MCK工控产线主机加固解决方案

数据安全解决方案专家

CNSINDA

CONTENT

PART 01
公 司 介 绍

关于我们

苏州深信达成立于2008年，是国家高新技术企业和国家软件企业，是国家信创（安可）联盟成员，是国内领先的数据安全解决方案供应商。公司主要产品覆盖从业务服务器安全、到员工终端安全，再到产线工控主机安全，再到出厂产品数据安全，围绕科技型企业安全需求，提供纵深数据安全服务。

深信达的客户

深信达成立10多年来，一直深耕信息安全领域，已成功为众多知名客户提供数据安全服务，涵盖通信、无人机、机器人、医疗仪器、汽车、研究院所等众多领域。

公司介绍 / 1-3


苏州市信息技术应用创新联合会
政务工作组成员单位
单位名称：苏州深信达网络科技有限公司
证书编号：No.SZXCZWZ027


信息安全管理体系认证证书
苏州深信达网络科技有限公司
ISO/IEC 27001:2022


涉密信息系统
产品检测证书


图谱收录通知
苏州深信达网络科技有限公司：


麒麟软件NeoCertify认证


麒麟软件有限公司
杰出伙伴


软件产品证书
深信达沙盒防泄密系统软件 V5.0
（T/SIA003-2019），评估为软件产品，特发此证。
申请企业：苏州深信达网络科技有限公司
软件类别：应用软件-安全与保密软件
证书编号：苏 RC-2024-E0469


信息技术应用创新工作委员会
技术活动单位
苏州深信达网络科技有限公司
有效期限：2024年8月 至 2025年7月
中国电子工业标准化技术协会
信息技术应用创新工作委员会
二〇二四年八月


统信软件产品互认证明


高新技术企业
证书
企业名称：苏州深信达网络科技有限公司
证书编号：GR202332006787
发证时间：2023 年 11 月 6 日
有 效 期：三 年
批准机关：

PART 02
需 求 背 景

产线工控安全事件不断

2019年3月份

全球最大铝制品生产商之一的Norsk Hydro遭遇勒索软件攻击，公司被迫关闭多条自动化生产线，震荡全球铝制品交易市场。

2018年8月3日

台积电被曝出在台湾地区的三大厂区遭病毒入侵，直到8月6日台积电官方才发表声明称已经恢复生产。

2019年6月

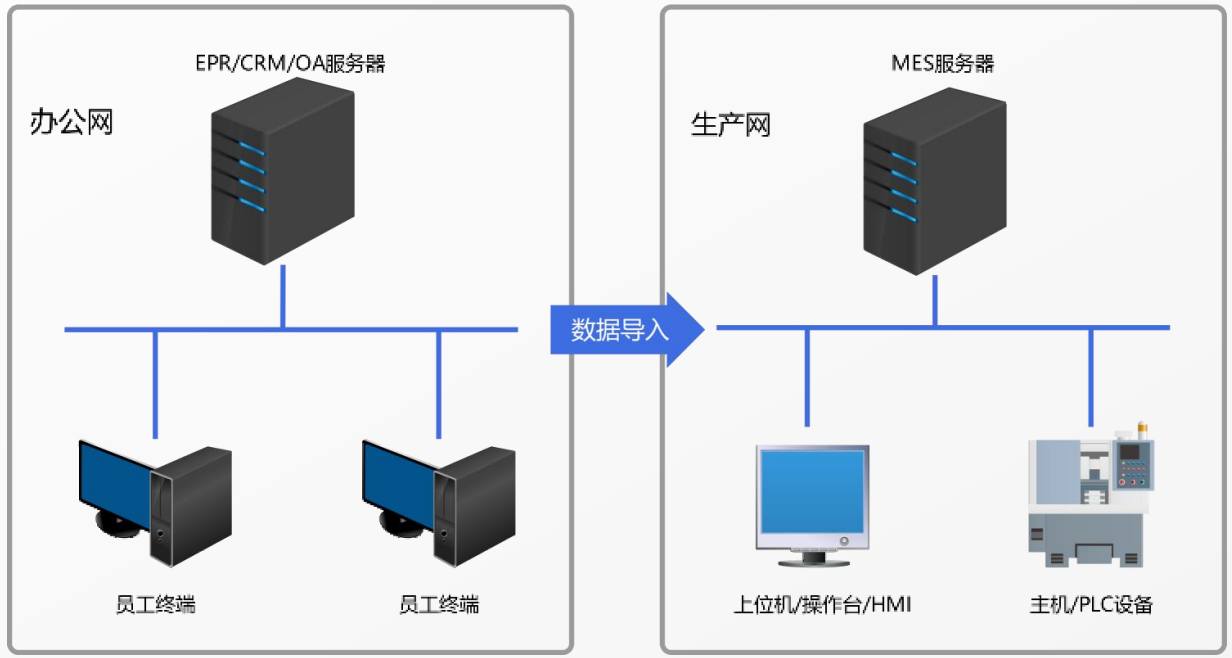
全球最大飞机零件供应商ASCO遭遇勒索病毒攻击，生产环境系统瘫痪，大约1000名工人停工，四国工厂被迫停产。

至今

勒索病毒依旧十分活跃。从勒索病毒攻击的地区分布看，广东、浙江、山东、河南、上海等经济较发达地区成为重点目标。从勒索病毒影响的行业看，数据价值较高的传统制造业、教育、医疗、政府机构非常容易成为攻击目标。

原因分析

随着工业4.0的发展，产线日益智能化，生产网已经发展成一个组网的计算机环境，虽然都进行了隔离，但仍需和外部进行数据交互，导致有病毒入侵可能。



生产网的特点

工作场景比较固定，变化少

不连外网

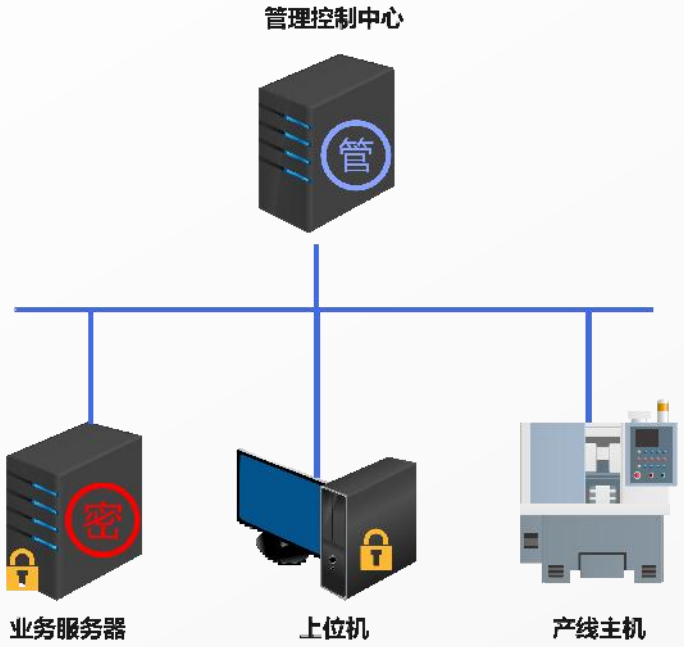
绝大多数杀毒软件不更新病毒库

工控主机操作系统不打补丁

PART 03
解 决 方 案

方案介绍

深信达MCK主机加固方案，针对产线工控主机的特点，是对服务器（MES）主机和产线电脑以及网络进行**加固**，构建可信白名单环境，以不变应万变，进行有效防病毒处理。



方案由主机加固白环境和网络可信白环境两部分组成：

主机加固白环境：

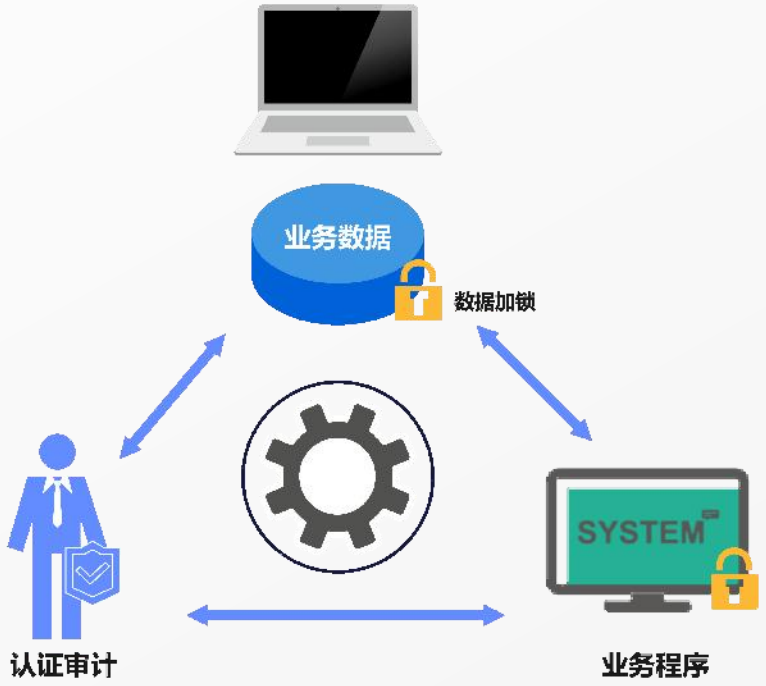
在服务器和产线电脑上安装**加固软件**，建立白名单可信工作环境，并进行资产管理。

网络可信白环境：

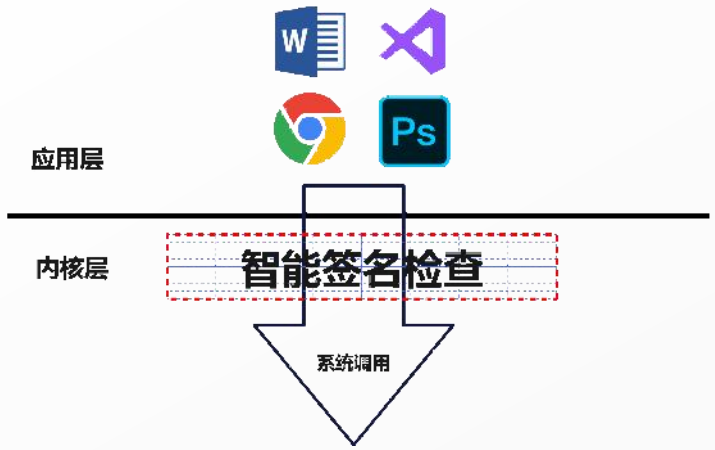
对无法安装防护软件的网络设备，通过**网络控制**进行间接防护，包括各种PLC设备、老旧的设备(如win32/95设备)

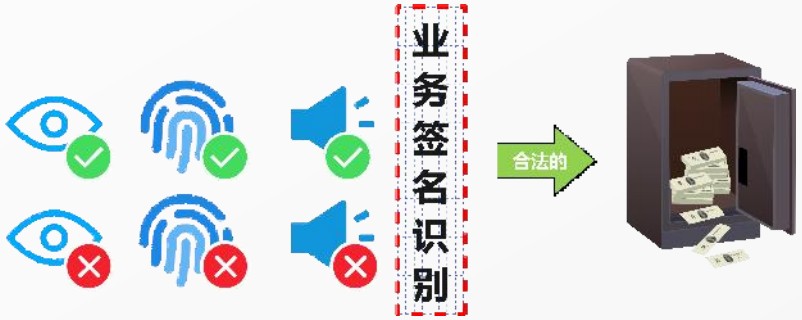
主机加固白环境

设计理念： 深信达MCK主机加固系统是基于**可信计算技术**，锁定工作场景、实行严格场景白名单控制，受**保护的主机只能做白名单规定的事情**，任何白名单之外的、陌生程序都无法运行。以不变应万变，彻底杜绝病毒骚扰，保护业务服务器主机和产线工控设备主机的安全。



核心功能





深信达MCK是针对业务服务器和工控产线主机的场景进行锁定，利用可信计算技术实现程序签名和文件保护。

程序可信

只有系统认证过的程序和业务场景才能运行。

文件保护

指定格式或制定目录下文件加密保护，如保护数据库文件不被篡改

多个加固后的主机构成可信环境

在可信环境内，任何应用执行都需要安全验证才能执行，业务场景锁定，白名单场景运行。

可信应用列表内的程序可以安全安装、运行，不受限制。

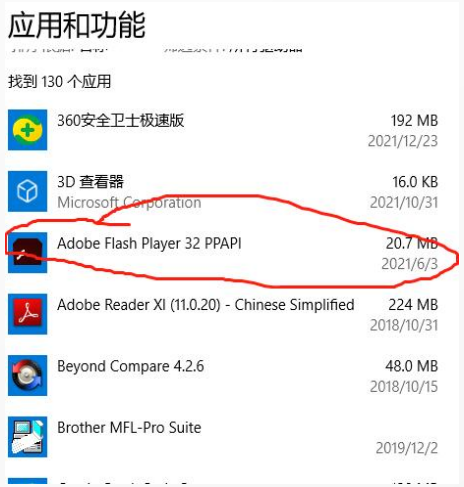
部署了MCK加固系统的主机，会把本地的软硬件信息上传至平台，进行资产管理。

-当软硬件设备发生变动，告警提示

-可以查询某硬件或软件在哪些主机上，并生成报表

硬件变动告警

软件变动告警

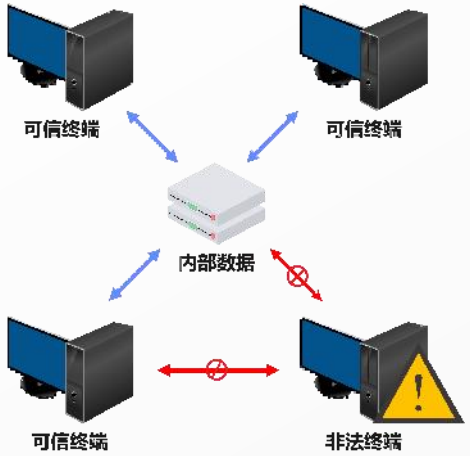


随时查询

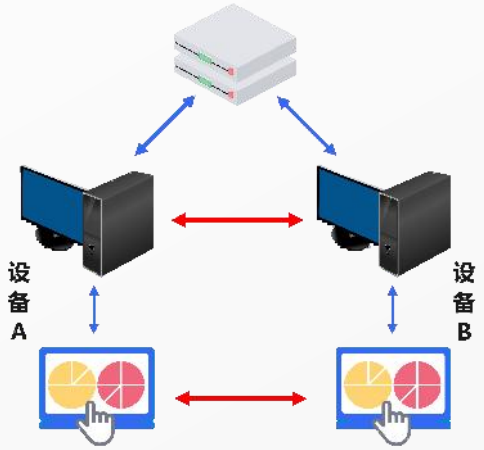
查询什么软件在哪些电脑上安装，如AutoCAD。

可信网络

通过网络白名单（准入、通信控制和流量控制），防止外部非法设备接入，防止病毒通过网络感染PLC设备和老旧的设备。



设备准入



定向通信

协议识别

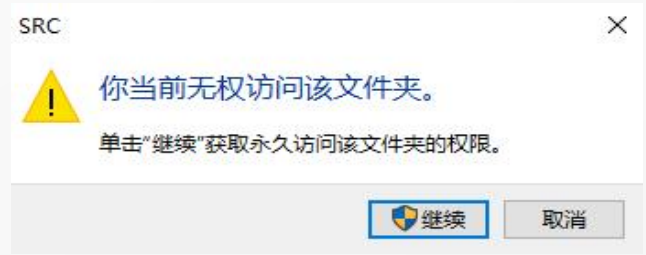
集中监控

通过Web管理控制台进行可视化管理。

方案特点

操作系统底层可信计算技术，以不变应万变白名单机制

只要上锁时无病毒，上锁后就可以高枕无忧



成本低、易实施、性价比高

不需要改变网络架构，不需要增添额外设备，成本低效果好

不但防病毒、而且数据防偷窥

主机上重要数据，可进行定向保护，不被使用者偷窥

软硬件要求

硬件要求：

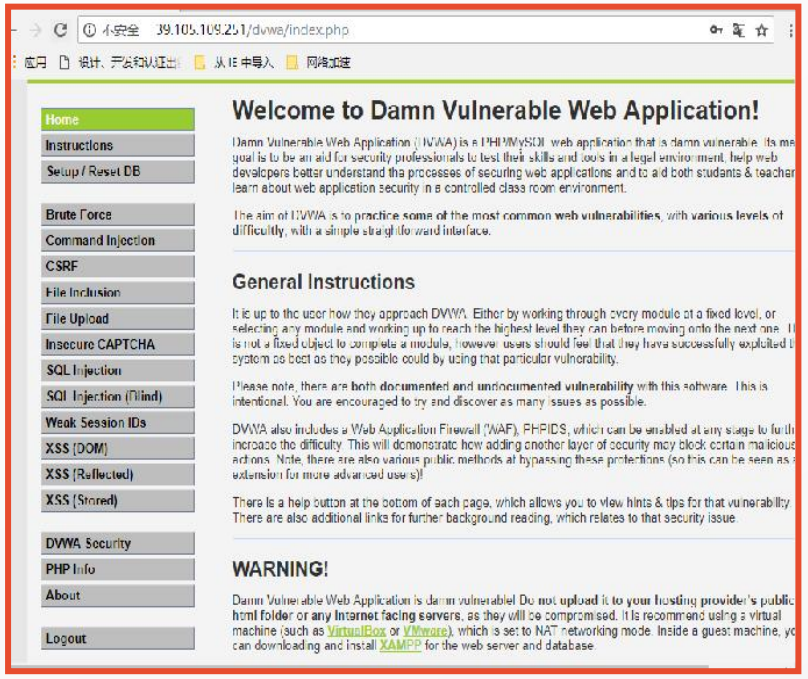
-CPU：1GHZ以上
-内存：512M以上
-硬盘：500M以上空间

OS要求：

-WindowsXP/7/Vista/8/8.1/10/2003/2008/2012
-Debian、Ubuntu、SUSE、Redhat Enterprise Linux、Fedora、Centos、Oracle Linux 内核2.6.32以后版本

产品能力

在国内最大的黑客平台--漏洞银行平台发布悬赏，结果是无人能破解！！



竞品比较

功能视角	MCK方案	其他方案
技术路线	操作系统级可信技术	进程级白名单技术
进程白名单	有	有
模块加载白名单(dll等模块)	有	无、无法对进程内部执行模块白名单加载
脚本白名单（bat等执行脚本）	有	无，无法控制解析类脚本
场景白名单	有、可锁定工作场景	没有工作场景锁定
集中管理	可以	可以
资产管理	可以	可以
数据防泄露	可以针对关键数据防拷贝、配合SDC可实现研发环境到产线无缝防泄露	无
可信运维	无需关闭保护，可通过预签名方式进行程序运维，如更新、调试	需要关闭保护才能运维更新、容易裸露

竞品比较（续）

功能视角	MCK方案	其他方案
漏洞防御	有	有
病毒扫描	无	有
外设管控	有	有
白名单U盘	有、指定的U盘(硬件序列号)可以在指定的主机上使用	有
是否适用服务器部署	有服务器用客户端，防护点更多，包含数据库保护	无
主机加固	有	有
网络保护	有	有
日志上报	有	有
资产管理	有，对所有终端的硬件监控，如有发生变动（更换、偷窃），及时通知管理员	无

PART 04

应 用 案 例

成功案例介绍

某无人机公司

实施方案： 研发环境部署SDC沙盒防泄露系统，在业务服务器及产线上位机部署MCK主机加固系统进行安全加固。

实施效果： 数据防泄露+防病毒一体化，免受勒索病毒 攻击威胁和数据泄露风险。

项目需求： 研发数据防泄露，服务器防病毒、产线工控主机防病毒和数据防泄露。

部署规模： 9000终端（含员工终端+产线PC）+300服务器

成功案例介绍

某国网电厂

项目需求： 2020年1月，该单位业务服务器出现“关键目录中文件/权限变更”告警信息， 要求对业务服务器及产线上位机进行进行安全加固工作，防止并网电厂网络危险蔓延，确保电力系统安全可靠运行。

实施方案： 在业务服务器及产线上位机部署MCK主机加固进行安全加固。

实施效果： 系统经测试安全稳定运行，免受勒索病毒攻击威胁。

直接解决的主要安全问题

序号	实施前	实施后	备注
1	担心员工U盘考数据容易带入病毒，必须对U盘使用严格限制	无需担心U盘带入病毒	可信系统
2	文件共享拷贝文件带入病毒风险	无需担心文件共享拷贝数据	可信系统
3	担心业务数据库文件被拷贝走或被勒索病毒加密	数据库文件禁止访问，无法拷贝和篡改	目录保护
4	设备中毒后，还原系统立刻又中毒了，网络内病毒清除不干净	还原后立刻上锁，不会再感染病毒	可信系统
5	供应商更新业务程序时带入病毒	更新前需要先签名再更新，病毒无法运行	可信系统
6	盗版软件屡禁不止	盗版软件无法运行，只有可信列表中的程序才能在环境内运行	可信环境

感谢您的观看

CNSINDA

深信达