360 网神工业主机防护系统

产品白皮书

■ 版权声明

目 录 | Contents

一. 引言

1.1 工控安全概述

随着工业 4.0 及两化融合的趋势到来，传统的工业控制系统网络安全(简称工控安全)问题已成为企业及国家安全面临的严峻挑战，受到越来越多的企业及政府关注。

针对广泛分布于工控网络的工作站、服务器等设备，360 企业安全提供了基于白名单主动防御技术的 360 网神工业终端安全管理系统（简称：360 工业主机防护），为用户构建可控、可靠、可管理的工控网络“白环境”纵深安全防御体系。

工业控制系统由于历史上相对封闭的使用环境，大多只重视系统的功能实现，对安全的关注相对缺乏，工控安全的现状处于“先天不足、后天失养、未来堪忧”的状态。工业控制系统的协议和设计，在研发时即偏重于功能的实时性和可靠实现，对安全攻击缺乏前期设计和有效抵御方法。另外，工业控制系统由于担心系统兼容性问题，通常不升级补丁，甚至有的工作站供应商明确要求用户不得自行升级系统，因此系统长期运行后会积累大量的安全漏洞；再加上运维过程中缺乏科学的安全意识、管理和技术方案，这些缺陷使工控系统面对网络安全攻击时极其脆弱，给安全生产带来极大隐患。

1.2 工作站面临威胁的特点

作为 DCS 系统重要组成部分的工程师站、操作员站，是系统的具体实施、维护、监控单元，直接关系到系统的最终实施，一旦遭受攻击，会直接导致生产停滞、财产损失、甚至人员伤亡的严重后果。所以对其系统安全性的管控是工业控制系统安全非常重要的一环。

但是不同于用于个人办公的普通 PC，工程师站有其独特的特点：

一 、网络封闭，工程师站直接接入企业的工业控制网络，很少能连接到互联网，在规避了大量接入外网风险的同时，也使系统管理员放松了应对网络攻击的警惕；

二、信息资产价值更大，工程师站存储的信息包含大量企业的流程、工艺、运行记录等机密数据，相较办公数据其价值更大，一旦丢失泄露对企业造成的风险、危害也更大；

三、使用的软件和协议有其专业性，工程师站和操作员站其运行的是专业的 DCS、SCADA 系统软件，可以实时监控系统运行的状态并及时调整其运行，下层连接的 PLC、阀门、仪表等设备运行的是 ModBus、OPC、IEC101/104 等工控专业协议，传统杀毒软件、终端管理软件对其深层行为分析无能为力；

四、移动存储介质使用风险大，工程师站由于其封闭性，更普遍使用 U 盘、移动硬盘等移动存储设备传递数据，但是由于系统漏洞多、升级慢，其遭受攻击的可能性更大，如 Stuxnet 震网病毒即通过此种途径传播，一旦病毒入侵，就会在内网迅速复制传播，感染整个控制网络。

所以，工作站遭受的网络安全攻击，有以下几个特点：一、目的性强，遭受的攻击往往是以造成系统损失或窃取价值信息资产为直接目的；二、专业性高，经常有专业的黑客或团队支持攻击工具的开发；三、危害性大，一旦遭受攻击，往往意味着大量的财产、信誉甚至生命安全的损失，如 2010 年 “震网”蠕虫对伊朗的核设施造成了严重的破坏，据 ISIS 研究所估计纳坦兹因此而发生故障的离心机可能多达 1000 台，占总数的 10%；四、公司员工、离职人员、外包人员实施攻击的可能性更大；五、某些操作人员的无意行为，实际会造成类似攻击的效果。

1.3 市场上的解决方案分析

目前，国内针对工作站、服务器的安全防护，普遍采用的安全防护手段就是安装杀毒软件，来阻止机器上的恶意软件运行和传播。但是杀毒软件是一种基于黑名单的查杀方式，“黑名单”是指“坏的”、“不被允许的”，即只有在恶意软件被加入黑名单时才会被阻止运行，黑名单之外的软件和行为被认为都是正常、可信的。但是，杀毒软件的特征库更新是必然晚于恶意软件的发现的，具有天然的滞后性，并不能对付未知的、新的恶意程序的攻击，如 0-Day 攻击，APT 攻击等。并且其对来自操作人员的行为攻击完全无能为力。

针对黑名单安全防护技术在工控网络的弱点，360 企业安全公司创新性的将应用程序白名单管理技术引入工控主机安全防护。“白名单”是指规则中设置的允许使用的名单列表，其意义是“好的”、“被允许的”，“应用程序白名单”是一组应用程序名单列表，只有在此列表中的应用程序是被允许在系统中运行，之外的任何程序都不被允许运行。通过机器智能学习技术，360 网神工业终端安全管理系统还将白名单技术用于工控主机行为的分析判断。通

过大数据采集和分析，智能学习模块自动生成的工业控制软件正常行为模式的白名单，与现网中的实时传输数据进行比较、匹配、判断。如果发现其用户节点的行为不符合白名单中的行为特征，360 工业主机防护系统将会对此行为进行阻断或告警，以此避免工业控制网络受到未知漏洞威胁，同时还可以有效的阻止操作人员异常操作带来的危害。

二. 360 网神工业主机防护系统产品介绍

2.1 产品概述

360 网神工业主机防护系统（简称：360 工业主机防护）产品主要具有以下三个部分功能：一是应用程序和操作性的监控和分析；二是应用程序和操作行为的访问控制；三是应用程序和操作行为特征信誉库的建立。

360 工业主机防护主要有以下三个产品组件：

1、360 工业主机防护是可部署安装运行在工作站上的客户端软件，能监控分析应用程序和人工操作的行为特征，生成白名单，控制恶意程序和操作的执行；

2、360 工业安全管理系统，统一管理企业内部所有 360 工业主机防护客户端，并收集、汇总、更新、同步单独客户端的黑白名单数据库，统一管理企业消息推送，统一管理企业自建可信应用信誉库，并与 360 工业安全网关联动；

3、360 企业安全可信应用信誉库，利用漏洞挖掘技术、智能分析技术建立的全球性应用信誉系统，可有效分析不同操作系统、不同应用厂家、不同工业行业的应用可信性，并针对不同行业、不同应用场景形成配置模板，能方便、有效的适配各种工作场景。

360 工业主机防护定位为工作站、服务器提供全生命周期的安全管理，保障工作站、服务器的可用性、可靠性和可信性：

1) 事前部署

- 人员资产匹配管理：对工程师站进行权责明确的资产管理，确保工作站系统、360 工业主机防护、控制软件只有特定的管理人员才可以操作，支持分权分域设计，对管理员的操作记录记入日志服务器供事后审计。

- 工作站白名单生成：可通过自动扫描、软件安装跟踪、软件升级跟踪、自定义添加等手段生成工作站应用、脚本的白名单。
- 厂商白名单库导入：可自动从 360 工业安全管理系统导入 360 企业安全维护的厂商白名单库，如：和利时软件白名单库、西门子软件白名单库、中控软件白名单库等。
- 行业白名单库匹配：对垂直管理的主要工控行业，如石化、石油、电力、烟草、化工厂、铁路、核能等，可自动从 360 工业安全管理系统导入 360 企业安全行业白名单库，减少现场添加白名单的工作量。
- 主机接口管理： 管理员可以配置管理工作站对外接口如，USB 接口、光驱、串口等，接口上的操作如插入 USB 接口拷入软件，都可配置记录和审计。
- 行为软件配置：配置工作站主要运行的核心软件，如石化 SCADA 自动化监控系统，360 工业主机防护自动监控分析核心软件的数据行为模型，对异常行为数据根据策略配置进行监控、告警或阻止。
- 控制策略配置：根据企业安全管控政策，配置 360 工业主机防护策略，如针对白名单外的程序运行是提示还是阻止，是否允许 USB 设备接入，对核心软件异常行为是进行告警、提示还是阻止等。
- 安全配置模板定制：企业针对运行特定任务的工作站，可以综合运用多种方法配置白名单，最后将白名单和控制策略等保存为模板，相同工作站可以一键式调用，减少配置工作量。
- 企业自建可信应用信誉库：建立企业内部的可信应用信誉库，为企业可信应用提供认证、下载和升级服务，可防止被恶意软件感染的工作软件通过 U 盘拷贝等方式在企业内传播，管理员可以进行应用的推荐、强制安装或卸载等操作。

2) 事中监控

- 白名单运行控制：监控系统运行情况，只允许运行白名单中的程序(正常系统程序、授权的组态软件、办公软件等)、脚本和插件，恶意软件/病毒/未授权安装的软件等都被阻止运行，软件的变动(增加、卸载、白名单的程序试图运行等)都被记录和审计。

- 业务软件行为分析及控制：360 工业主机防护已经配置的核心工作软件的运行监控，调用 360 工业安全管理系统综合智能分析模块生成数据行为模型，对异常行为数据根据策略配置进行告警、提示或阻止。
- 操作系统完整性监控：发现工作站操作系统完整性被破坏时进行告警，防止操作系统被篡改和植入后门。
- 进程内存空间保护：保护运行进程的内存空间的完整性，防止缓冲区溢出等攻击。
- 配置文件完整性保护：监控和报告关键配置文件的更改，需要监控的配置文件可以由管理员定制添加。
- 注册表保护：监控和报告操作系统关键注册表项的更改，需要监控的注册表项可以由管理员定制添加。
- 移动存储设备控制：只有经过认证的特定 USB 设备才可以在特定的主机上运行，根据策略执行是否允许所有或特定移动存储设备操作(如只允许 USB 键鼠设备运行)，可细分为允许读、允许写、允许读写、可配置禁止 USB 存储设备自动执行，防止恶意程序利用漏洞自动运行。
- 自身安全性保护：防止非法卸载、停止本软件的应用程序、服务及驱动，并对执行此类操作的行为进行记录、告警。

3) 事后审计

- 日志、告警记录：丰富、全面的日志记录，可以根据策略记录允许执行的管理员、应用程序名、时间、证书、公司名等；如果不允许执行，记录管理员、应用程序名、时间、失败原因；记录违反安全策略的行为。支持 syslog 接口，可以将日志输出到第三方日志服务器。
- 大数据安全关联分析：360 工业安全管理系统对企业内各安全卫士产生的日志和告警进行综合分析，深度挖掘安全事件，如某款不在白名单中的软件在多台工作站试图安装，某个账号在多台终端试图登录等，生成安全事件告警，并定期输出企业安全度检查报告。和 360 企业安全可信应用信用库进行同步，及时获得业界最新安全态势和最新的可信应用库。

- 安全态势分析报表：定期生成企业安全态势分析报表，对近期企业安全事件、风险和管理进行分析和汇报。

2.2 产品架构

360 工业主机防护系统系统架构如下，采用白名单技术，与 360 工业安全网关产品和 360 工业安全管理系统共同构建了“端管云”一体化的安全解决方案，为工业控制网络防护构建可信任的工作站级终端安全“白环境”。

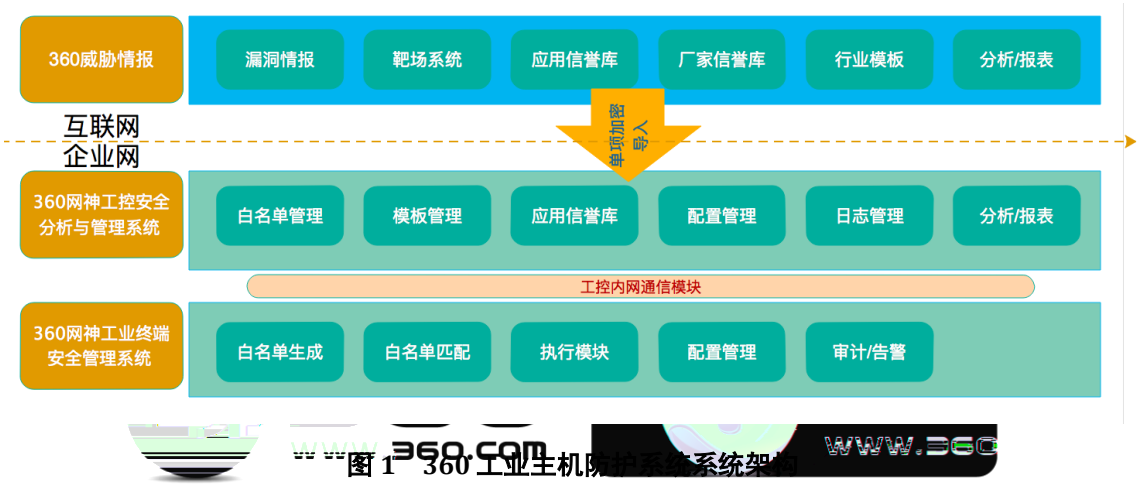

图 1 360 工业主机防护系统系统架构

2.3 主要功能

1. 工作站、服务器等工控主机的病毒、木马及恶意程序攻击防护

360 工业主机防护可以识别、阻止任何白名单外的程序、脚本运行，对通过网络、U 盘等传入系统的病毒、木马、恶意程序具有阻止运行、阻止传播、分析识别的能力。可以关闭无关的主机外设通道，有效防止无线连接、外接手机等情况下的数据外泄。

2. 操作员违规、危险操作防护

通过业务软件行为分析及控制技术，360 工业主机防护可以识别操作人员对业务软件的异常操作，比如异常关闭重要阀门，在非工作时间对系统的操作等，进行提示、告警、阻断等操作，能够有效防范类似离职人员恶意攻击，操作员误操作带来的安全风险。

3. 工控网络安全态势感知

利用大数据分析平台，综合分析整网安全态势，定期生成企业安全态势分析报表，对近期企业安全事件、风险和管理进行分析和汇报，协助完善企业安全生成管理策略。

4. 配置专用工作站

针对用途单一的工作站系统，运行专门的纯净系统模式，开机即运行特定业务软件，之外的任何软件、网络都不允许访问，特别针对和互联网有交互的柜员机、工作站，有效的防止工作站被用于工作无关的事情，或恶意人员利用涉外终端攻击企业内部的事件发生。

2.4 典型部署

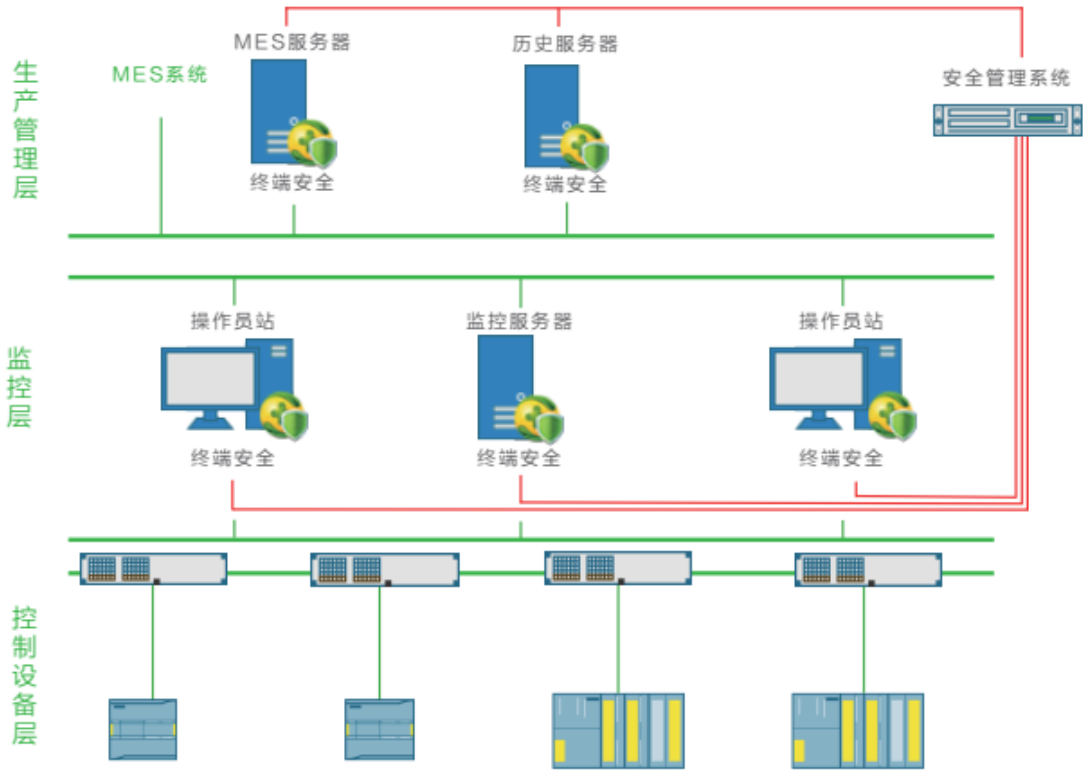

图 2　360 工业主机防护系统部署方案

1. 部署方案及原理

360 工业主机防护部署位置如图中所示，在企业内部每台工程师站、操作员站、服务器部署 360 工业主机防护客户端，和部署在服务器区的 360 工业安全管理系统形成整体解决方案。不但可以联合工作，还支持单台工作站离线运行，形成针对网络孤岛设备的防护。

2. 安装方法

- 可以采用 URL 地址访问 360 工业安全管理系统下载地址，下载 360 工业主机防护客户端；
- 也可以通过光盘方式安装。

3. 软件配置
   - 管理员扫描工作站，生成本地白名单；
   - 管理员可选择下载行业白名单模板、厂家白名单模板，将其和本地白名单进行合并；
   - 配置管理员策略、白名单策略、外设策略；
   - 可选择将白名单、策略保存为自有模板，通过 360 工业安全管理系统下发给制定终端；
   - 自有模板文件可以导出到 U 盘，在工作站中导入；
4. 升级维护
   - 通过 U 盘、光盘等导入离线升级包升级；
   - 通过 360 工业安全管理系统统一升级。

2.5 产品优势

1. 智能机器匹配白名单生成技术
   - 软件安装、升级智能跟踪
   - 软件证书、签名智能匹配
   - 白名单智能冲突检测
2. 高安全外部设备控制
   - 只有经过认证的特定 USB 设备才可以在特定的主机上运行
   - 策略可配置是否允许移动存储设备操作，可细分为允许读、允许写、允许读写等
   - 可配置禁止 USB 存储设备自动执行
3. 进程完整性保护和操作系统完整性保护
   - 进程运行内存空间的完整性保护
   - 防止缓冲区溢出攻击
   - 防止操作系统被篡改和置入后门
4. 未知软件分析沙盒技术

- 针对未知软件进行系统级安全沙盒隔离分析
- 基于人机工程学的行为分析模型
- 工控协议报文应用层深度解析
- 基于 5W1H 的多维度行为关联分析

5. 针对专用工作站的纯净系统技术

- 专用工程站纯净系统，只能运行特定软件
- 开机自启动，不允许切出、关闭
- 系统主机外设通道关闭
- 系统升级，配置更改只能通过 360 工业安全管理系统

2.6 应用场景

360 工业主机防护系统目前运用于各行业主机操作系统中，其优良的用户体验效果和兼容性使得 360 工业主机防护系统在众多工控企业深入使用，管理粒度更是深入到主机硬件驱动层，具有力保护主机安全。

目前运用的行业场景包括：

1. 电力发电、电力输送
2. 石油开采、石油运输、石油炼化
3. 煤矿开采、煤化工
4. 烟草制丝、卷包
5. 钢铁炼化
6. 有色金属
7. 化工厂
8. 市政行业
9. 水利枢纽
10. 制造业生产
11. 轨道交通

三. 客户价值

3.1 自主知识产权，杜绝后门隐患

360 工业主机防护系统（简称：360 工业主机防护）具有完全自主的知识产权，能够帮助涉密单位、关系国计民生的大型工控企业对工控网络工作站、服务器进行安全防护和安全加固，杜绝安全后门隐患，响应国家信息安全国产化政策及号召。

3.2 解决主机安全问题，减少安全生产事故

360 工业主机防护使用先进白名单防护技术，能够有效抵御病毒、木马、恶意软件、零日攻击、高级持久威胁(APT)攻击对工控网络工作站、服务器的攻击与破坏行为，真正帮助企业发现工控网络攻击，解决安全问题，使企业的安全投入物有所值。

3.3 提高工控系统稳定性，减少系统停车时间

360 工业主机防护能够有效检测到操作员针对工作站、服务器的违规、异常操作并加以阻止，进而避免工控系统的意外停车事故。同时，基于白名单技术的解决方案无需对工控网络结构进行改造，避免频繁升级工控系统，减少系统维护停车时间。

四. 总结

360 工业主机防护系统是 360 企业安全集团面向石油、石化、电力、天然气、先进制造、核设施、钢铁、有色金属、化工、水利枢纽、环境保护、铁路、城市轨道交通、民航、供水、供气及供热等工控行业及相关研究机构推出的针对工程师站、操作员站、服务器的终端安全防护产品。其创新性的引入业界领先的白名单技术，构建可控、可靠、可管理的工控网络“白环境”，和 360 工业安全网关组成完善的工控安全防御体系，能够为用户有效抵御针对工业控制系统的病毒、木马、恶意软件的安全攻击。并在业界首次采用针对工作软件的行为分析

技术，有效防护人为因素造成的工控系统安全威胁，为客户带来工控安全防护和管理的真正价值。