AVCOMM™恩创®

工控主机卫士
Datasheet

恩创致力于将先进的信息技术带入工业控制与工业信息领域。

安通恩创信息技术（北京）有限公司 www.avcomm.cn

电子邮箱: sales@n-tron.com.cn

电话： （010）- 82859971

地址：北京市海淀区马甸东路19号金澳国际公寓3105

恩创工控主机卫士

恩创工控主机卫士+安全U盘产品

产品概述

恩创工控主机卫士是国内首款针对操作员站、工程师站、数据服务器等工业现场主机进行可执行程序管理，防止病毒木马等恶意程序感染的安全软件产品，采用不同于传统防病毒软件的轻量级“白名单”机制，系统资源占用小，不影响工控系统监控软件和组态软件的正常使用，可有效阻止包括STUXNET、Flame、Havex、WannaCry、BlackEnergy等工控恶意程序或代码在工控主机上的执行、扩散。

主机卫士产品可以通过截取系统调用实现对文件、目录、进程、注册表和服务的强制访问控制，结合文件和服务的完整性检测、防缓冲区溢出等功能，将普通操作系统透明提升为安全操作系统；产品具有用户身份鉴别，访问权限控制、外设控制、完整性校验、日志审计等功能，采用集中式管理，满足国家信息安全等级保护和分级保护标准中关于安全计算环境的相关技术要求。

主机卫士产品分为单机版和集中管理版，集中管理版可通过恩创统一安全管理平台对分布安装的工控主机卫士进行策略下发、配置、日志收集等管理操作。

安全U盘是基于安全芯片的移动存储设备，产品充分利用移动存储白名单系统的高安全、高性能、高功效等特性，可实现工控主机对移动存储设备从加载到卸载的全生命周期的安全保证。

产品特点

“四重锁定，两个中心”构建工业主机安全计算环境

- 应用锁定

采用“白名单”防护机制，锁定工业主机上应用程序的运行，阻止任何白名单外的程序运行，避免恶意代码、非法程序的运行，最大限度保障工程师站、操作员站以及服务器等重要设备安全稳定运行。

- 系统锁定

通过安全基线管理和强制访问控制功能，锁定工业主机运行环境和资源，确保工业主机上的设置符合安全基线策略要求，并按照设定的主客体制定读写访问控制策略进行访问。

- 网络锁定

锁定工业主机的网络访问环境，只允许工业主机和特定的服务器之间进行通信，控制恶意代码的在网络内部的传播、扩散。

- 外设锁定

锁定外接输入设备的使用，只有经过认证的安全可信的USB设备才可以在工业主机上运行，防止通过U盘等外接输入设备引入恶意程序导致感染病毒和泄露敏感数据。

- 管理中心和日志中心

通过管理中心实现对网络中部署客户端的状态监测、集中管理，统一策略配置，通过安全日志中心可以实现对安全事件和实时告警的统一收集和分析，动态评估工业主机的安全状态和风险级别

兼容性强，适用各种业务场景

- 支持Windows、Linux平台，应用程序白名单、主机加固功能二合一的工业主机安全产品
- 已适配50个Linux&Unix发行版本，32个windows build版本，针对操作系统Build版本号，内核版本进行兼容性适配并已在多个行业数万台终端上现网应用。

功能规格

文件白名单 • 支持自动扫描Windows和Linux系统生成文件级白名单；	**安全基线** • 支持对账户及账户密码的长度、复杂度、使用期限进行基线设置；

- 支持应用程序安装扫描，安装程序释放的可执行文件一键添加白名单；
- 根据白名单列表对可执行文件的执行进行监控；
- 支持白名单的编辑、删除、追加、查询、导入和导出等操作；
- 支持配置例外路径，指定不被扫描的例外目录；
- 支持配置信任路径和信任进程；
- 支持观察模式和防护模式，在观察模式下只记录告警不阻拦；

网络白名单

- 支持针对主机的SYN攻击防护；
- 支持配置控制程序连接以及TCP或UDP端口连接的规则；

外设管理

- 支持配置安全U盘、普通U盘属性：禁用、只读、可读写，默认可读写；
- 支持配置光驱的属性：启用、禁用，默认为启用状态；
- 支持配置无线网卡的属性：启用、禁用，默认为启用状态；
- 对移动存储设备非法操作实时告警；

访问控制

- 支持基于BLP和BIBA模型的强制访问控制；
- 支持配置文件和注册表完整性保护；
- 支持进程内存空间保护；

安全检测

- 支持检测主机系统安全状态并形成检测报告；
- 支持对系统登录事件、账户登录事件、对象访问等进行基线设置；
- 支持对交互式登录、网络访问、自动播放、默认共享、关机时清空内存页面等进行基线设置；
- 支持对操作系统日志保留大小和时间进行基线设置；
- 支持对操作系统的数据执行保护进行设置；

双因子认证

- 支持USB-KEY+口令的方式进行用户身份鉴别；
- 支持重置和修改设备PIN码；
- 支持生成紧急密钥，用于其它客户端紧急登录；

安全U盘

- 支持私有ID识别技术，安全U盘只能在安装工控主机卫士主机上使用；
- 支持专用安全U盘驱动，支持安全U盘动态加载
- 内置安全芯片，支持U盘认证和数据加密

非法外联

- 支持对自定义的ip或者域名访问检测，对非法网络访问提供日志记录和告警信息；

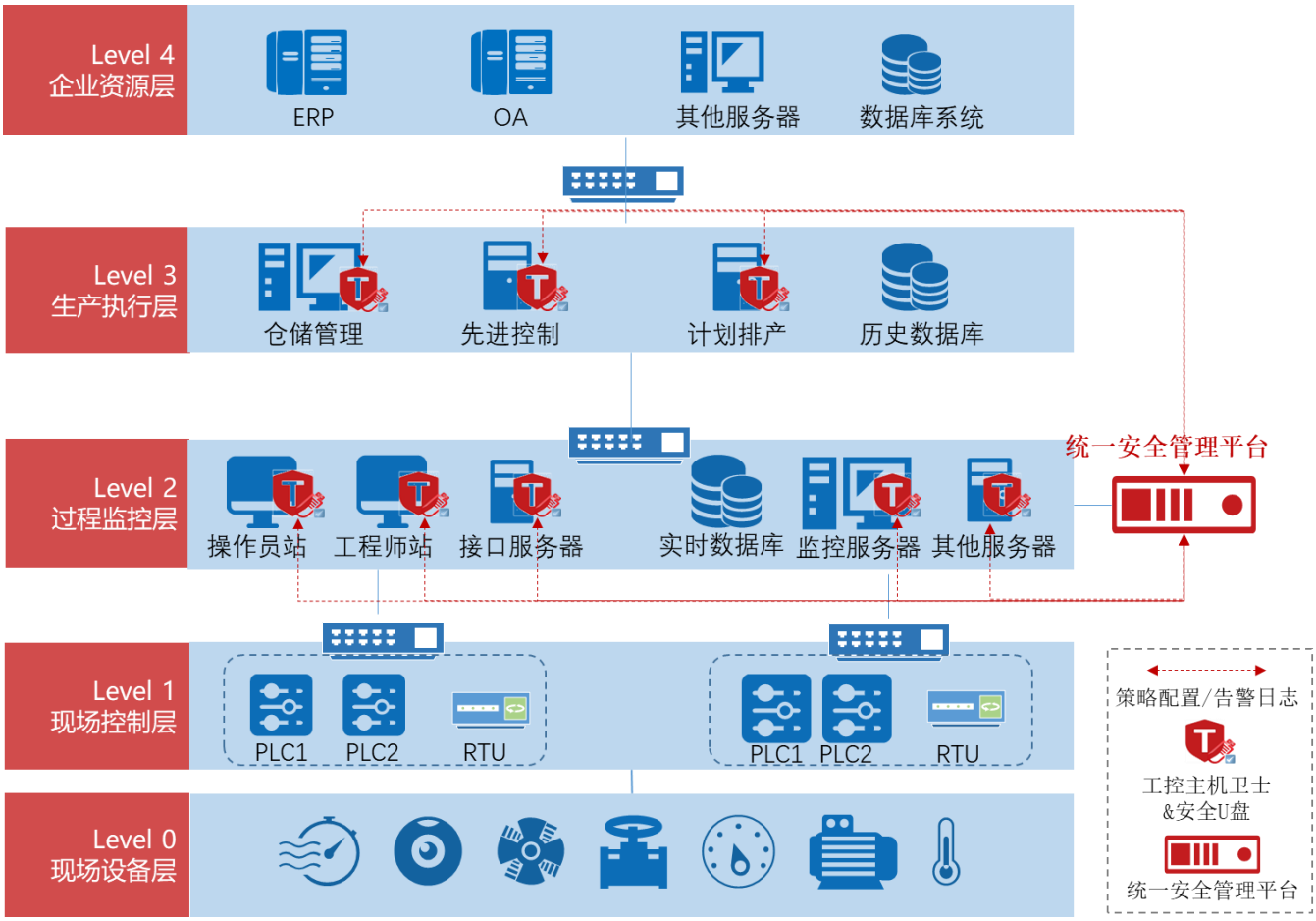
告警审计

- 支持应用程序、操作系统、用户操作、外设操作产生的日志查询、审计和分析；
- 支持白名单外程序运行、外设异常操作、违反网络白名单规则、非法外联等进行实时告警；
- 支持日志备份，支持保存1000万条日志或3个月的日志数据；
- 支持统一管理平台进行告警事件集中管理，对日志进行大数据分析处理

系统兼容性

Windows	Linux
• 支持Windows2000、Win XP SP2、Win XP SP3、win Vista、Win7、Win8、Win10 • 支持Windows2003 Server、Windows2008 Server、Windows2012 Server、Windows2016 Server	• 支持Redhat5.x，Redhat 6.x，Redhat 7.x，CentOS 5.x，CentOS 6.x，CentOS 7.x • 支持Kylin v3，Kylin 3.2 • 支持凝思6.0.42，凝思6.0.60，凝思6.0.80

应用场景



生产执行层主机安全加固

- 安装部署到生产执行层主机及服务器设备
- 检查操作系统开机时加载的系统文件的完整性，防止操作系统被篡改或植入后门
- 对进程的内存空间进行保护，对系统配置文件和注册表完整性进行保护
- 对主机及服务器的账户策略、审核策略、安全选项、IP安全、进程审计、系统日志等安全基线进行配置
- 对主机及服务器设备安全状态进行检测，包括安全基线、分区状态、共享目录列表、服务列表、已安装程序列表、进程列表、用户列表等

过程监控层恶意代码防护

- 安装部署到过程监控层操作员站及工程师站
- 提供USBKEY+口令的认证方式，有效提升系统安全性
- 对主机及服务器设备外设端口进行管控，包括USB接口、光驱、无线网卡等
- 自动扫描建立工控主机白名单数据库，识别、阻止白名单以外的程序运行，对通过网络、U盘等传入系统的病毒、木马、恶意程序的运行行为进行拦截
- 对自定义的IP或者域名进行网络检查，及时发现设备的违规外联行为，并提供详细的日志记录和告警信息