主机一体化安全防护软件，通过智能生成白名单管控技术、外设管控技术、病毒入口拦截、运行拦截、扩散拦截等技术，实现防御病毒攻击、勒索行为，恶意程序运行、违规外设接入等针对工业主机的威胁。从而实现对工业主机的全生命周期的安全防护，保障生产的连续和稳定。

用户价值 CUSTOMER VALUE

工业主机安全防护，保障生产连续性

采用多维度白名单防护技术、关卡式病毒拦截、主机加固、外设管控等一体化复合防护技术，有效抵御勒索行为、病毒、木马、漏洞利用等对工业主机的攻击与破坏行为，真正帮助企业解决主机安全问题。

工业主机风险集中管控，提高运维效率

能够对工业主机的告警进行实时的集中展示和管理，提升工业生产网安全运维的时效性和便捷性，保证管理员对于工业主机安全风险第一时间进行处置和响应。

工业资产自助管理，维护完整资产清单

能够自动识别工业主机硬件基础信息，形成资产清单；同时，管理员可以自助录入主机所属的业务部门、编号等资产信息，基于组织架构实现资产属性的统一维护，从而代替传统手工登记方式，降低管理成本。

产品功能 PRODUCT FUNCTIONS

白名单管控

扫描工业主机中的程序，对确认无风险的可执行文件生成一个唯一的特征码，将特征码集合起来形成特征库，即程序白名单。只有白名单内的程序才可以运行，其它程序启动都被拦截，以此防止来自病毒、木马、违规软件的攻击。

关卡式病毒拦截

从“病毒入口-病毒运行-病毒扩散”三个环节层层设防，步步拦截，进行漏洞防御、病毒扫描、白名单管控、外设管控、已有病毒防扩散等安全管理，做到病毒进不来、启不动、扩散不了，实现主机安全无死角病毒防护。

工业主机资产管控

自动识别工业主机CPU、内存、硬盘等基础信息，形成资产清单；同时，管理员自助可以基于组织架构录入工业主机所属的业务部门、编号等资产信息，实现资产属性的统一维护，代替传统手工录入维护方式，降低管理成本。

主机安全加固

可针对核心工业参数配置等重要文件、目录及注册表进行保护，不允许进行修改、删除以及目录、文件重命名等操作，当正常修改需要允许访问权限时可以将正常访问进程名或进程路径加入到例外设置中进行操作的允许，其他修改行为均进行阻止和记录日志。

奇安信 新一代网络安全领军者

集中配置管理

通过控制中心对网内所有工业主机进行安全策略管理、配置下发、模块定制等，实现统一管控和安全风险分析。同时，针对于分部和总部可进行级联部署和配置、风险管理，尤其对于较大规模主机防护环境，集中管理会显著提升运维效率。

安装
- 安装前：感染型病毒自动检测
- 白名单部署前：病毒全盘扫描、病毒处理

运行
- 入口、运行、扩散拦截：漏洞防御/白名单管控、外设管控/主机加固、病毒实时防护/网络防护

监控
- 风险管理
- 资产管理
- 配置管理
- 用户管理

白名单工作模式	告警模式 / 防护模式 / 关闭模式	
白名单管理	全盘扫描、一键追加、控制中心管理	信任列表、扫描例外 / 安装追踪
病毒处理	全盘/自定义扫描	病毒实时防护 / 病毒强杀 / 病毒隔离 / 病毒信任

产品优势 PRODUCT ADVANTAGES

软硬件适配能力强

“多样式”主机兼容：
除主流系统环境外，支持Win2000、Windows Server2003等老旧操作系统；各类Linux系统及国产化操作系统；兼容各种工业组态软件的复杂环境，支持256M内存等低配硬件环境。

工业网络威胁与异常行为的全面监测

“关卡式”病毒拦截：
可从病毒入口进行防御，如外设管控、病毒查杀、网络防护，“永恒之蓝”漏洞等，在运行时进行白名单管控和病毒实时防护，病毒在生产网扩散时进行网络防护。

无损部署对工控系统零影响

“无感式”生产防护：
对工业主机性能的影响极低，不影响工控软件的正常运行，保证了业务环境的高实时性和高可用性。

集中式的运维管理分析

“集中式”运维管理：
配置策略集中管理和日志、风险集中展示和分析，可以进行单机版、网络版、级联部署。

部署场景 DEPLOYMENT SCENARIO

奇安信网神工业主机安全防护系统分为单机版和网络版，部署位置如图中所示，在工业企业的管理网和生产网中每台工程师站、操作员站、服务器等部署工业主机安全防护系统终端（当无法进行网络互连时安装单机版），在可联网情况下部署工业主机安全防护系统控制中心，通过控制中心对网络里终端进行集中管理和配置。