

九方智联 USB 病毒隔离盒

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。

二、产品介绍

九方智联 USB 病毒隔离盒是一款由深圳市九方智联科技有限公司完全自主研发的专门针对 USB 存储器进行病毒隔离及查杀的产品，其通过控制 USB 移动存储介质的授权合法接入，对存储介质中的数据文件进行有效控制及实时查杀隔离并告警，并对上传下载的数据文件进行记录审计，能有效的防止 USB 移动存储器上的文件携带病毒进入内网，究根溯源，提高了内网的安全，避免出现安全事故。

三、产品形态

1、桌面型



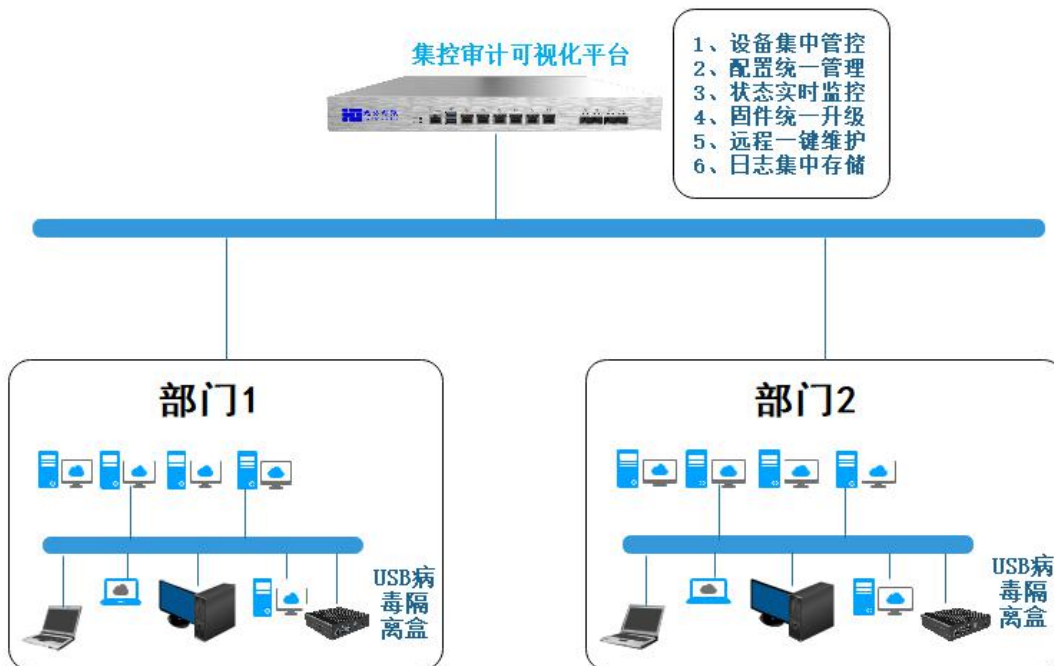
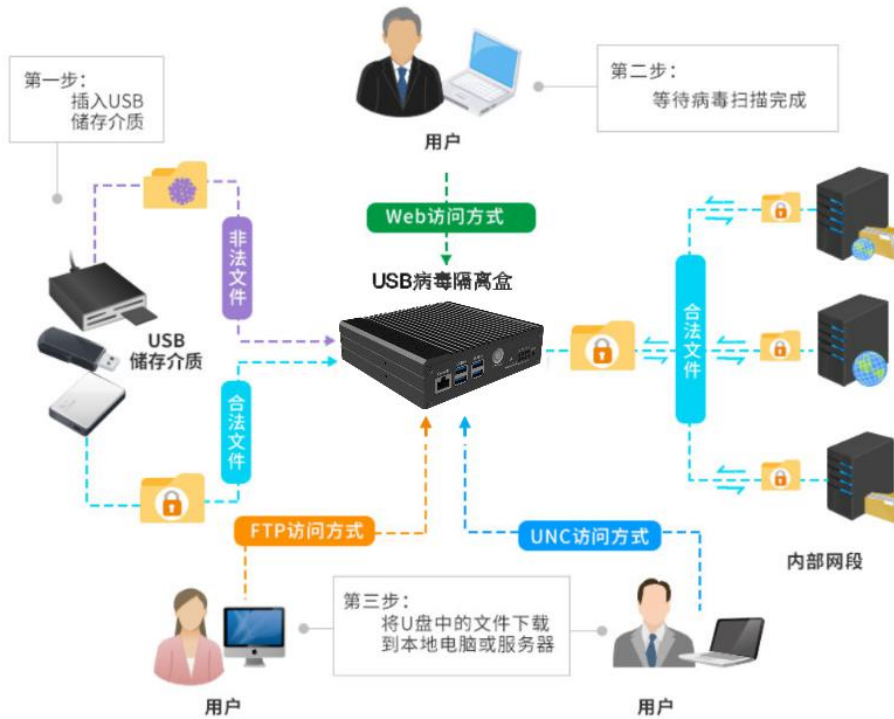
桌面型一般应用于网络共享环境，办公人员通过网络对插入的USB 存储介质进行访问。

2、光驱型



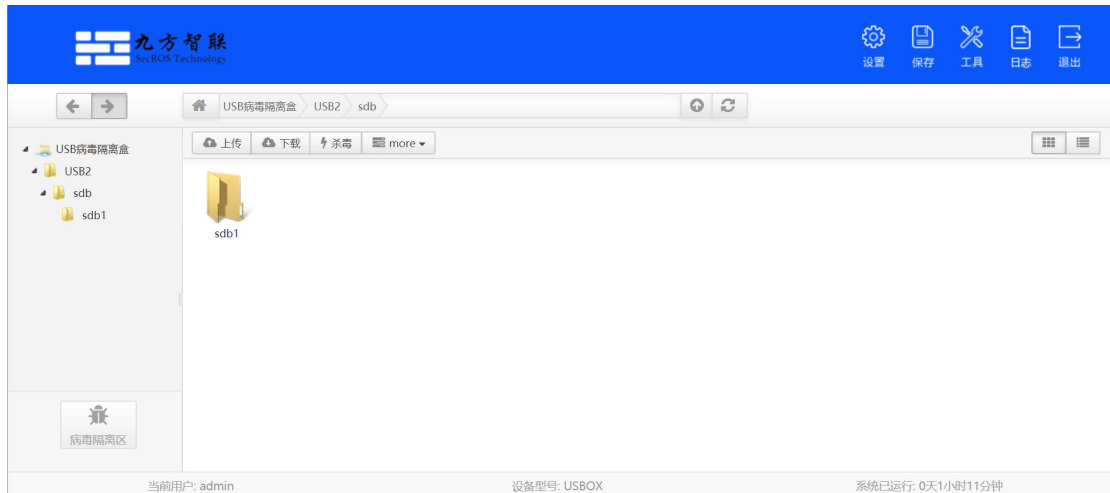
光驱型产品适用于和服务器集成，可以内置于传统服务器的光驱位，其由服务器上的电源 4Pin 接口进行供电，并通过服务器主板上的 USB3.0 接与隔离盒后面板上的 USB 口连接后进行访问。

四、使用方式及场景

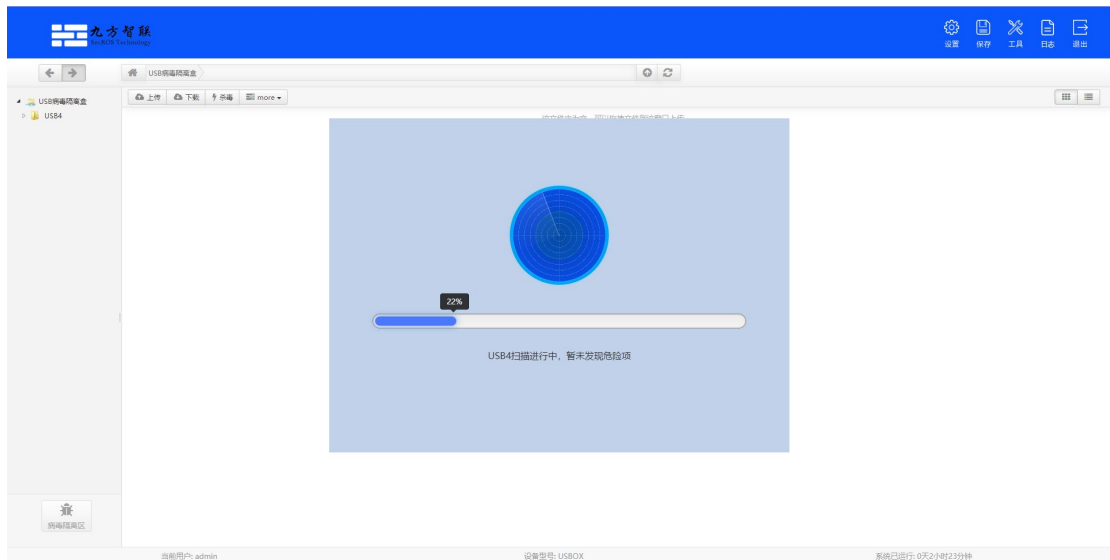


五、产品界面

插入 U 盘



等待 U 盘病毒扫描完成



六、功能说明

功能		特性说明
系统设置	系统设置	查看设备序列号、系统版本、系统运行状态灯信息
	固件升级	升级固件
网络设置	网络设置	修改接口 IP 地址、子网掩码和网关
文件管理	文件白名单	支持常见的视频类文件格式
		支持常见的音频类文件格式
		支持常见的图片类文件格式
		支持特殊的自定义文件格式
	文件智能学习	支持对特殊的自定义文件类型进行深度学习
USB 管理	USB 准入策略	允许所有的U盘接入或者只允许USB白名单列表中的U盘接入
	USB 白名单	可通过USB口插入的U盘进行白名单配置
用户管理	用户管理	用户添加、删除、修改
	权限管理	上传下载删除等权限设置
病毒防护	病毒防护	定义病毒检测方式、处理策略及压缩文件处理策略
	病毒库升级	支持在线或离线升级病毒库
远程日志	远程日志	支持通过syslog工具发送日志给远程日志服务器
密码修改	密码修改	对当前登录用户的密码进行修改
集审平台	集审平台	支持统一接入集审平台进行统一配置管控,日志集中存储,远程维护

七、产品优势

1、灵活多样的访问方式：

支持 Windows 或者苹果 Mac 等操作系统的 PC 主机使用 FTP 客户端，文件共享或者 Web 浏览器直接进行数据访问下载。无需在 PC 主机上安装任何驱动，减少对主机的影响，设备安全稳定随时可进行相关文件过滤访问，保障内网安全性。

2、多用户多安全策略：

可定义用户直接访问 USB 存储设备对文件进行如读、写、删除、重命名等多方面的安全操作，同时可设置 USB 存储数据读写有单独的密码，防止内部文件非法操作拷贝；多用户通过网络共享方式访问 USB 隔离盒，可以多人同时使用同一个隔离盒，隔离盒上多个 USB 口可以同时进行访问读写。



3、安全隔离过滤：

隔离盒采用嵌入式硬件架构，实时监控主机 USB 接口的接入情况，

对于非法移动存储设备的接入进行屏蔽，杜绝移动存储病毒的传播，安全有效地把内、外部网络隔离，通过独有的数据传输协议，保证文档数据传输的安全性。

4、文件白名单过滤：

实现对隔离盒所有 USB 接口操作全面的扫描和过滤，内置基于文件内容深度检测算法能准确快速识别病毒伪装文件，保证对 USB 移动存储介质访问的安全性，高效安全阻断病毒通过 USB 移动存储介质进行传输的可能性，从而保证内网的安全性。白名单过滤对所有 PC 通过 USB 接口移动存储设备进行的读取和写入操作进行分析和过滤，支持目前主流的音视频、图片、文档、P2 卡等多种格式。



5、U 盘准入策略：

USB 病毒隔离盒支持 U 盘准入策略配置，通过添加 U 盘白名单的方式，只允许通过授权的 USB 存储介质的安全接入，有效杜绝非法 U 盘、移动硬盘等移动存储介质的非法接入，对于非法移动存储设备的

接入进行屏蔽，为内网安全保驾护航。



6、文件智能学习：

USB 病毒隔离盒支持文件智能学习，对于模式匹配库中没有的文件类型，可以通过自主学习的方式，将文件导入系统中进行学习，学习完成之后，模式库中就加入了该种文件的特征码，以后的文件检查过程就能顺利识别出学习过的文件类型。



7、病毒检测与病毒库在线升级：

USB 病毒隔离盒内置病毒检测模块，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。



八、相关参数



1. 嵌入式架构：

采用嵌入式 linux 硬件架构高速网络处理器，基本配置包括 4 个 USB3.0，1 个 1000M 网络接口，并支持多种卡槽格式外接存储接入如 TF、M2、MICO SD、SD、MS、MMC、XD、CF 等存储介质；

2. 文件白名单过滤：

内置常见的 doc、docx、xls、xlsx、mpeg、mpg、rm、m4v、asf、mov、avi、swf、wav、mp3、mp4、mid、ac3、bmp、jif、jpg、png 等 100 多种格式文件并支持文件过滤格式可自定义；

3. 深度检查：

支持深度过滤检测，防止修改文件后缀名欺骗；

4. 多种访问方式:

支持 UNC 文件共享、FTP 和 WEB 三种方式访问，可通过网上邻居、FTP 客户端或者 Web 浏览器访问外接存储介质

5. 用户权限管理:

支持多用户接入并可对不同用户访问进行权限划分，如文件上传下载、文件编辑、查看、新建、复制、粘贴、删除、重命名等操作。

6. USB 准入管理:

通过配置 U 盘准入策略，通过 USB 白名单的管理，有效杜绝 U 盘等存储介质的非法接入。

7. 文件智能学习:

对于模式匹配库中没有的文件类型，可以通过自主学习的方式，将文件导入系统中进行学习

8. 病毒检测与病毒库在线升级:

USB 病毒隔离盒内置病毒检测模块，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。

9. 完善的审计日志

USB 病毒隔离盒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、文件共享传输日志已经病毒查杀日志，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。

10.支持集中管控

USB 病毒隔离盒支持统一接入集控审计可视化平台进行集中管控。通过集控审计可视化平台，能够实现对所有设备的配置进行统一管理、实时了解设备运行状态、对文件传输状态进行存储统计，并能实现固件统一升级及维护。

九、版本功能参数对比表

版本 功能	标准版	集审版	专业版	国密版
产品外观	桌面型/光驱型	桌面型/光驱型	桌面型	桌面型
支持多用户	●	●	●	●
权限配置	●	●	●	●
文件白名单	●	●	●	●
文件智能学习	●	●	●	●
文件深度检测	●	●	●	●
U 盘准入	●	●	●	●
U 盘容量显示	●	●	●	●
HTTP 访问	●	●	●	●
FTP 访问	●	●	●	●
UNC 访问	●	●	●	●
本地日志审计	●	●	●	●
HTTPS 访问		●	●	●
支持本地杀毒			●	●
支持边缘杀毒*		●		
支持集中管控*		●	●	●
支持日志集中审计*		●	●	●
支持策略统一管理*		●	●	●
支持态势感知与预警*		●	●	●
加密 U 盘隔离			●	●
支持国密算法证书*				●
支持国密 SM2 算法*				●
支持国密 SM3 算法*				●
支持国密 SM4 算法*				●

注：有*号标注的功能项需要配合集控审计可视化平台使用