奇安信网神工业防火墙ISG

纵深有边界，生产更安全

奇安信网神工业防火墙专用于工控场景进行边界安全逻辑隔离。产品采用四重白名单的深度防御和一体化引擎机制，既实现了工业安全的深度安全要求，又满足工业安全的低时延要求。硬件层面上，具有全封闭、无风扇、冗余电源等特性，满足工业级可靠性和稳定性要求，有效确保了工业网络内外部的边界安全。

用户价值 CUSTOMER VALUE

提升边界隔离防御能力 保证工业网络稳定性

通过对不同边界采取纵深防御的逻辑隔离防护，并借助四重白名单一体化的精细化管控方式，提升边界防御的整体能力，从而保障工业生产网的网络稳定性。

满足政策合规要求，降低安全责任风险

通过对边界的安全隔离措施，满足等保和行业安全的基本合规要求，并可对日志进行回溯查询，从而降低安全责任风险。

集中式的统一运维提升运维效率

通过对设备的集中运维管理，实现设备策略统一下发和异常监控，有效降低运维人员要求，大大提升日常的运维效率。

产品功能 PRODUCT FUNCTIONS

四重白名单一体化防护，构建工业生产安全环境

针对网络层、应用层、规约指令层、规约数据层进行四重白名单过滤的一体化纵深防护，将各种黑流量、灰流量进行过滤，满足不同场景下不同协议的精细化安全访问控制需求。同时，系统采用一体化的数据处理架构，保证在四重防护的情况下不影响数据流的时延，满足工业实时性的要求。

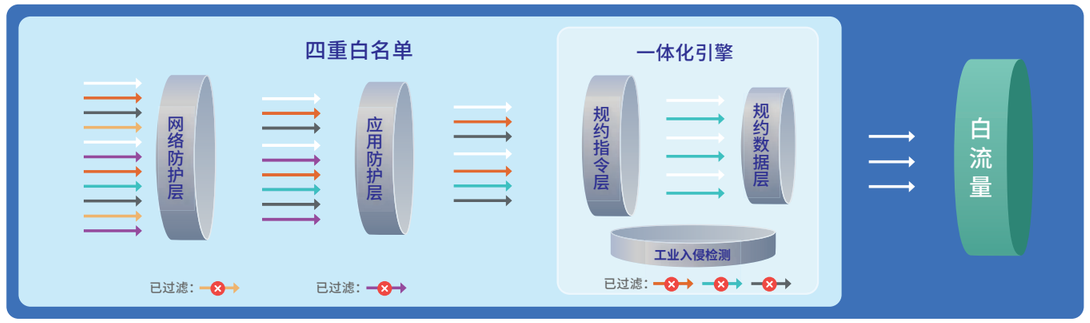
白名单规则自学习，建立完整准确防护基线

采用白名单机制设置安全策略，以适应工控网络通讯特点。设备实时监听网络之间的流量，通过自学习机制生成流量基线，由此建立白名

三段式运行模式，稳妥渐进实现防护目标

系统提供学习、告警和防护三段式运行模式，帮助用户稳妥渐进部署安全策略，以防误阻断正常流量，避免生产事故。学习模式即对工业协议流量进行分析学习建立白名单，不做任何阻断处理；告警模式，就是对学习建立的白名单进行测试验证，对违反策略的流量发出告警，但不阻断；防护模式，经过告警模式的观察磨合，确认安全策略已完全符合管理要求后，最终切换到该模式。

奇安信 新一代网络安全领军者



产品优势 PRODUCT ADVANTAGES

多种硬件形态、适用恶劣工业环境

充分考虑工业环境的特点，广泛支持X86、ARM、国产化各类硬件平台，采用导轨式或机架式安装，满足IP40规范，宽温、无风扇设计。支持电口/光口原生Bypass和冗余电源设计，保障生产连续性。

工控协议深度解析

精准的工控协议指令级控制，深度数据包解析引擎，对工控协议做到实时精准识别和合规性、畸形包检查，支持Modbus、S7、OPC、FINS、BACNet等二十几种主流工控协议。

IT/OT一体化防护

针对工控网络中IT/OT流量进行全方位安全防护，通过应用识别、深度数据包解析以及一体化安全策略进行安全过滤，结合白名单、入侵防御、病毒检测等技术进行安全威胁检测和防护，保障工控网络安全。

部署场景 DEPLOYMENT SCENARIO

奇安信网神工业防火墙可以部署在企业网络层（L4）与生产管理层（L3）之间，作为控制网边界的第一道防线。
奇安信工业防火墙也可以部署在生产管理层（L3）和过程监控层（L2）之间用于保护过程监控层网络及现场控制层网络。也可部署于过程监控层（L2）和现场控制层（L1）之间用于进行生产区域间隔离防护。工业防火墙可由管理平台进行统一安全管理。