360 工业主机安全防护系统

产品白皮书

目 录 | Contents

一. 引言

近年来，随着工业 4.0 及两化深度融合战略的持续推进，以及物联网等新兴技术在工业领域的应用，工业控制系统安全也倍受政府和企业关注。

其中，工业主机是工业控制系统安全的关键环节，工业信息安全建设也需要从主机防护开始。工业主机相对普通的 IT 系统主机和终端，在安全防护方面存在以下特点：

1. 工业主机生命周期长，硬件资源受限

在很多细分工业行业，工业主机在投运后会运行很多年，硬件资源受限，往往不能安装杀毒软件。

2. 工业主机不会随意增加应用软件

工业主机投运后，安装在主机上的软件不会随意升级或增加新的软件、插件。

3. 病毒库不能定期升级

杀毒软件防病毒库需要定期升级或进行在线云查杀。而工控系统不允许在运行期间进行系统升级，也不允许在线云查杀。在工控系统中的防病毒库如果三个月不升级，防病毒效果会大大降低。

4. 普通杀毒软件误杀关键进程

目前非工控专用杀毒软件没做过与工业软件的兼容性测试，在国内外都发生过非工控专用杀毒软件误杀工业软件进程，造成工控系统运行异常的事件。误杀进程在工业控制系统中是致命的。

5. 查毒、杀毒造成工业软件处理延时

杀毒软件一般会使用本地引擎或云端病毒库对工业主机进行病毒查杀，可能会造成工业软件的处理延时。

6. 移动存储介质使用风险

工业主机大多在封闭环境中，普遍使用 U 盘、移动硬盘等移动存储设备传递数据，容易造成病毒通过移动存储介质进行传播。

针对以上工业主机特殊性和安全性，360 企业安全推出的一款工控环境专用的终端安全产品 360 工业主机安全防护系统（简称：360 工业主机防护）。

二. 工业主机安全防护系统产品介绍

2.1 产品概述

360 工业主机防护产品是 360 全新推出的一款工控环境专用的软件产品，通过在工控上位机和服务器上安装基于智能匹配的白名单技术和基于 ID 的 USB 移动存储管控的工业主机防护系统，能够防范恶意程序的运行、非法外设接入、全面集中管理和终端安全风险管理等，实现对工业主机全面的安全防护。

360 工业主机防护产品包含单机版和网络版，单机版针对隔离情况下孤立的工业主机进行安全防护，网络版针对联网情况下工业主机进行安全防护和集中安全风险分析和配置管理。

2.2 设计理念

- **立体防护**

360 工业主机防护以轻量级“白名单”的技术方式，全方位地保护主机的资源使用。根据白名单策略，工业主机安全防护系统会禁止非法进程的运行，并通过基于单个 ID 的 USB 移动存储外设管控，禁止非法 USB 设备的接入以及合法 USB 设备的权限管控，从而切断病毒和木马的传播与破坏路径。

- **统一管控**

360 工业主机防护网络版包括控制中心和终端（客户端）两部分。管理员可以通过控制中心直接对网内所有工业主机上终端进行终端安全策略管理、配置下发等，实现统一管控和安全风险分析。

- **节约成本**

360 工业主机防护针对用户可能存在的工业设备搬迁、工业更替等引起安全防护软件授权无法替换使用的情况，创新提出授权回收机制，可以保证购买点数在设备替换等情况下不会丢失和额外增加投资成本，从而节约用户成本。

2.3 产品架构

- **白名单架构**

360 工业主机防护系统产品中，智能机器匹配白名单生成技术通过全盘自动扫描可以将系统中可执行文件形成唯一的特征码，特征码不依赖文件名称、文件路径或扩展名，而是依赖于可执行文件本身的数据特征，只要可执行文件变化，特征码就变化。

当扫描完成后可以进行一键切换工作模式进行白名单部署，处于告警模式时当异常程序执行可执行文件运行时会进行实时告警但不阻断，当处于防护模式时会进行告警同时进行阻断，异常程序无法运行。

同时部署完成后，当需要进行白名单软件更新时可以进行追加目录或追加文件进行白名单放行，也可设置信任目录或信任文件进行完全信任和放行。

当运行中白名单进行更新后需要进行应用生效使得当前库中白名单进行更新生效。

白名单可以扫描生成也可以进行导入生成，并可以将当前最新的白名单库进行导出和查询等。

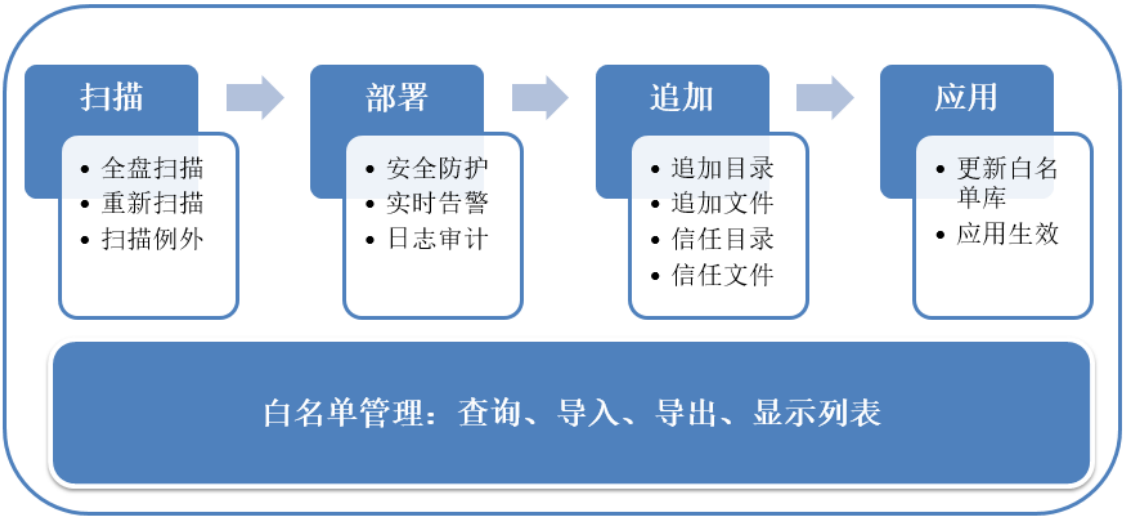

图 1　360 工业主机防护白名单架构

- **集中管理架构**

360 工业主机防护（网络版）集中管理包括安全控制中心和终端客户端两部分。

➢ **控制中心**

安全控制中心是 360 工业主机防护集中管理的核心，部署在服务器端，主要包括安全策略管控和安全日志收集告警等功能。

安全控制中心采用 B/S 架构，管理员可以随时随地的通过浏览器打开访问，对终端进行管理和控制。主要有分组管理、策略制定下发、统一白名单扫描（及定时扫描）、终端软硬件资产管理等。此外安全控制中心还提供了系统运维的基础服务，如：终端升级服务、数据服务、通讯服务等。

安全日志收集告警，通过管控中心，管理员可以了解全网终端的告警信息，通过日志分析，掌

握全网威胁状况。

➢ **终端客户端**

终端端部署在需要被保护的工业主机或服务器上，执行最终的白名单扫描和防护、外设管控、等安全防护操作。并与安全控制中心通信，提供控制中心管理所需的相关安全告警信息。

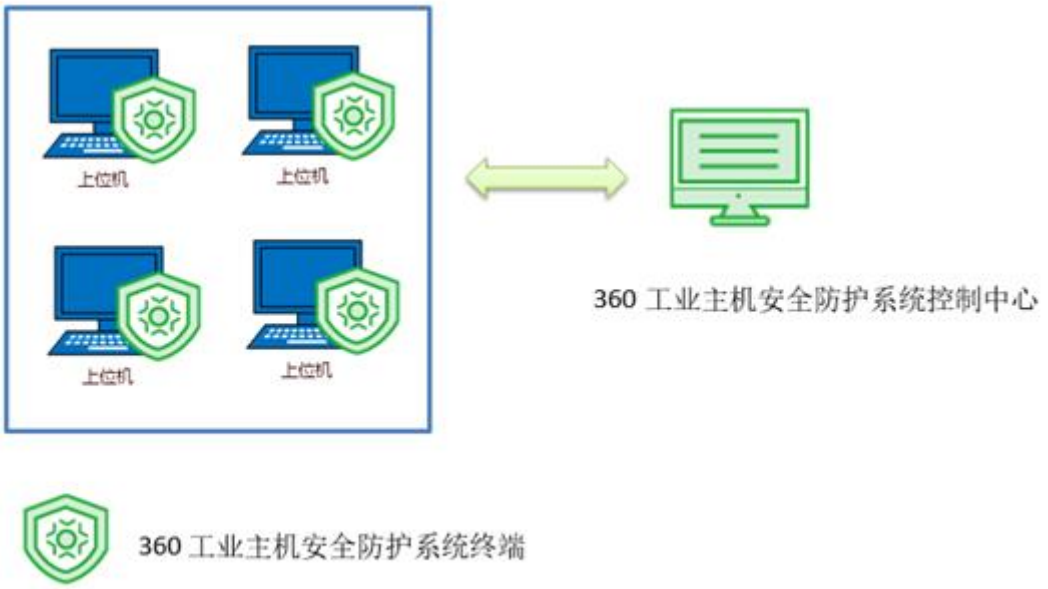

图 2　360 工业主机防护网络版架构

2.4 产品优势

360 工业主机防护系统的核心价值在于对工业主机安全的防护与管理。360 自身经过多年的投入与积累，沉淀下了多项针对终端安全防御的技术，这些技术在整个安全行业领域内都具有独创性与先进性，多项技术已经达到国际一流水平，并领先其他欧美企业的同类产品。同时，360 自身的安全技术能力也得到了国内广大用户的认可，在工业安全领域，360 工业主机防护已为汽车制造、半导体、烟草、轨交、电厂等众多客户提供了安全防护及终端安全管理。

- **智能机器匹配白名单生成技术**

针对工业主机进行一键全盘扫描智能生成白名单规则库，根据规则进行智能匹配，针对工业客户众多工业主机设备及操作系统、工业软件、低硬件资源设备均可进行兼容。

- **多种工作模式一键切换**

针对工业主机特点进行告警、防护、关闭三种工作模式，并可根据现场需求进行一键切换，立

刻生效。

- **基于 ID 的单个 USB 外设管控**

基于 ID 的 USB 移动存储管控，只有经过注册 USB 移动存储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、允许读写等，可配置禁止 USB 移动存储设备自动执行。

- **软件化控制中心**

网络版控制中心软件化安装，针对主机上终端进行集中管理和安全风险分析，基于用户组织架构进行安全风险管理并可以进行终端功能进行单点维护和定制化。

2.5 主要功能

1. 工业主机恶意程序攻击防护

360 工业主机防护可以通过应用程序白名单功能进行恶意程序攻击的防护，360 工业主机防护会对工业主机进行扫描，对每个可执行程序生成一个唯一的特征码，特征码集合起来形成特征库。在防护状态下，防护软件会使用特征库对待启动进程进行认证，只有经过认证的“白名单”软件才可以运行，其他病毒、木马、违规软件都被阻止。

2. USB 移动存储管控

360 工业主机防护可针对主机插入的 USB 移动存储进行权限管控，通过针对 USB 移动存储的硬件 ID 进行识别和匹配，对所允许的外设进行权限管控（读和读写），对不允许的外设进行禁用。从而，避免工业主机通过 USB 移动存储进行病毒传播和非法外设进行文件读取。

3. 控制中心软件化

360 工业主机防护控制中心采用软件化方式可以安装在客户的服务器以及虚拟机上，通过控制中心对工业主机终端进行集中策略配置、安全风险管控、终端版本推送、授权管理、以及终端单点维护和功能定制化。

4. 符合工业特点的终端安全防护

360 工业主机防护控制中心针对工业主机，可以根据工业软件运行需要进行白名单工作模式（防护、告警、关闭）设置，同时兼容低配置硬件、多种操作系统、多种工业软件，并可设置特定时间扫描生成白名单，从而保证工业主机安全又不影响工业企业生产的稳定。

5. 工业资产管理

- **终端发现**

360 工业主机防护具有强大的终端发现功能，管理员可以通过定义网络 IP 段分组，对指定的网络分组进行周期性地发现（采用多协议、多机制方式）与统计网络中的终端数量及类型。管理员通过此功能，了解生产网终端数量和工业主机安全防护系统终端的安装量，为工业企业主机安全管理运维提供有效的参考。

- **单点维护**

360 工业主机防护对单台终端具有全面的安全运维管理功能，包含终端的硬件资产管理、软件资产管理、账号管理、配置管理、终端安全统计等，并可以针对终端白名单进行单独管理以及白名单展现、查询、导入、导出等。

6. 终端安全审计

360 工业主机防护通过技术手段使各种管理条例落地，增强用户的安全和保密意识，保护内部的信息不外泄。所审计的内容只是跟生产网联网的终端安全白名单管理相关的信息，不对涉及终端用户的个人隐私信息，达到合规管理的审计的要求。主要审计终端：白名单违规日志、外设管控日志、终端用户操作日志、系统自身开关机和登陆账号日志。

7. 授权管理与回收

360 工业主机防护可以进行授权点数管理，通过控制中心查看生产网内工业主机的安装及剩余情况。同时，可以进行工业主机安全防护系统的授权点数回收，避免客户在工业主机更替或者迁移时授权点数丢失，需要额外再进行购买的情况，节约用户成本，保护用户资产。

2.6 典型部署

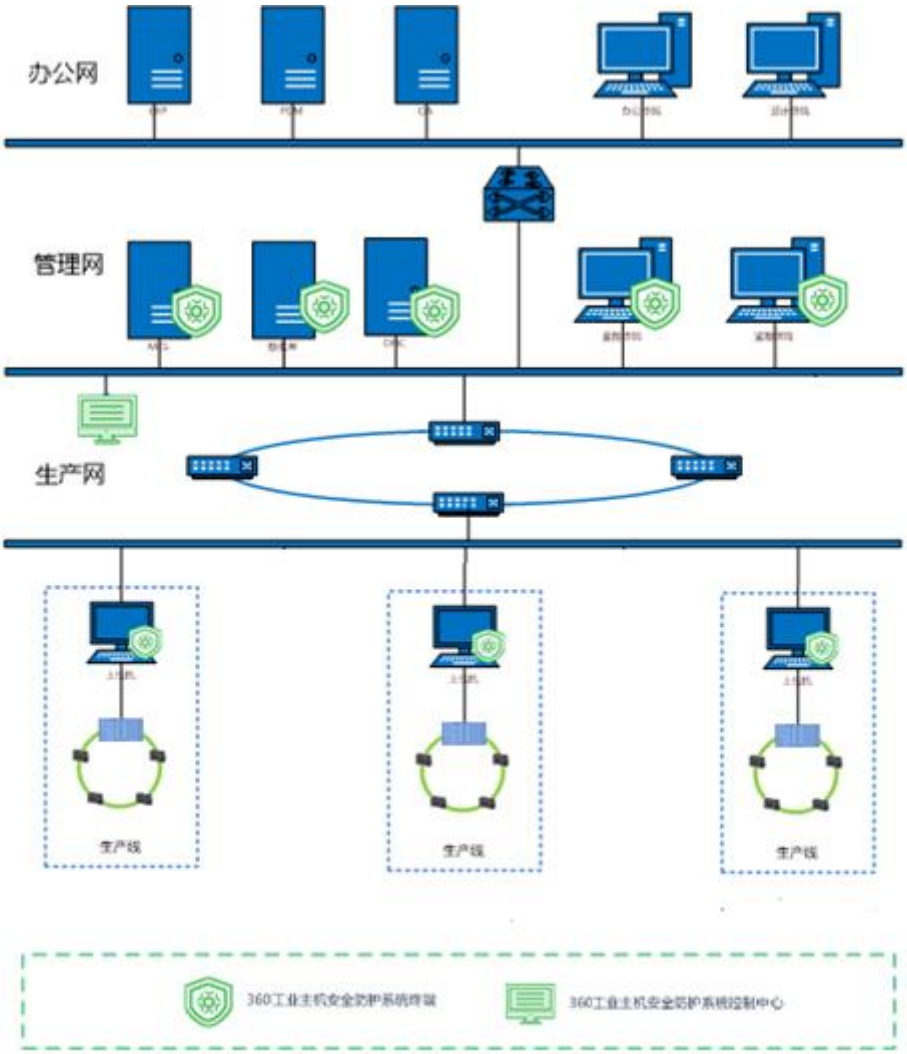

图 2　360 工控主机防护系统部署方案

- **部署方案**

360 工业主机防护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 360 工业主机防护终端（当无法进行网络互连时进行单机版部署进行单点管理和安全防护），在可以网络互连情况下部署 360 工业主机防护控制中心，通过控制中心对网络里终端进行集中管理和配置、单点维护和定制。

- **部署过程**

1.　单机版部署和配置：

- 工业主机进行单机版安装
- 白名单本地全盘扫描和外设管控设置
- 选择追加行业或企业内白名单模板，将其和本地白名单进行合并
- 配置白名单工作模式
- 配置用户策略、告警、日志审计等安全策略

2. 网络版部署和配置：

- 服务器进行控制中心安装
- 工业主机通过控制中心链接进行终端安装
- 白名单本地全盘扫描和外设管控设置（或者在控制中心进行统一配置）
- 选择追加行业或企业内白名单模板，将其和本地白名单进行合并
- 配置白名单工作模式
- 配置用户策略、告警、日志审计等安全策略
- 控制中心查看单机版安全风险和防护情况

三. 客户价值

3.1 工业主机安全防护，减少安全隐患

360 工业主机防护系采用的白名单防护技术结合外设管控，并基于工业环境下主机特点进行适配和兼容，能够有效抵御病毒、木马、恶意软件、零日攻击等对工控网络工作站、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，保障主机安全运行，提升工控系统稳定性，减少系统停车时间，保证生产稳定持续进行。

3.2 工业资产风险分析，提高运维效率

360 工业主机防护能够基于工业资产进行全面梳理和安全防护，对生产网中主机进行安全风险分析和配置策略下发和集中管理，提升工业生产网安全运维便捷性，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。

3.3 自主知识产权，杜绝后门隐患

360 工业主机防护具有完全自主的知识产权，能够帮助政府部门、涉密单位、以及关系国计民生的大型企业对网络进行安全管控和安全加固，杜绝安全后门隐患，响应国家信息安全国产化政策及号召。

四. 总结

360 工业主机防护是 360 企业安全集团面向先进制造、烟草、轨交、电力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、服务器的工控环境专用的终端安全防护产品。同时，360 工业主机防护和 360 工业安全网关等产品组成完善的工控安全防御体系，能够为用户进行全面的工业控制系统的病毒、木马、恶意软件的安全防护。