

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。

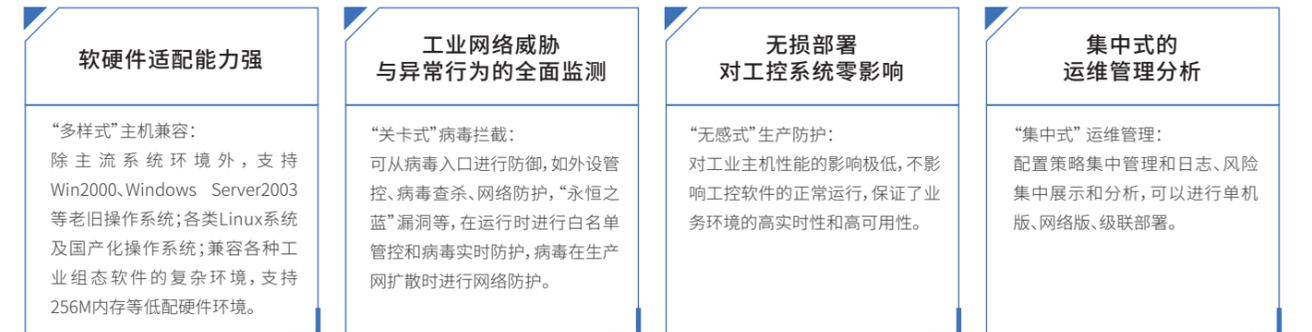


集中配置管理

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，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。



产品优势 PRODUCT ADVANTAGES



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。

