集控审计可视化管理平台

产品介绍

一、产品需求分析

随着互联网技术和信息产业的飞速发展，各政府机关以及企事业单位先后建设并完善了数字化、网络化、智能化、信息化等业务系统，各地党政机关及事业单位的内部网络建设以及电子政务也已进入实质性的应用阶段，办公电脑以及政务服务器等作为网络中的基础设施节点，其安全性以及保密性是非常重要的。许多政府机关以及企事业单位对于外来电子文档及资料的管理，大部分都是通过携带移动存储介质（U 盘、移动硬盘等）储存数据资料，进入内部网络后一般都是直接插入 USB 端口接入 PC 主机或服务器，由于 USB 移动存储介质往往在多台电脑使用过，因此 USB 移动存储器介质难免会携带病毒。病毒一旦侵入单位内部电脑主机就会迅速在网络内部传播，造成各种风险，严重时会影响正常的工作秩序，因此对于 USB 移动存储介质的有序管控，实时对 USB 存储介质上的带毒文件的隔离并查杀病毒，以及文件的上传下载记录审计，对于政府机关以及企事业单位来说，是尤其重要的。不遵守移动硬盘、U 盘等外设的使用管理规范，贪图使用便利而违反信息安全规章，或是随意将未授权的计算机接入信息内外网和内部人员内外网混用，很容易导致局域网病毒传播甚至内网机密信息的泄漏，给政府党政机关造成了重大的损失。

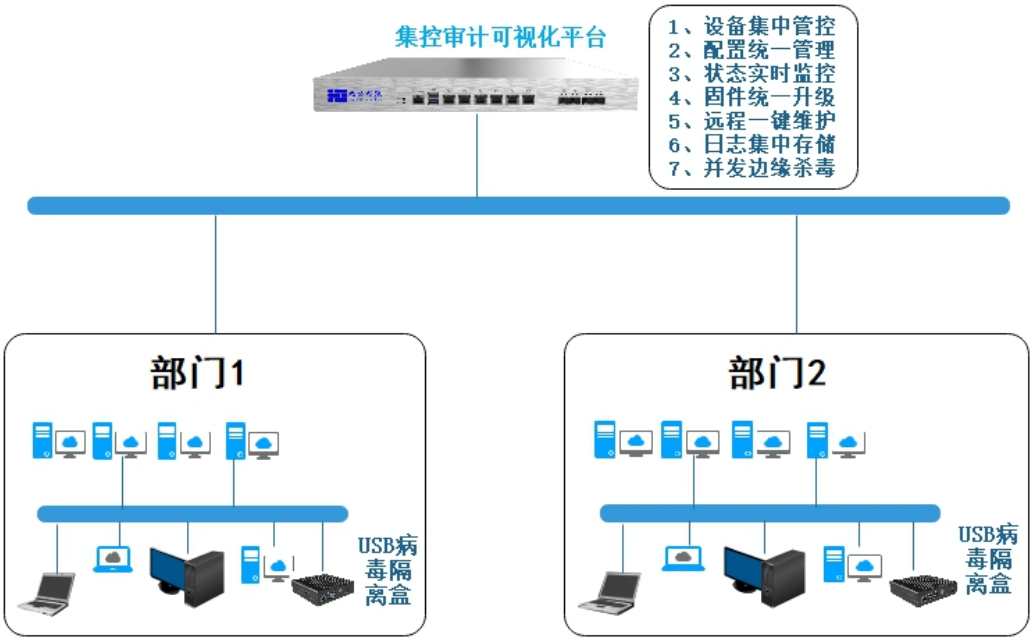
在拥有多台设备的情况下，很难做到配置的统一，繁琐的配置容易导致配置时人为的出错率更高。

二、产品介绍

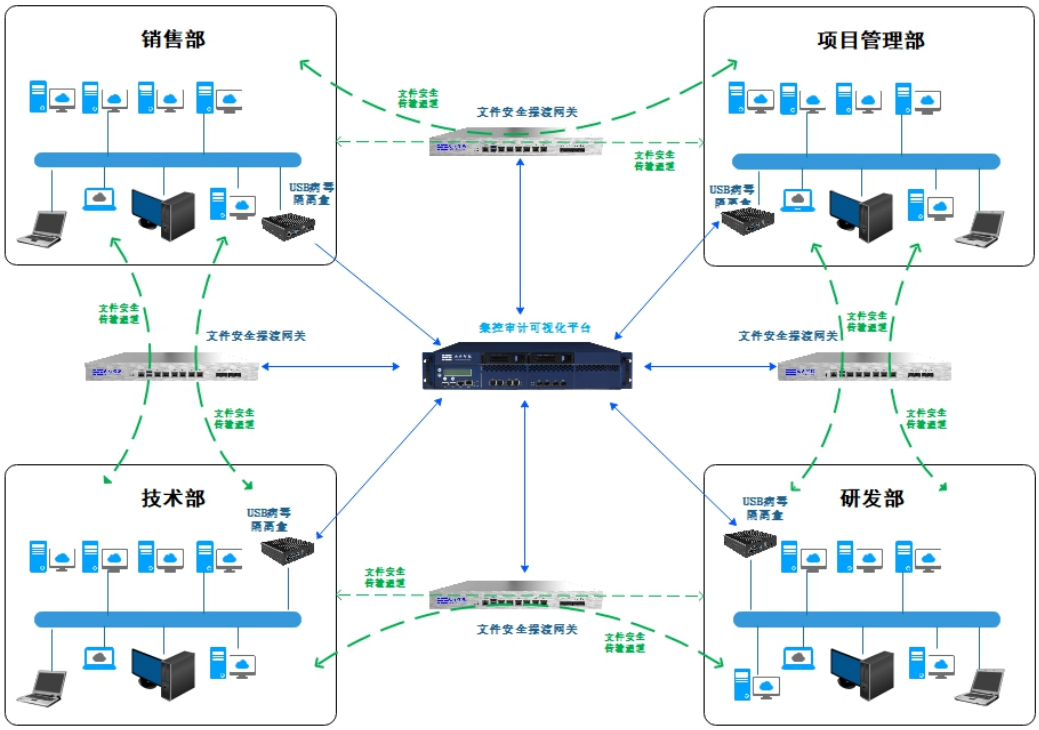
九方智联集控审计可视化平台是一款九方智联完全自主开发的专门针对 USB 病毒隔离盒、USB 外设安全摆渡系统和文件安全摆渡网关进行统一管控的一款的边缘计算产品。

集控审计可视化平台能够管理三种设备，实现高效集控管理。对多个设备的文件白名单管理、USB 移动介质白名单管理、用户权限、文件病毒报警、设备固件统一升级、设备日志、设备维护、设备证书等功能进行集控管理，实现了一平台多设备管控的高效工作理念。

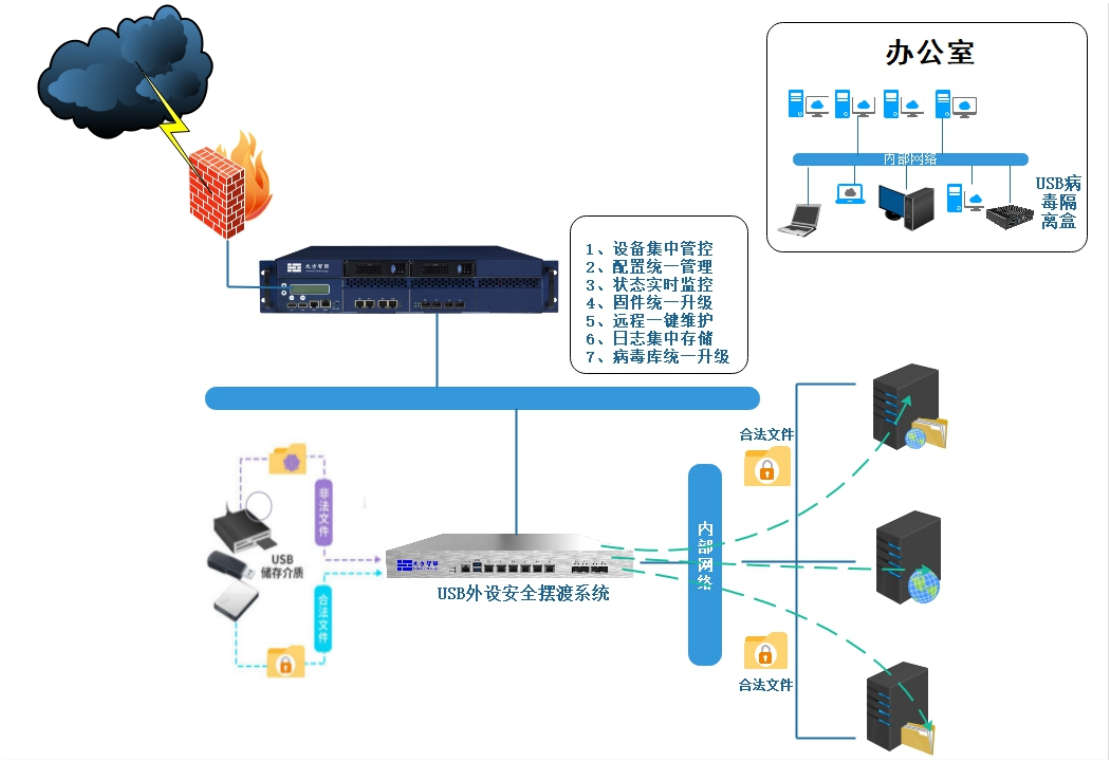
三、使用方式及场景



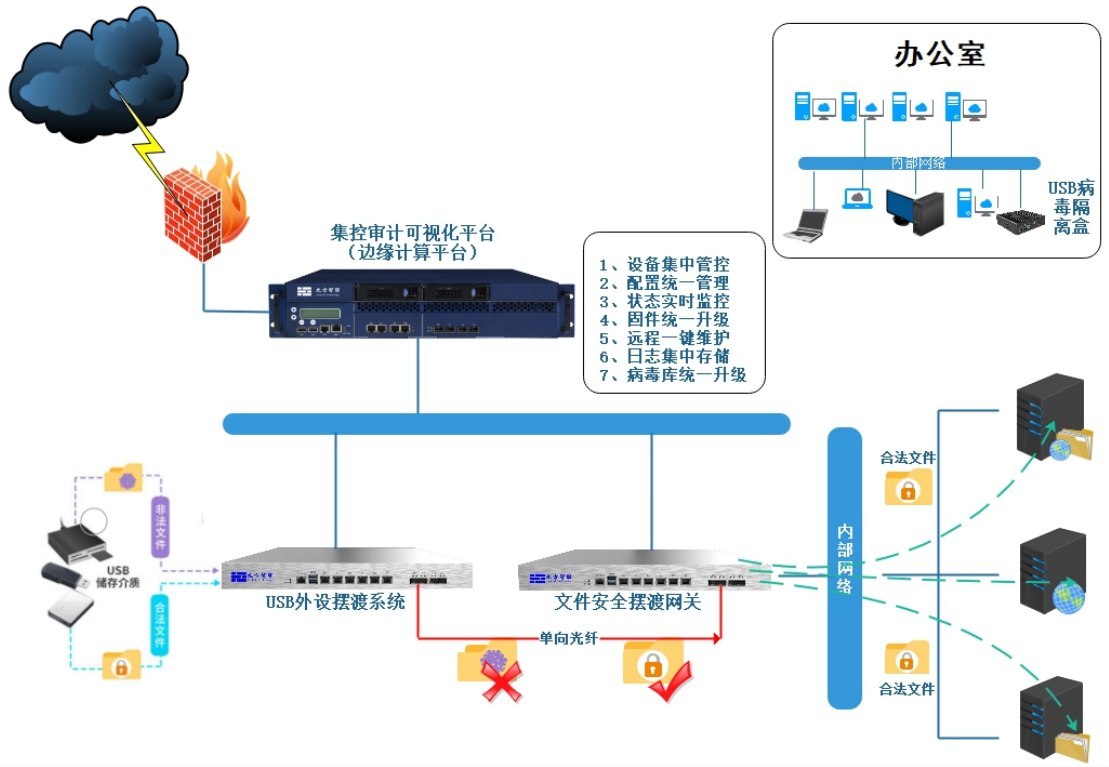
应用场景 1



应用场景 2


办公室
内部网络
USB病毒隔离盒
1、设备集中管控
2、配置统一管理
3、状态实时监控
4、固件统一升级
5、远程一键维护
6、日志集中存储
7、病毒库统一升级
合法文件
非法文件
USB储存介质
USB外设安全摆渡系统
内部网络
合法文件
合法文件

应用场景 3


办公室
内部网络
USB病毒隔离盒
集控审计可视化平台
（边缘计算平台）
1、设备集中管控
2、配置统一管理
3、状态实时监控
4、固件统一升级
5、远程一键维护
6、日志集中存储
7、病毒库统一升级
非法文件
USB储存介质
合法文件
USB外设摆渡系统
文件安全摆渡网关
单向光纤
内部网络
合法文件
合法文件

应用场景 4

四、功能指标

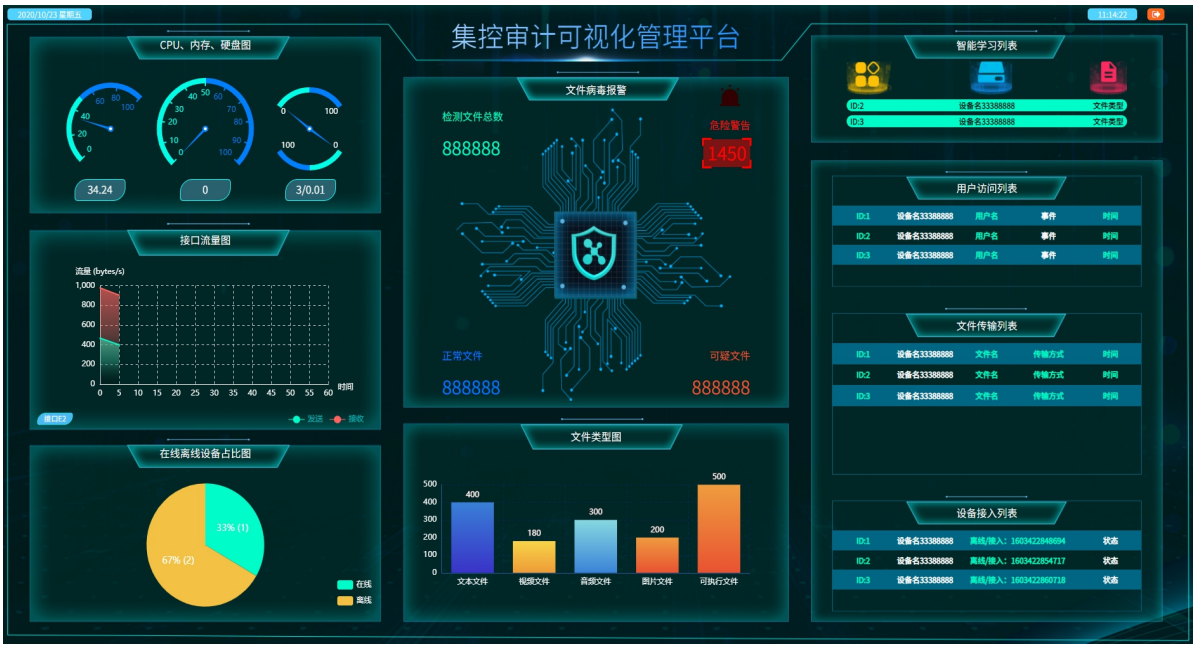
功能		特性说明
态势感知	CPU、内存、磁盘图	提供了集控审计可视化管理平台的 CPU、内存、磁盘状态。
	接口流量图	提供集控审计可视化管理平台发送接收数据流量。
	在线离线设备占比图	提供在线离线设备的占比图。
	文件病毒报警	提供文件病毒报警。数量变化来自与日志，删除对应日志便减少。
	文件类型图	提供各类型文件柱状图。数量变化来自与日志，删除对应日志便减少。
	智能学习列表	提供各设备智能学习文件白名单监控。点文件智能学习发布后生效。
	用户访问列表	提供各设备使用者操作行为监控。提供 WEB 访问操作监控。
	文件传输列表	提供各设备文件传输实时监控。
	设备接入列表	提供已接入态势感知平台设备列表。
系统管理	状态	查看基本信息、设备运行状态图等。
	设置	设置时间、双击热备。
	管理员	设置平台的用户、权限、黑名单等。
	维护	配置备份、恢复、固件升级、重启设备
	工具	Ping、traceroute、arping
网络设置	接口	设置接口
	路由	设置静态路由
	DNS	设置 DNS、SecROS 简域
	会话	查看会话，设置 ARP、高级选项
	链路	WAN 链路监控，设置链路连接
数字证书	本机证书	新建、导入、导出本机证书
	证书库	新建、吊销、删除、导出设备证书
	CA 证书	新建、删除、导入、导出 CA 证书
	证书作废表	导出导出删除作废证书
设备管理	USB 病毒隔离盒	新建、修改、删除 USB 病毒隔离盒设备

	USB 外设安全摆渡系统	新建、修改、删除 USB 外设安全摆渡系统设备
	文件安全摆渡网关	新建、修改、删除文件安全摆渡网关设备
白名单管理	**文件白名单**	自定义文件白名单
	USB 白名单	配置 USB 白名单
策略权限	**文件策略**	设置安全策略，发布
	文件智能学习	智能学习文件类型
	用户权限	自定义设备用户权限
边缘杀毒	**防病毒许可证**	设置防病毒许可，病毒库升级
远程维护	**在线维护**	远程访问已连接设备，重启设备
	统一升级	统一升级设备
日志审计	**平台日志**	平台操作日志
	设备日志	所有已连接的设备日志

五、功能优势

1、态势感知：

态势感知页面实时监控平台的 CPU、内存、磁盘状态，平台发送接收数据流量。设备的在线离线占比图，文件病毒报警。提供各类型文件柱状图。设备智能学习文件列表，用户访问监控。各设备文件传输实时监控，接入态势感知平台设备列表监控。



2、多设备统一管理：

集控审计可视化平台能对所有接入的集控审计可视化管理平台进行统一配置管理、固件升级、病毒库更新及远程维护，并能将所有日志记录包括 Web 传输日志，FTP 传输日志、操作日志、文件共享传输日志、摆渡日志、单向光导日志以及病毒查杀日志进行统一存储，协助网络管理员对文件来源进行审计记录，有效查找病毒源。

3、安全策略一键下发：

集控审计可视化管理平台内置病毒检测模块，对插入的移动存储识别进行实时病毒查杀，目前已有病毒特征库 1300 万种以上，能有效查杀包括勒索病毒及其变种等各类病毒，并支持联网在线升级病毒库及离线导入病毒库。

4、边缘杀毒与病毒库统一在线离线升级：

集控审计可视化管理平台创新边缘杀毒技术，内置病毒检测模块，能协助 USB 病毒隔离盒进行文件杀毒扫描，对插入的移动存储识别进行实时病毒查杀，目前已有病毒特征库 1300 万种以上，能有效查杀包括勒索病毒及其变种等各类病毒，并支持联网在线升级病毒库及离线导入病毒库。

5、完善的日志审计：

集控审计可视化管理平台收集所有设备的日志审计记录，能对用户的所有访问信息进行记录，包括 Web 传输日志，FTP 传输日志、操作日志、文件共享传输日志、摆渡日志、单向光导日志以及病毒查杀日志，协助网络管理员对文件来源进行审计记录，并有效查找病毒源。

六、产品参数

1. 多类别设备统一管理

支持 USB 病毒隔离盒、USB 外设安全摆渡系统以及文件安全摆渡网关的统一接入。

2. 多种认证方式：

支持 ID/密码以及证书两种认证方式。

3. 支持国密证书及国密算法：

支持使用 SM2 国密数字证书做 SM2 非对称加密，并支持 SM3 杂凑算法和 SM4 对称加密算法。

4. 创新边缘杀毒技术：

能利用平台自身强大的计算能力，为 USB 病毒隔离盒提供边缘杀

毒功能。

5. 个性化安全策略：

支持自定义配置，指定设备，指定文件白名单、USB 白名单、用户、病毒处理策略等。

6. 统一升级与远程维护：

对于所有接入平台的设备，通过导入升级固件文件，就能对相应型号的设备进行统一升级。

7. 完善的审计日志

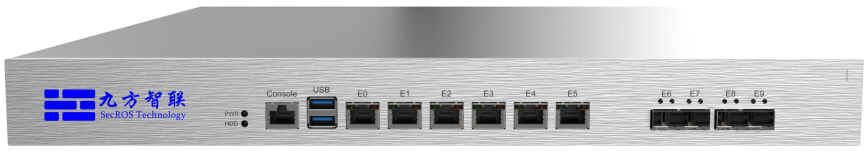
平台能存储所有接入设备的相关日志审计记录，包括用户的访问、Web 传输，FTP 传输、文件摆渡、文件共享传输、单向光导以及病毒查杀等日志。

七、产品选型与介绍

7.1 CAVP10

CAVP10 是一款标准 1U 机架式平台管控产品，支持 USB 病毒隔离盒、USB 外设安全摆渡系统、文件安全摆渡网关的统一接入认证，策略自定义、USB 准入控制、文件智能学习、安全认证、数据加密、用户配置、边缘杀毒、病毒库统一升级、在线设备维护、日志审计为一体的软硬件平台。基本配置包括 6 个千兆电口，1 个配置口，2 个 USB3.0 接口，采用 Intel X86 架构高速网络处理器。最大数据吞吐率 200Mbps，最大并发会话数 300,000，最大设备接入数 30，最大防病毒并发检测数 10。

7.2 CAVP30



CAVP30 是一款标准 1U 机架式平台管控产品，支持 USB 病毒隔离盒、USB 外设安全摆渡系统、文件安全摆渡网关的统一接入认证，策略自定义、USB 准入控制、文件智能学习、安全认证、数据加密、用户配置、边缘杀毒、病毒库统一升级、在线设备维护、日志审计为一体的软硬件平台。基本配置包括 6 个千兆电口，4 个 SFP 光口，1 个配置口，2 个 USB 接口，采用 Intel X86 架构高速网络处理器。最大数据吞吐率 500Mbps、最大并发会话数 500,000，最大设备接入数 80，最大防病毒并发检测数 30。

7.3 CAVP100

CAVP100 是一款标准 2U 机架式万兆外设安全摆渡产品，支持 USB 病毒隔离盒、USB 外设安全摆渡系统、文件安全摆渡网关的统一接入认证，策略自定义、USB 准入控制、文件智能学习、安全认证、数据加密、用户配置、边缘杀毒、病毒库统一升级、在线设备维护、日志审计为一体的软硬件平台。基本配置包括 4 个千兆电口，4 个万兆 SFP 光口，1 个配置口，2 个 USB3.0 接口，采用 Intel X86 架构高速硬件平台。最大数据吞吐率 20Gbps，最大并发会话数 2000,000，最大设备接入数 500，最大防病毒并发检测数 100。