网络机房信息安全设备厂家 网络机房信息安全隔离器

产品名称	网络机房信息安全设备厂家 网络机房信息安全隔离器
公司名称	北京七叶子科技有限公司
价格	70000.00/套
规格参数	
公司地址	北京市顺义区龙湾屯镇府前街13号北楼482
联系电话	15330050692

产品详情

产品介绍

USB病毒隔离器就是来隔离不可信网络与内部网络，过滤USB移动存储上素材文件，防范病毒而研发的信息安全产品。它通过网络接口与内部网络连接，使用国际标准的网络协议来和PC主机连接。内置过滤软件，将常见的素材文件作为白名单格式，移动存储上所有的文件都将经过白名单比对检测后才能显示，操作拷贝进网。任何一台能连通网络的主机，无论windows还是苹果还是其他操作系统，都可以通过标准的ftp客户端或者浏览器来访问USB病毒隔离器上插入的移动存储的内容（也可以采用单机方式*。它能有效地防止usb移动存储上的文件携带病毒对于PC主机带来的威胁。

新维讯XSEC USB3安全隔离器是一款基于ARM微处理器开发的隔离设备。它通过控制病毒传播途径--移动存储传播，实现病毒隔离。它采用USB接口和网络接口进行USB安全隔离和行为管理，USB隔离能有效地杜绝移动介质病毒传播；

策略可配置的“ 白名单 ”和“ 黑名单 ”相结合方式；

文件深度检测以及完善的行为管理日志；根据文件的机密性,用户可选择对指定文件类型进行加密管理；

产品可满足不同行业和网络环境下的多元化病毒隔离和文件安全需求。

新维讯XSEC USB3安全隔离器就是来解决USB移动存储上素材能可控、防病毒进入而研发的信息安全产品。它通过网络接口与编播网络连接，使用国际标准的网络协议来和PC主机连接，无需在主机上安装任何软件。内置过滤软件，将常见的素材文件作为白名单格式，移动存储上所有的文件都将经过白名单比对检测后才能显示，进而人工拷贝进网。任何一台能连通网络的主机，无论windows还是苹果还是其他操作系统，都可以通过浏览器来访问USB防毒盒上插入的移动存储的内容（也可以采用单机方式*）。它能有效地防止usb移动存储上的文件携带病毒对于PC主机带来的威胁。

产品特点

1.灵活访问支持Windows或者苹果Mac等操作系统的PC主机使用FTP或者Web浏览器直接进行数据访问下载。避免在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素材过滤访问，保障内网安全性。2.嵌入式专用系统新维讯XSEC USB3安全隔离器是基于ARM微处理器开发的安全设备，采用专用的硬件平台和软件系统相结合的方式，能够有效地杜绝病毒通过移动存储传播，支持7*24小时工作。3.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新维讯XSN USB安全隔离器，可以多人同时使用同一个隔离器，隔离器上多个USB口可以同时进行访问读写。4.安全隔离过滤新维讯XSEC USB3安全隔离器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，保证素材传输的安全性。5.基于文件内容的深度检测 新维讯XSEC USB3安全隔离器支持常用的视频、音频、图片及文本格式文件，如：MPEG2,AVI，TGA，BMP,JPG，DOC,TXT等多种格式，支持对已知文件的深度特征检测，严格过滤掉病毒伪装的文件。支持文件类型升级及定制文件类型。6.白名单过滤新维讯XSN USB安全隔离器对所有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，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。

部署示例

接到网络主干上，可以多人同时使用一台设备。病毒隔离器配置有网络接口（1000M，接入到网络中，所有访问该设备的PC都可以通过FTP客户端或者WEB浏览器来访问插在盒子上的USB存储。