

构筑工控网络安全“白环境”

北京威努特技术有限公司



内容提纲

1

工控安全现状及发展趋势

2

威努特工控安全“白环境”解决方案

3

威努特工控安全产品与服务



工控系统网络面临的众多安全问题

- 来自管理信息网的**病毒扩散**。
- 所有自控设备和计量设备均在一个网段，容易形成**网络风暴**，造成全网瘫痪。
- 缺少有效**访问控制**手段，从任何地方接入生产网段即可访问全厂生产设备。
- 服务器/工程师站任意安装软件，恶意程序**非法启动**运行。
- 服务器/工程师站上进行其它无关作业任务，**缺乏管控**。
- 使用U盘造成服务器/工程师站**感染病毒**。
- 服务器/工程师站出现系统**运行缓慢**，内存使用率高，卡死等故障。
- 无实时报警和诊断**工具**。



工业控制系统网络的发展趋势

封闭独立的工控网络



开放互联的工控网络

简单的控制网络



复杂的数据网络

工控技术的复杂多样化



工控技术的通用归一化

内容提纲

1

工控安全现状及发展趋势

2

威努特工控安全“白环境”解决方案

3

威努特工控安全产品与服务



生产控制系统信息安全防护的主要目标



保护工控系统免受病毒等恶意代码的侵袭。

防范外部、内部的网络攻击。

避免工控系统遭受人为恶意或者无意的违规操作。

在不利或遭受网络攻击条件下维护生产系统功能。

安全事件发生后能迅速定位找出问题根源。



通用防病毒软件用于工控系统的不足

很难有效防御新型病毒以及利用0day漏洞的高级病毒

工控系统通常无法及时更新病毒库

测试证明：通用杀毒软件普遍存在对工控软件的误杀



IT防火墙用于工控系统的不足

无法支持对工业控制协议的防护

IT防火墙的时延不一定满足要求

fail-close设计不适合工控系统

IT防火墙硬件设计无法满足要求



构筑工控网络安全“白环境”监控防护体系

运用**白名单**的思想，通过对工控网络流量、工作站软件运行状态等进行监控，运用大数据技术收集并分析流量数据及工作站状态，建立工控系统及网络正常工作的安全模型，进而构筑工业控制系统的网络“**安全白环境**”。

核心理念

1. 只有可信任的 **设备**，才允许接入控制网络；
2. 只有可信任的 **命令**，才能在网络上传输；
3. 只有可信任的 **软件**，才能在主机上执行；

核心技术

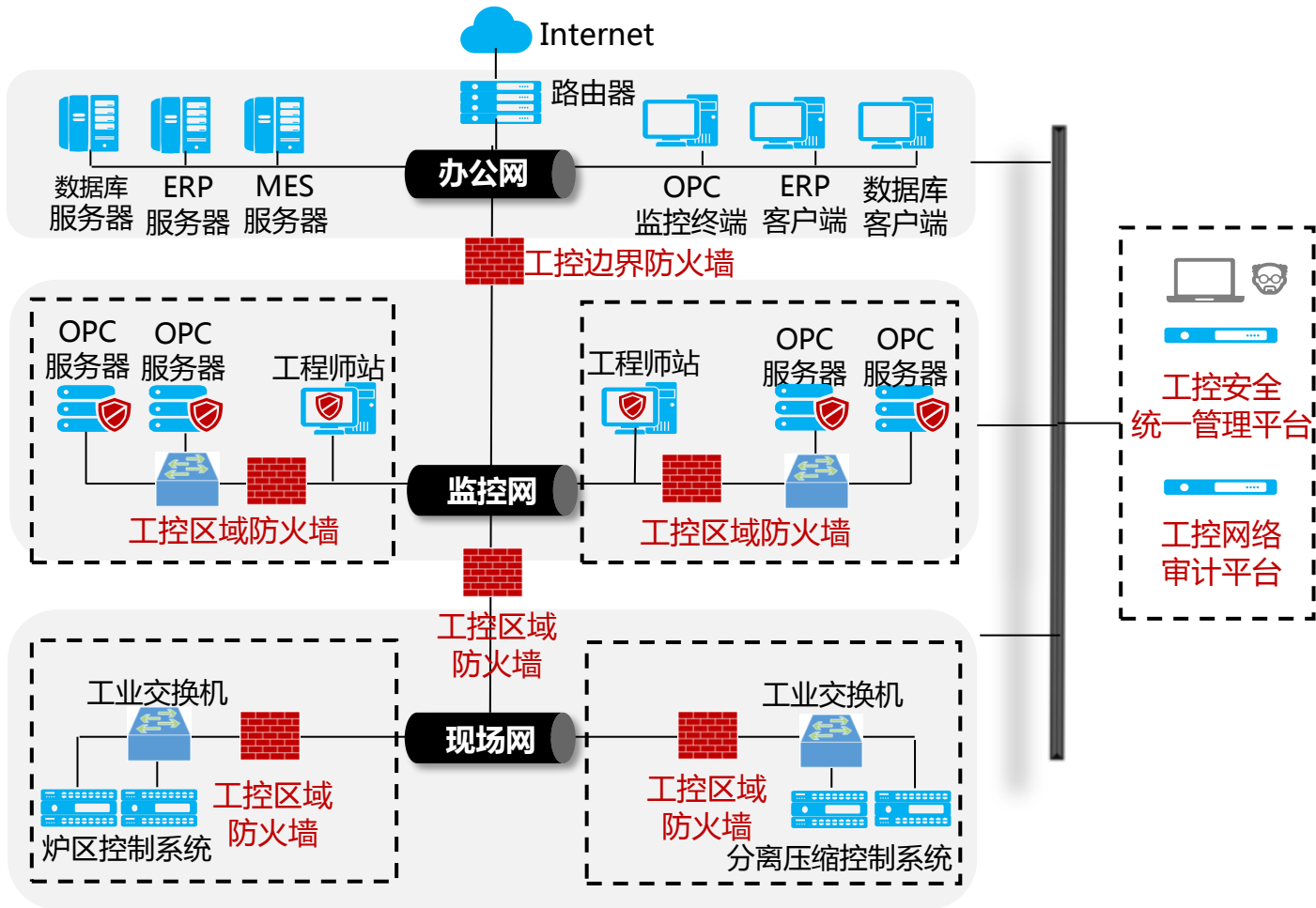
1. 创新的“**软可信**”计算技术，降低方案成本，提高实用性；
2. 机器自学习“白环境”**智能建模**技术，降低维护成本，提高易用性；
3. 高速工控协议**深度包解析技术**，具备高安全性，低时延影响；



工控网络“白环境”解决方案系统架构图

方案特点：

- ◆ 白名单机制
- ◆ 工业协议深度解析
- ◆ 纵深防御
- ◆ 实时监控审计
- ◆ 统一平台管理



内容提纲

1

工控安全现状及发展趋势

2

威努特工控安全“白环境”解决方案

3

威努特工控安全产品与服务

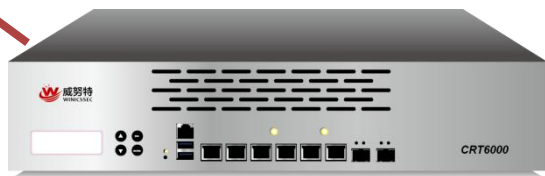


威努特工控安全产品与服务

工业防火墙（可信网关）



主机安全加固软件（可信卫士）



工控安全统一管理平台



工控系统漏洞挖掘系统



工控网络审计系统



工控防火墙(边界型)—TEG5000系列

● 产品定位

- 保护控制网与管理信息网的边界
- 阻止来自管理信息网的威胁

● 产品亮点

- 国内第一款千兆工业防火墙
- OPC深度白名单/OPC只读控制
- 低延迟 < 60us

● 产品功能

- 仅放开OPC动态端口

- 状态检测防火墙

- 数采协议(如OPC)深度白名单

- 静态路由与动态路由(OSPF)

- 数采协议(如OPC)的只读控制

- 违规报警及报告(支持短信)

- 白名单智能学习

- 统一可信组态管理平台





工控防火墙(区域型)—TZG2000系列

● 产品定位

- 保护控制网安全区域间的边界
- 阻止来自安全区域外的安全威胁
- 防止安全域内的攻击扩散

● 产品亮点

- 真千兆，低延迟 < 60us
- Modbus/S7/IEC104等协议深度解析
- 多种工业现场协议快速适配

● 产品功能

- Modbus协议的深度白名单
- 多种工业现场协议快速适配
- 白名单智能学习
- 状态检测防火墙
- 静态路由与动态路由(OSPF)
- 违规报警及报告(支持短信)
- 统一可信组态管理平台



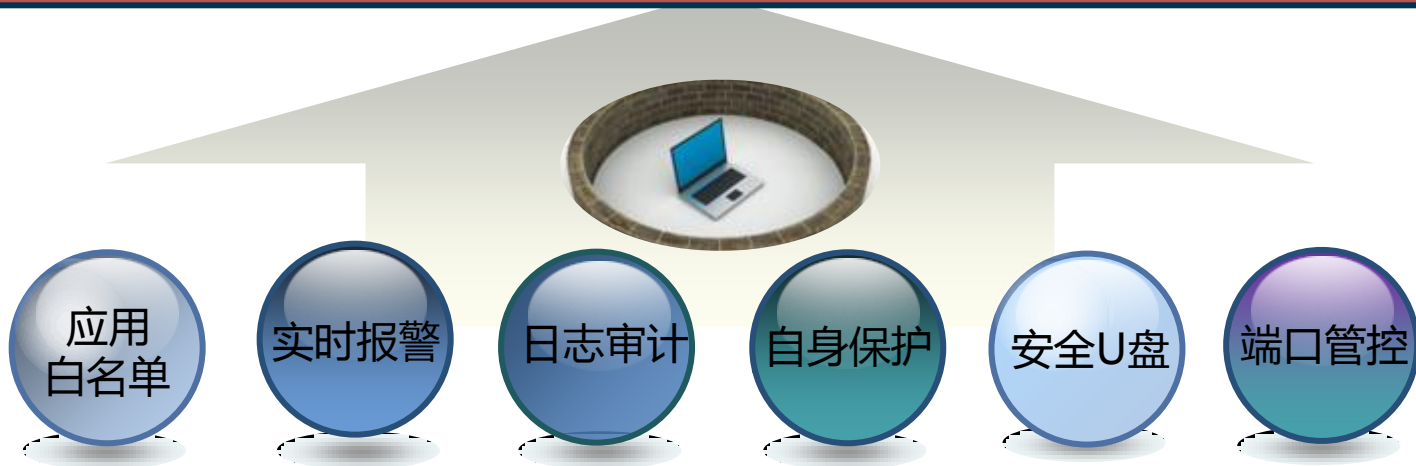


工控主机防病毒软件—可信卫士(TWG)

国内首家利用“白名单”技术保护工控系统主机安全的主机防护软件。保证只有经过认证的“白名单”软件才可以运行，任何其他的病毒、木马和违规软件都被阻止。



产品功能





产品定位

监控并记录工控系统运行过程中的一切操作行为，
为事故追溯、责任划分提供证据



产品功能

网络异常检测：忠实记录工控协议通信记录，自学习建立正常通信行为基线模型，对偏离基线异常操作行为进行告警上报；

网络攻击检测：识别并检测工控协议攻击、TCP/IP攻击、网络风暴、参数阈值检测；

关键事件检测：例对工程师站组态并更、操控指令变、PLC程序下装以及负载变更等关键事件告警

工业网络可视化：提供多维度网络流量视图，统计视图；



工控安全漏洞挖掘平台(CRT)



- ✓ 针对工业控制系统中各类设备进行**通讯健壮性专业评测**
- ✓ 建立我国工控安全**防护标准**的理论支撑和测试工具
- ✓ 完全**国产自主知识产权**，杜绝国外产品安全后门隐患
- ✓ 提供了发现工业控制系统和设备**零日漏洞**的工具
- ✓ 提供了设备漏洞**根源分析和定位**解决的工具
- ✓ 能够有效丰富我国自有**工业控制系统漏洞库**
- ✓ 增强产品出厂时的**健壮性和安全性**
- ✓ 提高评测认证通过能力，提升**生产效率**
- ✓ 减少漏洞修补费用，**降低**产品召回风险



工控信息安全统一管理平台

功能亮点：

- ◆ 监控、管理工控网络中运行的设备；
- ◆ 查看、管理主机配置合规性；
- ◆ 网络中、主机上的漏洞分析检测；
- ◆ 监控网络行为，透析入侵攻击；

工控信息安全统一管理平台

工控防火墙 主机加固 设备审计 漏洞分析

您好！admin 欢迎使用！ | 设置 | 关于 | 退出

网络管理

网络管理 分信管理

白名单管理

防火墙管理

设备管理

安全管理

攻击防范管理

工控系统行业规范

日志管理

短信告警通知

系统设置

网络列表

网关名称: [] 网关IP: [] 在线状态: [请选择] 工作模式: [请选择]

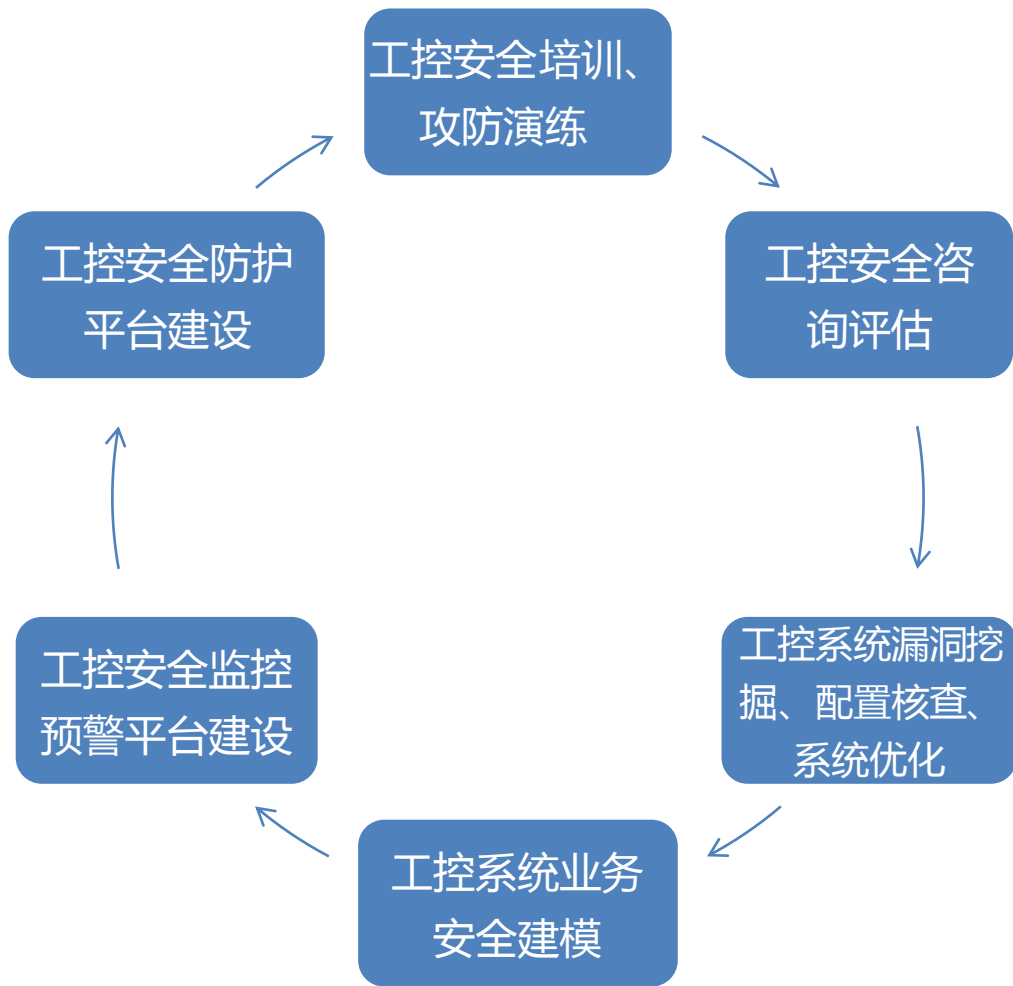
白名单模板名称: [请选择] 搜索

序号	网关名称	设备状态		网关编号	网关IP	在线状态	工作模式	白名单模板名称	白名单模板版本	上线时间	操作
1	新加网关150908020			150908020	192.168.10.191	离线	初始状态			2015-09-12 14:34:47.0	查看 修改 删除 升级
2	新加网关150908006			150908006	192.168.10.192	离线	初始状态			2015-09-12 14:34:47.0	查看 修改 删除 升级
3	新加防火墙150814015			150814015	192.168.10.161	离线	测试模式	OPC全范围白名单模板	1	2015-09-09 15:03:25.0	查看 修改 删除 升级
4	新加防火墙150814013			150814013	192.168.15.167	离线	初始状态			2015-09-09 11:24:39.0	查看 修改 删除 升级
5	新加防火墙150814012			150814012	192.168.15.166	离线	初始状态			2015-09-09 11:24:39.0	查看 修改 删除 升级
6	新加防火墙150814010			150814010	192.168.15.165	离线	初始状态			2015-09-09 11:24:40.0	查看 修改 删除 升级

版权所有 © 北京威特格技术有限公司



全方位全生命周期的工控安全建设方案



为您提供覆盖工控网络全生命周期的业务安全建设方案